Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Διοίκηση Τεχνολογία και Ποιότητα

Μεταπτυχιακή διατριβή

<<Κυβερνοασφάλεια και ευαισθητοποίηση περί ιδιωτικότητας και προστασίας δεδομένων>>

Φοίβος Χαραλάμπους

Επιβλέπων καθηγητής: Στέφανος Γκρίτζαλης

Λευκωσία, Μάιος 2023

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

«ΔΙΟΙΚΗΣΗ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΠΟΙΟΤΗΤΑ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

«Κυβερνοασφάλεια και ευαισθητοποίηση περί ιδιωτικότητας και προστασίας δεδομένων»

Φοίβος Χαραλάμπους

Επιβλέπων καθηγητής: Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στη Διοίκηση, Τεχνολογία και Ποιότητα από τη Σχολή Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Λευκωσία, Μάιος 2023

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Οι τεχνολογικές εξελίξεις σηματοδοτούσαν πάντοτε ένα καθοριστικό παράγοντα αλλαγών για την ανθρωπότητα. Η όλο και περισσότερη χρήση της τεχνολογίας προκάλεσε επιδράσεις σε όλους τους τομείς της ζωής μας. Ένα αρνητικό φαινόμενο που έκανε την εμφάνισή του λόγω της τεχνολογικής ανάπτυξης είναι το ηλεκτρονικό έγκλημα και οι κυβερνοεπιθέσεις. Η παρούσα μεταπτυχιακή διατριβή έχει σαν στόχο την ενημέρωση του κοινού για τις κυβερνοεπιθέσεις, ώστε να γίνει αντιληπτή η επικινδυνότητα τους, καθώς επίσης και την εξέταση της ευαισθητοποίησης των πολιτών σε θέματα που αφορούν την ιδιωτικότητά τους.

Στο πρώτο κεφάλαιο γίνεται αναφορά στην εξέλιξη των ηλεκτρονικών επιθέσεων στο πέρασμα του χρόνου φτάνοντας στο σήμερα και περιγράφοντας τα χαρακτηριστικά των επιθέσεων εν καιρώ πανδημίας. Ταυτόχρονα, παρουσιάζονται και τα κίνητρα που κρύβονται πίσω από τις κυβερνοεπιθέσεις, αλλά και τα διάφορα είδη με τα οποία οι εγκληματίες μπορεί να τις πραγματοποιήσουν. Το κεφάλαιο κλείνει με αναφορά σε παραδείγματα κυβερνοεπιθέσεων που έγιναν σε εταιρείες ή οργανισμούς που θεωρούνταν κολοσσοί, ωστόσο δεν στάθηκαν ικανοί να αποκρούσουν αυτές τις επιθέσεις.

Το δεύτερο κεφάλαιο έχει σαν στόχο την κατανόηση της έννοιας της κυβερνοασφάλειας, καθώς και την παρουσίαση προτεινόμενων τρόπων ενίσχυσης της προστασίας των προσωπικών δεδομένων. Ακόμη, γίνεται αναφορά στην ενημέρωση και τις δράσεις που πρέπει να υιοθετήσει η ευρύτερη κοινωνία, ώστε να επιτευχθεί ευαισθητοποίηση του κοινού σχετικά με την ιδιωτικότητα του.

Το τρίτο και τελευταίο κεφάλαιο ασχολείται αποκλειστικά με την περιγραφή της έρευνας που πραγματοποιήθηκε στα πλαίσια της μεταπτυχιακής διατριβής. Η μεθοδολογία που ακολουθήθηκε για διεξαγωγή της έρευνας ήταν μέσω ερωτηματολογίου. Μελετήθηκαν η συμπεριφορά και οι συνήθειες των ατόμων στο διαδικτυακό χώρο και εξετάστηκε κατά πόσο είναι ευαισθητοποιημένοι και ενήμεροι για θέματα ιδιωτικότητας. Τα αποτελέσματα της έρευνας ήταν αρκετά ανησυχητικά, αφού έδειξαν ότι οι πολίτες δεν είναι αρκετά ευαισθητοποιημένοι για την ασφάλεια των προσωπικών τους δεδομένων. Παρατηρήθηκε και η ύπαρξη του φαινομένου του παραδόξου, καθώς οι ανησυχίες των ερωτώμενων για τους κινδύνους του διαδικτύου δεν ήταν ανάλογες με τη συμπεριφορά τους. Γενικότερα, το

κύριο ζήτημα ήταν να γίνει αντιληπτή η σοβαρότητα του ηλεκτρονικού εγκλήματος και οι αναγνώστες να κατανοήσουν πως η ιδιωτικότητά τους αποτελεί υψίστης σημασίας.

Summary

Technological developments have always been a decisive factor of change for humanity. The increasing use of technology has impacted all areas of our lives. A negative phenomenon that appeared due to the technological development is electronic crime and cyber-attacks. The aim of this master's thesis is to inform the public about cyber-attacks, in order to understand how dangerous they are, and also to examine the citizens' privacy awareness.

In the first chapter, reference is made to the evolution of electronic attacks over time until today and description of the characteristics of attacks during pandemic. At the same time the motivations behind cyber-attacks are also presented, as well as the various ways in which criminals carry them out. The first chapter ends with reference to examples of cyberattacks of companies or organizations considered as giants but were not able to repel these attacks.

The second chapter deals with the understanding of the concept of cyber security and the proposal of ways to improve the privacy of personal data. In addition, the chapter mentions the information and the actions that need to be adopted by wider society in order to achieve public awareness in respect of their privacy.

Finally, the third and last chapter describes exclusively the research performed for the purpose of this master's thesis. The methodology followed to conduct the research was through a questionnaire. Peoples' behavior and habits were studied, and it was investigated whether they are sensitized and informed for privacy matters. The research's results were quit worrying, since they showed that the citizens are not sensitized enough for the security of their private information. It was also observed that the privacy paradox phenomenon, as the respondents' worries for the dangers of internet were not in line with their behavior. The main issue of this master's thesis was to make a point of the seriousness of cybercrime and to make readers understand the utmost importance of their privacy.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Στέφανο Γκρίτζαλη για τις πολύτιμες συμβουλές και τη συνεχή καθοδήγηση που μου προσέφερε κατά τη διάρκεια της συγγραφής της διατριβής μου, ώστε να μπορέσω να την ολοκληρώσω με επιτυχία.

Θερμές ευχαριστίες επίσης προς όλους όσοι συνέβαλαν στη συμπλήρωση του ερωτηματολογίου που χρησιμοποιήθηκε στη διατριβή, καθώς αφιέρωσαν προσωπικό χρόνο για να απαντήσουν ανιδιοτελώς και με κάθε σοβαρότητα στις ερωτήσεις που τους είχαν δοθεί.

