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
Ιλιάνα 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
Ιλιάνα 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 COVIT-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

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.

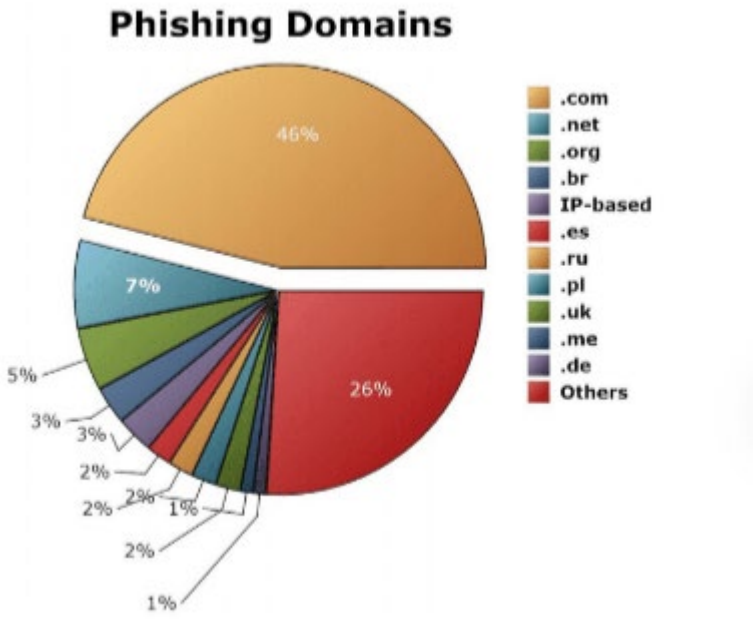


Figure 2.1.2: Statistics of phishing websites based on domain by E-crime Report 2013 Q4.

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]

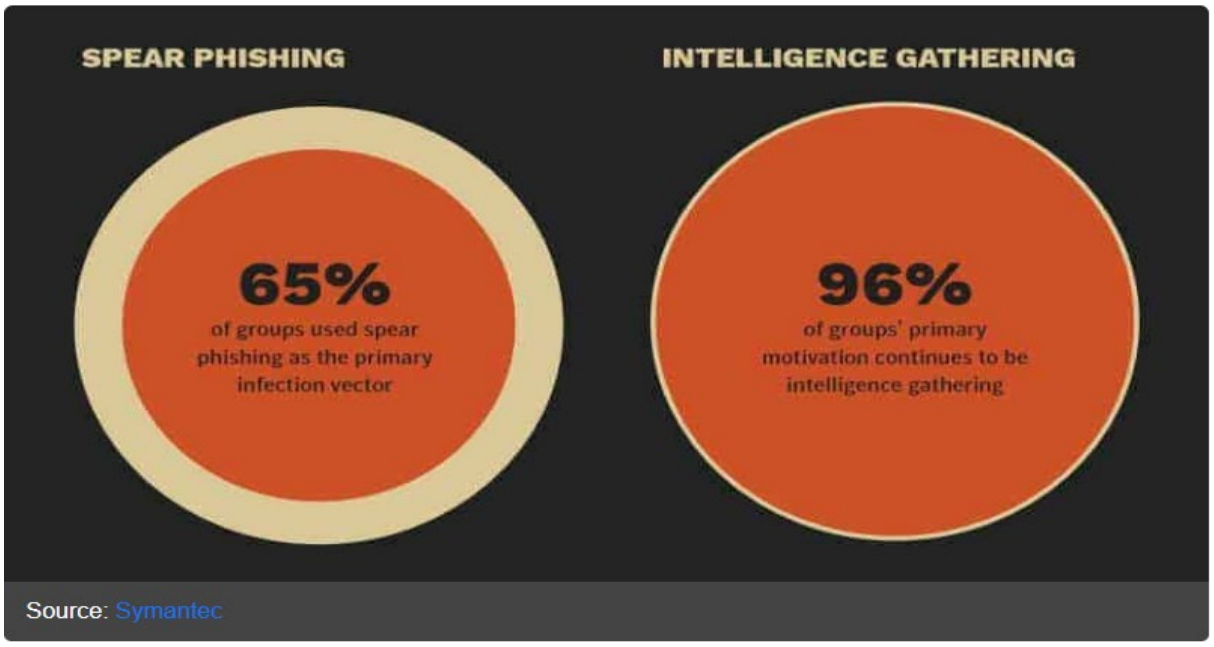


Figure 2.1.4: Symantec statistics about Spear phishing. [8]

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'.

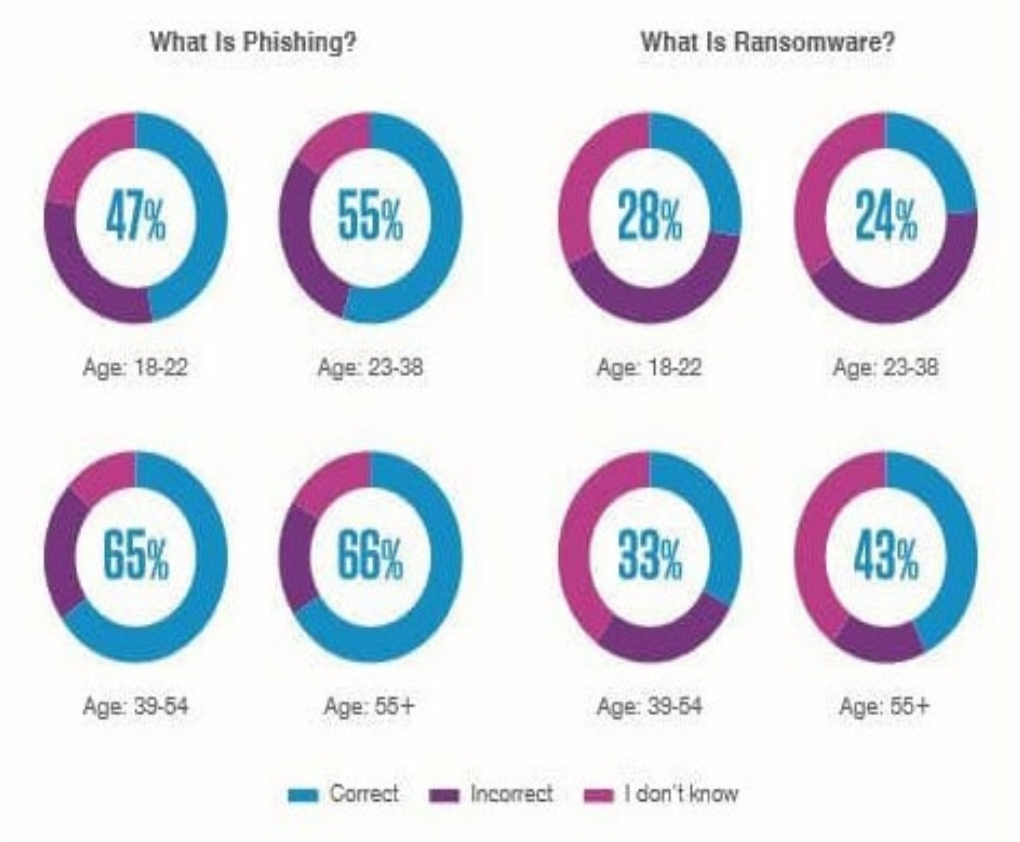


Figure 2.1.5: Knowledge of phishing terms varies among generations. [8]

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

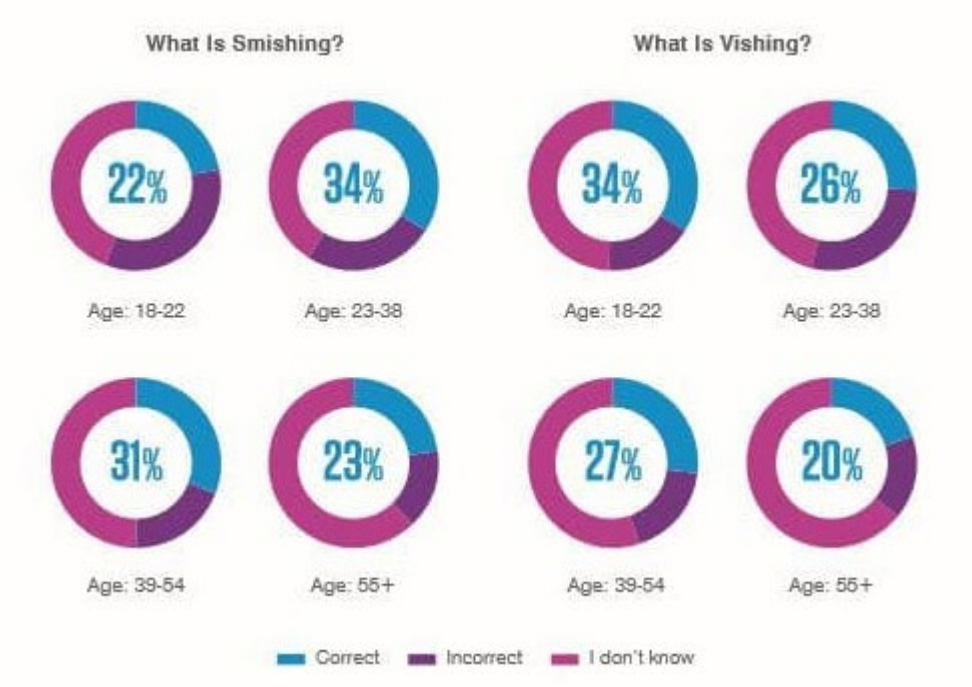


Figure 2.1.6: Smishing terms charts [8]

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.

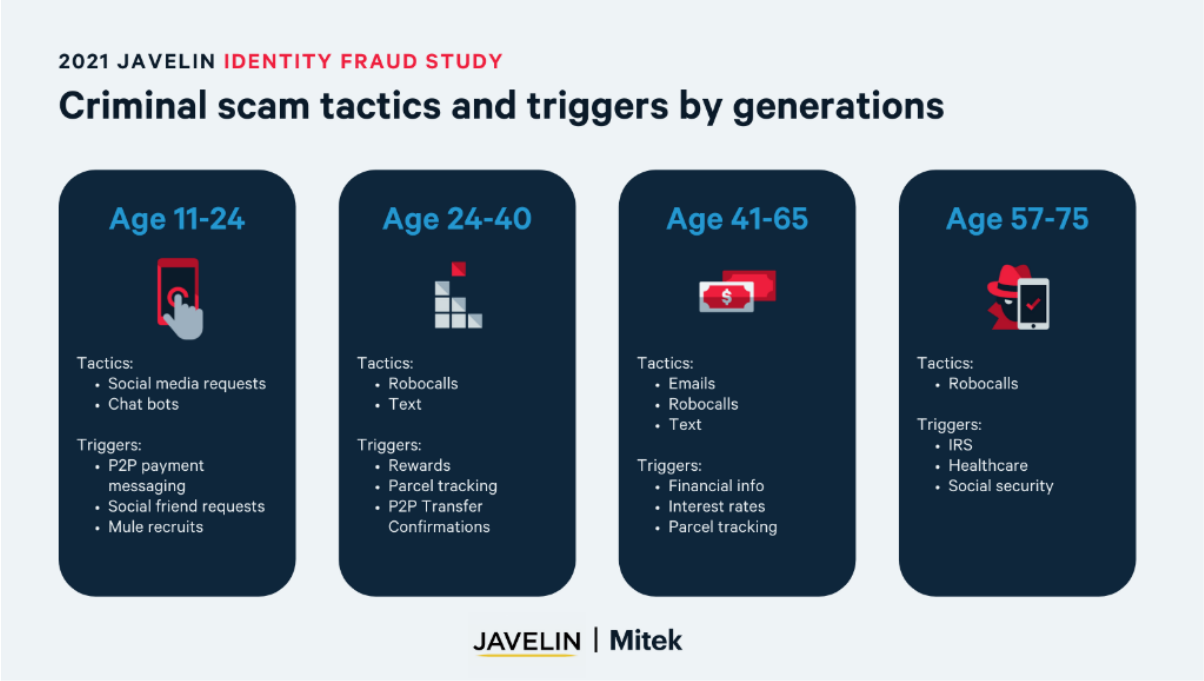


Figure 2.1.7: 4 types of generational fraud victims [10]

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

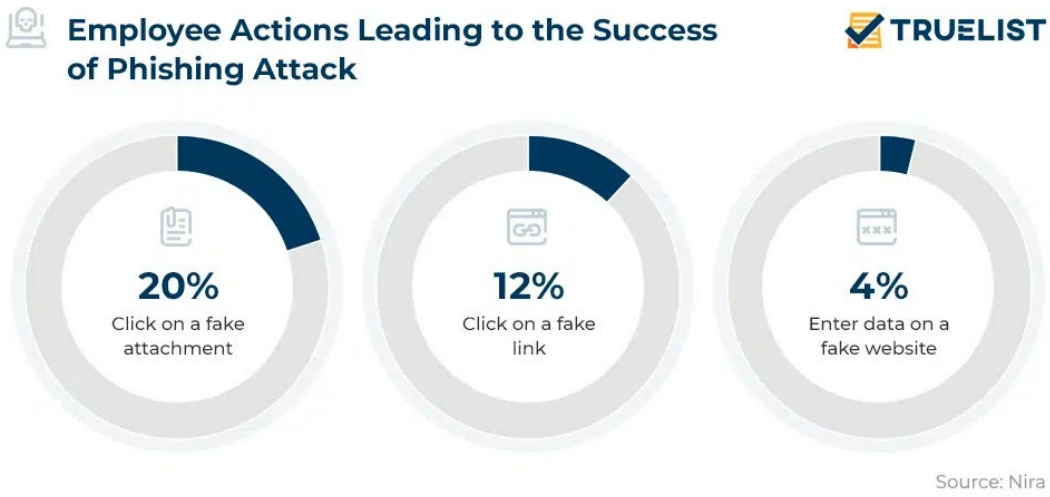


Figure 2.1.8: Employee Actions Leading to the Success of Phishing Attacks [10]

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.

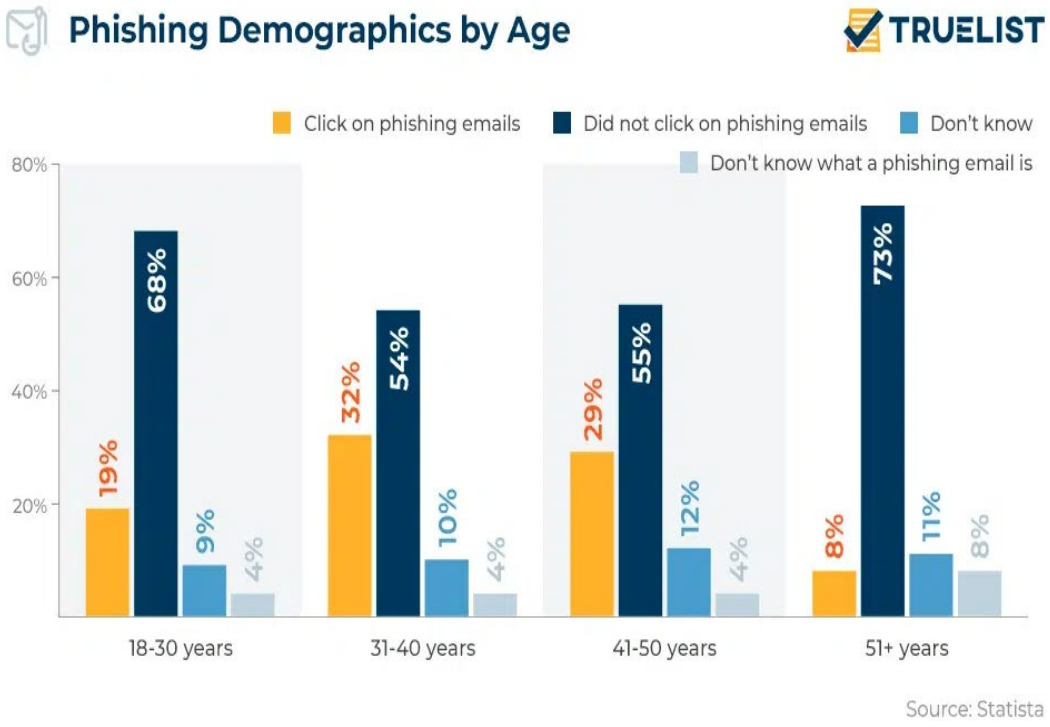


Figure 2.1.9: Phishing Demographics by Age [10]

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%).

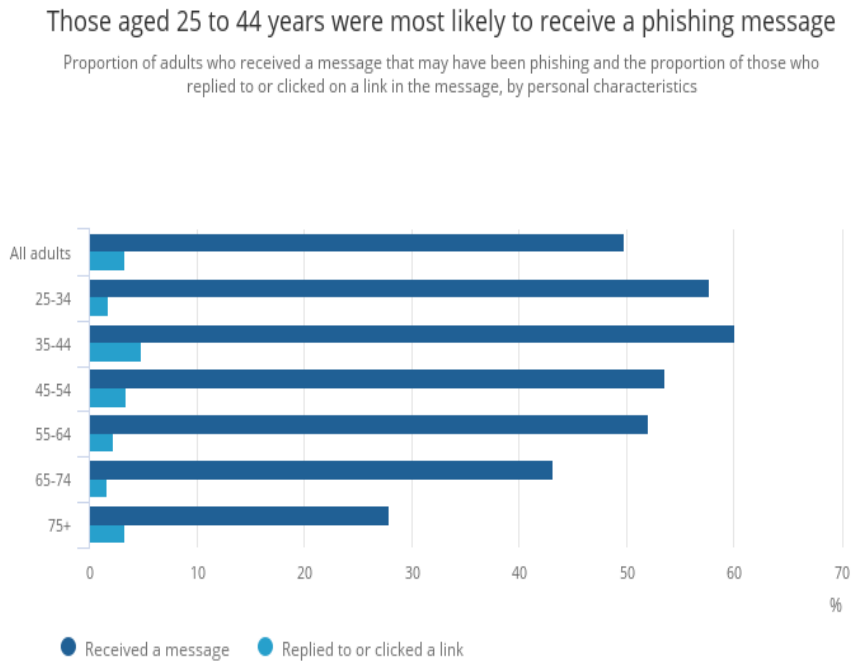


Figure 2.1.10: Proportion of adults who received a message that may have been phishing and the proportion of those who replied to or clicked on a link in the message, by personal characteristics [11]

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.

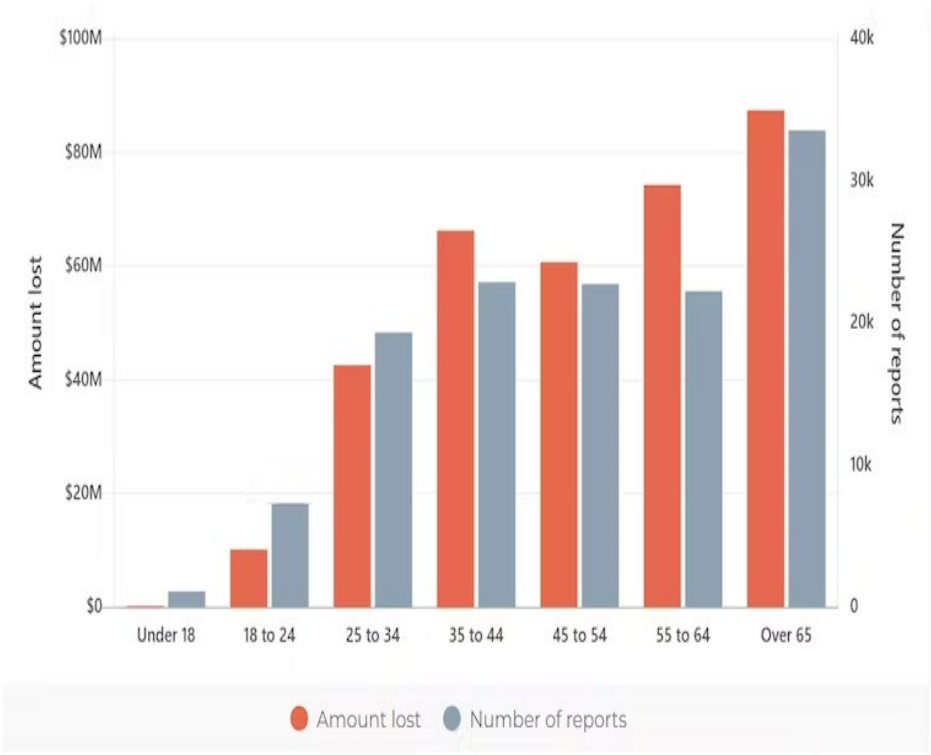


Figure 2.1.11: Age groups of scam victims on holidays.

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.

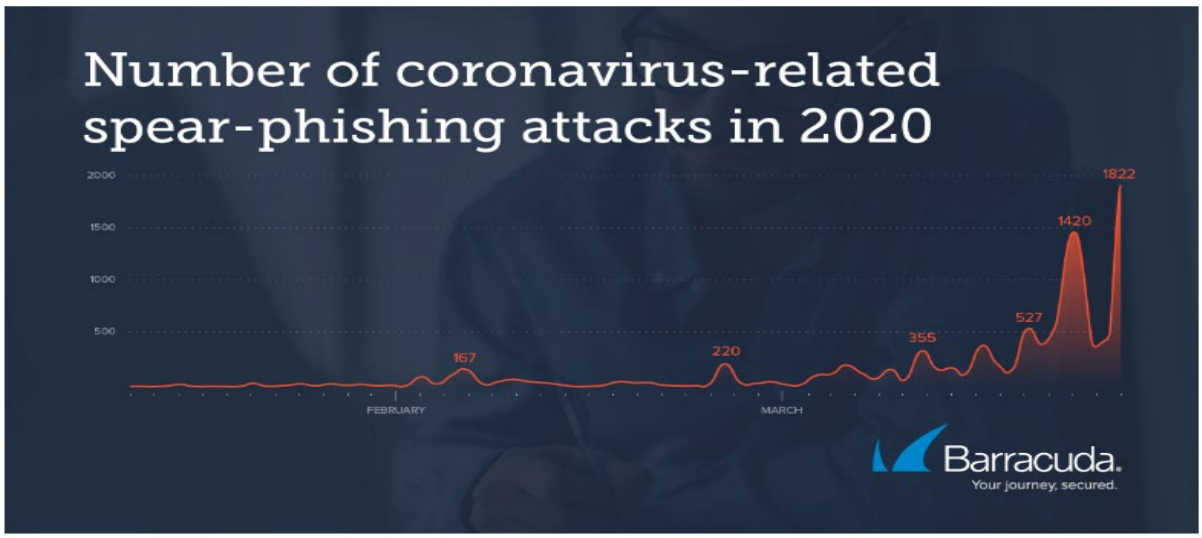


Figure 2.1.12: Spear phishing attacks related on Covid-19 [14]

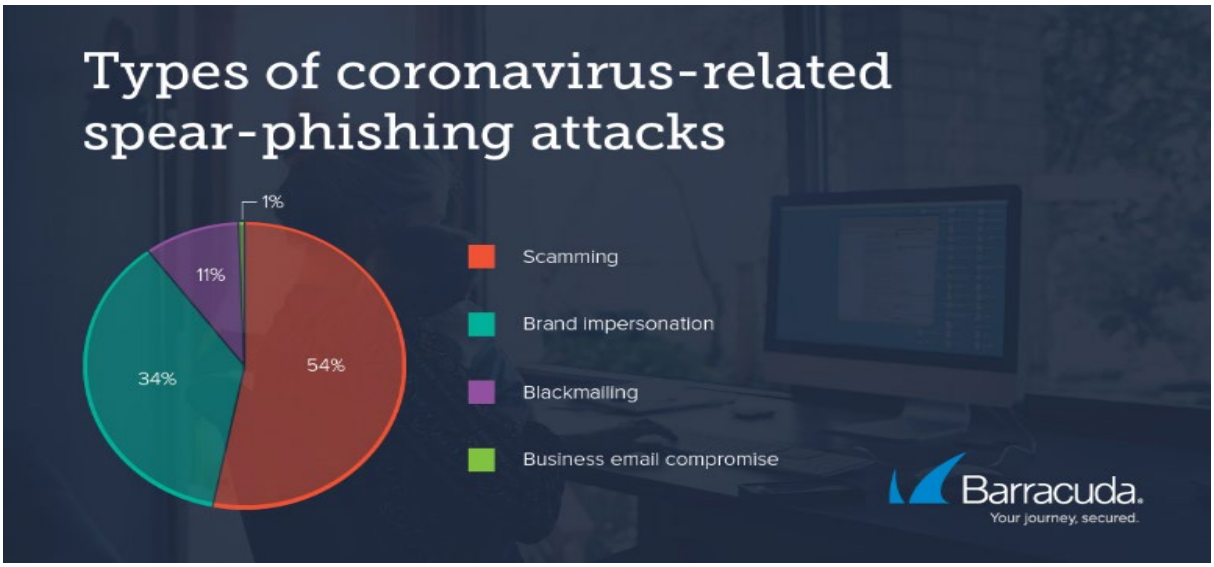


Figure 2.1.13: Types of **s**pear phishing attacks related on Covid-19 [14]

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.

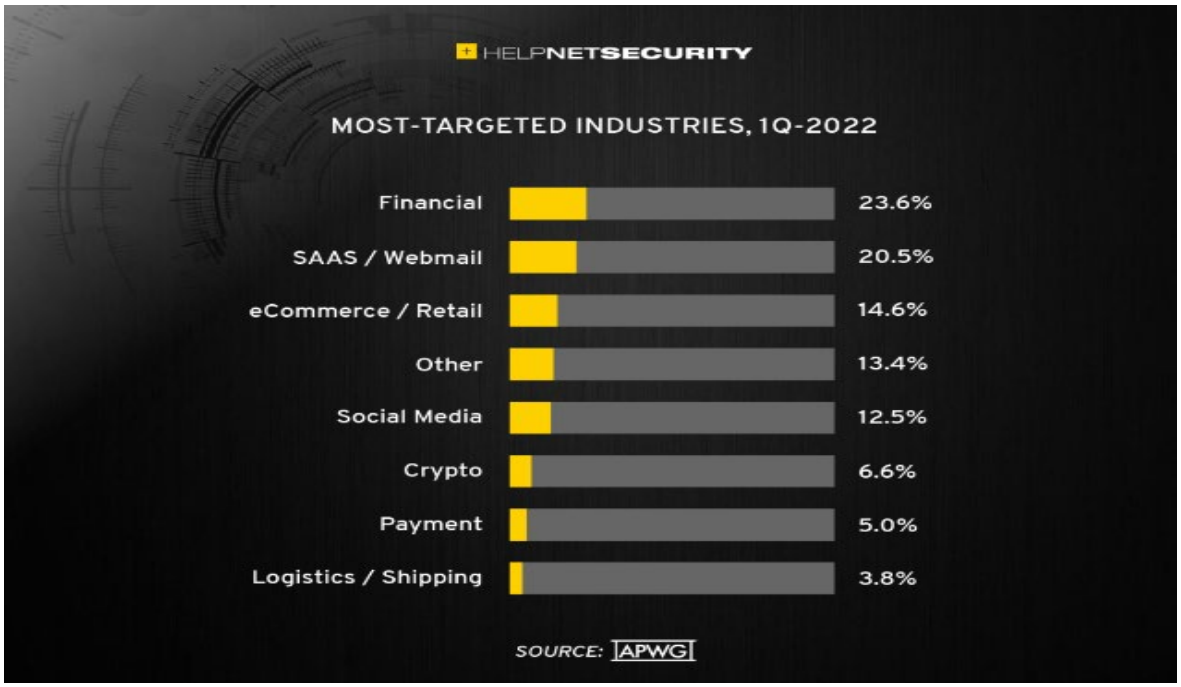


Figure 2.1.14: Trends of Phishing Attacks on 2022 by Help Net Security [14]

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.

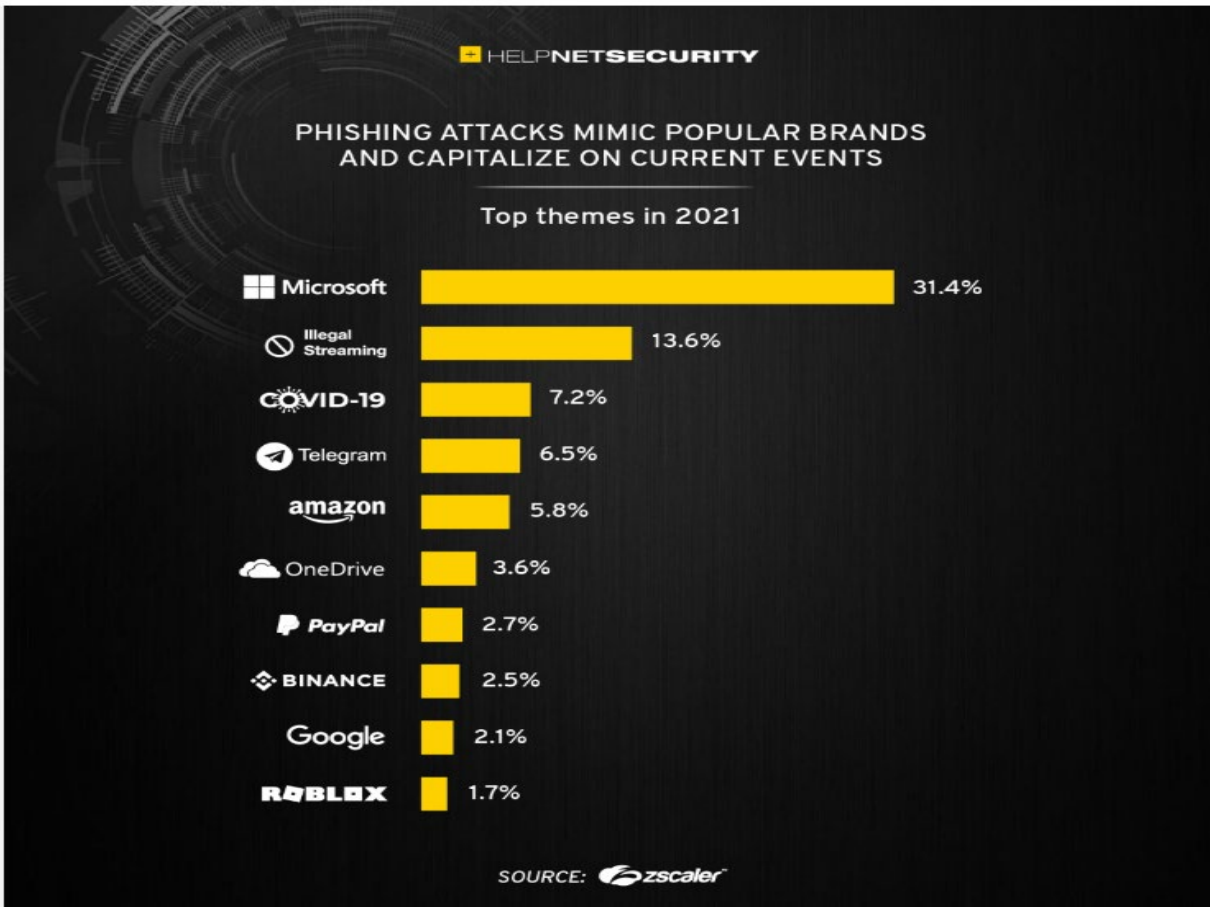


Figure 2.1.15: Phishing attacks mimic popular brands and capitalize on current events 2021 by Help Net Security [14]

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
Email	▪ An Unfamiliar Tone or Greeting ▪ Grammar and Spelling Errors ▪ Inconsistencies in Email Addresses, Links & Domain Names ▪ Threats or a Sense of Urgency ▪ Suspicious Attachments ▪ Request for Credentials, Payment Information or Other Personal Details ▪ Unusual Request	▪ Holidays ▪ Lottery ▪ Covid-19 ▪ Health	Malicious phishing	Girls Seniors Seniors
Smishing attacks	▪ Unknown/ hidden numbers ▪ The (pretended) sender. Institutions such as banks, IRS and debt collectors ▪ Clicking on a link or calling a phone number provided, to clear up the error			▪ 18-25 years old ▪ Men ▪ People with higher curiosity, urgency, and stress levels are more likely to be victims of text scams
Vishing attacks	▪ Never share or confirm your personal details over the phone, even if the person calling is claiming to be your bank. ▪ Don't answer calls from numbers you don't know.			▪ Seniors

Spear Phishing	▪ Check sender email address and name ▪ Check the email format ▪ Verify shared links		Targeted	▪ Seniors

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.

