

**Ανοικτό Πανεπιστήμιο Κύπρου**  
**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακή Διατριβή**  
**Στην Ασφάλεια Υπολογιστών και Δικτύων**



**Building Societal Resilience Against Phishing Attacks**  
**Χλόη Ζαχαριάδη**

**Επιβλέπων Καθηγήτρια**  
**Ιλιάννα Σταύρου**

**Μήνας Έτος**  
**Μάης 2023**

**Ανοικτό Πανεπιστήμιο Κύπρου  
Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

## **Μεταπτυχιακή Διατριβή**

**Building Societal Resilience Against Phishing Attacks**

**Χλόη Ζαχαριάδη**

**Επιβλέπων Καθηγήτρια**

**Ιλιάννα Σταύρου**

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε  
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών

στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών

του Ανοικτού Πανεπιστημίου Κύπρου

**Μήνας Έτος**

**Μάης 2023**



## Summary

Phishing attacks remain a huge threat and are becoming more prevalent every year. Phishing attacks are increasing and are becoming more frequent, events that hinder the ability of cybersecurity operations to effectively defend against them. The term 'phishing' comes from the concept of hackers 'fishing' for sensitive information by creating "bait" in the form of deceptive emails and texts.

Investigate phishing attacks before or during expected or unexpected social, political, economic events and create targeted information to effectively understand and address the problem. Despite awareness efforts by cybersecurity organizations, phishing attacks are still successful at the expense of much of society.

The main axes analyzed are the overview of phishing attacks by classifying them, based on events and population groups. Further identified and analyzed existing classifications. Also, included tables and figures from existing studies. Phishing attacks are categorized based on the main features used. Additionally, searched topics like phishing scams related to COVIT-19 and disinformation during the pandemic, etc., and investigated phishing attacks before the pandemic. Also, list the key characteristics of the attacks and then list the key information in a table. A list of anti-phishing countermeasures, e.g., how to recognize red flags for phishing etc. Identify awareness efforts aimed at educating people about phishing attacks.

Finally, evaluating one hundred infographics by collecting and analyzing the qualities through a framework for the overall quality of the awareness material. Analyzing the results and draw our conclusions based on them. In conclusion, by presenting elements for the correct creation of an infographic.

## Περίληψη

Οι επιθέσεις phishing παραμένουν μια τεράστια απειλή και διαδίδονται όλο και περισσότερο κάθε χρόνο. Οι επιθέσεις phishing αυξάνονται και είναι πιο συχνές, γεγονός που εμποδίζει την ικανότητα των λειτουργιών της κυβερνοασφάλειας να αμύνονται αποτελεσματικά εναντίον τους. Ο όρος 'ψάρεμα' προέρχεται από την έννοια των χάκερ που «ψαρεύουν» ευαίσθητες πληροφορίες δημιουργώντας «δόλωμα» με τη μορφή παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου και κειμένων.

Διερευνούμε τις επιθέσεις του ηλεκτρονικού ψαρέματος πριν ή κατά τη διάρκεια αναμενόμενων ή αναπάντεχων κοινωνικών, πολιτικών, οικονομικών γεγονότων και η δημιουργία στοχευμένης ενημέρωσης για αποτελεσματική κατανόηση και αντιμετώπιση του προβλήματος. Παρόλες τις ενημερωτικές προσπάθειες από μέρους των οργανισμών κυβερνοασφάλειας, οι επιθέσεις ηλεκτρονικού ψαρέματος εξακολουθούν να είναι επιτυχημένες εις βάρος μεγάλου μέρους της κοινωνίας.

Οι κυριότεροι άξονες που θα αναλύσουμε είναι η επισκόπηση των επιθέσεων του ηλεκτρονικού ψαρέματος ταξινομώντας τις, με βάση τα γεγονότα και τις ομάδες του πληθυσμού. Έχουμε προσδιορίσει και αναλύσει τις υπάρχουσες ταξινομήσεις. Επίσης, έχουμε συμπεριλάβει πίνακες και σχήματα από υπάρχουσες μελέτες. Τις έχουμε κατηγοριοποίηση με βάση τα βασικά χαρακτηριστικά που χρησιμοποιήσαμε. . Πραγματοποιήσαμε αναζήτηση σε θέματα όπως απάτες ηλεκτρονικού ψαρέματος που αφορούν το COVID-19 και την παραπληροφόρηση κατά τη διάρκεια της πανδημίας κ.λπ. Διερευνήσαμε επίσης τις επιθέσεις ηλεκτρονικού ψαρέματος πριν από την πανδημία. Ακόμη αναφέρουμε τα βασικά χαρακτηριστικά των επιθέσεων και, στη συνέχεια, να καταχωρούμε τις βασικές πληροφορίες σε έναν πίνακα.

Επίσης αναφέρουμε αντίμετρα κατά του phishing π.χ. πώς θα αναγνωρίσουμε κόκκινες σημαίες για μηνύματα ηλεκτρονικού ψαρέματος κ.λπ. Ακόμη θα προσδιορίσουμε προσπάθειες ευαισθητοποίησης που στοχεύουν στην εκπαίδευση των ανθρώπων σχετικά με επιθέσεις phishing.

Τέλος θα αξιολογήσουμε εκατό infographics συλλέγοντας και αναλύοντας τις ιδιότητες μέσω ενός πλαισίου για την συνολική της ποιότητα του υλικού ευαισθητοποίησης. Θα αναλύσουμε τα αποτελέσματα και βάση αυτών θα βγάλουμε τα συμπεράσματα μας. Εν κατακλείδι θα παρουσιάσουμε στοιχεία για την σωστή δημιουργία ενός infographic.



# CONTENTS

Summary.....	4
Περίληψη.....	5
Chapter 1.....	10
<b>Introduction</b> .....	10
Chapter 2.....	15
<b>Background work and Literature review</b> .....	15
2.1 Phishing taxonomies.....	16
2.2 Phishing attacks.....	30
2.3 Countermeasures against phishing.....	32
2.4 Discussion.....	40
Chapter 3.....	42
<b>Methodology</b> .....	42
Chapter 4.....	46
<b>Design</b> .....	46
4.1 Communication Strategy attribute.....	48
4.2 Behavior – change attributes.....	49
4.3 Presentation attributes.....	51
Chapter 5.....	53
<b>Analysis - Evaluation</b> .....	53
Chapter 6.....	73
<b>Recommendation</b> .....	73
Chapter 7.....	77
<b>Conclusions</b> .....	77
Appendix A.....	1
<b>Analysis Infographics</b> .....	1
A.1 Analysis Infographics 2020.....	2
A.2 Analysis Infographics 2021.....	27
A.3 Analysis Infographics 2022.....	52
A.4 Analysis Infographics 2023.....	77
Bibliography.....	102



# **Chapter 1**

## **Introduction**

Phishing attacks remain a huge threat and are growing more widespread every year. Phishing attacks are increasing and are more common, which hinders the ability of cybersecurity functions to effectively defend against them. The term 'Phishing' is derived from the notion of hackers 'fishing' for sensitive information by creating 'bait' in the form of deceitful emails and texts. Hackers commonly replace 'f' with 'ph' in their online language which is where the exact term comes from. Even though various news, reports, and anti-phishing campaigns attempt to spread awareness and knowledge, people still fall victim to novel phishing methods. There are many kinds of phishing attacks such as fake websites, spear phishing, deceptive phishing etc. 3.4 billion phishing emails are sent daily, and the annual number goes way beyond one trillion. The figure is growing, and the threats are getting more sophisticated. [1]

Phishing attacks [2] are most common in the form of an email, although mobile-phishing methods are quickly on the rise. 96% of phishing attacks arrive by email. The 3% are malicious websites and just 1% via phone. When it's done over the telephone, it is called vishing and when it's done via text message, it is called smishing. Phishing typically involves a criminal impersonating a well-known brand to encourage victims to either click a certain link that will allow the hacker access to their computer or enter sensitive information under false pretenses.

Typical examples include an 'urgent', 'important' or 'take action' style email claiming that you need to perform a specific action. Usually, individuals are targeted with an email or text that at first glance resembles a legitimate communication from a trusted organization, so the cybercriminals manipulate your trust to get you to respond to the panic they've created to capture your sensitive data. [3]

Phishing attacks impact many actors, from individual victims to companies and government agencies. Phishing is a type of social engineering attack that is used to steal user data, including login credentials and credit card numbers. That happens when an attacker, pretending to be a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Attackers always take the benefit of human factors that generally ignore the critical warning messages. Some of the driving factors behind these crimes are:

- Banking credential theft of credit card details, CVV number and online credentials for websites like PayPal and eBay etc.
- Identity theft- attackers steal sensitive identity details of a person such as ID number etc.
- Trade secrets and confidential document theft targets specific companies to steal sensitive information.
- Notoriety hackers sometimes carry out scams to gain popularity and recognition among peers.

Phishing attacks statistics reveal that users open only 3% of their spam emails, while 70% of them open and read their phishing emails. More than 50% of those who open spear-phishing emails click on malicious links within an hour of receipt. Despite the ever-evolving sophistication with which phishing scammers innovate, phishing strategies can never be 100% successful. They are close, however, phish statistics show that spear-phishing emails work because they are believable. Often, the user on the receiving end doesn't know what to watch out for. Despite awareness efforts by cybersecurity organizations, phishing attacks continue to be successful at the expense of a large portion of society. A recent example is the coronavirus pandemic, which has given food for malicious individuals to create multiple baits and fool unsuspecting citizens and organizations.

A phisher may use public resources, especially social networks, to collect background information about the personal and work experience of their victim. These sources are used to find information such as the potential victim's name, job title, and email address, as well as interests and activities. The attacker can then use this information to create a reliable fake message. Typically, the emails the victim receives appear to come from a known contact or organization. Attacks are carried out through malicious attachments and links to malicious

websites. Scammers often set up fake websites, which appear to be owned by a trusted entity like the victim's bank, workplace, or university. Through these websites, attackers attempt to collect private information like usernames and passwords, or payment information. Some phishing emails can be identified due to poor copywriting and improper use of fonts, logos, and layouts. However, many attackers are becoming more sophisticated at creating authentic looking messages and are using professional marketing techniques to test and improve the effectiveness of their emails.

With so much of our lives taking place online, especially with Covid-19 pandemic, attackers are getting increasingly inventive, using social engineering to persuade consumers to hand over information. That's why many organizations prepared a scary yet necessary list of phishing statistics to show you how sophisticated such schemes are anymore and hopefully, to give you an upper hand in your attempts to stay safe online individually and professionally. Also, cybersecurity companies have identified several campaigns by hackers who are attempting to exploit concerns about the COVID-19 outbreak for their own criminal ends. Crooks often use current affairs to make their scams timelier.

The strengthening of society's resilience to phishing attacks through targeted awareness of the possibility of such attacks before or during expected or unexpected social, political, economic events and crises. The paper will also investigate the practices used by organizations that inform citizens about cyber security issues and especially regarding phishing. Subsequently, targeted information material will be created which will be a model for effective countering of phishing.

Many organizations including ENISA, EUROPOL, SANS Institute and Cyber Safe Work, produce and distribute infographics to raise the Cybersecurity awareness of people. In addition, the infographic design and assessment are also massive based on unsystematic approaches. Consequently, this study examines and analyzes the properties that can guide or be useful for cybersecurity awareness infographic design and its quality. In the following chapters will develop an infographic framework to analyze one hundred infographics. Subsequently, by collecting the data of the analysis, creating graphs, and examining the results. Furthermore, listing ways to create the

right design of an infographic so, can individuals and employees be informed about phishing attacks. [4], [5]

# **Chapter 2**

## **Background work and Literature review**

## 2.1 Phishing taxonomies

Phishing attacks are divided into several categories, the most clickable phishing email in the U.S, Europe, Middle East, and Africa are the business phishing emails. In U.S phishing emails, the subjects that are most populated are focused on security alerts that are related to passwords and internal company policy charges. On the other hand, the top subjects in Europe are related to the user's everyday tasks such as more personalized subjects that are interesting to users. The subjects that business phishing emails are using for their attacks are by sending accept invitations such as staff meetings, employee portals, enclosed attachments, immediate password verification required and 'company name' invoice.

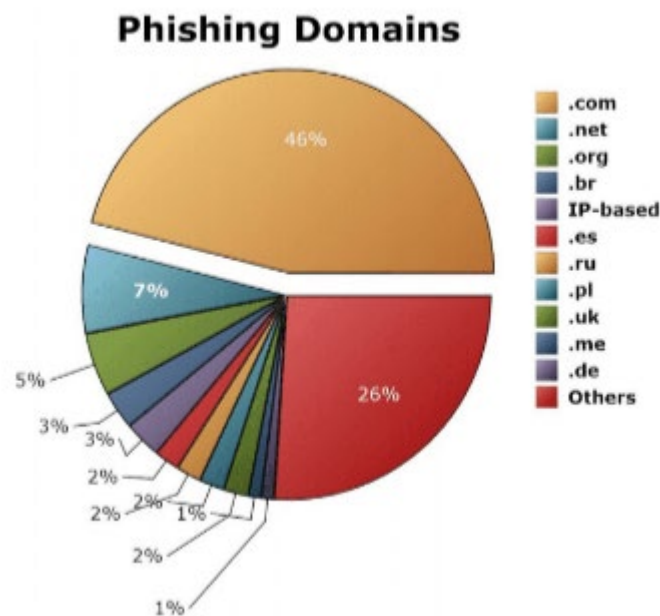
The top email categories on phishing attacks are shown below:

- Banking and Finance
- Online Services
- Human Resources
- IT
- Business
- Coronavirus/COVID-19 Phishing
- Mail Notifications
- Holiday
- Phishing for Sensitive Information
- Social Networking



**Image 2.1.1:** Top-clicked phishing email categories by Knowbe4

According to [6] in 2013 Malcovery reported that Facebook, WhatsApp Fargo etc. were the top organizations targeted by the attackers. Consistent to a 2021 analysis of phishing emails, women are less likely to both open and enter their data in a malicious phishing attempt. Allegedly, males are 225% more likely to respond to phishing emails than females. These findings are from the research of a study by Sheng et al. which suggested that men were less susceptible to being caught in a phishing attempt due to their better education in technical areas. However, in 2022 the educational gap in STEM subjects is much smaller and this is no longer the case. The age group 18-25 years are likely to be the attacker's victim. The figure 2.1.2 shows the statistics of phishing websites based on domain in the fourth quarter of 2104 .com (41%) was the most used domain to carry out phishing scams followed by .net (7%), .org (5%) and .br (3%). Phishing statistics of 2015 reported by Google Safe Browsing is that the number of malicious web pages fell from 18454 to 14977 but the number of phishing pages increased by 8707.



**Figure 2.1.2:** Statistics of phishing websites based on domain by E-crime Report 2013 Q4.

Social phishing attacks are increasing through the years because more than 80% of the population is using social media like Facebook, Twitter, and Instagram, so hackers love using it instead of email to gain your personal information or clicking on malicious links.



Figure 2.1.3: Social Phishing Statistics by Inspired eLearning [7]

Symantec’s Internet Security Threat Report 2019 shows spear phishing emails are used by almost 65% of all known groups. The report also tells, that 96% of targeted attacks are carried out for the purpose of intelligence gathering. In 2020 also Symantec reported an enormous spike in COVID-related emails being used. [8]

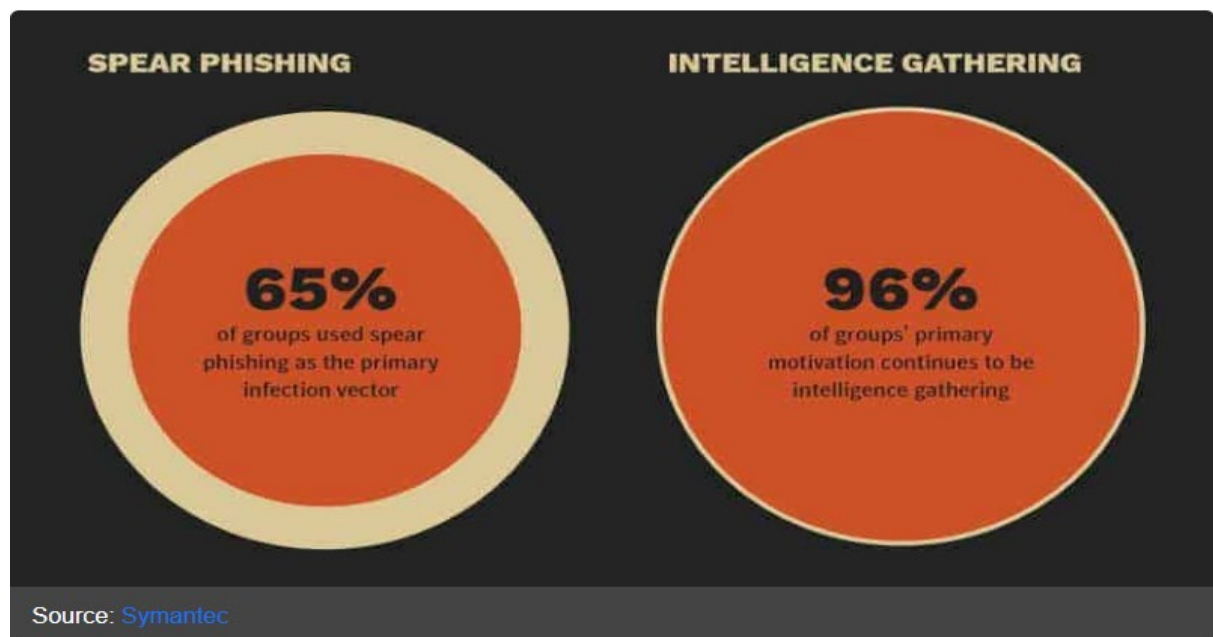
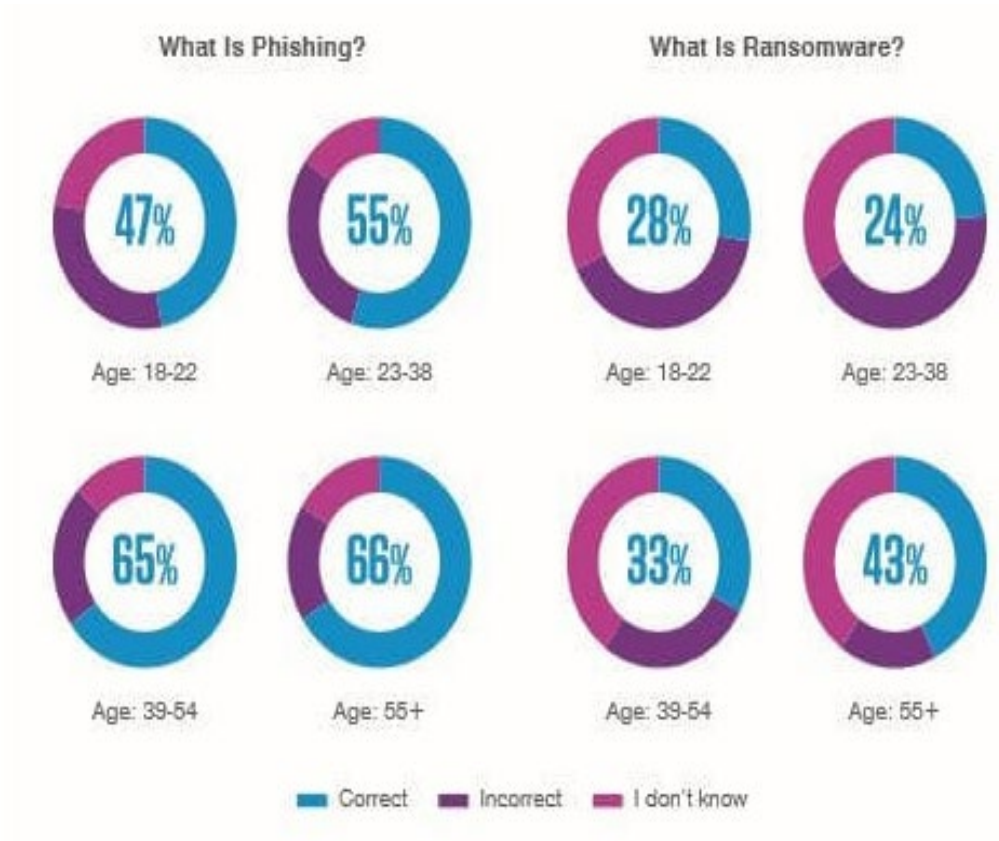


Figure 2.1.4: Symantec statistics about Spear phishing. [8]

Proofpoint provides information about employee knowledge of phishing terms. So, the statistics showed the four age groups, baby boomers (aged 55 plus) were most likely to recognize the terms 'phishing' and 'ransomware'.



**Figure 2.1.5:** Knowledge of phishing terms varies among generations. [8]

Although when it came to the terms ‘smishing’ and ‘vishing’, the older generation was the least likely to know the definitions.

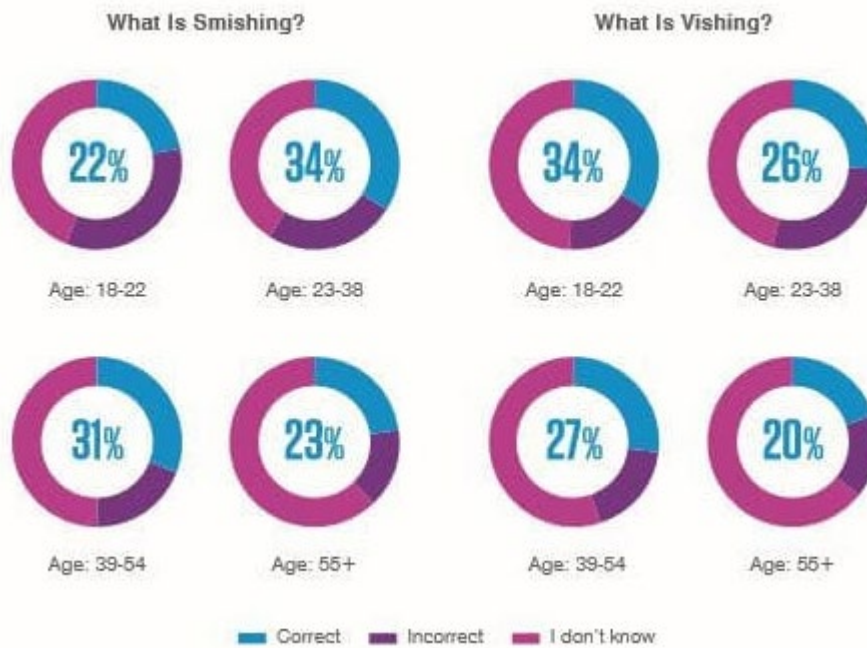


Figure 2.1.6: Smishing terms charts [8]

**Gen Z** has a demographic ranging from ages 11 to 24. Attackers target Gen Z victims and they use social media requests [9] and chatbots to engage with their victims. They're then prompted to make P2P payments like PayPal, unknowingly acting as players within money mule networks. The **Millennials** have also been exposed to technology, so they're generally comfortable with digital interactions. However, they tend to experience identity fraud at greater levels than other generations. According to the FTC, Millennials are 25% more likely than Gen X and Baby Boomers to report losing money to fraud. The victims have ages from 24 to 40 and are more likely to encounter fraud through robocalls and mobile texts. **Gen X** are between the ages of 41 to 65. Although they did not grow up with technology from an early age, they tend to have a considerable amount of experience using technology. However, the range of digital services that they're comfortable using is much narrower than that of Millennials and Gen Z. Some common attacks used to engage with Gen X include robocalls, SMS, and emails. Generation X are more likely to be vulnerable to triggers such as financial information and interest rates. Attackers tend to target **Baby Boomers**, from 57 to 75 years old, using more traditional methods. They usually respond to tactics such as robocalls, while younger generations are easier to reach through other forms of

technology and communications. Some common triggers include attacks related to the IRS, healthcare, social security, credit cards, and consumer warranties.

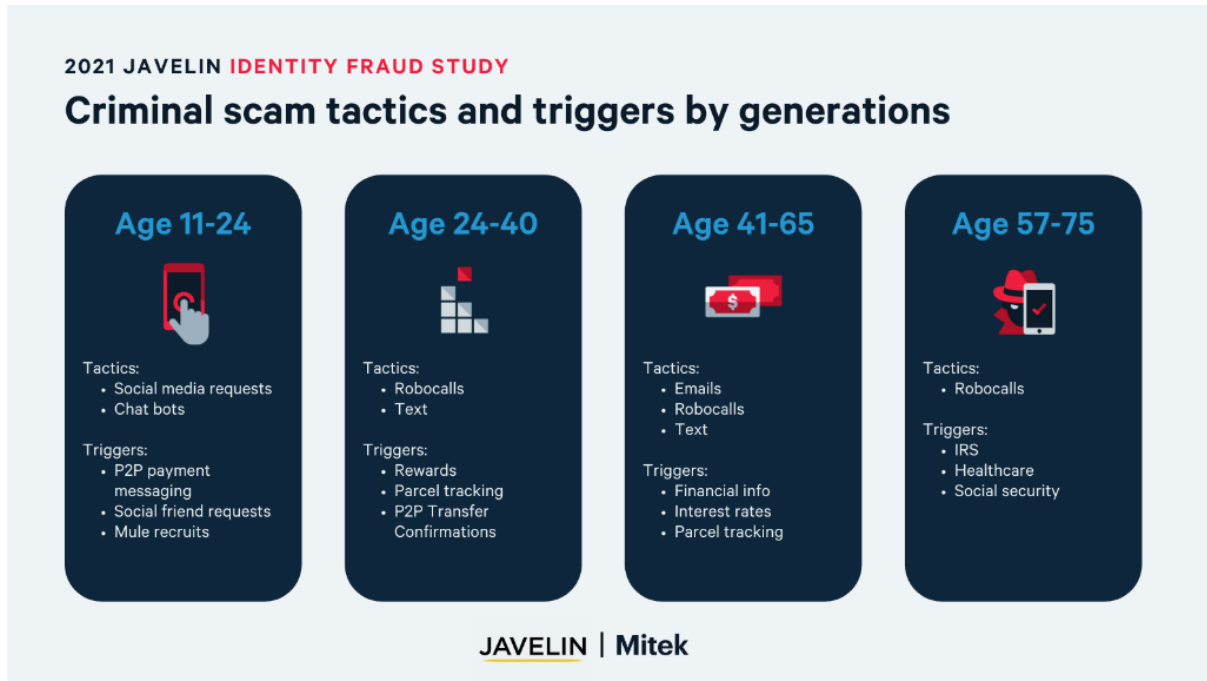


Figure 2.1.7: 4 types of generational fraud victims [10]

If the email contains a link, around 12% of people will click on it. On the upside, only 4% will enter data into the website the link leads them to. Now, let’s see what makes employees click on fake links, according to email phishing statistics

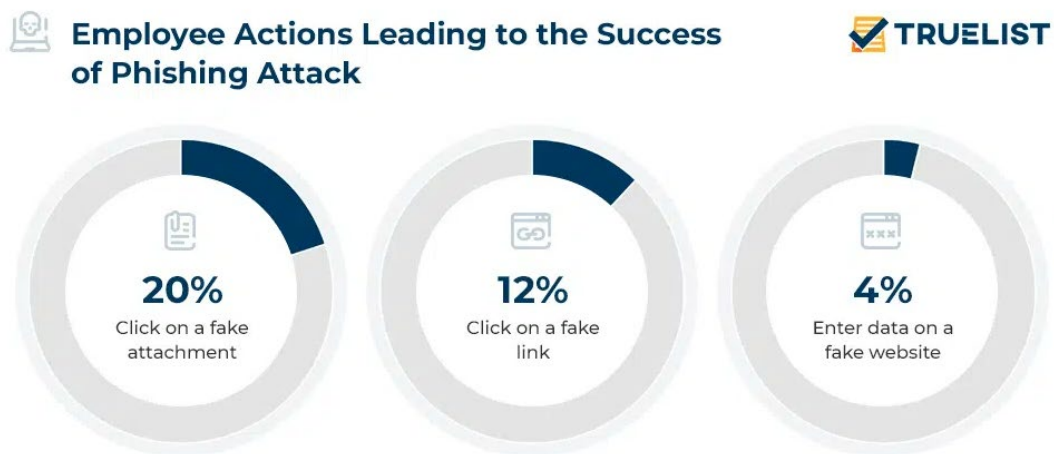
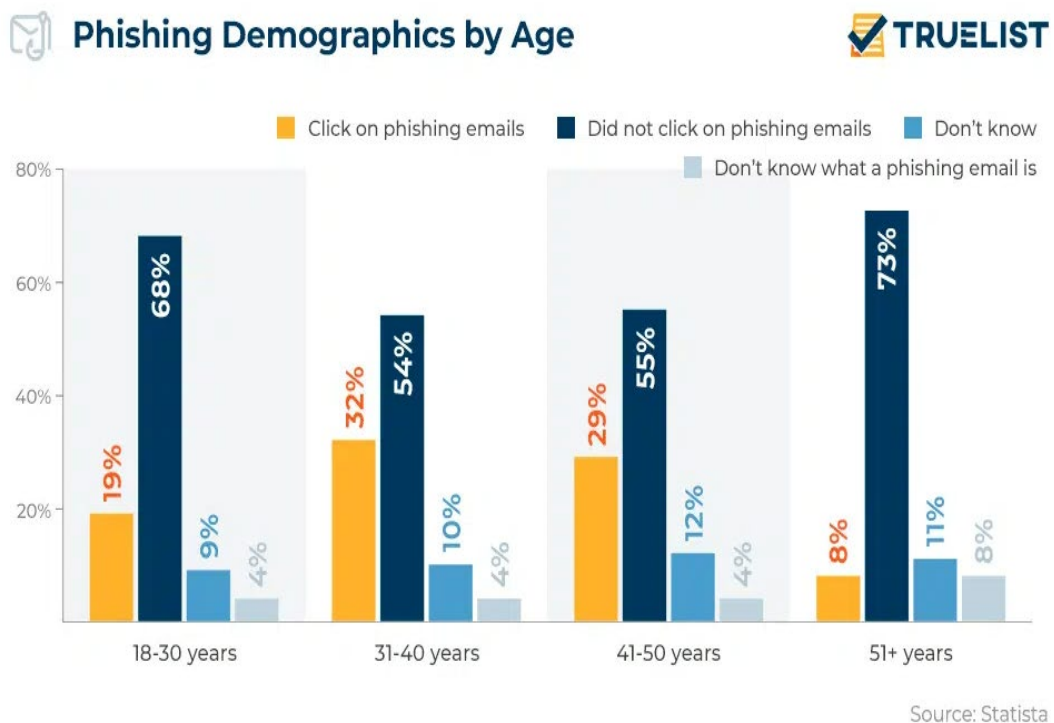


Figure 2.1.8: Employee Actions Leading to the Success of Phishing Attacks [10]

Phishing attacks saw a huge increase when the COVID pandemic started. New to online and remote work people make mistakes, and attackers saw their chance. In March 2020, saw 500,000 attacks alone, marking a massive spike in recent phishing attacks at the time, from 218,000 in January 2020, with Google blocking 18 million malware and phishing emails about Covid in April 2020.

LinkedIn is the top social media subject to watch out for. There is a massive 47%, phishing messages related to the professional network are the top social media subject to beware.

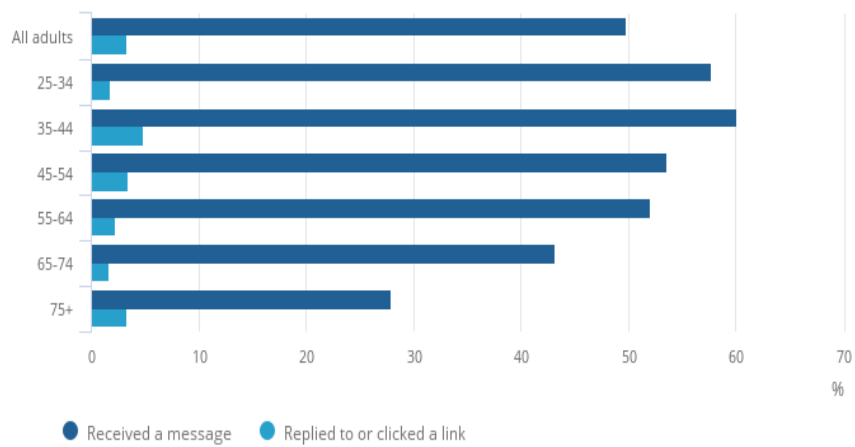


**Figure 2.1.9:** Phishing Demographics by Age [10]

Adults aged between 25 and 34 years or 35 and 44 years were more likely to receive a phishing message (58% and 60% respectively) than other age groups. Those aged 35 to 44 years also had the highest proportion of respondents who replied to the message or clicked a link (4.8%).

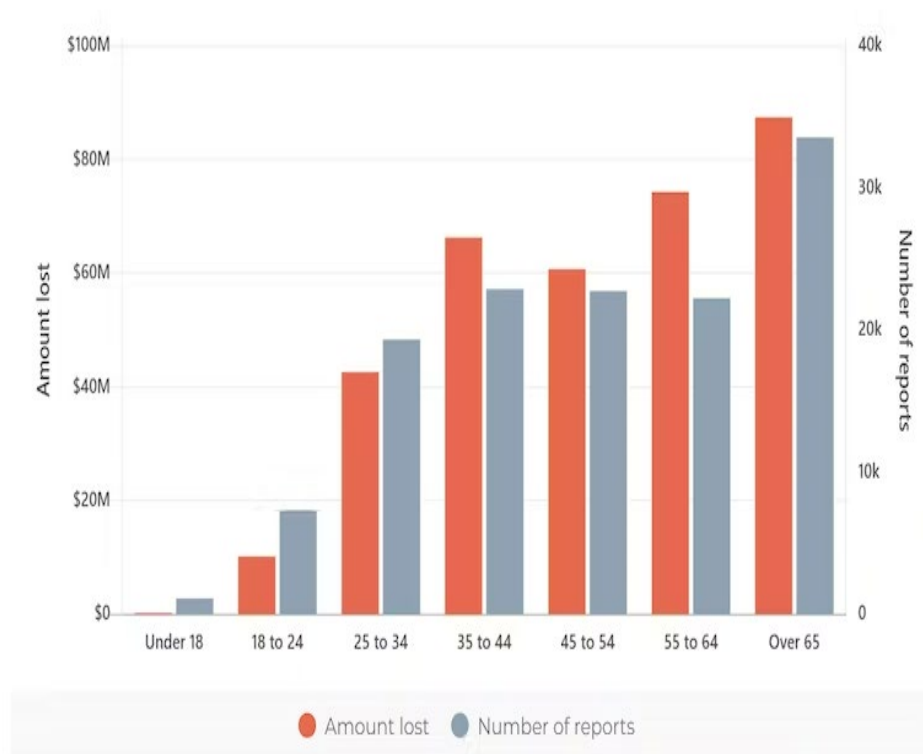
### Those aged 25 to 44 years were most likely to receive a phishing message

Proportion of adults who received a message that may have been phishing and the proportion of those who replied to or clicked on a link in the message, by personal characteristics



**Figure 2.1.10:** Proportion of adults who received a message that may have been phishing and the proportion of those who replied to or clicked on a link in the message, by personal characteristics [11]

Festive season attracts potential scammers trying to ruin the fun. This is because scammers become more active during the holidays, targeting all groups but most of the seniors.



**Figure 2.1.11:** Age groups of scam victims on holidays.

Barracuda researchers [12] have seen attacks about COVID-19-related spear-phishing attacks since January 2020, but they have observed a recent spike in this type of attack, up 66% since the end of February 2020. They observed three main types of phishing attacks using coronavirus COVID-19 theme scams [13], brand impersonation, and business email compromise. Through March, 54% were scams, 34% were brand impersonation attacks, 11% were blackmail, and 1% were business email compromise.

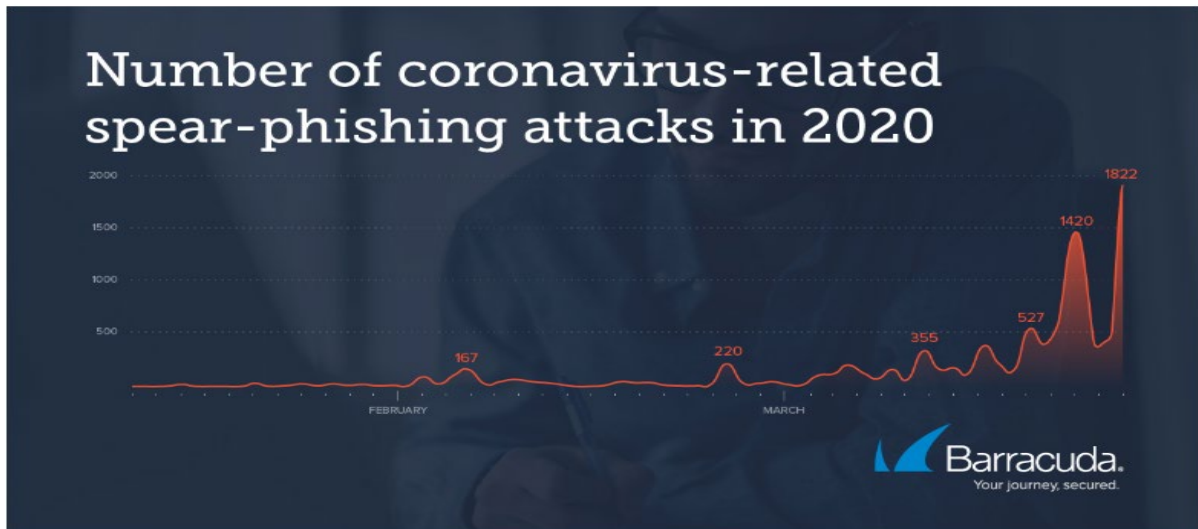


Figure 2.1.12: Spear phishing attacks related on Covid-19 [14]

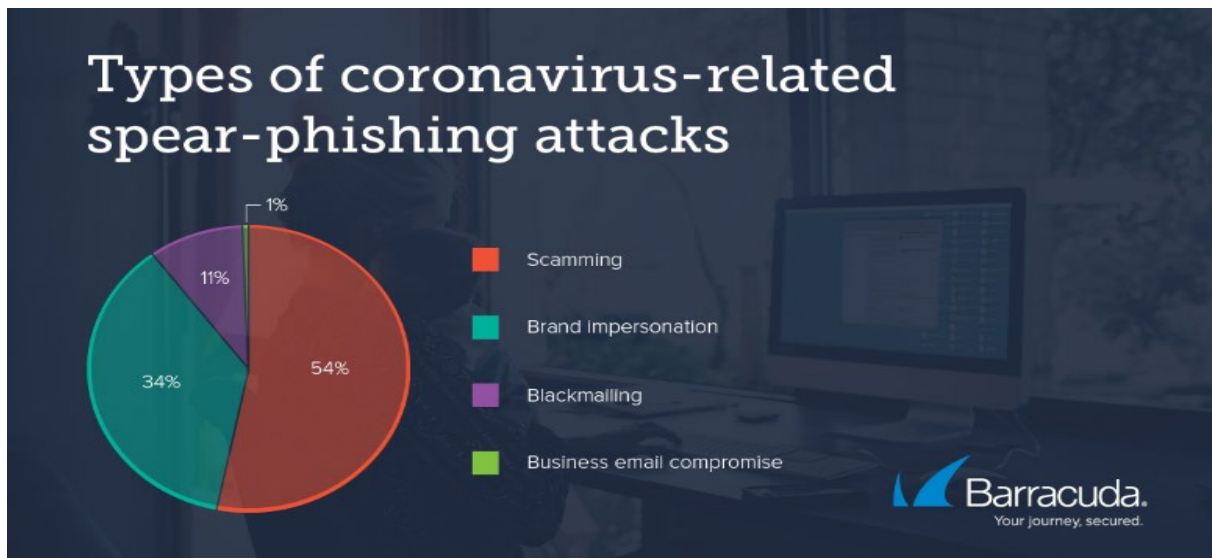
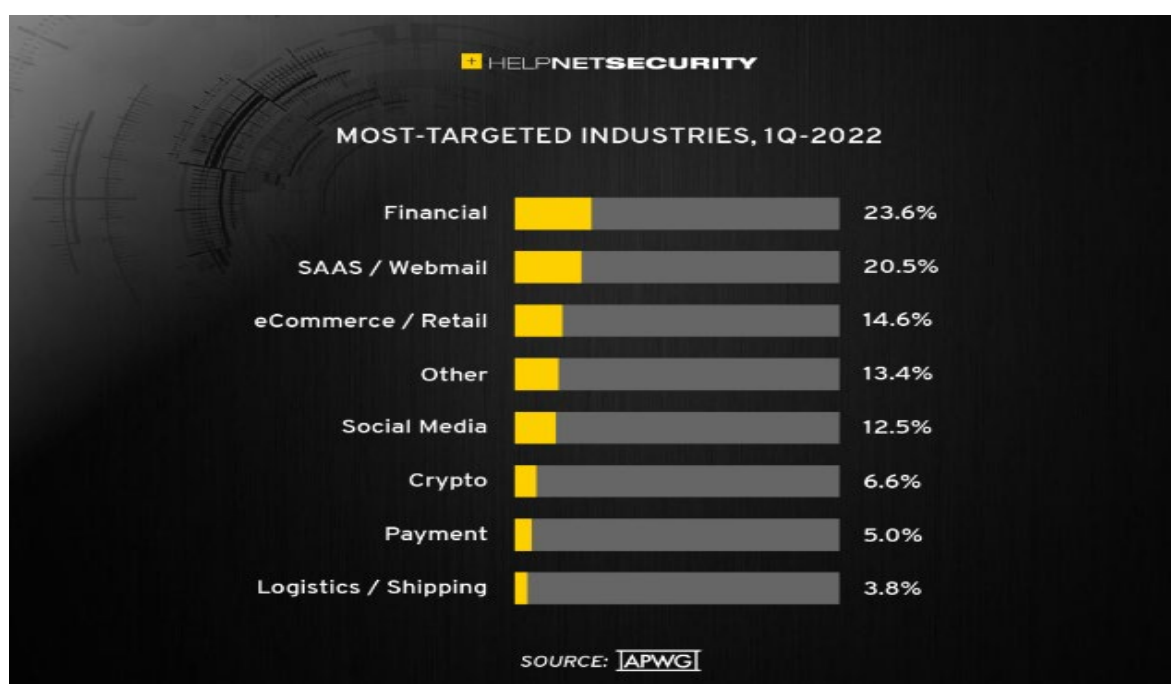


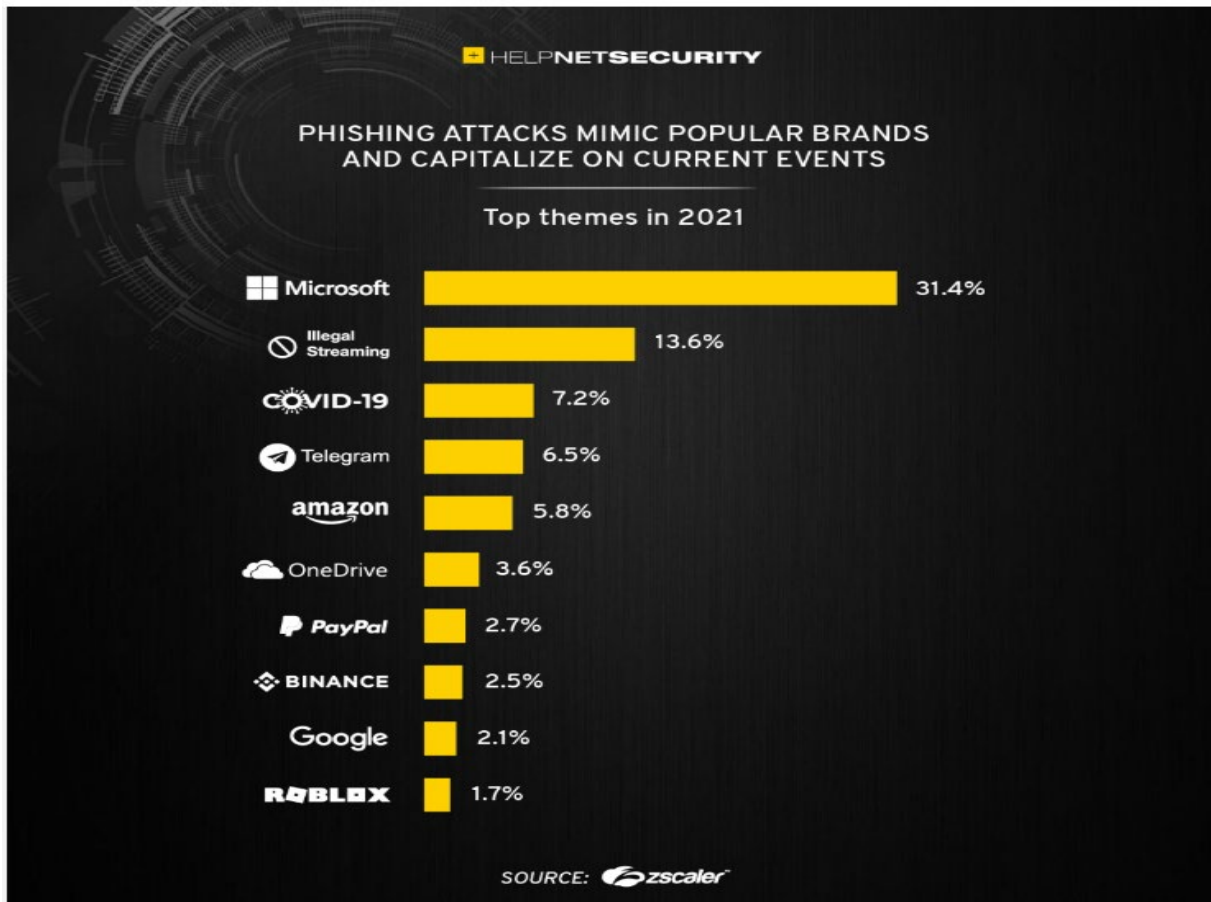
Figure 2.1.13: Types of spear phishing attacks related on Covid-19 [14]

Global phishing statistics further show that out of all security incidents during 2020, 80% were phishing attacks. Although in the first quarter of 2022 the total attacks were 1,025,968 so the phishing activity trends are shown below. Financial attacks remained the first choice of hackers with webmail and software-as-a-service (SaaS) providers remained in the second place of choice, while attacks against retail/ecommerce sites fell from 17.3 to 14.6 percent after the holiday shopping season.



**Figure 2.1.14:** Trends of Phishing Attacks on 2022 by Help Net Security [14]

Zscaler reviews twelve months of global phishing data from its security cloud to identify key trends which mimic popular brands. The 2021 report showed dramatic 29% growth in overall phishing attacks compared to previous years, with retail and wholesale companies bearing the brunt of the increase. Phishing attacks are impacting businesses and consumers with alarming frequency, complexity, and scope, with the rise in phishing as a service making it easier to launch successful attacks.



**Figure 2.1.15:** Phishing attacks mimic popular brands and capitalize on current events 2021 by Help Net Security [14]

Phishing Statistics from 2022 and beyond are as of Q3 2019, phishing attacks are at their highest they've been in three years and is the number one cause of data breaches. Fraudulent transfers are sent to more than 140 countries. 68% of all phishing websites use HTTPS protocol and 78% of known cyber-espionage incidents involve phishing. Also, 90% of successful data breaches and hacks spawn from phishing attacks. 66% of people aged 55 plus recognize the term phishing but only the 47% of 18-22 years old know what phishing means. SaaS and webmail are the most targeted industry sectors with 33% of all phishing attacks following financial institutions accounting for 19% and the less targeting area is Cloud storage and file hosting have a 4% target rate. [15], [11]

The most common phishing techniques that cybercriminals used to collect personal information from users are more advanced and their techniques that are being used are also advanced. [16], [17]

- Spear phishing is more targeted and after more valuable information than credit card data. They do research to make the attack more personalized and increase their chances of success.
- Link Manipulation is the type of attack in which the attacker sends a link to a fake website.
- Keyloggers refer to the malware used to recognize inputs from the keyboard and the information it will be sent to the hackers.
- Vishing is the voice phishing the attacker through phone calls asks users to dial a number. The purpose of this method is to get personal [18] details such as a bank account.
- Malware is phishing scams that involve malware to run on a user computer. Either the user clicks on a fake link or may also attach downloadable files on the mail that the attacker sends to the victim.

- Social Engineering is a technique that manipulates users by clicking questionable content for many technical and social reasons. Phishers count on victims not thinking twice before infecting the network.

## 2.2 Phishing attacks

The COVID-19 pandemic coincided with a global epidemic of scams and frauds. The unprecedented cybersecurity concerns emerged during the pandemic sparked a torrent of research to investigate cyber-attacks and to propose solutions and countermeasures. The phishing was by far the most frequent type of attack. Many reports by governmental bodies, security firms and the grey literature that investigated phishing attacks during COVID-19, or that proposed countermeasures against them. Fraudsters are always adapting their phishing attacks, and recent emerging trends have exploited the COVID-19 pandemic and rising cost of living. In the latest year, 4.8% of all fraud was perceived to be coronavirus-related, rising to 6.3% of all cyber fraud. In one campaign, victims received text messages apparently from the NHS claiming they had been in close contact with someone who had the Omicron variant. The message provides a link to a website claiming to be hosted by the NHS where they can book a test, prompting them to provide personal information and pay a delivery fee.

Cyberattack campaigns was revealed by analyzing and considering cyberattacks in the context of major world events. Following what appeared to be substantial gaps between the initial breakout of the virus and the first COVID-19-related cyber-attack, the investigation indicates how attacks became significantly more frequent over time, to the point where three or four different cyber-attacks were reported on certain days. An intense look into the recent advances that cybercriminals leverage, the dynamism, calculated measures to tackle it. The hacking attacks was the most frequent with a record of 330 out of 895 attacks, accounting for 37%. Next was Spam emails attack with 13%; emails with 13%; followed by malicious domains with 9%. Mobile apps followed with 8%, Phishing was 7%, Malware 7%, Browsing apps with 6%, DDoS has 6%, Website apps with 6%, and MSMM with 6%. BEC frequency was 4%, Ransomware with 2%, Botnet scored 2% and APT recorded 1%.

Attack channel	Lures	Launched period	Targeted or not	Victims
<b>Email</b>	<ul style="list-style-type: none"> <li>▪ An Unfamiliar Tone or Greeting</li> <li>▪ Grammar and Spelling Errors</li> <li>▪ Inconsistencies in Email Addresses, Links &amp; Domain Names</li> <li>▪ Threats or a Sense of Urgency</li> <li>▪ Suspicious Attachments</li> <li>▪ Request for Credentials, Payment Information or Other Personal Details</li> <li>▪ Unusual Request</li> </ul>	<ul style="list-style-type: none"> <li>▪ Holidays</li> <li>▪ Lottery</li> <li>▪ Covid-19</li> <li>▪ Health</li> </ul>	Malicious phishing	<ul style="list-style-type: none"> <li>Girls</li> <li>Seniors</li> <li>Seniors</li> </ul>
<b>Smishing attacks</b>	<ul style="list-style-type: none"> <li>▪ Unknown/ hidden numbers</li> <li>▪ The (pretended) sender. Institutions such as banks, IRS and debt collectors</li> <li>▪ Clicking on a link or calling a phone number provided, to clear up the error</li> </ul>			<ul style="list-style-type: none"> <li>▪ 18-25 years old</li> <li>▪ Men</li> <li>▪ People with higher curiosity, urgency, and stress levels are more likely to be victims of text scams</li> </ul>
<b>Vishing attacks</b>	<ul style="list-style-type: none"> <li>▪ Never share or confirm your personal details over the phone, even if the person calling is claiming to be your bank.</li> <li>▪ Don't answer calls from numbers you don't know.</li> </ul>			<ul style="list-style-type: none"> <li>▪ Seniors</li> </ul>

<b>Spear Phishing</b>	<ul style="list-style-type: none"> <li>▪ Check sender email address and name</li> <li>▪ Check the email format</li> <li>▪ Verify shared links</li> </ul>		Targeted	<ul style="list-style-type: none"> <li>▪ Seniors</li> </ul>
-----------------------	--	--	----------	---

## 2.3 Countermeasures against phishing

Individuals and organizations often fall to frauds that involve many forms of social engineering techniques, where the information required is garnered from a person rather than breaking into a system. [19] Cyber criminals can easily play on people’s psychology and perceptions. Also, they often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages. There are ways that can be protected from phishing attacks [18]. Attackers rely on the fact that people are busy, these spoof emails appear to be legitimate. As a result, recipients are more likely to take what is written in them seriously and act upon it. Here are some cyber scams and ways to protect and avoid them [20], [21]:

**Bank phishing emails** may look identical to the types of correspondence that real banks send by replicating the logos, layout, and tone of real emails. Also, they use language that transmits a sense of urgency, for instance implying a penalty if you do not respond, so it may ask you to download an attachment or click on a link. There are some tips that must be kept in mind to keep alert from these attacks.

- First, must keep our software updated, including your browser, antivirus, and operating system.

- Second, be especially vigilant if the 'bank' email requests sensitive information. A legitimate bank will only communicate with you securely through your online bank account.
- Third, check for inconsistencies and anything that does not make sense such as a slight difference in the sender's address. Also compare the sender's email address with previous real messages from your bank and check for bad spelling and grammar mistakes.
- Fourth, do not reply to a suspicious email, forward it to your bank by typing in the address and do not click on the link or download the attachment.

**Romance scams** usually take place on online dating websites, but defrauders often use social media or email to contact the victim. There are some ways to recognize the scammer. It must ring a bell that someone who has recently met online professes strong feelings and repeatedly asks to chat privately. Their messages are often poorly written and vague, and their online profile is not consistent with what they tell you. Also, they may also ask you to send intimate pictures or videos of yourself. Their profile is that they patiently wait to gain your trust, sometimes waiting up to weeks or months. They will always have an excuse to justify why their webcam is not working, being unable to travel to meet you and why they always need more money by elaborating a story and asking you for money, gifts, or your bank account or credit card details. If you do not cooperate, they may try to blackmail you. So, to avoid it, must be very careful about how much personal information we share on social networks and dating sites. Always have in mind the risks. Scammers are present on the most reputable sites. Research the person's photo and profile using online searches to see if the material has been used elsewhere and it is not fake. Be alerted to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera never working. Don't share personal pictures, videos, or any compromising material that the defrauder could later use to blackmail you. If you agree to meet in person, tell family and friends where you are going. Never send money or give credit card details, online account details, or copies of important personal documents.

**Lottery and Free Gift Card Scams** work because they play with people's desire for free money, so they post on social media claiming to give out free gift cards for popular stores like Starbucks or announcing that you have won the lottery. By clicking on them, you're taken to a site that asks you to enter your information to claim your winnings. They ask you for your phone number to secretly charge you in data fees or ask you, your banking information to wire you money and in the end, they steal from you instead.