Τέλος, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του μεταπτυχιακού προγράμματος «Διοίκηση, Τεχνολογία και Ποιότητα», οι οποίοι με την εμπειρία και τις γνώσεις τους μας δίδαξαν ενδιαφέροντα θέματα τα οποία θα αποτελέσουν σημαντικό οδηγό για την επαγγελματική μας κατάρτιση.

Περιεχόμενα

Περιεχόμενα vii
Εισαγωγή 1
Κεφάλαιο 1 2
1. Κυβερνοεπιθέσεις 2
1.1 Πώς ορίζεται η κυβερνοεπίθεση 2
1.2 Εξέλιξη Κυβερνοεπιθέσεων στο πέρασμα του χρόνου 3
1.3 Λόγοι που πραγματοποιούνται κυβερνοεπιθέσεις 6
1.4 Είδη κυβερνοεπιθέσεων 8
1.4.1 Malware (Ransomware, Spyware, Trojans κλπ.) 8
1.4.2 Phishing 9
1.4.3 Cryptojacking 9
1.4.4 Data breach 10
1.4.5 Supply chain attacks 11
1.4.6 Non malicious threats 11
1.5 Μεγάλες κυβερνοεπιθέσεις του 21ου αιώνα 12
1.5.1 TJX companies Inc. 12
1.5.2 Yahoo 13
1.5.3 The United State Office of Personnel Management 14
1.6 Κυβερνοεπιθέσεις εν καιρώ πανδημίας 15
1.7 Cloud computing εν καιρώ πανδημίας 16
Κεφάλαιο 2 19
2. Κυβερνοασφάλεια 19
2.1 Πώς ορίζεται η Κυβερνοασφάλεια 19
2.2 Οργανισμός ENISA 21
2.3 Τρόποι ενίσχυσης προστασίας από κυβερνοεπιθέσεις 22
2.3.1 Passwords 22
2.3.2 Antivirus 24
2.3.3 Ενθάρρυνση για ανώνυμη περιήγηση 25
2.3.4 Social Media 26
2.3.5 Σχολείο, πολιτεία, επαγγελματικό περιβάλλον 28
Κεφάλαιο 3 30
3. Διεξαγωγή Έρευνας 30
3.1 Privacy awareness και Privacy paradox 30

3.2 Περιγραφή Έρευνας 32
3.2.1 Μεθοδολογία έρευνας και δειγματοληψία 32
3.2.2 Δομή 32
3.2.3 Μέρη ερωτηματολογίου 33
3.3 Ανάλυση δεδομένων 34
3.4 Συμπεράσματα που εξάχθηκαν από την έρευνα 53
Επίλογος 56
Βιβλιογραφία 57
Παράρτημα Α 62

Εισαγωγή

Αδιαμφισβήτητα η εξέλιξη της τεχνολογίας επέφερε σημαντικές αλλαγές στον κόσμο παρέχοντας πολλά πλεονεκτήματα, όπως η αύξηση της παραγωγικότητας, η ενίσχυση της επικοινωνίας και η μείωση κόστους. Έχει παρατηρηθεί ότι όσο εμφανίζονται νέες τεχνολογικές ανακαλύψεις και αυξάνεται η χρήση του διαδικτύου, τόσο συχνότερα θα πραγματοποιούνται ηλεκτρονικές επιθέσεις.

Οι κυβερνοεπιθέσεις χωρίς αμφιβολία αποτελούν ένα παγκόσμιο πρόβλημα και δεν περιορίζονται μόνο σε πολυεθνικές εταιρείες και σε κράτη. Η ανάπτυξη του «Internet of Things» (διασύνδεση συσκευών σε σπίτια και γραφεία), των μαζικών δεδομένων και η ψηφιοποίηση παρέχουν τη δυνατότητα σε εγκληματίες ή οργανώσεις να στοχεύουν όλο και περισσότερα θύματα (Rolf H. Weber & Romana Weber, 2010). Επίσης, η τεχνολογική ανάπτυξη ευνοεί τους κυβερνοεγκληματίες, καθώς εξελίσσονται χρόνο με το χρόνο, ανακαλύπτοντας πιο σύγχρονες μεθόδους επιθέσεων. Έτσι, έχοντας την ικανότητα να βρίσκουν νέες τεχνικές με τη χρήση της τεχνολογίας, είναι ικανοί να παραβιάζουν πιο εύκολα τα συστήματα διάφορων υποδομών.

Κάθε επίθεση που πραγματοποιείται είναι διαφορετική, αφού σχεδιάζεται με βάση τα κίνητρα των ατόμων που τις εκτελούν. Οι ζημιές που επιφέρουν είναι πολυδιάστατες και δεν περιορίζονται μόνο στην απόκτηση οικονομικού οφέλους (Nivedita James, 2022). Έτσι, οι επιχειρήσεις και οι οργανισμοί καλούνται να λαμβάνουν προστατευτικά μέτρα, ώστε να είναι κατάλληλα προετοιμασμένοι για αντιμετώπισή τέτοιων επιθέσεων.

Κεφάλαιο 1

1. Κυβερνοεπιθέσεις

1.1 Πώς ορίζεται η κυβερνοεπίθεση

Στο πέρασμα του χρόνου έχουν δοθεί πολλαπλές ερμηνείες για το τι εστί κυβερνοεπίθεση (Cyber-attack). Σύμφωνα με το λεξικό το οποίο σύνταξε η διοίκηση του κυβερνοχώρου των Ηνωμένων Πολιτειών Αμερικής, κυβερνοεπίθεση ορίζεται ως η παράνομη απόπειρα απόκτησης πρόσβασης σε συσκευές, δίκτυα και εφαρμογές χωρίς την απαιτούμενη εξουσιοδότηση (Gen James & Cartright, 2011). Σκοπός των επιθέσεων αυτών είναι η τροποποίηση, η υποκλοπή και η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα του νόμιμου κατόχου, ώστε να προκληθεί ζημιά. Αυτό επιτυγχάνεται με ενέργειες οι οποίες στοχεύουν στην απενεργοποίηση, διαγραφή και αποκλεισμό των δεδομένων από τα συστήματα.

Μια κυβερνοεπίθεση μπορεί να λάβει χώρα σε οποιαδήποτε τοποθεσία, είτε από μεμονωμένα άτομα, είτε από οργανώσεις που ασχολούνται με τέτοιου είδους παράνομες δραστηριότητες. Η ανωνυμία που προσφέρει το διαδίκτυο στα άτομα που πραγματοποιούν αυτές τις επιθέσεις καθιστά δύσκολο τον εντοπισμό της προέλευσης τους. Οι κυβερνοεγκληματίες έχουν τη δυνατότητα να χρησιμοποιούν πληθώρα τεχνικών και μεθόδων για την παραβίαση των δικτύων, γι’ αυτό και η αντιμετώπιση τους πολλές φορές είναι εξαιρετικά δύσκολη (G Stevenson Smith, 2015). Σύνηθες φαινόμενο αποτελεί το γεγονός ότι οι hackers ζητούν χρηματικά λύτρα για την επιστροφή των δεδομένων και των πληροφοριών στον νόμιμο κάτοχό τους (Marleen Weulen Kranenbarg & Rutger Leukfeldt, 2021). Αυτό το χρηματικό ποσό χρησιμοποιείται για την αναβάθμιση και ενίσχυση του λογισμικού τους, ώστε να μπορούν εύκολα, αποτελεσματικά και χωρίς να ανιχνεύονται να επιτεθούν σε πιο μεγάλες επιχειρήσεις με απώτερο στόχο την μεγιστοποίηση των κερδών τους.