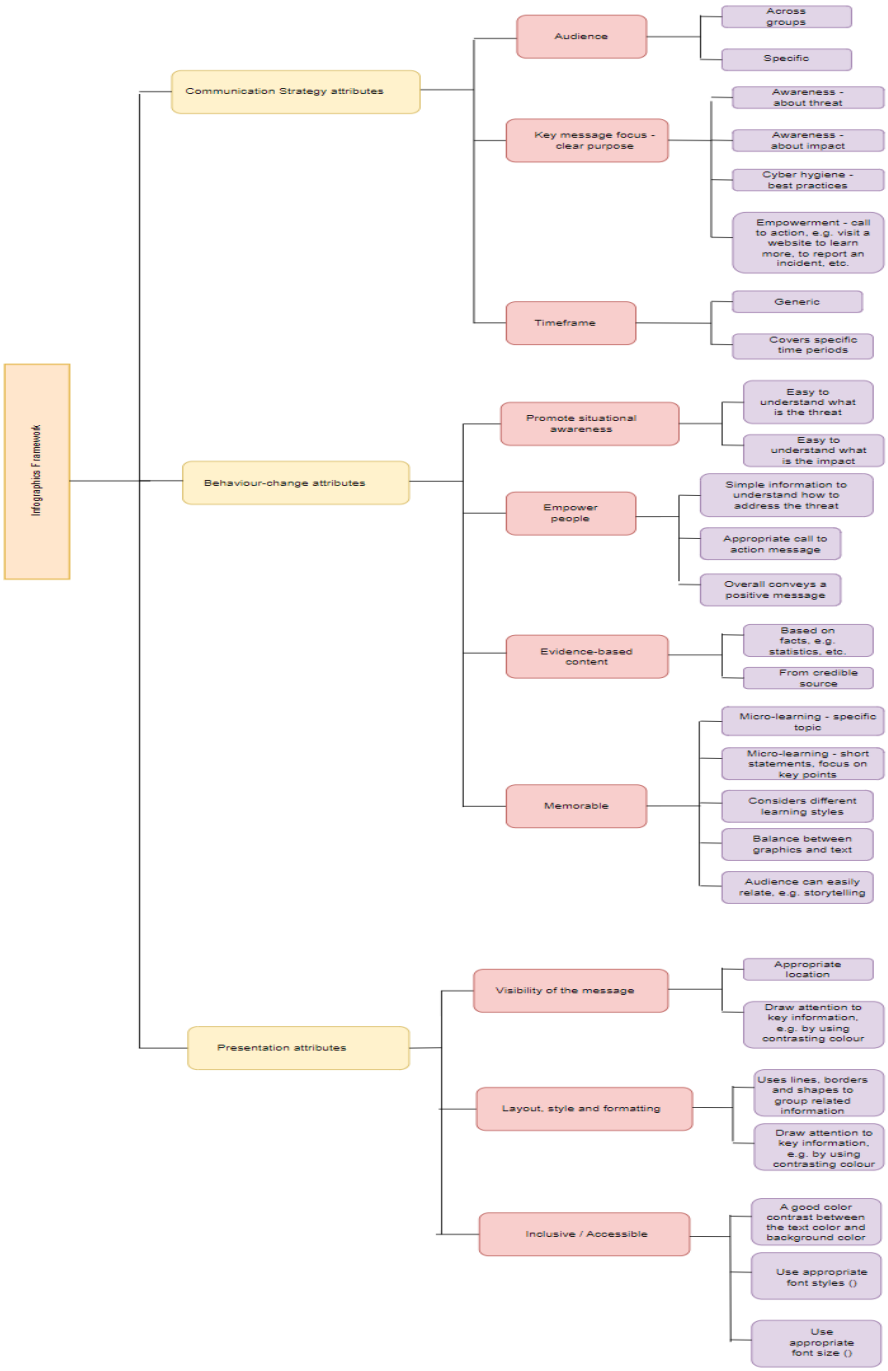


Figure 3.1: Infographics framework

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 coneys 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		**Communication Strategy attributes**					**Evaluation**			
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		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 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		**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						
55		3,2	Use appropriate font styles ()	1						
56		3,3	Use appropriate font size ()	1						
57										
58										
59										
60										
61		**Communication Strategy attributes**				0				
62		**Behaviour-change attributes**				0				
63		**Presentation attributes**				0				
64										
65				**TOTAL**		0				
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.

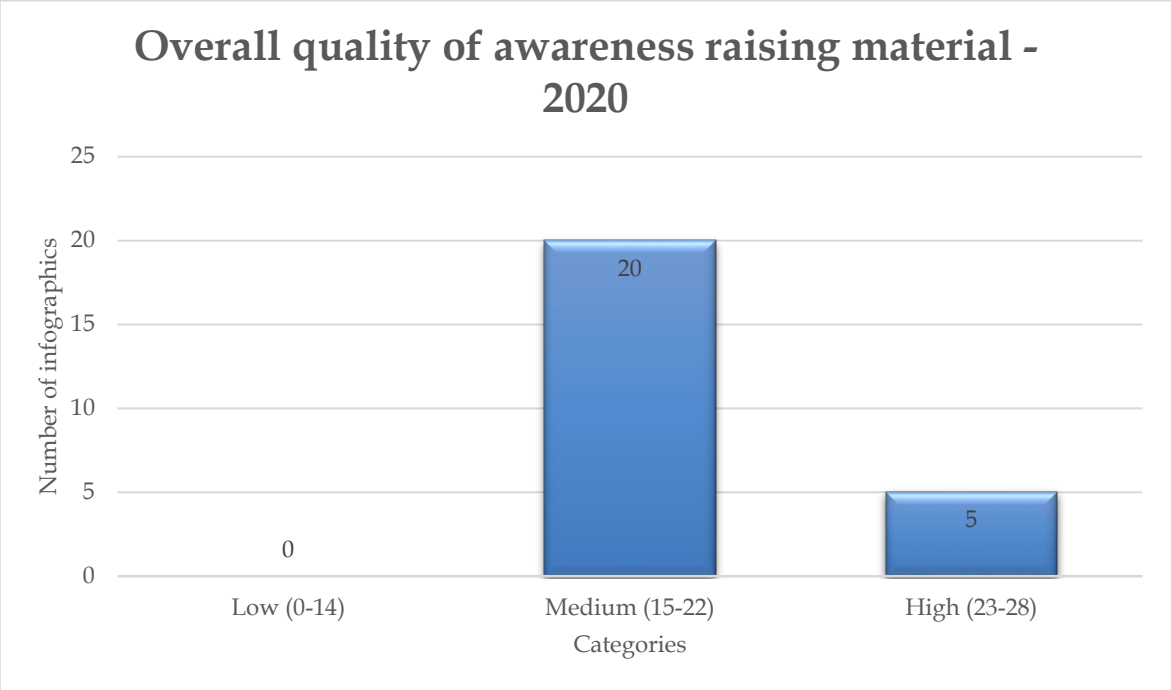


Figure 5.1: Chart of overall quality of awareness raising material - 2020

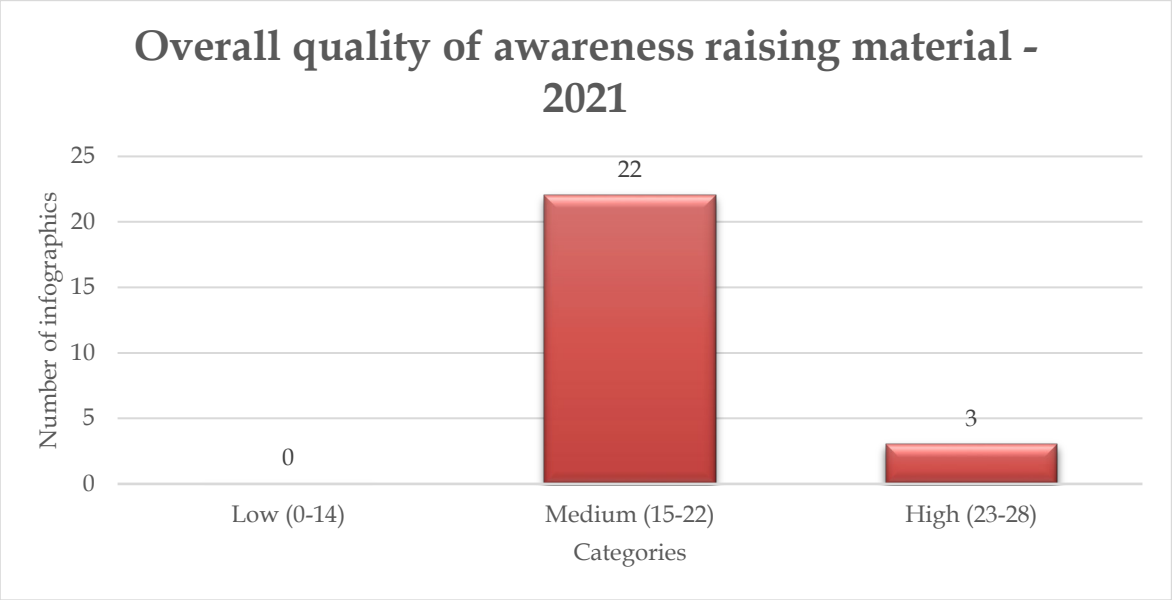


Figure 5.2: Chart of overall quality of awareness raising material - 2021

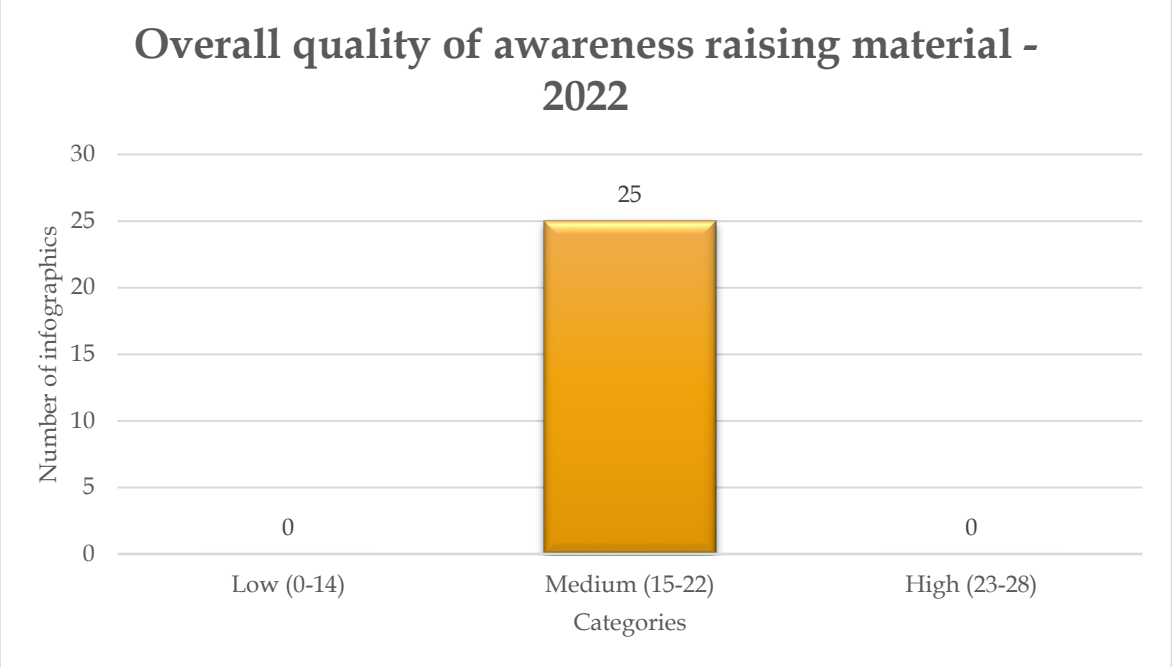


Figure 5.3: Chart of overall quality of awareness raising material - 2022

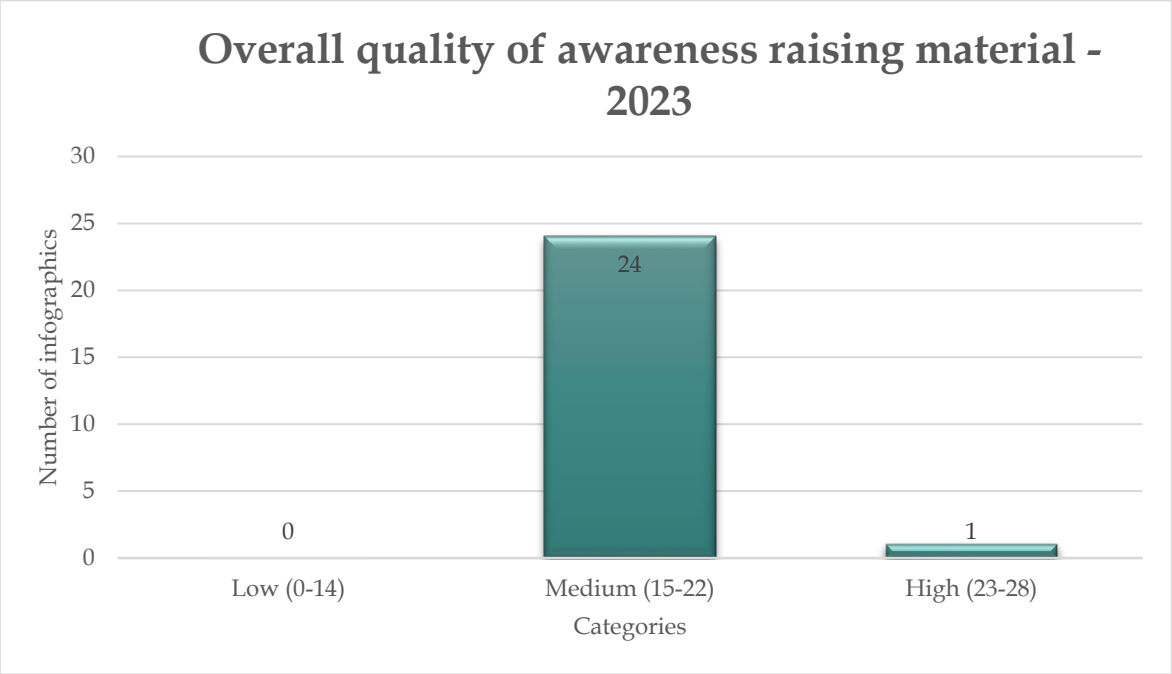


Figure 5.4: Chart of overall quality of awareness raising material – 2023

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.

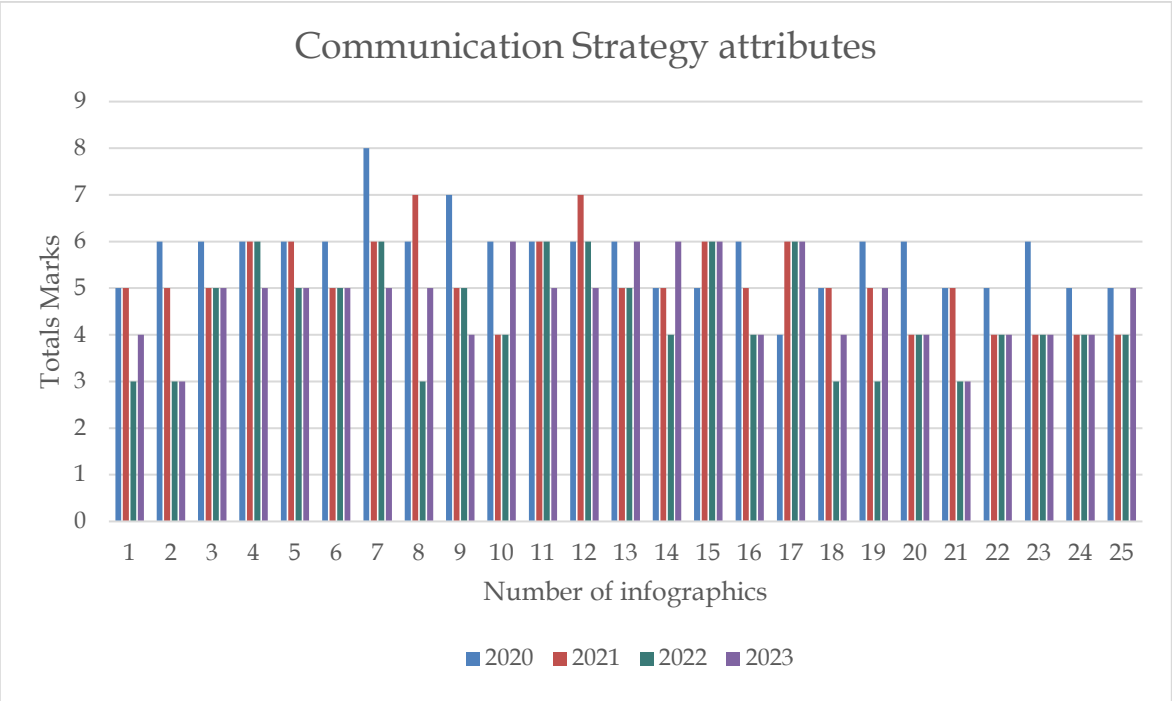


Figure 5.5: Chart of communication Strategy attributes

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.

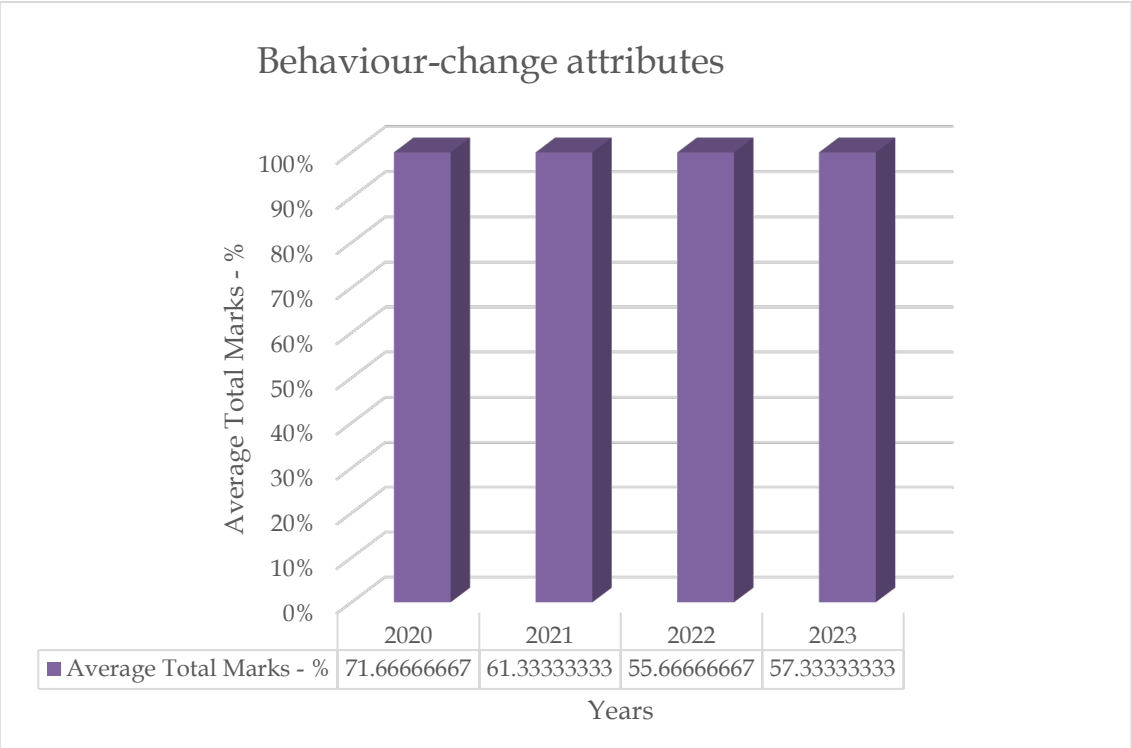


Figure 5.6: Chart of Behaviors-change attributes - %

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.

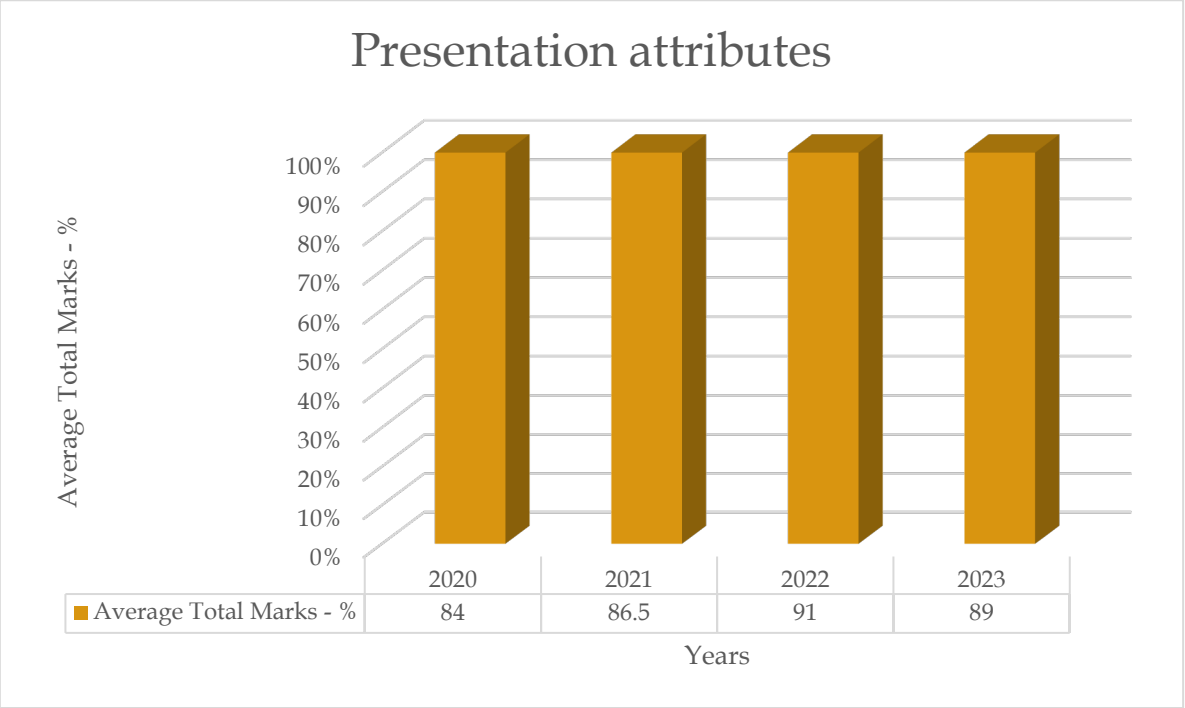


Figure 5.7: Chart of Presentation attributes – '%'

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.

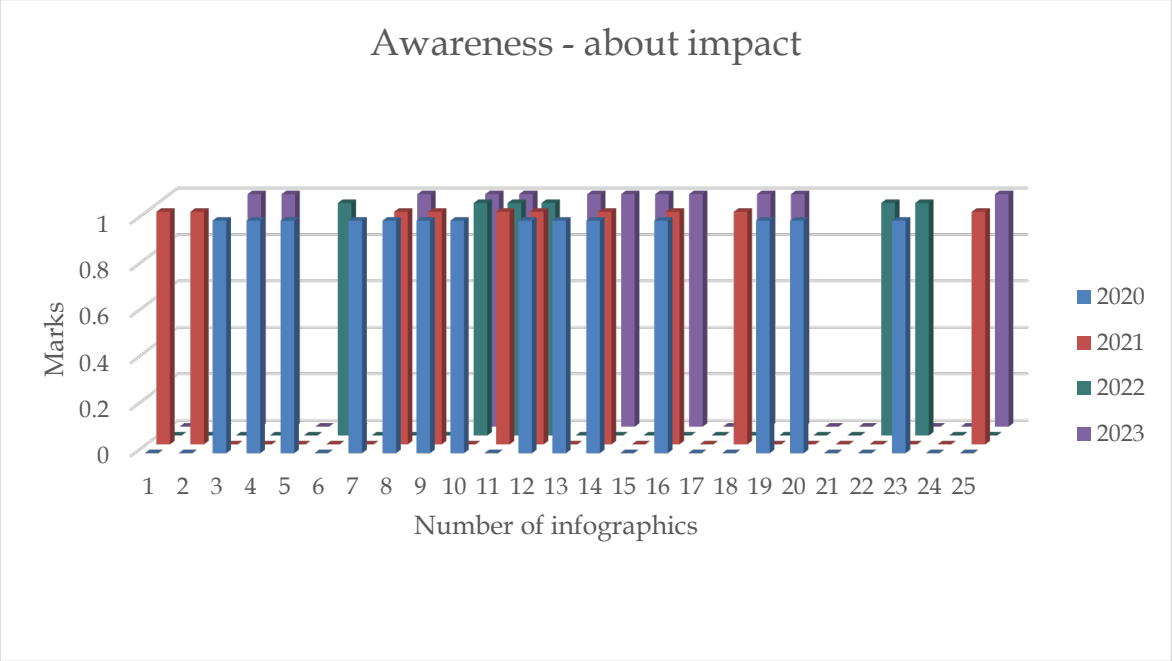


Figure 5.8: Chart of Awareness - about impact'

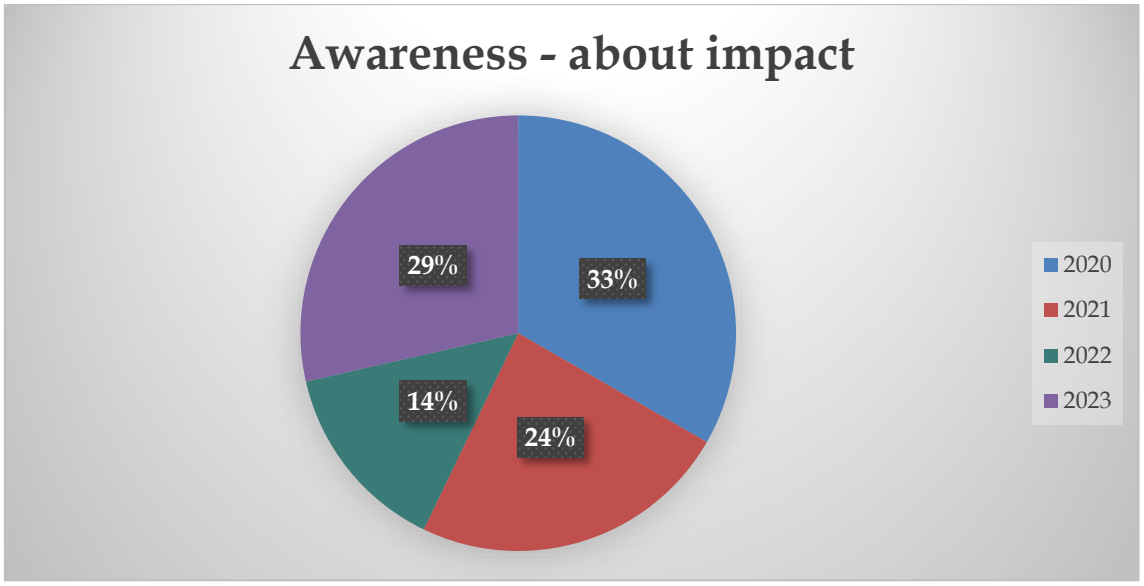


Figure 5.9: Chart of Awareness - about impact – '%'

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.

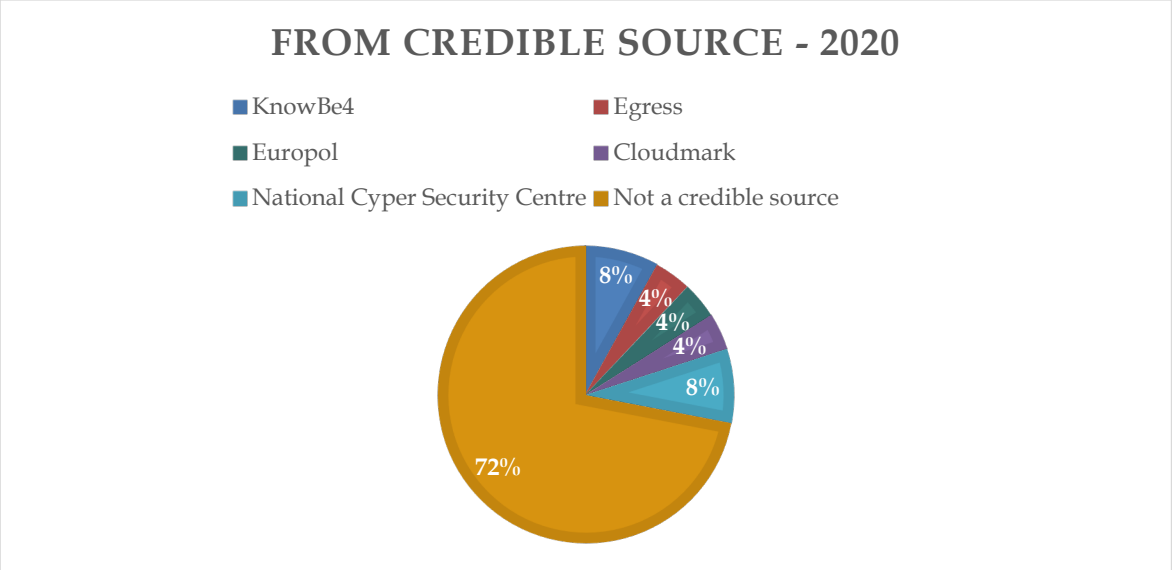


Figure 5.10: Chart - Credible source - 2020– '%'

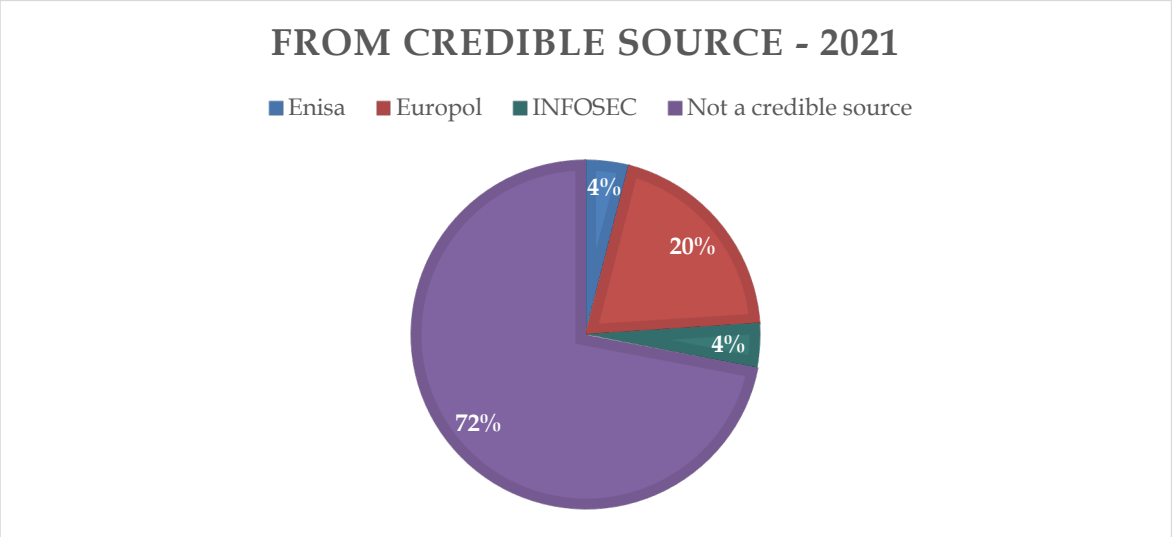


Figure 5.11: Chart - Credible source - 2021– '%'

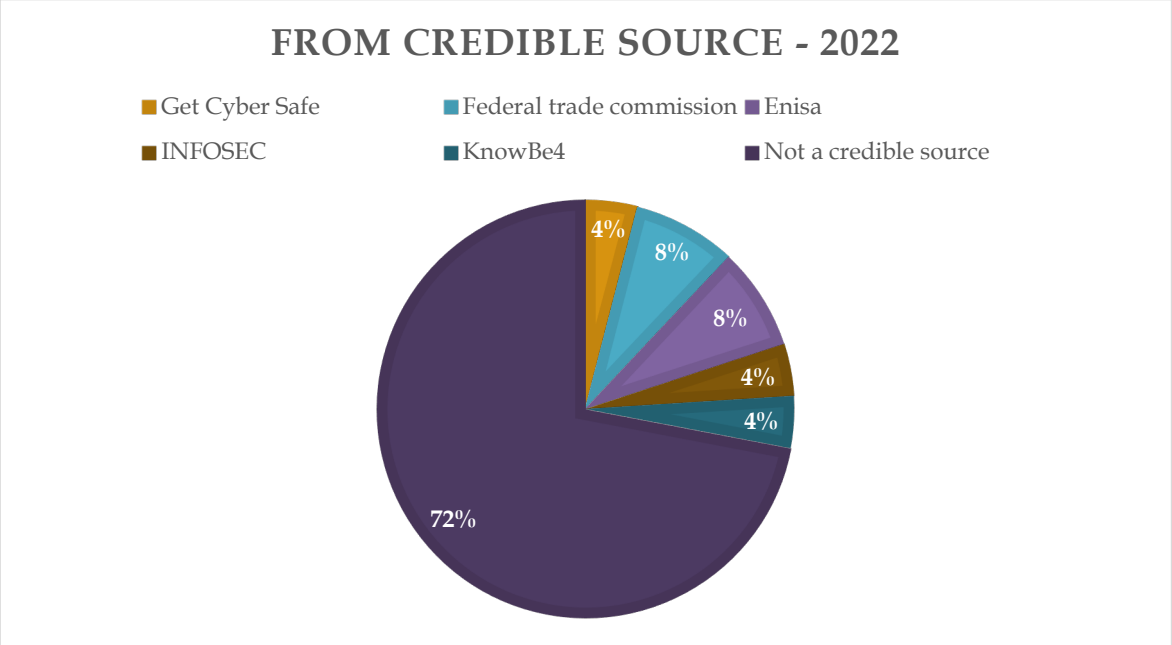


Figure 5.12: Chart - Credible source - 2022– '%'

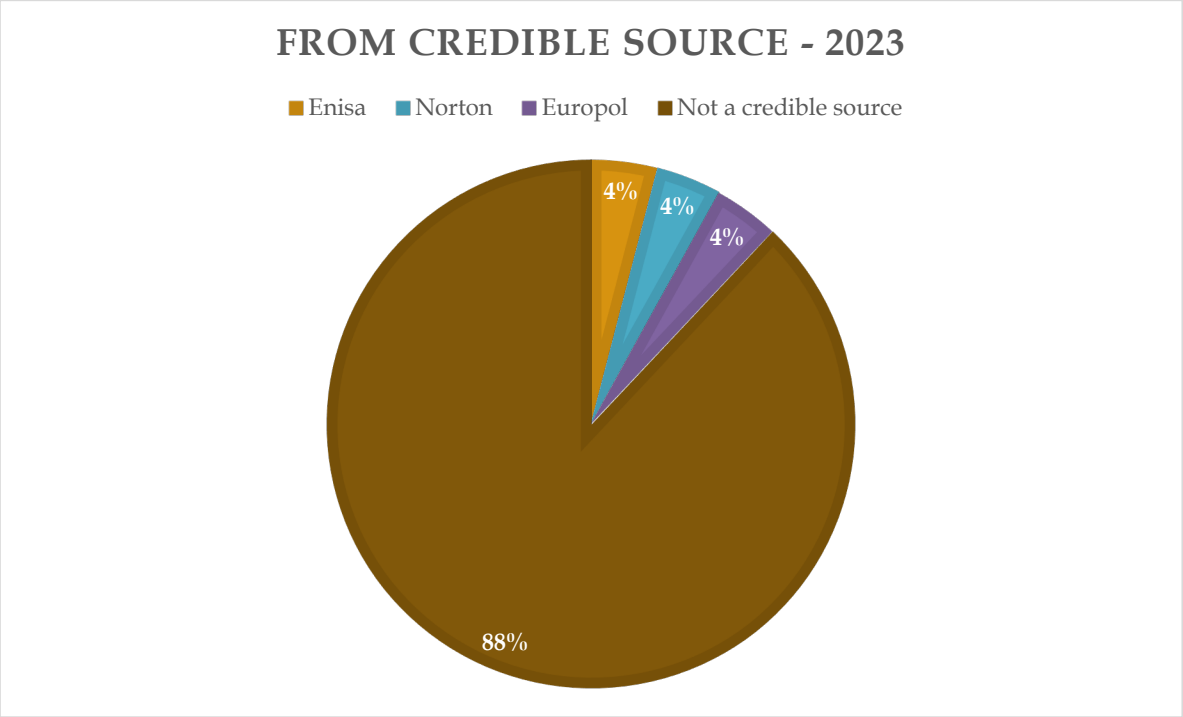


Figure 5.13: Chart - Credible source - 2023– '%'

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).