**Investment scams** may include profitable investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy. The signs that must be alert are receiving an unsolicited call, repeatedly and they promised quick returns and assured that the investment is safe. They try to convince that is a great offer and you have a limited time to accept the offer and it is only for you.

**Cryptocurrency investment scams** trick victims into buying an unknown cryptocurrency via an exchange platform. [22] They trick them into transferring their assets from their legitimate wallets to a dubious recipient. Scammers posted ads on the internet or social media. Unsolicited investment offers received by email, social media, or telephone. A few of the methods are fake crypto investment companies and they request to transfer your legit crypto investment to an alternate crypto address that is under the control of criminals. Here are some ways how can protect ourselves:

- Search and ask around before making a crypto investment.
- Be careful where you send cryptocurrency. Once the transaction is completed, you will be unable to recall it and you lose everything.
- If you receive an investment opportunity from a friend, confirm that the message really came from them.

- Beware of unsolicited requests encouraging you to open and fund new crypto accounts. They will direct you to wallets controlled by scammers.
- Be clear on the conditions of your purchase and cryptocurrency ownership.

**Healthcare Scam** is a popular form of false medicare or social security advertisements. They offer services such as a corrected social security card with the person's married name, a social security card to replace a lost card, a social security statement or a social security number for a child. These companies may have profiles that feature the Medicare logo to seem legitimate. Scammers play on people's healthcare needs, so must double check a service offered with other previous healthcare Insurance.

**Photo of You Scams** are phishing schemes that are often seen on social media too. People receive a message in their Facebook inbox saying something like 'Have you seen this photo of you? The message then links to a page that looks identical to the social media site and prompts you to log in. If you log in, they can gain access to your account and have your login credentials as well. They bet on people's reputation so can spot it and protect us by putting our profile in private so that only your connections can message you. Don't click on suspicious links and when logging into social media, must check that we use the correct URL.

**See Who Viewed Your Profile Scam** persuades a person to click on a link, where they are either directed to a fake login which can be used against you. We can prevent the attack by checking that the URL is legitimate. Individuals can ensure their information and identity are completely secure, try Panda Security's Identity Theft Protection or Bitdefender which works to keep your personal details safe from attackers.

**Tax Season Phishing Scams** are coinciding with tax deadlines. They can come in all forms such as emails, phone calls, social media, and text messages. The attackers cleverly spoof the name of a legitimate tax authority and attempt to use fear or urgency to get victims to divulge personal or sensitive company information that can be used for identity theft.

**Holiday scams** are the busiest time of year for scammers. They know surges in online shopping, holiday travel, and time constraints can make it easier to catch victims off their guard with relevant schemes. Here are four holidays' attacks:

- **Black Friday and Cyber Monday Deals:** must remember that when a 'special offer' sounds too good to be true, it usually is. Avoid clicking on links in emails or popups with very deep discount offers.
- **Charity Tricksters:** Holidays are traditionally the time for giving. It's also the time that attackers try to pry money out of people that mean well. Prefer to donate only to charities you already know.
- **Complimentary Vouchers or Gift Cards:** A popular holiday scam is big discounts on gift cards. Don't fall for offers from retailers or social media posts that offer mock vouchers or gift cards paired with special promotions.
- **Bogus Shipping Notices:** Individuals are going to see emails supposedly from Amazon or a shipping carrier in your inbox that claim your package has a problem or could not be delivered.

Some ways that Individuals can stay safe are to use strong passwords but not reuse them for a second time and avoid unprotected Wi-Fi because scammers can intercept data transfer. As well, must verify before buying, because fraudulent ads, apps and websites can be hard to spot, so must take time to read the customer's review and after use them. We should be alerted to watch out for 'Lookalikes'. 'Lookalikes' are sites that cybercriminals create that imitate familiar brands. These sites may sell goods and be infected with malware or steal credentials.

**Covid-19 scams** are related to represent the CDC, FDA, or WHO, or medical companies such as Pfizer or Moderna. Also, they informed the victims that fake products and kits that claim to prevent or treat COVID-19 have appeared, posing threats not only to victims' money and privacy but also their health. [23] The scammers may guarantee early access to the vaccines in exchange for a deposit or fee. They find their victims through phone calls, robocalls and phishing. To avoid Covid-19 scams individuals should first contact the organization agency directly to see if the contact is authentic. Do not click on any links or download attachments. Also, must ignore questionable offers of Covid-19 vaccines or test kits and never submit personal information through emails, text, or online forms. [24]

Individuals can recognize phishing scams by notice some clues such as:

- It says that they notice some suspicious activity or log-in attempts.
- They claim there is a problem with your account or your payment information.
- They say they need to confirm some personal or financial information
- If they include an invoice, you do not recognize it.
- They send a link to click to make a payment
- They say you are eligible to register for a government refund
- They offer a coupon for free stuff

In conclusion here are four ways to protect ourselves from phishing attacks:

- Protect your computer by using security software
- Protect your cell phone by setting software to update automatically
- Protect your accounts by using multifactor authentication
- Protect your data by backing it up

**Social engineering** attacks consist of numerous methods. The basic definition of social engineering is the psychological manipulation of others into divulging confidential information or carrying out certain actions. It is therefore distinct from conventional hacking attacks because it plays on people's natural tendency to trust as well as on their credulity and lack of awareness. The aim is usually to extract sensitive data from companies or individuals. This prevents data leaking out of a company by making employees aware of the threats. [25]

Companies use lots of different tools to protect themselves against cybercrime (e. g. anti-virus software), but the weakest point in an IT security system is usually the human being. Social engineering specialists are excellent psychologists. They can manipulate the victim and use clever arguments and formulations.

Social engineering is a difficult cybersecurity threat to protect against because the tactics that attackers use prey on an individuals' reasoning. When employees haven't been trained to recognize social engineering attacks, the risk of falling victim rises. Because social engineering training plays such a critical role in minimizing threats, many organizations take cyber awareness training very seriously.

By 2022, for example, research firm Gartner projects that 60% of large organizations will have a full-time equivalent dedicated to security awareness. Social engineering training, which is often a part of security awareness programs, gives employees the tools they need to recognize these types of attacks, which helps groom more discerning, responsible employees who are better equipped to protect both themselves and their organization.

To prevent such attacks, there are several social engineering and cyber security measures to bear in mind such as below:

**Training of employees on social engineering:** As have already mentioned, one of the most important aspects of social engineering prevention is risk awareness. It is therefore essential to organize staff workshops and educate them on the value of data.

**Putting employees to the test:** Occasionally, it is a good idea to put employees through a test to see if they would do the right things in the event of a real attack. Do they switch off their monitors when they leave their desks? Are there any important documents on their desks? What will they do if an unknown number of calls impersonates someone offering services the company is looking for? Answering these questions will help ensure that each person on the team is aware of what to do.

**Multi-factor authentication:** Even a strong password is not always enough. It is better not to rely on single factor authentication for important data. In addition to passwords, multi-factor verification can include fingerprint scanning, security questions, or SMS codes.

**Do not allow strangers to connect to your primary Wi-Fi network.** Strangers at home or in the workplace should be allowed to access Wi-Fi via a guest Wi-Fi connection. Such an arrangement allows the main encrypted, password-secured connection to stay secure and interception-free. If any third party tries to “eavesdrop” for information, they won’t be able to access the activity you and others have kept private.

**Use a VPN.** In scenarios where someone on the main wireless network finds a way to intercept traffic, a VPN can keep such intruders out. VPNs provide services that allow users to keep their internet connection private over an encrypted “tunnel”. The connection is safeguarded against third-party intruders and eavesdroppers. Users’ data is anonymized so that it cannot be traced back to the user via cookies or other means.

**Security of network-connected devices and services.** Securing network-connected devices, smart devices, and the cloud services associated with these devices is important. Protect the generally overlooked devices, such as home network routers or car infotainment systems, home theaters, etc. Data breaches on all these devices could spark personalization for a potential social engineering scam.

## 2.4 Discussion

Many citizen communities can be a target of phishing attacks such as students, staff, seniors, girls, and people working at specific industries. New data have revealed that ages between 25 and 44 years are most likely to be most targeted, according to results from the Telephone-operated Crime Survey of England and Wales (TCSEW). [11] Traditionally sent via email, phishing involves messages from attackers posing as legitimate organizations to extract personal information, or money, from the victims. They have taken advantage of age significant events, including the coronavirus pandemic and the rising cost of living, to target victims. There is also evidence of attackers taking advantage of widespread behavioral changes because of the pandemic, such as the rise in online shopping. This includes a nine-fold rise in "advance fee fraud" (victims making upfront payments for goods or services which then do not materialize) and a 57% rise in "consumer and retail fraud" from pre-pandemic levels.

In the UK, in 2018, 49000 elderly people are reported being scammed. People between 65 to 74-year-old are 54 times more likely to be a victim of phishing attacks than they are to be physically. [26] Also, 27% of single people were duped by an attack when they were targeted, compared with less than a tenth of people who lived with someone else. The average age of victims of mass marketing postal fraud is 75, including lottery and prize scams, and clairvoyant scams. Often, victims are at home alone all day, craving any opportunity for contact or interaction with the outside world. Scammers target people aged 55+ choosing investment scams, as this is the stage in life when a person's wealth is usually at its peak. [27]

Approximately 20% of Americans over the age of 65 have been exploited and taken advantage of financially. The most vulnerable group to senior scams was being between the ages of 80-89 and living alone. Over \$143 million lost through social media romance scams in 2018, it's no wonder that 32.9% of elder fraud cases are the result of credit card scams. [28] In Australia in 2016 the ages under 18 reported 1% and scam losses 0.3%. The ages 25-34, reported 7% and losses 4% and ages between 35 – 54 they reported 17% and losses from scams 15%. 40% of scam reports were made from over 55s. Also, more women reported fraud, but men lost two thirds more from Investments or dating and romance fraud by phone. [29]

The criminal scams tactics that trigger by generations are the follow: [30]

- Scammers go after the age 11 to 24 by using social media requests and chat bots by P2P payment messages and social media requests.
- The age 25 to 40 targeted by text scams, as well as social media scams that offer rewards, package tracking or peer-to-peer (P2P) money transfer confirmations.
- Gen X, who are between 41 to 56, get targeted by robocalls, as well as text and email phishing scams designed to steal their login credentials and payment data.
- Consumers over the age of 56 are prime targets for robocalls and other phone-based tactics that impersonate the IRS, Medicare, Social Security, banks, and other trusted institutions.

According to the Federal Trade Commission [31], younger people reported losing money to fraud more often than older people. Out of all reports, 43% were between the ages of 20-29, while 15% were 70 -79.

Another research demonstrates that as we get older our judgment deteriorates making us more easy targets to scammers. People over 60 are twice as likely to believe something even when the information is misleading. Also, over 60 our brain begins to deteriorate, as a result they're more trusting. Two thirds of frauded victims are over 56. As well, forty percent of adults are anxious that their parents will be victims of attackers. Their easy targets because one in five warn them about the different types of frauds. [32]

The online dating scams are involved in a new online relationship and are asked for money under false pretenses. 63% of dating scams victims are female.

# **Chapter 3**

## **Methodology**

The approach applied to work in this thesis is quantitative using survey methodology. A quantitative approach. Different focus groups of different ages and citizen communities that can be a target of phishing attacks, e.g., students, staff, seniors, girls, people working at specific industries were used to gather the relevant information needed to investigate the problem statement. The focus groups, along with their respective age groups, spanning from ages 18 to 65 and above. This chapter begins with a section describing the process of data collection, which refers to the selection of phishing attacks examples relevant to the study and the reason for their relevance. Using an infographic framework and analyzing them. As a result of the analysis, if the infographics have the correct standards and which criteria may be used to design the right infographic. The research conducted in this study is intended to be quantitative using survey methodology.

A collection of examples of infographics had to be retrieved to be conducted. Separate the infographics by year from 2020 until 2023. So, that compares with the results of the conference paper with title 'Properties for Cybersecurity Awareness Posters Design and Quality Assessment' [33] that was collected in 2018. Many individuals or employees does not know that they can be attack and steal from them valuable data stored on servers stationed in another country. Similarly, who is responsible for the surveillance and protection of what is unclear. For example, in an organization, it is well-defined that security guards are responsible for surveilling and protecting its physical premises and property, whereas the responsibility of surveilling and protecting its IT systems and assets from potential cyberattacks is on every employee. Obscurities like these make cybersecurity a difficult concept to understand and comprehend for many people. And raising awareness of this concept with the purpose to result in actions and a long-term behavior change by using static information on infographics is obviously a challenging endeavor.

Also, it refers to being mindful of cybersecurity issues that affect personal and professional life. It primarily entails cognition which leads to cybersecurity behavioral adjustments brought about by positive changes in cybersecurity attitudes. The ultimate purpose of the process is to persuade or motivate people (individuals and employees) to adopt secure behavior while discouraging them from engaging in risky activities. This is the correct way to deliver the correct security information in the right amount and format to the right audience at the right time, via

the right dissemination channels. The information provided is often enough to draw individuals' attention to security risks, comprehend their potential consequences, and respond appropriately.

Many organizations including ENISA, EUROPOL, InfoSec Institute, and Cyber Safe Work, produce and distribute infographics to inform people about phishing attacks. The popularity of an infographic could be because it is one of the simplest and cost-effective awareness mechanisms and people are familiar to its usage. The infographics initially used to be a conventional method of the organizations (i.e., uses textual and image content. Utilizing digital technology, infographics' information richness is easily improved, for example, infographics include a clickable link that directs interested people to a website with detailed information on the subject.

Currently, infographics with one-line text and whole page text, with and without images on them, with fancy and plain typography, or with and without weblink are in use. On the one hand, many organizations are trying to create a right infographic, but on the other hand, little effort has been made to make the infographic more uniform and effective for the purpose. For indication, it is still not well-defined what message to include for an effective infographic. Furthermore, the infographic design and assessment are also largely based on unsystematic approaches. Therefore, this study intends to distract and analyze the properties that can guide or be useful for infographic design and its quality assessment. By properties, mean aspects like the content of an infographic, the infographic's appearance, etc.

The first step of the analysis was to collect the infographics by google search 'phishing attacks infographics', 'holiday scams', 'romance scams' etc., by year starting from 2020. Collecting twenty-five infographics of each year until 2023. The infographics are from different organizations either from credible sources or not. Each infographic analyzed in each category shown on figure 3.1. Each infographic rated up to twenty-eight points, as a result of the analysis for the overall quality of awareness raising material of infographics. Each infographic, depending on the score, will separate in one of the three categories, Low, Medium, and High. In the next chapter will analyze the categories shown in figure 3.1.

The elicited properties and their respective sub-properties are listed in the figure below.

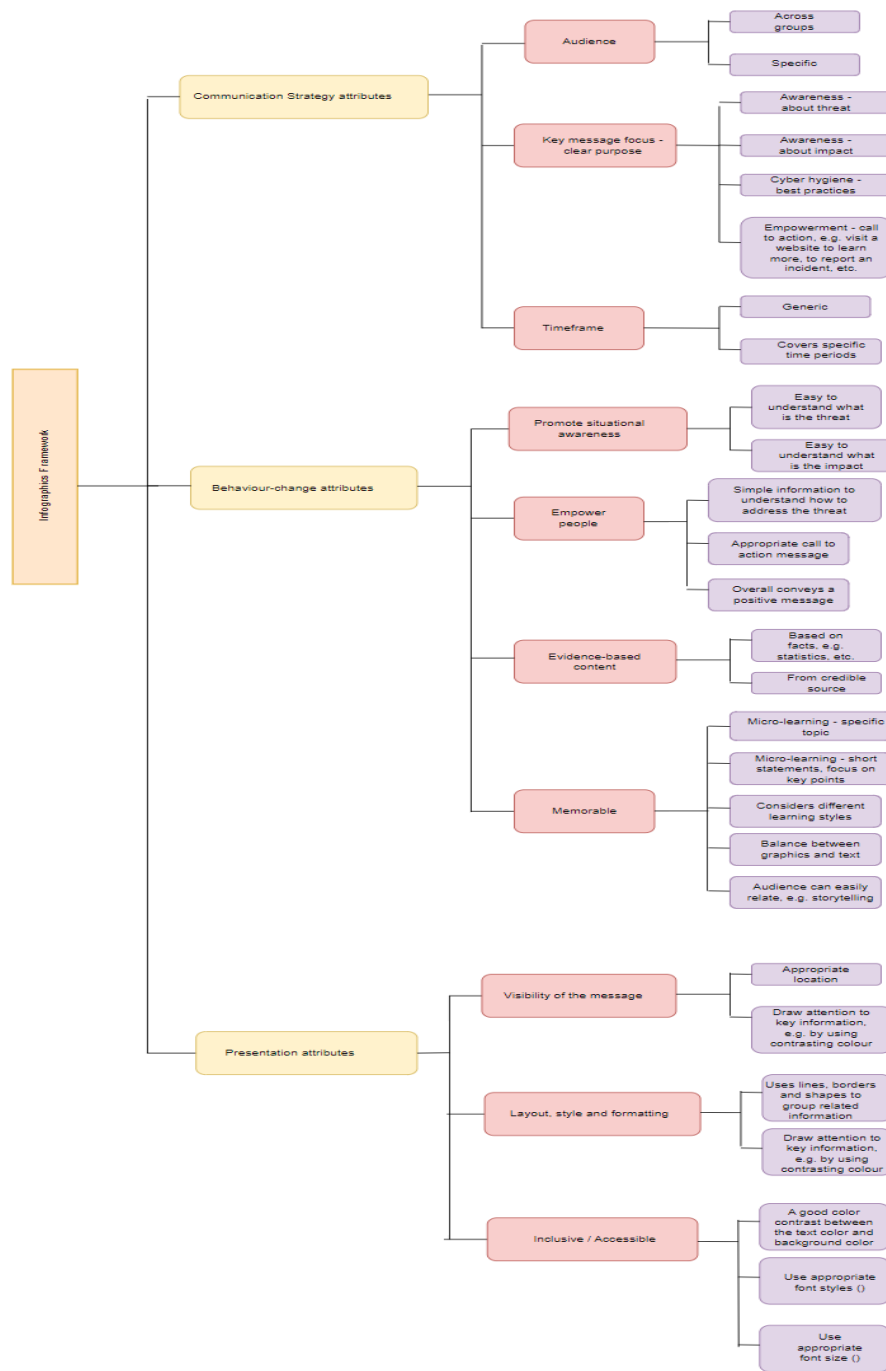


Figure 3.1: Infographics framework

# **Chapter 4**

## **Design**

We used an analysis tool to determine the degree to evaluate if the infographic is good or not. In order to do the evaluation, the analysis of each infographic, using Microsoft Excel. For the analysis needed four excel files, one for each year and displayed with the set of properties. Each infographic was analyzed for the overall quality of awareness raising material (Low, Medium, High). Every file contains twenty-five tabs, which each one has the analysis of each of twenty-five infographics for each year until 2023. The analysis used one hundred infographics from different organizations that are available for free. The infographics covered cybersecurity threats either for individuals or businesses for e.g., phishing, and social engineering attacks, holiday scams etc. [34]

The general idea for the design of a good infographic is to contain the below standards:

- Data: reliable, timely, content
- Design: theme color, fonts, readable
- Story: problem, clever message, solution
- Shareability: virality, SEO, location, social

Taking into consideration the above, how to design a good infographic, ending up creating a framework to evaluate one hundred infographics, if the infographics met the specifications. The following subsections will analyze each specification.

## 4.1 Communication Strategy attribute

The communication Strategy attributes is a specialized approach to distributing and receiving information. It means communicating the best message, through the correct channels, to the right people and at the right time. [35] So each infographic is analyzed from this point of view, resulting in its separation into three subcategories: Audience, Key message focus - clear purpose and Timeframe.

The subcategory 'Audience' is divided in two categories 'Across groups' and 'Specific'. The category 'Specific' is about the contents of the infographics that are related and align with the roles and responsibilities of the target audience or the goals and objectives of their organization. [36] The information should be explicitly directed at the audience. The information is more likely to be accepted and acted upon if the individual feels that it is explicitly directed than generically to everyone. The information can be made more direct and tangible by using evidence-based framing strategies. The category 'Across groups' is selected when the topic is referent for general information and the instructions can interest a large group of people and it is not specific on a target group such as different generation or referring only for companies and employees.

The subcategory 'Key message focus - clear purpose' is the number one thing the publisher wants the audience to remember or do as a result of an infographic. It is important to make a point that's useful. [37] It is split in four categories. The first category is 'Awareness - about threat'. This is referring to the infographic points and mentioning a thread that is clear to the audience. The second category is 'Awareness - about impact'. This category is about if an infographic talks about the impact of a phishing scam, for example what the impact will have to the victim's life, if will be a scam victim. The third category is about 'Cyber hygiene - best practices' [38] so on each infographic looking to ensure critical data and connected devices are handled safely, to minimize their exposure to risk on a thread. Also, if the infographic share involves implementing a set of best practices on a regular basis to ensure the security of an organization's network and data. The fourth category is called 'Empowerment - call to action, e.g, visit a website to learn more, to report an incident, etc.' This section is about call of action.

For example, if an infographic writes down a way how a reader can learn more about the attack or where can report the incident.

The last of this subcategory is 'Timeframe'. [39] Timeframe is a type of content of infographic that visually displays information in a time progression context. This subcategory is separate in two categories 'Generic' and 'Covers specific time periods'. 'Generic' means that each infographic satisfies this category because it is not referred to a specific timeframe. 'Covers specific time periods' is the category that is related if each infographic includes a specific timeframe such as holiday season.

## **4.2 Behavior – change attributes**

Behavior – change attributes are made up of a range of motives, traits, skills, and knowledge. The separation of Behavior – change attributes is in four subcategories called 'Promote situational awareness', 'Empower people', 'Evidence – based content' and 'Memorable'. 'Promote situational awareness' is a key principle of threat intelligence, where one must be aware of what is happening, in terms of phishing attacks and what is the impact that is considered a risk. [40] It is divided into categories 'Easy to understand what the threat is' and 'Easy to understand what is the impact'.

Choosing 'Easy to understand what is the threat' for an infographic is when the infographic is referring and makes it clear, legible, and easy to understand the thread that is talked about. If choosing 'Easy to understand what is the impact' category is related, if the infographic analyzes the impact that the attack will have in your life or business after the attack.

The 'Empower people' is a subcategory that looks for 'sentences' on each infographic, if exist, that empower the reader about the topic of phishing attacks. It is separated into three sections 'Simple information to understand how to address the threat', 'Appropriate call to action

message' and 'Overall conveys a positive message'. The 'Simple information to understand how to address the threat' meaning that the infographic informs the audience how to identify the threat. The 'Appropriate call to action message' is a message that the infographic calls the audience to do to protect them. The 'Overall conveys a positive message' is referring to an infographic that may include messages where the audience is expected to react to a positive manner. [41]

The 'Evidence-based content' subcategory refers to a collection of imagery, data visualizations like pie charts and bar graphs, and minimal text that gives an easy-to-understand overview of a topic. [42] The above subcategory is divided in two categories named 'Based on facts, e.g., statistics, etc.' and 'From credible source'. The first category 'Based on facts, e.g., statistics, etc.' mentions if the infographic has elements such as text image, chart, and diagram. The second category 'From credible source' is referring to if the infographic comes from a reliable source. [43]

The 'Memorable' [44] subcategory makes a point that's useful and it is easy to stick on your mind and it is simple to remember. It is separate in five categories called 'Micro-learning - specific topic', 'Micro-learning - short statements, focus on key point', 'Considers different learning styles', 'Balance between graphics and text' and 'Audience can easily relate, e.g., storytelling'. [45]

The 'Micro-learning - specific topic' talks about a particular topic and no general information about the thread. The 'Micro-learning - short statements, focus on key points' shows if an infographic contains short and to the point statements and if it is focusing on a key word. Also, the category 'Considers different learning styles' refers if the infographic has different learning styles like visual and text, so it is easier for the audience to understand how important it is to identify the thread. Category 'Balance between graphics and text' shows if an infographic has layouts with an even balance and, the graphics don't overpower the text and the infographics does not seem to tilt to one side or the other. [46] The last category of this subcategory is called 'Audience can easily relate, e.g., storytelling' for example the information explains the problem of the topic; 'the message/story is clever?' and the story ends with a solution.

## 4.3 Presentation attributes

'Presentation attributes' is referring to appropriate fonts, which will not only help your audience be able to easily read the infographic, but they can also actually make the information appear to be more credible (Well-structured, Use of image, Positive, Complete, and Clarity). [47] 'Presentation attributes' split in three subcategories named 'Visibility of the message', 'Layout, style, and formatting' and 'Inclusive / Accessible'.

'Visibility of the message' [48] are certain types of visuals that help to see and understand data, ideally in ways that lead us to have quick insights. Also, it can be short and simple or long and in-depth. [49] It contains two categories 'Appropriate location' and 'Draw attention to key information, e.g., by using contrasting color'. 'Appropriate location' is referring to the data that display on the infographic are short and simple and not too long and in-depth. 'Draw attention to key information, e.g., by using contrasting color' related concepts ideas in ways that are accessible, coherent, memorable, and compelling through contrast color. [50], [51], [52]

'Layout, style, and formatting' looks to have enough whitespace, so it won't look too busy. The colors are consistent. Highlight key information with a big image, different background color, or large font. [53] Separate the content into sections with subtitles, lines, or color blocks. It is separated into three categories named 'Uses lines, borders and shapes to group related information', 'Create text hierarchy (up to 3 different font styles)' and 'Maximum 4 colors'. 'Uses lines, borders and shapes to group related information'. 'Uses lines, borders and shapes to group related information' If the infographic has basic design elements like borders, lines, circles, and squares to visually organize our content, readers will find it easier to interpret that content. [42] 'Create text hierarchy (up to 3 different font styles)' if an infographic uses up to three font styles to show which information to focus on, and what is most important and what is simply supporting the main points. [54] 'Maximum 4 colors' if an infographic has too many colors, this can detract the reader from the purpose of the infographic. But too few colors will make a boring infographic. 2-4 colors are ideal. [55], [56]

The subcategory 'Inclusive / Accessible' is divided in three categories called 'A good color contrast between the text color and background color', 'Use appropriate font styles' and 'Use appropriate font size'. 'A good color contrast between the text color and background color' category referring to make content accessible, should have high contrast between all text and its background color. If the text is dark, the background should be light, and vice versa. When text and background color are too similar, it can be difficult for your audience to process the information. [57] To analyzed the above category of each infographic will use the website <https://webaim.org/resources/contrastchecker/> [58] 'Use appropriate font styles' and 'Use appropriate font size' are the process of analyzing these characteristics of the content of an infographic for defining the focus for each piece of text and style and engagement, or readability and legibility. [59]

# **Chapter 5**

## **Analysis - Evaluation**

The elicited properties have significance of infographic design and its quality assessment. The evaluation of each infographic was based on categories data, purpose, sources, organization and flows, sources, color, text, and overall aesthetics.

**Data:** present makes the information easier for the viewer to understand.

**Purpose:** if the reason for the infographic is clear.

**Sources:** are from credible sources and easy to see where data and information comes from.

**Organization and flow:** should be easy and for the eye to move through the content. Also, the data and the information must be clearly organized and connected.

**Color:** must be attractive and complemented each other and consistently used. As well color enhances the flow and visual appeal of the infographic.

**Text:** should consistently use fonts throughout the infographic. In addition, text has to be clearly described data, graphs, charts, images, and appears near relevant information.

**Overall aesthetic:** should engage the reader to read the infographic.

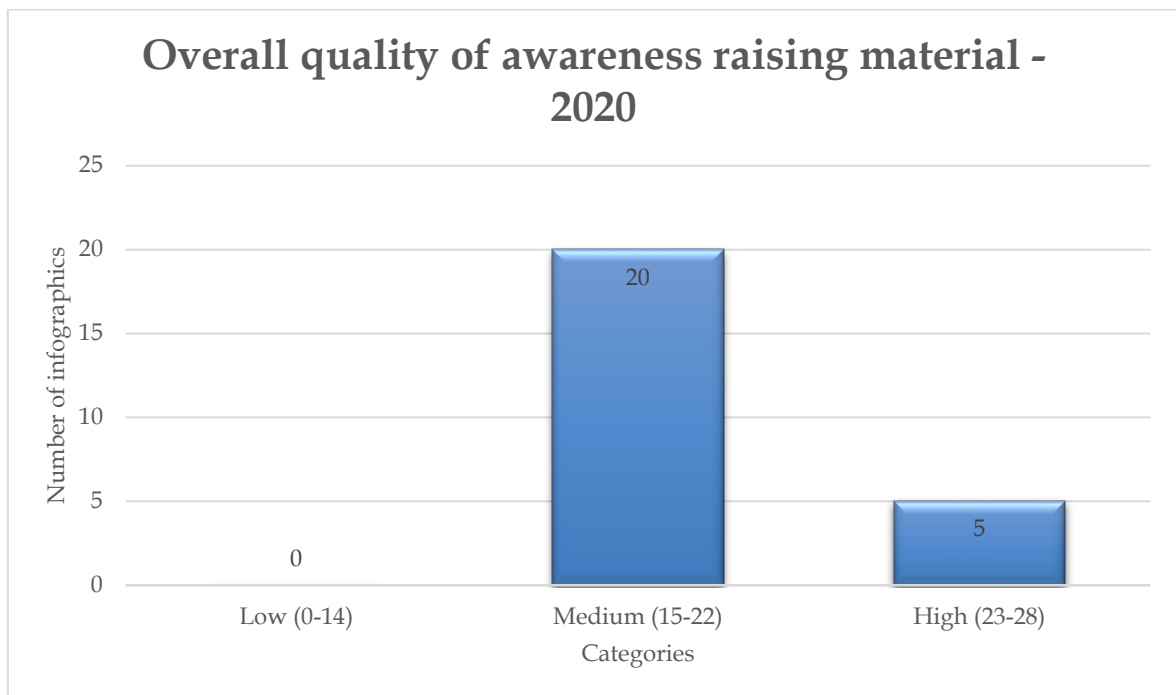
The analysis model that has been used to evaluate the infographics is shown below in figure 5.0.

	A	B	C	D	E	F	G	H	I	J
1										
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>				
3							Infographic - website			
4										
5		1 Audience		Marks			Marks	Comments		
6		1,1 Across groups			1					
7		1,2 Specific			2					
8										
9		2 Key message focus - clear purpose								
10		2,1 Awareness - about threat			1					
11		2,2 Awareness - about impact			1					
12		Cyber hygiene - best practices			1					
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.			1					
14										
15		3 Timeframe								
16		3,1 Generic			1					
17		Covers specific time periods			2					
18										
19										
20	<b>Behaviour-change attributes</b>									
21										
22		1 Promote situational awareness								
23		Easy to understand what is 1,1 the threat			1					
24		Easy to understand what is 1,2 the impact			1					
25										
26		2 Empower people								
27		Simple information to understand how to address 2,1 the threat			1					
28		Appropriate call to action 2,2 message			1					
29		Overall conveys a positive 2,3 message			1					
30										
31		3 Evidence-based content								
32		Based on facts, e.g. 3,1 statistics, etc.			1					
33		3,2 From credible source			1					
34										
35		4 Memorable								
36		Micro-learning - specific 4,1 topic			1					
37		Micro-learning - short 4,2 points			1					
38		Considers different 4,3 learning styles			1					
39		Balance between graphics 4,4 and text			1					
40		Audience can easily relate, 4,5 e.g. storytelling			1					
41										
42	<b>Presentation attributes</b>									
43										
44		1 Visibility of the message								
45		1,1 Appropriate location			1					
46		Draw attention to key 1,2 contrasting colour			1					
47										
48		2 Layout, style and formatting								
49		Uses lines, borders and 2,1 information			1					
50		Create text hierarchy (up to 2,2 3 different font styles)			1					
51		2,3 Maximum 4 colours			1					
52										
53		3 Inclusive / Accessible								
54		A good color contrast 3,1 between the text color and background color			1					
55		Use appropriate font styles 3,2 ( )			1					
56		3,3 Use appropriate font size ( )			1					
57										
58										
59										
60										
61		<b>Communication Strategy attributes</b>				0				
62		<b>Behaviour-change attributes</b>				0				
63		<b>Presentation attributes</b>				0				
64										
65										
66										
67		Overall quality of awareness raising material								
68		Low 0-14								
69		Medium 15-22								
70		High 23-28								
71										

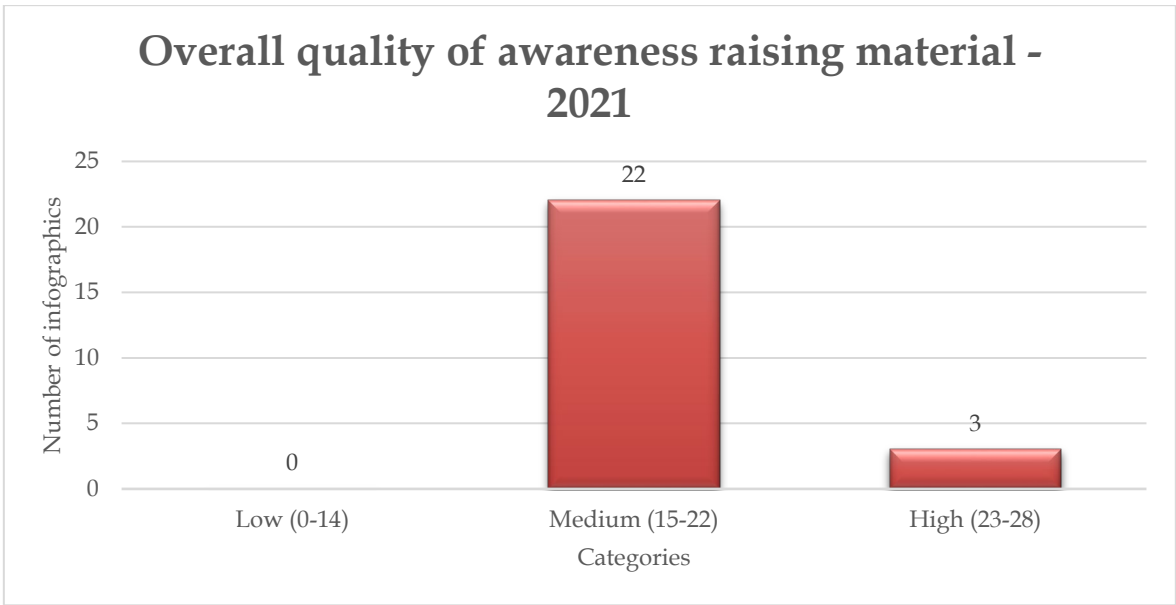
Figure 5.0: Infographic evaluation

Every category is marked with one or two points. The total mark for category Communication Strategy attributes is ten points, for category Behavior-change attributes the maximum points that can be collected are twelve. Additionally, category Presentation attributes collect up to eight points. Moreover, the total rate for the three categories is up to thirty points and it is separated in three stages. The first one is called Low, and it covers from zero to fourteen points. The second is named Medium and covers the range from fifteen to twenty-two points and the last stage is called High which covers the range from twenty-three to twenty-eight (thirty) points.

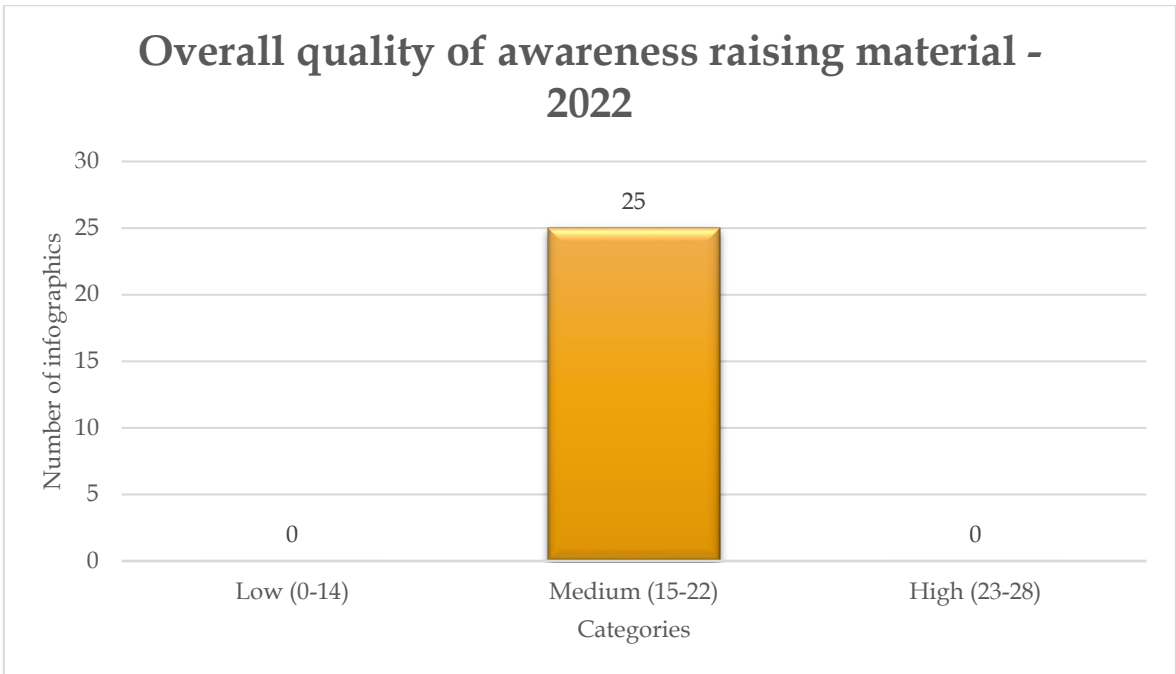
The general idea of the results of the evaluation that shown in appendix A1, A2, A3 and A4 for each year is that the infographics are medium quality of awareness raising material. So, the infographics are getting points between fifteen and twenty-two. Furthermore, for the years of analysis there were no low-quality infographics but only few high-quality infographics only for years 2020 (Figure 5.1), 2021 (Figure 5.2) and 2023 (Figure 5.4) as presented on charts below. The year 2022 (Figure 5.3) has no high-quality infographics. As a result, every year the quality of infographics stays the same or gets worse. So, there is not any progress over the years.



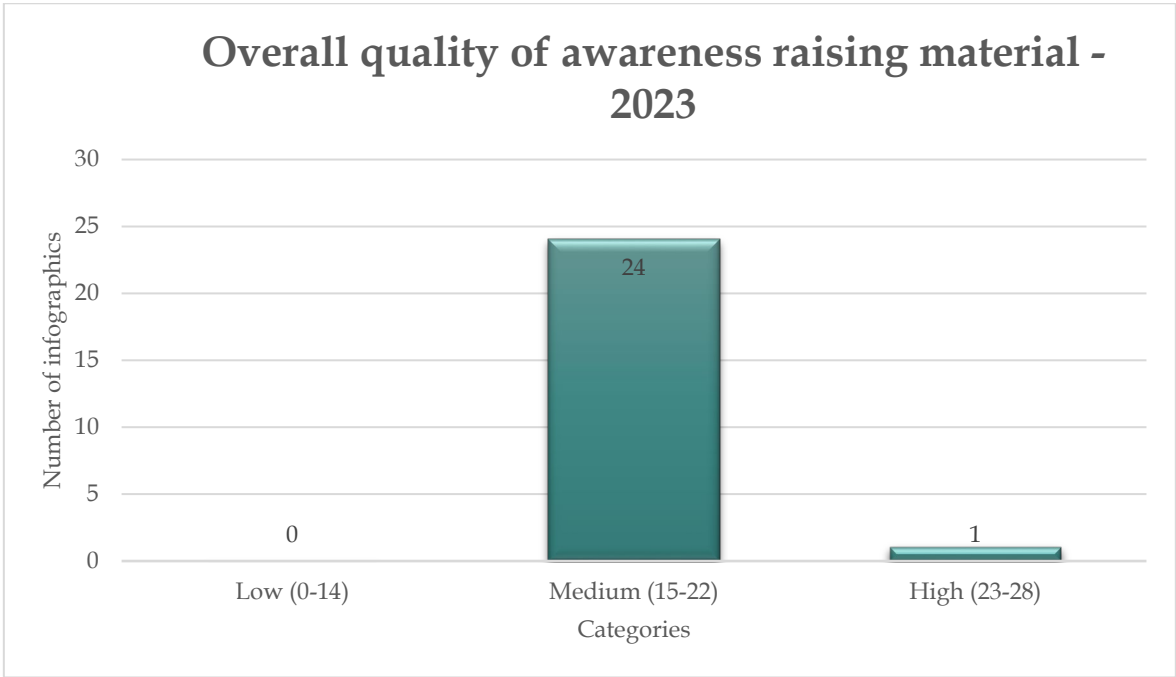
**Figure 5.1:** Chart of overall quality of awareness raising material - 2020



**Figure 5.2:** Chart of overall quality of awareness raising material - 2021

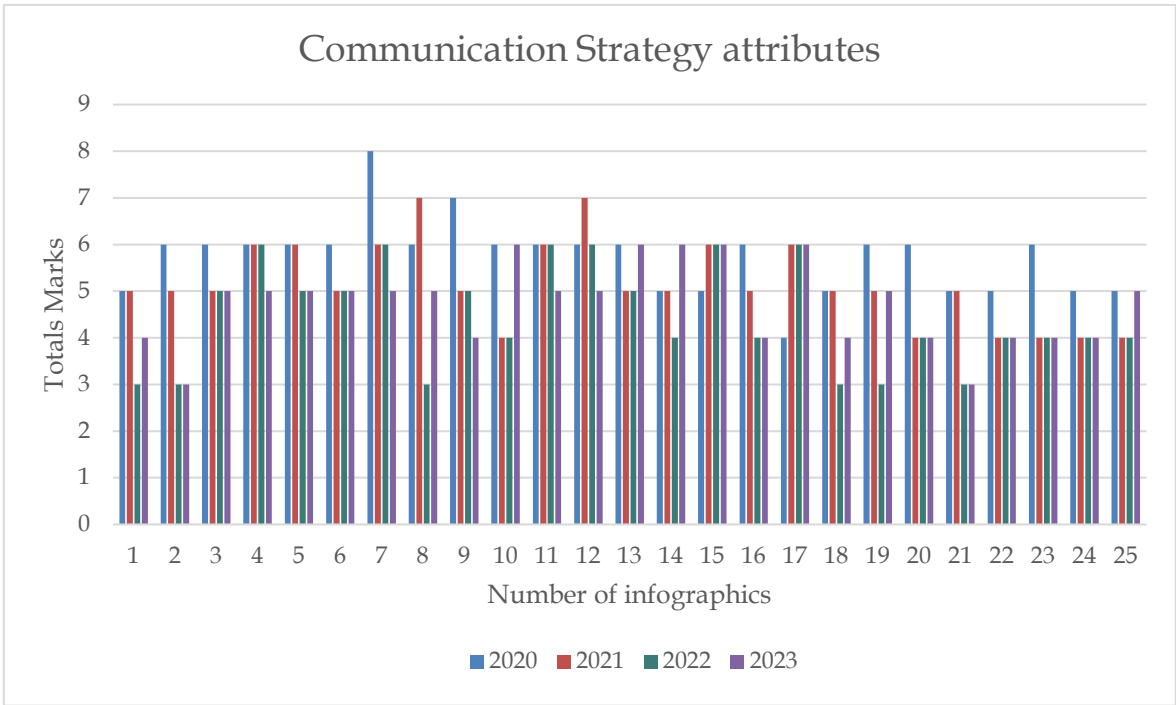


**Figure 5.3:** Chart of overall quality of awareness raising material - 2022



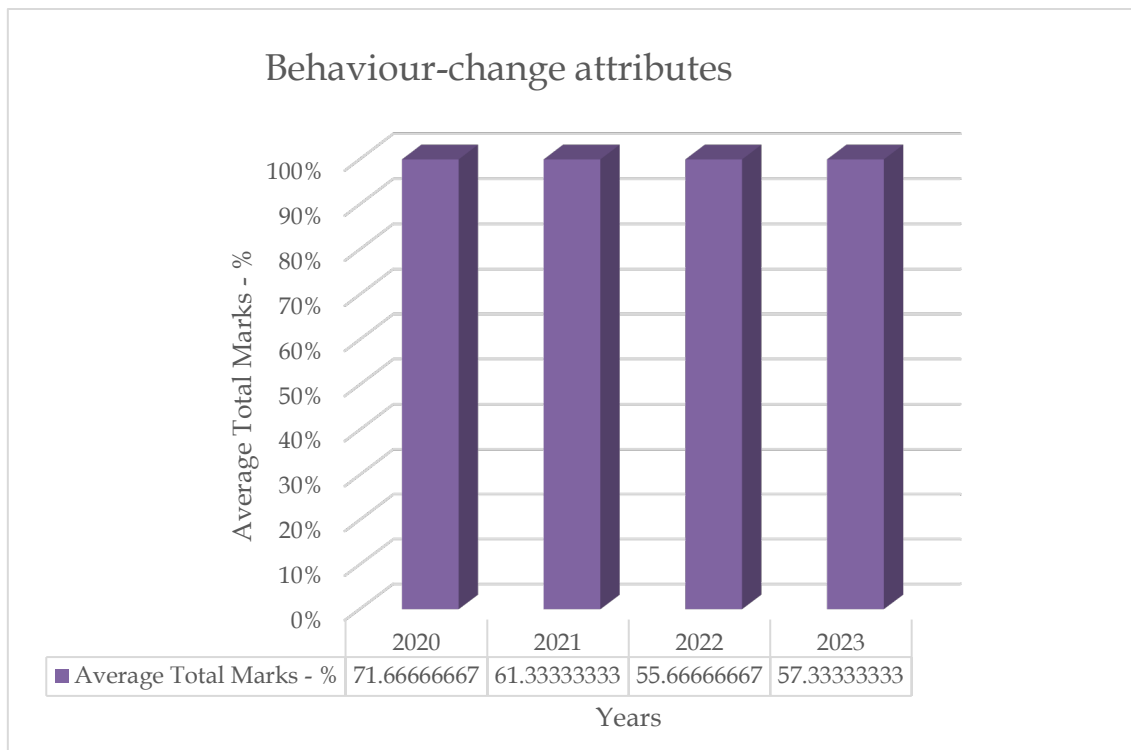
**Figure 5.4:** Chart of overall quality of awareness raising material – 2023

As well the evaluation contains three major categories to rate the infographics. The first category is 'Communication Strategy attributes.' By analyzing the chart (Figure 5.5), the total marks of the category showed that every year the result of the quality is worse year by year and the average total points that the category collects are 5 points. Therefore, the infographics every year do not use key messages or clear purpose on them. Also, the information that the infographics display is too general. The infographics do not refer to a specific audience or a specific time of year.



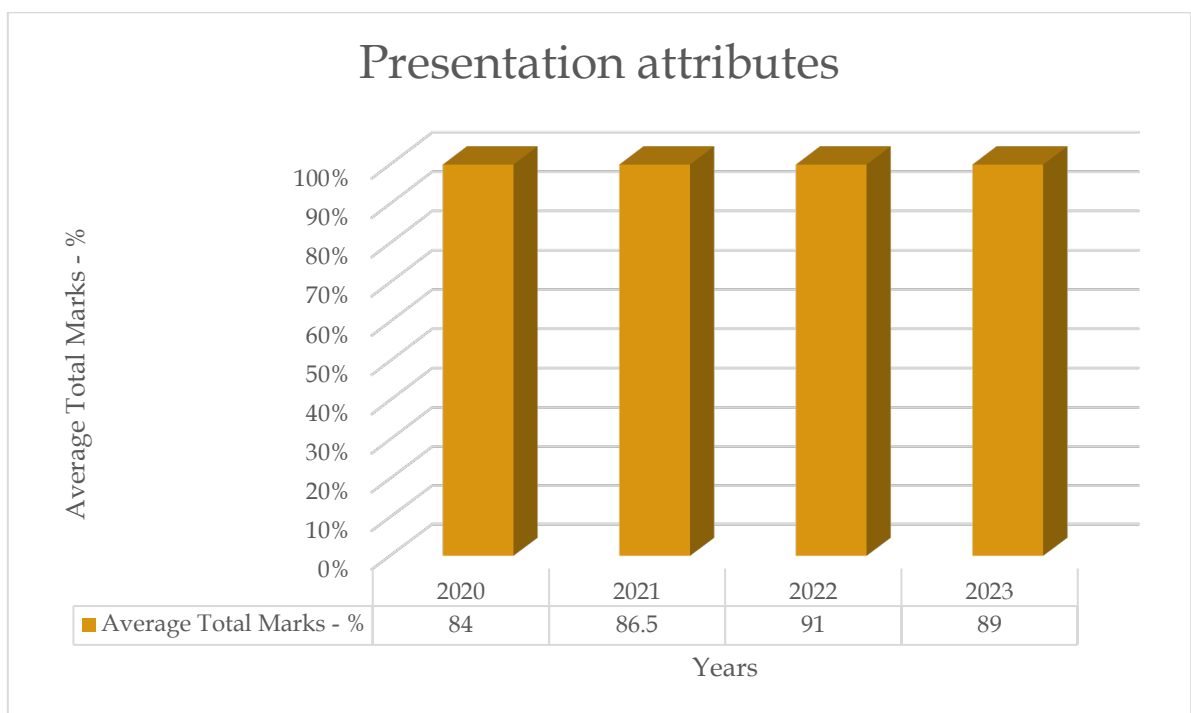
**Figure 5.5:** Chart of communication Strategy attributes

The second category which is called 'Behavior-change attributes' was evaluated and analyzed the average total points of each year as follows (Figure 5.6). The year 2023 was rated 57,33% but 2022 infographics were evaluated by 55,66%. In addition, in the year 2021 the infographics were collected 61,33%. The year 2020 was rated the highest at 71,66%. Also looking at the graph (Figure 5.6) realizing that the best quality of Behavior-change attributes per percent was for years 2020 and 2021. From the year 2020 and after the Behavior-change attributes on infographics shown that are less and less memorable. In addition, they do not empower the audience and they do not promote situational awareness about phishing attacks. Also, the infographics do not contain a lot of evidence-based content so that the readers can understand how it is important to protect themselves from phishing scams.



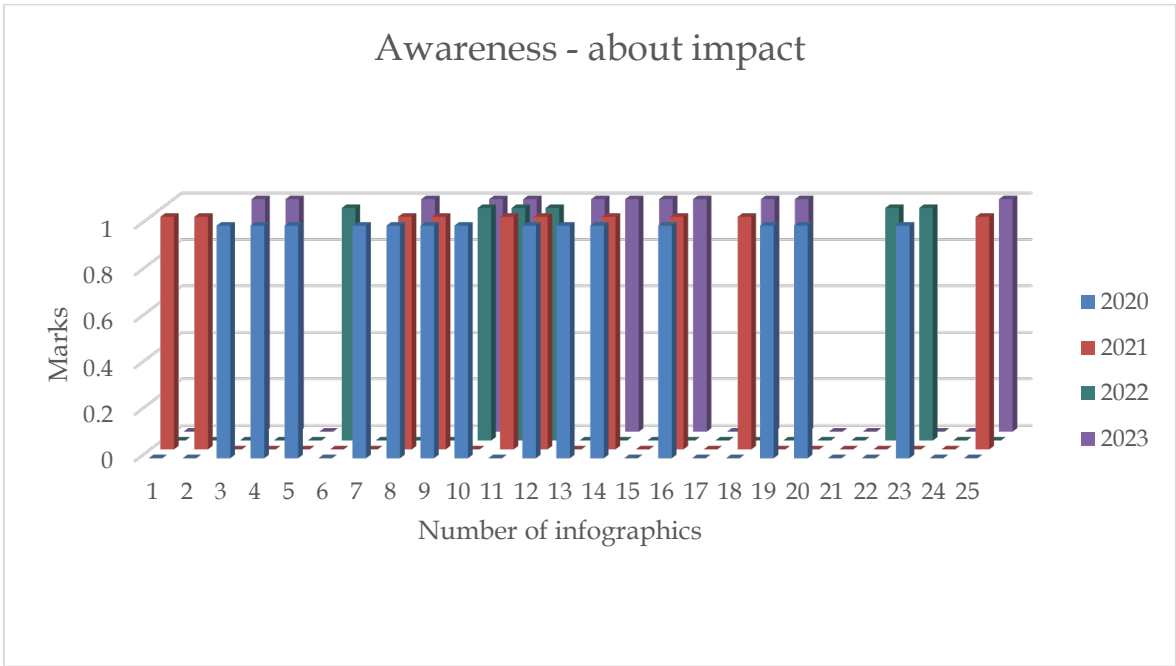
**Figure 5.6:** Chart of Behaviors-change attributes - %

The last major category 'Presentation attributes' was analyzed with the below results. With the following results we observe that the year with the best quality of infographics was 2022 with 91% than that of 2020 that was the lowest quality with 84% (Figure 5.7). Also, 2023 has a total average mark 89% and 2021 has 86,5%. According to the results, the infographics of all four years are keeping the quality in high standards (Figure 5.7). The infographics have a clear message according to the analysis and the infographics have a correct layout, format and fonts and will be readable and pleasant for the reader to read.

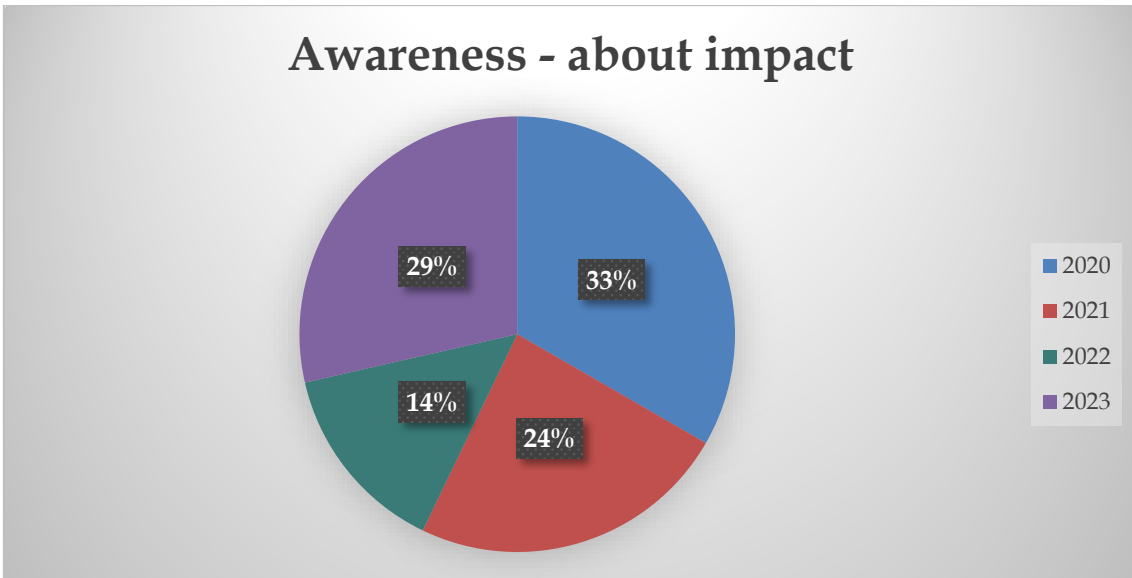


**Figure 5.7:** Chart of Presentation attributes – ‘%’

Delving into the analysis will examine furthermore the subcategories starting with subcategory 'Awareness - about impact' (Figure 5.8). As shown below, the middle years 2021 and 2022 (Figure 5.9) have the lower percentage, that is to say that the infographics for these years have not a lot of awareness about impact on their data display. The year that a lot of infographics have information about the impact that a phishing attack will challenge and inform the readers is 2020.