1.2 Εξέλιξη Κυβερνοεπιθέσεων στο πέρασμα του χρόνου

Η εμφάνιση των κυβερνοεπιθέσεων δεν αποτελεί ένα σύγχρονο φαινόμενο, καθώς οι πρώτες επιθέσεις πραγματοποιήθηκαν τον 20ο αιώνα, αποκτώντας στην πορεία μεγάλες διαστάσεις.

Το **1962**, ο Allan Scherr ο οποίος ήταν διδακτορικός υποψήφιος πραγματοποίησε την 1η «κυβερνοεπίθεση» κατά των υπολογιστών του MIT. Ο Allen δημιούργησε μια κάρτα διάτρησης, με την οποία ξεγέλασε το σύστημα του πανεπιστημίου, απέκτησε πρόσβαση στους κωδικούς των υπόλοιπων φοιτητών και έτσι μπορούσε να περιηγείται στο σύστημα για περισσότερες ώρες μέσα από τους λογαριασμούς τους (Arctic Wolf, 2022).

Το **1971** ο Bob Thomas, ένας μηχανικός της BBN Technologies, δημιούργησε ένα πρόγραμμα υπολογιστή, που είναι ευρέως γνωστό ως το πρώτο σκουλήκι σε ηλεκτρονικό υπολογιστή, με την ονομασία «Creeper Virus». Το συγκεκριμένο σκουλήκι, παρόλο που δεν θεωρείτο κακόβουλο και καταστροφικό, μπορούσε να μεταφερθεί από υπολογιστή σε υπολογιστή και να εμφανίζει το μήνυμα “I am the Creeper: Catch me if you can” στις οθόνες τις οποίες είχε μολύνει (Caleb Townsend, 2021). Αυτό ήταν αρκετά πρωτοποριακό για τη συγκεκριμένη εποχή, καθώς αποτελούσε τον πρώτο ιό που εμφανίστηκε ποτέ. Ο Ray Tomlinson, που ανακάλυψε το email, αποφάσισε τότε να δημιουργήσει έναν κώδικα που ονομαζόταν «Reaper» με στόχο να ανιχνεύει το σκουλήκι του Bob και να το καταστρέφει. Έτσι, θεωρείται ότι εμφανίστηκε το πρώτο λογισμικό ενάντια στους ιούς (antivirus software).

Το **1988** ο Robert Morris δημιούργησε ένα σκουλήκι το οποίο, αν και φτιάχτηκε με καλές προθέσεις, κατάφερε να επιφέρει απροσδόκητα αποτελέσματα. Γνωστό και ως «Morris Worm», είχε ως σκοπό τον εντοπισμό προβλημάτων ασφάλειας και αδύναμων κωδικών πρόσβασης. Ωστόσο, κάποιες λανθασμένες εντολές στον κώδικα του Morris, είχε ως αποτέλεσμα τον πολλαπλασιασμό των σκουληκιών, μολύνοντας περίπου 6.000 υπολογιστές και προκαλώντας ζημιές οι οποίες κυμαίνονταν από 100 χιλιάδες έως και 10 εκατομμύρια δολάρια (Siobhan Climer, 2018). Το σκουλήκι επηρέασε, ανάμεσα σε άλλα, συστήματα όπως του Stanford, NASA, Johns Hopkins και UC Berkeley. Ο Robert Morris ήταν ο πρώτος που καταδικάστηκε βάσει του νόμου περί απάτης και κατάχρησης υπολογιστών.

Το **1989** πραγματοποιήθηκε η πρώτη επίθεση ransomware, με τον βιολόγο Joseph Popp να δημιουργεί ένα κακόβουλο λογισμικό που ονομάστηκε «Aids_Trojan». Ο συγκεκριμένος ιός μεταφέρθηκε μέσω 20 χιλιάδων δισκετών σε παγκόσμιο συνέδριο με θέμα το Aids που διοργανώθηκε από τον Παγκόσμιου Οργανισμό Υγείας (Caleb Townsend, 2021). Ο Joseph είχε ως σκοπό να αποσπάσει χρήματα από τους συμμετέχοντες, ωστόσο το λογισμικό του ήταν κακοσχεδιασμένο και ο ιός μπορούσε εύκολα να αφαιρεθεί.

Από το **1990** και έπειτα, οι hackers εκμεταλλεύτηκαν την ανάπτυξη των τεχνολογιών και την αδυναμία εφαρμογής προστατευτικών μέτρων για να αυξήσουν τις επιθέσεις τους. Πολλοί ιοί εμφανίστηκαν μέσα στα επόμενα χρόνια, γεγονός που καταδείκνυε το μέγεθος του προβλήματος. Μέχρι το 1996, αναπτύχθηκαν νέες τεχνικές και πρωτοποριακές μέθοδοι ανάπτυξης ιών και επιθέσεων που επέτρεπαν την κλοπή δεδομένων και την πολυμορφία (Katie Chadd, 2020).

Το **1999** έκανε την εμφάνιση του ο ιός «Melissa», ο οποίος εισερχόταν σε υπολογιστές αφού οι χρήστες κατέβαζαν έγγραφα της Microsoft Word. Ο ιός οδηγούσε στην καταστροφή των δεδομένων που υπήρχαν στα έγγραφα, ενώ παράλληλα πολλαπλασιαζόταν καθώς μεταφερόταν μέσω email (Katie Chadd, 2020). Θεωρείται ένας από τους ταχύτερα εξαπλωμένους ιούς, ο οποίος μάλιστα επέφερε ζημιές που έφτασαν τα 80 εκατομμύρια δολάρια.

Την ίδια χρονιά στο Ηνωμένο Βασίλειο, ψηφίστηκε ένας από τους πρώτους νόμους που αφορούσαν στην ασφάλεια του κυβερνοχώρου. Συγκεκριμένα ψηφίστηκε Νόμος Περί Κατάχρησης Υπολογιστών, ο οποίος ποινικοποίησε την πειρατεία. Έτσι, οι ενέργειες πρόσβασης σε οποιοδήποτε σύστημα χωρίς την απαιτούμενη εξουσιοδότηση θεωρήθηκαν παράνομες. Πριν την ψήφιση του νόμου αυτού διεξάγονταν διάφορα ηλεκτρονικά εγκλήματα για τα οποία ήταν πολύ δύσκολο να ασκηθεί δίωξη.