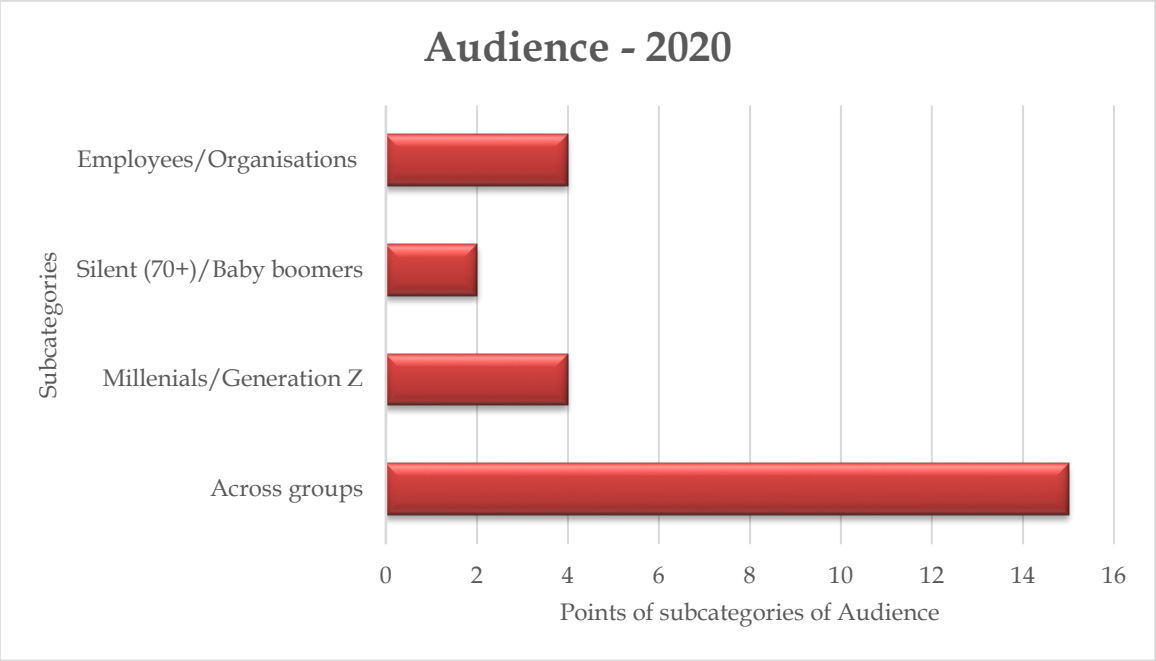


Figure 5.14: Chart – Audience – 2020

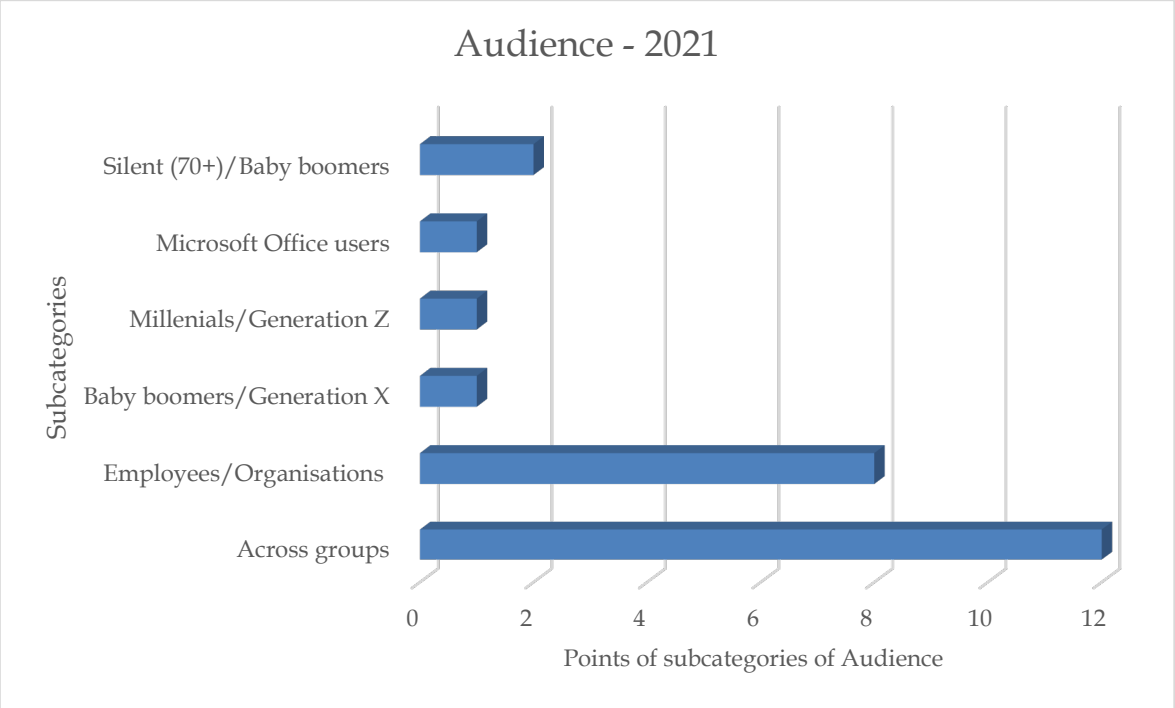


Figure 5.15: Chart – Audience – 2021

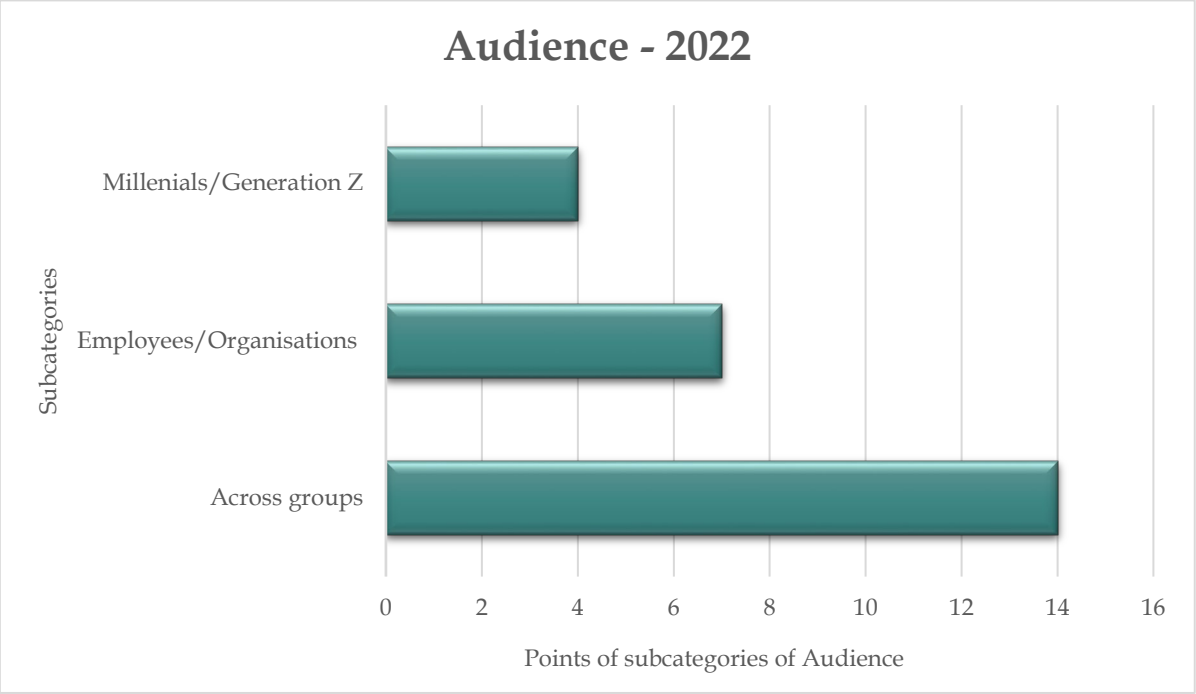


Figure 5.16: Chart – Audience – 2022

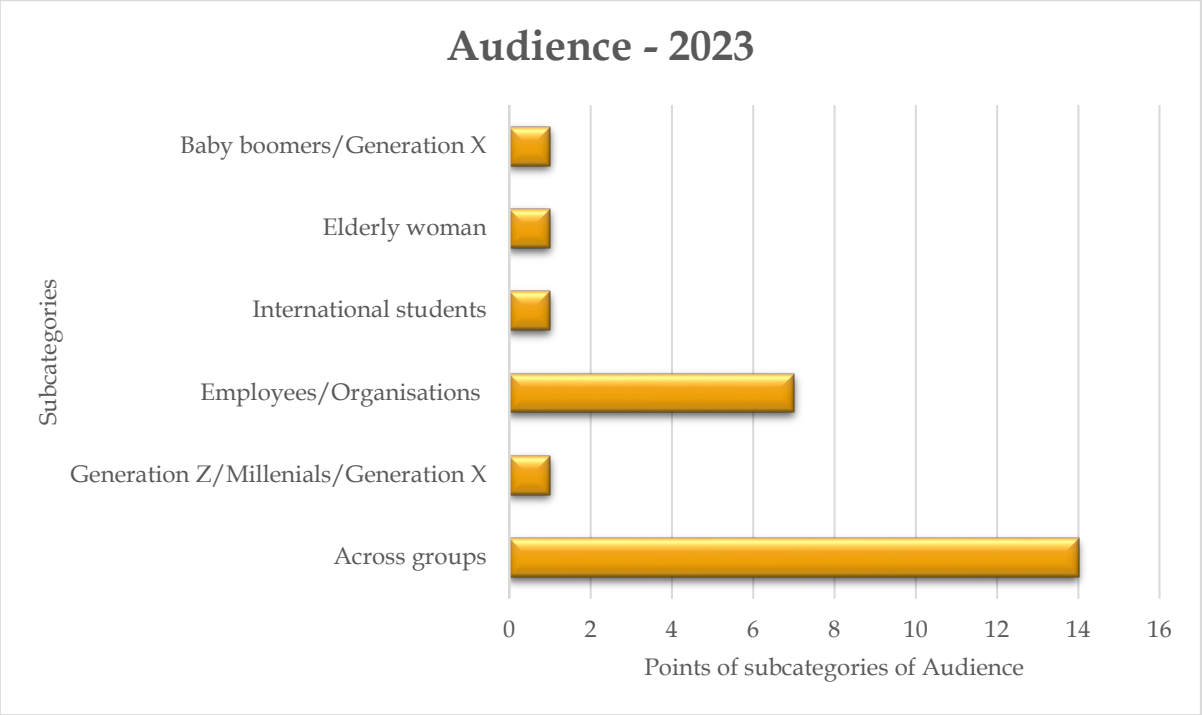


Figure 5.17: Chart – Audience – 2023

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.

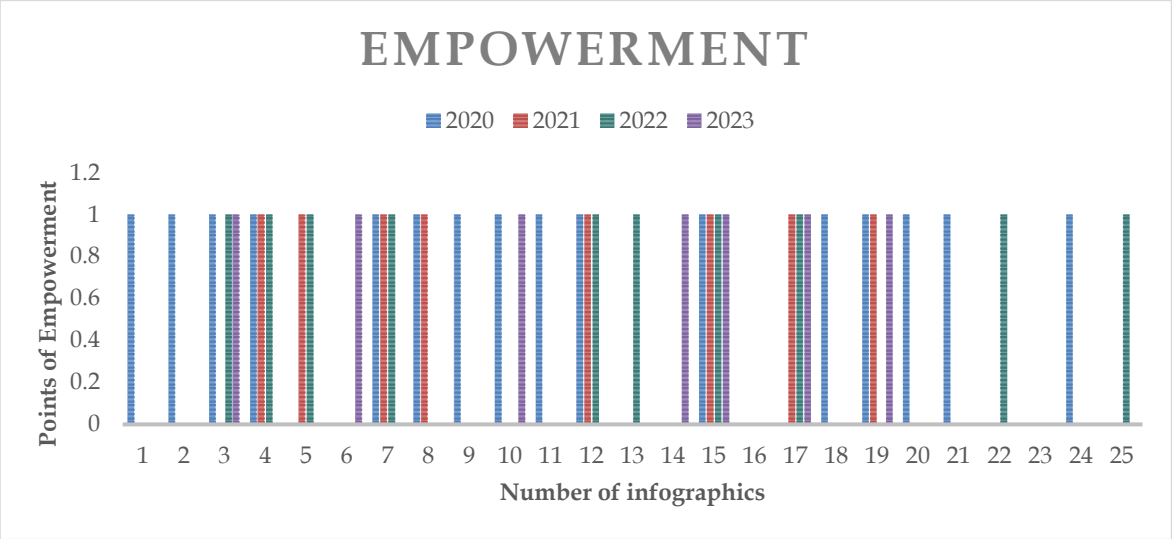


Figure 5.18: Chart – Empowerment - call to action, e.g., visit a website to learn more, to report an incident, etc.

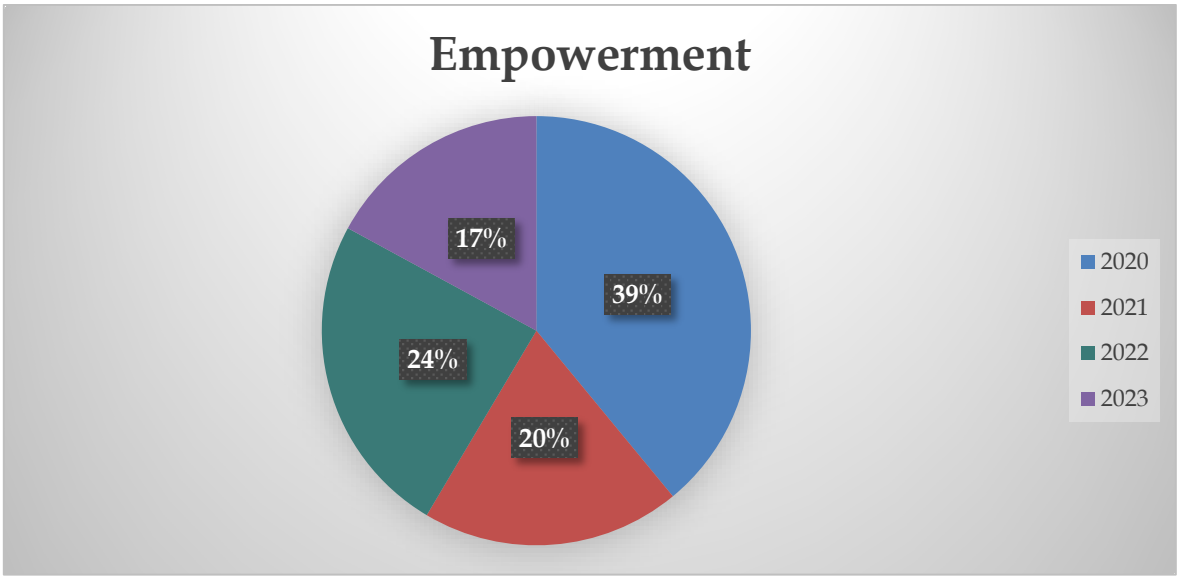


Figure 5.19: Chart – Empowerment - call to action, e.g., visit a website to learn more, to report an incident, etc.

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).

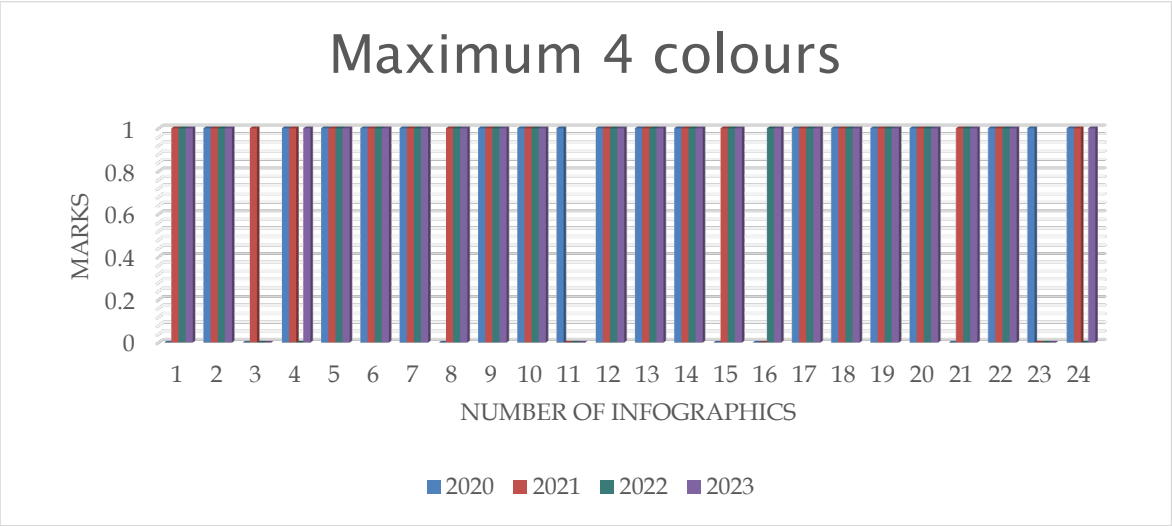


Figure 5.20: Chart – Maximum four colors

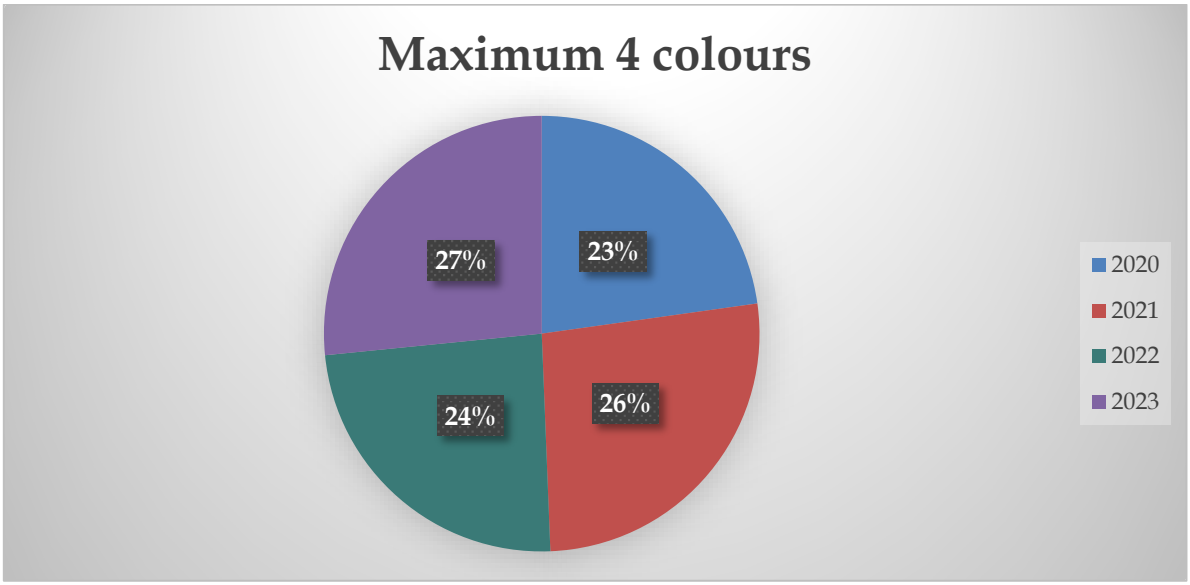


Figure 5.21: Chart – Maximum four colors – '% '

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).

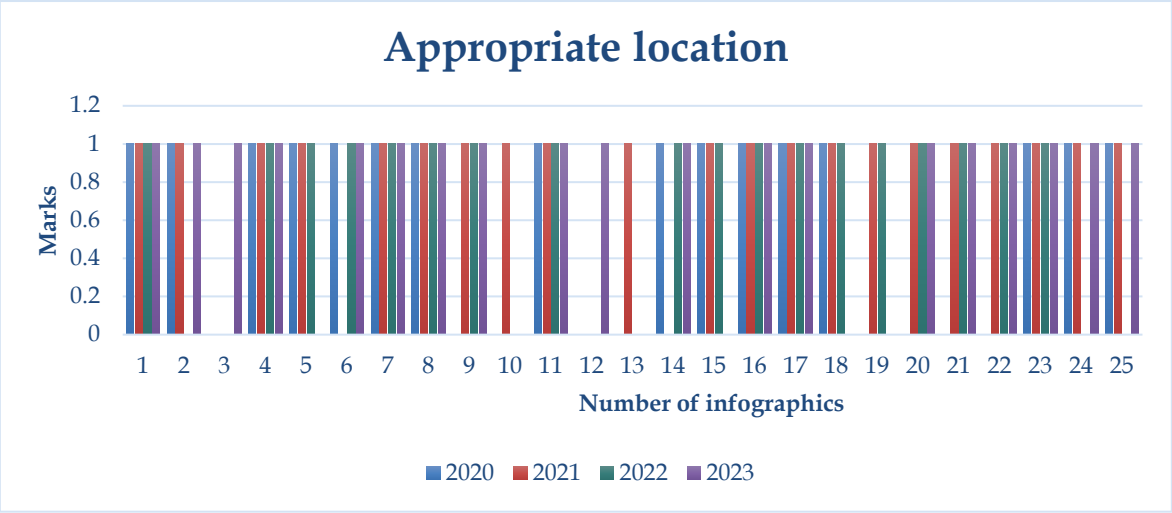


Figure 5.22: Chart – Appropriate location

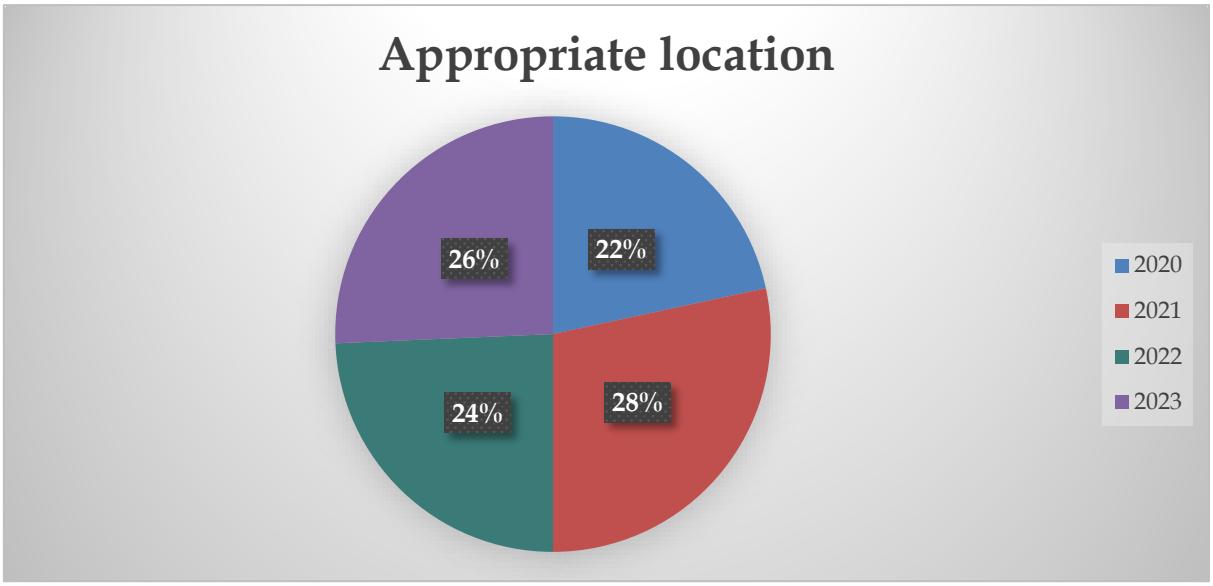


Figure 5.23: Chart – Appropriate location – '%'

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.