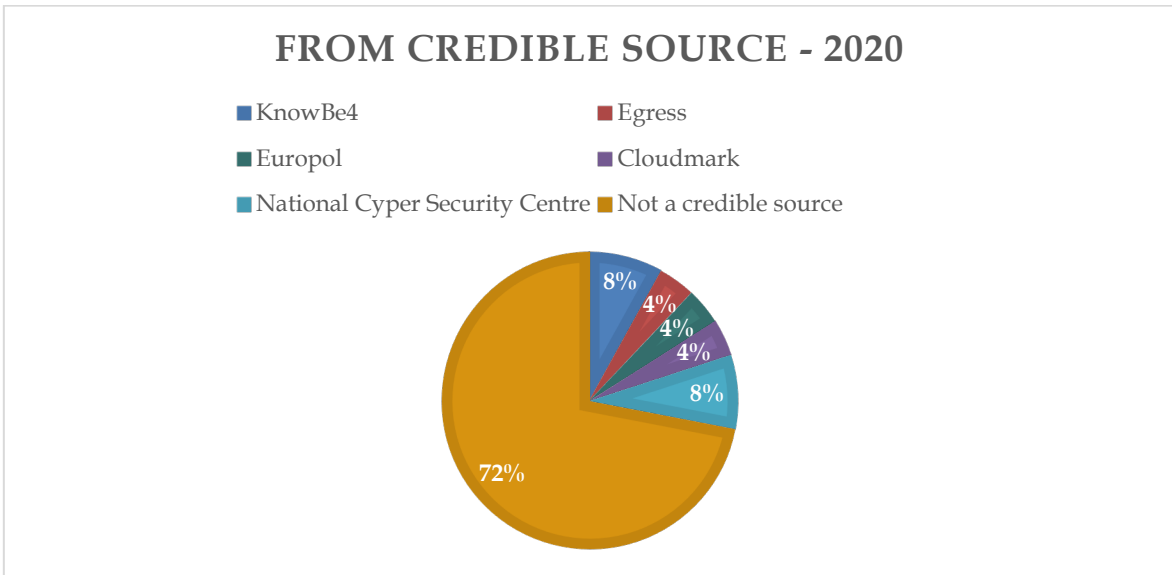


**Figure 5.8:** Chart of Awareness - about impact'

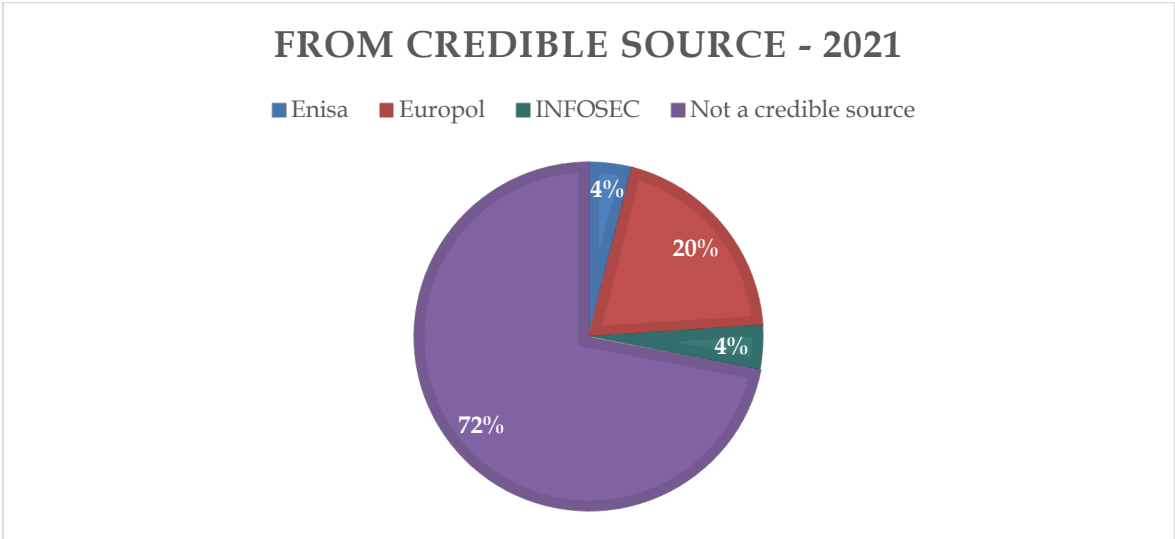


**Figure 5.9:** Chart of Awareness - about impact – ‘%’

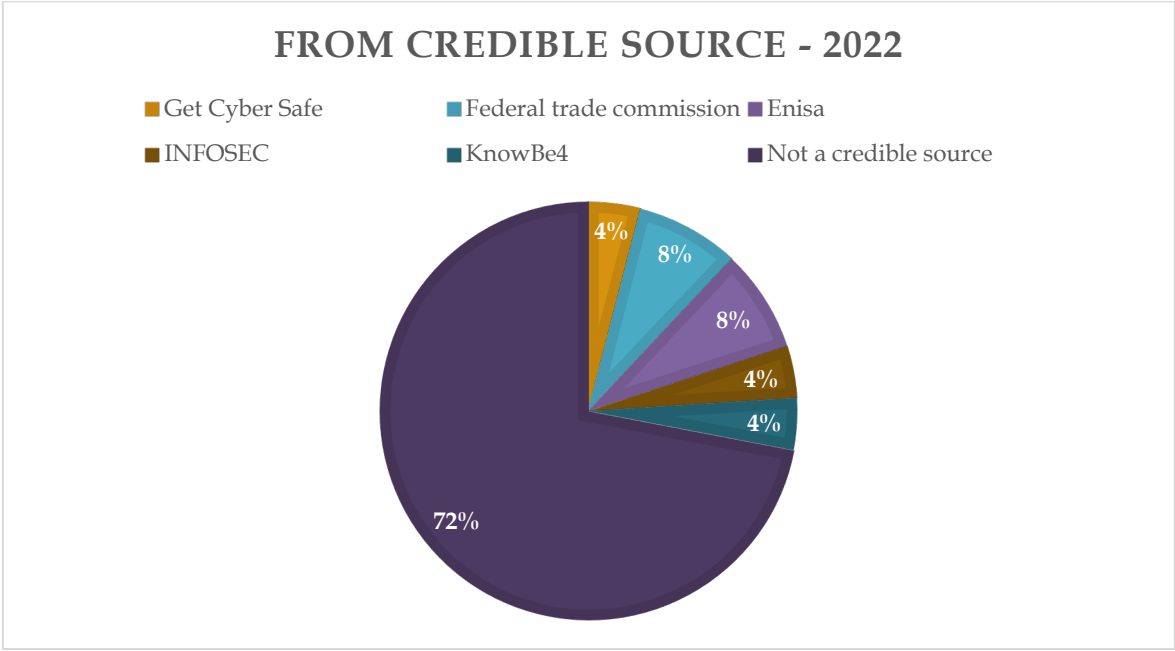
Looking for infographics to analyze using Google search, found out that it was easier to find infographics that was not from credible sources rather from credible sources. For these four years the percentage were the same: a small percentage was credible sources and 72 % - 88% not credible sources (Figure 5.10 to Figure 5.13). So, there is a gap from credible sources to create and share infographics to inform the audience.



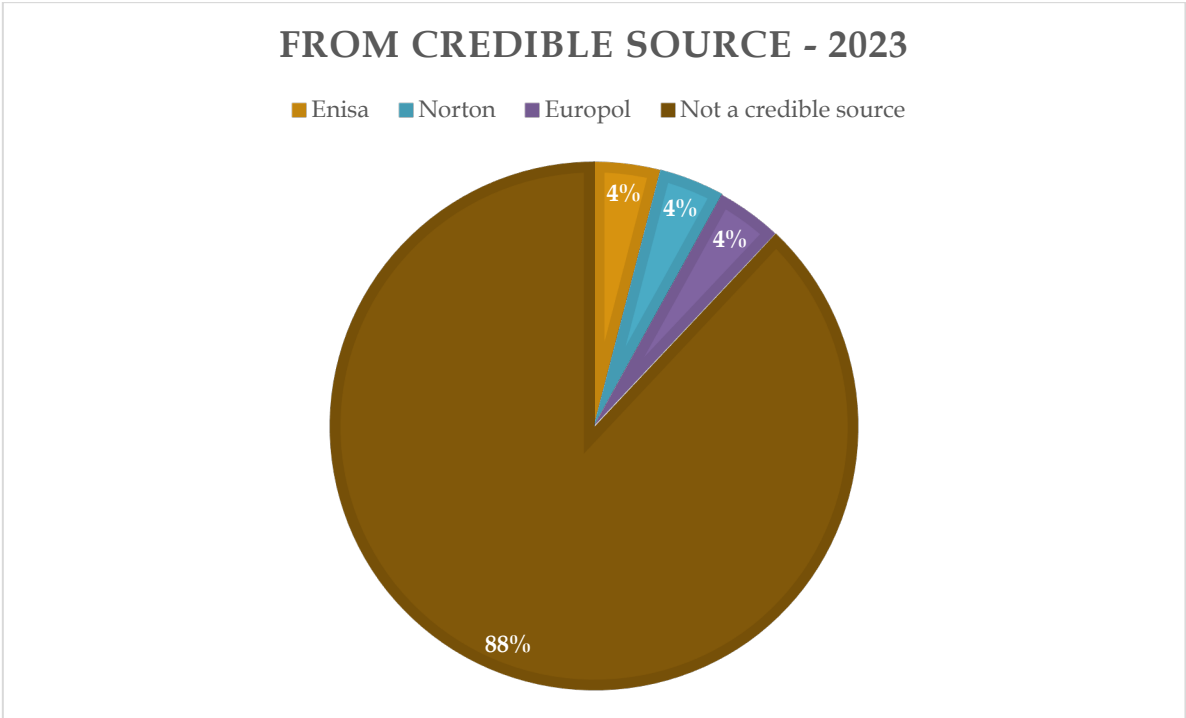
**Figure 5.10:** Chart - Credible source - 2020– ‘%’



**Figure 5.11:** Chart - Credible source - 2021- ‘%’

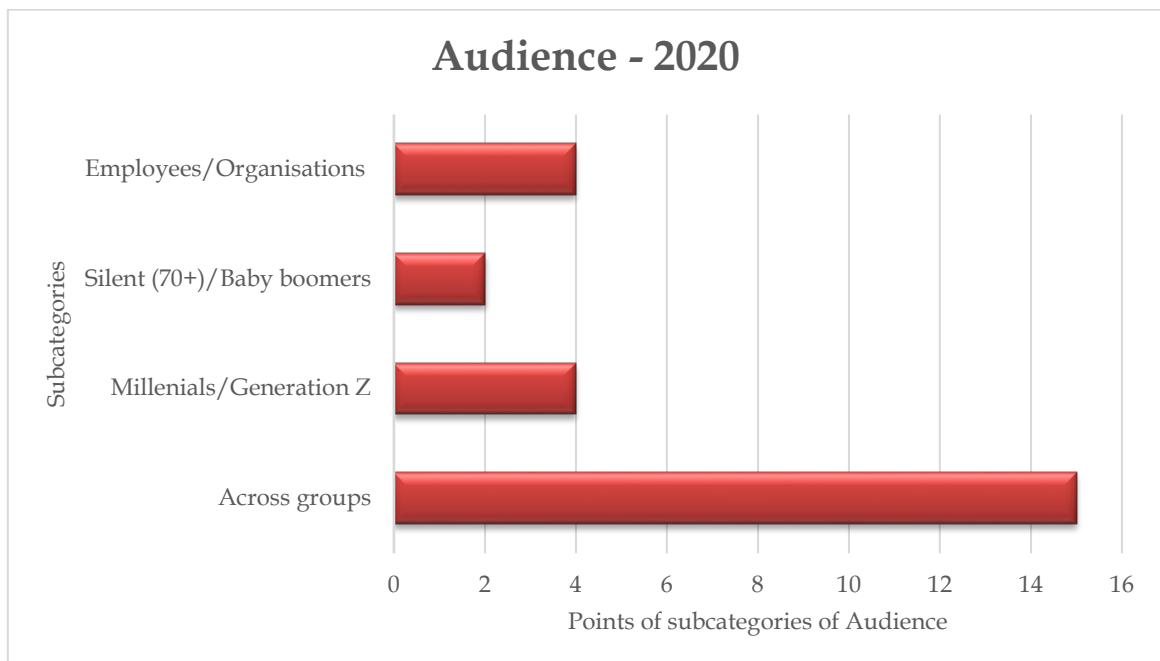


**Figure 5.12:** Chart - Credible source - 2022- ‘%’

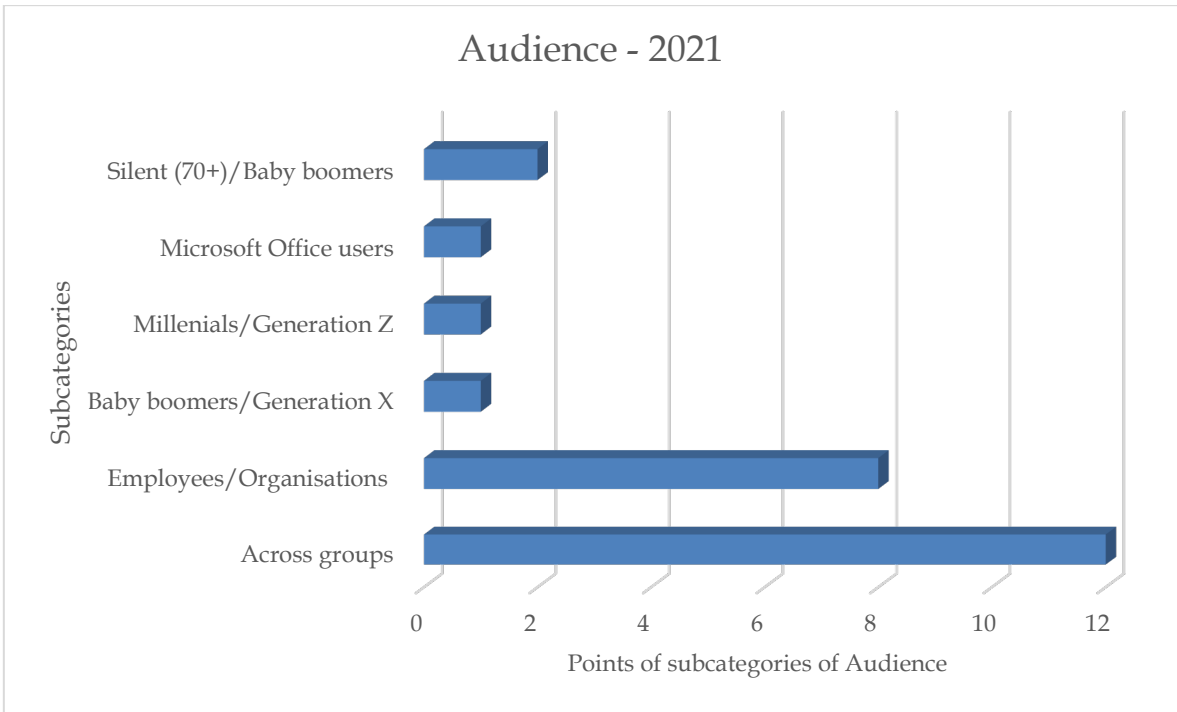


**Figure 5.13:** Chart - Credible source - 2023- ‘%’

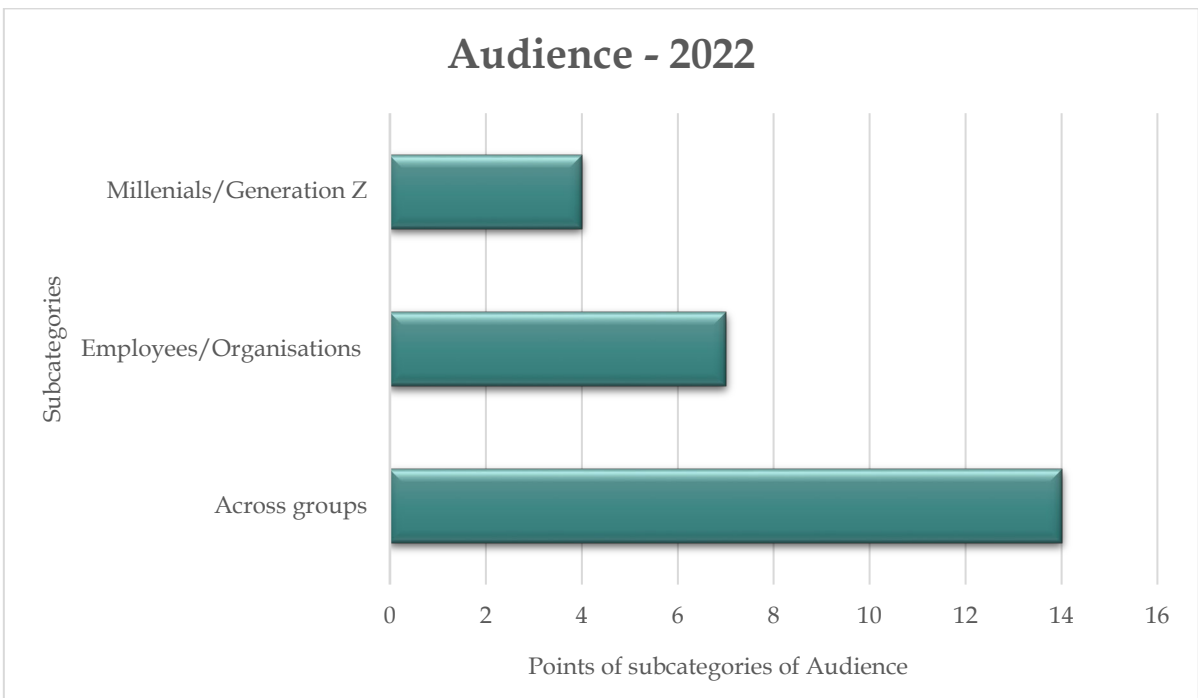
The next subcategory called 'Audience', indicates to whom it is addressed. So, as shown below the most familiar audience that infographics refer to is across groups. Moreover, companies that create infographics choose to mention general information that it concerns everyone. Also, the other category that a lot of infographics write about are related to employees and companies to inform them about how attackers can trick them. Furthermore, the other infographics are referenced in a specific generation (Figure 5.14 to Figure 5.17).



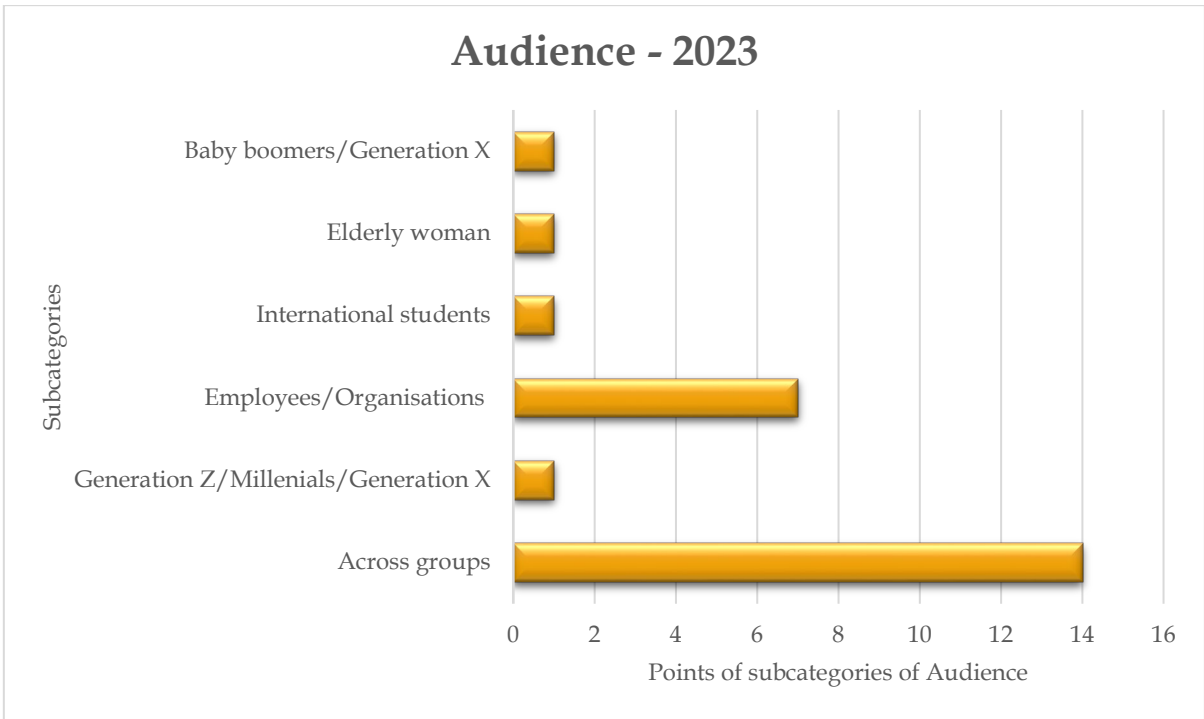
**Figure 5.14:** Chart – Audience – 2020



**Figure 5.15:** Chart – Audience – 2021

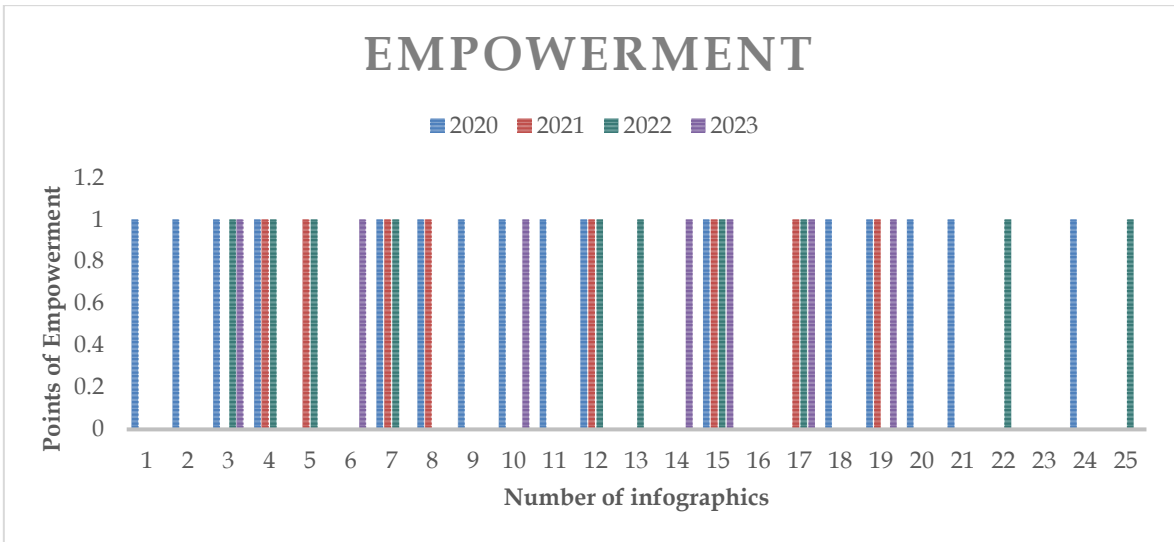


**Figure 5.16:** Chart – Audience – 2022

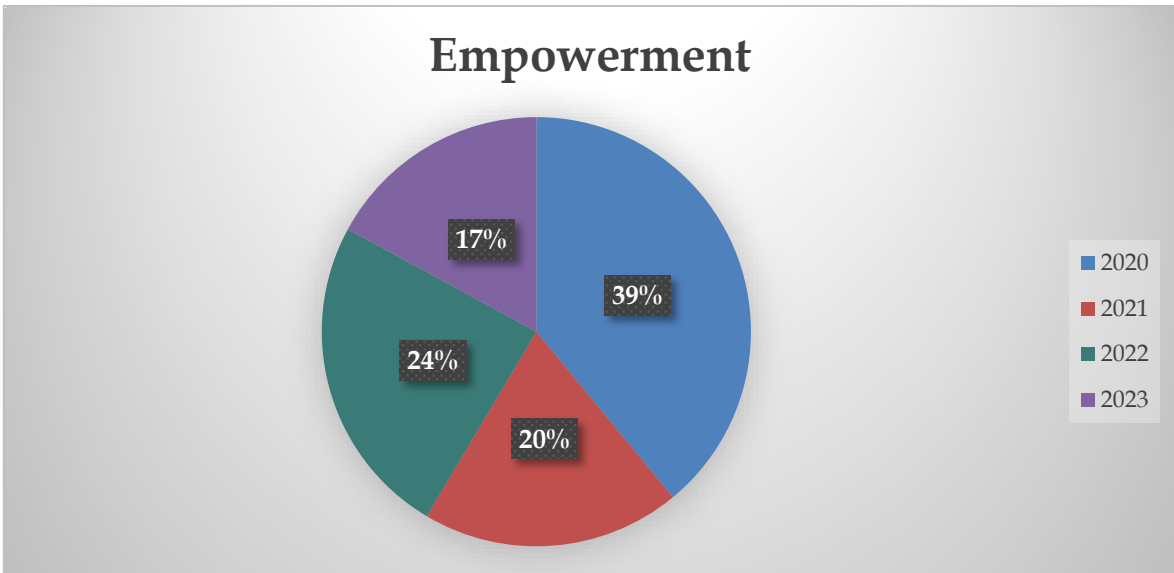


**Figure 5.17:** Chart – Audience – 2023

This subcategory Empowerment shows if infographics contain information about call of action, how the audience can educate about phishing attacks or reporting the incident (Figure 5.19). The results below show that the infographics that were created in 2020 (Figure 5.20) has 39% of empowerment but each year follow the empowerment was less and less and in 2023 has the lower percent of empowerment on infographics.



**Figure 5.18:** Chart – Empowerment - call to action, e.g., visit a website to learn more, to report an incident, etc.



**Figure 5.19:** Chart – Empowerment - call to action, e.g., visit a website to learn more, to report an incident, etc.

Subcategory 'Maximum 4 colors' refer to each infographic having to contain up to four colors because if using too many colors on it, this can detract the audience from the data that is trying to explain (Figure 5.21). Looking at the graphics, the year with the more correct infographics which contains up to four colors is 2023. Also, in general, most infographics use up to four colors (Figure 5.22).

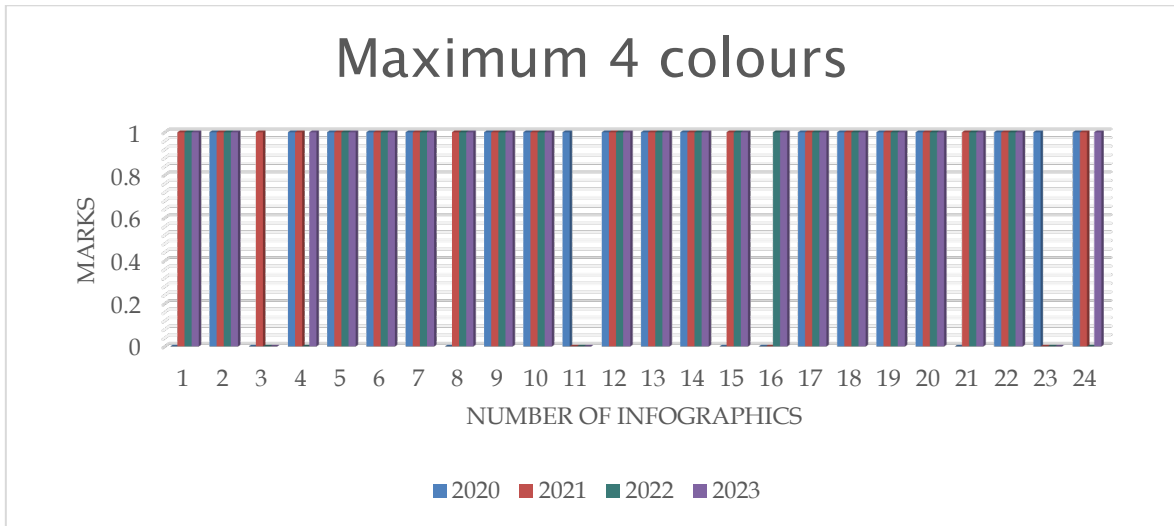


Figure 5.20: Chart – Maximum four colors

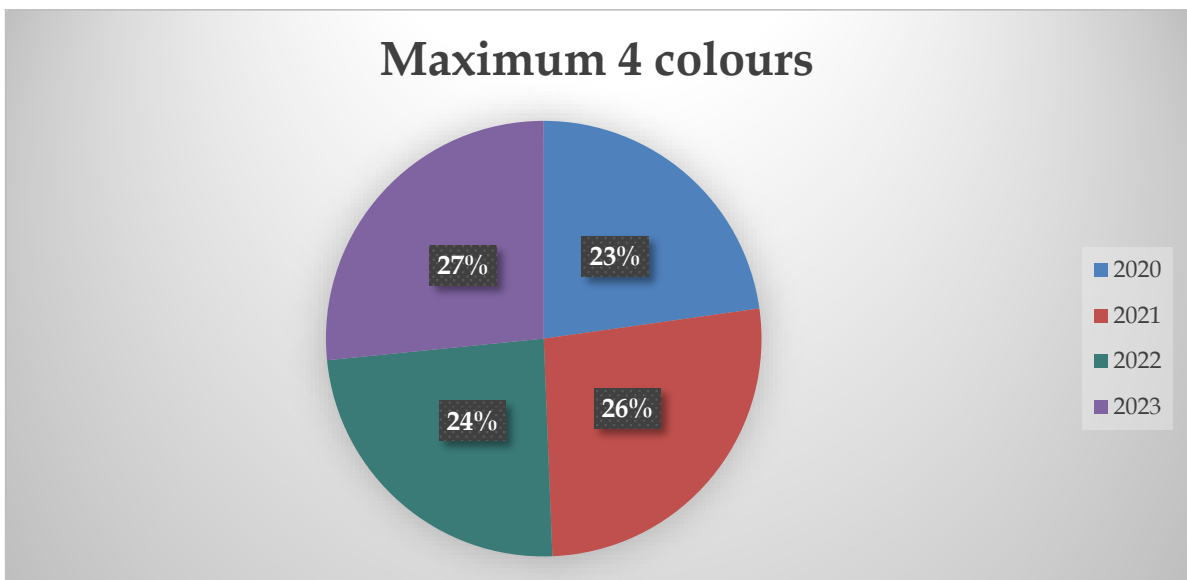


Figure 5.21: Chart – Maximum four colors – %

This subcategory called Appropriate location (Figure 5.23) refers if the infographic is very long or has a normal size and it is easy to read, and the audience find it interesting and not boring, because it is not too big and has not a lot of information. So, the infographics throw out the years almost everyone have the appropriate location (Figure 5.24).

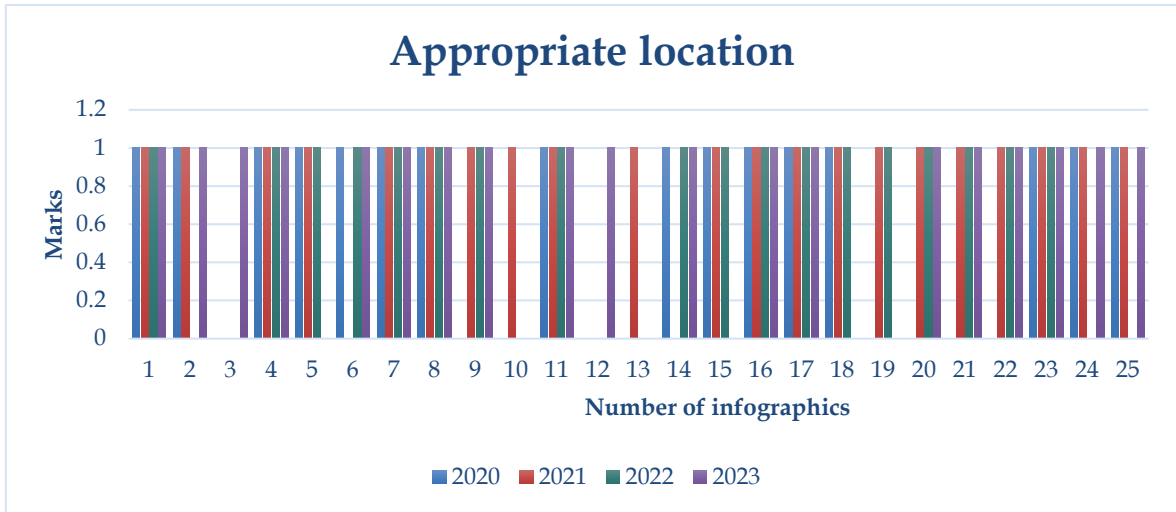


Figure 5.22: Chart – Appropriate location

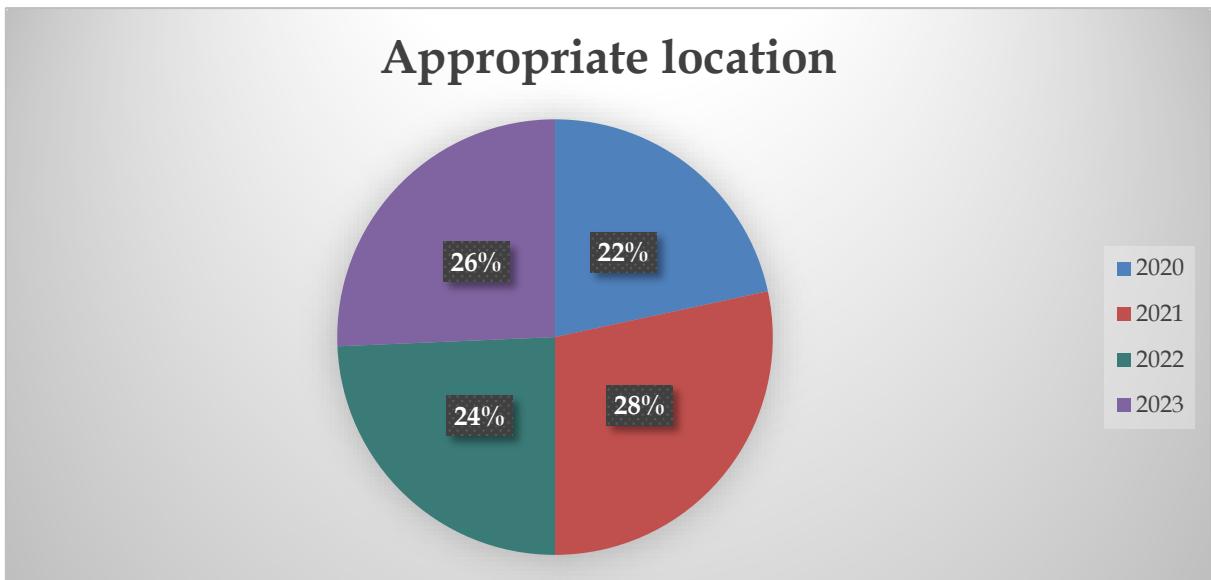
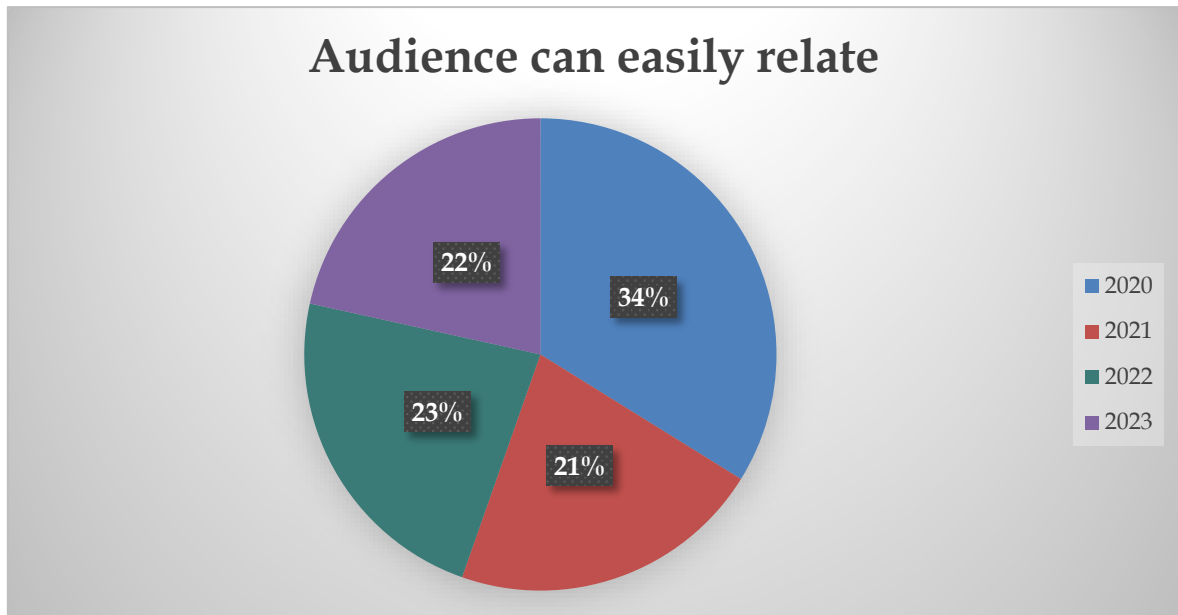


Figure 5.23: Chart – Appropriate location – ‘%’

The subcategory Audience can easily relate, e.g., storytelling tells a story with images, data visualizations, and text, so, the year which has the higher percentage which contains a large number of infographics this subcategory is 2020 and the year which has the lower percentage is 2021 (Figure 5.25). But there is no progression through the years in this category.



**Figure 5.24:** Chart – Audience can easily relate, e.g., storytelling – ‘%’

# **Chapter 6**

## **Recommendation**

After the analysis and the evaluation from the previous chapters, have come to some conclusions. The year with the better overall quality of awareness raising material on the total of twenty-five infographics is 2020. These results showed that instead of improving in quality of infographics every year, their quality is falling. Additionally credible sources that create infographics from 2020 and after having shared fewer phishing infographics than previous years.

Infographics combine visuals, data, and text to tell a complex and important story briefly. Displaying information visually in a clear, structured, and attention-grabbing way. An efficient infographic should have:

- A clear subject and story
  
- A unique, attention-grabbing title and tagline
  
- A clear storyline with a clean and well-structured layout. A layout that supports the audience browsing the information or jumping to the information that interests them the most.
  
- Audience should be able to get the immediate overarching message and then be able to dig deeper into the content with smaller chunks of information.
  
- An engaging and visually driven design ensures the graphic is not too crowded and is eye-catching.
  
- Text and images and data connect the dots of the story, and the story is chunked into sections in a way that makes sense.

- Appropriately themed like colors, designs, fonts, etc., have a big role to play in infographics creation. If the infographic theme looks off or contrasting from what information it's carrying, it can evoke the audience's wrong feelings.

Also, infographics with excessively lengthy text will be demotivating for the audience to read, understand, and practice in everyday life. Instead, these lengthy infographics can use an option like providing a link from where to get detailed information for the interested audience. Obviously, determining how much and what information to include in an infographic is a challenging endeavor and could depend on the audience type. A simple rule could be to concentrate on must-haves.

When laying out an infographic, employ a variety of information, from percentages and ratios to word clouds and bar graphs. This will keep the infographic interesting and show that it is more than just a series of Excel graphs.

In addition, a quality infographic has a typography rule such as:

- Avoid using more than 2-3 font families in the infographic.
- If using a variation of typography, change the styling of current font families.
- The coloring scheme of typography should balance out with icons and other elements.

- If using a different color scheme, the color choice should not exceed 2-3 coloring schemes. Anything more than three will be a deal-breaker for the 'engaging' aspect of the infographics.

As well infographics, have a visual hierarchy that refers to placing elements of a design according to the order of their importance. But this does not mean that every element of visual hierarchy should have a different size.

A great phishing attack infographic that contains the above tips will help protect the audience from successful phishing operations. For example, infographic provides a visual summary of how threat actors execute successful phishing operations. Details include metrics that compare the likelihood of certain types of 'bait' and how commonly each bait type succeeds in tricking the targeted individual. The infographic also provides detailed actions organizations and individuals can take to prevent successful phishing operations, from blocking phishing attempts to teaching individuals how to report successful phishing operations.

# **Chapter 7**

## **Conclusions**

Phishing attacks remain one of the major threats to individuals and organizations to date. Often scammers exploit human vulnerabilities in addition to technical vulnerabilities. It has been identified that age, gender, internet addiction, user stress, and many other attributes affect the susceptibility to phishing between people. Also, to traditional phishing channels (e.g., email, etc.), new types of phishing such as voice and SMS phishing are on the increase. Furthermore, the use of social media-based phishing has increased in use in parallel with the growth of social media. Concomitantly, phishing has developed beyond obtaining sensitive information and financial crimes to cyber hacktivism, damaging reputations, and nation-state attacks. This provides a wider outlook for phishing attacks and provides an accurate definition covering end-to-end exclusion and realization of the attack.

Although human education is the most effective defense for phishing, it is difficult to remove the threat completely due to the sophistication of the attacks and social engineering elements. Although continual security awareness training is the key to avoid phishing attacks and to reduce its impact, developing efficient anti-phishing techniques that prevent users from being exposed to the attack is an essential step in mitigating these attacks.

Furthermore, the goal of cybersecurity awareness is to change people's security knowledge, attitude, and behavior by putting what they have learned into practice. To raise people's cybersecurity awareness, security messages are communicated to them using diverse channels. Infographics are one of the most used channels. In spite of, very little effort has been made to produce a more uniform and effective infographics for cybersecurity awareness purposes. Further, approach used for cybersecurity awareness infographic design and its quality assessment. Therefore, addressing these issues of non-uniformity in cybersecurity awareness infographic design, and systematize the approach used for its design and quality assessment.

At the end a great phishing infographic must stand out to the audience. To create an effective and eye-catching infographic, there are some tips to keep infographics on track.

- Create an infographic that speaks for a target audience.
  
- Make the focal point stand out.
  
- Tell a story
  
- Make it simple
  
- Use contrasting colors

Concluded that a quality phishing attacks infographic will have to have the above structure that is analyzed in the previous chapters to be easier for the targeted readers to understand the thread and how to avoid the attack. Also, can include a link with more information if the reader wants to continue the reading. So, if the audience are properly informed it is easier to prevent and block successful phishing operations.

# **Appendix A**

## **Analysis Infographics**

# A.1 Analysis Infographics 2020

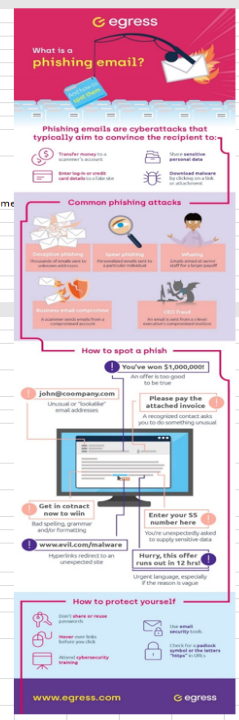
The excel file contains all the evaluation of the twenty-five infographics for the year 2020.



infographics\_frame  
work\_v2020.xlsx

1)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1														
2		<b>Communication Strategy attributes</b>				<b>Evaluation</b>								
3							Infographic - website	<a href="https://www.egress.com/blog/phishing/how-to-spot-a-phishing-email">https://www.egress.com/blog/phishing/how-to-spot-a-phishing-email</a>						
4														
5		1	Audience	Marks			Marks	Comments						
6			1.1 Across groups	1				1	Individuals and Employees					
7			1.2 Specific	2										
8														
9		2	Key message focus - clear purpose											
10			2.1 Awareness - about threat	1				1	List key information to know about phishing emails and how to spot them.					
11			2.2 Awareness - about impact	1										
12			2.3 Cyber hygiene - best practices	1				1	Tips to protect them selves from phishing emails					
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1				1	Call to action to detect and protect them selves but we don't see any powerful me					
14			2.4											
15		3	Timeframe											
16			3.1 Generic	1				1						
17			3.2 Covers specific time periods	2										
18														
19														
20														
21														
22		1	Promote situational awareness											
23			Easy to understand what is the threat	1				1	Easy to understand how to detect phishing emails					
24			Easy to understand what is the impact	1				0	Easy to protect them selves with examples					
25														
26		2	Empower people											
27			Simple information to understand how to address the threat	1				1						
28			Appropriate call to action message	1										
29			Overall conveys a positive message	1				neutral						
30			2.3											
31		3	Evidence-based content											
32			Based on facts, e.g. statistics, etc.	1				1						
33			3.2 From credible source	1				1	Egress					
34														
35		4	Memorable											
36			Micro-learning - specific 4.1 topic	1				1	email phishing					
37			Micro-learning - short statements, focus on key points	1				1						
38			4.2 Considers different learning styles	1				1	visual, text					
39			4.3 Balance between graphics and text	1				1						
40			4.4 Audience can easily relate, e.g. storytelling	1				1	Easy to explain the problem and give a solution, provides a real example					
41														
42														
43														
44		1	Visibility of the message											
45			1.1 Appropriate location	1				1						
46			Draw attention to key information, e.g. by using contrasting colour	1				1						
47			1.2											
48		2	Layout, style and formatting											
49			Uses lines, borders and shapes to group related information	1				1						
50			2.1 Create text hierarchy (up to 3 different font styles)	1				1						
51			2.2											
52			2.3 Maximum 4 colours	1										
53		3	Inclusive / Accessible											
54			A good color contrast between the text color and background color	1										
55			3.1 Use appropriate font styles ( )	1				1						
56			3.2 Use appropriate font size	1										
57			3.3 ( )	1										
58														
59														
60														
61														
62			Communication Strategy attributes					5						
63			Behaviour-change attributes					9						
64			Presentation attributes					5						
65								19						
66														
67														
68			Overall quality of awareness raising material											
69			Low 0-14											
70			Medium 15-22											
71			High 23-28											
72														



2)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2		Communication Strategy attributes				Evaluation									
3						Infographic - website	<a href="https://www.knowbe4.com/press/q2-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-spike">https://www.knowbe4.com/press/q2-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-spike</a>								
4															
5		1	Audience	Marks		Marks	Comments								
6			1.1 Across groups	1											
7			1.2 Specific	2			Millennials/Generation Z								
8															
9		2	Key message focus - clear purpose												
10			2.1 Awareness - about threat	1			Top 10 General email subjects of phishing emails								
11			2.2 Awareness - about impact	1											
12			2.3 Cyber hygiene - best practices				Subjects to avoid phishing emails								
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			Call to action(key takeaway)								
14															
15		3	Timeframe												
16			3.1 Generic	1			It can be advertised at any time								
17			Covers specific time periods	2											
18															
19															
20		Behaviour-change attributes													
21		1	Promote situational awareness												
22			Easy to understand what is the threat	1											
23			Easy to understand what is the impact	1											
24															
25		2	Empower people												
26			Simple information to understand how to address the threat	1											
27			Appropriate call to action message	1											
28			Overall conveys a positive message	1											
29															
30		3	Evidence-based content												
31			Based on facts, e.g. statistics, etc.	1											
32			From credible source	1			KnowBe4								
33															
34		4	Memorable												
35			Micro-learning - specific topic	1			email phishing								
36			Micro-learning - short statements, focus on key points	1											
37			Considers different learning styles	1			yes, visual and text								
38			Balance between graphics and text	1											
39			Audience can easily relate, e.g. storytelling	1			real examples								
40															
41															
42		Presentation attributes													
43		1	Visibility of the message												
44			1.1 Appropriate location	1											
45			Draw attention to key information, e.g. by using contrasting colour	1											
46															
47		2	Layout, style and formatting												
48			Uses lines, borders and shapes to group related information	1											
49			2.1 Create text hierarchy (up to 3 different font styles)	1											
50			2.2 Maximum 4 colours	1											
51															
52															
53		3	Inclusive / Accessible												
54			A good color contrast between the text color and background color	1											
55			Use appropriate font styles	1											
56			Use appropriate font size (l)	1											
57															
58															
59															
60															
61		Communication Strategy attributes				6									
62		Behaviour-change attributes				9									
63		Presentation attributes				7									
64															
65		TOTAL				22									
66															
67		Overall quality of awareness raising material													
68			Low	0-14											
69			Medium	15-22											
70			High	23-28											
71															
72															

**TOP-CCLICKED PHISHING TESTS**

**TOP SOCIAL MEDIA EMAIL SUBJECTS**

- LinkedIn: 40%
- Facebook: 13%
- Twitter: 11%
- Instagram: 10%
- WhatsApp: 10%
- YouTube: 10%
- Google+: 9%
- Skype: 7%
- Telegram: 7%

**TOP 10 GENERAL EMAIL SUBJECTS**

- Password Check Required Immediately: 40%
- CDC Health Alert Network: Coronavirus Outbreak Cases: 10%
- FTD Policy Changes: 7%
- Scheduled Server Maintenance - No Internet Access: 7%
- Test of the Emergency Alarm/ Emergency Notification System: 6%
- Remote Workforce SSO Time Policy: 6%
- Discontinuation of Emails in Process: 6%
- Please Read Important from Human Resources: 5%
- Someone special sent you a Valentine's Day ecard: 5%
- You have been added to a Team in Microsoft Teams: 5%

**NEW TAKEAWAY**

Spammers are playing the numbers game to remain mostly undetected. Unfortunately, the more you click on the subject line, the more likely you are to be targeted. Carefully read the subject line for the sender and about the email. Consider the sender's email address and the subject line. If you receive an email that looks suspicious, do not click on the subject line. Instead, hover over the subject line to see the full subject line. If you are still unsure, delete the email.

3)

Communication Strategy attributes			Evaluation	
Infographic - website			<a href="https://inspiredelearning.com/resource/social-media-phishing-infographic/">https://inspiredelearning.com/resource/social-media-phishing-infographic/</a>	
1	Audience	Marks	Marks	Comments
6	1.1 Across groups	1		
7	1.2 Specific	2		
9	2 Key message focus - clear purpose			
10	2.1 Awareness - about threat	1		1 Social media users is now being targeted in social media phishing attacks.
11	2.2 Awareness - about impact	1		1 Social media phishing statistics, examples, and tips for protecting yourself from attacks.
12	2.3 Cyber hygiene - best practices	1		1
13	2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1 Report the incident
15	3 Timeframe			
16	3.1 Generic	1		1
17	3.2 Covers specific time periods	2		
Behaviour-change attributes				
21	1 Promote situational awareness			
23	1.1 Easy to understand what is the threat	1		1
24	1.2 Easy to understand what is the impact	1		1
26	2 Empower people			
27	2.1 Simple information to understand how to address the threat	1		1
28	2.2 Appropriate call to action message	1		1
29	2.3 Overall conveys a positive message	1		
31	3 Evidence-based content			
32	3.1 Based on facts, e.g. statistics, etc.	1		1
33	3.2 From credible source	1		0
34				
35	4 Memorable			
36	4.1 Micro-learning - specific topic	1		1
37	4.2 Micro-learning - short statements, focus on key points	1		1
38	4.3 Considers different learning styles	1		1
39	4.4 Balance between graphics and text	1		0 overall a bit crowded
40	4.5 Audience can easily relate, e.g. storytelling	1		1
41				
Presentation attributes				
44	1 Visibility of the message			
45	1.1 Appropriate location	1		0
46	1.2 Draw attention to key information, e.g. by using contrasting colour	1		1
47	2 Layout, style and formatting			
49	2.1 Uses lines, borders and shapes to group related information	1		1
50	2.2 Create text hierarchy (up to 3 different font styles)	1		1
51	2.3 Maximum 4 colours	1		
52				
53	3 Inclusive / Accessible			
54	3.1 A good color contrast between the text color and background color	1		
55	3.2 Use appropriate font styles	1		1
56	3.3 Use appropriate font size	1		
57				
61	Communication Strategy attributes	6		
62	Behaviour-change attributes	9		
63	Presentation attributes	4		
64				
65	<b>TOTAL</b>	<b>19</b>		
66				
67	Overall quality of awareness raising material			
68	Low 0-14			
69	Medium 15-22			
70	High 23-28			
71				
72				



4)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
2	Communication Strategy attributes				Evaluation														
3					Infographic - website <a href="https://designedprivacy.com/phishing-infographic/">https://designedprivacy.com/phishing-infographic/</a>														
5	1	Audience		Marka		Marka		Comments											
6		1,1	Across groups	1				1											
7		1,2	Specific	2															
9	2	Key message focus - clear purpose																	
10		2,1	Awareness - about threat	1				1	Phishing Frequency/Phishing Trends/Keep your self from getting tricked										
11		2,2	Awareness - about impact	1															
12		2,3	Cyber hygiene - best practices	1				1	breath out										
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1				1	Call to an action - visit a website to learn more										
15	3	Timeframe																	
16		3,1	Generic	1				1											
17		3,2	Covers specific time periods	2															
20	Behaviour-change attributes																		
22	1	Promote situational awareness																	
23		1,1	Easy to understand what is the threat	1				1											
24		1,2	Easy to understand what is the impact	1															
26	2	Empower people																	
27		2,1	Simple information to understand how to address the threat	1				1											
28		2,2	Appropriate call to action message	1				1											
29		2,3	Overall conveys a positive message	1															
31	3	Evidence-based content																	
32		3,1	Based on facts, e.g. statistics, etc.	1				1											
33		3,2	From credible source	1															
35	4	Memorable																	
36		4,1	Micro-learning - specific topic	1				1											
37		4,2	Micro-learning - short statements, focus on key points	1				1											
38		4,3	Considers different learning styles	1				1											
39		4,4	Balance between graphics and text	1															
40		4,5	Audience can easily relate, e.g. storytelling	1															
42	Presentation attributes																		
44	1	Viability of the message																	
45		1,1	Appropriate location	1				1											
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1				1											
48	2	Layout, style and formatting																	
49		2,1	Use lines, borders and shapes to group related information	1				1											
50		2,2	Create text hierarchy (up to 3 different font styles)	1															
51		2,3	Maximum 4 colours	1				1											
53	3	Inclusive / Accessible																	
54		3,1	A good color contrast between the text color and background color	1															
55		3,2	Use appropriate font styles (i)	1															
56		3,3	Use appropriate font size (i)	1															
61	Communication Strategy attributes					6													
62	Behaviour-change attributes					7													
63	Presentation attributes					4													
65	TOTAL					17													
67	Overall quality of awareness raising material																		
68	Low					0-14													
69	Medium					15-22													
70	High					23-28													

**PHISHING: A Hacker's Delight**

### 1. PHISHING FREQUENCY

Phish remain a top method of attack – and are more successful than you might think

- 65% of US businesses experienced a successful phishing attack in 2020
- 96% of social engineering attacks are phishing
- 13% of users who open phishing emails engage with the email (click links, open attachments, etc.)