Το **2003** δημιουργήθηκε μια ομάδα hacker με το όνομα «anonymous» οι οποίοι χρησιμοποιούσαν διάφορα ψευδώνυμα για να μην αποκαλυφθεί η ταυτότητά τους. Η ομάδα αυτή είναι γνωστή για τις επιθέσεις που πραγματοποιούσε εναντίων κυβερνήσεων και κρατικών ιδρυμάτων (Leonhard Dobusch & Dennis Schoeneborn, 2015). Η συγκεκριμένη οργάνωση πραγματοποίησε επιθέσεις σε πολλές χώρες παγκόσμια, ενώ έχει και πολλούς υποστηρικτές οι οποίοι τους χαρακτηρίζουν ως μαχητές της ελευθερίας και ψηφιακούς

«Ρομπέν των δασών». Ωστόσο, υπάρχουν και επικριτές, καθώς στα μάτια τους θεωρούνται κυβερνοεγκληματίες λόγω των επιθέσεων που έχουν προκαλέσει. Αξιοσημείωτο είναι το γεγονός ότι τα μέλη της οργάνωσης φοράνε μάσκες Guy Fawkes και μέσω προγραμμάτων αλλοιώνουν τις φωνές τους όταν δημοσιεύουν βίντεο, στα οποία μεταφέρουν μηνύματα που φανερώνουν τις δράσεις και τις απαιτήσεις τους (Tom Huddleston, 2022).

Κατά τον 21^{ο} αιώνα οι κυβερνοεπιθέσεις αυξήθηκαν με ραγδαίο ρυθμό. Οι hackers αναβάθμιζαν διαρκώς τα λογισμικά τους, με αποτέλεσμα να επιτίθονται με επιτυχία στους στόχους τους. Το γεγονός ότι χρησιμοποιούν διάφορες τεχνικές εξαπάτησης, σε συνδυασμό με την έλλειψη σωστής ενημέρωσης του κοινού σχετικά με θέματα προστασίας του διαδικτύου, έκαναν το έργο τους ακόμα πιο εύκολο. Ένα σημαντικό παράδειγμα που καταδεικνύει την εξέλιξη των κυβερνοεπιθέσεων είναι και η εμφάνιση του WannaCry malware το 2017, το οποίο μόλυνε περισσότερους από 220 χιλιάδες υπολογιστές σε μία μέρα. Θεωρείται ως ένα από τα πιο καταστροφικά λογισμικά, καθώς κρυπτογραφούσε δεδομένα και απειλούσε τους χρήστες ζητώντας χρήματα σε Bitcoin ως αντάλλαγμα της επιστροφής των δεδομένων (Arctic Wolf, 2022).

1.3 Λόγοι που πραγματοποιούνται κυβερνοεπιθέσεις

Στην υποενότητα αυτή γίνεται αναφορά στις κυριότερες αιτίες που οδηγούν τους ηλεκτρονικούς εγκληματίες στην παραβίαση της ιδιωτικότητας των επιχειρήσεων και την υποκλοπή δεδομένων. Οι λόγοι που πραγματοποιούνται επιθέσεις στον κυβερνοχώρο ποικίλουν, αφού οι ανάγκες, τα κίνητρα και ο σκοπός του κάθε hacker διαφέρουν, γι' αυτό και τα θύματα μιας κυβερνοεπίθεσης δεν είναι ποτέ συγκεκριμένα. Η επιλογή των θυμάτων εξαρτάται από τις προθέσεις που έχει ο κάθε εγκληματίας, αλλά και την ικανότητά τους να εκμεταλλεύονται τα ευάλωτα σημεία του κυβερνοχώρου.

- Οικονομικά οφέλη

Αναμφίβολα, οι περισσότερες κυβερνοεπιθέσεις έχουν σαν κύριο στόχο την απόκτηση χρηματικού οφέλους. Οι hackers μέσω των κακόβουλων λογισμικών που χρησιμοποιούν προσπαθούν να εξαπατήσουν τους χρήστες, ώστε να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες, όπως τραπεζικούς λογαριασμούς και πιστωτικές κάρτες (Brian Cashell, Mark Jickling, and Baird Webel, 2004). Με την απόκτηση κωδικών πρόσβασης επιτυγχάνεται η μεταβίβαση χρημάτων στον προσωπικό τους λογαριασμό με μηχανισμούς και εργαλεία που αποτρέπουν τον εντοπισμό τους. Σύμφωνα με έρευνες που πραγματοποιήθηκαν τα τελευταία χρόνια, υπολογίζεται ότι μέχρι το 2025 οι ζημιές από το κυβερνοέγκλημα αναμένεται να ανέλθουν στα 10,5 τρισεκατομμύρια δολάρια παγκοσμίως (Steve Morgan, 2020). Αυτό το ποσό υπολογίζεται πως θα αυξάνεται κάθε χρόνο με ραγδαίους ρυθμούς, γι' αυτό και οι επιχειρήσεις αναγκάζονται να εντοπίσουν λύσεις, με την εφαρμογή των οποίων θα ενισχυθεί η προστασία από τέτοιες επιθέσεις και το ρίσκο υποκλοπής χρημάτων.

- Κυβερνοπόλεμος

Ζώντας στον 21ο αιώνα, θα ήταν αφελές να αγνοήσουμε και το γεγονός ότι αρκετές κυβερνήσεις ανά το παγκόσμιο εμπλέκονται σε διάφορες ηλεκτρονικές επιθέσεις, παρόλο που μπορεί να αρνούνται οποιαδήποτε ανάμειξη. Ο κυριότερος λόγος στον οποίο διεθνή κράτη καταφεύγουν σε τέτοιου είδους επιθέσεις είναι η υποψία ότι άλλες χώρες ενδέχεται να ετοιμάζουν επιθέσεις εναντίον τους. Έτσι, λαμβάνουν την πρωτοβουλία να αντιμετωπίσουν προδραστικά αυτήν την υποψία κινδύνου με τη δημιουργία κακόβουλων προγραμμάτων, των οποίων η χρήση θα επιτρέψει την πρόσβαση σε απόρρητες

πληροφορίες άλλων κυβερνήσεων, ώστε να αντιληφθούν τις προθέσεις τους (Mark A Gregory & David Glance, 2013). Επομένως, οι επιθέσεις που πραγματοποιούνται εναντίων άλλων εθνών δημιουργούν διαμάχες και κόντρες μεταξύ των κυβερνήσεων, με αποτέλεσμα να δυσχεραίνονται οι σχέσεις τους και πολλές φορές να διεξάγονται ακόμη και πόλεμοι (Chris Mark, 2020).