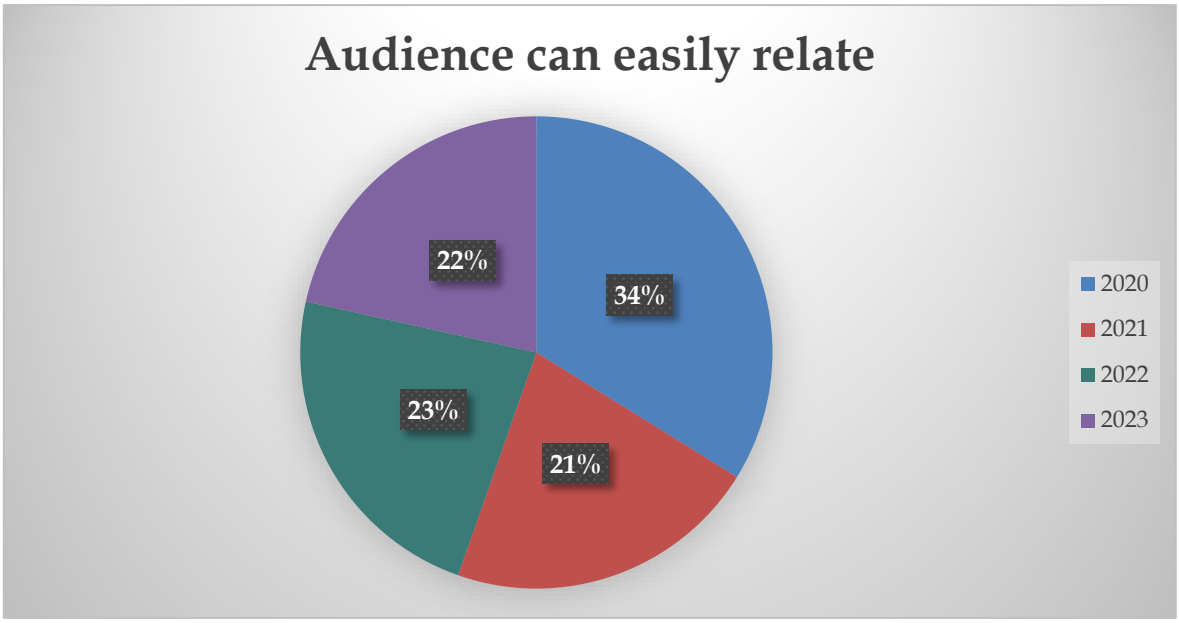


Figure 5.24: Chart – Audience can easily relate, e.g., storytelling – '%'

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

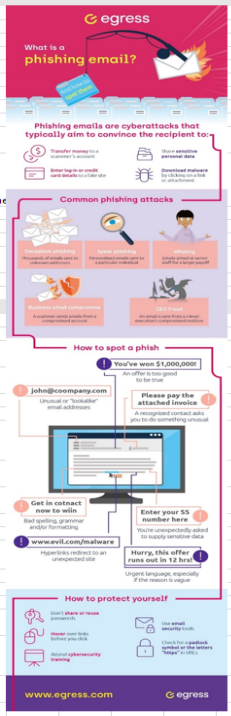
A.1 Analysis Infographics 2020

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

infographics_framework_v2020.xlsx

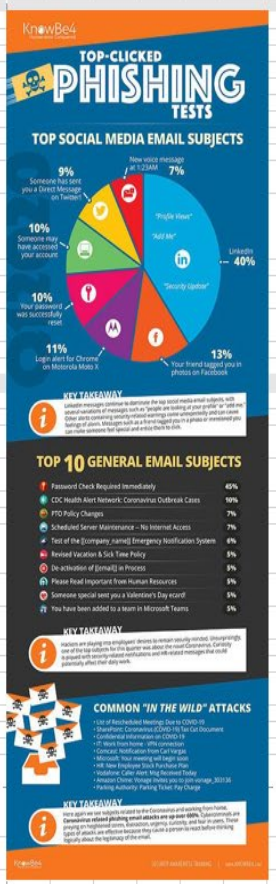
1)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website	https://www.egress.com/blog/phishing/how-to-spot-a-phishing-email		
1	Audience		Marks		Marks	Comments		
	1,1	Across groups	1		1	Individuals and Employees		
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1		1	List key information to know about phishing emails and how to spot them.		
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1		1	Tips to protect them selves from phishing emails		
	2,4	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		
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	Easy to understand how to detect phishing emails		
	1,2	Easy to understand what is the impact	1		0	Easy to protect them selves with examples		
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			
	3,2	From credible source	1		1	Egress		
4	Memorable							
	4,1	Micro-learning - specific topic	1		1	email phishing		
	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		1	Easy to explain the problem and give a solution, provides a real example		
		Presentation attributes						
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 4 colours	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					
		Communication Strategy attributes		5				
		Behaviour-change attributes		9				
		Presentation attributes		5				
			TOTAL	19				
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						



2)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website		https://www.knowbe4.com/press/q2-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-spike	
1	Audience		Marks		Marks		Comments	
	1,1	Across groups	1					
	1,2	Specific	2			2	Millenials/Generation Z	
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	Top 10 General email subjectsof phishing emails	
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1			1	Subjects to avoid phishing emails	
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	Call to action(key takeaway)	
3	Timeframe							
	3,1	Generic	1			1	It can be advertised at any time	
	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			0		
2	Empower people							
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			1		
	2,3	Overall conveys a positive message	1					
3	Evidence-based content							
	3,1	Based on facts, e.g. statistics, etc.	1			1		
	3,2	From credible source	1			1	KnowBe4	
4	Memorable							
	4,1	Micro-learning - specific topic	1			1	email phishing	
	4,2	Micro-learning - short statements, focus on key points	1					
	4,3	Considers different learning styles	1			1	yes, visual and text	
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples	
		Presentation attributes						
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 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1			1		
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1					
		Communication Strategy attributes			6			
		Behaviour-change attributes			9			
		Presentation attributes			7			
			TOTAL		22			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						



3)

	Communication Strategy attributes			**Evaluation**		
				Infographic - website	https://inspiredelearning.com/resource/social-media-phishing-infographic/	
1	Audience		Marks	Marks	Comments	
	1,1	Across groups	1	1		
	1,2	Specific	2			
2	Key message focus - clear purpose					
	2,1	Awareness - about threat	1	1	Social media users is now being targeted in social media phishing attacks.	
	2,2	Awareness - about impact	1	1	Social media phishing statistics, examples, and tips for protecting yourself from attacks.	
	2,3	Cyber hygiene - best practices	1	1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1	1	Report the insident	
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	1		
	2,3	Overall conveys a positive message	1			
3	Evidence-based content					
	3,1	Based on facts, e.g. statistics, etc.	1	1		
	3,2	From credible source	1	0		
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		
	4,4	Balance between graphics and text	1	0	overall a bit croweded	
	4,5	Audience can easily relate, e.g. storytelling	1	1		
	Presentation attributes					
1	Visibility of the message					
	1,1	Appropriate location	1	0		
	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 4 colours	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			
	Communication Strategy attributes			6		
	Behaviour-change attributes			9		
	Presentation attributes			4		
			TOTAL	19		
	Overall quality of awareness raising material					
	Low	0-14				
	Medium	15-22				
	High	23-28				

4)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://designedprivacy.com/phishing-infographic/	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	Phishing Frequency/Phishing Trends/Keep your self from getting tricked	
		2,2	Awareness - about impact	1		1		
		2,3	Cyber hygiene - best practices	1		1	breath out	
		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	
	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				
	2	Empower people						
		2,1	Simple information to understand how to address the threat	1		1		
		2,2	Appropriate call to action message	1		1		
		2,3	Overall conveys a positive message	1				
	3	Evidence-based content						
		3,1	Based on facts, e.g. statistics, etc.	1		1		
		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		
		4,4	Balance between graphics and text	1				
		4,5	Audience can easily relate, e.g. storytelling	1				
		Presentation attributes						
	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				
		2,3	Maximum 4 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				
		3,3	Use appropriate font size ()	1				
		Communication Strategy attributes				6		
		Behaviour-change attributes				7		
		Presentation attributes				4		
				TOTAL		17		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

5)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website		https://veritau.co.uk/phishing-and-its-risks-cyber-security-month/	
1	Audience		Marks		Marks		Comments	
	1,1	Across groups	1			1	General information about phishing and its risks	
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1		
	2,2	Awareness - about impact	1			1		
	2,3	Cyber hygiene - best practices	1			1	look for signs	
	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					
	3,2	Covers specific time periods	2			2	Holidays or out of the office	
		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					
3	Evidence-based content							
	3,1	Based on facts, e.g. statistics, etc.	1			1	use 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			0		
	4,3	Considers different learning styles	1			1		
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1		
		Presentation attributes						
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 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1			1		
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
		Communication Strategy attributes			6			
		Behaviour-change attributes			8			
		Presentation attributes			8			
				TOTAL	22			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

6)

	B	C	D	F	G	H
2	**Communication Strategy attributes**				**Evaluation**	
3					Infographic - website	https://veritau.co.uk/phishing-and-its-risks-cyber-security-month/
4						
5	Audience		Marks		Marks	Comments
6	1,1	Across groups	1		0	
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	holidays scams
11	2,2	Awareness - about impact	1		0	
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	Timeframe					
16	3,1	Generic	1			
17	3,2	Covers specific time periods	2		2	Holidays period
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		0	
25						
26	Empower people					
27	2,1	Simple information to understand how to address the threat	1		1	different types of holidays scams
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			
33	3,2	From credible source	1		1	KnowBe4
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		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						
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 (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			
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**			7		
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	23-28				

7)

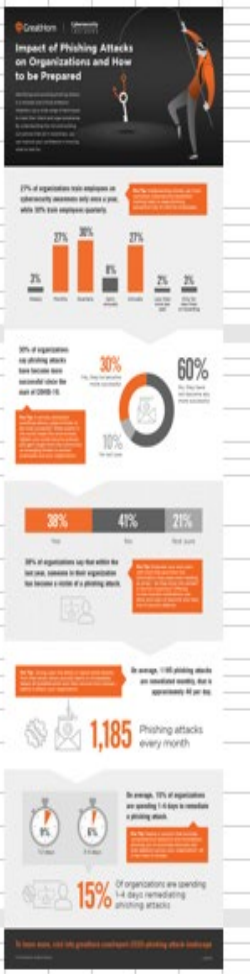
		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://twitter.com/envisiontech/status/1333405413523640325?s	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2		
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	Avoid online scams on season holidays	
	2,2	Awareness - about impact	1		1		
	2,3	Cyber hygiene - best practices	1		1	tips what you can do if your are a victum	
	2,4	Empowerment - call to action, e. g. visit a website to learn more, to report an incident, etc.	1		1	report the incident	
3	Timeframe						
	3,1	Generic	1				
	3,2	Covers specific time periods	2		2	Holiday period	
		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	How to avoid scams	
	2,2	Appropriate call to action message	1		1	what to do if you' re a victum	
	2,3	Overall conveys a positive message	1			neutral	
3	Evidence-based content						
	3,1	Based on facts, e. g. statistics, etc.	1		1	examples of scams	
	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		
	4,4	Balance between graphics and text	1		1		
	4,5	Audience can easily relate, e. g. storytelling	1		1	real examples	
		Presentation attributes					
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim. org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			8		
		Behaviour-change attributes			10		
		Presentation attributes			8		
				TOTAL	26		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

8)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://ciosmag.com/dont-get-phished-infographic/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to identify a phishing email	
	2,2	Awareness - about impact	1		1		
	2,3	Cyber hygiene - best practices	1		1	tips to not get phished	
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	Inform you how to identify phishing emails	
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	How to identify phishing emails	
	2,2	Appropriate call to action message	1		1	Identify threats	
	2,3	Overall conveys a positive message	1			Neutral	
3	Evidence-based content						
	3,1	Based on facts, e.g. statistics, etc.	1		1	examples of phishing emails	
	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	
	4,4	Balance between graphics and text	1		1		
	4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
		Presentation attributes					
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 4 colours	1				
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes		6			
		Behaviour-change attributes		10			
		Presentation attributes		7			
			TOTAL	23			
		Overall quality of awareness raising material					
	Low	0-14					
	Medium	15-22					
	High	23-28					

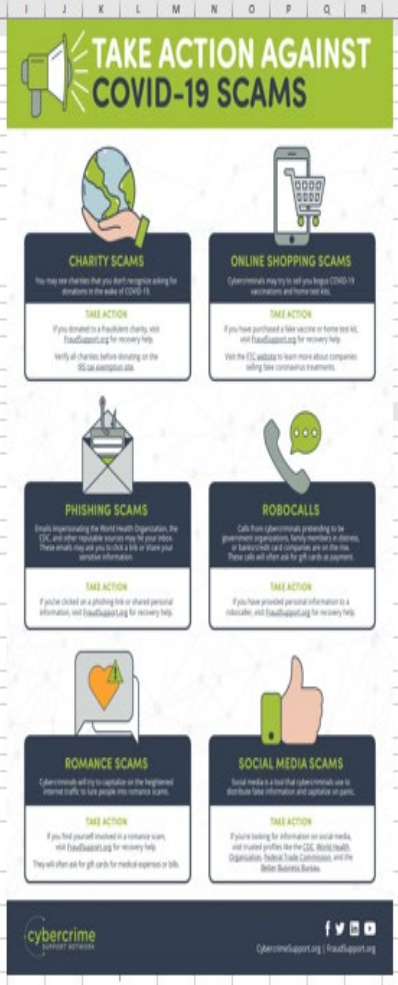
9)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.greathorn.com/resources/guides/infographic-impact-of-phishing-attacks-on-organizations-and-how-to-be-prepared/	
	1	Audience		Marks	Marks	Comments	
		1,1	Across groups	1			
		1,2	Specific	2	2	Employees/Organisations	
	2	Key message focus - clear purpose					
		2,1	Awareness - about threat	1	1	Impact of phishing attacks on organisations/ how to be prepared	
		2,2	Awareness - about impact	1	1		
		2,3	Cyber hygiene - best practices	1	1	tips how employees can be prepared about phishing attacks	
		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 tobe prepared about phishing attacks	
	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, visual, graphics	
		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	
		4,4	Balance between graphics and text	1	1		
		4,5	Audience can easily relate, e.g. storytelling	1	1	real examples/ statistics	
		Presentation attributes					
	1	Visibility of the message					
		1,1	Appropriate location	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 4 colours	1	1		
	3	Inclusive / Accessible					
		3,1	A good color contrast between the text color and background color	1		using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1	1		
		3,3	Use appropriate font size ()	1	1		
		Communication Strategy attributes			7		
		Behaviour-change attributes			9		
		Presentation attributes			6		
				TOTAL	22		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				



10)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.isu.edu/tech/support/information-security/covid-19-related-cyber-scams/	
1	Audience			Marks		Marks	Comments	
	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		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		
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		
	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	
	4,4	Balance between graphics and text		1		1		
	4,5	Audience can easily relate, e.g. storytelling		1		1	real examples	
		Presentation attributes						
1	Visibility of the message							
	1,1	Appropriate location		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			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()		1		1		
	3,3	Use appropriate font size ()		1		1		
		Communication Strategy attributes				6		
		Behaviour-change attributes				9		
		Presentation attributes				6		
				TOTAL		21		
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						



11)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website	https://www.ebf.eu/ebf-media-centre/cyberscams-ceo-business-email-compromise-bec-fraud/		
1	Audience		Marks		Marks	Comments		
	1,1	Across groups	1					
	1,2	Specific	2		2	Employees/Organisations		
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1		1	Invoice fraud		
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1		1			
	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		
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					
2	Empower people							
	2,1	Simple information to understand how to address the threat	1		1			
	2,2	Appropriate call to action message	1		1			
	2,3	Overall conveys 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		1	Europol		
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		1	real examples		
		Presentation attributes						
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 4 colours	1		1			
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/		
	3,2	Use appropriate font styles ()	1		1			
	3,3	Use appropriate font size ()	1		1			
		Communication Strategy attributes		6				
		Behaviour-change attributes		9				
		Presentation attributes		8				
			TOTAL	23				
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

12)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://vensgaga.com/gallery/post/6-common-phishing-attacks-and-how-to-avoid-them/	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1			1		
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	Six common phishing scams	
	2,2	Awareness - about impact	1			1		
	2,3	Cyber hygiene - best practices	1			1	How to avoid the threads	
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	Report the incident	
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					
2	Empower people							
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			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			1		
	4,3	Considers different learning styles	1			1	Visual, examples	
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples	
		Presentation attributes						
1	Visibility of the message							
	1,1	Appropriate location	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 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1					
		Communication Strategy attributes				6		
		Behaviour-change attributes				9		
		Presentation attributes				5		
				TOTAL		20		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

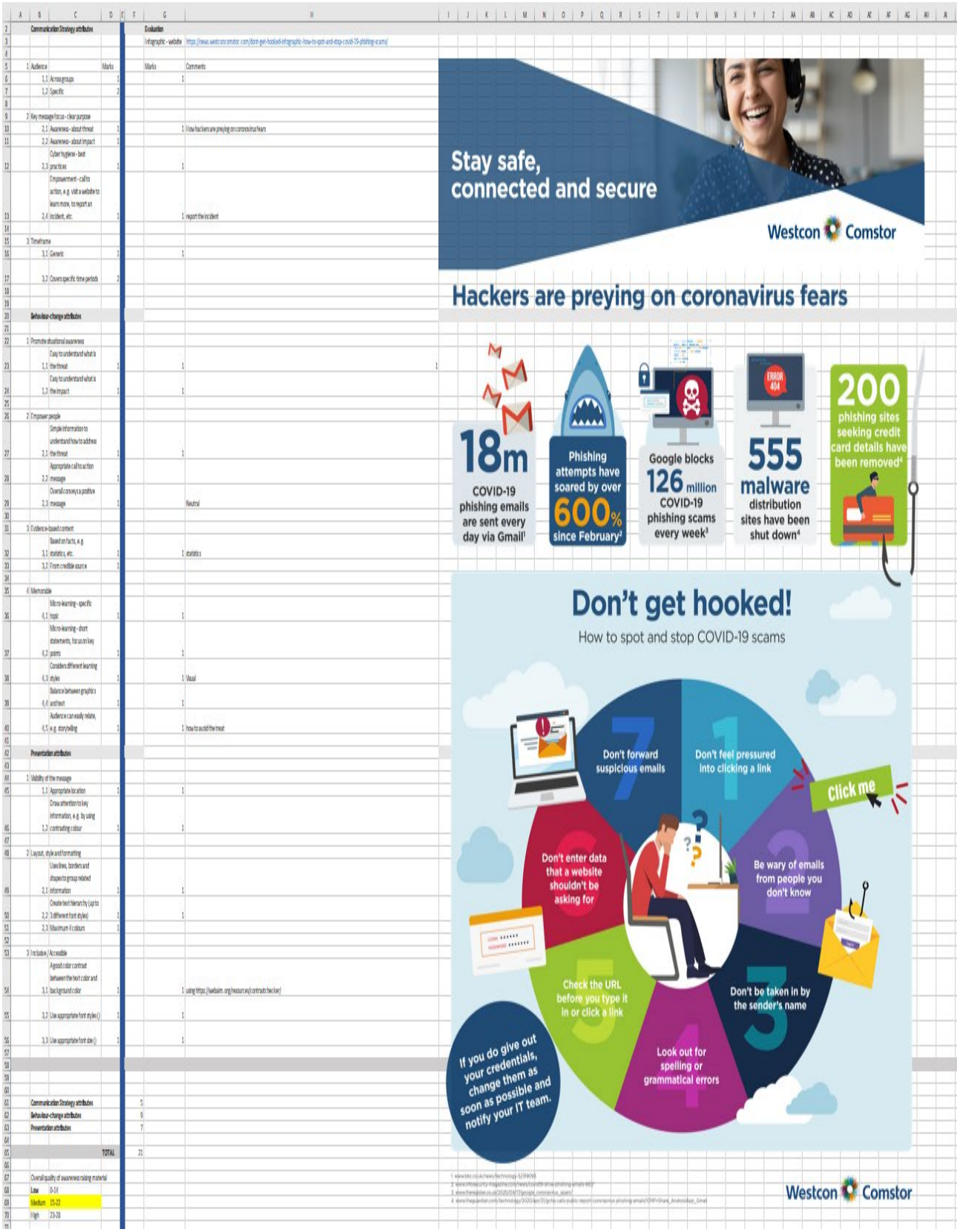
13)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.mcpc.com/insights/infographics/lets-go-phishing-a-guide-to-phishing-attacks/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Employees/Organisations	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	Guide for phishing attacks	
	2,2	Awareness - about impact	1		1		
	2,3	Cyber hygiene - best practices	1		1	How to avoid the threads	
	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		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		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				
		Presentation attributes					
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim. org/resource/es/contrastchecker/	
	3,2	Use appropriate font styles()	1		1		
	3,3	Use appropriate font size ()	1				
		Communication Strategy attributes		6			
		Behaviour-change attributes		8			
		Presentation attributes		6			
			TOTAL	20			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

14)

2		**Communication Strategy attributes**				**Evaluation**	
3						Infographic - website	https://blog.knowbe4.com/hs-fs/hubfs/cloudmark_top_ten_infographic.png?width=1294&height=3988&name=cloudmark_top_ten_infographic.png
4							
5	1	Audience		Marks		Marks	Comments
6		1,1	Across groups	1			
7		1,2	Specific	2		2	Employees/Organizations
8							
9	2	Key message focus - clear purpose					
10		2,1	Awareness - about threat	1		1	Top ten worst cybersecurity for spear phishing
11		2,2	Awareness - about impact	1		1	Impact about employees, revenue etc.
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		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		1	Cloudmark
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,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		**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 https://webaim.org/resources/contrastchecker/
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**			9		
63		**Presentation attributes**			8		
64							
65				**TOTAL**	22		
66							
67		Overall quality of awareness raising material					
68		**Low**	0-14				
69		Medium	15-22				
70		High	23-28				

15)

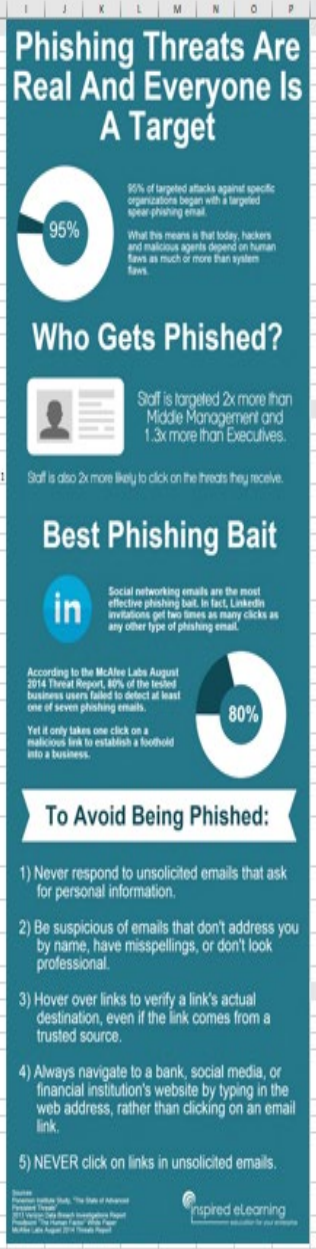

Stay safe,
connected and secure
Westcon Comstor
Hackers are preying on coronavirus fears
18m
COVID-19 phishing emails are sent every day via Gmail[1]
Phishing attempts have soared by over 600% since February[2]
Google blocks 126 million COVID-19 phishing scams every week[3]
555 malware distribution sites have been shut down[4]
200 phishing sites seeking credit card details have been removed[4]
Don't get hooked!
How to spot and stop COVID-19 scams
Don't forward suspicious emails
Don't feel pressured into clicking a link
Click me
Don't enter data that a website shouldn't be asking for
Be wary of emails from people you don't know
Check the URL before you type it in or click a link
Don't be taken in by the sender's name
Look out for spelling or grammatical errors
If you do give out your credentials, change them as soon as possible and notify your IT team.
Westcon Comstor

16)

		Communication Strategy attributes					**Evaluation**						
							Infographic - website	https://www.idology.com/senior-security-series/					
	1	Audience		Marks			Marks	Comments					
		1,1	Across groups	1									
		1,2	Specific	2			2	Silent (70+)/Baby boomers					
	2	Key message focus - clear purpose											
		2,1	Awareness - about threat	1			1	Cyber securing seniors during covid-19					
		2,2	Awareness - about impact	1			1						
		2,3	Cyber hygiene - best practices	1			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				
		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			1						
		4,3	Considers different learning styles	1			1	Visual					
		4,4	Balance between graphics and text	1			1						
		4,5	Audience can easily relate, e.g. storytelling	1			1	how to avoid the treat					
		Presentation attributes											
	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 4 colours	1									
	3	Inclusive / Accessible											
		3,1	A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/					
		3,2	Use appropriate font styles()	1			1						
		3,3	Use appropriate font size()	1			1						
		Communication Strategy attributes				6							
		Behaviour-change attributes				9							
		Presentation attributes				7							
				TOTAL		22							
		Overall quality of awareness raising material											
		Low	0-14										
		Medium	15-22										
		High	23-28										

17)

		Communication Strategy attributes				**Evaluation**			
						Infographic - website		https://inspiredelearning.com/resource/infographic-avoid-becoming-phished/	
1	Audience			Marks		Marks		Comments	
	1,1	Across groups		1			1	Individual & employees	
	1,2	Specific		2					
2	Key message focus - clear purpose								
	2,1	Awareness - about threat		1			1	Phishing threats are real everyone is a target	
	2,2	Awareness - about impact		1					
	2,3	Cyber hygiene - best practices		1			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
	1,2	Easy to understand what is the impact		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			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			1	how to avoid the threat	
		Presentation attributes							
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 4 colours		1			1		
3	Inclusive / Accessible								
	3,1	A good color contrast between the text color and background color		1			1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles()		1			1		
	3,3	Use appropriate font size ()		1			1		
		Communication Strategy attributes				4			
		Behaviour-change attributes				8			
		Presentation attributes				8			
				TOTAL		20			
		Overall quality of awareness raising material							
		Low	0-14						
		Medium	15-22						
		High	23-28						



18)

		Communication Strategy attributes					**Evaluation**					
							Infographic - website	https://www.suncoastcreditunion.com/blog/safety-and-protection/be-aware-of-imposter-scams-infographic				
	1	Audience		Marks			Marks	Comments				
		1,1	Across groups	1			1					
		1,2	Specific	2								
	2	Key message focus - clear purpose										
		2,1	Awareness - about threat	1			1	Be aware of imposter phone scams				
		2,2	Awareness - about impact	1								
		2,3	Cyber hygiene - best practices	1			1	Some tips to protect your self from phone scams				
		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	Call and report the incident				
	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								
	2	Empower people										
		2,1	Simple information to understand how to address the threat	1			1					
		2,2	Appropriate call to action message	1			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			1					
		4,3	Considers different learning styles	1			1	Visual/text				
		4,4	Balance between graphics and text	1								
		4,5	Audience can easily relate, e.g. storytelling	1			1	how to avoid the treat/ real examples				
		Presentation attributes										
	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 4 colours	1			1					
	3	Inclusive / Accessible										
		3,1	A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/				
		3,2	Use appropriate font styles ()	1			1					
		3,3	Use appropriate font size ()	1			1					
		Communication Strategy attributes					5					
		Behaviour-change attributes					8					
		Presentation attributes					8					
				TOTAL			21					
		Overall quality of awareness raising material										
		Low	0-14									
		Medium	15-22									
		High	23-28									

19)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.ncsc.gov.uk/information/infographics-ncsc	
	1	Audience		Marks		Marks		Comments
		1,1	Across groups	1			1	
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1			1	How to make your self harder target
		2,2	Awareness - about impact	1			1	
		2,3	Cyber hygiene - best practices	1			1	Some tips to protect your self from phishing attacks
		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report the incident
	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			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	National Cyber Security Centre
	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				
		4,5	Audience can easily relate, e.g. storytelling	1			1	how to avoid the treat / real examples
		Presentation attributes						
	1	Visibility of the message						
		1,1	Appropriate location	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 4 colours	1			1	
	3	Inclusive / Accessible						
		3,1	Agood color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/
		3,2	Use appropriate font styles ()	1			1	
		3,3	Use appropriate font size ()	1			1	
		Communication Strategy attributes				6		
		Behaviour-change attributes				10		
		Presentation attributes				7		
				TOTAL		23		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

20)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.ncsc.gov.uk/files/sextortion-scams-infographic.pdf	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to do if you are being blackmailed by sextortion scams	
	2,2	Awareness - about impact	1		1		
	2,3	Cyber hygiene - best practices	1		1	Some tips to protect your self from blackmailed	
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	report the incident	
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		1		
	2,3	Overall conveys 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		1	National Cyber Security Centre	
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				
	4,5	Audience can easily relate, e.g. storytelling	1		1	What to do if been blackmailed / real examples	
	Presentation attributes						
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			6			
	Behaviour-change attributes			9			
	Presentation attributes			7			
			TOTAL	22			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

21)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website		https://www.pherrus.com.au/phishing-scams-and-how-to-avoid-becoming-a-victim/
1	Audience		Marks		Marks		Comments
	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 practices	1			1	
	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
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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1			1	
	2,2	Appropriate call to action message	1			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	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			1	how to be guard and how to spot a phishing attack
	Presentation attributes						
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1			1	
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			1	using https://webaim. org/resource/c ontrastchecker/
	3,2	Use appropriate font styles ()	1			1	
	3,3	Use appropriate font size ()	1			1	
	Communication Strategy attributes			5			
	Behaviour-change attributes			9			
	Presentation attributes			7			
			TOTAL	21			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

22)

	Communication Strategy attributes					**Evaluation**							
						Infographic - website	https://www.getcybersafe.gc.ca/en/resources/social-engineering-how-cyber-scams-trick-us						
1	Audience			Marks		Marks	Comments						
		1,1	Across groups	1									
		1,2	Specific	2		2	Millenials/Generation Z						
2	Key message focus - clear purpose												
		2,1	Awareness - about threat	1		1	how do cyber scams trick people						
		2,2	Awareness - about impact	1									
		2,3	Cyber hygiene - best practices	1		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									
2	Empower people												
		2,1	Simple information to understand how to address the threat	1		1							
		2,2	Appropriate call to action message	1		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	Examples/ 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		1							
		4,3	Considers different learning styles	1		1	Visual/text						
		4,4	Balance between graphics and text	1									
		4,5	Audience can easily relate, e.g. storytelling	1		1	how to keep your information secure						
	Presentation attributes												
1	Visibility of the message												
		1,1	Appropriate location	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 4 colours	1									
3	Inclusive / Accessible												
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/						
		3,2	Use appropriate font styles ()	1		1							
		3,3	Use appropriate font size ()	1		1							
	Communication Strategy attributes					5							
	Behaviour-change attributes					8							
	Presentation attributes					6							
				TOTAL		19							
	Overall quality of awareness raising material												
	Low	0-14											
	Medium	15-22											
	High	23-28											

23)

1																									
2		**Communication Strategy attributes**					**Evaluation**																		
3							Infograpl	https://www.suncoastcreditunion.com/blog/safety-and-protection/how-to-avoid-scams-this-holiday-season-infographic																
4																									
5	1	Audience		Marks			Marks	Comments																	
6		1,1	Across	1			1																		
7		1,2	Specific	2																					
8																									
9	2	Key message focus - clear purpose																							
10		2,1	Awarene	1			1	How to avoid scams on holiday seasons																	
11		2,2	Awarene	1			1																		
12		2,3	Cyber	1			1																		
13		2,4	Empowe rment -	1																					
14																									
15	3	Timeframe																							
16		3,1	Generic	1																					
17		3,2	Covers	2			2	christmas holiday season																	
18																									
19																									
20		**Behaviour-change attributes**																							
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 informat	1			1																		
28		2,2	Appropr	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	Micro-learning -	1			1																		
38		4,3	Conside	1																					
39		4,4	Balance	1			1																		
40		4,5	Audienc	1			1	how to protect yourself from holiday scams																	
41																									
42		**Presentation attributes**																							
43																									
44	1	Visibility of the message																							
45		1,1	Appropr	1			1																		
46		1,2	Draw attentio	1			1																		
47																									
48	2	Layout, style and formatting																							
49		2,1	Uses fonts,	1			1																		
50		2,2	Create	1			1																		
51		2,3	Maximu	1			1																		
52																									
53	3	Inclusive / Accessible																							
54		3,1	A good color	1			1	using https://webaim.org/resources/contrastchecker/																	
55		3,2	Use	1			1																		
56		3,3	Use	1			1																		
57																									
58																									
59																									
60																									
61		**Communication Strategy attribut**					6																		
62		**Behaviour-change attributes**					9																		
63		**Presentation attributes**					8																		
64																									
65				**TOTAL**			23																		
66																									
67		Overall quality of awareness raising material																							
68		Low	0-14																						
69		Medium	15-22																						
70		High	23-28																						

24)

		Communication Strategy attributes					**Evaluation**			
							Infographic - website	https://www.jpcu.org/wp-content/uploads/2023/01/Visa-Phishing-Infographic-768x2644.jpg		
	1	Audience		Marks			Marks	Comments		
			1,1 Across groups		1			1		
			1,2 Specific		2					
	2	Key message focus - clear purpose								
			2,1 Awareness - about threat		1			1 Watch out for different Phishing scams		
			2,2 Awareness - about impact		1					
			2,3 Cyber hygiene - best practices		1			1		
			Empowerment - call to action, e.g. visit a website to learn more, to report an							
			2,4 incident, etc.		1			1 report the incident		
	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					
	2	Empower people								
			Simple information to understand how							
			2,1 to address the threat		1			1		
			2,2 Appropriate call to action message		1			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 Examples/ Statistics		
			3,2 From credible source		1					
	4	Memorable								
			4,1 Micro-learning - specific topic		1			1		
			Micro-learning - short statements, focus							
			4,2 on key points		1			1		
			4,3 Considers different learning styles		1			1 Visual/text		
			4,4 Balance between graphics and text		1			1		
			Audience can easily relate, e.g.							
			4,5 storytelling		1					
		Presentation attributes								
	1	Visibility 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								
			Uses lines, borders and shapes to group							
			2,1 related information		1			1		
			Create text hierarchy (up to 3 different							
			2,2 font styles)		1			1		
			2,3 Maximum 4 colours		1			1		
	3	Inclusive / Accessible								
			A good color contrast between the text							
			3,1 color and background color		1			1 using https://webaim.org/resources/contrastchecker/		
			3,2 Use appropriate font styles ()		1			1		
			3,3 Use appropriate font size ()		1			1		
		Communication Strategy attributes					5			
		Behaviour-change attributes					8			
		Presentation attributes					8			
				TOTAL			21			
		Overall quality of awareness raising material								
		Low	0-14							
		Medium	15-22							
		High	23-28							

25)