Phishing is the LEADING CAUSE of data breaches

### 2. PHISHING TRENDS

Scammers are using the pandemic to their benefit

- +3,000% increase in COVID-related phishing attacks in the first half of 2020
- 2/3 of all phishing attempts impersonate well-known brands
- Attackers frequently impersonate public health organizations, such as the WHO and the CDC

Phishing Attacks by Method

- 66% Impersonation
- 22% Suspicious Links
- 9% User-like Domains
- 3% Compromised Domains

### 3. BREATHE O.U.T.

Phishing attacks exploit human vulnerabilities. To keep yourself from getting tricked, use the Breathe O.U.T. method. First, take a breath before opening an email, then:

- O. Observe the sender** - Is the email coming from the right place?
- U. Check URLs and attachments** - Are they taking you to the right place?
- T. Take time** - Does anything look suspicious to you?

Learn more at [designedprivacy.com/blog](https://designedprivacy.com/blog)

SOURCES:  
<https://www.fish.com/industry-highlights/2020-2021-annual-report/>  
<https://www.gartner.com/en/newsroom/press-releases/2020-08-11-phishing-attacks>  
<https://www.pewresearch.org/internet/2020/08/11/phishing/>

designedprivacy

5)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>											
3						Infographic - website	<a href="https://veritau.co.uk/phishing-and-its-risks-cyber-security-month/">https://veritau.co.uk/phishing-and-its-risks-cyber-security-month/</a>									
4																
5	1	Audience	Marks		Marks	Comments										
6		1,1	Across groups	1												
7		1,2	Specific	2		General information about phishing and its risks										
8																
9	2	Key message focus - clear purpose														
10		2,1	Awareness - about threat	1												
11		2,2	Awareness - about impact	1												
12		2,3	Cyber hygiene - best practices	1		look for signs										
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1												
14																
15	3	Timeframe														
16		3,1	Generic	1												
17		3,2	Covers specific time periods	2		Holidays or out of the office										
18																
19																
20	<b>Behaviour-change attributes</b>															
21	1	Promote situational awareness														
22		1,1	Easy to understand what is the threat	1												
23		1,2	Easy to understand what is the impact	1												
24																
25																
26	2	Empower people														
27		2,1	Simple information to understand how to address the threat	1												
28		2,2	Appropriate call to action message	1												
29		2,3	Overall conveys a positive message	1												
30																
31	3	Evidence-based content														
32		3,1	Based on facts, e.g. statistics, etc.	1		use statistics										
33		3,2	From credible source	1												
34																
35	4	Memorable														
36		4,1	Micro-learning - specific topic	1												
37		4,2	Micro-learning - short statements, focus on key points	1												
38		4,3	Consider different learning styles	1												
39		4,4	Balance between graphics and text	1												
40		4,5	Audience can easily relate, e.g. storytelling	1												
41																
42	<b>Presentation attributes</b>															
43	1	Visibility of the message														
44		1,1	Appropriate location	1												
45		1,2	Draw attention to key information, e.g. by using contrasting colour	1												
46																
47	2	Layout, style and formatting														
48		2,1	Uses lines, borders and shapes to group related information	1												
49		2,2	Create text hierarchy (up to 3 different font styles)	1												
50		2,3	Maximum 4 colours	1												
51																
52	3	Inclusive / Accessible														
53		3,1	A good color contrast between the text color and background color	1												
54		3,2	Use appropriate font styles ()	1												
55		3,3	Use appropriate font size ()	1												
56																
57																
58																
59																
60																
61	<b>Communication Strategy attributes</b>					6										
62	<b>Behaviour-change attributes</b>					8										
63	<b>Presentation attributes</b>					8										
64																
65	<b>TOTAL</b>					22										
66																
67	Overall quality of awareness raising material															
68	Low	0-14														
69	Medium	15-22														
70	High	23-28														

CYBER SECURITY AWARENESS MONTH 

# PHISHING AND ITS RISKS

**What is phishing?**  
Phishing is a technique cybercriminals use to con you into giving them your data. They can gain access to financial information, personal data, or even bank accounts.

**How fraudsters target you**

 **EMAIL**  **PHONE**  **LETTER**

Phishing is often the gateway to different types of cyber fraud. The communication may ask you to enter your username and password, to hack your account and steal data, money, or install ransomware or malware.

 **22% of DATA BREACHES** involve phishing

**94% of MALWARE** is delivered by email 

Look out for...

- SENDER ADDRESS**
- POOR SPELLING/ GRAMMAR**
- SPOOFED EMAILS**
- SENSE OF URGENCY**
- BAD QUALITY COMMUNICATIONS**

Cybercriminals often use social engineering, monitoring social media to time their emails or phone calls for when people are on holiday or out of the office.

Source: Verizon DBIR, Gallagher 

6)

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>															
3						Infographic - website	<a href="https://verba.co.uk/shopping-and-it-risk-cyber-security-month/">https://verba.co.uk/shopping-and-it-risk-cyber-security-month/</a>													
4																				
5	<b>Audience</b>		<b>Marks</b>		<b>Marks</b>		<b>Comments</b>													
6	1,1	Across groups	1			0														
7	1,2	Specific	2			2	Slent (70+) / Baby boomers													
8																				
9	<b>Key message focus - clear purpose</b>																			
10	2,1	Awareness - about threat	1			1	holidayscams													
11	2,2	Awareness - about impact	1			0														
12		Cyber hygiene - best practices	1			1														
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																	
14																				
15	<b>Timeframe</b>																			
16	3,1	Generic	1																	
17	3,2	Covers specific time periods	2			2	Holidays period													
18																				
19																				
20	<b>Behaviour-change attributes</b>																			
21																				
22	<b>Promote situational awareness</b>																			
23	1,1	Easy to understand what's the threat	1			1														
24	1,2	Easy to understand what's the impact	1			0														
25																				
26	<b>Empower people</b>																			
27	2,1	Simple information to understand how to address the threat	1			1	different types of holiday scams													
28	2,2	Appropriate call to action message	1																	
29	2,3	Overall conveys a positive message	1																	
30																				
31	<b>Evidence-based content</b>																			
32	3,1	Based on facts, e.g. statistics, etc.	1																	
33	3,2	From credible source	1			1	KnowBe4													
34																				
35	<b>Memorable</b>																			
36	4,1	Micro-learning - specific topic	1			1														
37	4,2	Micro-learning - short statements, focus on key points	1																	
38	4,3	Considers different learning styles	1			1														
39	4,4	Balance between graphics and text	1			1														
40	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples													
41																				
42	<b>Presentation attributes</b>																			
43																				
44	<b>Visibility of the message</b>																			
45	1,1	Appropriate location	1			1														
46	1,2	Draw attention to key information, e.g. by using contrasting colour	1			1														
47																				
48	<b>Layout, style and formatting</b>																			
49	2,1	Use lines, borders and shapes to group related information	1			1														
50	2,2	Create text hierarchy (up to 3 different font styles)	1			1														
51	2,3	Maximum 4 colours	1			1														
52																				
53	<b>Inclusive / Accessible</b>																			
54	3,1	A good color contrast between the text color and background color	1																	
55	3,2	Use appropriate font styles ()	1			1														
56	3,3	Use appropriate font size ()	1			1														
57																				
58																				
59																				
60																				
61	<b>Communication Strategy attributes</b>				6															
62	<b>Behaviour-change attributes</b>				7															
63	<b>Presentation attributes</b>				7															
64																				
65	<b>TOTAL</b>				20															
66																				
67	<b>Overall quality of awareness raising material</b>																			
68	<b>Low</b> 0-14																			
69	<b>Medium</b> 15-22																			
70	<b>High</b> 23-28																			



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2			Communication Strategy attributes				Evaluation															
3							Infographic - website	<a href="https://twitter.com/envisiontech/status/111362541236482290">https://twitter.com/envisiontech/status/111362541236482290</a>														
4																						
5		1	Audience	Markets			Markets	Comments														
6			1.1	Across groups	1																	
7			1.2	Specific	2			2														
8																						
9		2	Key message focus - clear purpose																			
10			2.1	Awareness - about threat	1			1	Avoid online scams on season holidays													
11			2.2	Awareness - about impact	1			1														
12			2.3	Cyber hygiene - best practices	1			1	tips what you can do if you are a victim													
13			2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report the incident													
14																						
15		3	Timeframe																			
16			3.1	Generic	1																	
17			3.2	Covers specific time periods	2			2	Holiday period													
18																						
19																						
20			Behaviour-change attributes																			
21		1	Promote situational awareness																			
22			1.1	Easy to understand what is the threat	1			1														
23			1.2	Easy to understand what is the impact	1			1														
24																						
25																						
26		2	Empower people																			
27			2.1	Simple information to understand how to address the threat	1			1	How to avoid scams													
28			2.2	Appropriate call to action message	1			1	what to do if you're a victim													
29			2.3	Overall conveys a positive message	1			neutral														
30																						
31		3	Evidence-based content																			
32			3.1	Based on facts, e.g. statistics, etc.	1			1	examples of scams													
33			3.2	From credible source	1																	
34																						
35		4	Memorable																			
36			4.1	Micro-learning - specific topic	1			1														
37			4.2	Micro-learning - short statements, focus on key points	1			1														
38			4.3	Considers different learning styles	1			1														
39			4.4	Balance between graphics and text	1			1														
40			4.5	Audience can easily relate, e.g. storytelling	1			1	real examples													
41																						
42			Presentation attributes																			
43		1	Visibility of the message																			
44			1.1	Appropriate location	1			1														
45			1.2	Draw attention to key information, e.g. by using contrasting colour	1			1														
46																						
47		2	Layout, style and formatting																			
48			2.1	Uses lines, borders and shapes to group related information	1			1														
49			2.2	Create text hierarchy (up to 3 different font styles)	1			1														
50			2.3	Maximum 4 colours	1			1														
51																						
52		3	Inclusive / Accessible																			
53			3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
54			3.2	Use appropriate font styles ()	1			1														
55			3.3	Use appropriate font size ()	1			1														
56																						
57																						
58																						
59																						
60																						
61			Communication Strategy attributes				8															
62			Behaviour-change attributes				10															
63			Presentation attributes				8															
64																						
65			TOTAL				26															
66																						
67			Overall quality of awareness raising material																			
68			Low				0-14															
69			Medium				15-22															
70			High				23-28															

**ENVISION TECHNOLOGY ADVISORS**

# How to Avoid an ONLINE SCAM This Holiday Season

- CHECK THE URL FOR MISSPELLINGS & FAKE WEBSITES**

Small spelling changes in the URL, such as an extra letter, may indicate a fake website. Double check the URL before making a purchase!
- BE ON GUARD FOR PHISHING EMAILS**

Watch out - hackers will try to steal your identity and passwords by sending you a shipping notification asking you to verify your personal information.
- CONFIRM THAT CHARITIES & WEBSITES ARE LEGIT**

Always cross-check a charity with [www.give.org](http://www.give.org) before donating.
- BE WARY OF UNUSUAL REQUESTS**

Never pay with cash, a prepaid debit card, a gift card, or by wire transfer. Also look out for "impersonation attacks", wherein a hacker pretends to be someone you know asking for money.

### WHAT TO DO IF YOU BELIEVE YOU'RE A VICTIM

- Contact your bank ASAP and close any targeted accounts.
- Watch your bank account for suspicious/random charges.
- File a complain with the FBI's Internet Crime Complaint Center.
- Report the attack to your local police.
- File a report with the Federal Trade Commission.
- Immediately change any passwords you may have revealed.
- If compromised at work, report the problem to your IT team/provider.

**SOURCES**

<https://www.fbb.org/article/news-releases/2571-fbb-warning-avoid-these-holiday-scams>  
<https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams>  
<https://www.us-cert.gov/ncas/current-activity/2017/12/16/Holiday-Scams-and-Malware-Campaigns>

8)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
2	<b>Communication Strategy attributes</b>			<b>Evaluation</b>															
3				Infographic - website <a href="https://cisomag.com/don-get-phished-infographic/">https://cisomag.com/don-get-phished-infographic/</a>															
5	1	Audience	Marks	Maks		Comments													
6		1,1	Across groups	1															
7		1,2	Specific	2															
9	2	Key message focus - clear purpose																	
10		2,1	Awareness - about threat	1	1														
11		2,2	Awareness - about impact	1	1														
12		2,3	Cyber hygiene - best practices	1	1														
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1	1														
15	3	Timeframe																	
16		3,1	Generic	1	1														
17		3,2	Covers specific time periods	2															
20	<b>Behaviour-change attributes</b>																		
22	1	Promote situational awareness																	
23		1,1	Easy to understand what is the threat	1	1														
24		1,2	Easy to understand what is the impact	1	1														
26	2	Empower people																	
27		2,1	Simple information to understand how to address the threat	1	1														
28		2,2	Appropriate call to action message	1	1														
29		2,3	Overall conveys a positive message	1	Neutral														
31	3	Evidence-based content																	
32		3,1	Based on facts, e.g. statistics, etc.	1	1														
33		3,2	From credible source	1	1														
35	4	Memorable																	
36		4,1	Micro-learning - specific topic	1	1														
37		4,2	Micro-learning - short statements, focus on key points	1	1														
38		4,3	Considers different learning styles	1	1														
39		4,4	Balance between graphics and text	1	1														
40		4,5	Audience can easily relate, e.g. storytelling	1	1														
42	<b>Presentation attributes</b>																		
44	1	Visibility of the message																	
45		1,1	Appropriate location	1	1														
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1	1														
48	2	Layout, style and formatting																	
49		2,1	Uses lines, borders and shapes to group related information	1	1														
50		2,2	Create text hierarchy (up to 3 different font styles)	1	1														
51		2,3	Maximum 4 colours	1	1														
53	3	Inclusive / Accessible																	
54		3,1	Good color contrast between the text color and background color	1	1														
55		3,2	Use appropriate font styles (i)	1	1														
56		3,3	Use appropriate font size (j)	1	1														
61	<b>Communication Strategy attributes</b>			6															
62	<b>Behaviour-change attributes</b>			10															
63	<b>Presentation attributes</b>			7															
65	<b>TOTAL</b>			<b>23</b>															
67	Overall quality of awareness raising material																		
68	Low			0-14															
69	Medium			15-22															
70	High			23-30															



9)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	Communication Strategy attributes					Evaluation								
3						Infographic - website	<a href="https://www.growth.com/resources/guide/infographic-impact-of-phishing-attacks-on-organizations-and-how-to-be-prepared/">https://www.growth.com/resources/guide/infographic-impact-of-phishing-attacks-on-organizations-and-how-to-be-prepared/</a>							
5	1	Audience	Markets			Markets	Comments							
6		1,1	Across groups	1										
7		1,2	Specific	2			2 Employees/Organizations							
9	2	Key message focus - clear purpose												
10		2,1	Awareness - about threat	1			1 Impact of phishing attacks on organizations/how to be prepared							
11		2,2	Awareness - about impact	1			1							
12		2,3	Cyber hygiene - best practices	1			1 tips how employees can be prepared about phishing attacks							
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1 Inform you about impact and how to be prepared about phishing attacks							
15	3	Timeframe												
16		3,1	Generic	1			1							
17		3,2	Covers specific time periods	2										
20	Behaviour-change attributes													
22	1	Promote educational awareness												
23		1,1	Easy to understand what is the threat	1			1							
24		1,2	Easy to understand what is the impact	1			1							
26	2	Empower people												
27		2,1	Simple information to understand how to address the threat	1			1							
28		2,2	Appropriate call to action message	1										
29		2,3	Overall conveys a positive message	1			Neutral							
31	3	Evidence-based content												
32		3,1	Based on facts, e.g. statistics, etc.	1			1 Statistics, visual, graphics							
33		3,2	From credible source	1										
35	4	Memorable												
36		4,1	Micro-learning - specific topic	1			1							
37		4,2	Micro-learning - short statements, focus on key points	1			1							
38		4,3	Considers different learning styles	1			1 Visual							
39		4,4	Balance between graphics and text	1			1							
40		4,5	Audience can easily relate, e.g. storytelling	1			1 real examples/statistics							
42	Presentation attributes													
44	1	Viability of the message												
45		1,1	Appropriate location	1										
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1			1							
48	2	Layout, style and formatting												
49		2,1	Uses lines, borders and shapes to group related information	1			1							
50		2,2	Create text hierarchy (up to 3 different font styles)	1			1							
51		2,3	Maximum 6 colours	1			1							
53	3	Inclusive / Accessible												
54		3,1	A good color contrast between the text color and background color	1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>							
55		3,2	Use appropriate font styles ()	1			1							
56		3,3	Use appropriate font size ()	1			1							
61	Communication Strategy attributes					7								
62	Behaviour-change attributes					9								
63	Presentation attributes					6								
65	TOTAL					22								
67	Overall quality of awareness raising material													
68	Low	0-14												
69	Medium	15-22												
70	High	23-28												



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S													
2 Communication Strategy attributes				Evaluation																											
3				Infographic - website																											
4				<a href="https://www.tu.edu/tech/support/information-security/covid-19-related-cyber-scams/">https://www.tu.edu/tech/support/information-security/covid-19-related-cyber-scams/</a>																											
5 1 Audience				Marks		Marks														Comments											
6 1,1 Across groups				1		1																									
7 1,2 Specific				2																											
8																															
9 2 Key message focus - clear purpose																															
10 2,1 Awareness - about threat				1		1																									
11 2,2 Awareness - about impact				1		1																									
12 Cyber hygiene - best practices				1		1																									
13 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.				1		1																									
14																															
15 3) Timeframe																															
16 3,1 Generic				1		1																									
17 3,2 Covers specific time periods				2																											
18																															
19																															
20 Behaviour-change attributes																															
21																															
22 1 Promote situational awareness																															
23 1,1 Easy to understand what is the threat				1		1																									
24 1,2 Easy to understand what is the impact				1		1																									
25																															
26 2 Empower people																															
27 2,1 Simple information to understand how to address the threat				1		1																									
28 2,2 Appropriate call to action message				1																											
29 2,3 Overall conveys a positive message				1		Neutral																									
30																															
31 3 Evidence-based content																															
32 3,1 Based on facts, e.g. statistics, etc.				1		1																									
33 3,2 From credible source				1																											
34																															
35 4 Memorable																															
36 4,1 Micro-learning - specific topic				1		1																									
37 4,2 Micro-learning - short statements, focus on key points				1		1																									
38 4,3 Consider different learning styles				1		1 Visual																									
39 4,4 Balance between graphics and text				1		1																									
40 4,5 Audience can easily relate, e.g. storytelling				1		1 real examples																									
41																															
42 Presentation attributes																															
43																															
44 1 Visibility of the message																															
45 1,1 Appropriate location				1		1																									
46 1,2 Draw attention to key information, e.g. by using contrasting colour				1		1																									
47																															
48 2 Layout, style and formatting																															
49 2,1 Uses lines, borders and shapes to group related information				1		1																									
50 2,2 Create text hierarchy (up to 3 different font styles)				1		1																									
51 2,3 Maximum 3 colours				1		1																									
52																															
53 3 Inclusive / Accessible																															
54 3,1 A good color contrast between the text color and background color				1		using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>																									
55 3,2 Use appropriate font styles (i)				1		1																									
56 3,3 Use appropriate font size (i)				1		1																									
57																															
58																															
59																															
60																															
61 Communication Strategy attributes						6																									
62 Behaviour-change attributes						9																									
63 Presentation attributes						6																									
64																															
65 TOTAL						21																									
66																															
67 Overall quality of awareness-raising material																															
68 Low 0-14																															
69 Medium 15-22																															
70 High 23-28																															
71																															

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	Communication Strategy attributes				Evaluation											
3						Infographic - website	<a href="https://www.wcf.eu/inf-media-centre/cybercams-cas-business-email-compromise-bec-fraud/">https://www.wcf.eu/inf-media-centre/cybercams-cas-business-email-compromise-bec-fraud/</a>									
4																
5	1	Audience	Marks			Marks	Comments									
6		1,1	Across groups	1												
7		1,2	Specific	2			2 Employees/Organisations									
8																
9	2	Key message focus - clear purpose														
10		2,1	Awareness - about threat	1			1 Invoice fraud									
11		2,2	Awareness - about impact	1												
12		2,3	Cyber hygiene - best practices	1			1									
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1 to report the incident									
14																
15	3	Timeframe														
16		3,1	Generic	1			1									
17		3,2	Covers specific time periods	2												
18																
19																
20	Behaviour-change attributes															
21																
22	1	Promote situational awareness														
23		1,1	Easy to understand what is the threat	1			1									
24		1,2	Easy to understand what is the impact	1												
25																
26	2	Empower people														
27		2,1	Simple information to understand how to address the threat	1			1									
28		2,2	Appropriate call to action message	1			1									
29		2,3	Overall conveys a positive message	1			Neutral									
30																
31	3	Evidence-based content														
32		3,1	Based on facts, e.g. statistics, etc.	1												
33		3,2	From credible source	1			1 Europal									
34																
35	4	Memorable														
36		4,1	Micro-learning - specific topic	1			1									
37		4,2	Micro-learning - short statements, focus on key points	1			1									
38		4,3	Consider different learning styles	1			1 Visual/text									
39		4,4	Balance between graphics and text	1			1									
40		4,5	Audience can easily relate, e.g. storytelling	1			1 real examples									
41																
42	Presentation attributes															
43																
44	1	Visibility of the message														
45		1,1	Appropriate location	1			1									
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1			1									
47																
48	2	Layout, style and formatting														
49		2,1	Uses lines, borders and shapes to group related information	1			1									
50		2,2	Create text hierarchy (up to 3 different font styles)	1			1									
51		2,3	Maximum 4 colours	1			1									
52																
53	3	Inclusive / Accessible														
54		3,1	A good color contrast between the text color and background color	1			1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>									
55		3,2	Use appropriate font styles ()	1			1									
56		3,3	Use appropriate font size ()	1			1									
57																
58																
59																
60																
61							6									
62							9									
63							8									
64																
65						TOTAL	23									
66																
67																
68																
69																
70																
71																

**INVOICE FRAUD**

**HOW DOES IT WORK?**

- A business is approached by somebody pretending to represent a supplier/vendor/previous customer.
- A combination of approaches can be used (phone calls, email, etc.)
- The fraudster requests that the bank details for a payment (e.g. bank account page details of false invoices) be changed. The new account requested is controlled by the fraudster.

**WHAT CAN YOU DO?**

**AS A BUSINESS:**

- Ensure that employees are informed and aware of this type of fraud and how to avoid it.
- Ensure staff responsible for paying invoices to always check them for any irregularities.
- Review information posted on your company website, in particular contracts and suppliers. Ensure your staff know what they share about the company on their social media.
- Implement a procedure to verify the legitimacy of payment requests.









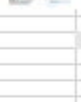
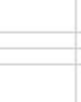
**AS AN EMPLOYEE:**

- Verify all requests supporting to be from your business, especially if they ask you to change your bank details for false invoices.
- Do not use the contact details on the letterhead when requesting for change. Use those from personal correspondence instead.
- For payments over a certain threshold, set up a procedure to confirm the correct bank account and to require it to be confirmed with the company.
- When an invoice is paid, send an email to confirm the request. Include the beneficiary bank name and the last four digits of the account to ensure security.
- Get an designated Single Points of Contact with companies to whom you make regular payments.
- Request information that you share about your employer on social media.

Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

**ELIPTICAL** **#CyberScams**

12)

A	B	C	D	E	F	G	H	I
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>		
3						Infographic - website	<a href="https://www.gage.com/gallery/post/6-common-phishing-attacks-and-how-to-avoid-them/">https://www.gage.com/gallery/post/6-common-phishing-attacks-and-how-to-avoid-them/</a>	
4								
5	1	Audience	Marked		Marked	Comments		
6		1.1 Across groups	1			1		
7		1.2 Specific	2					
8								
9	2	Key message focus - clear purpose						
10		2.1 Awareness - about threat	1			1	Six common phishing scams	
11		2.2 Awareness - about impact	1			1		
12		2.3 Cyber hygiene - best practices	1			1	How to avoid the threats	
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	Report the incident	
14								
15	3	Timeframe						
16		3.1 Generic	1			1		
17		3.2 Covers specific time periods	2					
18								
19								
20	<b>Behaviour-change attributes</b>							
21	1	Promote situational awareness						
22		Easy to understand what is the threat	1			1		
23		Easy to understand what is the impact	1					
24								
25								
26	2	Empower people						
27		Simple information to understand how to address the threat	1			1		
28		Appropriate call to action message	1			1		
29		Overall conveys a positive message	1				Neutral	
30								
31	3	Evidence-based content						
32		Based on facts, e.g. statistics, etc.	1			1	Statistics	
33		From credible source	1					
34								
35	4	Memorable						
36		Micro-learning - specific topic	1			1		
37		Micro-learning - short statements, focus on key points	1			1		
38		Considers different learning styles	1			1	Visual, examples	
39		Balance between graphics and text	1			1		
40		Audience can easily relate, e.g. storytelling	1			1	real examples	
41								
42	<b>Presentation attributes</b>							
43	1	Viability of the message						
44		1.1 Appropriate location	1					
45		Draw attention to key information, e.g. by using contrasting colour	1			1		
46		1.2						
47	2	Layout, style and formatting						
48		Uses lines, borders and shapes to group related information	1			1		
49		2.1						
50		Create text hierarchy (up to 3 different font styles)	1			1		
51		2.2						
52		2.3 Maximum 4 colours	1			1		
53	3	Inclusive / Accessible						
54		A good color contrast between the text color and background color	1				using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>	
55		3.1				1		
56		3.2 Use appropriate font styles ()	1					
57		3.3 Use appropriate font size ()	1					
58								
59								
60								
61	<b>Communication Strategy attributes</b>				6			
62	<b>Behaviour-change attributes</b>				9			
63	<b>Presentation attributes</b>				5			
64								
65	<b>TOTAL</b>				20			
66								
67	Overall quality of awareness raising material							
68	Low 0-14							
69	Medium 15-22							
70	High 23-28							

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>								
3						Infographic - website	<a href="https://www.mcpc.com/insights/infographic/lets-go-phishing-a-guide-to-phishing-attacks/">https://www.mcpc.com/insights/infographic/lets-go-phishing-a-guide-to-phishing-attacks/</a>							
4														
5	1	Audience		Marka		Marka	Comments							
6		1.1	Across groups	1										
7		1.2	Specific	2			Employee/Organisations							
8														
9	2	Key message focus - clear purpose												
10		2.1	Awareness - about threat	1			Guide for phishing attacks							
11		2.2	Awareness - about impact	1										
12		2.3	Cyber hygiene - best practices	1			How to avoid the threats							
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1										
14														
15	3	Timeframe												
16		3.1	Generic	1										
17		3.2	Covers specific time periods	2										
18														
19														
20	<b>Behaviour-change attributes</b>													
21														
22	1	Promote situational awareness												
23		1.1	Easy to understand what is the threat	1										
24		1.2	Easy to understand what is the impact	1										
25														
26	2	Empower people												
27		2.1	Simple information to understand how to address the threat	1										
28		2.2	Appropriate call to action message	1										
29		2.3	Overall conveys a positive message	1			Neutral							
30														
31	3	Evidence-based content												
32		3.1	Based on facts, e.g. statistics, etc.	1			Statistics							
33		3.2	From credible source	1										
34														
35	4	Memorable												
36		4.1	Micro-learning - specific topic	1										
37		4.2	Micro-learning - short statements, focus on key points	1										
38		4.3	Considers different learning styles	1			Visual, examples							
39		4.4	Balance between graphics and text	1										
40		4.5	Audience can easily relate, e.g. storytelling	1										
41														
42	<b>Presentation attributes</b>													
43														
44	1	Viability of the message												
45		1.1	Appropriate location	1										
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1										
47														
48	2	Layout, style and formatting												
49		2.1	Uses lines, borders and shapes to group related information	1										
50		2.2	Create text hierarchy (up to 3 different font styles)	1										
51		2.3	Maximum of colours	1										
52														
53	3	Inclusive / Accessible												
54		3.1	A good color contrast between the text color and background color	1			Using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>							
55		3.2	Use appropriate font styles ()	1										
56		3.3	Use appropriate font size ()	1										
57														
58														
59														
60														
61	Communication Strategy attributes						G							
62	Behaviour-change attributes						B							
63	Presentation attributes						G							
64														
65	<b>TOTAL</b>						<b>20</b>							
66	Overall quality of awareness raising material													
67	Low 0-14													
68	Medium 15-22													
69	High 23-28													
70														
71														



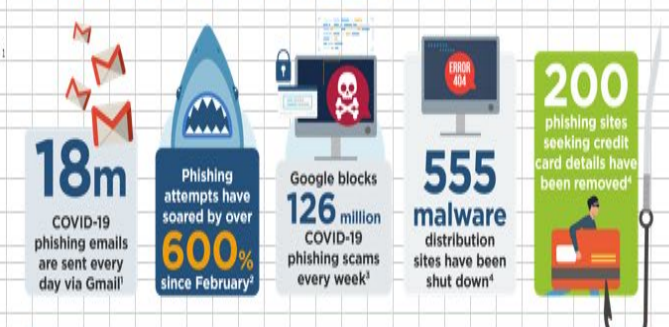
Communication Strategy attributes			Evaluation	
Infographic - website			<a href="https://blog.knowbe4.com/us-fy/hubfs/cloudmark_top_ten_infographic.png?width=1291&amp;height=3988&amp;name=cloudmark_top_ten_infographic.png">https://blog.knowbe4.com/us-fy/hubfs/cloudmark_top_ten_infographic.png?width=1291&amp;height=3988&amp;name=cloudmark_top_ten_infographic.png</a>	
1	Audience	Marks	Marks	Comments
1.1	Across groups	1		
1.2	Specific	2	2	Employee/Organisations
2	Key message focus - clear purpose			
2.1	Awareness - about threat	1	1	Top ten worst cybersecurity for spear phishing
2.2	Awareness - about impact	1	1	Impact about employees, revenue etc.
2.3	Cyber hygiene - best practices	1		
2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		
3	Timeframe			
3.1	Generic	1	1	
3.2	Covers specific time periods	2		
Behaviour-change attributes				
1	Promote situational awareness			
1.1	Easy to understand what is the threat	1	1	
1.2	Easy to understand what is the impact	1	1	
2	Empower people			
2.1	Simple information to understand how to address the threat	1	1	
2.2	Appropriate call to action message	1		
2.3	Overall conveys a positive message	1	Neutral	
3	Evidence-based content			
3.1	Based on facts, e.g. statistics, etc.	1	1	Statistics
3.2	From credible source	1	1	Cloudmark
4	Memorable			
4.1	Micro-learning - specific topic	1	1	
4.2	Micro-learning - short statements, focus on key points	1	1	
4.3	Considers different learning styles	1	1	Visual examples
4.4	Balance between graphics and text	1		
4.5	Audience can easily relate, e.g. storytelling	1	1	Real examples
Presentation attributes				
1	Viability of the message			
1.1	Appropriate location	1	1	
1.2	Draw attention to key information, e.g. by using contrasting colour	1	1	
2	Layout, style and formatting			
2.1	Use lines, borders and shapes to group related information	1	1	
2.2	Create text hierarchy (up to 3 different font styles)	1	1	
2.3	Maximum 6 colours	1	1	
3	Inclusive / Accessible			
3.1	A good color contrast between the text color and background color	1	1	using <a href="http://webaim.org/resources/contrastchecker/">http://webaim.org/resources/contrastchecker/</a>
3.2	Use appropriate font style (i)	1	1	
3.3	Use appropriate font size (i)	1	1	
Communication Strategy attributes			5	
Behaviour-change attributes			9	
Presentation attributes			8	
<b>TOTAL</b>			<b>22</b>	
Overall quality of awareness raising material				
Low			0-14	
Medium			15-22	
High			23-28	



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
2	Communication Strategy attributes				Evaluation																													
3	Infographic - website				<a href="https://www.westcon.comstor.com/learn/get-hooked-infographic-how-to-spot-and-stop-covid-19-phishing-scams/">https://www.westcon.comstor.com/learn/get-hooked-infographic-how-to-spot-and-stop-covid-19-phishing-scams/</a>																													
4																																		
5	1	Audience	Markets		Markets	Comments																												
6		1.1	Acronyms	1																														
7		1.2	Specific	2																														
8																																		
9	2	Key message focus - clear purpose																																
10		2.1	Awareness - about threat	1		How hackers are preying on coronavirus fears																												
11		2.2	Awareness - about impact	2																														
12		2.3	Open hygiene - best practices	1																														
13		2.4	Empowerment - calls to action, e.g. visit a website to learn more, to report an incident, etc.	1		report the incident																												
14																																		
15	3	Tone/voice																																
16		3.1	Generic	1																														
17		3.2	Covers specific time periods	2																														
18																																		
19																																		
20	Behavior change attributes																																	
21																																		
22	1	Promote situational awareness																																
23		1.1	Easy to understand what is the threat	1																														
24		1.2	Easy to understand what is the impact	1																														
25																																		
26	2	Empower people																																
27		2.1	Simple information to understand how to address the threat	1																														
28		2.2	Appropriate calls to action	1																														
29		2.3	Overall conveys a positive message	1		Neutral																												
30																																		
31	3	Evidence-based content																																
32		3.1	Based on facts, e.g. statistics, etc.	1		statistics																												
33		3.2	From credible source	1																														
34																																		
35	4	Memorable																																
36		4.1	Micro-learning - specific tips	1																														
37		4.2	Micro-learning - short statements, focused on key points	1																														
38		4.3	Considers different learning styles	1		Visual																												
39		4.4	Balance between graphics and text	1																														
40		4.5	Audience can easily relate, e.g. story telling	1		how to avoid the threat																												
41																																		
42	Presentation attributes																																	
43																																		
44	1	Readability of the message																																
45		1.1	Appropriate location	1																														
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1																														
47																																		
48	2	Layout, style and formatting																																
49		2.1	Clear lines, borders and shapes to group related information	1																														
50		2.2	Creates text hierarchy (upto 2.2.3 different font styles)	1																														
51		2.3	Maximum 11 columns	1																														
52																																		
53	3	Inclusion / Accessible																																
54		3.1	A good color contrast between the text color and background color	1		using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>																												
55		3.2	Use appropriate font style()	1																														
56		3.3	Use appropriate font size()	1																														
57																																		
58																																		
59																																		
60																																		
61	Communication Strategy attributes				5																													
62	Behavior change attributes				6																													
63	Presentation attributes				7																													
64																																		
65	TOTAL				21																													
66																																		
67	Overall quality of awareness raising material																																	
68	Low				0-10																													
69	Medium				11-20																													
70	High				21-30																													
71																																		



### Hackers are preying on coronavirus fears



1. <https://www.cisco.com/techcenter/technology/0379908>  
 2. <https://www.fortinet.com/resources/whitepapers/covid-19-phishing-scams.html>  
 3. <https://www.fortinet.com/resources/whitepapers/covid-19-phishing-scams.html>  
 4. <https://www.fortinet.com/resources/whitepapers/covid-19-phishing-scams.html>

A	B	C	D	E	F	G	H	I	J	K	L
2	Communication Strategy attributes					Evaluation					
3						Infographic - website	<a href="https://www.idology.com/secure-seniors-series/">https://www.idology.com/secure-seniors-series/</a>				
5	1	Audience		Marks		Marks	Comments				
6		1.1	Across groups	1							
7		1.2	Specific	2		2	Silver (70+)/Baby boomers				
9	2	Key message focus - clear purpose									
10		2.1	Awareness - about threat	1		1	Cyber securing seniors during covid-19				
11		2.2	Awareness - about impact	1		1					
12		2.3	Cyber hygiene - best practices	1		1					
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1							
15	3	Timeframe									
16		3.1	Generic	1		1					
17		3.2	Covers specific time periods	2							
20	Behaviour-change attributes										
22	1	Promote situational awareness									
23		1.1	Easy to understand what is the threat	1		1					
24		1.2	Easy to understand what is the impact	1		1					
26	2	Empower people									
27		2.1	Simple information to understand how to address the threat	1		1					
28		2.2	Appropriate call to action message	1							
29		2.3	Overall conveys a positive message	1		Neutral					
31	3	Evidence-based content									
32		3.1	Based on facts, e.g. statistics, etc.	1		1	statistics				
33		3.2	From credible source	1							
35	4	Memorable									
36		4.1	Micro-learning - specific topic	1		1					
37		4.2	Micro-learning - short statements, focus on key points	1		1					
38		4.3	Considers different learning styles	1		1	Visual				
39		4.4	Balance between graphics and text	1		1					
40		4.5	Audience can easily relate, e.g. storytelling	1		1	how to avoid the threat				
42	Presentation attributes										
44	1	Viability of the message									
45		1.1	Appropriate location	1		1					
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1					
48	2	Layout, style and formatting									
49		2.1	Uses lines, borders and shapes to group related information	1		1					
50		2.2	Create text hierarchy (up to 3 different font styles)	1		1					
51		2.3	Maximum 4 colours	1							
53	3	Inclusive / Accessible									
54		3.1	A good color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrast-checker/">https://webaim.org/resources/contrast-checker/</a>				
55		3.2	Use appropriate font styles ()	1		1					
56		3.3	Use appropriate font size ()	1		1					
61	Communication Strategy attributes					6					
62	Behaviour-change attributes					9					
63	Presentation attributes					7					
65	TOTAL					22					
67	Overall quality of awareness raising material										
68	Low 0-14										
69	Medium 15-22										
70	High 23-28										

**Cyber-Securing Seniors During COVID-19**

Americans over 65 lost **\$650 million** as victims of online crime in 2018.

**AND**

For those over 65, there was a **400% increase** in reported crime towards the age group over the past five years.

**25% of seniors** have personally been the victim of identity theft.

When identity theft occurred among seniors...

**60%** had personally used debit card online.

**55% of seniors** do not have or do not know if they have virus protection on their mobile device installed.





**209% surge** in reported mobile security issues from 2018 to 2019.

**STAY ALERT!**

- Identify and avoid email phishing scams.
- Don't click on links or download files from unknown sources.
- Watch out for online scams, mobile device issues and any strong phishing.
- Make sure your mobile device is secure and any strong phishing.

For helpful advice and resources on protecting your identity, visit <https://www.idology.com/secure-seniors-series/>.

Source: IDology

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	Communication Strategy attributes			Evaluation				<div style="background-color: #00728f; color: white; padding: 10px;"> <h2 style="margin: 0;">Phishing Threats Are Real And Everyone Is A Target</h2> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="text-align: center; margin-right: 10px;">  <p style="font-size: 0.8em; margin: 0;">95%</p> </div> <div> <p style="font-size: 0.7em; margin: 0;">95% of targeted attacks against specific organizations began with a targeted spear-phishing email.</p> <p style="font-size: 0.6em; margin: 0;">What this means is that today, hackers and malicious agents depend on human flaws as much or more than system flaws.</p> </div> </div> <h2 style="margin: 10px 0 0 0;">Who Gets Phished?</h2> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="text-align: center; margin-right: 10px;">  <p style="font-size: 0.8em; margin: 0;">Staff is targeted 2x more than Middle Management and 1.3x more than Executives.</p> </div> <div> <p style="font-size: 0.7em; margin: 0;">Staff is also 2x more likely to click on the threats they receive.</p> </div> </div> <h2 style="margin: 10px 0 0 0;">Best Phishing Bait</h2> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="text-align: center; margin-right: 10px;">  <p style="font-size: 0.8em; margin: 0;">in</p> </div> <div> <p style="font-size: 0.7em; margin: 0;">Social networking emails are the most effective phishing bait. In fact, LinkedIn invitations get two times as many clicks as any other type of phishing email.</p> </div> </div> <div style="text-align: center; margin-top: 10px;">  <p style="font-size: 0.8em; margin: 0;">80%</p> </div> <div> <p style="font-size: 0.7em; margin: 0;">According to the McAfee Labs August 2014 Threat Report, 80% of the business users failed to detect at least one of seven phishing emails.</p> <p style="font-size: 0.6em; margin: 0;">Yet if only takes one click on a malicious link to establish a foothold into a business.</p> </div> </div> <div style="background-color: white; color: #00728f; padding: 5px; text-align: center; margin-top: 10px;"> <b>To Avoid Being Phished:</b> </div> <ol style="list-style-type: none"> <li>1) Never respond to unsolicited emails that ask for personal information.</li> <li>2) Be suspicious of emails that don't address you by name, have misspellings, or don't look professional.</li> <li>3) Hover over links to verify a link's actual destination, even if the link comes from a trusted source.</li> <li>4) Always navigate to a bank, social media, or financial institution's website by typing in the web address, rather than clicking on an email link.</li> <li>5) NEVER click on links in unsolicited emails.</li> </ol> <div style="font-size: 0.6em; margin-top: 10px;"> <p>Source: McAfee Labs, "The State of Advanced Persistent Threats: 2014 Threat Report", 2014. <a href="http://www.mcafee.com/enterprise/en-us/assets/PDF/threat_report_2014.pdf">http://www.mcafee.com/enterprise/en-us/assets/PDF/threat_report_2014.pdf</a></p> <p>Source: LinkedIn, "2014 LinkedIn Security Report", 2014. <a href="http://www.linkedin.com/company/linkedin/insights/reports">http://www.linkedin.com/company/linkedin/insights/reports</a></p> <p>Source: Jolt Report, "2014 Jolt Report", 2014. <a href="http://www.joltreport.com">http://www.joltreport.com</a></p> </div>								
3							<a href="https://topredlearning.com/resource/infographic-avoid-being-phished/">https://topredlearning.com/resource/infographic-avoid-being-phished/</a>									
4																
5	1	Audience	Mark	Mark	Comments											
6		1.1 Across groups	1		1	Individual & employees										
7		1.2 Specific	2													
8																
9	2	Key message focus - clear purpose														
10		2.1 Awareness - about threat	1		1	Phishing threats are real everyone is a target										
11		2.2 Awareness - about impact	1													
12		Cyber hygiene - best practices	1		1											
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1													
14																
15	3	Timeframe														
16		3.1 Generic	1		1											
17		3.2 Covers specific time periods	2													
18																
19																
20	Behaviour-change attributes															
21	1	Promote situational awareness														
22		Easy to understand what is the threat	1		1											
23		Easy to understand what is the impact	1													
24																
25	2	Empower people														
26		Simple information to understand how to address the threat	1		1											
27		Appropriate call to action message	1													
28		Overall conveys a positive message	1			Neutral										
29																
30	3	Evidence-based content														
31		Based on facts, e.g. statistics, etc.	1		1	statistics										
32																
33		From credible source	1													
34																
35	4	Memorable														
36		Micro-learning - specific topic	1		1											
37		Micro-learning - short statements, focus on key points	1		1											
38		Considers different learning styles	1		1	Visual/bait										
39		Balance between graphics and text	1		1											
40		Audience can easily relate, e.g. story telling	1		1	how to avoid the threat										
41																
42	Presentation attributes															
43	1	Visibility of the message														
44		1.1 Appropriate location	1		1											
45		Draw attention to key information, e.g. by using contrasting colour	1		1											
46																
47	2	Layout, style and formatting														
48		Use lines, borders and shapes to group related information	1		1											
49		Create text hierarchy (up to 3 different font styles)	1		1											
50		Maximum 6 colours	1		1											
51																
52	3	Inclusive / Accessible														
53		A good color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>										
54		Use appropriate font style (i)	1		1											
55		Use appropriate font size (i)	1		1											
56																
57																
58																
59																
60																
61		Communication Strategy attributes			8											
62		Behaviour-change attributes			8											
63		Presentation attributes			8											
64																
65		TOTAL			20											
66																
67		Overall quality of awareness raising material														
68		Low 0-14														
69		Medium 15-22														
70		High 23-28														

A	B	C	D	E	F	G	H	I	J	K	L
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>					
3						Infographic - website	<a href="https://www.sansoatiremediation.com/blog/safety-and-protection/be-aware-of-imposter-scams-infographic">https://www.sansoatiremediation.com/blog/safety-and-protection/be-aware-of-imposter-scams-infographic</a>				
5	1	Audience	Marks			Marks	Comments				
6		1,1 Across groups	1				1				
7		1,2 Specific	2								
9	2	Key message focus - clear purpose									
10		2,1 Awareness - about threat	1				1	Be aware of imposter phone scams			
11		2,2 Awareness - about impact	1								
12		Cyber hygiene - best practices	1				1	Some tips to protect your self from phone scams			
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1				1	Call and report the incident			
15	3	Timeframe									
16		3,1 Generic	1				1				
17		3,2 Covers specific time periods	2								
20	<b>Behaviour-change attributes</b>										
22	1	Promote situational awareness									
23		1,1 Easy to understand what is the threat	1				1				
24		1,2 Easy to understand what is the impact	1								
26	2	Empower people									
27		2,1 Simple information to understand how to address the threat	1				1				
28		2,2 Appropriate call to action message	1				1				
29		2,3 Overall conveys a positive message	1				Neutral				
31	3	Evidence-based content									
32		3,1 Based on facts, e.g. statistics, etc.	1				1	statistics			
33		3,2 From credible source	1								
35	4	Memorable									
36		4,1 Micro-learning - specific topic	1				1				
37		4,2 Micro-learning - short statements, focus on key points	1				1				
38		4,3 Considers different learning styles	1				1	Visual/text			
39		4,4 Balance between graphics and text	1								
40		4,5 Audience can easily relate, e.g. storytelling	1				1	how to avoid the treat/ real examples			
42	<b>Presentation attributes</b>										
44	1	Visibility of the message									
45		1,1 Appropriate location	1				1				
46		1,2 Draw attention to key information, e.g. by using contrasting colour	1				1				
48	2	Layout, style and formatting									
49		2,1 Uses lines, borders and shapes to group related information	1				1				
50		2,2 Create text hierarchy (up to 3 different font styles)	1				1				
51		2,3 Maximum 4 colours	1				1				
53	3	Inclusive / Accessible									
54		3,1 A good color contrast between the text color and background color	1				1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>			
55		3,2 Use appropriate font styles ()	1				1				
56		3,3 Use appropriate font size ()	1				1				
61	<b>Communication Strategy attributes</b>					5					
62	<b>Behaviour-change attributes</b>					8					
63	<b>Presentation attributes</b>					8					
64											
65	<b>TOTAL</b>					21					
67	Overall quality of awareness raising material										
68	Low 0-14										
69	Medium 15-22										
70	High 23-28										



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
2	Communication Strategy attributes					Evaluation														
3						Infographic - website	<a href="https://www.ncsc.gov.uk/information/infographics-etc">https://www.ncsc.gov.uk/information/infographics-etc</a>													
5	1	Audience	Marka			Marka	Comments													
6		1.1	Across groups																	
7		1.2	Specific																	
9	2	Key message focus - clear purpose																		
10		2.1	Awareness - about threat				How to make your self harder target													
11		2.2	Awareness - about impact																	
12		2.3	Cyber hygiene - best practices				Some tips to protect your self from phishing attacks													
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.				report the incident													
15	3	Timeline																		
16		3.1	Generic																	
17		3.2	Covers specific time periods																	
20	Behaviour-change attributes																			
22	1	Promote situational awareness																		
23		1.1	Easy to understand what's the threat																	
24		1.2	Easy to understand what's the impact																	
26	2	Empower people																		
27		2.1	Simple information to understand how to address the threat																	
28		2.2	Appropriate call to action message																	
29		2.3	Overall conveys a positive message				Neutral													
31	3	Evidence-based content																		
32		3.1	Based on facts, e.g. statistics, etc.				statistics													
33		3.2	From credible source				National Cyber Security Centre													
35	4	Memorable																		
36		4.1	Micro-learning - specific topic																	
37		4.2	Micro-learning - short statements, focus on key points																	
38		4.3	Consider different learning styles				Visual/text													
39		4.4	Balance between graphics and text																	
40		4.5	Audience can easily relate, e.g. storytelling				How to avoid the threat / real examples													
43	Presentation attributes																			
45	1	Visibility of the message																		
46		1.1	Appropriate location																	
47		1.2	Draw attention to key information, e.g. by using contrasting colour																	
48	2	Layout, style and formatting																		
49		2.1	Uses lines, borders and shapes to group related information																	
50		2.2	Create text hierarchy (up to 3 different font styles)																	
51		2.3	Maximum 6 columns																	
53	3	Inclusive / Accessible																		
54		3.1	Good color contrast between the text color and background color				using <a href="http://webaim.org/resources/contrastchecker/">http://webaim.org/resources/contrastchecker/</a>													
55		3.2	Use appropriate font style(s)																	
56		3.3	Use appropriate font size(s)																	
61	Communication Strategy attributes					6														
62	Behaviour-change attributes					10														
63	Presentation attributes					7														
65	TOTAL					23														
67	Overall quality of awareness raising material																			
68	Low					0-14														
69	Medium					15-22														
70	High					23-28														


**Phishing attacks**  
Dealing with suspicious emails

**What is phishing?**  
Phishing is when criminals attempt to trick you into giving them sensitive information, such as your bank details or passwords, by pretending to be a trusted organisation. They do this by sending you emails, text messages or phone calls that look like they are from a legitimate organisation.

**Make yourself a harder target**  
Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:  
- Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.  
- Be aware what your family, friends and colleagues say about you online, as this can also reveal information that can be used to target you.  
- If you have received an email which looks suspicious, forward it to the NCSC's Suspicious Email Reporting Service (SERS) [sers@ncsc.gov.uk](mailto:sers@ncsc.gov.uk)

**Tell tale signs of phishing**  
Spotting a phishing email is becoming increasingly difficult, even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt:  
- The email address is not you or does it refer to 'support' or 'helpdesk'? This can be a sign that the sender does not really know you, and that it is part of a phishing scam.  
- Others will try and create phishing-looking emails by including logos and graphics, to change your identity what you request?  
- Does the email contain a web link that asks you to click against the backdrop of a clock or you have been a victim of crime, and how immediately.  
- Your bank (or any other official source) should never ask you to supply personal information in an email, if you need to check, call them directly.  
- If it sounds too good to be true, it probably is. It's their online that will tell you they're looking for the FBI, or claims to access files for the FBI.

**What to do if you've already clicked?**  
The most important thing to do is not to panic. There are a number of practical steps you can take:  
- Open your antivirus (AV) software, and run a full scan. Follow any instructions given.  
- If you've been tricked into providing your passwords, you should change your passwords on all your other accounts.  
- If you have lost money, you need to report it in a crime to Action Fraud. You can do this by calling [www.actionfraud.police.uk](http://www.actionfraud.police.uk).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>		 <b>Extortion phishing scams</b> How to protect yourself												
3						Infographic - website	<a href="https://www.ncsc.gov.uk/files/extortion-scams-infographic.pdf">https://www.ncsc.gov.uk/files/extortion-scams-infographic.pdf</a>													
5	1	Audience	Marks			Marks	Comments													
6		1.1	Across groups	1		1														
7		1.2	Specific	2																
9	2	Key message focus - clear purpose																		
10		2.1	Awareness - about threat	1		1	How to do if you are being blackmailed by extortion scams													
11		2.2	Awareness - about impact	1		1														
12		2.3	Practices - best Cyber hygiene - best	1		1	Some tips to protect your self from blackmailed													
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	report the incident													
15	3	Timeframe																		
16		3.1	Generic	1		1														
17		3.2	Covers specific time periods	2																
20	<b>Behaviour-change attributes</b>																			
22	1	Promote situational awareness																		
23		1.1	Easy to understand what's the threat	1		1														
24		1.2	Easy to understand what's the impact	1		1														
26	2	Empower people																		
27		2.1	Simple information to understand how to address the threat	1		1														
28		2.2	Appropriate call to action message	1		1														
29		2.3	Overall conveys a positive message	1		Neutral														
31	3	Evidence-based content																		
32		3.1	Based on facts, e.g. statistics, etc.	1																
33		3.2	From credible source	1		1	National Cyber Security Centre													
35	4	Memorable																		
36		4.1	Micro-learning - specific topic	1		1														
37		4.2	Micro-learning - short statements, focus on key points	1		1														
38		4.3	Considers different learning styles	1		1	Visual/text													
39		4.4	Balance between graphics and text	1																
40		4.5	Audience can easily relate, e.g. storytelling	1		1	What to do if been blackmailed / real examples													
43	<b>Presentation attributes</b>																			
45	1	Visibility of the message																		
46		1.1	Appropriate location	1																
47		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1														
49	2	Layout, style and formatting																		
50		2.1	Uses lines, borders and shapes to group related information	1		1														
51		2.2	Create text hierarchy (up to 3 different font styles)	1		1														
52		2.3	Maximum 4 colours	1		1														
53	3	Inclusive / Accessible																		
54		3.1	A good color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
55		3.2	Use appropriate font styles (i)	1		1														
56		3.3	Use appropriate font size (i)	1		1														
61	Communication Strategy attributes					6														
62	Behaviour-change attributes					9														
63	Presentation attributes					7														
65	<b>TOTAL</b>					<b>22</b>														
67	Overall quality of awareness raising material																			
68	Low					0-14														
69	Medium					15-22														
70	High					23-28														

21)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
2	Communication Strategy attributes					Evaluation									
3						Infographic - website		<a href="https://www.phemur.com.au/phishing-scams-and-how-to-avoid-becoming-a-victim/">https://www.phemur.com.au/phishing-scams-and-how-to-avoid-becoming-a-victim/</a>							
5	1	Audience	Marks			Marks	Comments								
6		1.1 Across groups	1			1									
7		1.2 Specific	2												
9	2	Key message focus - clear purpose													
10		2.1 Awareness - about threat	1			1									
11		2.2 Awareness - about impact	1												
12		2.3 Cyber hygiene - best practices	1			1									
13		2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	call the provider and ask for clarifications								
15	3	Timeframe													
16		3.1 Generic	1			1									
17		3.2 Covers specific time periods	2												
20	Behaviour-change attributes														
22	1	Promote situational awareness													
23		Easy to understand what is the threat	1			1									
24		Easy to understand what is the impact	1												
25		1.2 the impact	1												
26	2	Empower people													
27		Simple information to understand how to address the threat	1			1									
28		Appropriate call to action message	1			1									
29		Overall conveys a positive message	1				Neutral								
31	3	Evidence-based content													
32		Based on facts, e.g. statistics, etc.	1			1	Examples								
33		3.2 From credible source	1												
35	4	Memorable													
36		Micro-learning - specific topic	1			1									
37		Micro-learning - short statements, focus on key points	1			1									
38		Considers different learning styles	1			1	Visual/text								
39		Balance between graphics and text	1			1									
40		Audience can easily relate, e.g. storytelling	1			1	how to be guard and how to spot a phishing attack								
42	Presentation attributes														
45	1	Visibility of the message													
46		1.1 Appropriate location	1			1									
47		Draw attention to key information, e.g. by using contrasting colour	1			1									
48	2	Layout, style and formatting													
49		Uses lines, borders and shapes to group related information	1			1									
50		Create text hierarchy (up to 3 different font styles)	1			1									
51		2.3 Maximum 4 colours	1			1									
53	3	Inclusive / Accessible													
54		A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>								
55		3.2 Use appropriate font styles ()	1			1									
56		3.3 Use appropriate font size ()	1			1									
61	Communication Strategy attributes					5									
62	Behaviour-change attributes					9									
63	Presentation attributes					7									
64															
65	<b>TOTAL</b>					<b>21</b>									
67	Overall quality of awareness raising material														
68	Low 0-14														
69	Medium 15-22														
70	High 23-28														

**PHISHING SCAMS & HOW TO AVOID BECOMING A VICTIM**

**WHAT IS A PHISHING SCAM?**  
A phishing message will, at first sight, appear like a normal message from a legitimate business, and will contain a link or download that takes you to a fake site, where you will be asked to input confidential information.