- Πολιτικά κίνητρα

Ένας ακόμη σημαντικός λόγος που ωθεί τους εγκληματίες στην πραγματοποίηση κυβερνοεπιθέσων είναι και το πολιτικό πλαίσιο (Mary K. Pratt, 2022). Ειδικότερα, οι Hackers ενδέχεται να πραγματοποιούν τις επιθέσεις τους στοχευμένα, ενώ παράλληλα τα κίνητρα που οδηγούν σε αυτές είναι συχνά εκδικητικού χαρακτήρα. Δεν είναι άλλωστε λίγες οι φορές που πραγματοποιήθηκαν επιθέσεις εναντίων κυβερνήσεων, πολιτικών προσώπων και διεθνών οργανισμών, με στόχο να εκφραστεί η δυσαρέσκεια τους σε σχέση με τις ιδεολογίες, αξίες ή τον τρόπο δράσης τους. Λόγω της διαφοράς στα πιστεύω τους, οι hackers βρίσκουν διέξοδο σε ηλεκτρονικές επιθέσεις με σκοπό την πρόκληση μεγάλων ζημιών, ως ένδειξη της διαφωνίας τους με αυτούς (Robin Gandhi, Anup Sharma, William Mahoney,William Sousan & Phillip Laplante, 2011).

- Φήμη και αναγνώριση

Οι κυβερνοεπιθέσεις αποτελούν αδιαμφησβήτητα ένα από τα πλέον σημαντικότερα προβλήματα παγκοσμίως, καθώς σε περίπτωση μιας επιτυχημένης επίθεσης προκαλείται αναστάτωση και ανησυχία στην πλειοψηφία των ατόμων. Το γεγονός ότι μια κυβερνοεπίθεση θα οδηγήσει σε μεγάλη προβολή, ενδέχεται να ελκύει ανθρώπους να ξεκινήσουν την ενασχόληση με το hacking (Mary K. Pratt, 2022). Εξάλλου, υπάρχουν άτομα τα οποία έχουν εγγενή κίνητρα να πραγματοποιούν επιθέσεις σε οργανώσεις, εταιρείες ή κυβερνήσεις, με μοναδικό σκοπό την πρόκληση αναστάτωσης και χάους. Η παραβίαση ενός μεγάλου συστήματος οργανισμών ή εταιρειών πολλές φορές συναρπάζει, καθώς θεωρείται πρόκληση για τους ίδιους. Δεν είναι λίγες οι φορές που δημιουργείται και ανταγωνισμός ανάμεσα στους hackers, καθώς επιδιώκουν διαρκώς να αποδεικνύουν τις ικανότητές τους, ξεπερνώντας μερικές φορές τα όριά τους, εκτελώντας παράνομες δραστηριότητες.

1.4 Είδη κυβερνοεπιθέσεων

Οι τρόποι με τους οποίους πραγματοποιούνται κυβερνοεπιθέσεις ποικίλλουν, ωστόσο όπως αναφέρθηκε νωρίτερα, κοινός στόχος όλων είναι η επίτευξη κέρδους. Οι κυβερνοεγκληματίες χρησιμοποιούν διάφορες μεθόδους για τις επιθέσεις τους, ενώ ταυτόχρονα, αναζητούν συνεχώς και καινούργιες τεχνικές για την επίτευξη των στόχων τους, γεγονός που τους βοηθά να μην εντοπίζονται εύκολα. Πιο κάτω αναφέρονται οι δημοφιλέστερες και σύγχρονες μέθοδοι οι οποίες χρησιμοποιούνται από τους περισσότερους εγκληματίες στις ηλεκτρονικές τους επιθέσεις.

1.4.1 Malware (Ransomware, Spyware, Trojans κλπ.)

Το Malware είναι ένα κακόβουλο λογισμικό, το οποίο είναι προγραμματισμένο με στόχο την κλοπή δεδομένων από έναν υπολογιστή ή σύστημα. Οι hackers προωθούν το συγκεκριμένο λογισμικό σε χρήστες με στόχο να τους ξεγελάσουν και να το εγκαταστήσουν στον υπολογιστή τους. Το πιο διαδεδομένο και ζημιογόνο είδος Malware είναι το Ransomware, η χρήση του οποίου επιτρέπει την κρυπτογράφηση των δεδομένων και την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες του χρήστη. Στη συνέχεια, οι εγκληματίες ζητούν λύτρα από τους χρήστες, ώστε να τους επιστρέψουν τα δεδομένα που έχουν παραβιάσει και υποκλέψει (Martti Lehto & Pekka Neittaanmäki, 2022). Υπάρχουν διάφορα είδη ransomware, όπως το doxware, scareware, locker ransomware και crypto ransomware τα οποία αν και παρουσιάζουν διαφορές, έχουν ως κοινό σημείο την απαίτηση χρηματικού ανταλλάγματος για την επιστροφή των ευαίσθητων πληροφοριών (Kristan Stoddart, 2022). Έγκυρη έρευνα της Statista που πραγματοποιήθηκε το 2021, κατέδειξε ότι οι επιθέσεις ransomware παγκόσμια ανήλθαν στις 623.3 εκατομμύρια, αριθμός διπλάσιος σε σχέση με το 2020. Επίσης, τον Μάιο του 2021, η JBS USA, ένας από τους μεγαλύτερους παραγωγούς κρέατος, δέχθηκε επίθεση από ransomware και αναγκάστηκε να πληρώσει 11 εκατομμύρια δολάρια σε Bitcoin για να αποφύγει περαιτέρω ζημιά (Jacob Bunge, 2021).

1.4.2 Phishing

Το phishing είναι μια τεχνική ηλεκτρονικής εξαπάτησης που ξεγελά τους χρήστες, ώστε να τους αποσπάσει προσωπικές πληροφορίες, γι' αυτό και θεωρείται από τους πιο διαδεδομένους και επικίνδυνους τύπους κυβερνοεπιθέσεων. Αυτό το είδος επίθεσης επιτυγχάνεται με την αποστολή email ή συνδέσμων, τα οποία ενώ φαίνονται να προέρχονται από αξιόπιστες πηγές, οδηγούν τους παραλήπτες να αποκαλύπτουν ευαίσθητα δεδομένα (Mark Landahl & Tonya Thornton, 2021). Οι hackers, με στόχο να εξαλείψουν την αμφιβολία και την διστακτικότητα των χρηστών, χρησιμοποιούν στα μηνύματα ή τα email που αποστέλλουν ονόματα μεγάλων εταιρειών όπως η Google, Yahoo, Microsoft, ή ακόμη και των προσωπικών τους τραπεζών. Το κύρος και η αξιοπιστία των εταιρειών αυτών προσφέρει ένα αίσθημα ασφάλειας και εμπιστοσύνης, με αποτέλεσμα οι χρήστες να μην υποψιάζονται ότι μπορεί να πρόκειται για επίθεση. Σημαντικό είναι να σημειώσουμε πως με τα χρόνια εμφανίστηκαν και νέα είδη επίθεσης phishing, όπως το «Whaling», το οποίο στοχεύει άτομα με μεγαλύτερο κύρος, όπως διευθύνων σύμβουλους ή πολιτικούς. Η έκθεση της CISCO για την κυβερνοασφάλεια το 2021, αναφέρει πως το 90% των παραβιάσεων οφείλεται σε επιθέσεις τύπου phishing. Επίσης, μελέτες έδειξαν ότι οι εργαζόμενοι λαμβάνουν κάθε χρόνο περίπου 14 κακόβουλα email "ψαρέματος". Η IBM στην έκθεσή της αναφορικά με το κόστος παραβίασης δεδομένων που πραγματοποίησε το 2021, αναφέρει ότι το phishing αποτελεί την 2ο ακριβότερο φορέα επίθεσης, αφού η κάθε παραβίαση προκαλεί στις επιχειρήσεις ζημιές που ανέρχονται κατά μέσο όρο στα 4,65 εκατομμύρια δολάρια.