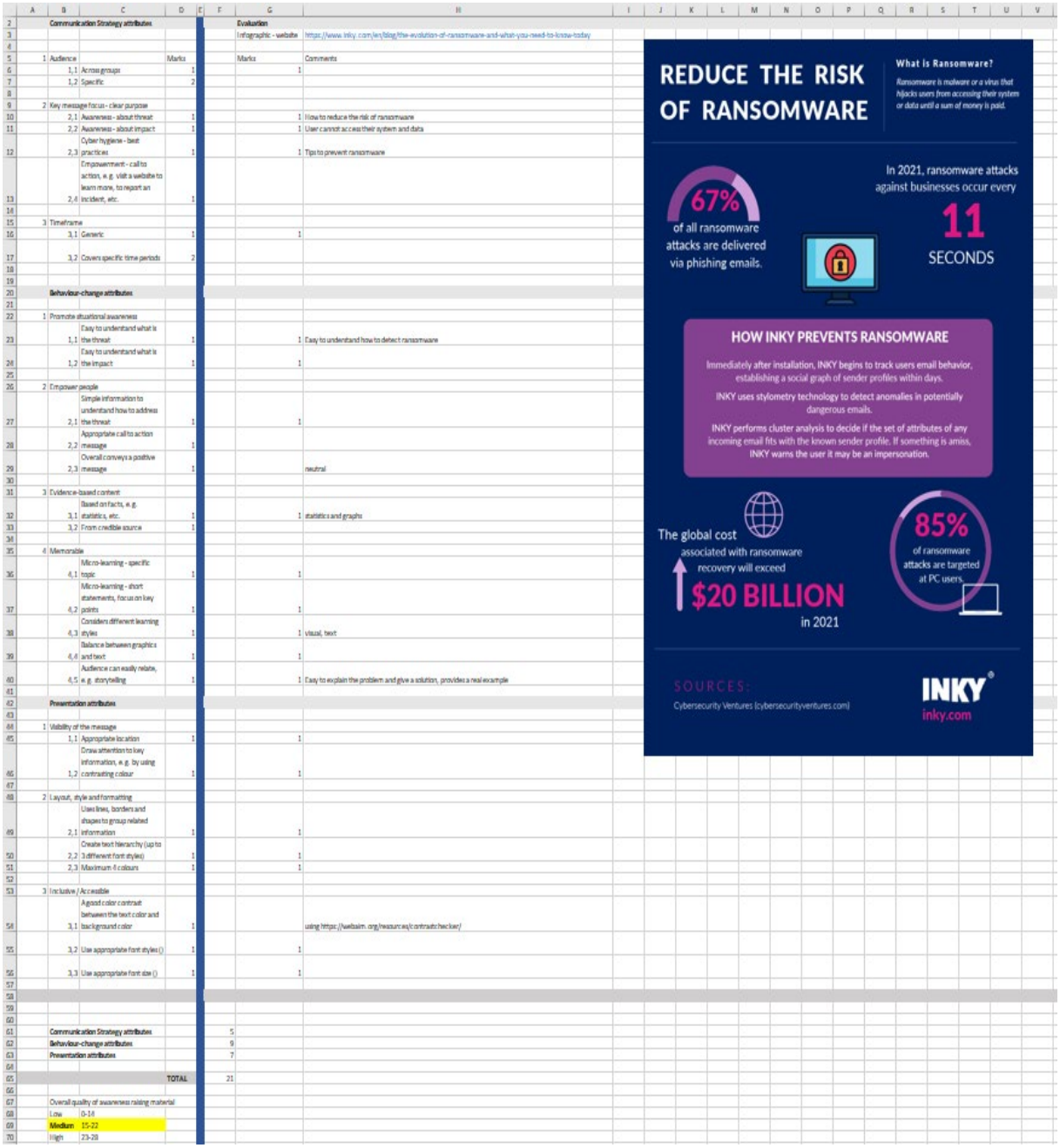
	Communication Strategy attributes				**Evaluation**				
					Infographic - website		https://symbolsecurity.com/2020/01/07/what-is-spear-phishing-and-why-is-it-so-dangerous-2/		
1	Audience		Marks		Marks		Comments		
		1,1 Across groups	1			1			
		1,2 Specific	2						
2	Key message focus - clear purpose								
		2,1 Awareness - about threat	1			1	difference between phishing and spear phishing		
		2,2 Awareness - about impact	1						
		2,3 Cyber hygiene - best practices	1			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						
2	Empower people								
		2,1 Simple information to understand how to address the threat	1			1			
		2,2 Appropriate call to action message	1			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	Examples/ 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			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			1	tips to avoid spear phishing		
	Presentation attributes								
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 4 colours	1			1			
3	Inclusive / Accessible								
		3,1 A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/		
		3,2 Use appropriate font styles ()	1			1			
		3,3 Use appropriate font size ()	1						
	Communication Strategy attributes				5				
	Behaviour-change attributes				8				
	Presentation attributes				6				
			TOTAL		19				
	Overall quality of awareness raising material								
	Low	0-14							
	Medium	15-22							
	High	23-28							

A.2 Analysis Infographics 2021

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

infographics_framework_v2021.xlsx

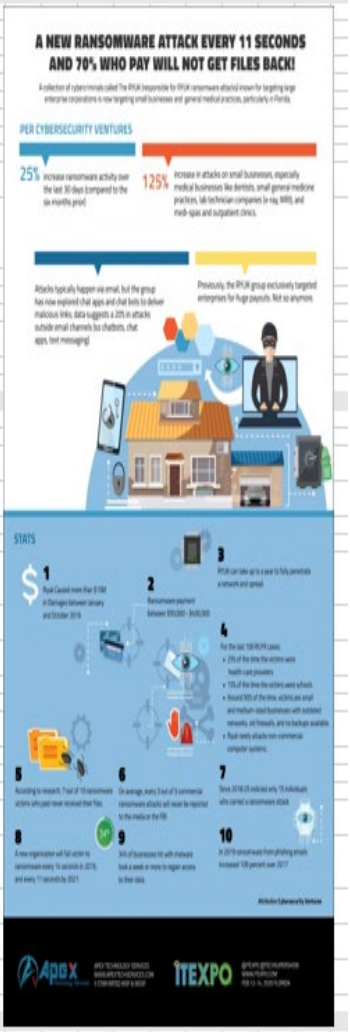
1)



	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.inky.com/en/blog/the-evolution-of-ransomware-and-what-you-need-to-know-today	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to reduce the risk of ransomware	
	2,2	Awareness - about impact	1		1	User cannot access their system and data	
	2,3	Cyber hygiene - best practices	1		1	Tips to prevent ransomware	
	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	Easy to understand how to detect ransomware	
	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 and graphs	
	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		1	Easy to explain the problem and give a solution, provides a real example	
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				5		
	Behaviour-change attributes				9		
	Presentation attributes				7		
			TOTAL		21		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

2)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://blog.trncnet.com/blog/rich-reinhart/security/infographic-a-new-ransomware-attack-every-11-seconds-70-who-pay-do-not-get-files-back.html	
1	Audience		Marks		Marks	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	Empowernment - 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 convey a positive message	1			neutral	
3	Evidence-based content						
	3,1	Based on facts, e.g. statistics, etc.	1		1	statistics/ 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				
	Presentation attributes						
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 4 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				
	Communication Strategy attributes			5			
	Behaviour-change attributes			8			
	Presentation attributes			6			
			TOTAL	19			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					



3)

	B	C	D	E	F	G	H
2	**Communication Strategy attributes**					**Evaluation**	
3						Infographic - website	https://content.transunion.com/v/fraud-trends-infographic-q3
4							
5	Audience		Marks			Marks	Comments
6	1,1	Across groups	1				
7	1,2	Specific	2			2	Employees/Organizations
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	**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				
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	**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	
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			**TOTAL**		18		
66							
67	Overall quality of awareness raising material						
68	Low	0-14					
69	**Medium**	15-22					
70	High	23-28					
71							

4)

Communication Strategy attributes				**Evaluation**			
				Infographic - website		https://www.clearconcepts.ca/insights/7-tips-to-identify-phishing-emails	
Audience			Marks		Marks	Comments	
1,1	Across groups		1				
1,2	Specific		2		2	Baby boomers/Generation X	
Key message focus - clear purpose							
2,1	Awareness - about threat		1		1	how to avoid phishing emails	
2,2	Awareness - about impact		1				
2,3	Cyber hygiene - best practices		1		1		
2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.		1		1	report the incident	
Timeframe							
3,1	Generic		1		1		
3,2	Covers specific time periods		2				
Behaviour-change attributes							
Promote situational awareness							
1,1	Easy to understand what is the threat		1		1		
1,2	Easy to understand what is the impact		1				
Empower people							
2,1	Simple information to understand how to address the threat		1		1		
2,2	Appropriate call to action message		1		1		
2,3	Overall conveys a positive message		1			neutral	
Evidence-based content							
3,1	Based on facts, e.g. statistics, etc.		1		1	examples	
3,2	From credible source		1				
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				
4,4	Balance between graphics and text		1		1		
4,5	Audience can easily relate, e.g. storytelling		1		1	tips to identify phishing emails	
Presentation attributes							
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		
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				
2,3	Maximum 4 colours		1		1		
Inclusive / Accessible							
3,1	A good color contrast between the text color and background color		1			using https://webaim.org/resources/contrastchecker/	
3,2	Use appropriate font styles ()		1		1		
3,3	Use appropriate font size ()		1		1		
Communication Strategy attributes				6			
Behaviour-change attributes				8			
Presentation attributes				6			
			TOTAL	20			
Overall quality of awareness raising material							
Low	0-14						
Medium	15-22						
High	23-28						

5)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://clara.comin.com/project/phishing-infographic/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Millenials/Generation Z	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1		
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	report an incident	
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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		1		
	2,3	Overall conveys a positive message	1				
3	Evidence-based content						
	3,1	Based on facts, e.g. statistics, etc.	1		1	statistics/examples	
	3,2	From credible source	1		1	enisa	
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		1	if your victim of phishing attacks what you do	
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			6			
	Behaviour-change attributes			10			
	Presentation attributes			8			
			TOTAL	24			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

6)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://logrhythm.com/blog/6-cybersecurity-predictions-for-2021/	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1					
	1,2	Specific	2			2	employees/ companies	
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1		
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1			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					
2	Empower people							
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			1		
	2,3	Overall conveys 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		
	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					
	Presentation attributes							
1	Visibility of the message							
	1,1	Appropriate location	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 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
	Communication Strategy attributes					5		
	Behaviour-change attributes					6		
	Presentation attributes					6		
			TOTAL			17		
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

7)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.europol.europa.eu/publications-events/publications/mobile-malware-infographics	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Millenials/Generation Z	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	how to install apps	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	download mobile secure app	
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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		1		
	2,3	Overall conveys 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		1	Europol	
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				
		Presentation attributes					
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			G		
		Behaviour-change attributes			B		
		Presentation attributes			B		
			TOTAL		22		
		Overall quality of awareness raising material					
	Low	0-14					
	Medium	15-22					
	High	23-28					

8)

	Communication Strategy attributes				**Evaluation**			
					Infographic - website		https://www.synovus.com/business/resource-center/protecting-your-business/how-to-recognize-bec-infographic/	
1	Audience		Marks		Marks	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			
	2,3	Cyber hygiene - best practices	1		1			
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	Education employees		
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		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		1			
	4,3	Considers different learning styles	1		1			
	4,4	Balance between graphics and text	1		1			
	4,5	Audience can easily relate, e.g. storytelling	1		1			
	Presentation attributes							
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 4 colours	1		1			
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1		1			
	3,2	Use appropriate font styles ()	1		1			
	3,3	Use appropriate font size ()	1		1			
	Communication Strategy attributes			7				
	Behaviour-change attributes			10				
	Presentation attributes			8				
			TOTAL	25				
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

9)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website	https://www.europol.europa.eu/publications-events/publications/carbanak/cobalt-infographic		
1	Audience		Marks		Marks	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	Financial institutions threat		
	2,2	Awareness - about impact	1		1	Impact to bank companies		
	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, visual, graphics		
	3,2	From credible source	1		1	Europol		
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		1	real examples/ statistics		
		Presentation attributes						
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 https://webaim.org/resources/contrastchecker/		
	3,2	Use appropriate font styles ()	1		1			
	3,3	Use appropriate font size ()	1		1			
		Communication Strategy attributes		5				
		Behaviour-change attributes		10				
		Presentation attributes		8				
			TOTAL	23				
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

10)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.acacu.com/privacy-security/common-phishing-scams	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1			1	Individuals and Employees	
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	Common holidays phishing attacks	
	2,2	Awareness - about impact	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					
	3,2	Covers specific time periods	2			2	Holiday season	
		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					
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					
	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					
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples	
		Presentation attributes						
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 https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles()	1			1		
	3,3	Use appropriate font size()	1			1		
		Communication Strategy attributes				4		
		Behaviour-change attributes				5		
		Presentation attributes				8		
				TOTAL		17		
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

11)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.i-scoop.eu/cybersecurity/phishing/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Microsoft Office users	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to be smart about credential Phishing	
	2,2	Awareness - about impact	1		1	It will get access to sensitive accounts and informations without setting off security alerts	
	2,3	Cyber hygiene - best practices	1		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				
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, examples	
	4,4	Balance between graphics and text	1		1		
	4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
	Presentation attributes						
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						
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			6			
	Behaviour-change attributes			8			
	Presentation attributes			7			
			TOTAL	21			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

12)

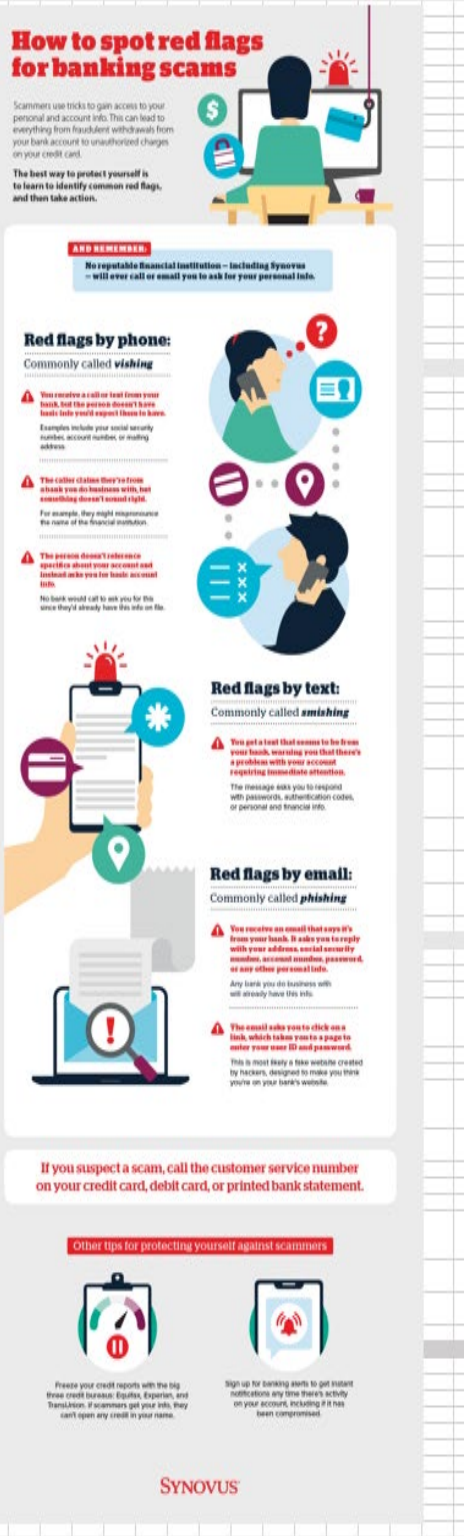
	Communication Strategy attributes						**Evaluation**							
							Infographic - website	https://www.kent.edu/it/security/phishing						
	1 Audience			Marks			Marks	Comments						
		1,1 Across groups		1										
		1,2 Specific		2				2 Baby boomers/Generation X						
	2 Key message focus - clear purpose													
		2,1 Awareness - about threat		1				1 How to not get hooked						
		2,2 Awareness - about impact		1				1						
		2,3 Cyber hygiene - best practices		1				1						
		Empowerment - call 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						
	3 Timeframe													
		3,1 Generic		1				1						
		3,2 Covers specific time periods		2										
	Behaviour-change attributes													
	1 Promote situational awareness													
		Easy to understand what is the												
		1,1 threat		1				1						
		Easy to understand what is the												
		1,2 impact		1				1						
	2 Empower people													
		Simple information to understand												
		2,1 how to address the threat		1										
		Appropriate call to action												
		2,2 message		1				1						
		Overall conveys a positive												
		2,3 message		1				Neutral						
	3 Evidence-based content													
		Based on facts, e.g. statistics,												
		3,1 etc.		1										
		3,2 From credible source		1										
	4 Memorable													
		4,1 Micro-learning - specific topic		1				1						
		Micro-learning - short												
		4,2 statements, focus on key points		1										
		4,3 Considers different learning styles		1				1 Visual, examples						
		Balance between graphics and												
		4,4 text		1										
		Audience can easily relate, e.g.												
		4,5 storytelling		1				1 real examples						
	Presentation attributes													
	1 Visibility of the message													
		1,1 Appropriate location		1										
		Draw attention to key												
		information, e.g. by using												
		1,2 contrasting colour		1				1						
	2 Layout, style and formatting													
		Use lines, borders and shapes to												
		2,1 group related information		1				1						
		Create text hierarchy (up to 3												
		2,2 different font styles)		1				1						
		2,3 Maximum 4 colours		1				1						
	3 Inclusive / Accessible													
		Agood color contrast between												
		the text color and background												
		3,1 color		1				1 using https://webaim.org/resources/contrastchecker/						
		3,2 Use appropriate font styles()		1				1						
		3,3 Use appropriate font size ()		1				1						
	Communication Strategy attributes						7							
	Behaviour-change attributes						6							
	Presentation attributes						7							
				TOTAL			20							
	Overall quality of awareness raising material													
	Low	0-14												
	Medium	15-22												
	High	23-28												

13)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website		https://www.europol.europa.eu/media-press/newsroom/news/love-online-shopping-here%E2%80%99s-how-to-protect-yourself-against-online-scammers
1	Audience		Marks		Marks		Comments
	1,1	Across groups	1				
	1,2	Specific	2			2	Individuals(Silvrit (70+)/Baby boomers)
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1			1	Rules of secure online shopping
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1			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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1			1	
	2,2	Appropriate call to action message	1			1	
	2,3	Overall conveys 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			1	Europol
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			1	
	4,5	Audience can easily relate, e.g. storytelling	1				
	Presentation attributes						
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 4 colours	1			1	
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/
	3,2	Use appropriate font styles ()	1			1	
	3,3	Use appropriate font size ()	1			1	
	Communication Strategy attributes				5		
	Behaviour-change attributes				8		
	Presentation attributes				7		
			TOTAL		20		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

14)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.synovus.com/personal/resource-center/financial-safety-and-security/infographic-how-to-spot-red-flags-for-banking-scams/	
	1 Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1	Individuals	
	1,2	Specific	2				
	2 Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to spot red flags for banking scams	
	2,2	Awareness - about impact	1		1		
	2,3	Cyber hygiene - best practices	1		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		1		
	2,3	Overall conveys 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		
	4,2	Micro-learning - short statements, focus on key points	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 Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
	3 Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				5		
	Behaviour-change attributes				7		
	Presentation attributes				7		
			TOTAL		19		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					



15)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://cba.ca/holiday-scams	
1	Audience		Marks		Marks	Comments	
	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 practices	1		1		
	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	
3	Timeframe						
	3.1	Generic	1				
	3.2	Covers specific time periods	2		2	Holiday scams	
	Behaviour-change attributes						
1	Promote situational awareness						
	1.1	Easy to understand what is the threat	1		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				
	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				
	4.4	Balance between graphics and text	1		1		
	4.5	Audience can easily relate, e.g. storytelling	1		1	learn how to avoid the treat	
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3.1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3.2	Use appropriate font styles ()	1		1		
	3.3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				6		
	Behaviour-change attributes				7		
	Presentation attributes				7		
			TOTAL		20		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

16)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.infosecinstitute.com/content-library/infographic-need-to-know-general-security/	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1			1	Individuals	
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1		
	2,2	Awareness - about impact	1			1		
	2,3	Cyber hygiene - best practices	1			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
	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			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	INFOSEC	
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			1	how to avoid the treat	
		Presentation attributes						
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 4 colours	1					
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
		Communication Strategy attributes				5		
		Behaviour-change attributes				10		
		Presentation attributes				6		
				TOTAL		21		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

17)

	B	C	D	E	F	G	H
2	**Communication Strategy attributes**					**Evaluation**	
3						Infographic - website	https://www.medsphere.com/resources/protecting-against-phishing-attacks-infographic-poster/
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	**Behaviour-change attributes**						
21							
22	Promote situational awareness						
23	1,1	Easy to understand what is the threat	1			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	**Presentation attributes**						
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 (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				using https://webaim.org/resources/contrastchecker/
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					

18)

	Communication Strategy attributes			Evaluation			
				Infographic - website		https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/safety-guide-for-new-normal-after-covid-19	
1	Audience		Marks	Marks		Comments	
	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		1		
	2,3	Cyber hygiene - best practices	1		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		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	EUROPOL	
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				
	4,5	Audience can easily relate, e.g. storytelling	1		1	how to avoid the treat/ real examples	
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			5			
	Behaviour-change attributes			10			
	Presentation attributes			7			
			TOTAL	22			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

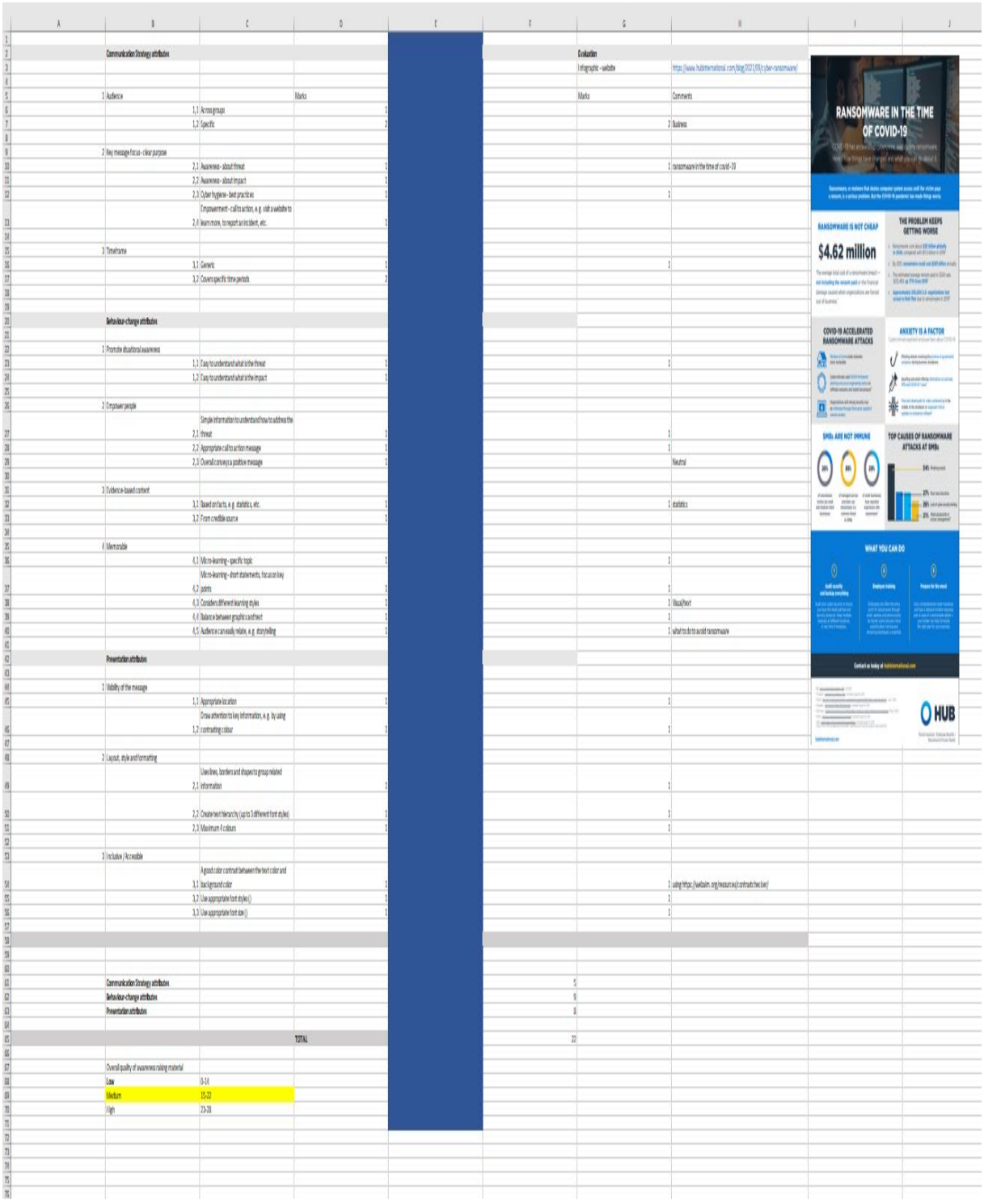
19)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to protect from cyber attacks	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	report the incident	
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		1		
	2,3	Overall conveys 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		1	EUROPOL	
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				
	4,5	Audience can easily relate, e.g. storytelling	1		1	how to avoid the treat/ real examples	
	Presentation attributes						
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	[illegible]					
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				5		
	Behaviour-change attributes				9		
	Presentation attributes				8		
			TOTAL		22		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

20)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Business	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1		
	2,2	Awareness - about impact	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				
	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				
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				
	4,5	Audience can easily relate, e.g. storytelling	1				
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1				
	Communication Strategy attributes			4			
	Behaviour-change attributes			5			
	Presentation attributes			6			
			TOTAL	15			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

21)



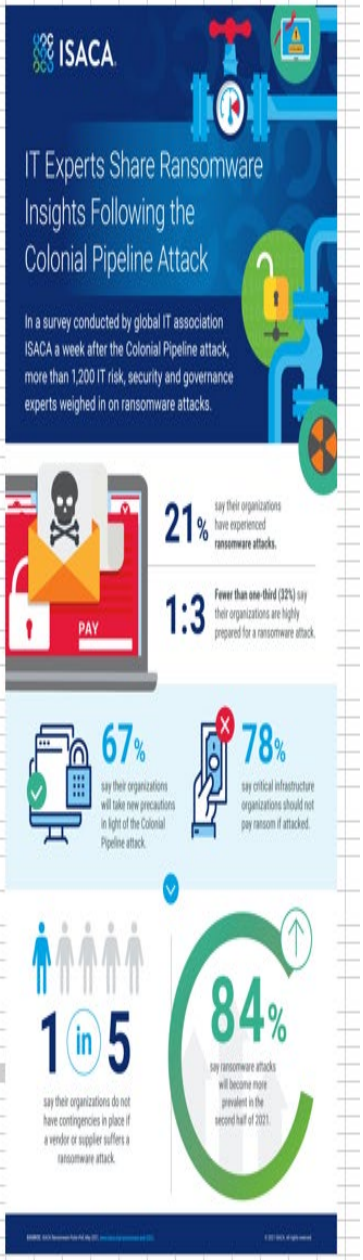
	Communication Strategy attributes					Evaluation			
						Infographic - website	https://www.hubinternational.com/blog/2021/09/cyber-ransomware/		
	1. Audience		Marks			Marks	Comments		
		1.1. Across groups	1						
		1.2. Specific	2				2. Business		
	2. Key message focus - clear purpose								
		2.1. Awareness - about threat	1				1. ransomware in the time of covid-19		
		2.2. Awareness - about impact	1						
		2.3. Cyber hygiene - best practices	1				1		
		Empowerment - call to action, e.g. visit a website to							
		2.4. 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. Promotes situational awareness								
		1.1. Easy to understand what is the threat	1				1		
		1.2. Easy to understand what is the impact	1						
	2. Empower people								
		Simple information to understand how to address the							
		2.1. threat	1				1		
		2.2. Appropriate call to action message	1				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		
		Micro-learning - short statements, focus on key							
		4.2. 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				1. what to do to avoid ransomware		
	Presentation attributes								
	1. Visibility of the message								
		1.1. Appropriate location	1				1		
		Draw attention to key information, e.g. by using							
		1.2. contrasting colour	1				1		
	2. Layout, style and formatting								
		Uses lines, borders and shapes to group related							
		2.1. information	1				1		
		2.2. Creates text hierarchy (up to 3 different font styles)	1				1		
		2.3. Maximum 4 colours	1				1		
	3. Inclusive / Accessible								
		A good color contrast between the text color and							
		3.1. background color	1				1. using https://webaim.org/resources/contrastchecker/		
		3.2. Use appropriate font style()	1				1		
		3.3. Use appropriate font size()	1				1		
	Communication Strategy attributes					5			
	Behaviour-change attributes					9			
	Presentation attributes					8			
			TOTAL			22			
	Overall quality of awareness raising material								
	Low	0-14							
	Medium	15-22							
	High	23-30							

22)

	Communication Strategy attributes					Evaluation		
						Infographic - website	https://www.ncsc.co.uk/collection/scams/	
	1 Audience		Marks			Marks	Comments	
		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 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					
	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					
		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					
	Presentation attributes							
	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 4 colours	1			1		
	3 Inclusive / Accessible							
		3_1 Good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/	
		3_2 Use appropriate font style(s)	1			1		
		3_3 Use appropriate font size ()	1			1		
	Communication Strategy attributes				4			
	Behaviour change attributes				5			
	Presentation attributes				0			
				TOTAL	17			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

23)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website		https://www.businesswire.com/news/home/20210524007268/en/ISACA-Survey-IT-Security-and-Risk-Experts-Share-Ransomware-Insights-in-the-Aftermath-of-the-Colonial-Pipeline-Attack
	1	Audience	Marks		Marks		Comments
		1,1 Across groups	1				
		1,2 Specific	2			2	Business
	2	Key message focus - clear purpose					
		2,1 Awareness - about threat	1			1	
		2,2 Awareness - about impact	1				
		2,3 Cyber hygiene - best practices	1				
		Empowerment - call to action, e.g. visit a website to learn more, to report an					
		2,4 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				
	2	Empower people					
		Simple information to understand how to					
		2,1 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	
		Micro-learning - short statements, focus on					
		4,2 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				
		Presentation attributes					
	1	Visibility of the message					
		1,1 Appropriate location	1			1	
		Draw attention to key information, e.g. by					
		1,2 using contrasting colour	1			1	
	2	Layout, style and formatting					
		Uses lines, borders and shapes to group					
		2,1 related information	1			1	
		Create text hierarchy (up to 3 different font					
		2,2 styles)	1			1	
		2,3 Maximum 4 colours	1			1	
	3	Inclusive / Accessible					
		Agood color contrast between the text					
		3,1 color and background color	1			1	using https://webaim.org/resources/contrastchecker/
		3,2 Use appropriate font styles()	1			1	
		3,3 Use appropriate font size ()	1			1	
		Communication Strategy attributes			4		
		Behaviour-change attributes			5		
		Presentation attributes			6		
				TOTAL	15		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

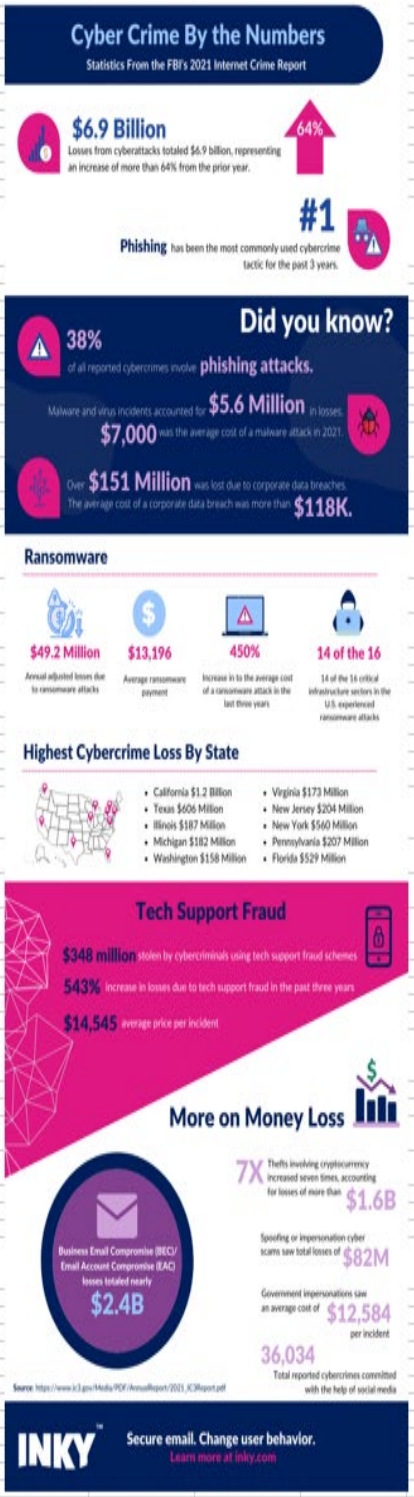


24)

			Marks	Evaluation Marks	Comments
Communication Strategy attributes				**Evaluation**	
				Infographic - website	https://gemma.gov.mt/phishing-scam/
1	Audience		Marks	Marks	Comments
	1,1	Across groups	1	1	
	1,2	Specific	2		
2	Key message focus - clear purpose				
	2,1	Awareness - about threat	1	1	Phishing attacks
	2,2	Awareness - about impact	1		
	2,3	Cyber hygiene - best practices	1	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		
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		
	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		
Presentation attributes					
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 4 colours	1		
3	Inclusive / Accessible				
	3,1	A good color contrast between the text color and background color	1	1	using https://webaim.org/resources/contrastchecker/
	3,2	Use appropriate font styles ()	1	1	
	3,3	Use appropriate font size ()	1	1	
Communication Strategy attributes				4	
Behaviour-change attributes				5	
Presentation attributes				6	
			TOTAL	15	
Overall quality of awareness raising material					
Low	0-14				
Medium	15-22				
High	23-28				

25)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.inky.com/en/blog/infographic-fbi-2021-internet-crime-report	
	1	Audience		Marks		Marks		Comments
			1,1	Across groups	1		1	
			1,2	Specific	2			
	2	Key message focus - clear purpose						
			2,1	Awareness - about threat	1		1	statistics about cyber crimes
			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			
		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		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		1	
			4,3	Considers different learning styles	1		1	Visual/text
			4,4	Balance between graphics and text	1			
			4,5	Audience can easily relate, e.g. storytelling	1			
		Presentation attributes						
	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 4 colours	1		1	
	3	Inclusive / Accessible						
			3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/
			3,2	Use appropriate font styles()	1		1	
			3,3	Use appropriate font size ()	1		1	
		Communication Strategy attributes				4		
		Behaviour-change attributes				5		
		Presentation attributes				6		
				TOTAL		15		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