**HOW CAN YOU SPOT A PHISHING ATTACK?**  
As a general rule, no financial provider will ask you for financial information via text, email or social media. If you have any doubts at all regarding the authenticity of an email or similar, call the provider using your usual number and ask for clarification.

**HOW TO BE ON GUARD**

**CHECK THE SPELLING OF URL & EMAIL ADDRESS**  
A lot of scammers use addresses that may contain misspellings or appear very similar to the real ones. Hover your mouse over the email address displayed to double check in your email client. In your web browser, click on the URL, bar so you can check the complete URL.

**CROSS CHECK THE BUSINESS DETAILS**  
Scammers don't always get business details correct. It only takes a couple of minutes to double check online and verify any business details before you make any further contact.

FIND OUT MORE: [HTTPS://WWW.PHISHPLUS.COM.AU](https://www.phishplus.com.au)

A	B	C	D	E	F	G	H	I	J	K	L
1											
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>					
3						Infographic - website <a href="https://www.gc.cyber.gc.ca/en/resources/social-engineering-how-cyber-scams-trick-us">https://www.gc.cyber.gc.ca/en/resources/social-engineering-how-cyber-scams-trick-us</a>					
4											
5	1 Audience		Marks		Marks	Comments					
6		1,1 Across groups	1								
7		1,2 Specific	2			2	Millennials/Generation Z				
8											
9	2 Key message focus - clear purpose										
10		2,1 Awareness - about threat	1				1	how do cyber scams trick people			
11		2,2 Awareness - about impact	1								
12		2,3 Cyber hygiene - best practices	1				1				
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1								
14											
15	3 Timeliness										
16		3,1 Generic	1			1					
17		3,2 Covers specific time periods	2								
18											
19											
20	<b>Behaviour-change attributes</b>										
21											
22	1 Promote situational awareness										
23		1,1 Easy to understand what is the threat	1			1					
24		1,2 Easy to understand what is the impact	1								
25											
26	2 Empower people										
27		2,1 Simple information to understand how to address the threat	1			1					
28		2,2 Appropriate call to action message	1			1					
29		2,3 Overall conveys a positive message	1				Neutral				
30											
31	3 Evidence-based content										
32		3,1 Based on facts, e.g. statistics, etc.	1			1	Examples/Statistics				
33		3,2 From credible source	1								
34											
35	4 Memorable										
36		4,1 Micro-learning - specific topic	1			1					
37		4,2 Micro-learning - short statements, focus on key points	1			1					
38		4,3 Considers different learning styles	1			1	Visual/text				
39		4,4 Balance between graphics and text	1								
40		4,5 Storytelling	1				1	how to keep your information secure			
41											
42	<b>Presentation attributes</b>										
43											
44	1 Visibility of the message										
45		1,1 Appropriate location	1								
46		1,2 Draw attention to key information, e.g. by using contrasting colour	1			1					
47											
48	2 Layout, style and formatting										
49		2,1 Uses lines, borders and shapes to group related information	1			1					
50		2,2 Create text hierarchy (up to 3 different font styles)	1			1					
51		2,3 Maximum 4 colours	1								
52											
53	3 Inclusive / Accessible										
54		3,1 A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>				
55		3,2 Use appropriate font styles (!)	1			1					
56		3,3 Use appropriate font size (!)	1			1					
57											
58											
59											
60											
61	<b>Communication Strategy attributes</b>					5					
62	<b>Behaviour-change attributes</b>					8					
63	<b>Presentation attributes</b>					6					
64											
65	<b>TOTAL</b>					19					
66											
67	<b>Overall quality of awareness raising material</b>										
68	Low	0-14									
69	Medium	15-22									
70	High	23-28									
71											



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X			
1																											
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>																					
3						Infograph <a href="https://www.suncoastcreditunion.com/blog/safety-and-protection/how-to-avoid-scams-this-holiday-season-infographic">https://www.suncoastcreditunion.com/blog/safety-and-protection/how-to-avoid-scams-this-holiday-season-infographic</a>																					
4																											
5	1	Audience		Meets			Meets	Comments																			
6		1,1	Across	1			1																				
7		1,2	Specific	2																							
8																											
9	2	Key message focus - clear purpose																									
10		2,1	Awareness	1			1	How to avoid scams on holiday seasons																			
11		2,2	Awareness	1			1																				
12		2,3	Cyber	1			1																				
13		2,4	Empowerment	1																							
14																											
15	3	Timeframe																									
16		3,1	Generic	1																							
17		3,2	Covers	2			2	christmas holiday season																			
18																											
19																											
20	<b>Behaviour change attributes</b>																										
21																											
22	1	Promote situational awareness																									
23		1,1	Easy to	1			1																				
24		1,2	Easy to	1			1																				
25																											
26	2	Empower people																									
27		2,1	Simple informal	1			1																				
28		2,2	Appropriate	1			1																				
29		2,3	Overall	1				Neutral																			
30																											
31	3	Evidence-based content																									
32		3,1	Based	1			1	Examples																			
33		3,2	From	1																							
34																											
35	4	Memorable																									
36		4,1	Micro-	1			1																				
37		4,2	Learning	1			1																				
38		4,3	Considerate	1																							
39		4,4	Balance	1			1																				
40		4,5	Authentic	1			1	how to protect yourself from holiday scams																			
41																											
42	<b>Presentation attributes</b>																										
43																											
44	1	Visibility of the message																									
45		1,1	Appropriate	1			1																				
46		1,2	Draw attention	1			1																				
47																											
48	2	Layout, style and formatting																									
49		2,1	Uses	1			1																				
50		2,2	Create	1			1																				
51		2,3	Maximize	1			1																				
52																											
53	3	Inclusive / Accessible																									
54		3,1	A good color	1			1	using <a href="https://wlbaim.org/resources/contactchecker/">https://wlbaim.org/resources/contactchecker/</a>																			
55		3,2	Use	1			1																				
56		3,3	Use	1			1																				
57																											
58																											
59																											
60																											
61	<b>Communication Strategy attributes</b>					6																					
62	<b>Behaviour change attributes</b>					9																					
63	<b>Presentation attributes</b>					8																					
64																											
65	<b>TOTAL</b>					<b>23</b>																					
66																											
67	<b>Overall quality of awareness raising material</b>																										
68	<b>Low</b>					0-14																					
69	<b>Medium</b>					15-22																					
70	<b>High</b>					23-28																					



	A	B	C	D	E	F	G	H	I	J
1										
2		<b>Communication Strategy attributes</b>						<b>Evaluation</b>		
3							Infographic - website		<a href="https://www.pccu.org/wp-content/uploads/2023/01/ViewPhishingInfographic-768x2644.jpg">https://www.pccu.org/wp-content/uploads/2023/01/ViewPhishingInfographic-768x2644.jpg</a>	
4										
5		1 Audience		Marks			Marks	Comments		
6			1,1 Across groups		1					
7			1,2 Specific		2					
8										
9		2 Key message focus - clear purpose								
10			2,1 Awareness - about threat		1					
11			2,2 Awareness - about impact		1			1 Watch out for different Phishing scams		
12			2,3 Cyber hygiene - best practices		1					
13			Impowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1			1 report the incident		
14										
15		3 Timeliness								
16			3,1 Generic		1					
17			3,2 Covers specific time periods		2					
18										
19										
20		<b>Behaviour-change attributes</b>								
21										
22		1 Promote situational awareness								
23			1,1 Easy to understand what is the threat		1					
24			1,2 Easy to understand what is the impact		1					
25										
26		2 Empower people								
27			Simple information to understand how to address the threat		1					
28			2,1 Appropriate call to action message		1					
29			2,3 Overall conveys a positive message		1			Neutral		
30										
31		3 Evidence-based content								
32			3,1 Based on facts, e.g. statistics, etc.		1			1 Examples/ Statistics		
33			3,2 from credible source		1					
34										
35		4 Memorable								
36			4,1 Micro-learning - specific topic		1					
37			Micro-learning - short statements, focus on key points		1					
38			4,2 Considers different learning styles		1			1 Visual/text		
39			4,4 Balance between graphics and text		1					
40			Audience can easily relate, e.g. storytelling		1					
41										
42		<b>Presentation attributes</b>								
43										
44		1 Visibility of the message								
45			1,1 Appropriate location		1					
46			Draw attention to key information, e.g. by using contrasting colour		1					
47										
48		2 Layout, style and formatting								
49			Uses lines, borders and shapes to group related information		1					
50			Create text hierarchy (up to 3 different font styles)		1					
51			Maximum 4 colours		1					
52										
53		3 Inclusive / Accessible								
54			A good color contrast between the text color and background color		1			1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>		
55			Use appropriate font styles ()		1					
56			Use appropriate font size ()		1					
57										
58										
59										
60										
61		Communication Strategy attributes					5			
62		Behaviour-change attributes					8			
63		Presentation attributes					8			
64										
65							21			
66										
67		Overall quality of awareness raising material								
68		Low	0-14							
69		Medium	15-22							
70		High	23-28							
71										
72										
73										

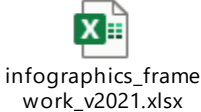


A	B	C	D	E	F	G	H	I	J	K	L	M	N
3	<b>Communication Strategy attributes</b>				<b>Evaluation</b>								
4					Infographic - website	<a href="https://symantecsecurity.com/2020/01/01/what-is-spear-phishing-and-why-is-it-so-dangerous-2/">https://symantecsecurity.com/2020/01/01/what-is-spear-phishing-and-why-is-it-so-dangerous-2/</a>							
6	1	Audience	Marks		Marks	Comments							
7		1.1	Across groups	1		1							
8		1.2	Specific	2									
10	2	Key message focus - clear purpose											
11		2.1	Awareness - about threat	1		1							
12		2.2	Awareness - about impact	1		1							
13		2.3	Cyber hygiene - best practices	1		1							
14		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1									
16	3	Timeliness											
17		3.1	Generic	1		1							
18		3.2	Covers specific time periods	2									
21	<b>Behaviour change attributes</b>												
23	1	Promote situational awareness											
24		1.1	Easy to understand what is the threat	1		1							
25		1.2	Easy to understand what is the impact	1									
27	2	Empower people											
28		2.1	Simple information to understand how to address the threat	1		1							
29		2.2	Appropriate call to action message	1		1							
30		2.3	Overall conveys a positive message	1		Neutral							
32	3	Evidence-based content											
33		3.1	Based on facts, e.g. statistics, etc.	1		1							
34		3.2	From credible source	1		1							
36	4	Memorable											
37		4.1	Micro-learning - specific topic	1		1							
38		4.2	Micro-learning - short statements, focus on key points	1		1							
39		4.3	Considers different learning styles	1		1							
40		4.4	Balance between graphics and text	1		1							
41		4.5	Audience can easily relate, e.g. storytelling	1		1							
43	<b>Presentation attributes</b>												
45	1	Visibility of the message											
46		1.1	Appropriate location	1		1							
47		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1							
49	2	Layout, style and formatting											
50		2.1	Uses lines, boxes and shapes to group related information	1		1							
51		2.2	Create text hierarchy (up to 3 different font styles)	1		1							
52		2.3	Maximum 4 colours	1		1							
54	3	Inclusive / Accessible											
55		3.1	A good color contrast between the text color and background color	1		1							
56		3.2	Use appropriate font styles ()	1		1							
57		3.3	Use appropriate font size ()	1		1							
62	<b>Communication Strategy attributes</b>					5							
63	<b>Behaviour change attributes</b>					8							
64	<b>Presentation attributes</b>					6							
66	<b>TOTAL</b>					<b>19</b>							
68	Overall quality of awareness raising material												
69	Low	0-14											
70	Medium	15-22											
71	High	23-28											



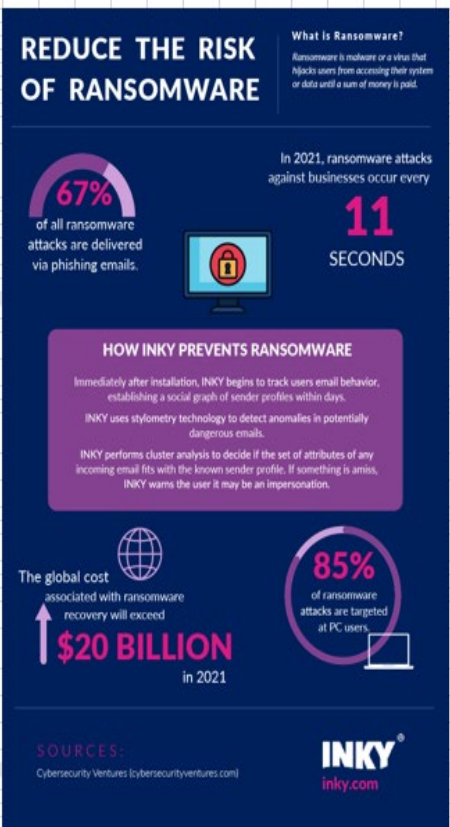
# A.2 Analysis Infographics 2021

The excel file contains all the evaluation of the twenty-five infographics for the year 2021.



1)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	2	Communication Strategy attributes				Evaluation																
	3					Infographic - website		<a href="https://www.inky.com/en/blog/the-evolution-of-ransomware-and-what-you-need-to-know-today">https://www.inky.com/en/blog/the-evolution-of-ransomware-and-what-you-need-to-know-today</a>														
	4					Mark																
	5	1	Audience	Mark		Comments																
	6		1.1 Across groups	1																		
	7		1.2 Specific	2																		
	8		2 Key message focus - clear purpose																			
	10		2.1 Awareness - about threat	1			1	How to reduce the risk of ransomware														
	11		2.2 Awareness - about impact	1			1	User cannot access their system and data														
	12		Cyber hygiene - best practices	1			1	Tips to prevent ransomware														
	13		Engagement - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																		
	14		3 Timeframe																			
	15		3.1 Generic	1			1															
	17		3.2 Covers specific time periods	2																		
	18		Behaviour-change attributes																			
	20		1 Promote situational awareness																			
	21		Easy to understand what is the threat					1	Easy to understand how to detect ransomware													
	23		1.1	1			1															
	24		1.2	1			1															
	25		2 Empower people																			
	26		Simple information to understand how to address the threat					1														
	27		2.1	1			1															
	28		2.2	1																		
	29		2.3	1			neutral															
	30		3 Evidence-based content																			
	31		Based on facts, e.g. statistics, etc.					1	statistics and graphs													
	32		3.1	1			1															
	33		3.2	1																		
	34		4 Memorable																			
	35		Micro-learning - specific topic					1														
	36		4.1	1			1															
	37		4.2	1			1															
	38		4.3	1			1	visual, text														
	39		4.4	1			1															
	40		4.5	1			1	Easy to explain the problem and give a solution, provides a real example														
	41		Presentation attributes																			
	42		1 Visibility of the message																			
	43		1.1 Appropriate location					1														
	44		Draw attention to key information, e.g. by using contrasting colour					1														
	45		1.2	1			1															
	46		2 Layout, style and formatting																			
	47		Use lines, borders and shapes to group related information					1														
	48		2.1	1			1															
	49		2.2	1			1															
	50		2.3	1			1															
	51		3 Inclusive / Accessible																			
	52		A good color contrast between the text color and background color					1	<a href="https://webaim.org/resources/contrastchecker/">using https://webaim.org/resources/contrastchecker/</a>													
	53		3.1	1			1															
	54		3.2	1			1															
	55		3.3	1			1															
	56																					
	57																					
	58																					
	59																					
	60																					
	61		Communication Strategy attributes					5														
	62		Behaviour-change attributes					9														
	63		Presentation attributes					7														
	64																					
	65		TOTAL					21														
	66		Overall quality of awareness raising material																			
	67		Low 0-14																			
	68		Medium 15-22																			
	69		High 23-28																			
	70																					



2)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
<b>Communication Strategy attributes</b>				<b>Evaluation</b>													
				Infographic - website				<a href="https://blog.tmcnet.com/blog/tech-behavior/infographic-a-new-ransomware-attack-every-11-seconds-70-who-pay-ds-not-get-files-back.html">https://blog.tmcnet.com/blog/tech-behavior/infographic-a-new-ransomware-attack-every-11-seconds-70-who-pay-ds-not-get-files-back.html</a>									
1	Audience	Markets	Markets	Comments													
	1.1	Across groups	1														
	1.2	Specific	2	2	Employees/Organizations												
2	Key message focus - clear purpose																
	2.1	Awareness - about threat	1	1													
	2.2	Awareness - about impact	1	1 If you pay you may not get back the files													
	2.3	Cyber hygiene - best practices	1														
	2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1														
3	Timeframe																
	3.1	Generic	1	1													
	3.2	Covers specific time periods	2														
<b>Behaviour-change attributes</b>																	
1	Promote situational awareness																
	1.1	Easy to understand what's the threat	1	1													
	1.2	Easy to understand what's the impact	1	1													
2	Empower people																
	2.1	Simple information to understand how to address the threat	1	1													
	2.2	Appropriate call to action message	1														
	2.3	Overall conveys a positive message	1	neutral													
3	Evidence-based content																
	3.1	Based on facts, e.g. statistics, etc.	1	1 statistic/examples													
	3.2	From credible source	1														
4	Memorable																
	4.1	Micro-learning - specific topic	1	1													
	4.2	Micro-learning - short statements, focus on key points	1	1													
	4.3	Considers different learning styles	1	1 visual/text													
	4.4	Balance between graphics and text	1	1													
	4.5	Audience can easily relate, e.g. storytelling	1														
<b>Presentation attributes</b>																	
1	Visibility of the message																
	1.1	Appropriate location	1	1													
	1.2	Draw attention to key information, e.g. by using contrasting colour	1	1													
2	Layout, style and formatting																
	2.1	Uses lines, borders and shapes to group related information	1	1													
	2.2	Create text hierarchy (up to 3 different font styles)	1	1													
	2.3	Maximum 6 colours	1	1													
3	Inclusive / Accessible																
	3.1	A good color contrast between the text color and background color	1														
	3.2	Use appropriate font styles()	1	1													
	3.3	Use appropriate font size()	1														
<b>Communication Strategy attributes</b>				5													
<b>Behaviour-change attributes</b>				8													
<b>Presentation attributes</b>				6													
<b>TOTAL</b>				19													
Overall quality of awareness raising material																	
Low				0-14													
Medium				15-22													
High				23-28													

**A NEW RANSOMWARE ATTACK EVERY 11 SECONDS AND 70% WHO PAY WILL NOT GET FILES BACK!**

A collection of cybercriminals called The RFAK (Responsible for RFAK ransomware) shared a new for targeting large enterprise operations is now targeting small businesses and general medical practices, particularly in Florida.

**PER CYBERSECURITY VENTURES**

- 25%** Increase in ransomware activity over the last 30 days (compared to the six months prior)
- 125%** Increase in attacks on small businesses, especially medical businesses like dentists, small general medicine practices, lab technician companies in ray, MRI, and med-spa and outpatient clinics.

Attacks typically happen via email, but the group has now expanded that apps and chat bots to deliver malicious links. Data suggests a 25% in attacks outside email channels like chatbots, chat apps, text messaging.

Previously, the RFAK group exclusively targeted enterprises for huge payouts. Not so anymore.

**STATS**

- Risk Costed more than \$10M in Changes between January and October 2019
- Ransomware payment between \$10,000 - \$400,000
- RFAK can take up to a year to fully penetrate a network and spread
- For the last 100 RFAK cases:
  - 25% of the time the victims were health care providers
  - 15% of the time the victims were schools
  - Around 50% of the time, attacks on small and medium-sized businesses with sensitive resources, not financial, are in healthcare industry
  - Most work attacks non-commercial computer systems.
- According to research, 7 out of 10 ransomware attacks will pay your ransom faster than the FBI
- On average, every 3rd of 3 commercial ransomware attacks will have to be reported to the media or the FBI
- Over 270 US medical centers, 71 hospitals who shared or mentioned attack
- A new ransomware will hit within 100 miles every 10 seconds in 2019, and every 11 seconds by 2021.
- 70% of businesses that will increase their ransomware response budget within 10 months by 2021
- 80% of IT executives from phishing attacks increased 10 percent over 2017

Attributed Cybersecurity Institute

3)

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>										
3					Infographic - website <a href="https://content.transition.com/v/fraud-trends-infographic-q3">https://content.transition.com/v/fraud-trends-infographic-q3</a>										
4															
5	Audience			Markets	Marks			Comments							
6	1,1	Across groups		1											
7	1,2	Specific		2	2 Employees/Organisations										
8															
9	Key message focus - clear purpose														
10	2,1	Awareness - about threat		1	1										
11	2,2	Awareness - about impact		1											
12	2,3	Cyber hygiene - best practices		1											
13	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1											
14															
15	Timeframe														
16	3,1	Generic		1											
17	3,2	Covers specific time periods		2	2 Holidays										
18															
19															
20	<b>Behaviour-change attributes</b>														
21															
22	Promote situational awareness														
23	1,1	Easy to understand what is the threat		1	1										
24	1,2	Easy to understand what is the impact		1											
25															
26	Empower people														
27	2,1	Simple information to understand how to address the threat		1	1										
28	2,2	Appropriate call to action message		1											
29	2,3	Overall conveys a positive message		1											
30															
31	Evidence-based content														
32	3,1	Based on facts, e.g. statistics, etc.		1	1 statistics/examples										
33	3,2	From credible source		1											
34															
35	Memorable														
36	4,1	Micro-learning - specific topic		1	1										
37	4,2	Micro-learning - short statements, focus on key points		1	1										
38	4,3	Considers different learning styles		1	1 visual/text										
39	4,4	Balance between graphics and text		1											
40	4,5	Audience can easily relate, e.g. storytelling		1											
41															
42	<b>Presentation attributes</b>														
43															
44	Visibility of the message														
45	1,1	Appropriate location		1											
46	1,2	Draw attention to key information, e.g. by using contrasting colour		1	1										
47															
48	Layout, style and formatting														
49	2,1	Uses lines, borders and shapes to group related information		1	1										
50	2,2	Create text hierarchy (up to 3 different font styles)		1	1										
51	2,3	Maximum 6 colours		1	1										
52															
53	Inclusive / Accessible														
54	3,1	A good color contrast between the text color and background color		1	1										
55	3,2	Use appropriate font styles ()		1	1										
56	3,3	Use appropriate font size ()		1	1										
57															
58															
59															
60															
61	Communication Strategy attributes				5										
62	Behaviour-change attributes				6										
63	Presentation attributes				7										
64															
65	<b>TOTAL</b>				<b>18</b>										
66															
67	Overall quality of awareness raising material														
68	Low 0-14														
69	<b>Medium 15-22</b>														
70	High 23-28														
71															



4)

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>											
3						Infographic - website	<a href="https://www.clearconcepts.ca/insights/7-tips-to-identify-phishing-emails">https://www.clearconcepts.ca/insights/7-tips-to-identify-phishing-emails</a>									
4																
5	Audience		Marks		Marks	Comments										
6	1,1	Across groups	1													
7	1,2	Specific	2			2	Baby boomers/Generation X									
8																
9	Key message focus - clear purpose															
10	2,1	Awareness - about threat	1			1	how to avoid phishing emails									
11	2,2	Awareness - about impact	1													
12	2,3	Cyber hygiene - best practices	1			1										
13	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report the incident									
14																
15	Timeframe															
16	3,1	Generic	1			1										
17	3,2	Covers specific time periods	2													
18																
19																
20	<b>Behaviour-change attributes</b>															
21																
22	Promote situational awareness															
23	1,1	Easy to understand what is the threat	1			1										
24	1,2	Easy to understand what is the impact	1													
25																
26	Empower people															
27	2,1	Simple information to understand how to address the threat	1			1										
28	2,2	Appropriate call to action message	1			1										
29	2,3	Overall conveys a positive message	1				neutral									
30																
31	Evidence-based content															
32	3,1	Based on facts, e.g. statistics, etc.	1			1	examples									
33	3,2	From credible source	1													
34																
35	Memorable															
36	4,1	Micro-learning - specific topic	1			1										
37	4,2	Micro-learning - short statements, focus on key points	1			1										
38	4,3	Considers different learning styles	1													
39	4,4	Balance between graphics and text	1			1										
40	4,5	Audience can easily relate, e.g. storytelling	1			1	tips to identify phishing emails									
41																
42	<b>Presentation attributes</b>															
43																
44	Visibility of the message															
45	1,1	Appropriate location	1			1										
46	1,2	Draw attention to key information, e.g. by using contrasting colour	1			1										
47																
48	Layout, style and formatting															
49	2,1	Use lines, borders and shapes to group related information	1			1										
50	2,2	Create text hierarchy (up to 3 different font styles)	1													
51	2,3	Maximum 4 colours	1			1										
52																
53	Inclusive / Accessible															
54	3,1	A good color contrast between the text color and background color	1				using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>									
55	3,2	Use appropriate font styles ()	1			1										
56	3,3	Use appropriate font size ()	1			1										
57																
58																
59																
60																
61	<b>Communication Strategy attributes</b>					6										
62	<b>Behaviour-change attributes</b>					8										
63	<b>Presentation attributes</b>					6										
64																
65						<b>TOTAL</b>	<b>20</b>									
66																
67	Overall quality of awareness raising material															
68	Low	0-14														
69	Medium	15-22														
70	High	23-28														
71																

**TIPS TO IDENTIFY PHISHING EMAILS!**

Before you click anything or reply to a suspicious email, remember to look for any of these signs first:

- 1 Always verify if the sender's address is correct and legitimate.
- 2 Be suspicious on misspellings and grammatical errors!
- 3 Threat actors will often avoid calls or other forms of direct communication.
- 4 Never open attachments or links found on suspicious emails.
- 5 Scammers commonly request Wire transfers, Bitcoins, or Gift cards.
- 6 Phishing emails can contain links that lead to fake login pages. Do not provide your account information when prompted.
- 7 Some of these emails are sent in bulk. Ask a colleague if they received a similar email from the same sender.

When in doubt or if the email doesn't feel right, call the organization or the sender directly.

Be cautious opening random emails with questionable content as phishing emails can come from either impersonated or stolen accounts.

WWW.CLEARCONCEPTS.CA

5)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
2	<b>Communication Strategy attributes</b>			<b>Evaluation</b>														
3						Infographic - website	<a href="https://claracamin.com/project/phishing-infographic/">https://claracamin.com/project/phishing-infographic/</a>											
4																		
5	1	Audience		Marks		Marks	Comments											
6		1.1	Across groups	1														
7		1.2	Specific	2			Millennials/Generation Z											
8																		
9	2	Key message focus - clear purpose																
10		2.1	Awareness - about threat	1			1											
11		2.2	Awareness - about impact	1														
12		2.3	Cyber hygiene - best practices	1			1											
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report an incident										
14																		
15	3	Timeframe																
16		3.1	Generic	1			1											
17		3.2	Covers specific time periods	2														
18																		
19																		
20	<b>Behaviour-change attributes</b>																	
21																		
22	1	Promote situational awareness																
23		1.1	Easy to understand what is the threat	1			1											
24		1.2	Easy to understand what is the impact	1														
25																		
26	2	Empower people																
27		2.1	Simple information to understand how to address the threat	1			1											
28		2.2	Appropriate call to action message	1			1											
29		2.3	Overall conveys a positive message	1														
30																		
31	3	Evidence-based content																
32		3.1	Based on facts, e.g. statistics, etc.	1			1	statistics/examples										
33		3.2	From credible source	1			1	links										
34																		
35	4	Memorable																
36		4.1	Micro-learning - specific topic	1			1											
37		4.2	Micro-learning - short statements, focus on key points	1			1											
38		4.3	Consider different learning styles	1			1	visual/text										
39		4.4	Balance between graphics and text	1			1											
40		4.5	Audience can easily relate, e.g. storytelling	1			1	If your victim of phishing attacks what you do										
41																		
42	<b>Presentation attributes</b>																	
43																		
44	1	Visibility of the message																
45		1.1	Appropriate location	1			1											
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1			1											
47																		
48	2	Layout, style and formatting																
49		2.1	Uses lines, borders and shapes to group related information	1			1											
50		2.2	Create text hierarchy (up to 3 different font styles)	1			1											
51		2.3	Maximum 4 colours	1			1											
52																		
53	3	Inclusive / Accessible																
54		3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>										
55		3.2	Use appropriate font styles (i)	1			1											
56		3.3	Use appropriate font size (j)	1			1											
57																		
58																		
59																		
60																		
61	<b>Communication Strategy attributes</b>						6											
62	<b>Behaviour-change attributes</b>						10											
63	<b>Presentation attributes</b>						8											
64																		
65	<b>TOTAL</b>						24											
66																		
67	<b>Overall quality of awareness raising material</b>																	
68	<b>Low</b>						0-14											
69	<b>Medium</b>						15-22											
70	<b>High</b>						23-28											
71																		



6)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N						
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>														
3	Infographic - website					<a href="https://logrhythm.com/blog/cybersecurity-predictions-for-2021/">https://logrhythm.com/blog/cybersecurity-predictions-for-2021/</a>														
4																				
5	1	Audience		Marks		Marks		Comments												
6		1.1	Across groups		1															
7		1.2	Specific		2			employees/companies												
8																				
9	2	Key message focus - clear purpose																		
10		2.1	Awareness - about threat		1			1												
11		2.2	Awareness - about impact		1															
12		2.3	Cyber hygiene - best practices		1			1												
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1															
14																				
15	3	Timeframe																		
16		3.1	Generic		1			1												
17		3.2	Covers specific time periods		2															
18																				
19																				
20	<b>Behaviour-change attributes</b>																			
21	1	Promote situational awareness																		
22		1.1	Easy to understand what is the threat		1			1												
23		1.2	Easy to understand what is the impact		1															
24																				
25	2	Empower people																		
26		2.1	Simple information to understand how to address the threat		1			1												
27		2.2	Appropriate call to action message		1			1												
28		2.3	Overall conveys a positive message		1			neutral												
29																				
30	3	Evidence-based content																		
31		3.1	Based on facts, e.g. statistics, etc.		1															
32		3.2	From credible source		1															
33																				
34	4	Memorable																		
35		4.1	Micro-learning - specific topic		1			1												
36		4.2	Micro-learning - short statements, focus on key points		1															
37		4.3	Considers different learning styles		1			1												
38		4.4	Balance between graphics and text		1			1												
39		4.5	Audience can easily relate, e.g. storytelling		1															
40																				
41																				
42	<b>Presentation attributes</b>																			
43	1	Visibility of the message																		
44		1.1	Appropriate location		1															
45		1.2	Draw attention to key information, e.g. by using contrasting colour		1			1												
46																				
47	2	Layout, style and formatting																		
48		2.1	Uses lines, borders and shapes to group related information		1			1												
49		2.2	Create text hierarchy (up to 3 different font styles)		1			1												
50		2.3	Maximum 4 colours		1			1												
51																				
52	3	Inclusive / Accessible																		
53		3.1	A good color contrast between the text color and background color		1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>												
54		3.2	Use appropriate font styles ( )		1			1												
55		3.3	Use appropriate font size ( )		1			1												
56																				
57																				
58																				
59																				
60																				
61	Communication Strategy attributes					5														
62	Behaviour-change attributes					6														
63	Presentation attributes					6														
64																				
65	<b>TOTAL</b>					<b>17</b>														
66																				
67	Overall quality of awareness raising material																			
68	Low 0-14																			
69	Medium 15-22																			
70	High 23-28																			

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>															
					Infographic - website	<a href="https://www.europol.europa.eu/publications-events/publications/mobile-malware-infographic">https://www.europol.europa.eu/publications-events/publications/mobile-malware-infographic</a>														
5	1	Audience	Mark	Mark	Comments															
6		1.1	Across groups	1																
7		1.2	Specific	2		Millennials/Generation Z														
9	2	Key message focus - clear purpose																		
10		2.1	Awareness - about threat	1		how to install apps														
11		2.2	Awareness - about impact	1																
12		2.3	Cyber hygiene - best practices	1																
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		download mobile secure app														
15	3	Timeframe																		
16		3.1	Generic	1																
17		3.2	Covers specific time periods	2																
20	<b>Behaviour-change attributes</b>																			
22	1	Promote situational awareness																		
23		1.1	Easy to understand what is the threat	1																
24		1.2	Easy to understand what is the impact	1																
26	2	Empower people																		
27		2.1	Simple information to understand how to address the threat	1																
28		2.2	Appropriate call to action message	1																
29		2.3	Overall conveys a positive message	1		neutral														
31	3	Evidence-based content																		
32		3.1	Based on facts, e.g. statistics, etc.	1																
33		3.2	From credible source	1		Europa														
35	4	Memorable																		
36		4.1	Micro-learning - specific topic	1																
37		4.2	Micro-learning - short statements, focus on key points	1																
38		4.3	Considers different learning styles	1																
39		4.4	Balance between graphics and text	1		visual/text														
40		4.5	Audience can easily relate, e.g. storytelling	1																
42	<b>Presentation attributes</b>																			
44	1	Visibility of the message																		
45		1.1	Appropriate location	1																
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1																
48	2	Layout, style and formatting																		
49		2.1	Uses lines, borders and shapes to group related information	1																
50		2.2	Create text hierarchy (up to 3 different font styles)	1																
51		2.3	Maximum 4 colours	1																
53	3	Inclusive / Accessible																		
54		3.1	Adequate color contrast between the text color and background color	1		using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>														
55		3.2	Use appropriate font styles ()	1																
56		3.3	Use appropriate font size ()	1																
61	<b>Communication Strategy attributes</b>					6														
62	<b>Behaviour-change attributes</b>					8														
63	<b>Presentation attributes</b>					8														
65	<b>TOTAL</b>					22														
67	Overall quality of awareness raising material																			
68	Low					0-14														
69	Medium					15-22														
70	High					23-28														



8)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N						
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>														
3						Infographic - website					<a href="https://www.synovus.com/business/resource-center/protecting-your-business/how-to-recognize-bec-infographic/">https://www.synovus.com/business/resource-center/protecting-your-business/how-to-recognize-bec-infographic/</a>									
4																				
5	1	Audience		Marks		Marks		Comments												
6		1.1	Across groups		1															
7		1.2	Specific		2		Employees/Organisations													
8																				
9	2	Key message focus - clear purpose																		
10		2.1	Awareness - about threat		1		1													
11		2.2	Awareness - about impact		1		1													
12		2.3	Cyber hygiene - best practices		1		1													
13		2.4	Engagement - call to action, e.g. visit a website to learn more, to report an incident, etc.		1		1 Education employees													
14																				
15	3	Timeframe																		
16		3.1	Generic		1		1													
17		3.2	Covers specific time periods		2															
18																				
19																				
20	<b>Behaviour-change attributes</b>																			
21	1	Promote situational awareness																		
22		1.1	Easy to understand what is the threat		1		1													
23		1.2	Easy to understand what is the impact		1		1													
24																				
25	2	Empower people																		
26		2.1	Simple information to understand how to address the threat		1		1													
27		2.2	Appropriate call to action message		1		1													
28		2.3	Overall conveys a positive message		1		Neutral													
29																				
30	3	Evidence-based content																		
31		3.1	Based on facts, e.g. statistics, etc.		1		1 Statistics													
32		3.2	From credible source		1															
33																				
34	4	Memorable																		
35		4.1	Micro-learning - specific topic		1		1													
36		4.2	Micro-learning - short statements, focus on key points		1		1													
37		4.3	Considers different learning styles		1		1													
38		4.4	Balance between graphics and text		1		1													
39		4.5	Audience can easily relate, e.g. storytelling		1		1													
40																				
41																				
42	<b>Presentation attributes</b>																			
43	1	Visibility of the message																		
44		1.1	Appropriate location		1		1													
45		1.2	Draw attention to key information, e.g. by using contrasting colour		1		1													
46																				
47	2	Layout, style and formatting																		
48		2.1	Uses links, borders and shapes to group related information		1		1													
49		2.2	Create text hierarchy (up to 3 different font styles)		1		1													
50		2.3	Maximum 4 columns		1		1													
51																				
52	3	Inclusive / Accessible																		
53		3.1	A good color contrast between the text color and background color		1		1													
54		3.2	Use appropriate font styles ()		1		1													
55		3.3	Use appropriate font size ()		1		1													
56																				
57																				
58																				
59																				
60																				
61	<b>Communication Strategy attributes</b>					7														
62	<b>Behaviour-change attributes</b>					10														
63	<b>Presentation attributes</b>					8														
64																				
65	<b>TOTAL</b>					<b>25</b>														
66																				
67	Overall quality of awareness raising material																			
68	<b>Low</b> 0-14																			
69	<b>Medium</b> 15-22																			
70	<b>High</b> 23-28																			
71																				

9)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	Communication Strategy attributes				Evaluation									
3					Infographic - website	<a href="https://www.europol.europa.eu/publications-events/publications/carbanak/cobalt-infographic">https://www.europol.europa.eu/publications-events/publications/carbanak/cobalt-infographic</a>								
5	1	Audience	Marks		Marks	Comments								
6		1.1	Across groups	1										
7		1.2	Specific	2		Employees/Organizations								
9	2	Key message focus - clear purpose												
10		2.1	Awareness - about threat	1		1 Financial institutions threat								
11		2.2	Awareness - about impact	1		1 Impact to bank companies								
12		2.3	Cyber hygiene - best practices	1										
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1										
15	3	Timeframe												
16		3.1	Generic	1		1								
17		3.2	Covers specific time periods	2										
20	Behaviour-change attributes													
22	1	Promote situational awareness												
23		1.1	Easy to understand what is the threat	1		1								
24		1.2	Easy to understand what is the impact	1		1								
26	2	Empower people												
27		2.1	Simple information to understand how to address the threat	1		1								
28		2.2	Appropriate call to action message	1										
29		2.3	Overall conveys a positive message	1		Neutral								
31	3	Evidence-based content												
32		3.1	Based on facts, e.g. statistics, etc.	1		1 Statistics, visual, graphics								
33		3.2	From credible source	1		1 Europol								
35	4	Memorable												
36		4.1	Micro-learning - specific topic	1		1								
37		4.2	Micro-learning - short statements, focus on key points	1		1								
38		4.3	Considers different learning styles	1		1 Visual/text								
39		4.4	Balance between graphics and text	1		1								
40		4.5	Audience can easily relate, e.g. storytelling	1		1 real examples/ statistics								
42	Presentation attributes													
44	1	Visibility of the message												
45		1.1	Appropriate location	1		1								
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1								
48	2	Layout, style and formatting												
49		2.1	Uses lines, borders and shapes to group related information	1		1								
50		2.2	Create text hierarchy (up to 3 different font styles)	1		1								
51		2.3	Maximum 4 colours	1		1								
53	3	Inclusive / Accessible												
54		3.1	Adequate color contrast between the text color and background color	1		1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>								
55		3.2	Use appropriate font styles ()	1		1								
56		3.3	Use appropriate font size ()	1		1								
61	Communication Strategy attributes				5									
62	Behaviour-change attributes				10									
63	Presentation attributes				8									
65	TOTAL				23									
67	Overall quality of awareness raising material													
68	Low				0-14									
69	Medium				15-22									
70	High				23-28									



10)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>												
3						Infographic - website <a href="https://www.scrum.com/privacy-security/common-phishing-scams">https://www.scrum.com/privacy-security/common-phishing-scams</a>												
4																		
5	1 Audience		Marks		Marks													
6	1.1 Across groups		1		1 Individuals and Employees													
7	1.2 Specific		2															
8																		
9	2 Key message focus - clear purpose																	
10	2.1 Awareness - about threat		1		1 Common holiday phishing attacks													
11	2.2 Awareness - about impact		1															
12	2.3 Cyber hygiene - best practices		1															
13	2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1															
14																		
15	3 Timeframe																	
16	3.1 Generic		1															
17	3.2 Covers specific time periods		2		2 Holiday season													
18																		
19																		
20	<b>Behaviour-change attributes</b>																	
21																		
22	1 Promote situational awareness																	
23	1.1 Easy to understand what is the threat		1		1													
24	1.2 Easy to understand what is the impact		1															
25																		
26	2 Empower people																	
27	2.1 Simple information to understand how to address the threat		1		1													
28	2.2 Appropriate call to action message		1															
29	2.3 Overall conveys a positive message		1		Neutral													
30																		
31	3 Evidence-based content																	
32	3.1 Based on facts, e.g. statistics, etc.		1															
33	3.2 From credible source		1															
34																		
35	4 Memorable																	
36	4.1 Micro-learning - specific topic		1		1													
37	4.2 Micro-learning - short statements, focus on key points		1															
38	4.3 Consider different learning styles		1															
39	4.4 Balance between graphics and text		1		1													
40	4.5 Audience can easily relate, e.g. storytelling		1		1 real examples													
41																		
42	<b>Presentation attributes</b>																	
43																		
44	1 Visibility of the message																	
45	1.1 Appropriate location		1		1													
46	1.2 Draw attention to key information, e.g. by using contrasting colour		1		1													
47																		
48	2 Layout, style and formatting																	
49	2.1 Use lines, borders and shapes to group related information		1		1													
50	2.2 Create text hierarchy (up to 3 different font styles)		1		1													
51	2.3 Maximum 4 colours		1		1													
52																		
53	3 Inclusive / Accessible																	
54	3.1 A good color contrast between the text color and background color		1		1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
55	3.2 Use appropriate font styles ()		1		1													
56	3.3 Use appropriate font size ()		1		1													
57																		
58																		
59																		
60																		
61	Communication Strategy attributes					4												
62	Behaviour-change attributes					5												
63	Presentation attributes					8												
64																		
65	<b>TOTAL</b>					<b>17</b>												
66																		
67	Overall quality of awareness-raising material																	
68	Low 0-14																	
69	Medium 15-22																	
70	High 23-28																	





	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1														
2		<b>Communication Strategy attributes</b>					<b>Evaluation</b>							
3														
4														
5		1	Audience		Marks		Marks		Comments					
6			1.1	Across groups	1									
7			1.2	Specific	2				2	Baby boomers/Generation X				
8														
9		2	Key message focus - clear purpose											
10			2.1	Awareness - about threat	1				1	How to not get hooked				
11			2.2	Awareness - about impact	1									
12			2.3	Clear bylines - best practice	1									
13				Engagement - call to action, e.g. visit a website to learn more, 2.6	1					1	visit a website to learn more			
14														
15		3	Timeframe											
16			3.1	Generic	1									
17			3.2	Covers specific time periods	2									
18														
19		<b>Behaviour-change attributes</b>												
20		1	Promote situational awareness											
21			1.1	Easy to understand what is the threat	1									
22			1.2	Easy to understand what is the impact	1									
23														
24		2	Empower people											
25			2.1	Simple information to understand how to address the threat	1									
26			2.2	Appropriate call to action message	1									
27			2.3	Overall convey a positive message	1					Neutral				
28														
29		3	Evidence-based content											
30			3.1	Based on facts, e.g. statistics, etc.	1									
31			3.2	From credible source	1									
32														
33		4	Memorable											
34			4.1	Micro-learning - specific topic	1									
35			4.2	Micro-learning - short statements, focus on key points	1									
36			4.3	Considers different learning styles	1					1	Visual examples			
37			4.4	Balances between graphics and text	1									
38			4.5	Audience can easily relate, e.g. storytelling	1					1	Real examples			
39														
40														
41		<b>Presentation attributes</b>												
42		1	Visibility of the message											
43			1.1	Appropriate location	1									
44			1.2	Clear attention to key information, e.g. by using contrasting colour	1									
45														
46		2	Layout, style and formatting											
47			2.1	Uses lines, borders and shapes to group related information	1									
48			2.2	Creates text hierarchy by using 3 different font styles	1									
49			2.3	Maximum 6 columns	1									
50														
51		3	Inclusive / Accessible											
52			3.1	A good color contrast between the text color and background color	1									
53			3.2	Use appropriate font style(s)	1									
54			3.3	Use appropriate font size	1									
55														
56														
57														
58														
59														
60														
61														
62														
63														
64														
65														
66														
67														
68														
69														
70														
71														



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2	Communication Strategy attributes				Evaluation																
3					Infographic - website <a href="https://www.eurostat.eu/media-pwg/newsroom/news/low-online-shopping-how-to-protect-yourself-against-online-scams">https://www.eurostat.eu/media-pwg/newsroom/news/low-online-shopping-how-to-protect-yourself-against-online-scams</a>																
4																					
5	1	Audience	Marks		Marks																
6		1.1	Across groups	1																	
7		1.2	Specific	2	2 Individuals/Gender 70+ (Baby boomers)																
8																					
9	2	Key message factor - clear purpose			1 Rules of secure online shopping																
10		2.1	Awareness - about threat	1																	
11		2.2	Awareness - about impact	1																	
12		2.3	Open/hygiene - best practices	1																	
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																	
14																					
15	3	Timeframe			1																
16		3.1	Generic	1																	
17		3.2	Covers specific time periods	2																	
18																					
19																					
20	Behaviour-change attributes																				
21	1	Promote situational awareness																			
22		1.1	Easy to understand what is the threat	1	1																
23		1.2	Easy to understand what is the impact	1																	
24			Overall conveys a positive message	1	Neutral																
25	2	Empower people																			
26		2.1	Simple information to understand how to address the threat	1	1																
27		2.2	Appropriate call to action	1																	
28		2.3	Overall conveys a positive message	1	Neutral																
29			Overall conveys a positive message	1	Neutral																
30																					
31	3	Evidence-based content																			
32		3.1	Based on facts, e.g. statistics, etc.	1	1																
33		3.2	From credible source	1	1																
34																					
35	4	Memorable																			
36		4.1	Micro-learning - specific topic	1	1																
37		4.2	Micro-learning - short statements, focus on key points	1	1																
38		4.3	Considers different learning styles	1	1																
39		4.4	Balance between graphics and text	1	1																
40		4.5	Audience can easily relate, e.g. storytelling	1	1																
41																					
42	Presentation attributes																				
43																					
44	1	Ability of the message																			
45		1.1	Appropriate location	1	1																
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1	1																
47																					
48	2	Layout, style and formatting																			
49		2.1	Use lines, borders and shapes to group related information	1	1																
50		2.2	Create text hierarchy (upto 3 different font styles)	1	1																
51		2.3	Maximum of colours	1	1																
52																					
53	3	Inclusive / Accessible																			
54		3.1	A good color contrast between the text color and background color	1	1																
55		3.2	Use appropriate font style(s)	1	1																
56		3.3	Use appropriate font size(s)	1	1																
57																					
58																					
59																					
60																					
61	Communication Strategy attributes			5																	
62	Behaviour-change attributes			8																	
63	Presentation attributes			7																	
64																					
65	TOTAL			20																	
66																					
67	Overall quality of awareness-raising material																				
68	Low 0-14																				
69	Medium 15-22																				
70	High 23-30																				



14)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
2	Communication Strategy attributes				Evaluation																	
3						Infographic - website	<a href="https://www.synovus.com/persona/awareness-center/financial-safety-and-security/infographic-how-to-spot-red-flags-for-banking-scams/">https://www.synovus.com/persona/awareness-center/financial-safety-and-security/infographic-how-to-spot-red-flags-for-banking-scams/</a>															
5	1	Audience	Mark		Mark	Comments																
6		1.1	Across groups	1																		
7		1.2	Specific	2		1 Individual																
9	2	Key message focus - clear purpose																				
10		2.1	Awareness - about threat	1			1	How to spot red flags for banking scams														
11		2.2	Awareness - about impact	1			1															
12		2.3	Cyber hygiene - best practices	1			1															
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1															
15	3	Time/area																				
16		3.1	Generic	1			1															
17		3.2	Covers specific time periods	2																		
20	Behaviour-change attributes																					
22	1	Promote situational awareness																				
23		1.1	Easy to understand what's the threat	1			1															
24		1.2	Easy to understand what's the impact	1			1															
26	2	Empower people																				
27		2.1	Simple information to understand how to address the threat	1			1															
28		2.2	Appropriate call to action message	1			1															
29		2.3	Overall conveys a positive message	1			Neutral															
31	3	Evidence-based content																				
32		3.1	Based on facts, e.g. statistics, etc.	1																		
33		3.2	From credible source	1																		
35	4	Memorable																				
36		4.1	Micro-learning - specific topic	1			1															
37		4.2	Micro-learning - short statements, focus on key points	1																		
38		4.3	Considers different learning styles	1			1	Visual examples														
39		4.4	Balance between graphics and text	1																		
40		4.5	Audience can easily relate, e.g. storytelling	1			1	Real examples														
42	Presentation attributes																					
45	1	Visibility of the message																				
46		1.1	Appropriate location	1																		
47		1.2	Draw attention to key information, e.g. by using contrasting colour	1			1															
49	2	Layout, style and formatting																				
50		2.1	Use lines, borders and shapes to group related information	1			1															
51		2.2	Create text hierarchy (up to 3 different font styles)	1			1															
52		2.3	Maximum 4 colours	1			1															
53	3	Inclusive / Accessible																				
54		3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/awareness/contrastchecker/">https://webaim.org/awareness/contrastchecker/</a>														
55		3.2	Use appropriate font style(s)	1			1															
56		3.3	Use appropriate font size(s)	1			1															
61	Communication Strategy attributes						5															
62	Behaviour-change attributes						7															
63	Presentation attributes						7															
65	TOTAL						19															
67	Overall quality of awareness raising material																					
68	Low	0-14																				
69	Medium	15-22																				
70	High	23-30																				

## How to spot red flags for banking scams

Scammers use tricks to gain access to your personal and account info. This can lead to everything from fraudulent withdrawals from your bank account to unauthorized charges on your credit card.

**The best way to protect yourself is to learn to identify common red flags, and then take action.**

**AND REMEMBER:**  
No reputable financial institution – including Synovus – will ever call or email you to ask for your personal info.

### Red flags by phone:

Commonly called **vishing**

- You receive a call or text from your bank, but the person doesn't have basic info you'd expect them to have. Examples include your social security number, account number, or mailing address.
- The caller claims they're from a bank you do business with, but something doesn't sound right. For example, they might mispronounce the name of the financial institution.
- The person doesn't reference specific details about your account and instead asks you for basic account info. No bank would call to ask you for this since they'd already have this info on file.

### Red flags by text:

Commonly called **smishing**

- You get a text that seems to be from your bank, warning you that there's a problem with your account requiring immediate attention. The message asks you to respond with passwords, authentication codes, or personal and financial info.

### Red flags by email:

Commonly called **phishing**

- You receive an email that says it's from your bank. It asks you to reply with your address, social security number, account number, password, or any other personal info. Any bank you do business with will already have this info.
- The email asks you to click on a link, which takes you to a page to enter your user ID and password. This is most likely a fake website created by hackers, designed to make you think you're on your bank's website.

**If you suspect a scam, call the customer service number on your credit card, debit card, or printed bank statement.**

**Other tips for protecting yourself against scammers**

- Freeze your credit reports with the big three credit bureaus: Equifax, Experian, and TransUnion. If scammers get your info, they can't open any credit in your name.
- Sign up for banking alerts to get instant notifications any time there's activity on your account, including if it has been compromised.