1.4.3 Cryptojacking

Το Cryptojacking αποτελεί ένα είδος κυβερνοεπίθεσης το οποίο τα τελευταία χρόνια βρίσκεται σε έξαρση. Σε αντίθεση με τα πλείστα κακόβουλα λογισμικά που σκοπός τους είναι η παραβίαση συστημάτων και η υποκλοπή δεδομένων, το cryptojacking χρησιμοποιείται με στόχο την εξόρυξη κρυπτονομισμάτων (Caner Asbas & Sule Tuzlukaya, 2022). Έγινε ευρέως γνωστό το 2017, αφού οι τιμές των bitcoin και άλλων κρυπτονομίσματων έφτασαν στα ύψη, γεγονός που έδωσε κίνητρο στους εγκληματίες για επίτευξη οικονομικού κέρδους. Για να επιτευχθεί μια επίθεση cryptojacking, οι hackers εγκαθιστούν στις συσκευές των ανυποψίαστων χρηστών ένα ειδικά σχεδιασμένο

λογισμικό, με στόχο την αναζήτηση κρυπτονομισμάτων. Ωστόσο, για να πραγματοποιηθεί η εγκατάσταση, οι χρήστες θα πρέπει να ανοίξουν κακόβουλους συνδέσμους ή email που τους έστειλαν οι εγκληματίες, ενώ πρόσφατες έρευνες έδειξαν ότι ο ιός εμφανίζεται και σε διαφημίσεις, οι οποίες συνήθως περιέχουν κωδικό JavaScript. Αφού εγκατασταθεί με επιτυχία το συγκεκριμένο λογισμικό, θα ακολουθήσει αναζήτηση πληροφοριών σχετικά με κρυπτονομίσματα ή πορτοφόλια κρυπτονομισμάτων που πιθανόν να έχουν οι χρήστες. Εάν βρεθούν κρυπτονομίσματα στην κατοχή των ατόμων, οι hackers με έντεχνους μηχανισμούς θα προβούν στην κλοπή τους. Ταυτόχρονα, η δραστηριότητα αυτή ενδέχεται να προκαλέσει και καθυστερήσεις στην απόδοση του συστήματος των συσκευών των θυμάτων. Επιπλέον, σύμφωνα με την έκθεση «Cyber threat 2021» της SonicWall, κατά το πρώτο εξάμηνο του 2021 πραγματοποιήθηκαν περίπου 51.1 εκατομμύρια επιθέσεις cryptojacking, αριθμός που είναι κατά 23% μεγαλύτερος από τον αντίστοιχο του προηγούμενου έτους (SonicWall, 2021).

1.4.4 Data breach

Η παραβίαση δεδομένων είναι μια μορφή κυβερνοεπίθεσης, με την οποία οι εισβολείς αποκτούν παράνομη πρόσβαση σε ευαίσθητες πληροφορίες άλλων ατόμων ή οργανισμών. Οι εγκληματίες επιτυγχάνουν την παράνομη πρόσβαση δεδομένων, λόγω αδυναμιών στο σύστημα ή στην συμπεριφορά των χρηστών. Οι επιθέσεις αυτές στοχεύουν στην παραβίαση προσωπικών δεδομένων, όπως αριθμό πιστωτικών καρτών, αριθμό τραπεζικών λογαριασμών, ιατρικά στοιχεία, ενώ στην περίπτωση επιχειρήσεων αναζητούνται και λίστες πελατών (Pete Finnigan, 2018). Με αυτό τον τρόπο παραβιάζεται η ιδιωτικότητα και η ελευθερία του ατόμου, γι’ αυτό και εάν προκύψουν τέτοιου είδους περιστατικά, κάθε επιχείρηση οφείλει να ενημερώσει την εποπτική αρχή έγκαιρα, ώστε να ληφθούν τα κατάλληλα μέτρα. Σύμφωνα με την εταιρεία παροχής υπηρεσιών VPN Surfshark, κατά το 2021 υπήρξαν 952.8 εκατομμύρια παραβάσεις λογαριασμών παγκοσμίως, εκ των οποίων 212 εκατομμύρια έγιναν στην Αμερική (Surfshark, 2022). Οι μεγαλύτερες παραβιάσεις δεδομένων το 2021 προκλήθηκαν σε εταιρείες τεράστιου βελησνεκούς όπως η Facebook, RAYCHAT και COMB.

1.4.5 Supply chain attacks

Η εφοδιαστική αλυσίδα μπορεί να χαρακτηριστεί ως ένα δίκτυο στο οποίο υπάρχει αλληλεπίδραση και αλληλεξάρτηση ατόμων και πόρων, με στόχο την ολοκλήρωση των δραστηριοτήτων μιας επιχείρησης μέχρι την τελική πώληση ενός προϊόντος. Οι επιθέσεις που στοχεύουν στην εφοδιαστική αλυσίδα ενός οργανισμού, επιδιώκουν την πρόκληση ζημιάς μέσω της διείσδυσης σε δεδομένα τμημάτων που παρουσιάζουν τις μεγαλύτερες αδυναμίες. Έτσι, οι hackers με ύπουλες τεχνικές εισέρχονται στο δίκτυο ενός οργανισμού εκμεταλλευόμενοι τις καλές σχέσεις και την εμπιστοσύνη που έχουν οι επιχειρήσεις με τους προμηθευτές τους και τοποθετούν κακόβουλα λογισμικά, αποκτώντας έτσι πρόσβαση σε σημαντικές πληροφορίες. Εάν οι επιθέσεις αυτές πραγματοποιηθούν με επιτυχία, οι επιχειρήσεις ενδέχεται να έρθουν αντιμέτωπες με οικονομικές και λειτουργικές συνέπειες ή ακόμη και με καταστροφή της φήμης τους. Μια μελέτη που πραγματοποιήθηκε από την εταιρεία BlueVoyant το 2020 που ασχολείται με θέματα κυβερνοασφάλειας και έχει έδρα την Νέα Υόρκη, αποκάλυψε ότι το 80% των οργανισμών δέχτηκαν παραβίαση που προήλθε από τρίτους. Μάλιστα το 2021 παρατηρήθηκε αύξηση κατά 51% στην εμφάνιση τέτοιων επιθέσεων, γεγονός που προκαλεί ανησυχία και προβληματισμό σε μεγάλους οργανισμούς που ασχολούνται με θέματα κυβερνοασφάλειας (Phil Muncaster, 2022).