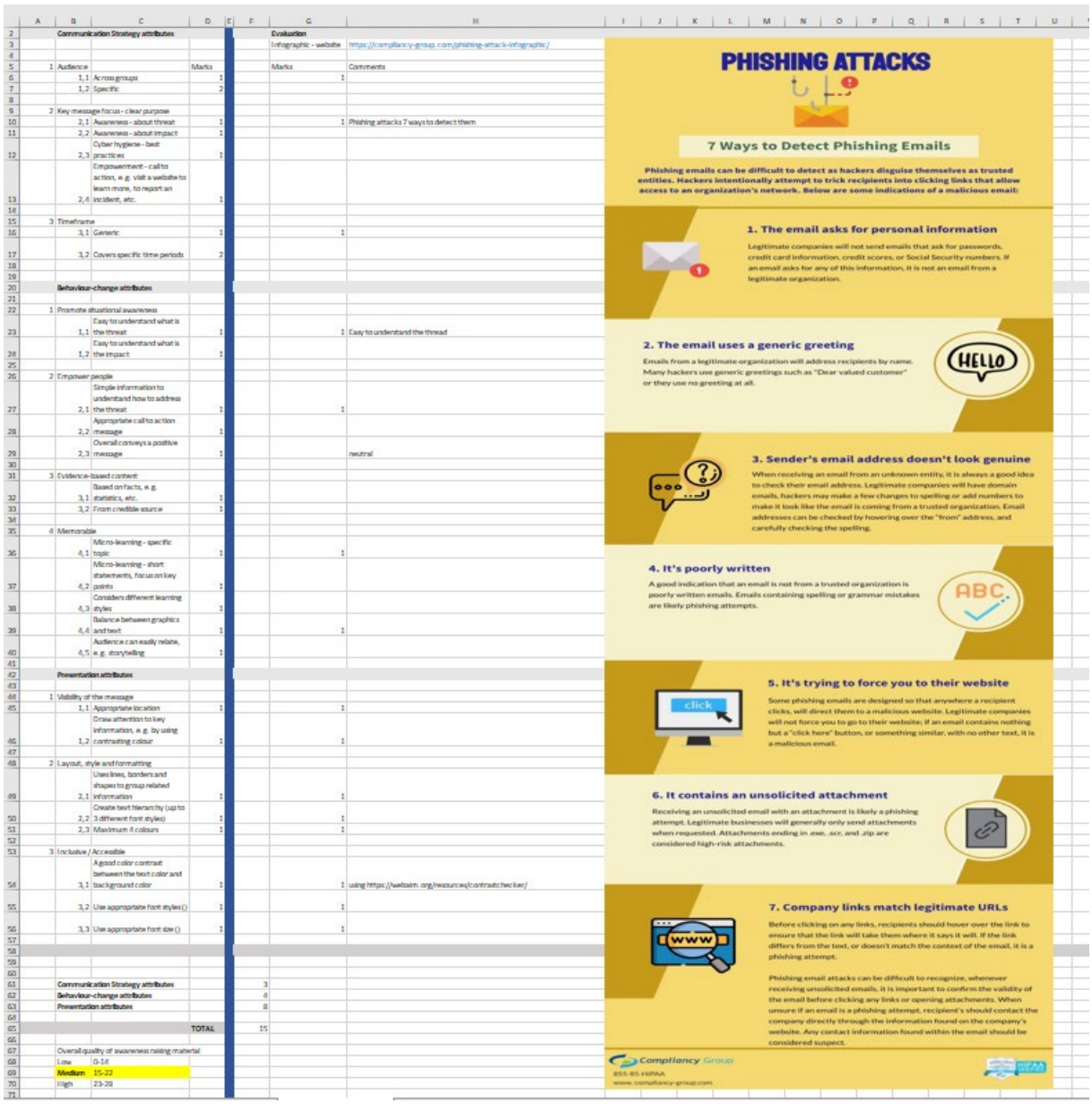


A.3 Analysis Infographics 2022

The excel file contains all the evaluation of the twenty-five infographics for the year 2022.

infographics_framework_v2022.xlsx

1)



		Communication Strategy attributes				Evaluation		
						Infographic - website	https://compliancy-group.com/phishing-attack-infographic/	
	1	Audience		Marks		Marks		Comments
		1,1	Across groups	1			1	
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1			1	Phishing attacks 7 ways to detect them
		2,2	Awareness - about impact	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				
		Behaviour-change attributes						
	1	Promote situational awareness						
		1,1	Easy to understand what is the threat	1			1	Easy to understand the thread
		1,2	Easy to understand what is the impact	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				
		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				
		4,4	Balance between graphics and text	1			1	
		4,5	Audience can easily relate, e.g. storytelling	1				
		Presentation attributes						
	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 https://webaim.org/resources/contrastchecker/
		3,2	Use appropriate font styles ()	1			1	
		3,3	Use appropriate font size ()	1			1	
		Communication Strategy attributes			3			
		Behaviour-change attributes			4			
		Presentation attributes			8			
				TOTAL	15			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

2)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.judge.com/resources/blogs/cybersecurity-statistics-infographic-2022-data/	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	cyber statistics	
		2,2	Awareness - about impact	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				
		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				
	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/ 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				
		4,3	Considers different learning styles	1		1	visual/text	
		4,4	Balance between graphics and text	1				
		4,5	Audience can easily relate, e.g. storytelling	1				
		Presentation attributes						
	1	Visibility of the message						
		1,1	Appropriate location	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 4 colours	1		1		
	3	Inclusive / Accessible						
		3,1	Agood color contrast between the text color and background color	1		1		
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			3			
		Behaviour-change attributes			5			
		Presentation attributes			7			
				TOTAL	15			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

3)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	7 red flags of phishing threats	
		2,2	Awareness - about impact	1				
		2,3	Cyber hygiene - best practices	1		1		
		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	
	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				
	2	Empower people						
		2,1	Simple information to understand how to address the threat	1		1		
		2,2	Appropriate call to action message	1		1		
		2,3	Overall conveys 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		1	Get Cyber Safe	
	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				
		4,4	Balance between graphics and text	1				
		4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
		Presentation attributes						
	1	Visibility of the message						
		1,1	Appropriate location	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 4 colours	1				
	3	Inclusive / Accessible						
		3,1	A good color contrast between the text color and background color	1		1		
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			5			
		Behaviour-change attributes			6			
		Presentation attributes			6			
				TOTAL	17			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

3)

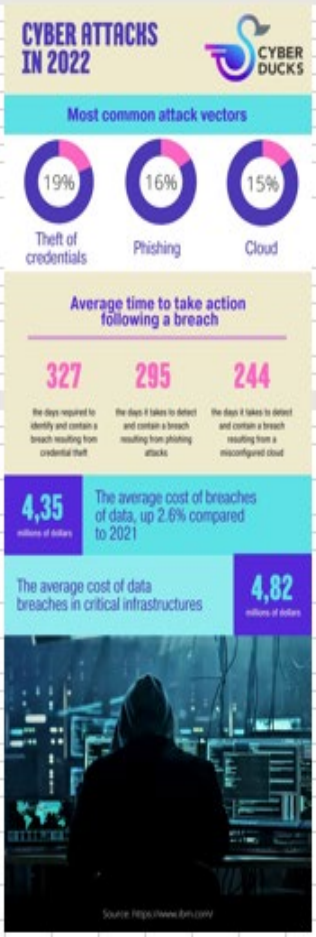
		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.hoxhunt.com/blog/infographic-make-or-break-phishing-metrics	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Employees	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	How to measure phishing metrics of organization	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		1	report the incident	
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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		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		1		
	4,3	Considers different learning styles	1				
	4,4	Balance between graphics and text	1		1		
	4,5	Audience can easily relate, e.g. storytelling	1		1	tips to identify phishing emails	
		Presentation attributes					
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 4 colours	1				
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes		6			
		Behaviour-change attributes		8			
		Presentation attributes		6			
			TOTAL	20			
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

4)

		Communication Strategy attributes			**Evaluation**			
					Infographic - website		https://consumer.ftc.gov/articles/dont-recognize-debt-infographic	
1	Audience		Marks		Marks		Comments	
	1,1	Across groups	1			1	Individuals	
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	If you do not recognize that debt what to do	
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1			1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report the incident	
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					
2	Empower people							
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			1		
	2,3	Overall conveys 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			1	Federal trade commission	
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					
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	how to spot the scam	
	Presentation attributes							
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 style)	1			1		
	2,3	Maximum 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
	Communication Strategy attributes				5			
	Behaviour-change attributes				8			
	Presentation attributes				8			
			TOTAL		21			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

5)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://cyberducks.it/en/infographics/255-cyber-attacks-in-2022.html	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Millenials/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				
	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				
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				
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			5			
	Behaviour-change attributes			7			
	Presentation attributes			8			
			TOTAL	20			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					



6)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/cyber-energy-week	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1					
	1,2	Specific	2			2	companies	
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	how to stay safe from ransomware	
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1			1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	report the incident	
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					
2	Empower people							
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			1		
	2,3	Overall conveys 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			1	enisa	
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					
		Presentation attributes						
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 4 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
		Communication Strategy attributes				6		
		Behaviour-change attributes				7		
		Presentation attributes				8		
				TOTAL		21		
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

7)

		Communication Strategy attributes			Evaluation			
					Infographic - website		https://www.enisa.europa.eu/news/cybersecurity-foreign-interference-in-the-eu-information-ecosystem	
1	Audience			Marks	Marks		Comments	
	1,1	Across groups	1			1		
	1,2	Specific	2					
2	Key message focus - clear purpose							
	2,1	Awareness - about threat	1			1	top cyber threats	
	2,2	Awareness - about impact	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					
		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					
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	enisa	
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		
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples	
		Presentation attributes						
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 8 colours	1			1		
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1			1		
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
		Communication Strategy attributes			3			
		Behaviour-change attributes			9			
		Presentation attributes			8			
				TOTAL	20			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

8)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://it.rutgers.edu/2022/11/22/cybersecurity-shopping-tips-for-the-holiday-season/	
	1 Audience		Marks		Marks	Comments	
		1,1 Across groups	1		1		
		1,2 Specific	2				
	2 Key message focus - clear purpose						
		2,1 Awareness - about threat	1		1	holiday shopping scams to avoid	
		2,2 Awareness - about impact	1				
		2,3 Cyber hygiene - best practices	1		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				
		3,2 Covers specific time periods	2		2	holiday season	
	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				
	2 Empower people						
		2,1 Simple information to understand how to address the threat	1		1		
		2,2 Appropriate call to action message	1		1		
		2,3 Overall conveys 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		
		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				
	Presentation attributes						
	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 4 colours	1		1		
	3 Inclusive / Accessible						
		3,1 A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2 Use appropriate font styles ()	1		1		
		3,3 Use appropriate font size ()	1		1		
	Communication Strategy attributes			5			
	Behaviour-change attributes			7			
	Presentation attributes			8			
			TOTAL	20			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

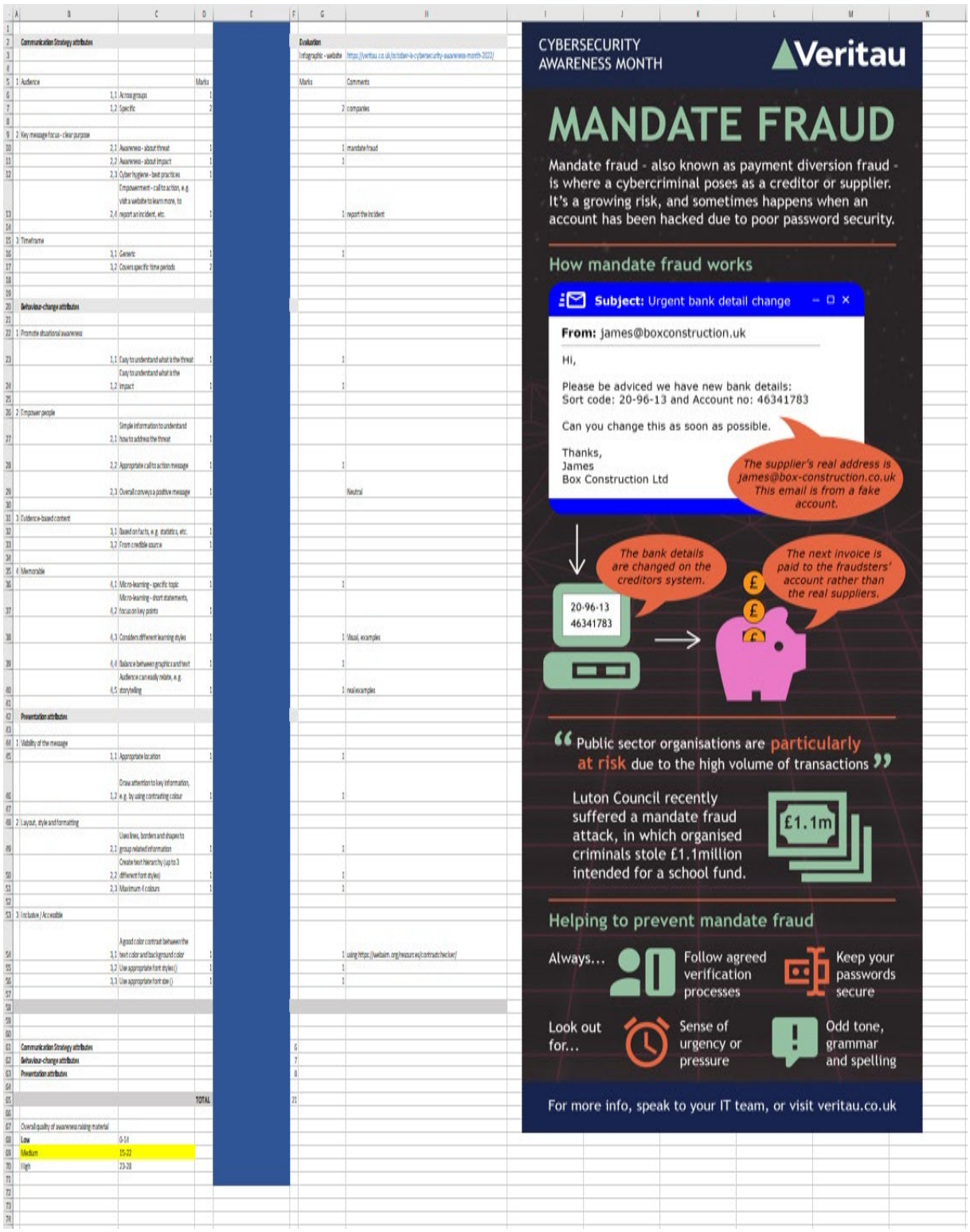
9)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.hongkiat.com/blog/internet-scam-hotspots-infographic/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1	Individuals	
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	different scams	
	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				
	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		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				
	4,4	Balance between graphics and text	1		1		
	4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
	Presentation attributes						
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			4			
	Behaviour-change attributes			8			
	Presentation attributes			7			
			TOTAL	19			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

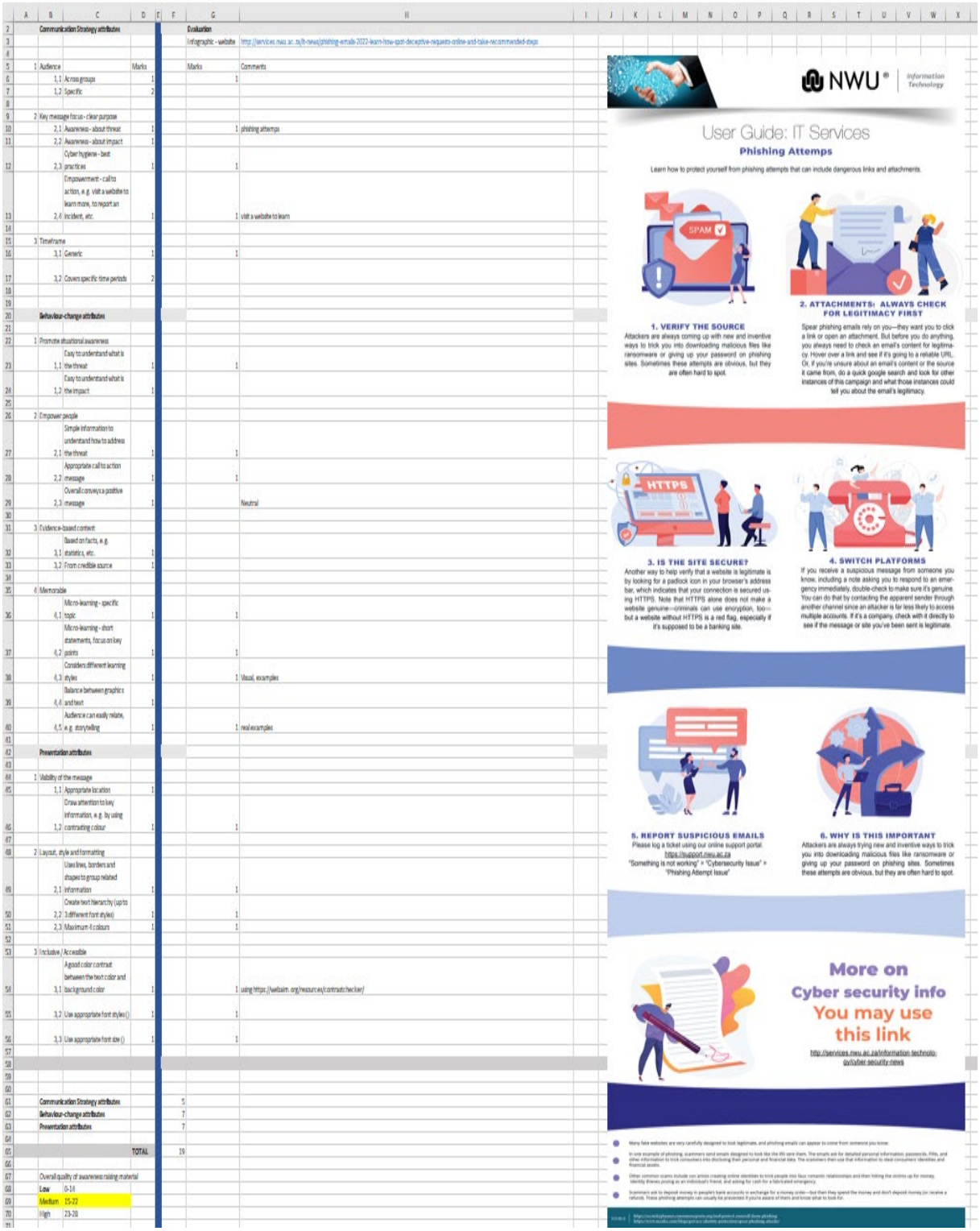
10)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.infosecinstitute.com/content-library/infographic-need-to-know-social-engineering/	
1	Audience		Marks			Marks	Comments	
	1,1	Across groups	1					
	1,2	Specific	2			2	Millenials/Generation Z	
2	Key message focus - clear purpose							
	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 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			1		
	2,3	Overall conveys 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			1	Infosec	
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, examples	
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	real examples	
		Presentation attributes						
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 4 colours	1					
3	Inclusive / Accessible							
	3,1	A good color contrast between the text color and background color	1				using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1					
		Communication Strategy attributes				6		
		Behaviour-change attributes				9		
		Presentation attributes				5		
					TOTAL	20		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

11)


CYBERSECURITY AWARENESS MONTH
Veritau
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 adviced 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.
20-96-13
46341783
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.
£1.1m
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

12)



	Communication Strategy attributes				**Evaluation**		
					Infographic - website		http://services.nwu.ac.za/it-news/phishing-emails-2022-learn-how-spot-deceptive-requests-online-and-take-recommended-steps
1	Audience		Marks		Marks		Comments
	1,1	Across groups	1			1	
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1			1	phishing attemps
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1			1	
	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
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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1			1	
	2,2	Appropriate call to action message	1			1	
	2,3	Overall conveys 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	
	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	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1			1	
3	Inclusive / Accessible						
	3,1	Agood color contrast between the text color and background color	1			1	using https://webaim.org/resource/x/contrastchecker/
	3,2	Use appropriate font styles()	1			1	
	3,3	Use appropriate font size ()	1			1	
	Communication Strategy attributes				5		
	Behaviour-change attributes				7		
	Presentation attributes				7		
			TOTAL		19		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

13)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.europol.europa.eu/publications-events/publications/crypto-investment-scams-infographic	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	crypto investment scams	
		2,2	Awareness - about impact	1				
		2,3	Cyber hygiene - best practices	1		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				
	2	Empower people						
		2,1	Simple information to understand how to address the threat	1		1		
		2,2	Appropriate call to action message	1		1		
		2,3	Overall conveys 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		1	europol	
	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				
		4,4	Balance between graphics and text	1		1		
		4,5	Audience can easily relate, e.g. storytelling	1		1	Real examples	
		Presentation attributes						
	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 4 colours	1		1		
	3	Inclusive / Accessible						
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes				6		
		Behaviour-change attributes				7		
		Presentation attributes				8		
				TOTAL		19		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

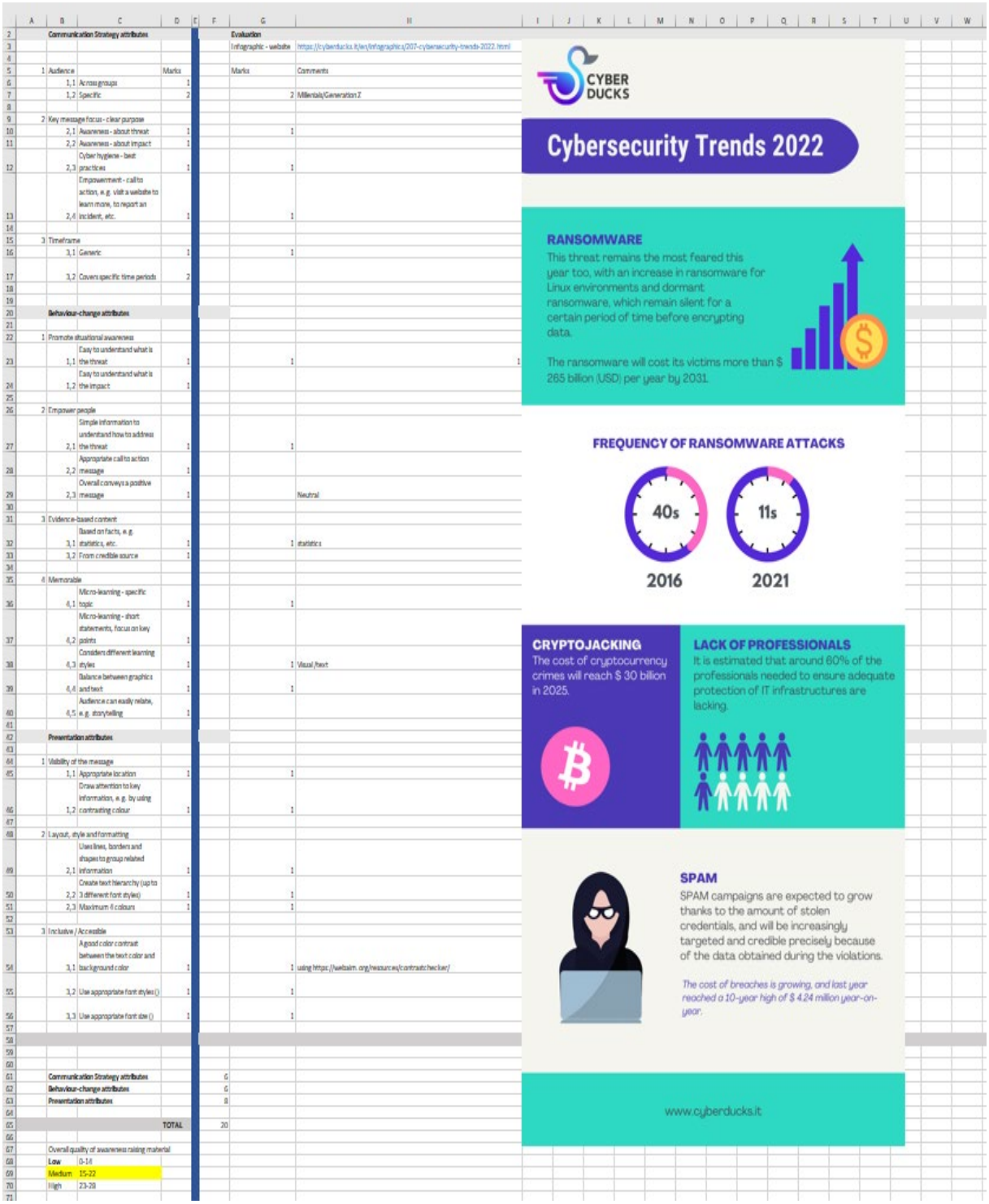
14)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.aba.com/news-research/analysis-guides/how-to-safely-use-mobile-payment-apps-and-services	
1		Audience		Marks		Marks	Comments	
	1,1	Across groups	1					
	1,2	Specific	2			2	Individuals (Millenials/Generation Z)	
2		Key message focus - clear purpose						
	2,1	Awareness - about threat	1			1		
	2,2	Awareness - about impact	1					
	2,3	Cyber hygiene - best practices	1			1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			1	to report an incident	
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					
2		Empower people						
	2,1	Simple information to understand how to address the threat	1			1		
	2,2	Appropriate call to action message	1			1		
	2,3	Overall conveys 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		
	4,2	Micro-learning - short statements, focus on key points	1			1		
	4,3	Considers different learning styles	1					
	4,4	Balance between graphics and text	1			1		
	4,5	Audience can easily relate, e.g. storytelling	1			1	how to protect your account	
		Presentation attributes						
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 https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1			1		
	3,3	Use appropriate font size ()	1			1		
		Communication Strategy attributes				6		
		Behaviour-change attributes				7		
		Presentation attributes				8		
				TOTAL		21		
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

15)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.ncitech.co.uk/blog/2022-03-15-spear-phishing-how-to-keep-your-organisation-off-the-hook	
	1	Audience	Marks		Marks	Comments	
		1,1 Across groups	1		1	Individuals/groups	
		1,2 Specific	2				
	2	Key message focus - clear purpose					
		2,1 Awareness - about threat	1		1	spear phishing	
		2,2 Awareness - about impact	1				
		2,3 Cyber hygiene - best practices	1		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
		1,2 Easy to understand what is the impact	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		1		
		2,3 Overall conveys 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		
		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		1	how to avoid the treat	
		Presentation attributes					
	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 4 colours	1		1		
	3	Inclusive / Accessible					
		3,1 A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2 Use appropriate font styles ()	1		1		
		3,3 Use appropriate font size ()	1		1		
		Communication Strategy attributes		4			
		Behaviour-change attributes		7			
		Presentation attributes		8			
			TOTAL	19			
		Overall quality of awareness raising material					
		Low 0-14					
		Medium 15-22					
		High 23-28					

16)

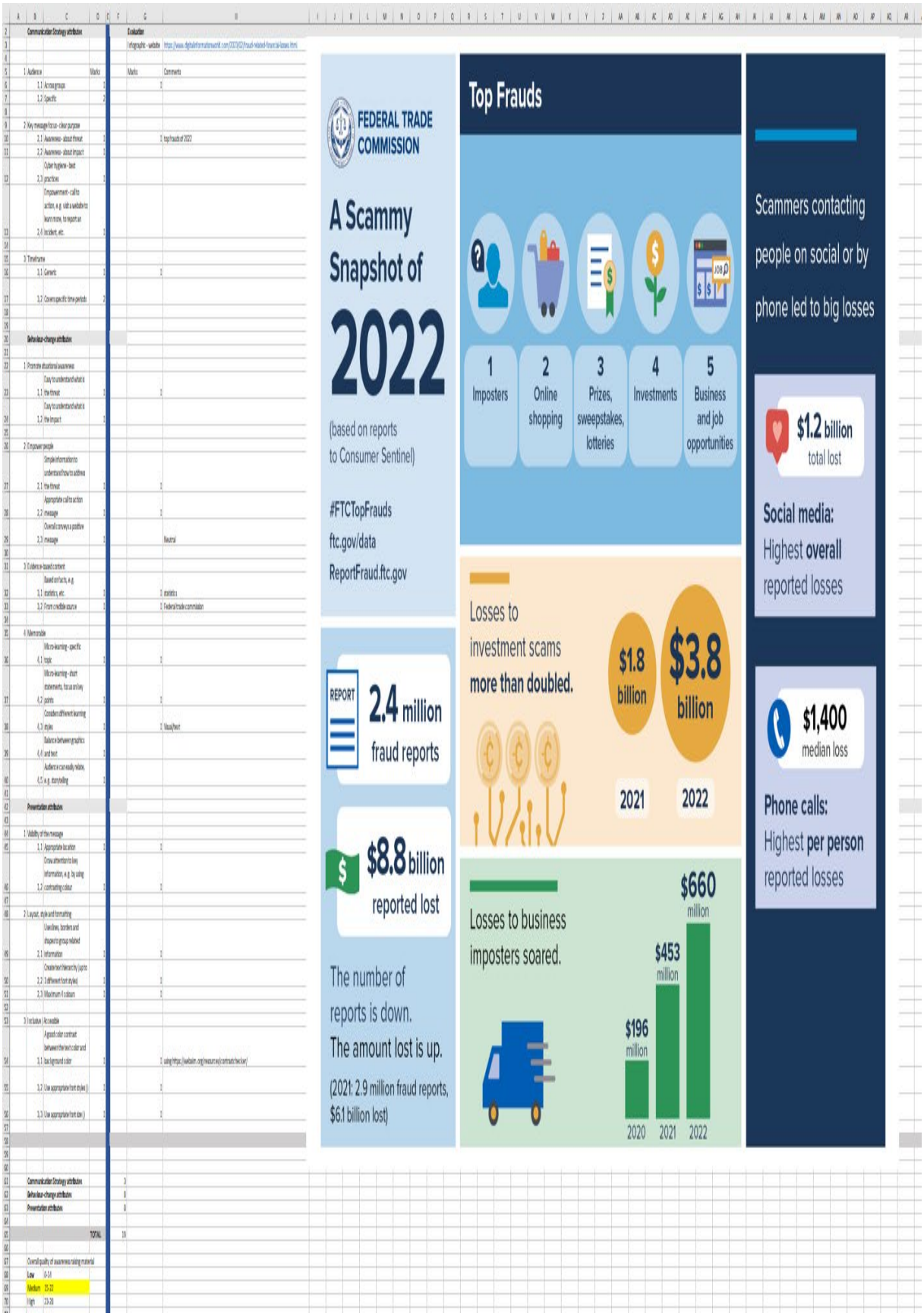


	Communication Strategy attributes				**Evaluation**			
					Infographic - website		https://cyberducks.it/en/infographics/2017-cybersecurity-trends-2022.html	
	1	Audience		Marks	Marks		Comments	
		1,1	Across groups	1				
		1,2	Specific	2		2	Millenials/Generation Z	
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1		
		2,2	Awareness - about impact	1				
		2,3	Cyber hygiene - best practices	1		1		
		2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1		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
		1,2	Easy to understand what is the impact	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				
	Presentation attributes							
	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 4 colours	1		1		
	3	Inclusive / Accessible						
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				6			
	Behaviour-change attributes				6			
	Presentation attributes				8			
				TOTAL	20			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

17)