**SYNOVUS**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2	Communication Strategy attributes			Evaluation		Infographic - website <a href="https://cta.ca/holiday-scams">https://cta.ca/holiday-scams</a>															
5	1	Audience	Marks	Marks	Comments																
6		1.1	Across groups	1																	
7		1.2	Specific	2																	
9	2	Key message focus - clear purpose																			
10		2.1	Awareness - about threat	1																	
11		2.2	Awareness - about impact	1																	
12		2.3	Cyber hygiene - best practices	1																	
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1 visit a website to learn more															
15	3	Timeframe																			
16		3.1	Generic	1																	
17		3.2	Covers specific time periods	2		2 Holiday scams															
20	Behaviour-change attributes																				
22	1	Promote situational awareness																			
23		1.1	Easy to understand what's the threat	1		1															
24		1.2	Easy to understand what's the impact	1		1															
26	2	Empower people																			
27		2.1	Simple information to understand how to address	1		1															
28		2.2	Appropriate call to action message	1																	
29		2.3	Overall convey a positive message	1		Neutral															
31	3	Evidence-based content																			
32		3.1	Based on facts, e.g. statistics, etc.	1																	
33		3.2	From credible source	1																	
35	4	Memorable																			
36		4.1	Micro-learning - specific topic	1		1															
37		4.2	Micro-learning - short statements, focus on key points	1		1															
38		4.3	Considers different learning styles	1		1															
39		4.4	Balance between graphics and text	1		1															
40		4.5	Audience can easily relate, e.g. storytelling	1		1 learn how to avoid the threat															
42	Presentation attributes																				
44	1	Visibility of the message																			
45		1.1	Appropriate location	1		1															
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1															
48	2	Layout, style and formatting																			
49		2.1	Uses lines, borders and shapes to group related information	1		1															
50		2.2	Create text hierarchy (upto 3 different font styles)	1		1															
51		2.3	Adjustment of colours	1		1															
53	3	Inclusive / Accessible																			
54		3.1	A good color contrast between the text color and background color	1		using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>															
55		3.2	Use appropriate font styles()	1		1															
56		3.3	Use appropriate font size()	1		1															
61	Communication Strategy attributes			6																	
62	Behaviour-change attributes			7																	
63	Presentation attributes			7																	
65	TOTAL			20																	
67	Overall quality of awareness raising material																				
68	Low			0-14																	
69	Medium			15-22																	
70	High			23-28																	



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>																
3					Infographic - website	<a href="https://www.infosecinsights.com/content-library/infographic-need-to-know-general-security/">https://www.infosecinsights.com/content-library/infographic-need-to-know-general-security/</a>															
5	1	Audience	Marks		Marks	Comments															
6		1.1 Across groups	1			1	Individuals														
7		1.2 Specific	2																		
9	2	Key message focus - clear purpose																			
10		2.1 Awareness - about threat	1			1															
11		2.2 Awareness - about impact	1			1															
12		2.3 Cyber hygiene - best practices	1			1															
13		2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																		
15	3	Timeframe																			
16		3.1 Generic	1			1															
17		3.2 Covers specific time periods	2																		
20	<b>Behaviour-change attributes</b>																				
22	1	Promote situational awareness																			
23		1.1 Easy to understand what is the threat	1			1															
24		1.2 Easy to understand what is the impact	1			1															
26	2	Empower people																			
27		2.1 Simple information to understand how to address the threat	1			1															
28		2.2 Appropriate call to action message	1			1															
29		2.3 Overall conveys a positive message	1				Neutral														
31	3	Evidence-based content																			
32		3.1 Based on facts, e.g. statistics, etc.	1			1	statistics														
33		3.2 From credible source	1			1	INFOSEC														
35	4	Memorable																			
36		4.1 Micro-learning - specific topic	1			1															
37		4.2 Micro-learning - short statements, focus on key points	1																		
38		4.3 Considers different learning styles	1			1	Visual/text														
39		4.4 Balance between graphics and text	1			1															
40		4.5 Audience can easily relate, e.g. storytelling	1			1	how to avoid the threat														
42	<b>Presentation attributes</b>																				
44	1	Visibility of the message																			
45		1.1 Appropriate location	1			1															
46		1.2 Draw attention to key information, e.g. by using contrasting colour	1			1															
48	2	Layout, style and formatting																			
49		2.1 Uses lines, borders and shapes to group related information	1			1															
50		2.2 Create text hierarchy (up to 3 different font styles)	1			1															
51		2.3 Maximum 6 colours	1																		
53	3	Inclusive / Accessible																			
54		3.1 A good color contrast between the text color and background color	1				<a href="https://webaim.org/resources/contrastchecker/">using https://webaim.org/resources/contrastchecker/</a>														
55		3.2 Use appropriate font styles (i)	1			1															
56		3.3 Use appropriate font size (i)	1			1															
61	<b>Communication Strategy attributes</b>					5															
62	<b>Behaviour-change attributes</b>					10															
63	<b>Presentation attributes</b>					6															
65	<b>TOTAL</b>					21															
67	Overall quality of awareness-raising material																				
68	Low 0-14																				
69	Medium 15-23																				
70	High 24-30																				



	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U		
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>																	
3					Infographic - website <a href="https://www.medsphere.com/resources/protecting-against-phishing-attacks-infographic-poster/">https://www.medsphere.com/resources/protecting-against-phishing-attacks-infographic-poster/</a>																	
4																						
5	Audience		Marks		Marks		Comments															
6	1,1 Across groups		1																			
7	1,2 Specific		2		2		Silent (70+) Baby boomers															
8																						
9	Key message focus - clear purpose																					
10	2,1 Awareness - about threat		1				1															
11	2,2 Awareness - about impact		1																			
12	2,3 Cyber hygiene - best practices		1				1															
13	2,4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1				1															
14																						
15	Timeframe																					
16	3,1 Generic		1				1															
17	3,2 Covers specific time periods		2																			
18																						
19																						
20	<b>Behaviour-change attributes</b>																					
21																						
22	Promote situational awareness																					
23	1,1 Easy to understand what is the threat		1				1															
24	1,2 Easy to understand what is the impact		1																			
25																						
26	Empower people																					
27	2,1 Simple information to understand how to address the threat		1				1															
28	2,2 Appropriate call to action message		1																			
29	2,3 Overall conveys a positive message		1				Neutral															
30																						
31	Evidence-based content																					
32	3,1 Based on facts, e.g. statistics, etc.		1				1 statistics															
33	3,2 From credible source		1																			
34																						
35	Memorable																					
36	4,1 Micro-learning - specific topic		1				1															
37	4,2 Micro-learning - short statements, focus on key points		1																			
38	4,3 Considers different learning styles		1																			
39	4,4 Balance between graphics and text		1				1															
40	4,5 Audience can easily relate, e.g. storytelling		1																			
41																						
42	<b>Presentation attributes</b>																					
43																						
44	Visibility of the message																					
45	1,1 Appropriate location		1				1															
46	1,2 Draw attention to key information, e.g. by using contrasting colour		1				1															
47																						
48	Layout, style and formatting																					
49	2,1 Uses lines, borders and shapes to group related information		1				1															
50	2,2 Create text hierarchy (lights/different font styles)		1				1															
51	2,3 Maximum 4 colours		1				1															
52																						
53	Inclusive / Accessible																					
54	3,1 A good color contrast between the text color and background color		1				using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>															
55	3,2 Use appropriate font styles()		1				1															
56	3,3 Use appropriate font size()		1				1															
57																						
58																						
59																						
60																						
61	Communication Strategy attributes						6															
62	Behaviour-change attributes						5															
63	Presentation attributes						7															
64																						
65	TOTAL						18															
66																						
67	Overall quality of awareness-raising material																					
68	Low				0-14																	
69	Medium				15-22																	
70	High				23-28																	





A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
2	Communication Strategy attributes				Evaluation												
3						Infographic - website	<a href="https://www.eurojust.europa.eu/operations-services-and-innovations/public-awareness-and-prevention/guide/make-your-home-cyber-safe-stronghold">https://www.eurojust.europa.eu/operations-services-and-innovations/public-awareness-and-prevention/guide/make-your-home-cyber-safe-stronghold</a>										
5	1	Audience	Marka		Marka	Comments											
6		1.1	Across groups	1													
7		1.2	Specific	3													
9	2	Key message focus - clear purpose															
10		2.1	Awareness - about threat	1													
11		2.2	Awareness - about impact	1			How to protect from cyber attacks										
12		2.3	Cyber hygiene - best practices	1													
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			report the incident										
15	3	Timeframe															
16		3.1	Generic	1													
17		3.2	Covers specific time periods	3													
20	Behaviour-change attributes																
22	1	Promote situational awareness															
23		1.1	Easy to understand what is the threat	1													
24		1.2	Easy to understand what is the impact	1													
26	2	Empower people															
27		2.1	Simple information to understand how to address the threat	1													
28		2.2	Appropriate call to action message	1													
29		2.3	Overall conveys a positive message	1			Neutral										
31	3	Evidence-based content															
32		3.1	Based on facts, e.g. statistics, etc.	1													
33		3.2	From credible source	1			EUROPOL										
35	4	Memorable															
36		4.1	Micro-learning - specific topic	1													
37		4.2	Micro-learning - short statements, focus on key points	1													
38		4.3	Considers different learning styles	1			Visual/text										
39		4.4	Balance between graphics and text	1													
40		4.5	Audience can easily relate, e.g. storytelling	1			how to avoid the threat/real examples										
42	Presentation attributes																
44	1	Viability of the message															
45		1.1	Appropriate location	1													
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1													
48	2	Layout, style and formatting															
49		2.1	Use lines, borders and shapes to group related information	1													
50		2.2	Create text hierarchy (up to 3 different font styles)	1													
51		2.3	Use consistent colours	1													
53	3	Inclusive / Accessible															
54		3.1	A good color contrast between the text color and background color	1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>										
55		3.2	Use appropriate font styles()	1													
56		3.3	Use appropriate font size()	1													
61	Communication Strategy attributes					5											
62	Behaviour-change attributes					9											
63	Presentation attributes					8											
65	<b>TOTAL</b>					<b>22</b>											
67	Overall quality of awareness-raising material																
68	Low					0-14											
69	Medium					15-22											
70	High					23-28											



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
2	Communication Strategy attributes						Evaluation														
3							Infographic - website	<a href="https://ironcales.com/blog/ironcales-releases-findings-from-state-of-cybersecurity-survey/">https://ironcales.com/blog/ironcales-releases-findings-from-state-of-cybersecurity-survey/</a>													
4																					
5	1	Audience			Marks		Marks	Comments													
6		1.1	Across groups		1																
7		1.2	Specific		2		2	Business													
8																					
9	2	Key message focus - clear purpose																			
10		2.1	Awareness - about threat		1		1														
11		2.2	Awareness - about impact		1																
12		2.3	Cyber hygiene - best practices		1																
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1																
14																					
15	3	Timeframe																			
16		3.1	Generic		1		1														
17		3.2	Covers specific time periods		2																
18																					
19																					
20	Behaviour-change attributes																				
21																					
22	1	Promote situational awareness																			
23		1.1	Easy to understand what is the threat		1		1														
24		1.2	Easy to understand what is the impact		1																
25																					
26	2	Empower people																			
27		2.1	Simple information to understand how to address the threat		1		1														
28		2.2	Appropriate call to action message		1																
29		2.3	Overall conveys a positive message		1		Neutral														
30																					
31	3	Evidence-based content																			
32		3.1	Based on facts, e.g. statistics, etc.		1		1	Statistics													
33		3.2	From credible source		1																
34																					
35	4	Memorable																			
36		4.1	Micro-learning - specific topic		1		1														
37		4.2	Micro-learning - short statements, focus on key points		1																
38		4.3	Considers different learning styles		1		1	Visual/text													
39		4.4	Balance between graphics and text		1																
40		4.5	Audience can easily relate, e.g. storytelling		1																
41																					
42	Presentation attributes																				
43																					
44	1	Visibility of the message																			
45		1.1	Appropriate location		1		1														
46		1.2	Draw attention to key information, e.g. by using contrasting colour		1		1														
47																					
48	2	Layout, style and formatting																			
49		2.1	Uses lines, borders and shapes to group related information		1		1														
50		2.2	Create text hierarchy (up to 3 different font styles)		1		1														
51		2.3	Maximum 4 columns		1		1														
52																					
53	3	Inclusive / Accessible																			
54		3.1	Adequate color contrast between the text color and background color		1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
55		3.2	Use appropriate font style(s)		1		1														
56		3.3	Use appropriate font size (s)		1		1														
57																					
58																					
59																					
60																					
61																					
62																					
63																					
64																					
65																					
66																					
67																					
68																					
69																					
70																					
71																					



## THE STATE OF CYBERSECURITY: PHISHING ON THE RISE

In a digital-first world, cybercrime is to be expected. However, cybercriminals are taking advantage of the increased reliance on cloud-based technology and turning to more sophisticated tactics. This is especially true when it comes to phishing attacks against business email inboxes.

The IRONSCALES State of Cybersecurity Report surveyed IT managers and directors and found **81% have experienced an increase in email phishing attacks in the last 18 months** - since the start of the COVID-19 pandemic (March 2020).

### The Fear of Phishing is Real

Because of the steep increase in email phishing attacks, **90% of IT professionals** believe email phishing is the top cyber threat to their organizations.

**Most respondents (90%)** feel more confident in their organization's ability to respond to and remedy a phishing attack now than the year prior.

### The C-Suite Sees It

**64% of IT professionals** claim their senior leadership has placed **a lot more importance** on cybersecurity in the last year, while **37% say** that senior leadership has placed **more importance** on cybersecurity but not enough.

### Employees Are on "Mute"...

When it comes to cybersecurity compliance, increased phishing threats appear to stem from the need to remote work.

More than **eight out of 10 (84%)** agree that working from home made employees in their respective organizations more compliant to cybersecurity prevention.

Only **one percent** of respondents strongly disagreed with this statement.

### So Many Phishing Attacks. So Little Time.

**Slightly more than half (52%) of IT professionals** spend an equal amount of time dealing with phishing attacks as they do on other cybersecurity issues.

However, **37% of respondents** say remedying phishing attacks is the most resource-consuming task compared to other attacks and nearly **three in 10 (30%) IT professionals** spend about **all their time** addressing phishing attacks.

On average, here's how much time IT professionals and their teams spend remedying each individual phishing attack:

- 74% spend more than 30 minutes per attack**
- 16% spend more than two hours per attack**

	A	B	C	D	E	F	G	H	I	J
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
35										
36										
37										
38										
39										
40										
41										
42										
43										
44										
45										
46										
47										
48										
49										
50										
51										
52										
53										
54										
55										
56										
57										
58										
59										
60										
61										
62										
63										
64										
65										
66										
67										
68										
69										
70										
71										
72										
73										
74										
75										
76										
77										
78										
79										
80										
81										
82										
83										
84										
85										
86										
87										
88										
89										
90										
91										
92										
93										
94										
95										
96										
97										
98										
99										
100										

**RANSOMWARE IN THE TIME OF COVID-19**  
 COVID-19 has affected everyone and every business. Now the threat has changed and what you do is critical.

**RANSOMWARE IS NOT CHEAP**  
**\$4.62 million**  
 The average total cost of a ransomware attack is \$4.62 million. This includes the ransom payment, the cleanup, damage caused when operations are brought out of business.

**THE PROBLEM KEEPS GETTING WORSE**  
 Ransomware can cost 20% more globally in 2020 compared to 2019. In the US, ransomware cost and 2020 attacks are up 30% compared to 2019.

**COVID-19 ACCELERATED RANSOMWARE ATTACKS**  
 Cybercriminals are taking advantage of the chaos and uncertainty of the COVID-19 pandemic to launch ransomware attacks.

**ANXIETY IS A FACTOR**  
 Cybercriminals are taking advantage of the chaos and uncertainty of the COVID-19 pandemic to launch ransomware attacks.

**SPMs ARE NOT PROTECTING**  
 28% of ransomware attacks are attributed to SPMs.

**TOP CAUSES OF RANSOMWARE ATTACKS AT SPMs**  
 28% of ransomware attacks are attributed to SPMs.

**WHAT YOU CAN DO**  
 1. Audit security infrastructure  
 2. Reduce risk  
 3. Prepare for the worst

Contact us today at [info@hub.com](mailto:info@hub.com)

**HUB**  
 HUB Cyber Security  
 HUB Cyber Security

Communication Strategy attributes			Evaluation	
Infographic - website			<a href="https://www.nccsc.co.uk/Clscam/">https://www.nccsc.co.uk/Clscam/</a>	
	Mark	Comments		
1 Audience	1.1 Across groups	1	1	
	1.2 Specific	2		
2 Key message focus - clear purpose	2.1 Awareness - about threat	1	1	
	2.2 Awareness - about impact	1		
	2.3 Cyber hygiene - best practice	1		
	Empowerment - calls to action, e.g. visit website to learn more, to report an			
	2.4 Incident, etc.	2		
3 Tone/language	3.1 Generic	1	1	
	3.2 Covers specific time periods	2		
Behaviour-change attributes				
1 Promote behavioural awareness	1.1 Easy to understand what is the threat	1	1	
	1.2 Easy to understand what is the impact	2		
2 Empower people	Simple information to understand how to			
	2.1 Address the threat	1	1	
	2.2 Appropriate calls to action message	1		
	2.3 Overall convey a positive message	1	Neutral	
3 Evidence-based content	3.1 Based on facts, e.g. statistics, etc.	1		
	3.2 From credible source	1		
4 Memorable	4.1 Micro-learning - specific topic	1	1	
	Micro-learning - short messages, focus			
	4.2 on key points	1		
	4.3 Consider different learning styles	1	1	1. Misaligned
	4.4 Balance between graphics and text	1		
	Audience can easily relate, e.g.			
	4.5 Storytelling	1		
Presentation attributes				
1 Ability of the message	1.1 Appropriate location	1	1	
	Draw attention to key information, e.g.			
	1.2 by using contrasting colour	1	1	
2 Layout, style and formatting	Use lines, borders and shapes to group			
	2.1 related information	1	1	
	Overuse text hierarchy (size & offset)			
	2.2 font styles	1	1	
	2.3 Maximum 1 colour	1	1	
3 Inclusive / Accessible	A good color contrast between the text			
	3.1 color and background color	1	1	Using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>
	3.2 (Use appropriate font styles)	1	1	
	3.3 (Use appropriate font size)	1	1	
Communication Strategy attributes			0	
Behaviour-change attributes			5	
Presentation attributes			0	
<b>TOTAL</b>			<b>15</b>	
Overall quality of awareness-raising material				
Low	0-14			
Medium	15-22			
High	23-28			



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																				
2			<b>Communication Strategy attributes</b>				<b>Evaluation</b>													
3									https://www.businesstimes.com/asia/story/2022/07/08/ISACA-Survey-IT-Security-and-Risk-Experts-Share-Ransomware-Insights-in-the-Wake-of-the-Colonial-Pipeline-Attack											
4																				
5			1 Audience		Marks		Marks	Comments												
6			1.1 Across groups		1															
7			1.2 Specific		2		2 Issues													
8																				
9			2 Message focus - clear purpose																	
10			2.1 Awareness - about threat		1		1													
11			2.2 Awareness - about impact		1															
12			2.3 Cyber hygiene - best practices		1															
13			2.3.1 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1															
14																				
15			3 Timeframe																	
16			3.1 Generic		1		1													
17			3.2 Covers specific time periods		2															
18																				
19																				
20			<b>Behavior-change attributes</b>																	
21																				
22			1 Promote situational awareness																	
23			1.1 Easy to understand what is the threat		1		1													
24			1.2 Easy to understand what is the impact		1															
25																				
26			2 Empower people																	
27			2.1 Simple information to understand how to address the threat		1		1													
28			2.2 Appropriate call to action message		1															
29			2.3 Overall convey a positive message		1		Neutral													
30																				
31			3 Evidence-based content																	
32			3.1 Based on facts, e.g. statistics, etc.		1		1 statistics													
33			3.2 From credible source		1															
34																				
35			4 Memorable																	
36			4.1 Micro-learning - specific topics		1		1													
37			4.2 Micro-learning - short statements, focus on key points		1		1													
38			4.3 Considers different learning styles		1		1 Visual/text													
39			4.4 Balance between graphics and text		1		1													
40			4.5 Audience can easily relate, e.g. storytelling		1															
41																				
42			<b>Presentation attributes</b>																	
43																				
44			1 Visibility of the message																	
45			1.1 Appropriate location		1		1													
46			1.2 Draw attention to key information, e.g. by using contrasting colour		1		1													
47																				
48			2 Layout, style and formatting																	
49			2.1 Use lines, borders and shapes to group related information		1		1													
50			2.2 Create text hierarchy (up to 3 different font sizes)		1		1													
51			2.3 Maximum 7 colours		1		1													
52																				
53			3 Includes / Accessible																	
54			3.1 Adjust color contrast between the text color and background color		1		1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
55			3.2 Use appropriate font styles()		1		1													
56			3.3 Use appropriate font size()		1		1													
57																				
58																				
59																				
60																				
61			Communication Strategy attributes				4													
62			Behavior-change attributes				5													
63			Presentation attributes				6													
64																				
65			<b>TOTAL</b>				<b>15</b>													
66																				
67			Overall quality of awareness-raising material																	
68			Low 0-10																	
69			Medium 11-22																	
70			High 23-28																	
71																				

**ISACA**

**IT Experts Share Ransomware Insights Following the Colonial Pipeline Attack**

In a survey conducted by global IT association ISACA a week after the Colonial Pipeline attack, more than 1,200 IT risk, security and governance experts weighed in on ransomware attacks.

**21%** say their organizations have experienced ransomware attacks.

**1:3** Fewer than one-third (32%) say their organizations are highly prepared for a ransomware attack.

**67%** say their organizations will take new precautions in light of the Colonial Pipeline attack.

**78%** say critical infrastructure organizations should not pay ransom if attacked.

**1 in 5** say their organizations do not have contingencies in place if a vendor or supplier suffers a ransomware attack.

**84%** say ransomware attacks will become more prevalent in the second half of 2021.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															
41															
42															
43															
44															
45															
46															
47															
48															
49															
50															
51															
52															
53															
54															
55															
56															
57															
58															
59															
60															
61															
62															
63															
64															
65															
66															
67															
68															
69															
70															
71															
72															
73															

## PHISHING

You are targeted via email whereby you are encouraged to click through to fraudulent sites, give personal information about yourself or even send money. The scams vary widely but a majority of them are fairly easy to spot. What to look out for:

- Do you know the sender of the email? If not, do not open and do not click on any internal links. If you do, still be cautious.
- Are there any unrequested / unexpected attachments? If so, do not open before contacting the sender via another means to verify contents.
- Are there any grammatical errors or spelling mistakes? If so, be wary.
- Does the email ask for personal information? If so, ignore it.
- If you are associated with the business in question, are they addressing you by name?
- Check any and all links by hovering the cursor over it to see the URL. Will it take you to the expected website or a different one?

**NOTIFICATION**

/ESkillsMalta
 @eSkills\_Malta
 www.eskills.org.mt

A	B	C	D	E	F	G	H	I	J	K	L
1											
2	Communication Strategy attributes				Evaluation						
3					Infographic - website	<a href="https://www.inky.com/en/blog/infographic-49-2021-internet-crime-report">https://www.inky.com/en/blog/infographic-49-2021-internet-crime-report</a>					
4											
5	1	Audience	Markets		Markets	Comments					
6		1.1	Across groups	1							
7		1.2	Specific	2							
8											
9	2	Key message focus - clear purpose									
10		2.1	Awareness - about threat	1		1	statistics about cyber crime				
11		2.2	Awareness - about impact	1		1					
12		2.3	Cyber hygiene - best practices	1							
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1							
14											
15	3	Timeframe									
16		3.1	Generic	1		1					
17		3.2	Covers specific time periods	2							
18											
19											
20	Behavior-change attributes										
21											
22	1	Promote situational awareness									
23		1.1	Easy to understand what is the threat	1		1					
24		1.2	Easy to understand what is the impact	1		1					
25											
26	2	Empower people									
27		2.1	Simple information to understand how to address the threat	1		1					
28		2.2	Appropriate call to action message	1		1					
29		2.3	Overall conveys a positive message	1		Neutral					
30											
31	3	Evidence-based content									
32		3.1	Based on facts, e.g. statistics, etc.	1		1	statistics				
33		3.2	From credible source	1							
34											
35	4	Memorable									
36		4.1	Micro-learning - specific topic	1		1					
37		4.2	Micro-learning - short statements, focus on key points	1		1					
38		4.3	Considers different learning styles	1		1	Visual/text				
39		4.4	Balance between graphics and text	1							
40		4.5	Audience can easily relate, e.g. storytelling	1							
41											
42	Presentation attributes										
43											
44	1	Visibility of the message									
45		1.1	Appropriate location	1		1					
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1					
47											
48	2	Layout, style and formatting									
49		2.1	Use lines, borders and shapes to group related information	1		1					
50		2.2	Create text hierarchy (up to 3 different font styles)	1		1					
51		2.3	Maximum 4 colours	1		1					
52											
53	3	Inclusive / Accessible									
54		3.1	Against color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>				
55		3.2	Use appropriate font styles()	1		1					
56		3.3	Use appropriate font size ()	1		1					
57											
58											
59											
60											
61	Communication Strategy attributes					4					
62	Behavior-change attributes					5					
63	Presentation attributes					6					
64											
65			TOTAL			15					
66											
67	Overall quality of awareness raising material										
68	Low		0-14								
69	Medium		15-22								
70	High		23-28								
71											
72											
73											

## Cyber Crime By the Numbers

Statistics From the FBI's 2021 Internet Crime Report

**\$6.9 Billion**

Losses from cyberattacks totaled \$6.9 billion, representing an increase of more than 64% from the prior year.

**64%**

**#1**

Phishing has been the most commonly used cybercrime tactic for the past 3 years.

### Did you know?

38% of all reported cybercrimes involve phishing attacks.

Malware and virus incidents accounted for **\$5.6 Million** in losses. **\$7,000** was the average cost of a malware attack in 2021.

Over **\$151 Million** was lost due to corporate data breaches. The average cost of a corporate data breach was more than **\$118K**.

### Ransomware

**\$49.2 Million**

Annual adjusted losses due to ransomware attacks

**\$13,196**

Average ransomware payment

**450%**

Increase in the average cost of a ransomware attack in the last three years

**14 of the 16**

critical infrastructure sectors in the US experienced ransomware attacks

### Highest Cybercrime Loss By State

- California \$1.2 Billion
- Texas \$606 Million
- Illinois \$187 Million
- Michigan \$182 Million
- Washington \$158 Million
- Virginia \$173 Million
- New Jersey \$204 Million
- New York \$560 Million
- Pennsylvania \$207 Million
- Florida \$529 Million

### Tech Support Fraud

**\$348 million** stolen by cybercriminals using tech support fraud schemes

**543%** increase in losses due to tech support fraud in the past three years

**\$14,545** average price per incident

**More on Money Loss**

**Business Email Compromise (BEC) / Email Account Compromise (EAC) losses totaled nearly**

**\$2.4B**

**7X** Threats involving cryptocurrency increased seven times, accounting for losses of more than **\$1.6B**

Sp spoofing or impersonation cyber scams saw total losses of **\$82M**

Government impersonations saw an average cost of **\$12,584** per incident

**36,034** Total reported cybercrimes committed with the help of social media

Source: [https://www.ic3.gov/Hubs/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Hubs/PDF/AnnualReport/2021_IC3Report.pdf)

**INKY** Secure email. Change user behavior. [Learn more at inky.com](https://www.inky.com)



2)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
2	Communication Strategy attributes				Evaluation										
3					Infographic - website <a href="https://www.judge.com/resources/blog/cybersecurity-statistics-infographic-2022-dara/">https://www.judge.com/resources/blog/cybersecurity-statistics-infographic-2022-dara/</a>										
4	1	Audience	Markus		Markus		Comments								
5		1.1	Across groups	1											
6		1.2	Specific	2											
7															
8	2	Key message focus - clear purpose													
9		2.1	Awareness - about threat	1											
10		2.2	Awareness - about impact	1			cyber statistics								
11		2.3	Cyber hygiene - best practices	1											
12		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1											
13															
14	3	Timeframe													
15		3.1	Generic	1											
16		3.2	Covers specific time periods	2											
17															
18															
19															
20	Behaviour-change attributes														
21	1	Promote situational awareness													
22		1.1	Easy to understand what is the threat	1											
23		1.2	Easy to understand what is the impact	1											
24															
25	2	Empower people													
26		2.1	Simple information to understand how to address the threat	1											
27		2.2	Appropriate call to action message	1											
28		2.3	Overall conveys a positive message	1											
29							neutral								
30	3	Evidence-based content													
31		3.1	Based on facts, e.g. statistics, etc.	1											
32		3.2	From credible source	1											
33															
34															
35	4	Memorable													
36		4.1	Micro-learning - specific topic	1											
37		4.2	Micro-learning - short statements, focus on key points	1											
38		4.3	Considers different learning styles	1											
39		4.4	Balance between graphics and text	1											
40		4.5	Audience can easily relate, e.g. storytelling	1											
41															
42	Presentation attributes														
43	1	Viability of the message													
44		1.1	Appropriate location	1											
45		1.2	Draw attention to key information, e.g. by using contrasting colour	1											
46															
47	2	Layout, style and formatting													
48		2.1	Uses lines, borders and shapes to group related information	1											
49		2.2	Create text hierarchy (up to 3 different font styles)	1											
50		2.3	Maximum 4 colours	1											
51															
52	3	Inclusive / Accessible													
53		3.1	A good color contrast between the text color and background color	1											
54		3.2	Use appropriate font style (i)	1											
55		3.3	Use appropriate font size (i)	1											
56															
57															
58															
59															
60															
61															
62															
63		Communication Strategy attributes				3									
64		Behaviour-change attributes				5									
65		Presentation attributes				7									
66															
67															
68		Overall quality of awareness raising material													
69		Low				0-14									
70		Medium				15-22									
71		High				23-28									



3)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	Communication Strategy attributes				Evaluation											
3					Infographic - website	<a href="https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing">https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing</a>										
5	1	Audience	Marks		Marks	Comments										
6		1,1	Across groups	1												
7		1,2	Specific	2												
9	2	Key message focus - clear purpose														
10		2,1	Awareness - about threat	1		7 red flags of phishing threats										
11		2,2	Awareness - about impact	1												
12		2,3	Cyber hygiene - best practices	1												
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		visit a website to learn more										
15	3	Timeframe														
16		3,1	Generic	1												
17		3,2	Covers specific time periods	2												
20	Behaviour-change attributes															
22	1	Promote situational awareness														
23		1,1	Easy to understand what is the threat	1												
24		1,2	Easy to understand what is the impact	1												
26	2	Empower people														
27		2,1	Simple information to understand how to address the threat	1												
28		2,2	Appropriate call to action message	1												
29		2,3	Overall conveys a positive message	1		neutral										
31	3	Evidence-based content														
32		3,1	Based on facts, e.g. statistics, etc.	1												
33		3,2	From credible source	1		Get Cyber Safe										
35	4	Memorable														
36		4,1	Micro-learning - specific topic	1												
37		4,2	Micro-learning - short statements, focus on key points	1												
38		4,3	Considers different learning styles	1												
39		4,4	Balance between graphics and text	1												
40		4,5	Audience can easily relate, e.g. storytelling	1		real examples										
42	Presentation attributes															
45	1	Visibility of the message														
46		1,1	Appropriate location	1												
47		1,2	Draw attention to key information, e.g. by using contrasting colour	1												
48	2	Layout, style and formatting														
49		2,1	Uses lines, borders and shapes to group related information	1												
50		2,2	Create text hierarchy (up to 3 different font styles)	1												
51		2,3	Maximum of 4 colours	1												
53	3	Inclusive / Accessible														
54		3,1	A good color contrast between the text color and background color	1												
55		3,2	Use appropriate font styles (i)	1												
56		3,3	Use appropriate font size (i)	1												
61	Communication Strategy attributes				5											
62	Behaviour-change attributes				6											
63	Presentation attributes				6											
65	TOTAL				17											
67	Overall quality of awareness raising material															
68	Low				0-14											
69	Medium				15-22											
70	High				23-28											

3)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	Communication Strategy attributes				Evaluation											
3					Infographic - website	<a href="https://www.hackjourn.com/blog/infographic-make-or-break-phishing-metrics">https://www.hackjourn.com/blog/infographic-make-or-break-phishing-metrics</a>										
5	1	Audience	Marks		Marks	Comments										
6		1,1	Across groups	1												
7		1,2	Specific	2		2	Employees									
9	2	Key message focus - clear purpose														
10		2,1	Awareness - about threat	1			How to measure phishing metrics of organization									
11		2,2	Awareness - about impact	1												
12		2,3	Cyber hygiene - best practices	1												
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			report the incident									
15	3	Timeframe														
16		3,1	Generic	1												
17		3,2	Covers specific time periods	2												
20	Behaviour-change attributes															
22	1	Promote situational awareness														
23		1,1	Easy to understand what is the threat	1												
24		1,2	Easy to understand what is the impact	1												
25	2	Empower people														
27		2,1	Simple information to understand how to address the threat	1												
28		2,2	Appropriate call to action message	1												
29		2,3	Overall conveys a positive message	1			neutral									
31	3	Evidence-based content														
32		3,1	Based on facts, e.g. statistics, etc.	1			statistics									
33		3,2	From credible source	1												
35	4	Memorable														
36		4,1	Micro-learning - specific topic	1												
37		4,2	Micro-learning - short statements, focus on key points	1												
38		4,3	Considers different learning styles	1												
39		4,4	Balance between graphics and text	1												
40		4,5	Audience can easily relate, e.g. storytelling	1			tips to identify phishing emails									
42	Presentation attributes															
44	1	Visibility of the message														
45		1,1	Appropriate location	1												
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1												
48	2	Layout, style and formatting														
49		2,1	Uses lines, borders and shapes to group related information	1												
50		2,2	Create text hierarchy (up to 3 different font styles)	1												
51		2,3	Maximum 4 colours	1												
53	3	Inclusive / Accessible														
54		3,1	A good color contrast between the text color and background color	1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>									
55		3,2	Use appropriate font styles (i)	1												
56		3,3	Use appropriate font size (j)	1												
61	Communication Strategy attributes					G										
62	Behaviour-change attributes					B										
63	Presentation attributes					G										
64	TOTAL					20										
67	Overall quality of awareness raising material															
68	Low 0-14															
69	Medium 15-22															
70	High 23-28															



4)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>													
3						Infographic - website	<a href="https://consumer.ftc.gov/articles/dont-recognize-debt-infographic">https://consumer.ftc.gov/articles/dont-recognize-debt-infographic</a>											
4																		
5	1	Audience	Marks			Marks	Comments											
6		1.1	Across groups	1			Individuals											
7		1.2	Specific	2														
8																		
9	2	Key message focus - clear purpose																
10		2.1	Awareness - about threat	1			If you do not recognize that debt what to do											
11		2.2	Awareness - about impact	1														
12		2.3	Cyber hygiene - best practices	1														
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			report the incident											
14																		
15	3	Timeframe																
16		3.1	Generic	1														
17		3.2	Covers specific time periods	2														
18																		
19																		
20	<b>Behaviour-change attributes</b>																	
21																		
22	1	Promote situational awareness																
23		1.1	Easy to understand what is the threat	1														
24		1.2	Easy to understand what is the impact	1														
25																		
26	2	Empower people																
27		2.1	Simple information to understand how to address the threat	1														
28		2.2	Appropriate call to action message	1														
29		2.3	Overall conveys a positive message	1			neutral											
30																		
31	3	Evidence-based content																
32		3.1	Based on facts, e.g. statistics, etc.	1														
33		3.2	From credible source	1			Federal trade commission											
34																		
35	4	Memorable																
36		4.1	Micro-learning - specific topic	1														
37		4.2	Micro-learning - short statements, focus on key points	1														
38		4.3	Considers different learning styles	1														
39		4.4	Balance between graphics and text	1														
40		4.5	Audience can easily relate, e.g. storytelling	1			how to spot the scam											
41																		
42	<b>Presentation attributes</b>																	
43																		
44	1	Viability of the message																
45		1.1	Appropriate location	1														
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1														
47																		
48	2	Layout, style and formatting																
49		2.1	Uses lines, borders and shapes to group related information	1														
50		2.2	Create text hierarchy (up to 3 different font styles)	1														
51		2.3	Maximum 4 colours	1														
52																		
53	3	Inclusive / Accessible																
54		3.1	A good color contrast between the text color and background color	1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>											
55		3.2	Use appropriate font styles ()	1														
56		3.3	Use appropriate font size ()	1														
57																		
58																		
59																		
60																		
61						Communication Strategy attributes	5											
62						Behaviour-change attributes	8											
63						Presentation attributes	8											
64																		
65						<b>TOTAL</b>	<b>21</b>											
66																		
67						Overall quality of awareness raising material												
68						Low	0-14											
69						Medium	15-22											
70						High	23-28											

**Don't recognize that debt?**

Learn more about dealing with debt collectors at [ftc.gov/debtcollectors](https://ftc.gov/debtcollectors)

Report a scam? Report it to [ReportFraud.ftc.gov](https://ReportFraud.ftc.gov)

**FEDERAL TRADE COMMISSION**

Did you get a collection call about a debt you don't recognize? Before you pay:

- Find out who's calling.**
  - Get the name of the collector, the collection company, its address, and phone number.
- Did they refuse to give you this information? That's a red flag.**
  - Get "validation" information about the debt.
  - Within 5 days of first contacting you, debt collectors have to "validate" or tell you the amount of the debt, the name of the current creditor, and how to get the name of the original creditor.
- Did the collector refuse to tell you more about the debt? That's a red flag.**
- Don't respond to threats.**
  - When scammers threaten to arrest you, suspend your driver's license, or call your employer if you don't pay immediately, hang up and report the collector to the FTC at [ReportFraud.ftc.gov](https://ReportFraud.ftc.gov).
- Do your own detective work.**
  - Check with the original creditor to the debt you? Did they sell the debt or hire a company to collect it? If so, is it their collector?
- Dispute the debt.**
  - If you think you don't owe some - or all - of the debt, dispute it with the collector by mail or online. Even if you get validation information.

5)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
<b>Communication Strategy attributes</b>					<b>Evaluation</b>											
					Infographic - website		<a href="https://cyberducks.it/en/infographic/255-cyber-attacks-in-2022.html">https://cyberducks.it/en/infographic/255-cyber-attacks-in-2022.html</a>									
	1	Audience	Marka		Marka	Comments										
		1,1	Across groups	1												
		1,2	Specific	2		2	Millennials/Generation Z									
	2	Key message focus - clear purpose														
		2,1	Awareness - about threat	1		1	most common attacks									
		2,2	Awareness - about impact	1		1										
		2,3	Cyber hygiene - best practices	1												
		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1												
	3	Timeframe														
		3,1	Generic	1		1										
		3,2	Covers specific time periods	2												
<b>Behaviour-change attributes</b>																
	1	Promote situational awareness														
		1,1	Easy to understand what is the threat	1		1										
		1,2	Easy to understand what is the impact	1		1										
	2	Empower people														
		2,1	Simple information to understand how to address the threat	1		1										
		2,2	Appropriate call to action message	1												
		2,3	Overall conveys a positive message	1			neutral									
	3	Evidence-based content														
		3,1	Based on facts, e.g. statistics, etc.	1		1	statistics									
		3,2	From credible source	1												
	4	Memorable														
		4,1	Micro-learning - specific topic	1		1										
		4,2	Micro-learning - short statements, focus on key points	1												
		4,3	Considers different learning styles	1		1	visual/text									
		4,4	Balance between graphics and text	1		1										
		4,5	Audience can easily relate, e.g. storytelling	1												
<b>Presentation attributes</b>																
	1	Visibility of the message														
		1,1	Appropriate location	1		1										
		1,2	Draw attention to key information, e.g. by using contrasting colour	1		1										
	2	Layout, style and formatting														
		2,1	Uses lines, borders and shapes to group related information	1		1										
		2,2	Create text hierarchy (up to 3 different font styles)	1		1										
		2,3	Maximum 6 colours	1		1										
	3	Inclusive / Accessible														
		3,1	A good color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>									
		3,2	Use appropriate font styles ()	1		1										
		3,3	Use appropriate font size ()	1		1										
<b>Communication Strategy attributes</b>					5											
<b>Behaviour-change attributes</b>					7											
<b>Presentation attributes</b>					8											
<b>TOTAL</b>					20											
Overall quality of awareness raising material																
Low 0-14																
Medium 15-22																
High 23-28																

**CYBER ATTACKS IN 2022**

**Most common attack vectors**

- 19% Theft of credentials
- 16% Phishing
- 15% Cloud

**Average time to take action following a breach**

- 327 days: identify and contain a breach resulting from credential theft
- 295 days: detect and contain a breach resulting from phishing attacks
- 244 days: detect and contain a breach resulting from a misconfigured cloud

**4,35 million of dollars**: The average cost of breaches of data, up 2.6% compared to 2021

**4,82 million of dollars**: The average cost of data breaches in critical infrastructures

Source: <https://www.fortinet.com>

6)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2	Communication Strategy attributes				Evaluation																
3					Infographic - website	<a href="https://www.entia.europa.eu/typic/cybersecurity-educator/awareness-campaign/cyber-energy-website">https://www.entia.europa.eu/typic/cybersecurity-educator/awareness-campaign/cyber-energy-website</a>															
5	1	Audience	Marks		Marks	Comments															
6		1.1	Across groups	1																	
7		1.2	Specific	2		2 companies															
9	2	Key message focus - clear purpose																			
10		2.1	Awareness - about threat	1		1 how to stay safe from ransomware															
11		2.2	Awareness - about impact	1																	
12		2.3	Cyber hygiene - best practices	1																	
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1 report the incident															
15	3	Timeline																			
16		3.1	Generic	1																	
17		3.2	Covers specific time periods	2																	
20	Behaviour-change attributes																				
22	1	Promote situational awareness																			
23		1.1	Easy to understand what is the threat	1		1															
24		1.2	Easy to understand what is the impact	1																	
26	2	Empower people																			
27		2.1	Simple information to understand how to address the threat	1		1															
28		2.2	Appropriate call to action message	1		1															
29		2.3	Overall conveys a positive message	1		neutral															
31	3	Evidence-based content																			
32		3.1	Based on facts, e.g. statistics, etc.	1																	
33		3.2	From credible source	1		1 entia															
35	4	Memorable																			
36		4.1	Micro-learning - specific topic	1		1															
37		4.2	Micro-learning - short statements, focus on key points	1																	
38		4.3	Consider different learning styles	1		1 visual/text															
39		4.4	Balance between graphics and text	1																	
40		4.5	Audience can easily relate, e.g. storytelling	1																	
42	Presentation attributes																				
44	1	Viability of the message																			
45		1.1	Appropriate location	1		1															
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1		1															
48	2	Layout, style and formatting																			
49		2.1	Use lines, borders and shapes to group related information	1		1															
50		2.2	Create text hierarchy (up to 3 different font styles)	1		1															
51		2.3	Maximum of colours	1		1															
53	3	Inclusive / Accessible																			
54		3.1	A good color contrast between the text color and background color	1		1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>															
55		3.2	Use appropriate font style()	1		1															
56		3.3	Use appropriate font size()	1		1															
61	Communication Strategy attributes					6															
62	Behaviour-change attributes					7															
63	Presentation attributes					8															
65	TOTAL					21															
67	Overall quality of awareness-raising material																				
68	Low					0-14															
69	Medium					15-22															
70	High					23-28															

**Be the cybersecurity transmitter!**  
Stay safe from ransomware

Did you know that ransomware can affect our company both directly and indirectly? No matter if your organization can be directly targeted by an attack, but it can also be the lateral victim of an attack to a third-party provider, particularly a supply chain attack. Let's take a look at both cases...

**Your company could be under attack**  
Your company could be the direct victim of an attack aimed against your assets.

**A third party is under attack**  
Your company could be affected by an attack against a third party.

**How can this happen?**  
Your organization is breached through vulnerabilities in its supply chain, meaning ODS or other partnering companies.

The main entry vectors exploited are remote services and phishing.

The attack has affected a supplier, rendering its operations unusable, with direct repercussions on the services they provide to you. Or suppliers are used as stepping stones to spread the attack.

**So... may the entry points be cybersealed... How can you protect your company?**

- Reduce the attack surface
  - Apply Awareness Training Plans
  - Protect your perimeter: fire security software, maintain strict security awareness, security policies, and privacy protection policies up to date keeping personal data encrypted according to the GDPR
  - Restrict administrative privileges according to the PLOP (Principle of Least Privilege)
  - Stick to good practices (pay special attention to backup policies)
  - Have a continuity plan
- By building cyber secure relations with third parties:
  - Enforce security policies of third parties (requiring a minimum level of security requirements)
  - Apply Awareness Training Plans
  - Define obligations of suppliers regarding protection of assets, sharing of information, audit rights, business continuity
  - Include all obligations and requirements in contracts, e.g. GDPR
  - Restrict administrative privileges according to PLOP (Principle of least privilege)
  - Monitor service performance and perform routine security audits

**In case of suspicion always REPORT to the corresponding IT Department!**  
If you suffer a ransomware attack...

- Quarantine affected systems to contain the infection and stop the spread
- Lock down access to backup systems until after the infection gets removed
- Contact the national cybersecurity authorities or law enforcement on how to handle and deal with ransomware
- Visit the [No More Ransom Project](#), a European initiative that can decrypt variants of ransomware
- Do not pay the ransom and do not negotiate with the threat actors

entia #PowerYourCyber

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>												
3					Infographic - website	<a href="https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem">https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem</a>											
5	1	Audience	Markis		Markis	Comments											
6		1,1	Across groups	1													
7		1,2	Specific	2													
9	2	Key message focus - clear purpose															
10		2,1	Awareness - about threat	1		top cyber threats											
11		2,2	Awareness - about impact	1													
12		2,3	Cyber hygiene - best practices	1													
13			Empowerment - call to action, e.g. visit a website to learn more, to report an														
14		2,4	incident, etc.	1													
15	3	Timeframe															
16		3,1	Generic	1													
17		3,2	Covers specific time periods	2													
20	<b>Behaviour-change attributes</b>																
22	1	Promote situational awareness															
23		1,1	Easy to understand what is the threat	1													
24		1,2	Easy to understand what is the impact	1													
26	2	Empower people															
27		2,1	Simple information to understand how to address the threat	1													
28		2,2	Appropriate call to action message	1													
29		2,3	Overall conveys a positive message	1		Neutral											
31	3	Evidence-based content															
32		3,1	Based on facts, e.g. statistics, etc.	1		Statistics											
33		3,2	From credible source	1		enisa											
35	4	Memorable															
36		4,1	Micro-learning - specific topic	1													
37		4,2	Micro-learning - short statements, focus on key points	1													
38		4,3	Considers different learning styles	1													
39		4,4	Balance between graphics and text	1													
40		4,5	Audience can easily relate, e.g. storytelling	1		real examples											
42	<b>Presentation attributes</b>																
45	1	Visibility of the message															
46		1,1	Appropriate location	1													
47		1,2	Draw attention to key information, e.g. by using contrasting colour	1													
49	2	Layout, style and formatting															
50		2,1	Uses lines, borders and shapes to group related information	1													
51		2,2	Create text hierarchy (up to 3 different font styles)	1													
52		2,3	Maximum of colours	1													
53	3	Inclusive / Accessible															
54		3,1	A good color contrast between the text color and background color	1													
55		3,2	Use appropriate font styles (i)	1													
56		3,3	Use appropriate font size (i)	1													
61	<b>Communication Strategy attributes</b>					3											
62	<b>Behaviour-change attributes</b>					9											
63	<b>Presentation attributes</b>					8											
65	<b>TOTAL</b>					20											
67	Overall quality of awareness raising material																
68	Low					0-14											
69	Medium					15-22											
70	High					23-28											



8)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1																			
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>														
3								Infographic - website <a href="https://it.rutgers.edu/2022/11/22/cybersecurity-shopping-tips-for-the-holiday-season/">https://it.rutgers.edu/2022/11/22/cybersecurity-shopping-tips-for-the-holiday-season/</a>											
4																			
5	1	Audience		Marks		Marks		Comments											
6		1,1	Across groups	1				1											
7		1,2	Specific	2															
8																			
9	2	Key message focus - clear purpose																	
10		2,1	Awareness - about threat	1				1											
11		2,2	Awareness - about impact	1															
12		2,3	Cyber hygiene - best practices	1				1											
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1															
14																			
15	3	Timeline																	
16		3,1	Generic	1															
17		3,2	Covers specific time periods	2				2											
18																			
19																			
20	<b>Behaviour-change attributes</b>																		
21																			
22	1	Promote situational awareness																	
23		1,1	Easy to understand what is the threat	1				1											
24		1,2	Easy to understand what is the impact	1															
25																			
26	2	Empower people																	
27		2,1	Simple information to understand how to address the threat	1				1											
28		2,2	Appropriate call to action message	1				1											
29		2,3	Overall conveys a positive message	1															
30								Neutral											
31	3	Evidence-based content																	
32		3,1	Based on facts, e.g. statistics, etc.	1															
33		3,2	From credible source	1															
34																			
35	4	Memorable																	
36		4,1	Micro-learning - specific topic	1				1											
37		4,2	Micro-learning - short statements, focus on key points	1				1											
38		4,3	Considers different learning styles	1				1											
39		4,4	Balance between graphics and text	1				1											
40		4,5	Audience can easily relate, e.g. storytelling	1															
41																			
42	<b>Presentation attributes</b>																		
43																			
44	1	Visibility of the message																	
45		1,1	Appropriate location	1				1											
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1				1											
47																			
48	2	Layout, style and formatting																	
49		2,1	Uses lines, borders and shapes to group related information	1				1											
50		2,2	Create text hierarchy (up to 3 different font styles)	1				1											
51		2,3	Maximum 4 colours	1				1											
52																			
53	3	Inclusive / Accessible																	
54		3,1	A good color contrast between the text color and background color	1				1											
55		3,2	Use appropriate font styles ()	1				1											
56		3,3	Use appropriate font size ()	1				1											
57																			
58																			
59																			
60																			
61	<b>Communication Strategy attributes</b>							5											
62	<b>Behaviour-change attributes</b>							7											
63	<b>Presentation attributes</b>							8											
64																			
65								<b>TOTAL</b>											
66								20											
67	<b>Overall quality of awareness raising material</b>																		
68	Low							0-14											
69	Medium							15-22											
70	High							23-28											
71																			



9)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>									
3						Infographic - website <a href="https://www.hongkiat.com/blog/internet-scams-hotspots-infographic/">https://www.hongkiat.com/blog/internet-scams-hotspots-infographic/</a>									
4															
5	1	Audience		Marks			Marks								
6		1,1	Across groups	1			1								
7		1,2	Specific	2											
8															
9	2	Key message focus - clear purpose													
10		2,1	Awareness - about threat	1											
11		2,2	Awareness - about impact	1											
12		2,3	Cyber hygiene - best practices	1											
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1											
14															
15	3	Timeframe													
16		3,1	Generic	1											
17		3,2	Covers specific time periods	2											
18															
19															
20	<b>Behaviour-change attributes</b>														
21	1	Promote situational awareness													
22		1,1	Easy to understand what is the threat	1											
23		1,2	Easy to understand what is the impact	1											
24															
25															
26	2	Empower people													
27		2,1	Simple information to understand how to address the threat	1											
28		2,2	Appropriate call to action message	1											
29		2,3	Overall conveys a positive message	1											
30															
31	3	Evidence-based content													
32		3,1	Based on facts, e.g. statistics, etc.	1											
33		3,2	From credible source	1											
34															
35	4	Memorable													
36		4,1	Micro-learning - specific topic	1											
37		4,2	Micro-learning - short statements, focus on key points	1											
38		4,3	Considers different learning styles	1											
39		4,4	Balance between graphics and text	1											
40		4,5	Audience can easily relate, e.g. storytelling	1											
41															
42	<b>Presentation attributes</b>														
43															
44	1	Visibility of the message													
45		1,1	Appropriate location	1											
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1											
47															
48	2	Layout, style and formatting													
49		2,1	Uses lines, borders and shapes to group related information	1											
50		2,2	Create text hierarchy (up to 3 different font styles)	1											
51		2,3	Maximum 4 colours	1											
52															
53	3	Inclusive / Accessible													
54		3,1	A good color contrast between the text color and background color	1											
55		3,2	Use appropriate font styles ()	1											
56		3,3	Use appropriate font size ()	1											
57															
58															
59															
60															
61	<b>Communication Strategy attributes</b>					6									
62	<b>Behaviour-change attributes</b>					8									
63	<b>Presentation attributes</b>					7									
64															
65	<b>TOTAL</b>					<b>19</b>									
66															
67	Overall quality of awareness raising material														
68	Low 0-14														
69	Medium 15-22														
70	High 23-28														



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
<b>Communication Strategy attributes</b>					<b>Evaluation</b>																			
					Infographic - website		<a href="https://www.infosecinstitute.com/content-library/infographic-need-to-know-social-engineering/">https://www.infosecinstitute.com/content-library/infographic-need-to-know-social-engineering/</a>																	
<b>1 Audience</b>					Marks	Marks	Comments																	
1.1 Across groups					1																			
1.2 Specific					2		2	Milestones/Generation 2																
<b>2 Key message focus - clear purpose</b>																								
2.1 Awareness - about threat					1		1	social engineering																
2.2 Awareness - about impact					1		1																	
2.3 Cyber hygiene - best practices					1		1																	
2.4 Empowerment - call to actions, e.g. visit a website to learn more, to report an incident, etc.					1		1																	
<b>3 Timeframe</b>																								
3.1 Generic					1		1																	
3.2 Covers specific time periods					2																			
<b>Behaviour-change attributes</b>																								
<b>1 Promote situational awareness</b>																								
Easy to understand what is the threat					1		1																	
Easy to understand what is the impact					1		1																	
<b>2 Empower people</b>																								
Simple information to understand how to address the threat					1		1																	
Appropriate call to action message					1		1																	
Overall conveys a positive message					1																			
<b>3 Evidence-based content</b>																								
Based on facts, e.g. statistics, etc.					1																			
From credible source					1		1	Infosec																
<b>4 Memorable</b>																								
Micro-learning - specific topic					1		1																	
Micro-learning - short statements, focus on key points					1																			
Considers different learning styles					1		1	Visual examples																
Balance between graphics and text					1		1																	
Audience can easily relate, e.g. storytelling					1		1	Real examples																
<b>Presentation attributes</b>																								
<b>1 Visibility of the message</b>																								
Appropriate location					1		1																	
Draw attention to key information, e.g. by using contrasting colour					1		1																	
<b>2 Layout, style and formatting</b>																								
Use lines, borders and shapes to group related information					1		1																	
Create text hierarchy (up to 3 different font styles)					1		1																	
Maximum 6 colours					1																			
<b>3 Inclusive / Accessible</b>																								
A good color contrast between the text color and background color					1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>																
Use appropriate font styles ()					1		1																	
Use appropriate font size ()					1																			
<b>Communication Strategy attributes</b>						6																		
<b>Behaviour-change attributes</b>						9																		
<b>Presentation attributes</b>						5																		
<b>TOTAL</b>						20																		
<b>Overall quality of awareness raising material</b>																								
Low (0-14)																								
Medium (15-22)																								
High (23-28)																								



A	B	C	D	E	F	G	H	I	J	K	L	M	N
1													
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>								
3					Infographic - website <a href="https://veritau.co.uk/october-is-cybersecurity-awareness-month-2022/">https://veritau.co.uk/october-is-cybersecurity-awareness-month-2022/</a>								
5	1 Audience		Marks		Marks		Comments						
6	1.1 Across groups		1										
7	1.2 Specific		2		7		companies						
9	2 Key message focus - clear purpose												
10	2.1 Awareness - about threat		1		1		mandate fraud						
11	2.2 Awareness - about impact		1		1								
12	2.3 Cyber hygiene - best practices		1										
13	2.4 Empowerment - call to actions, e.g. visit a website to learn more, to report an incident, etc.		1		1		report the incident						
15	3 Tone/style												
16	3.1 Generic		1										
17	3.2 Covers specific time periods		2										
20	<b>Behaviour-change attributes</b>												
22	1 Promote situational awareness												
23	1.1 Easy to understand what is the threat		1		1								
24	1.2 Impact		1		1								
25	2 Empower people												
27	2.1 Single information to understand how to address the threat		1		1								
28	2.2 Appropriate calls to action message		1		1								
29	2.3 Overall convey a positive message		1		1		Neutral						
32	3 Evidence-based content												
33	3.1 Based on facts, e.g. statistics, etc.		1		1								
34	3.2 From credible source		1		1								
35	4 Memorable												
36	4.1 Micro-learning - specific topic		1		1								
37	4.2 Micro-learning - short statements, focus on key points		1		1								
38	4.3 Considers different learning styles		1		1		Visual examples						
39	4.4 Balance between graphics and text		1		1								
40	4.5 Audience can easily relate, e.g. easy to follow		1		1		Real examples						
42	<b>Presentation attributes</b>												
44	1 Visibility of the message												
45	1.1 Appropriate location		1		1								
46	1.2 e.g. by using contrasting colour		1		1								
48	2 Layout, style and formatting												
49	2.1 Use lines, borders and shapes to group related information		1		1								
50	2.2 Create text hierarchy (up to 3 different font styles)		1		1								
51	2.3 Maximum 4 colours		1		1								
53	3 Inclusive / Accessible												
54	3.1 Agreed color contrast between the text color and background color		1		1		Using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>						
55	3.2 Use appropriate font styles()		1		1								
56	3.3 Use appropriate font size()		1		1								
61	<b>Communication Strategy attributes</b>				6								
62	<b>Behaviour-change attributes</b>				7								
63	<b>Presentation attributes</b>				8								
64					21								
65	<b>TOTAL</b>				21								
67	Overall quality of awareness-raising material												
68	Low		0-11										
69	Medium		12-22										
70	High		23-28										

CYBERSECURITY AWARENESS MONTH

## MANDATE FRAUD

Mandate fraud - also known as payment diversion fraud - is where a cybercriminal poses as a creditor or supplier. It's a growing risk, and sometimes happens when an account has been hacked due to poor password security.