1.4.6 Non malicious threats

Οι μη κακόβουλες απειλές προέρχονται από εργαζόμενους μιας εταιρείας, οι οποίοι από απροσεξία και αμέλεια μπορεί να δημιουργήσουν σοβαρά θέματα σε ένα οργανισμό, μη έχοντας κακές προθέσεις (Manuel Sanchez, 2022). Χωρίς να το αντιλαμβάνονται, επιτρέπουν στους hackers την είσοδο στο σύστημα της εταιρείας που εργάζονται. Αυτό επιτυγχάνεται μέσα από απλές καθημερινές δραστηριότητες, όπως η αποστολή συνδέσμων και email σε λάθος παραλήπτες, γεγονός που εκμεταλλεύονται οι hackers για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες. Επίσης, πολλές φορές οι εργαζόμενοι των εταιρειών χρησιμοποιούν αδύναμους κωδικούς πρόσβασης στους υπολογιστές τους ή επιχειρούν την είσοδο σε ευαίσθητα δεδομένα μέσα από δημόσια δίκτυα, γεγονός που δίνει την ευκαιρία στους εγκληματίες να πραγματοποιήσουν επίθεση στον οργανισμό. Η

έκθεση «Cost of insider threats» του ινστιτούτου Ponemon, κατέδειξε ότι οι απροσεξίες των εργαζομένων προκαλούν το 62% των περιστατικών ασφαλείας ενός οργανισμού, κοστίζοντας κατά μέσο όρο περίπου 307 χιλιάδες δολάρια για κάθε περιστατικό (Jennifer Gregory, 2022). Επομένως, έκδηλα αντιλαμβανόμαστε ότι οι ενέργειες των υπαλλήλων μιας εταιρείας έχουν τεράστιο αντίκτυπο στα θέματα ασφάλειας.

1.5 Μεγάλες κυβερνοεπιθέσεις του 21ου αιώνα

1.5.1 TJX companies Inc.

Η TJX companies Inc είναι μια μεγάλη αμερικάνικη πολυεθνική εταιρεία πολυκαταστημάτων που βασίζει τη λειτουργία της στην εκπτωτική τιμολόγηση, καθώς προσφέρει ποικιλία επώνυμων ενδυμάτων, κοσμημάτων και είδη σπιτιού σε πολύ χαμηλές τιμές. Η εταιρεία απαρτίζεται από 578 καταστήματα σε όλη την Αμερική, ενώ διατηρεί αρκετά σε Καναδά και Ευρώπη. Με τις συνεχόμενες προσπάθειες της TJX companies inc, αλλά και την πελατοκεντρική προσέγγιση που έχει υιοθετήσει, η εταιρεία έχει καταφέρει να κερδίσει μια ξεχωριστή θέση στο μυαλό του καταναλωτή, αποκτώντας εκατομμύρια πιστούς πελάτες (Edwin Covert, 2021).

Ωστόσο, υπήρξε μια περίοδος όπου η εταιρεία δέχθηκε κυβερνοεπίθεση. Συγκεκριμένα, το 2007 hackers κατάφεραν με επιτυχία να παραβιάσουν τα συστήματα της εταιρείας και τα δεδομένα της και να κλέψουν πάνω από 45 εκατομμύρια πιστωτικές και χρεωστικές κάρτες πελατών της (Andrew Miller, 2007). Αξιοσημείωτο είναι επίσης και το γεγονός ότι η εταιρεία αν και είχε επενδύσει σε πληροφοριακές τεχνολογίες με στόχο την ενίσχυση της ασφάλειάς της, εντούτοις απέτυχε να αποκρούσει τη συγκεκριμένη επίθεση.

Οι έρευνες που ακολούθησαν αποκάλυψαν αρκετά κενά ασφαλείας στο σύστημα της TJX companies Inc, τα οποία ευνόησαν την εκδήλωση της επίθεσης. Αρχικά, η TJX αποθήκευε άσκοπα πολλά δεδομένα πελατών της για μεγάλο χρονικό διάστημα. Έτσι, οι ευαίσθητες αυτές πληροφορίες ήταν ευάλωτες και πολύ ευκολά μπορούσαν να περάσουν στα χέρια μη εξουσιοδοτημένων ατόμων. Επίσης, όπως αποκαλύφτηκε μεταγενέστερα, η εταιρεία χρησιμοποιούσε και μεθόδους κρυπτογράφησης δεδομένων, οι οποίες όμως σύμφωνα με ερευνητές, περιείχαν αρκετές αδυναμίες.

Η συγκεκριμένη κυβερνοεπίθεση επέφερε τεράστιες επιπτώσεις στην εταιρεία. Από οικονομικής άποψης, η TJX αναγκάστηκε να πληρώσει περίπου 70 εκατομμύρια δολάρια στη visa και τη master card για την διευθέτηση διάφορων ζητημάτων. Ακόμη, αποζημίωσε μεγάλο αριθμό πελατών, οι οποίοι επηρεαστήκαν από αυτή την ηλεκτρονική απάτη (Edwin Covert, 2021).

Εξίσου μεγάλο ποσό δαπανήθηκε για να μπορέσει η εταιρεία να εξοπλιστεί με την κατάλληλη τεχνολογία που θα τη βοηθούσε να ανταπεξέλθει σε θέματα κυβερνοασφάλειας. Οι επιπτώσεις όμως δεν περιορίστηκαν στον οικονομικό τομέα, αλλά είχε και αρνητικό αντίκτυπο στη φήμη της, καθώς έχασε εκατομμύρια πελάτες. Ο φόβος και η ανησυχία ότι προσωπικά δεδομένα μπορεί να εκτεθούν οποιαδήποτε στιγμή, ώθησε τους πελάτες της να στραφούν σε ανταγωνιστές της εταιρείας και να απολαμβάνουν προϊόντα και υπηρεσίες από αυτούς.

Για αρκετά χρόνια η φήμη και το brand name της εταιρείας είχαν κλονιστεί. Ωστόσο με σκληρή δουλειά, υπομονή και θέληση η TJX companies Inc κατάφερε να ανέβει ξανά ψηλά στα μάτια του καταναλωτή.

1.5.2 Yahoo

Η Yahoo είναι μια εταιρεία παροχής υπηρεσιών διαδικτύου και συγκεκριμένα είναι η δεύτερη μεγαλύτερη μηχανή αναζήτηση μετά από την Google. Ιδρύθηκε το 1994 και έχει σαν έδρα το Σανιβέιλ των Ηνωμένων Πολιτειών Αμερικής (Tim Fisher, 2022). Η εταιρεία παρέχει πληθώρα υπηρεσιών και επιλογών, όπως ηλεκτρονικό ταχυδρομείο, μηχανή αναζήτησης, παιχνίδια κλπ.