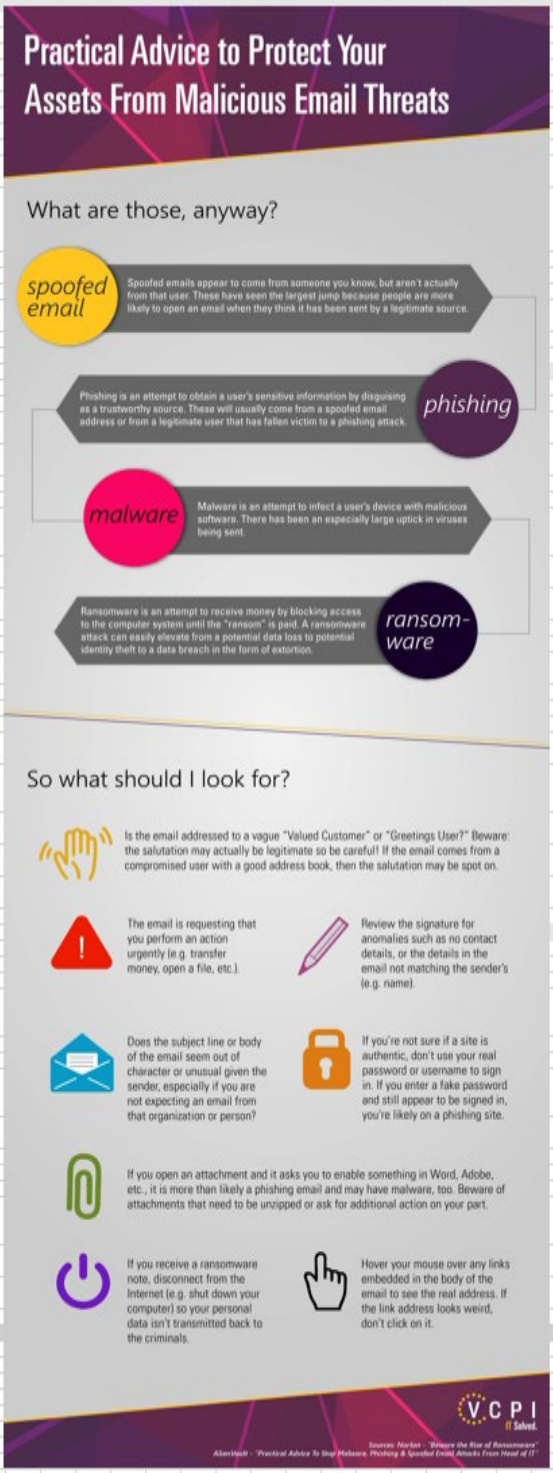
	Communication Strategy attributes				Evaluation		
					Infographic - website	https://www.slicktext.com/blog/2022/10/17-spam-text-statistics-for-2022/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	Spam texting	
	2,2	Awareness - about impact	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				
	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				
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		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		1	how to avoid the treat/ real examples	
	Presentation attributes						
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	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	Agood color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font style()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			3			
	Behaviour-change attributes			0			
	Presentation attributes			0			
			TOTAL	10			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

18)


FEDERAL TRADE COMMISSION
A Scammy Snapshot of 2022
(based on reports to Consumer Sentinel)
#FTCTopFrauds
ftc.gov/data
ReportFraud.ftc.gov
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)
Top Frauds
1 Imposters
2 Online shopping
3 Prizes, sweepstakes, lotteries
4 Investments
5 Business and job opportunities
Losses to investment scams more than doubled.
$1.8 billion
$3.8 billion
2021
2022
Losses to business imposters soared.
$196 million
$453 million
$660 million
2020
2021
2022
Scammers contacting people on social or by phone led to big losses
$1.2 billion total lost
Social media: Highest overall reported losses
$1,400 median loss
Phone calls: Highest per person reported losses

19)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.vcpi.com/how-to-protect-yourself-from-malicious-email-threats/	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	how to protect your assets from malicious email threads	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		1		
	2,3	Overall conveys 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		
	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				
	4,5	Audience can easily relate, e.g. storytelling	1				
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			4			
	Behaviour-change attributes			5			
	Presentation attributes			8			
			TOTAL	17			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					



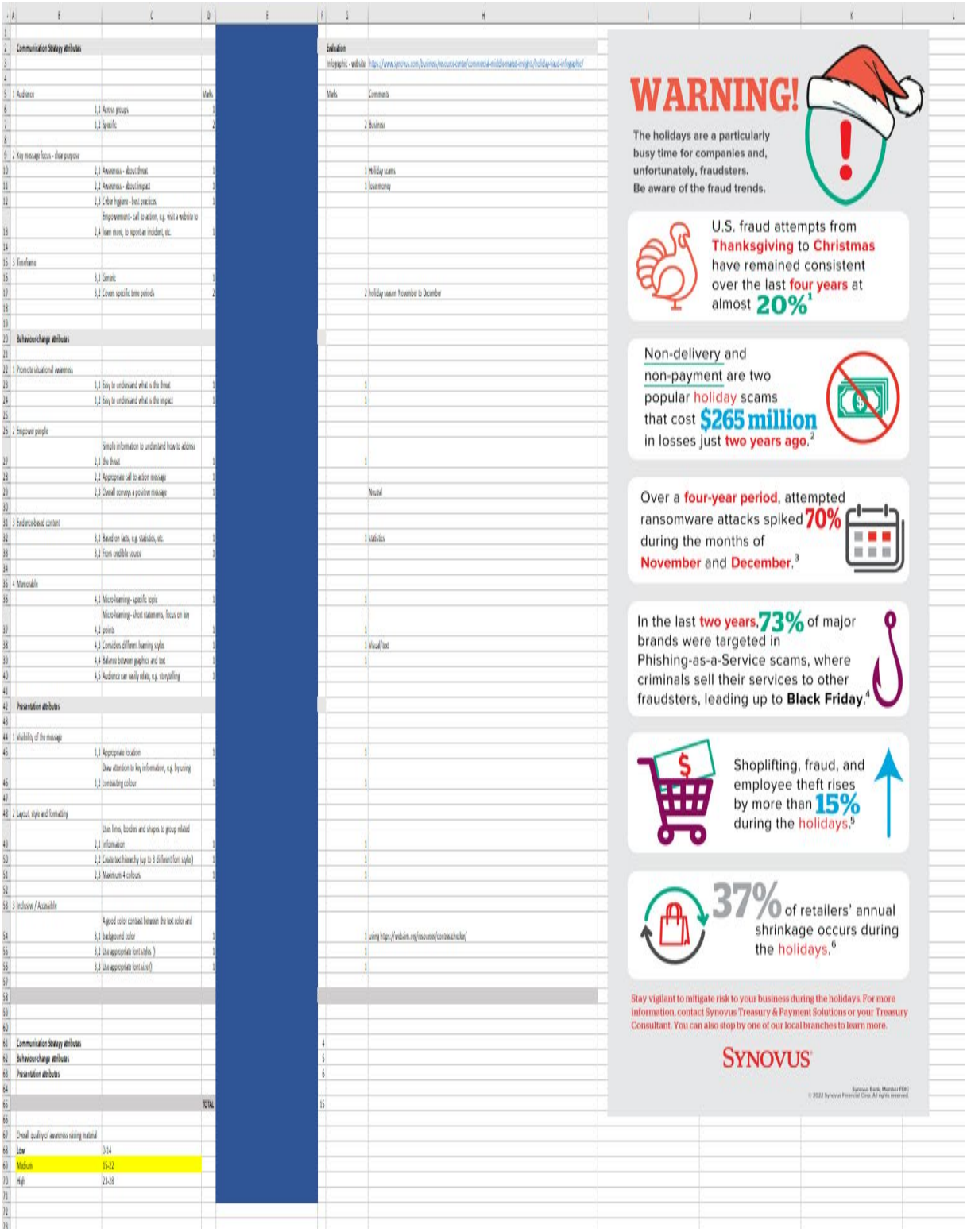
20)

	Communication Strategy attributes					Evaluation						
						Infographic - website	https://ciosea.economictimes.indiatimes.com/news/security/infographic-top-security-threats-in-2022/89340447?redirect=1					
	1 Audience			Marks		Marks	Comments					
		1.1	Across groups	1			1 individuals/employees					
		1.2	Specific	2								
	2 Key message focus - clear purpose											
		2.1	Awareness - about threat	1			1 top security threats					
		2.2	Awareness - about impact	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								
	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								
	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			1					
	Presentation attributes											
	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 4 colours	1			1					
	3 Inclusive / Accessible											
		3.1	A good color contrast between the text color and background color	1			1 using https://webaim.org/resources/contrastchecker/					
		3.2	Use appropriate font styles ()	1			1					
		3.3	Use appropriate font size ()	1			1					
	Communication Strategy attributes					3						
	Behaviour-change attributes					7						
	Presentation attributes					0						
				TOTAL		10						
	Overall quality of awareness raising material											
	Low	0-14										
	Medium	15-22										
	High	23-28										

21)

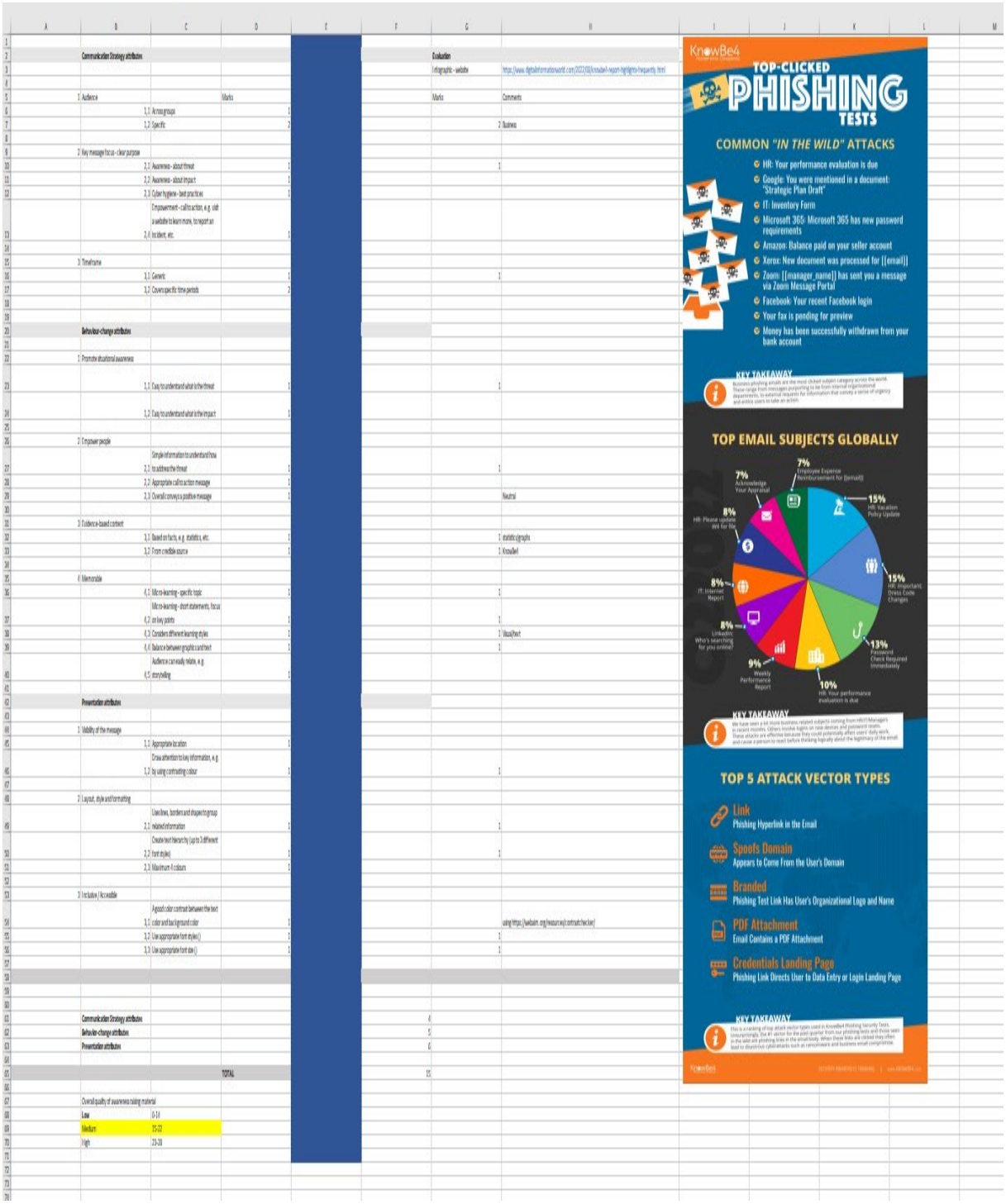

Evaluation
Marks
Comments
Communication Strategy attributes
Behaviour-change attributes
Presentation attributes
TOTAL
Overall quality of awareness raising material
Low
Medium
High
One Click Can Be Costly
Bob manages inventory at a mid-size manufacturer. On a very busy day, Bob sees an email from the 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.
RANSOM
$500,000
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 misses $75,000 worth of deliveries.
THE IMPACT SEVERITY
$45 K
The company decides not to pay the ransom, but spends $45,000 recovering its data and investigating the breach.
$325 K
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.
$15 K
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

22)



	Communication Strategy attributes				Education		
					Infographic - website	https://www.synovus.com/business/resourcecenter/commercial-middlemarket-insights/holiday-fraud-infographic/	
	1 Audience		Marks		Marks	Comments	
		1.1 Across groups	1				
		1.2 Specific	2		2	Business	
	2 Key message focus - clear purpose						
		2.1 Awareness - about threat	1		1	Holiday scams	
		2.2 Awareness - about impact	1		1	lose money	
		2.3 Cyber hygiene - best practices	1				
		Empowerment - call to action, e.g. visit a website to 2.4 learn more, to report an incident, etc.	1				
	3 Timeframe						
		3.1 Generic	1				
		3.2 Covers specific time periods	2		2	holiday season November to December	
	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						
		Simple information to understand how to address 2.1 the threat	1		1		
		2.2 Appropriate call 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		1	statistics	
		3.2 From credible source	1				
	4 Memorable						
		4.1 Micro-learning - specific topic	1		1		
		Micro-learning - short statements, focus on key 4.2 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				
	Presentation attributes						
	1 Visibility of the message						
		1.1 Appropriate location	1		1		
		Draw attention to key information, e.g. by using 1.2 contrasting colour	1		1		
	2 Layout, style and formatting						
		Uses lines, borders and shapes to group related 2.1 information	1		1		
		2.2 Create text hierarchy (up to 3 different font styles)	1		1		
		2.3 Maximum 4 colours	1		1		
	3 Inclusive / Accessible						
		A good color contrast between the text color and 3.1 background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3.2 Use appropriate font styles ()	1		1		
		3.3 Use appropriate font size ()	1		1		
	Communication Strategy attributes				4		
	Behaviour-change attributes				5		
	Presentation attributes				6		
			TOTAL		15		
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

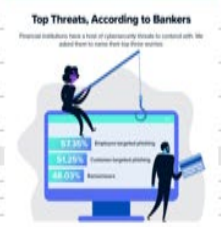
23)



	A	B	C	D	E	F	G	H	I	J	K	L	M
1													
2		Communication Strategy attributes					Evaluation						
3							Infographic - website	https://www.digitalinformationworld.com/2022/08/knowbe4-report-highlights-frequently.html					
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			Empowerment - call to action, e.g. visit a website to learn more, to report an 2.4 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			Simple information to understand how 2.1 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 statistic/graphs					
33			3.2 From credible source	1				1 Knowbe4					
34													
35		4. Memorable											
36			4.1 Micro-learning - specific topic	1				1					
37			Micro-learning - short statements, focus 4.2 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			Audience can easily relate, e.g. 4.5 storytelling	1									
41													
42		Presentation attributes											
43													
44		1. Visibility of the message											
45			1.1 Appropriate location	1									
46			Draw attention to key information, e.g. 1.2 by using contrasting colour	1				1					
47													
48		2. Layout, style and formatting											
49			Uses lines, borders and shapes to group 2.1 related information	1				1					
50			Creates text hierarchy (up to 3 different 2.2 font styles)	1				1					
51			2.3 Maximum 4 colours	1									
52													
53		3. Inclusive / Accessible											
54			Agood color contrast between the text 3.1 color and background color	1				using https://webaim.org/resources/contrastchecker/					
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					4						
62		Behaviour-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													

24)

	Communication Strategy attributes					Evaluation					
						Infographic - website		https://www.calweb.com/what-to-know/content-hub/blog/infographic-what-are-bankers-top-cybersecurity-concerns-for-2022/			
1	Audience			Marks		Marks		Comments			
		1,1	Across groups	1							
		1,2	Specific	2			2	Employees/Organisations			
2	Key message focus - clear purpose										
		2,1	Awareness - about threat	1			1	most concerning threads 2022			
		2,2	Awareness - about impact	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			1	visit a website to learn more			
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							
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							
		4,5	Audience can easily relate, e.g. storytelling	1			1	real examples			
	Presentation attributes										
1	Visibility of the message										
		1,1	Appropriate location	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 4 colours	1							
3	Inclusive / Accessible										
		3,1	A good color contrast between the text color and background color	1			1				
		3,2	Use appropriate font styles ()	1			1				
		3,3	Use appropriate font size ()	1			1				
	Communication Strategy attributes					4					
	Behaviour-change attributes					5					
	Presentation attributes					6					
				TOTAL		15					
	Overall quality of awareness raising material										
	Low	0-14									
	Medium	15-22									
	High	23-28									

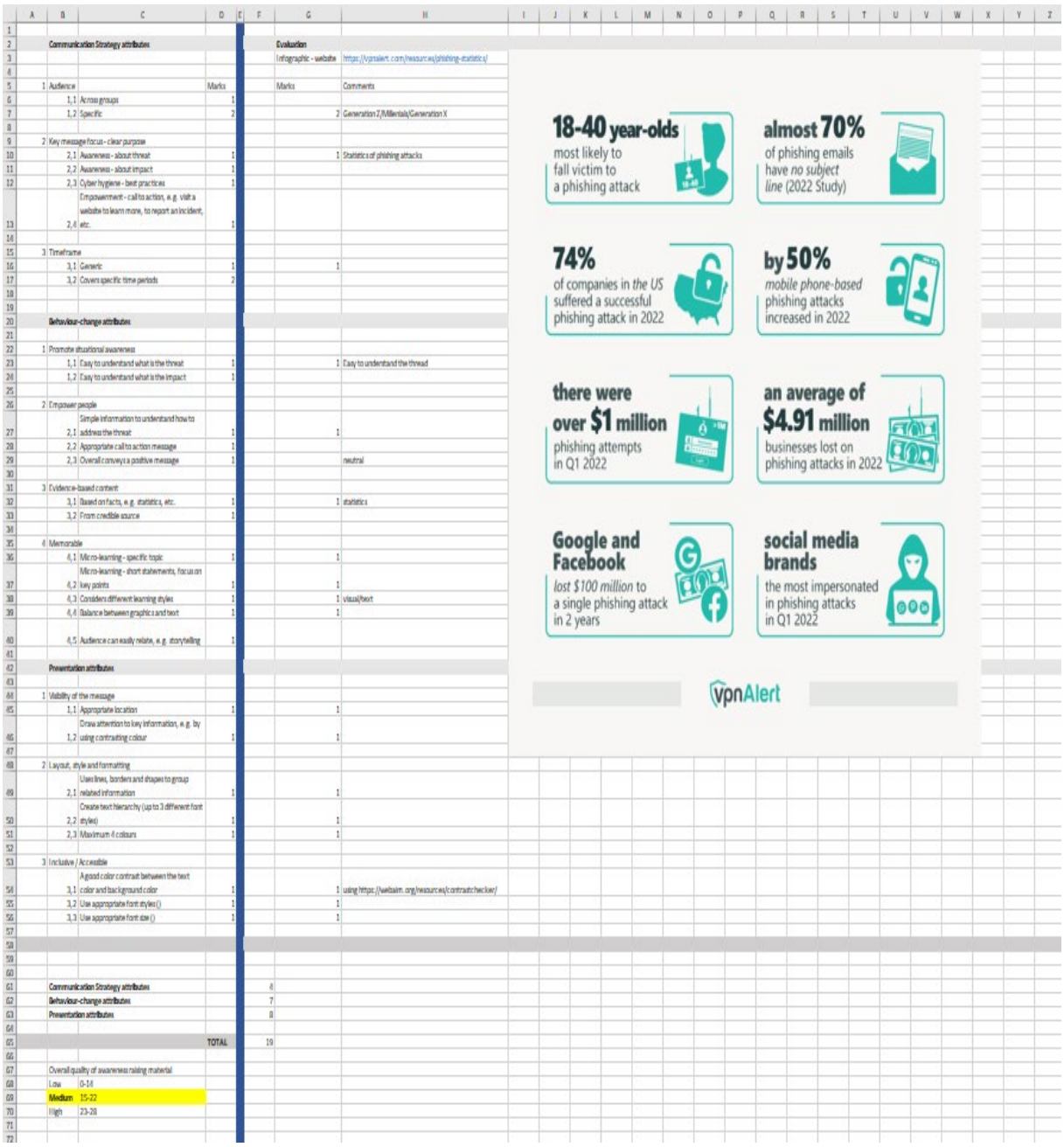


A.4 Analysis Infographics 2023

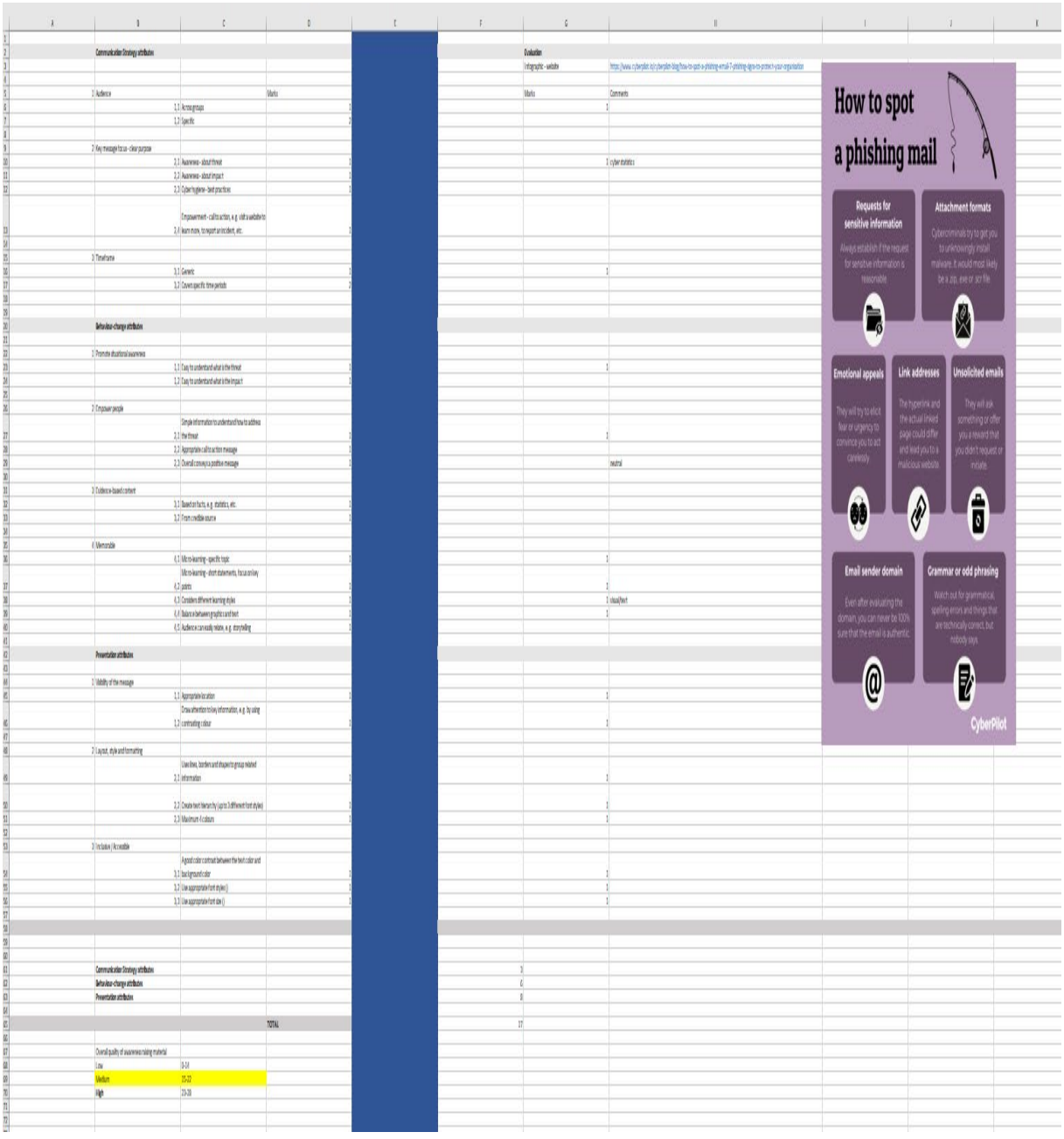
The excel file contains all the evaluation of the twenty-five infographics for the year 2023.

infographics_framework_v2023.xlsx

1)



2)



	Communication Strategy attributes					**Evaluation**					
						Infographic - website	https://www.cyberpilot.io/cyberpilot-blog/how-to-spot-a-phishing-email-7-phishing-signs-to-protect-your-organisation				
	1. Audience		Marks			Marks	Comments				
		1.1. Across groups		1			1				
		1.2. Specific		2							
	2. Key message to us - clear purpose										
		2.1. Awareness - about threat		1			1 cyber statistics				
		2.2. Awareness - about impact		1							
		2.3. Cyber hygiene - best practices		1							
		Empowerment - calls to action, e.g. visit a website to									
		2.4. learn more, to report an incident, etc.		1							
	3. Timeframe										
		3.1. Generic		1			1				
		3.2. Covers specific time periods		1							
	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							
	2. Empower people										
		Simple information to understand how to address									
		2.1. 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							
		3.2. From credible source		1							
	4. Memorable										
		4.1. Micro-learning - specific topic		1			1				
		Micro-learning - short statements, focus on key									
		4.2. 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							
	Presentation attributes										
	1. Visibility of the message										
		1.1. Appropriate location		1			1				
		Draw attention to key information, e.g. by using									
		1.2. contrasting colour		1			1				
	2. Layout, style and formatting										
		Uses lines, borders and shapes to group related									
		2.1. information		1			1				
		2.2. Create text hierarchy (up to 3 different font styles)		1			1				
		2.3. Maximum 4 colours		1			1				
	3. Inclusive / Accessible										
		A good color contrast between the text color and									
		3.1. background color		1			1				
		3.2. Use appropriate font style(s)		1			1				
		3.3. Use appropriate font size(s)		1			1				
	Communication Strategy attributes					3					
	Behaviour-change attributes					6					
	Presentation attributes					8					
			TOTAL			17					
	Overall quality of awareness raising material										
	Low	0-14									
	Medium	15-22									
	High	23-28									

3)

1								
2	**Communication Strategy attributes**				**Evaluation**			
3					Infographic - website	https://greenphire.com/infographic-technology-is-key-to-patient-engagement-2/		
4								
5	1	Audience		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		1	phishing/smishing 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 2,4 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	**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			Simple information to understand how to 2,1 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			Micro-learning - short statements, focus on 4,2 key points	1				
38			4,3 Considers different learning styles	1		1	visula/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 threads	
41								
42	**Presentation attributes**							
43								
44	1	Visibility of the message						
45			1,1 Appropriate location	1		1		
46			Draw attention to key information, e.g. by 1,2 using contrasting colour	1		1		
47								
48	2	Layout, style and formatting						
49			Uses lines, borders and shapes to group 2,1 related information	1		1		
50			Create text hierarchy (up to 3 different font 2,2 styles)	1		1		
51			2,3 Maximum 4 colours	1				
52								
53	3	Inclusive / Accessible						
54			A good color contrast between the text 3,1 color and background color	1		1		
55			3,2 Use appropriate font style()	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**				6			
64								
65				TOTAL	17			
66								
67	Overall quality of awareness raising material							
68	Low		0-14					
69	Medium		15-22					
70	High		23-28					
71								
72								
73								

4)

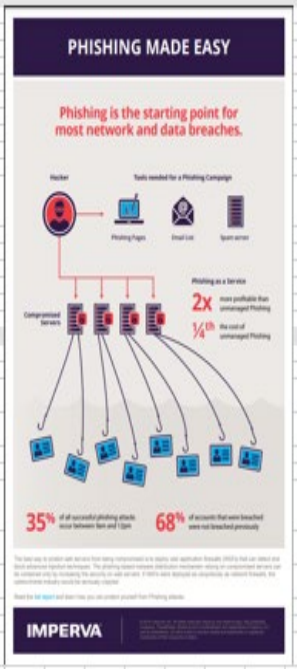
	Communication Strategy attributes				**Evaluation**		
					Infographic - website		https://phishingtackle.com/ransomware-infographic/
1	Audience		Marks		Marks		Comments
	1,1	Across groups	1			1	individual/business
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1			1	how to protect your data from ransomware attacks
	2,2	Awareness - about impact	1			1	encrypts your files
	2,3	Cyber hygiene - best practices	1			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			1	
	2,3	Overall conveys 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	
	4,2	Micro-learning - short statements, focus on key points	1				
	4,3	Considers different learning styles	1				
	4,4	Balance between graphics and text	1			1	
	4,5	Audience can easily relate, e.g. storytelling	1			1	tips to protect your data
	Presentation attributes						
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 4 colours	1			1	
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			1	using https://webaim.org/resources/contrastchecker/
	3,2	Use appropriate font styles ()	1			1	
	3,3	Use appropriate font size ()	1			1	
	Communication Strategy attributes			5			
	Behaviour-change attributes			7			
	Presentation attributes			8			
			TOTAL	20			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

5)

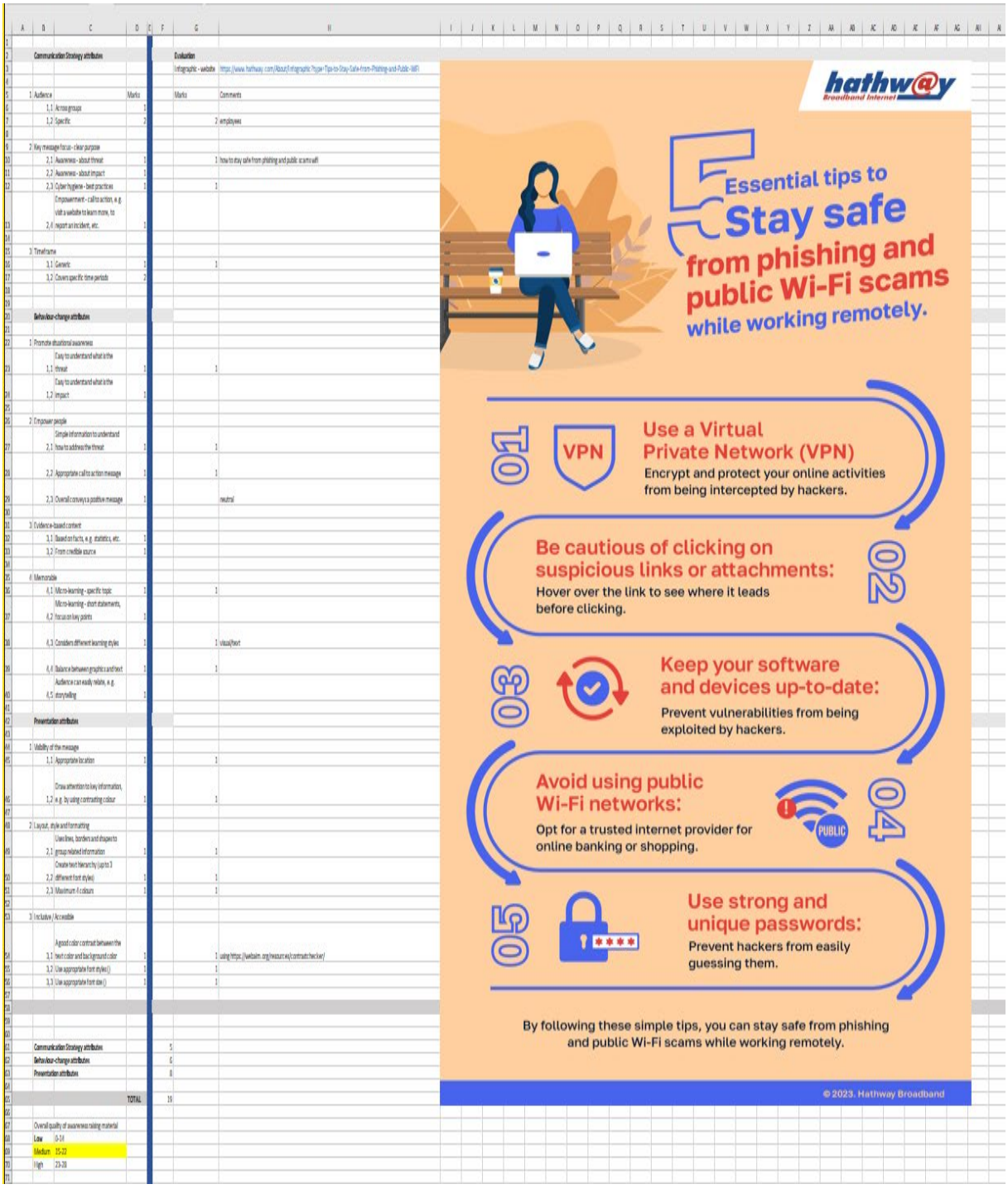
	Communication Strategy attributes				**Evaluation**					
					Infographic - website	https://au.insight.com/en_AU/content-and-resources/2023/your-2023-cybersecurity-checklist.html				
	1 Audience		Marks		Marks	Comments				
		1,1 Across groups	1							
		1,2 Specific	2			2 Business				
	2 Key message focus - clear purpose									
		2,1 Awareness - about threat	1			1 security check list				
		2,2 Awareness - about impact	1							
		2,3 Cyber hygiene - best practices	1			1				
		Empowerment - call to action, e.g. visit a website to learn more, to report an incident,								
		2,4 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							
	2 Empower people									
		Simple information to understand how to								
		2,1 address the threat	1			1				
		2,2 Appropriate call to action message	1			1				
		2,3 Overall conveys a positive message	1			1				
	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 statements, focus on								
		4,2 key points	1			1				
		4,3 Considers different learning styles	1			1 visual/text				
		4,4 Balance between graphics and text	1							
		4,5 Audience can easily relate, e.g. storytelling	1			1 Can you check off each of the list				
	Presentation attributes									
	1 Visibility of the message									
		1,1 Appropriate location	1							
		Draw attention to key information, e.g. by								
		1,2 using contrasting colour	1			1				
	2 Layout, style and formatting									
		Uses lines, borders and shapes to group								
		2,1 related information	1			1				
		Create text hierarchy (up to 3 different font								
		2,2 styles)	1			1				
		2,3 Maximum 4 colours	1			1				
	3 Inclusive / Accessible									
		A good color contrast between the text color								
		3,1 and background color	1			1 using https://webaim.org/resources/contrastchecker/				
		3,2 Use appropriate font styles()	1			1				
		3,3 Use appropriate font size ()	1			1				
	Communication Strategy attributes				5					
	Behaviour-change attributes				8					
	Presentation attributes				7					
			TOTAL		20					
	Overall quality of awareness raising material									
	Low	0-14								
	Medium	15-22								
	High	23-28								