### How mandate fraud works

**Subject:** Urgent bank detail change

**From:** james@boxconstruction.uk

Hi,

Please be advised we have new bank details:  
Sort code: 20-96-13 and Account no: 46341783

Can you change this as soon as possible.

Thanks,  
James  
Box Construction Ltd

*The supplier's real address is james@box-construction.co.uk. This email is from a fake account.*

*The bank details are changed on the creditors system.*

*The next invoice is paid to the fraudsters' account rather than the real suppliers.*

**“ Public sector organisations are particularly at risk due to the high volume of transactions ”**

Luton Council recently suffered a mandate fraud attack, in which organised criminals stole £1.1million intended for a school fund.

### Helping to prevent mandate fraud

Always... Follow agreed verification processes Keep your passwords secure

Look out for... Sense of urgency or pressure Odd tone, grammar and spelling

For more info, speak to your IT team, or visit [veritau.co.uk](https://veritau.co.uk)

12)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
2	<b>Communication Strategy attributes</b>			<b>Evaluation</b>																			
3				[Infographic - website]		<a href="http://services.nwu.ac.za/it-security/phishing-emails-2022-learn-how-spott-deceptive-requests-online-and-take-recommended-steps">http://services.nwu.ac.za/it-security/phishing-emails-2022-learn-how-spott-deceptive-requests-online-and-take-recommended-steps</a>																	
4																							
5	1	Audience	Marks	Marks		Comments																	
6		1.1 Across groups	1																				
7		1.2 Specific	2																				
8																							
9	2	Key message focus- clear purpose																					
10		2.1 Awareness - about threat	1			phishing attempts																	
11		2.2 Awareness - about impact	1																				
12		2.3 Cyber hygiene - best practices	1																				
13		Engagement - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1 visit a website to learn																	
14																							
15	3	Timeframe																					
16		3.1 Generic	1																				
17		3.2 Covers specific time periods	2																				
18																							
19																							
20	<b>Behaviour-change attributes</b>																						
21																							
22	1	Promote situational awareness																					
23		1.1 the threat	1																				
24		1.2 the impact	1																				
25																							
26	2	Empower people																					
27		2.1 the threat	1																				
28		2.2 Appropriate call to action message	1																				
29		2.3 Overall conveys a positive message	1			Neutral																	
30																							
31	3	Evidence-based content																					
32		3.1 statistics, etc.	1																				
33		3.2 From credible source	1																				
34																							
35	4	Memorable																					
36		4.1 topic	1																				
37		4.2 points	1																				
38		4.3 style	1			1 visual examples																	
39		4.4 and text	1																				
40		4.5 e.g. storytelling	1			1 real examples																	
41																							
42	<b>Presentation attributes</b>																						
43																							
44	1	Usability of the message																					
45		1.1 Appropriate location	1																				
46		1.2 contrasting colour	1																				
47																							
48	2	Layout, style and formatting																					
49		2.1 information	1																				
50		2.2 different font styles	1																				
51		2.3 Maximum 4 columns	1																				
52																							
53	3	Inclusive / Accessible																					
54		3.1 background color	1			1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>																	
55		3.2 Use appropriate font styles()	1																				
56		3.3 Use appropriate font size()	1																				
57																							
58																							
59																							
60																							
61	Communication Strategy attributes			5																			
62	Behaviour-change attributes			7																			
63	Presentation attributes			7																			
64																							
65	<b>TOTAL</b>			<b>19</b>																			
66																							
67	Overall quality of awareness-raising material																						
68	Low 0-5																						
69	Medium 6-22																						
70	High 23-28																						



### User Guide: IT Services Phishing Attempts

Learn how to protect yourself from phishing attempts that can include dangerous links and attachments.

**1. VERIFY THE SOURCE**  
Attackers are always coming up with new and inventive ways to trick you into downloading malicious files like ransomware or giving up your password on phishing sites. Sometimes these attempts are obvious, but they are often hard to spot.

**2. ATTACHMENTS: ALWAYS CHECK FOR LEGITIMACY FIRST**  
Suspicious phishing emails rely on you—they want you to click a link or open an attachment. But before you do anything, you always need to check an email's content for legitimacy. Hover over a link and see if it's going to a reliable URL. Or, if you're unsure about an email's content or the source it came from, do a quick Google search and look for other instances of this campaign and what those instances could tell you about the email's legitimacy.

**3. IS THE SITE SECURE?**  
Another way to help verify that a website is legitimate is by looking for a padlock icon in your browser's address bar, which indicates that your connection is secured using HTTPS. Note that HTTPS alone does not make a website secure—criminals can use encryption, too—but a website without HTTPS is a red flag, especially if it's supposed to be a banking site.

**4. SWITCH PLATFORMS**  
If you receive a suspicious message from someone you know, including a note asking you to respond to an emergency immediately, double-check to make sure it's genuine. You can do that by contacting the apparent sender through another channel since an attacker is far less likely to access multiple accounts. If it's a company, check with it directly to see if the message or site you've been sent is legitimate.

**5. REPORT SUSPICIOUS EMAILS**  
Please log a ticket using our online support portal: <https://support.nwu.ac.za>.  
"Something is not working" in "Cybersecurity Issues" > "Phishing Attempts Issue"

**6. WHY IS THIS IMPORTANT**  
Attackers are always trying new and inventive ways to trick you into downloading malicious files like ransomware or giving up your password on phishing sites. Sometimes these attempts are obvious, but they are often hard to spot.

### More on Cyber security info You may use this link

<http://services.nwu.ac.za/information-technology/cyber-security/news>

- Many fake websites are very carefully designed to look legitimate, and phishing emails can appear to come from someone you know.
- In one example of phishing, customers send emails designed to look like the IRS and share. The emails ask for detailed personal information, passwords, files, and other information to look like someone who discloses their personal and financial data. The customer then use that information to steal customer identities and financial assets.
- Other common scams include scam artists creating online identities to trick people who have romantic relationships and then hitting the internet up for money. Identify them using an on internet friend, and avoid for what for a direct bank transfer.
- Scammers ask to deposit money in people's bank accounts in exchange for a money order—but they then spend the money and don't deposit money for receive a receipt. These phishing attempts can usually be prevented by people aware of these and know what to look for.

13)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
2	Communication Strategy attributes			Evaluation															
3				Infographic - website															
4				<a href="https://www.europa.europa.eu/publications-events/publications/crypto-investment-scams-infographic">https://www.europa.europa.eu/publications-events/publications/crypto-investment-scams-infographic</a>															
5	1	Audience	Marks	Marks	Comments														
6		1.1 Across groups	1																
7		1.2 Specific	2																
8																			
9	2	Key message focus - clear purpose																	
10		2.1 Awareness - about threat	1																
11		2.2 Awareness - about impact	1			crypto investment scams													
12		2.3 Cyber hygiene - best practices	1																
13		2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																
14																			
15	3	Timeframe																	
16		3.1 Generic	1																
17		3.2 Covers specific time periods	2																
18																			
19																			
20	Behaviour-change attributes																		
21																			
22	1	Promote situational awareness																	
23		1.1 Easy to understand what is the threat	1																
24		1.2 Easy to understand what is the impact	1																
25																			
26	2	Empower people																	
27		2.1 Simple information to understand how to address the threat	1																
28		2.2 Appropriate call to action message	1																
29		2.3 Overall convey a positive message	1			Neutral													
30																			
31	3	Evidence-based content																	
32		3.1 Based on facts, e.g. statistics, etc.	1																
33		3.2 From credible source	1			europa													
34																			
35	4	Memorable																	
36		4.1 Micro-learning - specific topic	1																
37		4.2 Micro-learning - short statements, focus on key points	1																
38		4.3 Consider different learning styles	1																
39		4.4 Balance between graphics and text	1																
40		4.5 Audience can easily relate, e.g. storytelling	1			Real examples													
41																			
42	Presentation attributes																		
43																			
44	1	Visibility of the message																	
45		1.1 Appropriate location	1																
46		1.2 Draw attention to key information, e.g. by using contrasting colour	1																
47																			
48	2	Layout, style and formatting																	
49		2.1 Uses lines, borders and shapes to group related information	1																
50		2.2 Create text hierarchy (up to 3 different font styles)	1																
51		2.3 Maximum 4 colours	1																
52																			
53	3	Inclusive / Accessible																	
54		3.1 A good color contrast between the text color and background color	1			using <a href="https://webaim.org/visualc/contrastchecker/">https://webaim.org/visualc/contrastchecker/</a>													
55		3.2 Use appropriate font styles (i)	1																
56		3.3 Use appropriate font size (i)	1																
57																			
58																			
59																			
60																			
61	Communication Strategy attributes			6															
62	Behaviour-change attributes			7															
63	Presentation attributes			8															
64																			
65	TOTAL			19															
66																			
67	Overall quality of awareness-raising material																		
68	Low			0-14															
69	Medium			15-22															
70	High			23-30															

**Crypto investment scams - how do they work?**

**THE ROMANCE FRAUDSTER**  
A fraudster approaches you on a dating app or social media platform. It can start as a romance scam, quickly turning into an investment fraud with potentially serious financial losses for you.

**THE FRIEND IMPERSONATOR**  
A fraudster targets you by compromising your friends' social media accounts. Because you believe you are communicating with a trusted person, you can be more open to make the investment.

**THE BUSINESS OPPORTUNITY**  
A fraudster calls and shows you a fraudulent crypto investment website. They convince you to invest based on a fake potential growth. In many cases, you will only realise the money cannot be withdrawn after a long period of investment time.

**THE PHISHING ADS**  
You come across a crypto investment advertisement on social media. You click on it and provide your contact information. The fraudster contacts you by phone and convinces you to invest.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
2	<b>Communication Strategy attributes</b>			<b>Evaluation</b>																	
3						Infographic - website	<a href="https://www.aba.com/news-research/articles/guide/how-to-safely-use-mobile-payment-apps-and-services">https://www.aba.com/news-research/articles/guide/how-to-safely-use-mobile-payment-apps-and-services</a>														
5	1	Audience	Marks			Marks	Comments														
6		1.1	Cross/age	1																	
7		1.2	Specific	2			Individuals (Millennials/Generation Z)														
9	2	Key message focus - clear purpose																			
10		2.1	Awareness - about threat	1																	
11		2.2	Awareness - about impact	1																	
12		2.3	Cyber hygiene - best practices	1																	
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1				1													
15	3	Timeframe																			
16		3.1	Generic	1																	
17		3.2	Covers specific time periods	2																	
20	<b>Behaviour-change attributes</b>																				
22	1	Promote situational awareness																			
23		1.1	Easy to understand what is the threat	1																	
24		1.2	Easy to understand what is the impact	1																	
26	2	Empower people																			
27		2.1	Simple information to understand how to address the threat	1																	
28		2.2	Appropriate call to action message	1																	
29		2.3	Overall conveys a positive message	1				Neutral													
31	3	Evidence-based content																			
32		3.1	Based on facts, e.g. statistics, etc.	1																	
33		3.2	From credible source	1																	
35	4	Memorable																			
36		4.1	Micro-learning - specific topic	1																	
37		4.2	Micro-learning - short statements, focus on key points	1																	
38		4.3	Considers different learning styles	1																	
39		4.4	Balance between graphics and text	1																	
40		4.5	Audience can easily relate, e.g. storytelling	1																	
42	<b>Presentation attributes</b>																				
45	1	Visibility of the message																			
46		1.1	Appropriate location	1																	
47		1.2	Draw attention to key information, e.g. by using contrasting colour	1																	
48	2	Layout, style and formatting																			
49		2.1	Uses lines, borders and shapes to group related information	1																	
50		2.2	Create text hierarchy (up to 3 different font styles)	1																	
51		2.3	Maximum 4 colours	1																	
53	3	Inclusive / Accessible																			
54		3.1	A good color contrast between the text color and background color	1																	
55		3.2	Use appropriate font styles ()	1																	
56		3.3	Use appropriate font size ()	1																	
61	<b>Communication Strategy attributes</b>			6																	
62	<b>Behaviour-change attributes</b>			7																	
63	<b>Presentation attributes</b>			8																	
64	<b>TOTAL</b>			<b>21</b>																	
67	Overall quality of awareness raising material																				
68	Low			0-10																	
69	Medium			15-22																	
70	High			23-28																	

### How to Safely Use Mobile Payment Apps and Services

Online payment systems or apps like Zelle, Venmo, and CashApp let you quickly send and receive money. If you link the service to your bank account or debit card, it's almost like handing someone cash. Be sure you know who you're sending money to. Once you send money, it's nearly impossible to get it back.

**AVOID SENDING MONEY TO A SCAMMER**

Don't click on links in an unexpected email, text message, or direct message that asks you to send money. Don't give any personal or sensitive information like your username, PIN, or password.

Confirm that you know the person you're sending money to.

When sending to someone you know, double-check their information before you hit send.

**PROTECT YOUR ACCOUNTS**

Use multi-factor authentication. This means you need two or more credentials to get into your account: your password plus something else like an authentication code or fingerprint.

Never share your credentials, like a verification code you get via text or authentication app.

Set up alerts in the payment app to get transaction notifications outside of the app environment, such as via email or text.

Regularly check your payment app and bank accounts to make sure no unauthorized payments have been sent from or accepted by your account.

**Paid a Scammer Through a Payment App?**

- Report it to the payment app or service and ask to reverse the transfer.
- Tell your financial institution.
- Report it to the Federal Trade Commission at ReportFraud.ftc.gov.

Learn more at [ftc.gov/paymentapps](https://ftc.gov/paymentapps) and [aba.com/consumers](https://aba.com/consumers)





A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
2	Communication Strategy attributes			Evaluation																		
3				Infographic - website		<a href="https://cyberducks.it/en/infographics/2021-cybersecurity-trends-2022.html">https://cyberducks.it/en/infographics/2021-cybersecurity-trends-2022.html</a>																
4				Marks																		
5	1	Audience		Marks	Comments																	
6		1,1	Across groups	1																		
7		1,2	Specific	2	Millennials/Generation Z																	
8																						
9	2	Key message focus - clear purpose																				
10		2,1	Awareness - about threat	1																		
11		2,2	Awareness - about impact	1																		
12		2,3	Cyber hygiene - best practices	1																		
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																		
14																						
15	3	Timeframe																				
16		3,1	Generic	1																		
17		3,2	Covers specific time periods	2																		
18																						
19	Behaviour-change attributes																					
20																						
21	1	Promote situational awareness																				
22		1,1	Easy to understand what is the threat	1																		
23		1,2	Easy to understand what is the impact	1																		
24		2,1	Empower people	1																		
25		2,2	Simple information to understand how to address the threat	1																		
26		2,3	Appropriate call to action message	1																		
27		2,3	Overall conveys a positive message	1	Neutral																	
28	3	Evidence-based content																				
29		3,1	Based on facts, e.g. statistics, etc.	1	statistics																	
30		3,2	From credible source	1																		
31																						
32	4	Memorable																				
33		4,1	Micro-learning - specific topic	1																		
34		4,2	Micro-learning - short statements, focus on key points	1																		
35		4,3	Considers different learning styles	1	Visual/text																	
36		4,4	Balance between graphics and text	1																		
37		4,5	Audience can easily relate, e.g. storytelling	1																		
38																						
39	Presentation attributes																					
40																						
41	1	Visibility of the message																				
42		1,1	Appropriate location	1																		
43		1,2	Draw attention to key information, e.g. by using contrasting colour	1																		
44																						
45	2	Layout, style and formatting																				
46		2,1	Uses lines, borders and shapes to group related information	1																		
47		2,2	Create text hierarchy (up to 3 different font styles)	1																		
48		2,3	Maximum 6 colours	1																		
49																						
50	3	Inclusive / Accessible																				
51		3,1	A good color contrast between the text color and background color	1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>																	
52		3,2	Use appropriate font styles()	1																		
53		3,3	Use appropriate font size()	1																		
54																						
55																						
56																						
57																						
58																						
59																						
60																						
61	Communication Strategy attributes			6																		
62	Behaviour-change attributes			6																		
63	Presentation attributes			8																		
64																						
65	TOTAL			20																		
66																						
67	Overall quality of awareness raising material																					
68	Low			0-14																		
69	Medium			15-22																		
70	High			23-28																		
71																						

**CYBER DUCKS**

## Cybersecurity Trends 2022

**RANSOMWARE**  
This threat remains the most feared this year too, with an increase in ransomware for Linux environments and dormant ransomware, which remain silent for a certain period of time before encrypting data.  
The ransomware will cost its victims more than \$ 265 billion (USD) per year by 2031.

**FREQUENCY OF RANSOMWARE ATTACKS**

40s (2016) vs 11s (2021)

**CRYPTOJACKING**  
The cost of cryptocurrency crimes will reach \$ 30 billion in 2025.

**LACK OF PROFESSIONALS**  
It is estimated that around 80% of the professionals needed to ensure adequate protection of IT infrastructures are lacking.

**SPAM**  
SPAM campaigns are expected to grow thanks to the amount of stolen credentials, and will be increasingly targeted and credible precisely because of the data obtained during the violations.  
The cost of breaches is growing, and last year reached a 10-year high of \$ 4.24 million year-on-year.

[www.cyberducks.it](http://www.cyberducks.it)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
2	Communication Strategy attributes				3	Evaluation																								
3					4	Infographic - website				<a href="https://www.slicktext.com/blog/2022/01/spam-text-statistics-for-2022/">https://www.slicktext.com/blog/2022/01/spam-text-statistics-for-2022/</a>																				
5	1 Audience		Marka	1	Marka		Comments																							
6	1.1 Across groups			1			1																							
7	1.2 Specific			2																										
9	2 Key message focus - clear purpose																													
10	2.1 Awareness - about threat			1			1		Spam texting																					
11	2.2 Awareness - about impact			1																										
12	2.3 Cyber hygiene - best practices			1																										
13	2.4 Engagement - calls to action, e.g. visit a website to learn more, to report an incident, etc.			1																										
15	3 Timeframe																													
16	3.1 Generic			1			1																							
17	3.2 Covers specific time periods			2																										
20	Behavior-change attributes																													
22	1 Promote situational awareness																													
23	1.1 Easy to understand what the threat					1			1																					
24	1.2 Easy to understand what the impact					1																								
26	2 Empower people																													
27	2.1 Simple information to understand how to address the threat					1			1																					
28	2.2 Appropriate call to action message					1																								
29	2.3 Overall conveys a positive message					1			Neutral																					
31	3 Evidence-based content																													
32	3.1 Based on facts, e.g. statistics, etc.					1			1		statistics																			
33	3.2 From credible source					1																								
35	4 Memorable																													
36	4.1 Micro-learning - specific topic					1			1																					
37	4.2 Micro-learning - short statements, focus on key points					1			1																					
38	4.3 Considers different learning styles					1			1		Visual/text																			
39	4.4 Balance between graphics and text					1			1																					
40	4.5 Audience can easily relate, e.g. storytelling					1			1		How to avoid the threat/real examples																			
42	Presentation attributes																													
45	1 Ability of the message																													
46	1.1 Appropriate location					1			1																					
47	1.2 Draw attention to key information, e.g. by using contrasting colour					1			1																					
48	2 Layout, style and formatting																													
49	2.1 Use lines, borders and shapes to group related information					1			1																					
50	2.2 Create text hierarchy (upto 2.2.3 different font styles)					1			1																					
51	2.3 Maximum 4 colours					1			1																					
53	3 Include / Accessible																													
54	3.1 Agood color contrast between the text color and background color					1			1		<a href="https://webaim.org/resources/contrastchecker/">using https://webaim.org/resources/contrastchecker/</a>																			
55	3.2 Use appropriate font styles()					1			1																					
56	3.3 Use appropriate font size()					1			1																					
61	Communication Strategy attributes					3																								
62	Behavior-change attributes					8																								
63	Presentation attributes					8																								
65	TOTAL					19																								
67	Overall quality of awareness raising material																													
68	Low					0-14																								
69	Medium					15-27																								
70	High					28-28																								

### The Rise of Spam Texting in 2021 & 2022

It's not just you — most Americans have seen a dramatic uptick in spam texting. While there's no one reason for this increase, the COVID-19 pandemic and adapting to a more remote lifestyle has been a significant factor.

**2022**

**↑ 58%**

From 2020 to 2021, there was a **58% increase in spam texts sent**.

**10B**

In September of 2021, the number of spam texts sent was **1.227 million**. By comparison, in August of 2022, **10.89 billion** spam texts were sent.

**2021**

In April of 2021, Americans received around **16.9 spam texts a month**. In April of 2022, that number skyrocketed to **41 spam texts a month**.

**1/3**

In fact, as of 2021, **1 in 3 Americans** had reported falling for a mobile phone scam.

**35%**

Less than **35% of people** realize that they're a target of a **spam texting attack**.

**6B**

It's impossible to get a break from spam texts. In fact, in 2021, January and February were the only months with fewer than **6 billion** spam messages sent.

**87B**

Spam calls decreased by **50%** from April to June of 2020, as the COVID-19 pandemic changed the way society operated.

**87B**

Spam text frequency surpassed spam call frequency for the first time in 2020, with the gap continuing to widen in 2021 and 2022 (**87,850,585,036** spam texts sent vs. **72,236,675,541** spam calls placed).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ
2	Communication Strategy attributes		Evaluation		Info graphic - website		https://www.digitaleconomy.gov.au/2022/02/fraud-related-issues.html																																												
5	1 Audience		Markets	Markets	Comments																																														
6	1.1 Anonymous																																																		
7	1.2 Specific																																																		
9	2 Key message from - clear purpose																																																		
10	2.1 Awareness - about threat																																																		
11	2.2 Awareness - about impact																																																		
12	2.3 Practices																																																		
13	2.4 Empowerment - calls to action, e.g. visit website to learn more, to report an incident, etc.																																																		
15	3 Timeliness																																																		
16	3.1 Current																																																		
17	3.2 Covers specific time periods																																																		
20	Behaviour Change attributes																																																		
22	1 Promote situational awareness																																																		
23	1.1 To understand what's																																																		
24	1.2 To understand what's																																																		
26	2 Empower people																																																		
27	2.1 Simple information																																																		
28	2.2 Appropriate calls to action																																																		
29	2.3 Overall, can you provide																																																		
31	3 Evidence-based content																																																		
32	3.1 Based on facts, e.g.																																																		
33	3.2 From credible sources																																																		
35	4 Memorable																																																		
36	4.1 Micro-learning - specific																																																		
37	4.2 Micro-learning - short																																																		
38	4.3 Consistent with learning																																																		
39	4.4 Balance between graphics																																																		
40	4.5 Address can easily relate																																																		
42	Presentation attributes																																																		
43	1 Visibility of the message																																																		
44	1.1 Appropriate location																																																		
45	1.2 Draw attention to key information, e.g. by using																																																		
46	1.3 Contrasting colour																																																		
48	2 Layout, style and formatting																																																		
49	2.1 Usability, readability and																																																		
50	2.2 Choice and hierarchy (upto																																																		
51	2.3 Maximum 7 columns																																																		
53	3 Font style / readability																																																		
54	3.1 Agree on color contrast																																																		
55	3.2 Use appropriate font style																																																		
56	3.3 Use appropriate font size																																																		
61	Communication Strategy attributes																																																		
62	Behaviour Change attributes																																																		
63	Presentation attributes																																																		
64	TOTAL																																																		
67	Overall quality of awareness-raising material																																																		
68	Low																																																		
69	Medium																																																		
70	High																																																		

## A Scammy Snapshot of 2022

(based on reports to Consumer Sentinel)

#FTCTopFrauds  
ftc.gov/data  
ReportFraud.ftc.gov

### Top Frauds

- 1 Imposters
- 2 Online shopping
- 3 Prizes, sweepstakes, lotteries
- 4 Investments
- 5 Business and job opportunities

Scammers contacting people on social or by phone led to big losses

**\$1.2 billion** total lost

Social media: Highest overall reported losses

**REPORT** 2.4 million fraud reports

**\$8.8 billion** reported lost

The number of reports is down.  
The amount lost is up.  
(2021: 2.9 million fraud reports, \$6.1 billion lost)

Losses to investment scams more than doubled.

**\$1.8 billion** (2021) vs **\$3.8 billion** (2022)

**\$1,400** median loss

Phone calls: Highest per person reported losses

Losses to business imposters soared.

**\$196 million** (2020) vs **\$453 million** (2021) vs **\$660 million** (2022)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
2	Communication Strategy attributes				Evaluation																			
3					Infographic - website			https://www.vcpi.com/how-to-protect-yourself-from-malicious-email-threats/																
4																								
5	1	Audience	Marks		Marks	Comments																		
6		1.1	Across groups	1																				
7		1.2	Specific	2																				
8																								
9	2	Key message focus - clear purpose																						
10		2.1	Awareness - about threat	1																				
11		2.2	Awareness - about impact	1				how to protect your assets from malicious email threats																
12		2.3	Cyber hygiene - best practices	1																				
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																				
14																								
15	3	Timeframe																						
16		3.1	Generic	1																				
17		3.2	Covers specific time periods	2																				
18																								
19																								
20	Behaviour-change attributes																							
21																								
22	1	Promote emotional awareness																						
23		1.1	Easy to understand what is the threat	1																				
24		1.2	Easy to understand what is the impact	1																				
25																								
26	2	Empower people																						
27		2.1	Simple information to understand how to address the threat	1																				
28		2.2	Appropriate call to action message	1																				
29		2.3	Overall conveys a positive message	1		Neutral																		
30																								
31	3	Evidence-based content																						
32		3.1	Based on facts, e.g. statistics, etc.	1																				
33		3.2	From credible source	1																				
34																								
35	4	Memorable																						
36		4.1	Micro-learning - specific topic	1																				
37		4.2	Micro-learning - short statements, focus on key points	1																				
38		4.3	Consider different learning styles	1				Visual/text																
39		4.4	Balance between graphics and text	1																				
40		4.5	Audience can easily relate, e.g. storytelling	1																				
41																								
42	Presentation attributes																							
43																								
44	1	Visibility of the message																						
45		1.1	Appropriate location	1																				
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1																				
47																								
48	2	Layout, style and formatting																						
49		2.1	Uses lines, borders and shapes to group related information	1																				
50		2.2	Create text hierarchy (up to 3 different font styles)	1																				
51		2.3	Maximum 4 colours	1																				
52																								
53	3	Inclusive / Accessible																						
54		3.1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/																
55		3.2	Use appropriate font style ()	1																				
56		3.3	Use appropriate font size ()	1																				
57																								
58																								
59																								
60																								
61		Communication Strategy attributes				4																		
62		Behaviour-change attributes				5																		
63		Presentation attributes				8																		
64																								
65		TOTAL				17																		
66																								
67		Overall quality of awareness raising material																						
68		Low				0-14																		
69		Medium				15-22																		
70		High				23-28																		

A	B	C	D	E	F	G	H	I	J	K	L
1											
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>					
3											
4											
5	1. Audience		Markets								
6		1.1 Across groups									
7		1.2 Specific									
8											
9	2. Key message focus - clear purpose										
10		2.1 Awareness - about threat									
11		2.2 Awareness - about impact									
12		2.3 Cyber hygiene - best practices									
13		Empowerment - call to action, e.g. visit a website to learn more, to report									
14		2.4 an incident, etc.									
15	3. Tone/style										
16		3.1 Generic									
17		3.2 Covers specific time periods									
18											
19	<b>Behaviour-change attributes</b>										
20											
21											
22	1. Promote situational awareness										
23		1.1 Easy to understand what is the threat									
24		1.2 Easy to understand what is the impact									
25											
26	2. Empower people										
27		Simple information to understand									
28		2.1 how to address the threat									
29		2.2 Appropriate call to action message									
30		2.3 Overall conveys a positive message									
31											
32	3. Evidence-based content										
33		3.1 Based on facts, e.g. statistics, etc.									
34		3.2 From credible source									
35	4. Memorable										
36		4.1 Micro-learning - specific topic									
37		Micro-learning - short statements,									
38		4.2 Focus on key points									
39		4.3 Consistent different learning styles									
40		4.4 Balance between graphics and text									
41		Audience can easily relate, e.g.									
42		4.5 storytelling									
43	<b>Presentation attributes</b>										
44											
45	1. Visibility of the message										
46		1.1 Appropriate location									
47		Draw attention to key information,									
48		1.2 e.g. by using contrasting colour									
49	2. Layout, style and formatting										
50		Use lines, borders and shapes to									
51		2.1 group related information									
52		Create text hierarchy (up to 3)									
53		2.2 different font styles									
54		2.3 Maximum of colours									
55	3. Inclusive / Accessible										
56		Appropriate contrast between the									
57		3.1 text color and background color									
58		3.2 Use appropriate font style(s)									
59		3.3 Use appropriate font size(s)									
60											
61	<b>Communication Strategy attributes</b>										
62	<b>Behaviour-change attributes</b>										
63	<b>Presentation attributes</b>										
64											
65											
66											
67											
68	<b>Overall quality of awareness-raising material</b>										
69	Low										
70	Medium										
71	High										
72											
73											

## TOP SECURITY THREATS IN 2022

A 2022 Securix Threat Report highlights the trends, required data, and detection summaries for key threats. Additionally, the report covers techniques observed from the trenches across insider threat, cloud infrastructure misuse/abuse, and preemptive ransomware detection. Here are its key highlights and focus points.

### THREAT TRENDS IN 2022

- ◆ AWARENESS: 867 THREATS OBSERVED + 481.9%
- ◆ DISCOVERY: 35,776 IOCS + 380%
- ◆ INVESTIGATIONS: 582 THREATS DETECTED, ANALYSED AND REPORTED + 218%

### MOST POPULAR THREATS IN 2022

- ◆ **Insider Threats:** Email (68%) and content management products (68%) continue to be top egress vectors.
- ◆ **Cloud Infrastructure:** Cloud content management, cloud services, cloud authorisation, and MS Office 365 have the highest percentage of tenants that have use cases to detect cloud threats.
- ◆ **Ransomware:** Phishing is responsible for almost half of the top policy violations related to initial access, and 60% of customers have recognised that consistent threat by ingesting some form of email logs.

### CHARACTERISTICS OF IOT AND OT THAT ARE MOST EXPLOITED BY CYBERCRIMINALS

- ◆ Deficient Physical Security
- ◆ Limited Energy Capacity
- ◆ Inadequate Authentication
- ◆ Improper Encryption
- ◆ Unnecessary Open Ports
- ◆ Insufficient Access Control
- ◆ Improper Patch Management Capabilities

**ET CIO.com**  
SOUTH EAST ASIA II

Source: Securix Report

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1													
2	Communication Strategy attributes				Evaluation								
3					Infographic - website <a href="https://www.pratum.com/blog/50-infographic-lessons-of-remote-working-2020">https://www.pratum.com/blog/50-infographic-lessons-of-remote-working-2020</a>								
4													
5	1 Audience			Maks									
6		1.1	Access groups	1									
7		1.2	Specific	2									
8													
9	2 Key message focus - clear purpose												
10		2.1	Awareness - about threat	1									
11		2.2	Awareness - about impact	1									
12		2.3	Cyber hygiene - best practices	1									
13		2.4	Improvement - call to action, e.g. visit a website to learn more, to report an incident, etc.	1									
14													
15	3 Timeliness												
16		3.1	Generic	1									
17		3.2	Covers specific time periods	2									
18													
19													
20	Behavior-change attributes												
21	1 Protect situational awareness												
22			Stay to understand what is the										
23		1.1	threat	1									
24		1.2	impact	1									
25													
26	2 Empower people												
27		2.1	Simple information to understand	1									
28		2.2	How to address the threat	1									
29		2.3	Appropriate call to action message	1									
30													
31	3 Evidence-based content												
32		3.1	Based on facts, e.g. statistics, etc.	1									
33		3.2	From credible source	1									
34													
35	4 Memorable												
36		4.1	Mico-learning - specific topic	1									
37		4.2	Mico-learning - short statements	1									
38		4.3	Focus on key points	1									
39		4.4	Considers different learning styles	1									
40		4.5	Balance between graphics and text	1									
41			Audience can easily relate, e.g. storytelling	1									
42	Presentation attributes												
43	1 Visibility of the message												
44		1.1	Appropriate location	1									
45		1.2	Draw attention to key information, e.g. by using contrasting colour	1									
46													
47	2 Layout, style and formatting												
48		2.1	Uses lines, borders and shapes to group related information	1									
49		2.2	Create text hierarchy (up to 3 different font styles)	1									
50		2.3	Maximum 4 colours	1									
51													
52	3 Inclusive / Accessible												
53		3.1	A good color contrast between text color and background color	1									
54		3.2	Use appropriate font styles ()	1									
55		3.3	Use appropriate font size ()	1									
56													
57													
58													
59													
60													
61	Communication Strategy attributes												
62	Behavior-change attributes												
63	Presentation attributes												
64													
65			TOTAL										
66													
67	Overall quality of awareness raising material												
68			Low										
69			Medium										
70			High										
71													

## One Click Can Be Costly

Bob manages inventory at a mid-size manufacturer. On a very busy day, Bob sees an email from the IT team asking him to confirm his login information. He clicks a link, confirms his login credentials and gets back to what he was doing.

Without knowing it, Bob just gave his credentials to a hacker, who logs into the company environment and starts figuring out what they can access.

**A few seconds of carelessness by Bob trigger a chain of events:**

A month later, the hackers send the company an email announcing that they have encrypted most of the company's data and want a **\$500,000 ransom** to release it.

### THE IMPACT

- While the company decides what to do, **all operations at the plant shut down.**
- Managers send **55 workers home** for two days at half pay.
- The company loses **\$75,000 worth of deliveries.**

### THE IMPACT SEVERITY


- The company decides not to pay the ransom, but spends **\$45,000** recovering its data and investigating the breach.
- Three major customers lose faith in the company's ability to deliver and decide not to renew their contracts totaling **\$325,000** in lost business.
- Because of the breach, the company's cyber security premium goes up **\$15,000 per year** at renewal time.
- The combined costs of the breach mean the company misses its revenue target and **can't pay bonuses.**
- Reduced demand next year requires the company to **lay off 5 employees.**

Be prepared for Bob's mistake! Perform a business impact analysis to understand how various cyberattacks will affect your business.


Pratum®

A	B	C	D	E	F	G	H	I	J	K	L
1	<b>Communication Strategy attributes</b>										
2	Evaluation										
3	Info@phish - website <a href="https://www.synovus.com/business/securecommerce/mid-market/industry/holiday-hack-01@phish/">https://www.synovus.com/business/securecommerce/mid-market/industry/holiday-hack-01@phish/</a>										
4	Website Comments										
5	Audience										
6	1.1	Across groups	1								
7	1.2	Specific	2								
8											
9	2 Key message focus - clear purpose										
10	2.1	Awareness - about threat	1								
11	2.2	Awareness - about impact	2	1 Holiday seasons							
12	2.3	Cyber hygiene - best practices	1	1 Loss recovery							
13	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.										
14											
15	3 Timeliness										
16	3.1	Generic	1								
17	3.2	Covers specific time periods	2	2 Holiday season November to December							
18											
19											
20	<b>Behaviour-change attributes</b>										
21											
22	1 Protect vital personal systems										
23	1.1	Stay to understand what is the threat	1	1							
24	1.2	Stay to understand what is the impact	1	1							
25											
26	2 Empower people										
27	Simple information to understand how to address the threat										
28	2.1	Appropriate call to action message	1	1							
29	2.2	Overall convey a positive message	1	Neutral							
30											
31	3 Evidence-based content										
32	3.1	Based on facts, e.g. statistics, etc.	1	1 Statistics							
33	3.2	From credible source	1								
34											
35	4 Memorable										
36	4.1	Micro-learning - specific topics	1	1							
37	4.2	Micro-learning - short statements, focus on key points	1	1							
38	4.3	Consider different learning styles	1	1 Visual/Text							
39	4.4	Balance between graphics and text	1	1							
40	4.5	Audience can easily relate, e.g. storytelling	1								
41											
42	<b>Presentation attributes</b>										
43											
44	1 Visibility of the message										
45	1.1	Appropriate location	1	1							
46	1.2	Draw attention to key information, e.g. by using contrasting colour	1	1							
47											
48	2 Layout, style and formatting										
49	2.1	Use links, borders and shapes to group related information	1	1							
50	2.2	Create text hierarchy (up to 3 different font styles)	1	1							
51	2.3	Maximum 4 colours	1	1							
52											
53	3 Inclusive / Accessible										
54	3.1	A good color contrast between the text color and background color	1	1 Using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>							
55	3.2	Use appropriate font styles	1	1							
56	3.3	Use appropriate font size	1	1							
57											
58											
59											
60											
61	<b>Communication Strategy attributes</b>										
62	<b>Behaviour-change attributes</b>										
63	<b>Presentation attributes</b>										
64											
65	<b>Overall quality of awareness raising material</b>										
66											
67	Low	0-34									
68	Medium	35-62									
69	High	63-100									
70											
71											
72											
73											
74											

# WARNING!




The holidays are a particularly busy time for companies and, unfortunately, fraudsters. Be aware of the fraud trends.




U.S. fraud attempts from **Thanksgiving to Christmas** have remained consistent over the last **four years** at almost **20%**<sup>1</sup>


Non-delivery and non-payment are two popular **holiday** scams that cost **\$265 million** in losses just **two years ago**.<sup>2</sup>




Over a **four-year period**, attempted ransomware attacks spiked **70%** during the months of **November and December**.<sup>3</sup>





In the last **two years**, **73%** of major brands were targeted in Phishing-as-a-Service scams, where criminals sell their services to other fraudsters, leading up to **Black Friday**.<sup>4</sup>






Shoplifting, fraud, and employee theft rises by more than **15%** during the **holidays**.<sup>5</sup>





**37%** of retailers' annual shrinkage occurs during the **holidays**.<sup>6</sup>

Stay vigilant to mitigate risk to your business during the holidays. For more information, contact Synovus Treasury & Payment Solutions or your Treasury Consultant. You can also stop by one of our local branches to learn more.



Synovus Bank, Member FDIC  
© 2022 Synovus Financial Corp. All rights reserved.

A	B	C	D	E	F	G	H	I	J	K	L	M
1												
2												
3												
4												
5	1	Adverse		Malicious								
6			1.1	Acquaintance								
7			1.2	Specific								
8												
9	2	Key message focus - clear purpose										
10			2.1	Awareness - about threat								
11			2.2	Awareness - about impact								
12			2.3	Clear hygiene - best practices								
13				(Department - collection, e.g. job available to learn more, to report an incident, etc.)								
14												
15	3	Timeliness										
16			3.1	Generic								
17			3.2	Covers specific time periods								
18												
19												
20												
21												
22												
23	4	Promote educational awareness										
24			4.1	Day to understand what is the threat								
25			4.2	Day to understand what is the impact								
26												
27	5	Empower people										
28			5.1	Single information to understand how to address the threat								
29			5.2	Appropriate call to action message								
30			5.3	Overall conveys a positive message								
31												
32	6	Evidence-based content										
33			6.1	Based on facts, e.g. statistics, etc.								
34			6.2	From credible source								
35												
36	7	Memoizable										
37			7.1	Micro-learning - specific topic								
38			7.2	Micro-learning - short statements, focus on key points								
39			7.3	Consider different learning styles								
40			7.4	Balance between graphics and text								
41			7.5	Address commonly known, e.g. everything								
42												
43												
44												
45												
46												
47												
48												
49												
50												
51												
52												
53												
54												
55												
56												
57												
58												
59												
60												
61												
62												
63												
64												
65												
66												
67												
68												
69												
70												
71												
72												
73												
74												
75												
76												
77												
78												
79												
80												

**KnowBe4**

## TOP-CLICKED PHISHING TESTS

**COMMON "IN THE WILD" ATTACKS**

- HR: Your performance evaluation is due
- Google: You were mentioned in a document: "Strategic Plan Draft"
- IT: Inventory Form
- Microsoft 365: Microsoft 365 has new password requirements
- Amazon: Balance paid on your seller account
- Xerox: New document was processed for [[email]]
- Zoom: [[manager name]] has sent you a message via Zoom Message Portal
- Facebook: Your recent Facebook login
- Your fax is pending for preview
- Money has been successfully withdrawn from your bank account

**KEY TAKEAWAY**

Business phishing attacks are the most trusted subject category across the world. These are the most messages purporting to be from internal organizational departments. Be critical! Request for information that comes a series of going and asking you to take an action.

### TOP EMAIL SUBJECTS GLOBALLY

**KEY TAKEAWAY**

HR has been a top threat because subject suggests coming from HRIT Managers in recent months. Others include topics like new device or password resets. These attacks are effective because they usually purport to affect your daily work and cause a person to react before looking regularly at the legitimacy of the email.

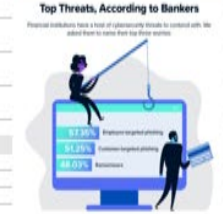
### TOP 5 ATTACK VECTOR TYPES

- Link**  
Phishing Hyperlink in the Email
- Spoofted Domain**  
Appears to Come From the User's Domain
- Branded**  
Phishing Test Link Has User's Organizational Logo and Name
- PDF Attachment**  
Email Contains a PDF Attachment
- Credentials Landing Page**  
Phishing Link Directs User to Data Entry or Login Landing Page

**KEY TAKEAWAY**

This is a warning of the attack vector types used in KnowBe4 Phishing Security Tests. This is a warning of the attack vector types used in KnowBe4 Phishing Security Tests. This is a warning of the attack vector types used in KnowBe4 Phishing Security Tests.

A	B	C	D	E	F	G	H	I	J	K
1										
2	Communication Strategy attributes				Evaluation					
3										
4										
5	1 Audience		Mark		Mark	Comments				
6		1.1 Across groups	1							
7		1.2 Specific	2			2 Employee/Organisations				
8										
9	2 Key message focus - clear purpose									
10		2.1 Awareness - about threat	1				1 most concerning threats 2022			
11		2.2 Awareness - about impact	1							
12		2.3 Cyber hygiene - best practices	1							
13		Empowerment - calls to action, e.g. visit a website to learn more, 2.4 to report an incident, etc.	1				1 visit a website to learn more			
14										
15	3 Timeframe									
16		3.1 Generic	1				1			
17		3.2 Covers specific time periods	2							
18										
19										
20	Behaviour-change attributes									
21										
22	1 Promote situational awareness									
23		Easy to understand what is the 1.1 threat	1				1			
24		Easy to understand what is the 1.2 impact	1							
25										
26	2 Empower people									
27		Simple information to understand 2.1 how to address the threat	1				1			
28		2.2 Appropriate call to action message	1							
29		Overall conveys a positive 2.3 message	1				neutral			
30										
31	3 Evidence-based content									
32		3.1 Based on facts, e.g. statistics, etc.	1				1 statistics			
33		3.2 From credible source	1							
34										
35	4 Memorable									
36		4.1 Micro-learning - specific topic	1				1			
37		4.2 Micro-learning - short statements, focus on key points	1							
38		4.3 Consider different learning styles	1				1 Visual/text			
39		4.4 Balance between graphic and text	1							
40		4.5 Audience can easily relate, e.g. easy telling	1				1 real examples			
41										
42	Presentation attributes									
43										
44	1 Visibility of the message									
45		1.1 Appropriate location	1							
46		1.2 Draw attention to key information, e.g. by using contrasting colour	1				1			
47										
48	2 Layout, style and formatting									
49		2.1 Uses lines, borders and shapes to group related information	1				1			
50		2.2 Create text hierarchy (up to 3 different font styles)	1				1			
51		2.3 Maximum 6 colours	1							
52										
53	3 Inclusive / Accessible									
54		3.1 A good color contrast between the text color and background color	1				1			
55		3.2 Use appropriate font size(s)	1				1			
56		3.3 Use appropriate font size (l)	1				1			
57										
58										
59										
60										
61	Communication Strategy attributes				8					
62	Behaviour-change attributes				5					
63	Presentation attributes				6					
64										
65										
66										
67	Overall quality of awareness-raising material									
68	Low				0-14					
69	Medium				15-22					
70	High				23-28					
71										



# A.4 Analysis Infographics 2023

The excel file contains all the evaluation of the twenty-five infographics for the year 2023.



infographics\_frame  
work\_v2023.xlsx

1)


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1																									
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>																				
3					Infographic - website <a href="https://vpnalert.com/resources/phishing-statistics/">https://vpnalert.com/resources/phishing-statistics/</a>																				
4																									
5	1	Audience		Marks	Marks																				
6		1.1	Across groups	1	Comments																				
7		1.2	Specific	2	Generation Z/Millennials/Generation X																				
8																									
9	2	Key message focus - clear purpose																							
10		2.1	Awareness - about threat	1	1																				
11		2.2	Awareness - about impact	1	Statistics of phishing attacks																				
12		2.3	Cyber hygiene - best practices	1																					
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, 2.4 etc.	1																					
14																									
15	3	Timeframe																							
16		3.1	Generic	1	1																				
17		3.2	Covers specific time periods	2																					
18																									
19																									
20	<b>Behaviour-change attributes</b>																								
21																									
22	1	Promote situational awareness																							
23		1.1	Easy to understand what is the threat	1	1																				
24		1.2	Easy to understand what is the impact	1	Easy to understand the threat																				
25																									
26	2	Empower people																							
27		2.1	Simple information to understand how to address the threat	1	1																				
28		2.2	Appropriate call to action message	1																					
29		2.3	Overall conveys a positive message	1	neutral																				
30																									
31	3	Evidence-based content																							
32		3.1	Based on facts, e.g. statistics, etc.	1	1																				
33		3.2	From credible source	1	statistics																				
34																									
35	4	Memorable																							
36		4.1	Micro-learning - specific topic	1	1																				
37			Micro-learning - short statements, focus on key points	1																					
38		4.3	Considers different learning styles	1	1																				
39		4.4	Balance between graphics and text	1	visual/text																				
40		4.5	Audience can easily relate, e.g. storytelling	1	1																				
41																									
42	<b>Presentation attributes</b>																								
43																									
44	1	Visibility of the message																							
45		1.1	Appropriate location	1	1																				
46			Draw attention to key information, e.g. by using contrasting colour	1	1																				
47																									
48	2	Layout, style and formatting																							
49		2.1	Uses lines, borders and shapes to group related information	1	1																				
50			Create text hierarchy (up to 3 different font styles)	1	1																				
51		2.3	Maximum 4 colours	1	1																				
52																									
53	3	Inclusive / Accessible																							
54		3.1	A good color contrast between the text color and background color	1	1																				
55		3.2	Use appropriate font styles()	1	1																				
56		3.3	Use appropriate font size()	1	1																				
57																									
58																									
59																									
60																									
61	<b>Communication Strategy attributes</b>				8																				
62	<b>Behaviour-change attributes</b>				7																				
63	<b>Presentation attributes</b>				8																				
64																									
65	<b>TOTAL</b>				<b>19</b>																				
66																									
67	Overall quality of awareness raising material																								
68	Low 0-14																								
69	Medium 15-22																								
70	High 23-28																								
71																									
72																									



2)


	A	B	C	D	E	F	G	H	I	J	K
1											
2		<b>Communicator Strategy attributes</b>									
3						<b>Solution</b>					
4						Integrative - website	<a href="http://www.cyberpilot.com/learn/how-to-spot-a-phishing-email?utm_medium=email&amp;utm_source=newsletter">http://www.cyberpilot.com/learn/how-to-spot-a-phishing-email?utm_medium=email&amp;utm_source=newsletter</a>				
5		1 Audience			Notes	Notes	Comments				
6			1.1 Acronym								
7			1.2 Specific								
8											
9		2 Key message focus - clear purpose									
10			2.1 Awareness - about threat								
11			2.2 Awareness - about impact								
12			2.3 Open to give - best practices								
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											
31											
32											
33											
34											
35											
36											
37											
38											
39											
40											
41											
42											
43											
44											
45											
46											
47											
48											
49											
50											
51											
52											
53											
54											
55											
56											
57											
58											
59											
60											
61											
62											
63											
64											
65											
66											
67											
68											
69											
70											
71											
72											
73											
74											
75											
76											
77											
78											
79											
80											
81											
82											
83											
84											
85											
86											
87											
88											
89											
90											
91											
92											
93											
94											
95											
96											
97											
98											
99											
100											

## How to spot a phishing mail




**Requests for sensitive information**

Always establish if the request for sensitive information is reasonable.




**Attachment formats**

Cybercriminals try to get you to unknowingly install malware. It would most likely be a .zip, .exe or .jar file.




**Emotional appeals**

They will try to elicit fear or urgency to convince you to act carelessly.




**Link addresses**

The hyperlink and the actual linked page could differ and lead you to a malicious website.




**Unsolicited emails**

They will ask something or offer you a reward that you didn't request or initiate.




**Email sender domain**

Even after evaluating the domain, you can never be 100% sure that the email is authentic.



**Grammar or odd phrasing**

Watch out for grammatical, spelling errors and things that are technically correct, but nobody says.



CyberPilot

3)

Communication Strategy attribute			Evaluation
Infographic - website			<a href="https://greenphire.com/infographic-technology-a-key-to-patient-engagement/">https://greenphire.com/infographic-technology-a-key-to-patient-engagement/</a>
1	Audience	Marks	
6	1.1 Across groups	1	1
7	1.2 Specific	2	
9	2 Key message focus - clear purpose		
10	2.1 Awareness - about threat	1	1 phishing/avoiding prevention tips
11	2.2 Awareness - about impact	1	1 steal data and damage the network
12	2.3 Cyber hygiene - best practices	1	1
13	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1	1 report the incident
15	3 Timeliness		
16	3.1 Generic	1	1
17	3.2 Covers specific time periods	2	
Behaviour-change attribute			
22	1 Promote situational awareness		
23	1.1 Easy to understand what is the threat	1	1
24	1.2 Easy to understand what is the impact	1	1
26	2 Empower people		
27	2.1 Simple information to understand how to address the threat	1	1
28	2.2 Appropriate call to action message	1	1
29	2.3 Overall conveys a positive message	1	neutral
31	3 Evidence-based content		
32	3.1 Based on facts, e.g. statistics, etc.	1	
33	3.2 From credible source	1	
35	4 Memorable		
36	4.1 Micro-learning - specific topic	1	1
37	4.2 Micro-learning - short statements, focus on key points	1	
38	4.3 Consider different learning styles	1	1 video/text
39	4.4 Balance between graphics and text	1	1
40	4.5 Audience can easily relate, e.g. storytelling	1	1 tips how to prevent the threats
Presentation attribute			
46	1 Visibility of the message		
45	1.1 Appropriate location	1	1
46	1.2 Draw attention to key information, e.g. by using contrasting colour	1	1
48	2 Layout, style and formatting		
49	2.1 Use lines, borders and shapes to group related information	1	1
50	2.2 Create text hierarchy (up to 3 different font styles)	1	1
51	2.3 Maximum 4 colours	1	
53	3 Inclusive / Accessible		
54	3.1 A good color contrast between the text color and background color	1	1
55	3.2 Use appropriate font styles()	1	1
56	3.3 Use appropriate font size()	1	1
Communication Strategy attribute			5
Behaviour-change attribute			6
Presentation attribute			6
TOTAL			17
Overall quality of awareness-raising material			
68	Low	0-10	
69	Medium	10-22	
70	High	23-28	

## PHISHING/SMISHING PREVENTION TIPS

### Know The Targets

Phishing attacks target people through emails.

Smishing attacks target people through SMS messages.

### Look For Red Flags

Phishing emails tend to include:

- Misspellings, grammatical errors, and abnormal spacing
- Requests for sensitive/personal information such as: passwords, credit card information, SSN, or information about another person
- Request immediate action or open an attachment to avoid a consequence like account closure

### Check URLs

Hover over hyperlinks to determine if the URL makes sense coming from the sender.

The sender name should match the URL, there shouldn't be a different name or location in the URL.

### Check The Source

Carefully review the Sender and Subject Line before opening any email. Delete any suspicious emails before you open them.

DO NOT open attachments from, reply to, or click on URLs from unknown and untrusted sources.

### Report Immediately

Report any suspicious emails, even if you're not sure, to your manager and ITSG for further review and investigation.

Use common sense: If it doesn't look right, trust your judgment.

### Protect Your Email Address

Never provide your company email address for personal communications.

Passwords, credit card numbers, social security numbers, or account numbers should never be shared via email.

### Understand The Impact

An attack includes emails or SMS messages designed to trick you into visiting malicious sites or downloading malware used to steal data and damage networks.

Nearly one-third of all cybersecurity breaches involve phishing.\*

### Adherence is critical

It is crucial for employees to remain knowledgeable and vigilant about phishing & smishing attempts and how to avoid them.

Thank you for your ongoing support to promote Greenphire's compliance & ethics program!

greenphire

4)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	<b>Communication Strategy attributes</b>				<b>Evaluation</b>															
					Infographic - website	<a href="https://phishingtackle.com/ransomware-infographic/">https://phishingtackle.com/ransomware-infographic/</a>														
	<b>1 Audience</b>			Marks	Marks	Comments														
	1.1	Across groups	1			1	Individual/Business													
	1.2	Specific	2																	
	<b>2 Key message focus - clear purpose</b>																			
	2.1	Awareness - about threat	1			1	how to protect your data from ransomware attacks													
	2.2	Awareness - about impact	1			1	encrypt your files													
	2.3	Cyber hygiene - best practices	1			1														
		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1																	
	<b>3 Timeframe</b>																			
	3.1	Generic	1			1														
	3.2	Covers specific time periods	2																	
	<b>Behaviour-change attributes</b>																			
	<b>1 Promote situational awareness</b>																			
	1.1	Easy to understand what is the threat	1			1														
	1.2	Easy to understand what is the impact	1			1														
	<b>2 Empower people</b>																			
		Simple information to understand how to address the threat	1			1														
	2.1	Appropriate call to action message	1			1														
	2.2	Overall conveys a positive message	1			neutral														
	<b>3 Evidence-based content</b>																			
	3.1	Based on facts, e.g. statistics, etc.	1			1														
	3.2	From credible source	1			1														
	<b>4 Memorable</b>																			
	4.1	Micro-learning - specific topic	1			1														
		Micro-learning - short statements, focus on key points	1			1														
	4.2	Consider different learning styles	1			1														
	4.3	Balance between graphics and text	1			1														
	4.4	Audience can easily relate, e.g. storytelling	1			1	tips to protect your data													
	<b>Presentation attributes</b>																			
	<b>1 Visibility of the message</b>																			
	1.1	Appropriate location	1			1														
		Draw attention to key information, e.g. by using contrasting colour	1			1														
	<b>2 Layout, style and formatting</b>																			
		Uses lines, borders and shapes to group related information	1			1														
	2.1	Create text hierarchy (up to 3 different font styles)	1			1														
	2.2	Maximum 4 colours	1			1														
	2.3	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>													
	3.1	Use appropriate font style (i)	1			1														
	3.2	Use appropriate font size (i)	1			1														
	3.3		1			1														
	<b>3 Inclusive / Accessible</b>																			
		A good color contrast between the text color and background color	1			1														
	3.1		1			1														
	3.2		1			1														
	3.3		1			1														
	<b>Communication Strategy attributes</b>					5														
	<b>Behaviour-change attributes</b>					7														
	<b>Presentation attributes</b>					8														
	<b>TOTAL</b>					<b>20</b>														
	<b>Overall quality of awareness raising material</b>																			
	<b>Low</b>	0-14																		
	<b>Medium</b>	15-22																		
	<b>High</b>	23-28																		



5)

A	B	C	D	E	F	G	H	I	J	K
1										
2	<b>Communication Strategy attribute</b>				<b>Evaluation</b>					
3						Infographic - website	<a href="https://au.insight.com/en_AU/content-nsd-resources/2023/year-2023-cybersecurity-checklist.html">https://au.insight.com/en_AU/content-nsd-resources/2023/year-2023-cybersecurity-checklist.html</a>			
4										
5	1	Audience	Marks			Marks	Comments			
6		1.1	Across groups	1						
7		1.2	Specific	2			2	Business		
8										
9	2	Key message focus - clear purpose								
10		2.1	Awareness - about threat	1			1	security check list		
11		2.2	Awareness - about impact	1						
12		2.3	Cyber hygiene - best practices	1			1			
13			Empowerment - call to action, e.g. video available to learn more, to report an incident,							
14			2.4 etc.	1						
15										
16		3	Timeframe							
17		3.1	Generic	1			1			
18		3.2	Covers specific time periods	2						
19										
20	<b>Behaviour-change attribute</b>									
21										
22	1	Promote situational awareness								
23		1.1	Easy to understand what's the threat	1			1			
24		1.2	Easy to understand what's the impact	1						
25										
26	2	Empower people								
27			Simple information to understand how to address the threat	1			1			
28		2.1	Appropriate call to action message	1			1			
29		2.2	Overall conveys a positive message	1			1			
30		2.3	Overall conveys a positive message	1			1			
31										
32	3	Evidence-based content								
33		3.1	Based on facts, e.g. statistics, etc.	1						
34		3.2	From credible source	1						
35										
36	4	Memorable								
37		4.1	Micro-learning - specific topic	1			1			
38			Micro-learning - short statements, for action							
39		4.2	Key points	1			1			
40		4.3	Considers different learning styles	1			1	visual/text		
41		4.4	Balance between graphics and text	1						
42										
43		4.5	Audience can easily relate, e.g. storytelling	1			1	Can you check off each of the list		
44										
45	<b>Presentation attribute</b>									
46	1	Visibility of the message								
47		1.1	Appropriate location	1						
48			Draw attention to key information, e.g. by using contrasting colour	1			1			
49										
50	2	Layout, style and formatting								
51		2.1	Use lines, borders and shapes to group related information	1			1			
52		2.2	Create text hierarchy (up to 3 different font styles)	1			1			
53		2.3	Maximum 4 colours	1			1			
54										
55	3	Inclusive / Accessible								
56		3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>		
57		3.2	Use appropriate font style(s)	1			1			
58		3.3	Use appropriate font size	1			1			
59										
60										
61	<b>Communication Strategy attribute</b>						5			
62	<b>Behaviour-change attribute</b>						8			
63	<b>Presentation attribute</b>						7			
64	<b>TOTAL</b>						20			
65										
66	Overall quality of awareness raising material									
67		Low	0-14							
68		Medium	15-22							
69		High	23-28							
70										
71										

**Insight** <sup>##</sup>

**Your 2023 Security Checklist**

As we enter a new year ... and cyberthreats continue to evolve ... it's time to consider your current security measures. Is your business thoroughly protected?

In this checklist, we've outlined key technologies that will bolster your defense against modern attacks. Many of these strategies overlap, but it's important to note their usefulness against various security threats.

Hang onto this list for reference throughout the year, and talk with an Insight expert to ensure that each area of your business is secure.

---

**Modern workforce protection**

When it comes to securing your hybrid workforce, there are several components to keep in mind:

- Email security to thwart phishing, viruses and ransomware
- Identity and Access Management (IAM) to control visibility and user control
- Endpoint protection to secure devices from any location
- Firewalls and Virtual Private Networks (VPN) to extend your infrastructure
- AI-powered security tools to detect threats and mitigate risk
- Employee education to minimize the likelihood of human error

---

**Crucial cloud security**

As more data moves to the cloud, you need robust protection against critical cloud attacks.

Make sure your cloud defenses include:

- Secure encryption to streamline information from mobile to protected text
- Application security to minimize threats, breaches and code spacing
- IAM, such as multi-factor authentication, to ensure that nothing is possible without enough to validate your systems
- Threat detection and risk monitoring to prevent cloud attacks before they begin

---

**Ransomware prevention**

Ransomware remains one of the largest cybersecurity threats. These security tools can lessen your risk and accelerate recovery:

- Advanced email protection to shield against the specific method of ransomware delivery, phishing attacks
- IAM to restrict permissions and limit network access
- Regular system updates to help protect against malware
- Staff education to recognize malicious messages better
- And, in the event of a ransomware attack, established and secure data backup tools for faster recovery

---

**Powerful data defense**

Data is the backbone of modern business, and powerful security is essential for protecting your clients, businesses and organization.

Modern data protection should include:

- Encryption and tokenization to reduce the risk of data breach
- Rigorous retention and access to properly store data and filter threat among clients
- IAM to limit access, restrict permissions and expand visibility
- Regulatory compliance to bolster the integrity of data availability and confidence in data security

---

**CAN YOU CHECK OFF EACH ITEM ON THE LIST?**

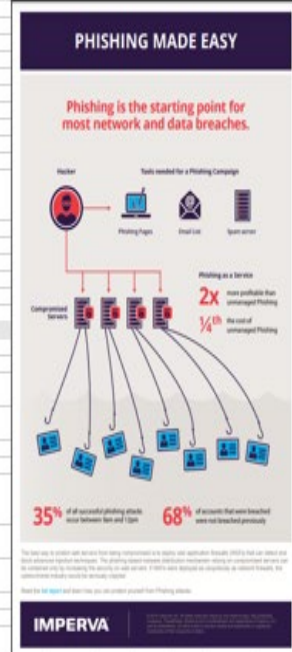
Insight is here to make sure daily items of your business are secure. Our digital security tool lets you find, manage and mitigate these (threats/cyber) risks. We'll help you understand your compliance and more. Talk with a team member today to get started.

Unlock cutting-edge security for a hybrid world. See what Insight can do for you.

**Insight** <sup>##</sup>

6)

B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
<b>Communication Strategy attributes</b>			<b>Evaluation</b>											
			Infographic - website <a href="https://www.imperva.com/resources/resource-library/infographic/phishing-made-easy-time-to-rethink-your-prevention-strategy/">https://www.imperva.com/resources/resource-library/infographic/phishing-made-easy-time-to-rethink-your-prevention-strategy/</a>											
<b>Audience</b>			Marks		Marks		Comments							
1	1.1	Across groups	1											
2	1.2	Specific	2		2	Business								
<b>Key message focus - clear purpose</b>														
3	2.1	Awareness - about threat	1		1	phishing is the most network and data breaches								
4	2.2	Awareness - about impact	1											
5	2.3	Cyber hygiene - best practices	1											
<b>Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.</b>														
6	2.4	visit a website to learn more, to report an incident, etc.	1		1	visit a website to learn more								
<b>Timeframe</b>														
7	3.1	Generic	1		1									
8	3.2	Covers specific time periods	2											
<b>Behaviour-change attributes</b>														
<b>Promote situational awareness</b>														
1	1.1	Easy to understand what is the threat	1		1									
2	1.2	Easy to understand what is the impact	1											
<b>Empower people</b>														
3	2.1	Simple information to understand how to address the threat	1		1									
4	2.2	Appropriate call to action message	1											
5	2.3	Overall conveys a positive message	1		neutral									
<b>Evidence-based content</b>														
1	3.1	Based on facts, e.g. statistics, etc.	1		1	statistics								
2	3.2	From credible source	1											
<b>Memorable</b>														
1	4.1	Micro-learning - specific topic	1		1									
2	4.2	Micro-learning - short statements, focus on key points	1		1									
3	4.3	Consider different learning styles	1		1	visual/text								
4	4.4	Balance between graphics and text	1		1									
5	4.5	Audience can easily relate, e.g. storytelling	1											
<b>Presentation attributes</b>														
<b>Visibility of the message</b>														
1	1.1	Appropriate location	1		1									
2	1.2	Draw attention to key information, e.g. by using contrasting colour	1		1									
<b>Layout, style and formatting</b>														
1	2.1	Uses lines, borders and shapes to group related information	1		1									
2	2.2	Create text hierarchy (up to 3 different font styles)	1		1									
3	2.3	Maximum of colours	1		1									
<b>Inclusive / Accessible</b>														
1	3.1	A good color contrast between the text color and background color	1		1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>								
2	3.2	Use appropriate font styles()	1		1									
3	3.3	Use appropriate font size()	1		1									
<b>Communication Strategy attributes</b>			5											
<b>Behaviour-change attributes</b>			7											
<b>Presentation attributes</b>			8											
<b>TOTAL</b>			20											
<b>Overall quality of awareness raising material</b>														
1	Low	0-14												
2	Medium	15-22												
3	High	23-28												





8)


A	B	C	D	E	F	G	H	I	J	K
1										
2	Communication Strategy attributes					Evaluation				
3						Infographic - website <a href="https://international.catholic.edu/learning/learn-alert/learn-alert.html">https://international.catholic.edu/learning/learn-alert/learn-alert.html</a>				
4										
5	1 Audience			Marks		Marks	Comments			
6		1,1 Across groups	1							
7		1,2 Specific	2				International students			
8										
9	2 Key message focus - clear purpose									
10		2,1 Awareness - about threat	1				how to protect yourself from scams			
11		2,2 Awareness - about impact	1				1			
12		2,3 Cyber hygiene - best practices	1							
13		Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1							
14										
15	3 Timeframe									
16		3,1 Generic	1				1			
17		3,2 Covers specific time periods	2							
18										
19										
20	Behavior-change attributes									
21										
22	1 Promote situational awareness									
23		1,1 Easy to understand what is the threat	1				1			
24		1,2 Easy to understand what is the impact	1				1			
25										
26	2 Empower people									
27		Simple information to understand how to address the threat	1				1			
28		2,1 Address the threat	1							
29		2,2 Appropriate call to action message	1							
30		2,3 Overall conveys a positive message	1				Neutral			
31										
32	3 Evidence-based content									
33		3,1 Based on facts, e.g. statistics, etc.	1				1 Statistics			
34		3,2 From credible source	1				1 links			
35										
36	4 Memorable									
37		4,1 Micro-learning - specific topic	1				1			
38		4,2 Micro-learning - short statements, focus on key points	1							
39		4,3 Consider different learning styles	1				1			
40		4,4 Balance between graphics and text	1				1			
41		4,5 Audience can easily relate, e.g. storytelling	1				1 real examples			
42										
43	Presentation attributes									
44										
45	1 Viability of the message									
46		1,1 Appropriate location	1				1			
47		Draw attention to key information, e.g. by using contrasting colour	1				1			
48										
49	2 Layout, style and formatting									
50		Use lines, borders and shapes to group related information	1				1			
51		2,1 Create text hierarchy (up to 3 different font styles)	1				1			
52		2,2 Font style(s)	1				1			
53		2,3 Maximum # colours	1				1			
54										
55	3 Inclusive / Accessible									
56		A good color contrast between the text color and background color	1							
57		3,1 Use appropriate font style(s)	1				1			
58		3,2 Use appropriate font size(s)	1				1			
59										
60										
61	Communication Strategy attributes					5				
62	Behavior-change attributes					6				
63	Presentation attributes					7				
64										
65			TOTAL			21				
66										
67	Overall quality of awareness-raising material									
68										
69		Low	0-14							
70		Medium	15-22							
71		High	23-28							
72										

## PROTECT YOURSELF FROM SCAMS

Stay vigilant. Scams targeting international students are increasing.


### GOVERNMENT IMPOSTER SCAMS

Scammers impersonating officials from government agencies such as USCIS, ICE, embassies etc., claim the student owes money and demands immediate payment.



### EMPLOYMENT SCAMS

Many cases begin with students receiving an unsolicited job advertisement. Should you reply, scammers will quickly hire you. They will instruct you to purchase certain equipment necessary for your training, and will provide a check to compensate for the costs. Eventually, you will discover that the check they provided has bounced. By then, you have already paid out of pocket to their recommended vendor, which was their goal all along.




### HOUSING SCAMS

Scammers list a rental at an attractively lower price. They offer you photos but will never agree to show the property in person or virtually. They will ask you to send money or a check to secure the property before no one else takes it.



### COVID-19 TRACING SCAMS

Students receive messages that they were in contact with someone who has COVID-19. Scammers will ask for personal information for contact tracing. They will use the information for identity theft.



9)

A	B	C	D	E	F	G	H	I	J	K	L	M
2	<b>Communication Strategy attributes</b>			<b>Evaluation</b>								
				Infographic - website <a href="https://cyberclan.com/uk/resources/cybersecurity-threats-in-2023/">https://cyberclan.com/uk/resources/cybersecurity-threats-in-2023/</a>								
				Marks								
5	1. Audience			Marks								
6	1.1 Across groups			1								
7	1.2 Specific			2								
9	2. Key message focus - clear purpose			1								
10	2.1 Awareness - about threat			1								
11	2.2 Awareness - about impact			1								
12	2.3 Cyber hygiene - best practice			1								
13	2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.			1								
15	3. Timeliness			1								
16	3.1 Generic			1								
17	3.2 Covers specific time periods			2								
21	<b>Behaviour-change attributes</b>											
22	1. Promote situational awareness			1								
23	1.1 Easy to understand what is the threat			1								
24	1.2 Easy to understand what is the impact			1								
26	2. Empower people			1								
27	Simple information to understand how to address the threat			1								
28	2.2 Appropriate call to action message			1								
29	2.3 Overall convey a positive message			Neutral								
31	3. Evidence-based content			1								
32	3.1 Based on facts, e.g. statistics, etc.			1								
33	3.2 From credible source			1								
35	4. Memorable			1								
36	4.1 Micro-learning - specific topic			1								
37	4.2 Micro-learning - short statements, focus on key points			1								
38	4.3 Consider different learning styles			1								
39	4.4 Balance between graphics and text			1								
40	4.5 Audience can easily relate, e.g. everything			1								
42	<b>Presentation attributes</b>											
43	1. Visibility of the message			1								
44	1.1 Appropriate location			1								
45	1.2 Draw attention to key information, e.g. by using contrasting colour			1								
47	2. Layout, style and formatting			1								
48	2.1 Use lines, borders and shapes to group related information			1								
49	2.2 Create text hierarchy (up to 3 different font styles)			1								
50	2.3 Maximum 4 colours			1								
52	3. Inclusive / Accessible			1								
53	3.1 Align color contrast between the text color and background color			1								
54	3.2 Use appropriate font styles()			1								
55	3.3 Use appropriate font size()			1								
57												
58												
61	<b>Communication Strategy attributes</b>			4								
62	<b>Behaviour-change attributes</b>			9								
63	<b>Presentation attributes</b>			8								
64												
65	<b>TOTAL</b>			<b>21</b>								
67	<b>Overall quality of awareness-raising material</b>											
68	Low			0-10								
69	Medium			15-22								
70	High			23-28								



A	B	C	D	E	F	G	H	I	J
1									
2	Communication Strategy attributes					Evaluation			
3						Infographic - website	<a href="https://us.norton.com/blog/online-scams/romance-scams/">https://us.norton.com/blog/online-scams/romance-scams/</a>		
4									
5	Audience		Marks			Marks	Comments		
6		1.1	Across groups	1			1	Individual	
7		1.2	Specific	2					
8									
9	Key message focus - clear purpose								
10		2.1	Awareness - about threat	1			1	romance scams	
11		2.2	Awareness - about impact	1			1	they ask for money and they disappear	
12		2.3	Cyber hygiene - best practices	1			1		
13		2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	visit a website to learn more	
14									
15	Timeframe								
16		3.1	Generic	1			1		
17		3.2	Covers specific time periods	2					
18									
19									
20	Behaviour-change attributes								
21									
22	Promote situational awareness								
23		1.1	Easy to understand what is the threat	1			1		
24		1.2	Easy to understand what is the impact	1			1		
25									
26	Empower people								
27		2.1	Simple information to understand how to address the threat	1			1		
28		2.2	Appropriate call to action message	1			1		
29		2.3	Overall conveys a positive message	1			Neutral		
30									
31	Evidence-based content								
32		3.1	Based on facts, e.g. statistics, etc.	1			1	statistics	
33		3.2	From credible source	1			1	norton	
34									
35	Memorable								
36		4.1	Micro-learning - specific topic	1			1		
37		4.2	Micro-learning - short statements, focus on key points	1					
38		4.3	Considers different learning styles	1					
39		4.4	Balance between graphics and text	1					
40		4.5	Audience can easily relate, e.g. storytelling	1			1	real examples	
41									
42	Presentation attributes								
43									
44	Visibility of the message								
45		1.1	Appropriate location	1					
46		1.2	Draw attention to key information, e.g. by using contrasting colour	1			1		
47									
48	Layout, style and formatting								
49		2.1	Uses lines, borders and shapes to group related information	1			1		
50		2.2	Create text hierarchy (up to 3 different font styles)	1			1		
51		2.3	Maximum 4 colours	1			1		
52									
53	Inclusive / Accessible								
54		3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>	
55		3.2	Use appropriate font styles()	1			1		
56		3.3	Use appropriate font size()	1			1		
57									
58									
59									
60									
61	Communication Strategy attributes					6			
62	Behaviour-change attributes					8			
63	Presentation attributes					7			
64									
65									
66			TOTAL			21			
67	Overall quality of awareness raising material								
68	Low		0-14						
69	Medium		15-22						
70	High		23-28						
71									

**Love Is In The Air And Romance Scams Are Everywhere**

Protect your heart (and wallet) your loved ones with the following online dating scam statistics and protection tips.

**How A Romance Scam Works**

- A cybercriminal creates a fake profile to court people online.
- The relationship grows fast and trust is gained.
- The scammer asks their target for money, jewellery, and vouchers.

**Heartbreaking Statistics**

Romance scammers target all sorts of heartbreakers.

- The median individual loss from romance scams was \$4,800 in 2021.
- Over 68,000 consumers filed a report about romance scams with the FTC in 2021, with losses amounting to \$887 million.
- Romance scams were the third highest internet crime loss in 2021.

**Is Your Cyber Sweetheart Swindling You?**

Here are our advice on how our romance scammers can fool you, too. Look for those red flags.

**Do's and Don'ts of Online Dating**

**Do**

- Pay attention to red flags
- Evaluate your online presence
- Approach relationships slowly
- Set up a phone or video chat early
- Carry out your own snooping
- Outsource their asks for help
- Ask someone you trust for a second opinion
- Stop communicating and report the incident

**Don't**

- Send compromising pictures
- Reveal too much personal information
- Pay someone you haven't met
- Feel safe because you made the first contact
- Believe everything they say
- Buy plane tickets or gift cards
- Move communication off dating sites early
- Accept money from someone you haven't met

**norton**

Security. Available at [www.norton.com](https://www.norton.com)

© 2022 Norton. All rights reserved. Some statistics may be estimates or may otherwise vary.

A	B	C	D	E	F	G	H	I	J	K	L
1											
2	Communication Strategy attributes				Evaluation						
3					Infographic - website <a href="https://www.subintvsaak.com/technology/financial-impacts-of-phishing-attacks/">https://www.subintvsaak.com/technology/financial-impacts-of-phishing-attacks/</a>						
4											
5	1	Audience	Mark		Mark	Comments					
6		1.1 Across groups	1								
7		1.2 Specific	2			2 Employees/Organisations					
8											
9	2	Key message focus - clear purpose									
10		2.1 Awareness - about threat	1			1 phishing attacks					
11		2.2 Awareness - about impact	1			1 financial impact					
12		2.3 Cyber hygiene - best practices	1								
13		Empowerment - call to action, e.g. visit a website to learn more, to report									
14		2.4 an incident, etc.	1								
15											
16	3	Timeframe									
17		3.1 Generic	1			1					
18		3.2 Cover specific time periods	2								
19											
20	Behaviour-change attributes										
21											
22	1	Promote situational awareness									
23		1.1 Easy to understand what is the threat	1			1					
24		1.2 Easy to understand what is the impact	1			1					
25											
26	2	Empower people									
27		2.1 Simple information to understand how to address the threat	1			1					
28		2.2 Appropriate call to action message	1								
29		2.3 Overall convey a positive message	1			Neutral					
30											
31	3	Evidence-based content									
32		3.1 Based on facts, e.g. statistics, etc.	1			1 statistics					
33		3.2 From credible source	1								
34											
35	4	Memorable									
36		4.1 Micro-learning - specific topic	1			1					
37		4.2 Micro-learning - short statements, focus on key points	1								
38		4.3 Consider different learning styles	1			1 Visual examples					
39		4.4 Balance between graphics and text	1			1					
40		4.5 Audience can easily relate, e.g. storytelling	1			1 real examples					
41											
42	Presentation attributes										
43											
44	1	Visibility of the message									
45		1.1 Appropriate location	1			1					
46		1.2 Draw attention to key information, e.g. by using contrasting colour	1			1					
47											
48	2	Layout, style and formatting									
49		2.1 Use lines, borders and shapes to group related information	1			1					
50		2.2 Create text hierarchy (up to 3 different font styles)	1			1					
51		2.3 Maximum 4 colours	1			1					
52											
53	3	Inclusive / Accessible									
54		3.1 Good color contrast between the text color and background color	1			1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>					
55		3.2 Use appropriate font styles()	1			1					
56		3.3 Use appropriate font size()	1			1					
57											
58											
59											
60											
61	Communication Strategy attributes				5						
62	Behaviour-change attributes				8						
63	Presentation attributes				7						
64											
65	<b>TOTAL</b>				<b>30</b>						
66											
67	Overall quality of awareness raising material										
68	Low	0-14									
69	Medium	15-22									
70	High	23-30									
71											
72											
73											

## Financial Impact of Phishing Attacks

**24%**

**\$4.6m**

\$4.6 million costing IBM's Cost of Data Breach Report for 2021 found that phishing attacks were the second most expensive type of attack

**\$150**

**7,91,790**

**\$4.1b**

average cost per data breach statistics showed in 2018

IC3 received compliant

\$4.1 billion recorded loss

**\$9.05m**

\$9.05 million according to IBM, USA had the highest rate of costly data breaches in 2021

**2021**

2021 was one of the costliest years in terms of data breaches

**\$2.3m**

\$2.3 million difference in cost between companies that are largely compliant and those that are non-compliant

**\$71,000 to \$106,000**

from 2020 to 2021 increased the average BEC attacks requesting wire transfers

**PhishProtection.**

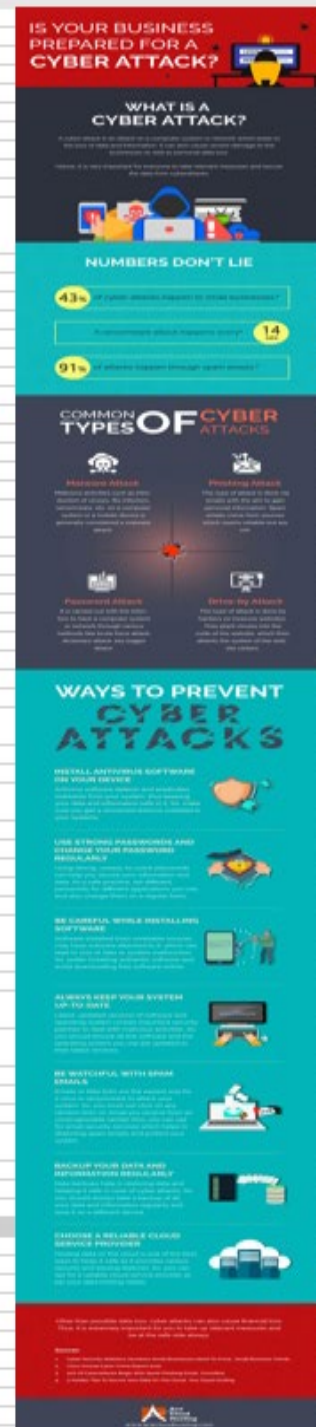
[www.phishprotection.com](http://www.phishprotection.com)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															
16															
17															
18															
19															
20															
21															
22															
23															
24															
25															
26															
27															
28															
29															
30															
31															
32															
33															
34															
35															
36															
37															
38															
39															
40															
41															
42															
43															
44															
45															
46															
47															
48															
49															
50															
51															
52															
53															
54															
55															
56															
57															
58															
59															
60															
61															
62															
63															
64															
65															
66															
67															
68															
69															
70															
71															
72															
73															
74															
75															
76															
77															
78															
79															
80															
81															
82															
83															
84															
85															
86															
87															
88															
89															
90															
91															
92															
93															
94															
95															
96															
97															
98															
99															
100															



13)

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1															
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>										
3						Infographic - website	<a href="https://www.aeccloudhosting.com/blog/infographic-cyber-attack/">https://www.aeccloudhosting.com/blog/infographic-cyber-attack/</a>								
4															
5	<b>Audience</b>		Marka		Marka	Comments									
6	1.1	Across groups	1												
7	1.2	Specific	2			2	business								
8															
9	<b>Key message focus - clear purpose</b>														
10	2.1	Awareness - about threat	1			1	cyber attacks								
11	2.2	Awareness - about impact	1			1	financial loss								
12	2.3	Cyber hygiene - best practices	1			1									
13	2.4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1												
14															
15	<b>Timeframe</b>														
16	3.1	Generic	1			1									
17	3.2	Covers specific time periods	2												
18															
19															
20	<b>Behaviour-change attributes</b>														
21															
22	<b>Promote situational awareness</b>														
23	1.1	Easy to understand what is the threat	1			1									
24	1.2	Easy to understand what is the impact	1			1									
25															
26	<b>Empower people</b>														
27	2.1	Simple information to understand how to address the threat	1			1									
28	2.2	Appropriate call to action message	1			1									
29	2.3	Overall conveys a positive message	1				Neutral								
30															
31	<b>Evidence-based content</b>														
32	3.1	Based on facts, e.g. statistics, etc.	1			1	statistics								
33	3.2	From credible source	1												
34															
35	<b>Memorable</b>														
36	4.1	Micro-learning - specific topic	1			1									
37		Micro-learning - short statements, focus on key points	1												
38	4.3	Considers different learning styles	1			1	Visual, examples								
39	4.4	Balance between graphics and text	1												
40	4.5	Audience can easily relate, e.g. storytelling	1			1	real examples								
41															
42	<b>Presentation attributes</b>														
43															
44	<b>Visibility of the message</b>														
45	1.1	Appropriate location	1												
46		Draw attention to key information, e.g. by using contrasting colour	1			1									
47															
48	<b>Layout, style and formatting</b>														
49	2.1	Uses lines, borders and shapes to group related information	1			1									
50	2.2	Create text hierarchy (up to 3 different font styles)	1			1									
51	2.3	Maximum 6 colours	1			1									
52															
53	<b>Inclusive / Accessible</b>														
54	3.1	A good color contrast between the text color and background color	1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>								
55	3.2	Use appropriate font styles (i)	1			1									
56	3.3	Use appropriate font size (i)	1			1									
57															
58															
59															
60															
61	<b>Communication Strategy attributes</b>					6									
62	<b>Behaviour-change attributes</b>					8									
63	<b>Presentation attributes</b>					7									
64															
65															
66															
67	<b>Overall quality of awareness raising material</b>														
68	<b>Low</b>					0-14									
69	<b>Medium</b>					15-22									
70	<b>High</b>					23-28									
71															
72															



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1																			
2	<b>Communication Strategy attributes</b>					<b>Evaluation</b>													
3						Infographic - website <a href="https://whatismyaddress.com/signs-of-a-romance-scam">https://whatismyaddress.com/signs-of-a-romance-scam</a>													
4																			
5	1	Audience			Marks		Marks	Comments											
6		1.1	Across groups		1		1												
7		1.2	Specific		2														
8																			
9	2	Key message focus - clear purpose																	
10		2.1	Awareness - about threat		1		1	romance scams											
11		2.2	Awareness - about impact		1		1	steal money											
12		2.3	Cyber hygiene - best practices		1		1												
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1		1	visit a website to learn more											
14																			
15	3	Timeframe																	
16		3.1	Generic		1		1												
17		3.2	Covers specific time periods		2														
18																			
19																			
20	<b>Behaviour-change attributes</b>																		
21																			
22	1	Promote situational awareness																	
23		1.1	Easy to understand what is the threat		1		1												
24		1.2	Easy to understand what is the impact		1		1												
25																			
26	2	Empower people																	
27		2.1	Simple information to understand how to address the threat		1		1												
28		2.2	Appropriate call to action message		1		1												
29		2.3	Overall conveys a positive message		1			Neutral											
30																			
31	3	Evidence-based content																	
32		3.1	Based on facts, e.g. statistics, etc.		1														
33		3.2	From credible source		1		1	europal											
34																			
35	4	Memorable																	
36		4.1	Micro-learning - specific topic		1		1												
37			Micro-learning - short statements, focus on key points		1		1												
38		4.3	Consider different learning styles		1		1	visual/text											
39		4.4	Balance between graphics and text		1		1												
40		4.5	Audience can easily relate, e.g. storytelling		1		1	Real examples											
41																			
42	<b>Presentation attributes</b>																		
43																			
44	1	Visibility of the message																	
45		1.1	Appropriate location		1		1												
46		1.2	Draw attention to key information, e.g. by using contrasting colour		1		1												
47																			
48	2	Layout, style and formatting																	
49		2.1	Use lines, borders and shapes to group related information		1		1												
50		2.2	Create text hierarchy (up to 3 different font styles)		1		1												
51		2.3	Maximum 4 colours		1		1												
52																			
53	3	Inclusive / Accessible																	
54		3.1	A good color contrast between the text color and background color		1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>											
55		3.2	Use appropriate font style (i)		1		1												
56		3.3	Use appropriate font size (i)		1		1												
57																			
58																			
59																			
60																			
61	<b>Communication Strategy attributes</b>					5													
62	<b>Behaviour-change attributes</b>					10													
63	<b>Presentation attributes</b>					7													
64																			
65	<b>TOTAL</b>					<b>23</b>													
66																			
67	<b>Overall quality of awareness raising material</b>																		
68	<b>Low</b>	0-14																	
69	<b>Medium</b>	15-22																	
70	<b>High</b>	23-28																	
71																			





	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2		<b>Communication Strategy attributes</b>					<b>Evaluation</b>								
3							Infographic - website	<a href="https://www.proofpoint.com/uk/impostor-email-threats-infographic">https://www.proofpoint.com/uk/impostor-email-threats-infographic</a>							
4															
5		1	Audience		Marked		Marked	Comments							
6			1,1 Across groups		1										
7			1,2 Specific		2			2 Employees							
8															
9		2	Key message focus - clear purpose												
10			2,1 Awareness - about threat		1			1 email threats							
11			2,2 Awareness - about impact		1										
12			2,3 Cyber hygiene - best practices		1			1							
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1			1 visit a website to learn more							
14															
15		3	Timeframe												
16			3,1 Generic		1			1							
17			3,2 Covers specific time periods		2										
18															
19															
20		<b>Behaviour-change attributes</b>													
21		1	Promote situational awareness												
22			1,1 Easy to understand what is the threat		1			1							
23			1,2 Easy to understand what is the impact		1										
24															
25															
26		2	Empower people												
27			Simple information to understand how to address the threat		1			1							
28			2,2 Appropriate call to action message		1										
29			2,3 Overall conveys a positive message		1			Neutral							
30															
31		3	Evidence-based content												
32			3,1 Based on facts, e.g. statistics, etc.		1			1 statistics							
33			3,2 From credible source		1										
34															
35		4	Memorable												
36			4,1 Micro-learning - specific topic		1			1							
37			4,2 Micro-learning - short statements, focus on key points		1			1							
38			4,3 Considers different learning styles		1			1 Visual/text							
39			4,4 Balance between graphics and text		1										
40			4,5 Audience can easily relate, e.g. storytelling		1										
41															
42		<b>Presentation attributes</b>													
43		1	Visibility of the message												
44			1,1 Appropriate location		1										
45			Draw attention to key information, e.g. by using contrasting colour		1			1							
46															
47		2	Layout, style and formatting												
48			Uses lines, borders and shapes to group related information		1			1							
49			Create text hierarchy (up to 3 different font styles)		1			1							
50			2,2		1			1							
51			2,3 Maximum of colours		1			1							
52															
53		3	Inclusive / Accessible												
54			A good color contrast between the text color and background color		1			using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>							
55			3,2 Use appropriate font styles ()		1			1							
56			3,3 Use appropriate font size ()		1			1							
57															
58															
59															
60															
61			<b>Communication Strategy attributes</b>					6							
62			<b>Behaviour-change attributes</b>					6							
63			<b>Presentation attributes</b>					6							
64															
65			<b>TOTAL</b>					18							
66															
67			Overall quality of awareness raising material												
68			Low 0-14												
69			Medium 15-22												
70			High 23-28												
71															



A	B	C	D	E	F	G	H	I	J	K	L
1											
2	Communication Strategy attributes				Evaluation						
3					Infographic - website	<a href="https://www.darkowl.com/webpages/infographic-trends-in-the-global-landscape-of-online-scams/">https://www.darkowl.com/webpages/infographic-trends-in-the-global-landscape-of-online-scams/</a>					
4											
5	1	Audience	Marks								
6		1.1	Across groups	1							
7		1.2	Specific	2							
8											
9	2	Key message focus - clear purpose									
10		2.1	Awareness - about threat	1							
11		2.2	Awareness - about impact	1							
12		2.3	Open hygiene - best practices	1							
13			Empowerment - call to action, e.g. visit a website to learn more, to								
14		2.4	report an incident, etc.	1							
15											
16	3	Timeframe									
17		3.1	Generic	1							
18		3.2	Covers specific time periods	2							
19											
20	Behaviour-change attributes										
21	1	Promote situational awareness									
22		1.1	Easy to understand what is the threat	1							
23			Easy to understand what is the								
24		1.2	impact	1							
25											
26	2	Empower people									
27			Simple information to understand								
28		2.1	how to address the threat	1							
29		2.2	Appropriate call to action message	1							
30		2.3	Overall convey a positive message	1							
31											
32	3	Evidence-based content									
33		3.1	Based on facts, e.g. statistics, etc.	1							
34		3.2	From credible source	1							
35											
36	4	Memorable									
37		4.1	Micro-learning - specific topics	1							
38			Micro-learning - short statements,								
39		4.2	focus on key points	1							
40		4.3	Consider different learning styles	1							
41		4.4	Balance between graphics and text	1							
42		4.5	Audience can easily relate, e.g. storytelling	1							
43											
44	Presentation attributes										
45	1	Mobility of the message									
46		1.1	Appropriate location	1							
47			Draw attention to key information,								
48		1.2	e.g. by using contrasting colour	1							
49											
50	2	Layout, style and formatting									
51			Use lines, borders and diags to								
52		2.1	group related information	1							
53			Create text hierarchy (up to 3)								
54		2.2	different text styles	1							
55		2.3	Maximum 4 colours	1							
56											
57	3	Inclusive / Accessible									
58			Aligned color contrast between the								
59		3.1	text color and background color	1							
60		3.2	Use appropriate font size(s)	1							
61		3.3	Use appropriate font size(s)	1							
62											
63											
64											
65											
66											
67											
68											
69											
70											
71											
72											
73											
74											
75											
76											
77											
78											
79											
80											
81											
82											
83											
84											
85											
86											
87											
88											
89											
90											
91											
92											
93											
94											
95											
96											
97											
98											
99											
100											
101											
102											
103											
104											
105											
106											
107											
108											
109											
110											
111											
112											
113											
114											
115											
116											
117											
118											
119											
120											
121											
122											
123											
124											
125											
126											
127											
128											
129											
130											
131											
132											
133											
134											
135											
136											
137											
138											
139											
140											
141											
142											
143											
144											
145											
146											
147											
148											
149											
150											
151											
152											
153											
154											
155											
156											
157											
158											
159											
160											
161											
162											
163											
164											
165											
166											
167											

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1														
2	<b>Communication Strategy attributes</b>				<b>Evaluation</b>									
3					Infographic - website	<a href="https://www.fintbank.net/home/resources/online-security-privacy/fakecheckscams">https://www.fintbank.net/home/resources/online-security-privacy/fakecheckscams</a>								
4														
5	1	Audience		Marks		Marks	Comments							
6		1,1	Across groups	1										
7		1,2	Specific	2										
8														
9	2	Key message focus - clear purpose												
10		2,1	Awareness - about threat	1			1 check scams							
11		2,2	Awareness - about impact	1			1 the scammer has your money							
12		2,3	Cyber hygiene - best practices	1										
13		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1 report the incident							
14														
15	3	Timeframe												
16		3,1	Generic	1			1							
17		3,2	Covers specific time periods	2										
18														
19														
20	<b>Behaviour-change attributes</b>													
21														
22	1	Promote situational awareness												
23		1,1	Easy to understand what is the threat	1			1							
24		1,2	Easy to understand what is the impact	1			1							
25														
26	2	Empower people												
27		2,1	Simple information to understand how to address the threat	1			1							
28		2,2	Appropriate call to action message	1			1							
29		2,3	Overall conveys a positive message	1			Neutral							
30														
31	3	Evidence-based content												
32		3,1	Based on facts, e.g. statistics, etc.	1										
33		3,2	From credible source	1										
34														
35	4	Memorable												
36		4,1	Micro-learning - specific topic	1			1							
37		4,2	Micro-learning - short statements, focus on key points	1										
38		4,3	Consider different learning styles	1			1 Visual/text							
39		4,4	Balance between graphics and text	1										
40		4,5	Audience can easily relate, e.g. storytelling	1			1 real examples							
41														
42	<b>Presentation attributes</b>													
43														
44	1	Visibility of the message												
45		1,1	Appropriate location	1										
46		1,2	Draw attention to key information, e.g. by using contrasting colour	1			1							
47														
48	2	Layout, style and formatting												
49		2,1	Uses lines, borders and shapes to group related information	1			1							
50		2,2	Create text hierarchy (up to 3 different font styles)	1			1							
51		2,3	Maximum 4 colours	1			1							
52														
53	3	Inclusive / Accessible												
54		3,1	A good color contrast between the text color and background color	1			1 using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>							
55		3,2	Use appropriate font styles ()	1			1							
56		3,3	Use appropriate font size ()	1			1							
57														
58														
59														
60														
61														
62														
63														
64														
65														
66														
67														
68														
69														
70														
71														
72														



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1														
2			<b>Communication Strategy attributes</b>				<b>Evaluation</b>							
3							Infographic - website	<a href="https://www.diderhans.net/NutshellAgarwal181/phishinginfographic-257295671">https://www.diderhans.net/NutshellAgarwal181/phishinginfographic-257295671</a>						
4														
5		1	Audience		Marked		Marked	Comments						
6			1,1 Across groups		1			1						
7			1,2 Specific		2									
8														
9		2	Key message focus - clear purpose											
10			2,1 Awareness - about threat		1			1	phishing attack					
11			2,2 Awareness - about impact		1									
12			2,3 Cyber hygiene - best practices		1			1						
13			Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1									
14														
15		3	Timeframe											
16			3,1 Generic		1			1						
17			3,2 Covers specific time periods		2									
18														
19														
20			<b>Behaviour-change attributes</b>											
21														
22		1	Promote situational awareness											
23			1,1 Easy to understand what is the threat		1			1						
24			1,2 Easy to understand what is the impact		1									
25														
26		2	Empower people											
27			Simple information to understand how to address the threat		1			1						
28			Appropriate call to action message		1			1						
29			Overall conveys a positive message		1			Neutral						
30														
31		3	Evidence-based content											
32			3,1 Based on facts, e.g. statistics, etc.		1									
33			3,2 From credible source		1									
34														
35		4	Memorable											
36			4,1 Micro-learning - specific topic		1			1						
37			Micro-learning - short statements, focus on key points		1									
38			4,3 Considers different learning styles		1			1	Visual/text					
39			4,4 Balance between graphics and text		1									
40			Audience can easily relate, e.g. storytelling		1			1	actions to help to prevent to be hooded					
41														
42			<b>Presentation attributes</b>											
43														
44		1	Visibility of the message											
45			1,1 Appropriate location		1			1						
46			Draw attention to key information, e.g. by using contrasting colour		1			1						
47														
48		2	Layout, style and formatting											
49			Uses lines, borders and shapes to group related information		1			1						
50			Create text hierarchy (up to 3 different font styles)		1			1						
51			Maximum 4 colours		1			1						
52														
53		3	Inclusive / Accessible											
54			A good color contrast between the text color and background color		1			1	using <a href="https://webaim.org/resources/contrastchecker/">https://webaim.org/resources/contrastchecker/</a>					
55			Use appropriate font styles (i)		1			1						
56			Use appropriate font size (i)		1			1						
57														
58														
59														
60														
61			Communication Strategy attributes			4								
62			Behaviour-change attributes			6								
63			Presentation attributes			0								
64														
65						<b>TOTAL</b>		10						
66														
67			Overall quality of awareness raising material											
68			Low			0-14								
69			Medium			15-22								
70			High			23-28								
71														

**4 ACTIONS TO HELP PREVENT BEING HOOKED IN A PHISHING ATTACK**

**BLOCK THE BAIT**

1. Don't click on suspicious links or attachments in emails or text messages.
2. Don't click on links or attachments in social media posts or messages.
3. Don't click on links or attachments in pop-up windows or ads.
4. Don't click on links or attachments in search engine results.

**DON'T TAKE THE BAIT**

1. Don't provide personal information to anyone who asks for it.
2. Don't provide your password to anyone who asks for it.
3. Don't provide your credit card information to anyone who asks for it.
4. Don't provide your bank account information to anyone who asks for it.

**REPORT THE HOOK!**

1. Report suspicious emails to your IT department or the FBI.
2. Report suspicious social media posts to the platform.
3. Report suspicious text messages to your carrier.
4. Report suspicious pop-up windows or ads to the browser.

**PROTECT THE WATERS**

1. Use strong, unique passwords for all accounts.
2. Enable two-factor authentication for all accounts.
3. Keep your software and operating system up to date.
4. Use a reputable antivirus program.
5. Use a secure network connection.
6. Use a secure email provider.
7. Use a secure search engine.
8. Use a secure social media platform.
9. Use a secure text messaging service.
10. Use a secure pop-up window or ad.











# Bibliography

- [1] Knowbe4. Knowbe4. [Online].  
<https://www.knowbe4.com/phishing>
- [2] SecureTeam. (2022, May) Phishing Report 2022: Which Individuals Are Most at Risk. [Online].  
<https://secureteam.co.uk/articles/phishing-report-2022-which-individuals-are-most-at-risk/>
- [3] Critical Insight. Critical Insight. [Online].  
<https://www.criticalinsight.com/resources/news/article/the-attackers-playbook-phishing>
- [4] Global Knowledge. (2022) Cybersecurity Awareness Post. [Online].  
<https://www.globalknowledge.com/us-en/topics/cybersecurity/cybersecurityawarenessposters/#gref>
- [5] SANS Institute. (2022) Posters. [Online].  
<https://www.sans.org/security-awarenesstraining/resources/posters>
- [6] B. B. Gupta, Nailin A.G. Arachchilage, Kostas E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication Systems*, 2018.
- [7] Inspired eLearning. (2018) Inspired eLearning. [Online].  
<https://inspiredelearning.com/resource/social-media-phishing-infograp>
- [8] Sam Cook. (2022, October) Comparitech. [Online].  
<https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/>
- [9] Panda Security. (2018) Panda Security Mediacenter. [Online].  
<https://www.pandasecurity.com/en/mediacenter/panda-security/social-media-scams/?amp=1>
- [10] Marija. (2022, October) Truelist. [Online].  
<https://truelist.co/blog/phishing-statistics/>
- [11] Office for National Statistics. (2022, September) Office for National Statistics. [Online].  
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26>

- [12] Security Magazine. (April, 2020) Security. [Online].  
<https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020>
- [13] Brenda R. Sharton. (2020, March) Harvard Business Review Home. [Online]. <https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks>
- [14] Help Net Security. (2022, June) Help Net Security. [Online].  
<https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks/>
- [15] Lucy Harrison. (2021, January) UK Web Host Review. [Online].  
<https://www.ukwebhostreview.com/phishing-statistics/>
- [16] C. Goggi. (2013, December) The 13 worst security threats of 2013," Decem-. [Online]. <http://www.gfi.com/blog/the-13-worst-security-threats-of-2013/>
- [17] James Mackay. (2022, September) Metacompliance. [Online].  
<https://www.metacompliance.com/blog/phishing-and-ransomware/identify-spear-phishing-attack>
- [18] Europol. (2022, May) Europol. [Online].  
<https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/take-control-of-your-digital-life-don%e2%80%99t-be-victim-of-cyber-scams>
- [19] Daniel Brecht. (2019, February) Infosec. [Online].  
<https://resources.infosecinstitute.com/topic/who-is-being-targeted-by-phishers/>
- [20] University of Miami's Department of Information Technology. University of Miami's Department of Information Technology. [Online]. <https://www.it.miami.edu/about-umit/it-news/phishing/dont-get-phished/index.html>
- [21] Juliana De Groot. (2022, December) Digital Guardian. [Online].  
<https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks>
- [22] Jeb Webb, Syed Wajid Ali Shah, Mohammad Reza Nosouhi, Jongkil Jay Jeong, Ashish Nanda. (2022, November) The Conversation. [Online]. <https://theconversation.com/crypto-scams-will-increase-over-the-holidays-heres-what-you-need-to-know-to-not-fall-victim-194064>
- [23] Sherrod Degrippo. (2020, February) Proofpoint. [Online].  
<https://www.proofpoint.com/us/corporate-blog/post/attackers-expand-coronavirus-themed-attacks-and-prey-conspiracy-theoriesd-coronavirus-themed-attacks-and-prey-conspiracy->

[theories?utm\\_post\\_id=b41a3f93-7d39-48e6-8a75-79fedc3148ec&utm\\_social\\_network=twitter](https://news.trendmicro.com/2021/03/05/covid-19-scams-how-they-work-and-how-to-avoid-them/)

- [24] Trendmicro. (2021, March) Trendmicro. [Online].  
<https://news.trendmicro.com/2021/03/05/covid-19-scams-how-they-work-and-how-to-avoid-them/>
- [25] Stu Sjouwerman. (2021) KnowBe4. [Online]. ;  
[blog.knowbe4.com/infographic- q4- 2020- work- fromhome-phishing-emails-on-the-rise.](https://blog.knowbe4.com/infographic-q4-2020-work-from-home-phishing-emails-on-the-rise)
- [26] Equifax. (2018) Equifax. [Online].  
<https://www.equifax.co.uk/resources/identity-protection/older-people-and-scams.html>
- [27] Age UK. (2018, March) Age UK. [Online].  
[https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb\\_mar18\\_applying\\_the\\_brakes.pdf](https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf)
- [28] Dailyinfographic. (2020, June) Dailyinfographic. [Online].  
<https://www.dailyinfographic.com/risk-of-senior-scams>
- [29] ACCC. (2016, May) ACCC. [Online].  
<https://www.accc.gov.au/media-release/australians-lose-over-229-million-to-scams-in-2015>
- [30] Denise Purtzer. (2021, December) Retail Touch Points. [Online].  
<https://www.retailtouchpoints.com/topics/security/does-customer-age-matter-for-fraud-prevention>
- [31] Seth Ryan. (2022, October) Ryan Investigations. [Online].  
<https://lawrenceryaninvestigations.com/blog/a-step-by-step-guide-on-reporting-financial-fraud/>
- [32] As our parents age. (2015, April) As our parents age. [Online].  
<https://asourparentsage.net/2015/04/03/perfect-infographic-on-scams-print-put-together-post/>
- [33] Sunil Chaudhary, Sebastian Pape, Marko Kompara, Vasileios Gkioulos, "Properties for Cybersecurity Awareness Posters' Design and Quality Assessment," in *Conference acronym 'XX*, New York, 2018, pp. 03-05.
- [34] Ann Smarty. (2020, February) Venngage. [Online].  
<https://venngage.com/blog/accessible-infographics/>
- [35] Simpplr. (2023) Simpplr. [Online].  
<https://www.simpplr.com/glossary/strategic-communications/>

- [36] Katy French. Column five. [Online].  
<https://www.columnfivemedia.com/3-ways-infographics-engage-your-audience/>
- [37] Olivia Mitchell. (2018) Olivia Mitchell. [Online].  
<https://speakingaboutpresenting.com/content/memorable-key-message-10-minutes/#:~:text=A%20key%20message%20is%20the,deciding%20on%20your%20key%20message.>
- [38] Ollis,Akers,Arney. (2022, July) Ollis/ Akers/ Arney. [Online].  
<https://ollisakersarney.com/blog/cyber-hygiene-best-practices/>
- [39] IcoGrams. ICOGRAMS. [Online]. <https://icograms.com/usage-timeline-infographics#:~:text=A%20timeline%20infographic%20is%20a,%2C%20strategic%20reports%2C%20and%20presentations.>
- [40] Flashpoint. (2020, October) Flashpoint. [Online].  
<https://flashpoint.io/blog/what-is-situational-awareness/>
- [41] Lumen. (2017) Lumen. [Online].  
[https://courses.lumenlearning.com/wm-businesscommunicationmgrs/chapter/the-right-message/?fbclid=IwAR0bTMvP-40q7il1HYXTftwxM6yUBdMNHY1H3PF\\_21Y1SMO6whKGUHLlqX4](https://courses.lumenlearning.com/wm-businesscommunicationmgrs/chapter/the-right-message/?fbclid=IwAR0bTMvP-40q7il1HYXTftwxM6yUBdMNHY1H3PF_21Y1SMO6whKGUHLlqX4)
- [42] Midori Nediger. (July, 2022) Venngage. [Online].  
<https://venngage.com/blog/what-is-an-infographic/?fbclid=IwAR04QA6-pc5A4jrMuMcBkPmwBqGq3xLwGjSC6lFcO40sY6jwdyMr-4bicRw>
- [43] Infogram. Infogram. [Online].  
<https://infogram.com/page/infographic?fbclid=IwAR1-5ULGjSGeV8OpfjRv3PCsPK31WvbO7iptQwvb3ndhll1A2-my1lCmoAE>
- [44] Web accessibility in mind. (2023) Web accessibility in mind. [Online]. <https://webaim.org/resources/contrastchecker/>
- [45] Bureau of Internet Accessibility. (2017, May) Bureau of Internet Accessibility. [Online]. <https://www.boia.org/blog/best-fonts-to-use-for-website-accessibility>
- [46] Designshack. Designshack. [Online].  
<https://designshack.net/articles/layouts/how-to-balance-text-and-visual-content-in-design/?fbclid=IwAR1-5ULGjSGeV8OpfjRv3PCsPK31WvbO7iptQwvb3ndhll1A2-my1lCmoAE>

- [47] Jacci Howard Bear. (2019, December) Thoughtco. [Online]. <https://www.thoughtco.com/balance-in-design-1078231>
- [48] StatSilk. StatSilk's. [Online]. <https://www.statsilk.com/blog/real-difference-between-infographics-and-data-visualizations#:~:text=Both%20are%20visual%20representations%20of,elements%20like%20narrative%20and%20graphics>.
- [49] Lydia Hooper. (2021, February) Venngage. [Online]. <https://venngage.com/blog/good-infographic/>
- [50] Bureau of Internet Accessibility. (2021, February) Bureau of Internet Accessibility. [Online]. <https://www.boia.org/blog/using-infographics-while-keeping-your-site-accessible>
- [51] Vision Australia. Vision Australia. [Online]. <https://www.visionaustralia.org/business-consulting/digital-access/resources/colour-contrast-analyser>
- [52] Government of South Australia logo. (2021, June) Government of South Australia logo. [Online]. <https://www.accessibility.sa.gov.au/your-role/visual-design/colour-and-contrast>
- [53] Chelsea Yang | . Edraw. [Online]. <https://www.edrawsoft.com/infographics/infographic-layout-templates.html?fbclid=IwAR23i7ao0PCJIqfjEfJKcxwGSBk9UI7wA3qE21DMKLzsF8VFyCUflfXpIEI>
- [54] Cameron Chapman. Designers. [Online]. <https://www.toptal.com/designers/typography/typographic-hierarchy>
- [55] Hailey Hudson. (2021, December) Visme. [Online]. <https://visme.co/blog/infographic-color-schemes/#:~:text=Decide%20on%20A%20Number%20of%20Colors&text=But%20too%20few%20colors%20will,the%20graphic%20easier%20to%20follow>.
- [56] Computer Graphics Design. (2023, April) LinkedIn. [Online]. <https://www.linkedin.com/advice/0/how-do-you-test-improve-usability-accessibility-1e>
- [57] The University of North Carolina at Greensboro. (2019) The University of North Carolina at Greensboro. [Online]. <https://accessibility.uncg.edu/getting-started-with-accessibility/accessible-design/>

- [58] Dallas College. Dallas College. [Online].  
<https://www.dallascollege.edu/about/accessibility/guidelines/pages/color-contrast.aspx>
- [59] Midori Nediger. (2018, January) Venngage. [Online].  
<https://venngage.com/blog/how-to-choose-fonts/#:~:text=Fonts%20for%20print%20infographics%20should,highly%20readable%2C%20and%20highly%20legible>
- [60] Office for National Statistics. (September, 2022) Office for National Statistics. [Online].  
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26>
- [61] Bureau of Internet Accessibility. (2021, October) Bureau of Internet Accessibility. [Online]. <https://www.boia.org/blog/designing-for-color-contrast-guidelines-for-accessibility#:~:text=Designing%20for%20Color%20Contrast%3A%20Guidelines%20for%20Accessibility%201,text%20contrast%20ratio%20of%207%3A1.%20.%20More%20items>