6)

Communication Strategy attributes					**Evaluation**		
					Infographic - website		https://www.imperva.com/resources/resource-library/infographics/phishing-made-easy-time-to-rethink-your-prevention-strategy/
Audience			Marks		Marks		Comments
1,1	Across groups		1				
1,2	Specific		2			2	Business
Key message focus - clear purpose							
2,1	Awareness - about threat		1			1	phishing is the most network and data breaches
2,2	Awareness - about impact		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			1	visit a website to learn more
Timeframe							
3,1	Generic		1			1	
3,2	Covers specific time periods		2				
Behaviour-change attributes							
Promote situational awareness							
1,1	Easy to understand what is the threat		1			1	
1,2	Easy to understand what is the impact		1				
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
Evidence-based content							
3,1	Based on facts, e.g. statistics, etc.		1			1	statistics
3,2	From credible source		1				
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				
Presentation attributes							
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	
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 4 colours		1			1	
Inclusive / Accessible							
3,1	A good color contrast between the text color and background color		1			1	using https://webaim.org/resources/contrastchecker/
3,2	Use appropriate font styles ()		1			1	
3,3	Use appropriate font size ()		1			1	
Communication Strategy attributes					5		
Behaviour-change attributes					7		
Presentation attributes					8		
			TOTAL		20		
Overall quality of awareness raising material							
Low	0-14						
Medium	15-22						
High	23-28						

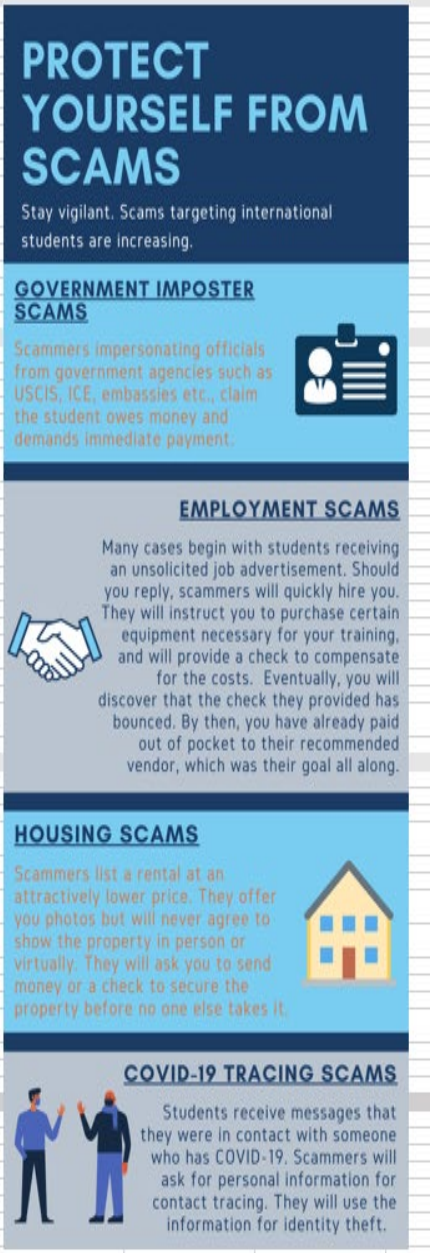


7)


hathway
Broadband Internet
Essential tips to
Stay safe
from phishing and
public Wi-Fi scams
while working remotely.
01
VPN
Use a Virtual
Private Network (VPN)
Encrypt and protect your online activities
from being intercepted by hackers.
Be cautious of clicking on
suspicious links or attachments:
Hover over the link to see where it leads
before clicking.
02
03
Keep your software
and devices up-to-date:
Prevent vulnerabilities from being
exploited by hackers.
Avoid using public
Wi-Fi networks:
Opt for a trusted internet provider for
online banking or shopping.
PUBLIC
04
05
Use strong and
unique passwords:
Prevent hackers from easily
guessing them.
By following these simple tips, you can stay safe from phishing
and public Wi-Fi scams while working remotely.
© 2023. Hathway Broadband

8)

	Communication Strategy attributes				Evaluation					
					Infographic - website		https://international.catholic.edu/advising/scam-alert/scam-alert.html			
1	Audience		Marks		Marks		Comments			
		1,1 Across groups	1							
		1,2 Specific	2			2	International students			
2	Key message focus - clear purpose									
		2,1 Awareness - about threat	1			1	how to protect yourself from scams			
		2,2 Awareness - about impact	1			1				
		2,3 Cyber hygiene - best practices	1							
		Empowerment - call to action, e.g. visit a website to learn more, to report an								
		2,4 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									
		Simple information to understand how to								
		2,1 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	ervisa			
4	Memorable									
		4,1 Micro-learning - specific topic	1			1				
		Micro-learning - short statements, focus								
		4,2 on key points	1							
		4,3 Considers different learning styles	1			1				
		4,4 Balance between graphics and text	1			1				
		4,5 Audience can easily relate, e.g. storytelling	1			1	real examples			
	Presentation attributes									
1	Visibility of the message									
		1,1 Appropriate location	1			1				
		Draw attention to key information, e.g. by								
		1,2 using contrasting colour	1			1				
2	Layout, style and formatting									
		Uses lines, borders and shapes to group								
		2,1 related information	1			1				
		Create text hierarchy (up to 3 different								
		2,2 font styles)	1			1				
		2,3 Maximum 4 colours	1			1				
3	Inclusive / Accessible									
		A good color contrast between the text								
		3,1 color and background color	1							
		3,2 Use appropriate font styles()	1			1				
		3,3 Use appropriate font size ()	1			1				
	Communication Strategy attributes				5					
	Behaviour-change attributes				9					
	Presentation attributes				7					
			TOTAL		21					
	Overall quality of awareness raising material									
	Low	0-14								
	Medium	15-22								
	High	23-28								



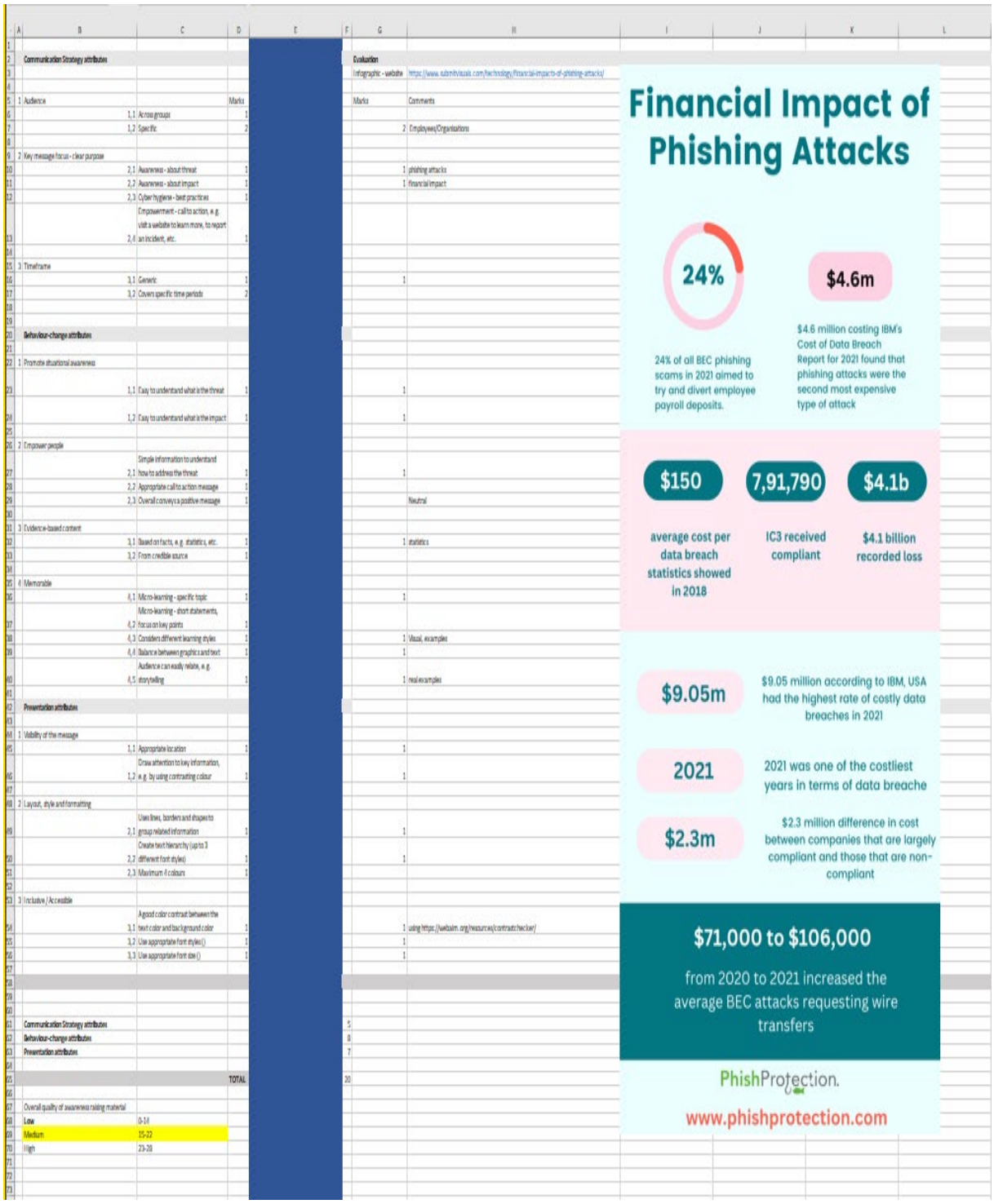
9)

	A	B	C	D	E	F	G	H	I	J	K	L	M
1													
2		Communication Strategy attributes					Evaluation						
3							Infographic - website	https://cyberclan.com/ua/resources/cybersecurity-threats-in-2023/					
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	cybersecurity threats in 2023					
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		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			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			1						
40			4.5 Audience can easily relate, e.g. storytelling	1			1	how to prepare for emerging cyber security					
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 https://webaim.org/resources/contrastchecker/					
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					9						
63		Presentation attributes					8						
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													

10)

	Communication Strategy attributes				**Evaluation**				
					Infographic - website		https://us.norton.com/blog/online-scams/romance-scams#		
1	Audience		Marks		Marks		Comments		
		1,1	Across groups	1		1	Individuals		
		1,2	Specific	2					
2	Key message focus - clear purpose								
		2,1	Awareness - about threat	1		1	romance scams		
		2,2	Awareness - about impact	1		1	they ask for money and they disappear		
		2,3	Cyber hygiene - best practices	1		1			
		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		
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		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	norton		
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					
		4,4	Balance between graphics and text	1					
		4,5	Audience can easily relate, e.g. storytelling	1		1	real examples		
	Presentation attributes								
1	Visibility of the message								
		1,1	Appropriate location	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 4 colours	1		1			
3	Inclusive / Accessible								
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/		
		3,2	Use appropriate font styles()	1		1			
		3,3	Use appropriate font size()	1		1			
	Communication Strategy attributes				6				
	Behaviour-change attributes				8				
	Presentation attributes				7				
				TOTAL	21				
	Overall quality of awareness raising material								
	Low	0-14							
	Medium	15-22							
	High	23-28							

11)



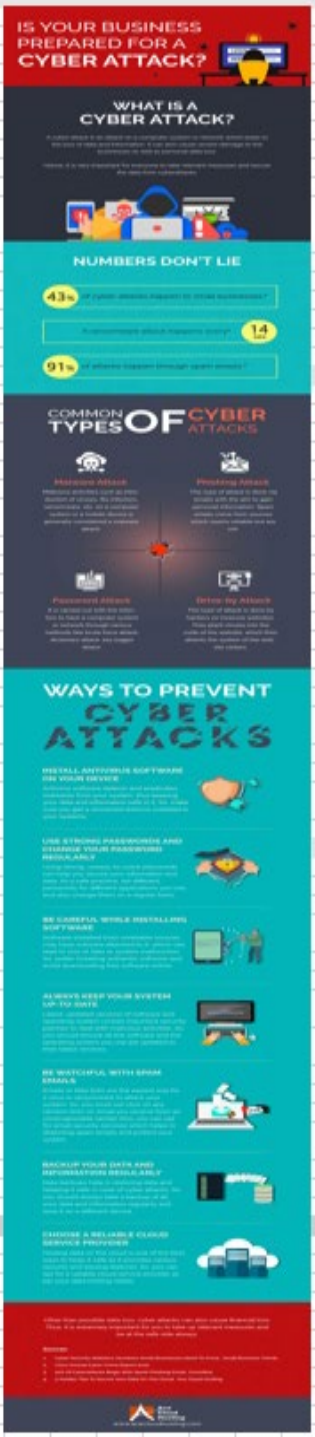
					Evaluation			
					Infographic - website	https://www.submitvisuals.com/technology/financial-impacts-of-phishing-attacks/		
	Communication Strategy attributes							
1	Audience		Marks		Marks	Comments		
		1,1	Across groups	1				
		1,2	Specific	2		2	Employees/Organisations	
2	Key message focus - clear purpose							
		2,1	Awareness - about threat	1		1	phishing attacks	
		2,2	Awareness - about impact	1		1	financial impact	
		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				
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, examples	
		4,4	Balance between graphics and text	1		1		
		4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
	Presentation attributes							
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 4 colours	1				
3	Inclusive / Accessible							
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes				5			
	Behaviour-change attributes				8			
	Presentation attributes				7			
				TOTAL	20			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

12)

						Evaluation		
						Infographic - website	https://www.shutterstock.com/image-vector/phone-call-scam-infographic-confused-elderly-2093596261	
	1. Audience		Marks			Marks	Comments	
		1.1. Across groups		1				
		1.2. Specific		2		2	elderly woman	
	2. Key message focus - clear purpose							
		2.1. Awareness - about threat		1		1	phone scams	
		2.2. Awareness - about impact		1				
		2.3. Cyber hygiene - best practices		1		1		
		Empowerment - call to action, e.g. visit a website to learn more, to						
		2.4. 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							
		Easy to understand what is the						
		1.1. threat		1		1		
		Easy to understand what is the						
		1.2. impact		1				
	2. Empower people							
		Simple information to understand						
		2.1. how to address the threat		1		1		
		2.2. Appropriate call to action message		1		1		
		2.3. Overall conveys 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 statements,						
		4.2. focus on key points		1				
		4.3. Considers different learning styles		2		1	Visual, examples	
		4.4. Balance between graphics and text		1		1		
		Audience can easily relate, e.g.						
		4.5. storytelling		1		1	real examples	
	Presentation attributes							
	1. Visibility of the message							
		1.1. Appropriate location		1		1		
		Draw attention to key information,						
		1.2. e.g. by using contrasting colour		2		1		
	2. Layout, style and formatting							
		Uses lines, borders and shapes to						
		2.1. group related information		1		1		
		Creates text hierarchy (up to 3						
		2.2. different font styles)		2		1		
		2.3. Maximum 4 colours		2		1		
	3. Inclusive / Accessible							
		Appropriate color contrast between the						
		3.1. text color and background color		2		1	using https://webaim.org/resources/contrastchecker/	
		3.2. Use appropriate font style(s)		1		1		
		3.3. Use appropriate font size (s)		1		1		
	Communication Strategy attributes					5		
	Behaviour-change attributes					7		
	Presentation attributes					8		
				TOTAL		20		
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

13)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://www.acecloudhosting.com/blog/infographic-cyber-attack/	
	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	business	
	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	cyber attacks	
	2,2	Awareness - about impact	1		1	financial loss	
	2,3	Cyber hygiene - best practices	1		1		
	2,4	Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1				
	Timeframe						
	3,1	Generic	1		1		
	3,2	Covers specific time periods	2				
	Behaviour-change attributes						
	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		
	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		1		
	2,3	Overall conveys a positive message	1			Neutral	
	Evidence-based content						
	3,1	Based on facts, e.g. statistics, etc.	1		1	statistics	
	3,2	From credible source	1				
	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, examples	
	4,4	Balance between graphics and text	1				
	4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
	Presentation attributes						
	Visibility of the message						
	1,1	Appropriate location	1				
	1,2	Draw attention to key information, e.g. by using contrasting colour	1		1		
	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 4 colours	1		1		
	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			6			
	Behaviour-change attributes			8			
	Presentation attributes			7			
			TOTAL	21			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					



14)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://whatismyipaddress.com/signs-of-a-romance-scam	
1		Audience	Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2		Key message focus - clear purpose					
	2,1	Awareness - about threat	1		1	romance scams	
	2,2	Awareness - about impact	1		1	steal money	
	2,3	Cyber hygiene - best practices	1		1		
	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	
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		1		
	2,3	Overall conveys 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		1	europol	
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		1	Real examples	
		Presentation attributes					
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 4 colours	1		1		
3		Inclusive / Accessible					
	3,1	A good color contrast between the text color and background color	1			using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			6		
		Behaviour-change attributes			10		
		Presentation attributes			7		
			TOTAL		23		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

15)

	Communication Strategy attributes				**Evaluation**			
					Infographic - website	https://risk.lexisnexis.com/insights-resources/infographic/top-six-fraud-trends-in-the-public-sector-to-watch-in-2023		
	1 Audience		Marks		Marks	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 G fraud trends in public sector		
		2,2 Awareness - about impact	1			1 money loss		
		2,3 Cyber hygiene - best practices	1					
		Empowerment - call to action, e.g. visit a website to learn more, to report an						
		2,4 incident, etc.	1			1 visit a website to learn more		
	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	
		1,2 Easy to understand what is the impact	1			1		
	2 Empower people							
		Simple information to understand how						
		2,1 to address the threat	1			1		
		2,2 Appropriate call 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			1 statistics		
		3,2 From credible source	1					
	4 Memorable							
		4,1 Micro-learning - specific topic	1			1		
		Micro-learning - short statements, focus						
		4,2 on key points	1			1		
		4,3 Considers different learning styles	1					
		4,4 Balance between graphics and text	1			1		
		Audience can easily relate, e.g.						
		4,5 storytelling	1					
	Presentation attributes							
	1 Visibility of the message							
		1,1 Appropriate location	1					
		Draw attention to key information, e.g.						
		1,2 by using contrasting colour	1			1		
	2 Layout, style and formatting							
		Uses lines, borders and shapes to group						
		2,1 related information	1			1		
		Create text hierarchy (up to 3 different						
		2,2 font styles)	1			1		
		2,3 Maximum 4 colours	1			1		
	3 Inclusive / Accessible							
		A good color contrast between the text						
		3,1 color and background color	1			using https://webaim.org/resource/e/contrastchecker/		
		3,2 Use appropriate font styles ()	1			1		
		3,3 Use appropriate font size ()	1			1		
	Communication Strategy attributes				G			
	Behaviour-change attributes				7			
	Presentation attributes				G			
				TOTAL	19			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

16)

	Communication Strategy attributes					Evaluation							
						Infographic - website	https://www.thebornewpost.com/						
	1 Audience		Marks			Marks	Comments						
		1.1 Across groups	1				1 individuals						
		1.2 Specific	2										
	2 Key message focus - clear purpose												
		2.1 Awareness - about threat	1				1 online shopping scam						
		2.2 Awareness - about impact	1				1 financial lose etc						
		2.3 Cyber hygiene - best practices	1										
		Empowerment - call to action, e.g. visit a website to learn more,											
		2.4 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												
		Easy to understand what is the 1.1 threat	1				1	1					
		Easy to understand what is the 1.2 impact	1				1						
	2 Empower people												
		Simple information to understand 2.1 how to address the threat	1				1						
		2.2 Appropriate call to action message	1										
		Overall conveys a positive 2.3 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 statements, 4.2 focus on key points	1				1						
		4.3 Considers different learning styles	1				1 Visual/text						
		Balance between graphics and 4.4 text	1				1						
		Audience can easily relate, e.g. 4.5 storytelling	1										
	Presentation attributes												
	1 Visibility of the message												
		1.1 Appropriate location	1				1						
		Draw attention to key information, e.g. by using 1.2 contrasting colour	1				1						
	2 Layout, style and formatting												
		Uses lines, borders and shapes to 2.1 group related information	1				1						
		Create text hierarchy (up to 3 2.2 different font styles)	1				1						
		2.3 Maximum 4 colours	1				1						
	3 Inclusive / Accessible												
		A good color contrast between the 3.1 text color and background color	1				1 using https://webaim.org/resources/contrastchecker/						
		3.2 Use appropriate font style(s)	1				1						
		3.3 Use appropriate font size ()	1				1						
	Communication Strategy attributes					6							
	Behaviour-change attributes					7							
	Presentation attributes					8							
			TOTAL			10							
	Overall quality of awareness raising material												
	Low	0-14											
	Medium	15-22											
	High	23-28											

17)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.proofpoint.com/uk/impostor-email-threats-infographic	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Employees	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	email threads	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		1		
	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	
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
	1,2	Easy to understand what is the impact	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		1		
	4,3	Considers different learning styles	1		1	Visual /text	
	4,4	Balance between graphics and text	1				
	4,5	Audience can easily relate, e.g. storytelling	1				
		Presentation attributes					
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1			using https://webaim. org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			6		
		Behaviour-change attributes			6		
		Presentation attributes			6		
			TOTAL		18		
		Overall quality of awareness raising material					
	Low	0-14					
	Medium	15-22					
	High	23-28					

18)

					Evaluation			
	Communication Strategy attributes				Infographic - website	https://www.darkowl.com/whitepapers/infographic-trends-in-the-global-landscape-of-online-scams/		
1	Audience		Marks		Marks	Comments		
		1,1 Across groups	1			1 Individuals / Employees		
		1,2 Specific	2					
2	Key message focus - clear purpose							
		2,1 Awareness - about threat	1			1 online scams		
		2,2 Awareness - about impact	1			1 financial loss		
		2,3 Cyber hygiene - best practices	1					
		Empowerment - call to action, e.g. visit a website to learn more, to 2,4 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		
		Easy to understand what is the 1,2 impact	1			1		
2	Empower people							
		Simple information to understand 2,1 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		
		Micro-learning - short statements, 4,2 focus on key points	1					
		4,3 Considers different learning styles	1			1 Visual/text		
		4,4 Balance between graphics and text	1					
		Audience can easily relate, e.g. 4,5 storytelling	1			1 how to avoid the treat/ real examples		
	Presentation attributes							
1	Visibility of the message							
		1,1 Appropriate location	1					
		Draw attention to key information, 1,2 e.g. by using contrasting colour	1			1		
2	Layout, style and formatting							
		Uses lines, borders and shapes to 2,1 group related information	1			1		
		Create text hierarchy (up to 3 2,2 different font styles)	1			1		
		2,3 Maximum 4 colours	1			1		
3	Inclusive / Accessible							
		A good color contrast between the 3,1 text color and background color	1			1 using https://webaim.org/resources/contrastchecker/		
		3,2 Use appropriate font styles ()	1			1		
		3,3 Use appropriate font size ()	1			1		
	Communication Strategy attributes				6			
	Behaviour-change attributes				7			
	Presentation attributes				7			
			TOTAL		18			
	Overall quality of awareness raising material							
	Low	0-14						
	Medium	15-22						
	High	23-28						

19)

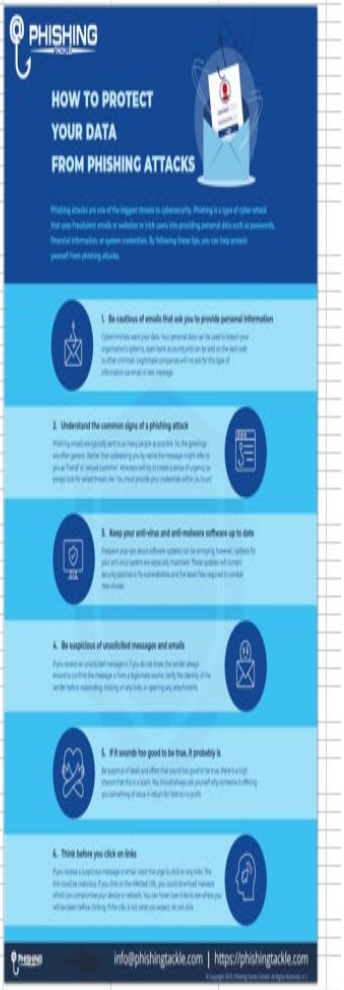
		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.firstbank.net/home/resources/online-security-privacy/fakecheckscams	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	check scams	
	2,2	Awareness - about impact	1		1	the scammer has your money	
	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		1	report the incident	
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		1		
	2,3	Overall conveys 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		
	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				
	4,5	Audience can easily relate, e.g. storytelling	1		1	real examples	
		Presentation attributes					
1	Visibility of the message						
	1,1	Appropriate location	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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim. org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			5		
		Behaviour-change attributes			7		
		Presentation attributes			7		
			TOTAL		19		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

20)

		Communication Strategy attributes			**Evaluation**		
					Infographic - website	https://www.slideshare.net/AbhishekAgarwal101/phishing-infographic-257295671	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1		1		
	1,2	Specific	2				
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	phishing attack	
	2,2	Awareness - about impact	1				
	2,3	Cyber hygiene - best practices	1		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				
2	Empower people						
	2,1	Simple information to understand how to address the threat	1		1		
	2,2	Appropriate call to action message	1		1		
	2,3	Overall conveys 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		
	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				
	4,5	Audience can easily relate, e.g. storytelling	1		1	actions to help to prevent to be hooked	
		Presentation attributes					
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			4		
		Behaviour-change attributes			6		
		Presentation attributes			8		
			TOTAL		18		
		Overall quality of awareness raising material					
		Low	0-14				
		Medium	15-22				
		High	23-28				

21)

	B	C	D	F	G	H
2	**Communication Strategy attributes**				**Evaluation**	
3					Infographic - website	https://phishingtackle.com/phishing-infographic/
5	Audience		Marks		Marks	Comments
6		1.1 Across groups	1		1	Individuals/employees
7		1.2 Specific	2			
9	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			
13		2.4 Empowerment - call to action, e.g. visit a website to learn more, to report an incident, etc.	1			
15	Timeframe					
16		3.1 Generic	1		1	
17		3.2 Covers specific time periods	2			
20	**Behaviour-change attributes**					
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			
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
31	Evidence-based content					
32		3.1 Based on facts, e.g. statistics, etc.	1			
33		3.2 From credible source	1			
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		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	
42	**Presentation attributes**					
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	
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	
53	Inclusive / Accessible					
54		3.1 A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/
55		3.2 Use appropriate font styles()	1		1	
56		3.3 Use appropriate font size ()	1		1	
61	**Communication Strategy attributes**			3		
62	**Behaviour-change attributes**			0		
63	**Presentation attributes**			0		
65			**TOTAL**	17		
67	Overall quality of awareness raising material					
68	**Low**	0-14				
69	Medium	15-22				
70	High	23-28				



22)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://securenetworksitc.com/guide-holiday-scams/	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	holiday scams	
		2,2	Awareness - about impact	1				
		2,3	Cyber hygiene - best practices	1		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				
		3,2	Covers specific time periods	2		2	holiday season	
		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				
	2	Empower people						
		2,1	Simple information to understand how to address the threat	1		1		
		2,2	Appropriate call to action message	1		1		
		2,3	Overall conveys 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		
		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				
		Presentation attributes						
	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 4 colours	1		1		
	3	Inclusive / Accessible						
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			4			
		Behaviour-change attributes			5			
		Presentation attributes			6			
				TOTAL	15			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

23)

		Marks		Marks	Comments
Communication Strategy attributes				**Evaluation**	
				Infographic - website	https://www.123rf.com/photo_155410295_shopping-safely-online-infographic-safety-and-cyber-security-tips-for-secure-orders-and-transactions.html
1	Audience	Marks		Marks	Comments
1,1	Across groups	1		1	
1,2	Specific	2			
2	Key message focus - clear purpose				
2,1	Awareness - about threat	1		1	shopping scams
2,2	Awareness - about impact	1			
2,3	Cyber hygiene - best practices	1		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			
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			
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			
Presentation attributes					
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	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 4 colours	1		1	
3	Inclusive / Accessible				
3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/
3,2	Use appropriate font styles ()	1		1	
3,3	Use appropriate font size ()	1		1	
Communication Strategy attributes			4		
Behaviour-change attributes			5		
Presentation attributes			6		
		TOTAL	15		
Overall quality of awareness raising material					
Low	0-14				
Medium	15-22				
High	23-30				

24)

		Communication Strategy attributes				**Evaluation**		
						Infographic - website	https://www.bernama.com/en/infographics/index.php?v=10051	
	1	Audience		Marks		Marks	Comments	
		1,1	Across groups	1		1		
		1,2	Specific	2				
	2	Key message focus - clear purpose						
		2,1	Awareness - about threat	1		1	phishing scams	
		2,2	Awareness - about impact	1				
		2,3	Cyber hygiene - best practices	1		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				
	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				
		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				
		Presentation attributes						
	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 4 colours	1				
	3	Inclusive / Accessible						
		3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
		3,2	Use appropriate font styles ()	1		1		
		3,3	Use appropriate font size ()	1		1		
		Communication Strategy attributes			6			
		Behaviour-change attributes			5			
		Presentation attributes			6			
				TOTAL	15			
		Overall quality of awareness raising material						
		Low	0-14					
		Medium	15-22					
		High	23-28					

25)

	Communication Strategy attributes				**Evaluation**		
					Infographic - website	https://security.harvard.edu/ransomware-infographic	
1	Audience		Marks		Marks	Comments	
	1,1	Across groups	1				
	1,2	Specific	2		2	Baby boomers/Generation X	
2	Key message focus - clear purpose						
	2,1	Awareness - about threat	1		1	ransomware scams	
	2,2	Awareness - about impact	1		1	lock your data on your pc	
	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		1		
	2,3	Overall conveys 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		1	Harvard	
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				
	4,5	Audience can easily relate, e.g. storytelling	1				
	Presentation attributes						
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 4 colours	1		1		
3	Inclusive / Accessible						
	3,1	A good color contrast between the text color and background color	1		1	using https://webaim.org/resources/contrastchecker/	
	3,2	Use appropriate font styles ()	1		1		
	3,3	Use appropriate font size ()	1		1		
	Communication Strategy attributes			4			
	Behaviour-change attributes			5			
	Presentation attributes			6			
			TOTAL	15			
	Overall quality of awareness raising material						
	Low	0-14					
	Medium	15-22					
	High	23-28					

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, Octomber) Compatitech. [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, Octomber) 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, Febrary) 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, Noverber) 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, Febrary) 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

[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.

[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

[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, Febrary) 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=IwAR0bTMyP-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-myl1CmoAE

[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-myl1CmoAE

[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, Febrouary) 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=IwAR23i7ao0PCJIqfjEfJKcxwGSBk9Ul7wA3qE21DMKLzsF8VFyCUflfXpIEI

[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