Το 2013 η εταιρεία δέχτηκε μια από τις μεγαλύτερες κυβερνοεπιθέσεις που έγιναν ποτέ. Ενώ αρχικά έγινε λόγος για παραβίαση ενός δισεκατομμυρίου λογαριασμών, μετά από χρόνια ανακοινώθηκε πως ο αριθμός λογαριασμών που επηρεαστήκαν από την επίθεση ανέρχεται στα 3 δισεκατομμύρια. Οι κυβερνοεγκληματίες κατάφεραν να υποκλέψουν δεδομένα όπως usernames, ημερομηνίες γέννησης, κωδικούς πρόσβασης και αριθμούς τηλεφώνων (Ioannis Giagkinis, 2017).

Η Yahoo ξεκαθάρισε πως δεν υποκλάπηκαν στοιχεία που αφορούν τραπεζικούς λογαριασμούς, πιστωτικές και χρεωστικές κάρτες (Alina Selyukh, 2017). Η εταιρεία

κατηγορήθηκε για αμέλεια και μη επαρκή συστήματα ασφαλείας, γεγονός που θεωρείται αδιανόητο αν αναλογιστούμε το μέγεθος και τον αριθμό πελατών που εξυπηρετεί.

Το 2014 και 2016 πραγματοποιήθηκαν και άλλες κυβερνοεπιθέσεις κατά της εταιρείας, οι οποίες ήρθαν να μειώσουν ακόμη περισσότερο το κύρος και τη φήμη της. Αυτό οδήγησε μεγάλο ποσοστό των πελατών να απομακρυνθούν από αυτή, καθώς η εταιρεία δεν κατάφερε να δημιουργήσει ένα αίσθημα ασφάλειας και αξιοπιστίας προς αυτούς.

1.5.3 The United State Office of Personnel Management

Το γραφείο διαχείρισης προσωπικού των Ηνωμένων Πολιτειών Αμερικής είναι μια ανεξάρτητη υπηρεσία, η οποία ασχολείται με την ηγεσία και υποστήριξη ανθρώπινου δυναμικού σε ομοσπονδιακούς οργανισμούς (Josh Fruhlinger, 2020). Συγκεκριμένα, ασχολείται με θέματα που αφορούν ιατρική περίθαλψη, ανθρώπινους πόρους και ασφάλιση ζωής για υπαλλήλους της ομοσπονδιακής κυβέρνησης.

Το 2015, στελέχη του πληροφορικού τμήματος του οργανισμού ανακάλυψαν ότι παραβιάστηκαν αρχεία του προσωπικού. Έρευνες φανέρωσαν ότι το κακόβουλο λογισμικό που χρησιμοποιήθηκε για την επίθεση ήταν εγκατεστημένο στο σύστημα του οργανισμού από το 2013 (Adam Botek, 2021). Η επίθεση πραγματοποιήθηκε από άγνωστη ομάδα η οποία χρηματοδοτείτο από την κινέζικη κυβέρνηση. Στόχος της επίθεσης ήταν η απόκτηση εξαιρετικά ευαίσθητων πληροφοριών για τα άτομα της Αμερικάνικης υπηρεσίας.

Η κατασκοπευτική εκστρατεία οδήγησε στην κλοπή προσωπικών δεδομένων περισσότερων από 21,5 εκατομμύρια ατόμων που αφορούσαν ονόματα, ημερομηνίες γέννησης, αριθμό κατοικίας και αριθμό κοινωνικών ασφαλίσεων (Adam Botek, 2021).

Η συγκεκριμένη επίθεση είχε ως αποτέλεσμα την παραίτηση υψηλόβαθμων στελεχών του γραφείου διαχείρισης προσωπικού. Επιπλέον, υπήρξαν πολλές μηνύσεις κατά του οργανισμού σχετικά με την αδυναμία προστασίας της ιδιωτικότητας του αμερικάνικου πληθυσμού. Από οικονομικής άποψης η κυβέρνηση αναγκάστηκε να πληρώσει αρκετά δισεκατομμύρια και να προσφέρει προνόμια στους πολίτες που ήταν θύματα αυτής της παραβίασης. Τέλος, αν και η κινέζικη κυβέρνηση δεν κατηγορήθηκε επίσημα για το

περιστατικό αυτό, η πεποίθηση της Αμερικής για εμπλοκή της Κίνας στο συμβάν οδήγησε στην ρήξη των σχέσεων των δύο χωρών (Josh Fruhlinger, 2020).

1.6 Κυβερνοεπιθέσεις εν καιρώ πανδημίας

Η πανδημία του κορονοϊού προκάλεσε τεράστιες ανακατατάξεις στη ζωή δισεκατομμυρίων ανθρώπων σε ολόκληρο τον πλανήτη. Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ), μέχρι τον Νοέμβριο του 2022 είχαν επιβεβαιωθεί περισσότερα από 630 εκατομμύρια κρούσματα κορονοϊού και 6,58 εκατομμύρια θάνατοι. Από τη μια μέρα στην άλλη, όλοι οι τομείς της ζωής μας άλλαξαν ριζικά, αναγκάζοντάς μας να προσαρμοστούμε στα νέα δεδομένα, ώστε να ανταπεξέλθουμε στην πρωτόγνωρη αυτή κατάσταση.

Επιπρόσθετα, οι επιχειρήσεις υποχρεώθηκαν να επαναπροσδιορίσουν το μοντέλο λειτουργίας τους, υιοθετώντας την εργασία από το σπίτι. Έτσι, η χρήση της τεχνολογίας έγινε ακόμη πιο σημαντική τόσο για την επαγγελματική όσο και την προσωπική μας ζωή. Αναπόφευκτά πλέον, ο πληθυσμός εκτελούσε τις περισσότερες υποχρεώσεις της καθημερινότητάς του μέσω του διαδικτύου, αφού δεν ήταν εφικτό να τις πραγματοποιήσει με φυσική παρουσία (Ruti Gafni &Tal Pavel, 2021). Η μεγαλύτερη και εντονότερη χρήση της τεχνολογίας έδωσε ευκαιρία στους hackers να εντείνουν την δράση τους και τις επιθέσεις τους. Επιπλέον, το γεγονός ότι ο κόσμος είχε άφθονο ελεύθερο χρόνο στο σπίτι χωρίς ιδιαίτερες ασχολίες, οδήγησε πολλά άτομα στην εκμάθηση και την ενασχόληση με παράνομες ενέργειες του hacking. Επομένως, εύκολα συμπεραίνουμε τον λόγο για την εκτόξευση των κυβερνοεπιθέσεων παγκοσμίως. Δεν είναι τυχαίο πως οι επίσημες καταγγελίες σχετικά με απάτες στον κυβερνοχώρο τους πρώτους μήνες την πανδημίας αυξήθηκαν κατά 300%-400%.

Ένα άλλο χαρακτηριστικό της περιόδου αυτής ήταν και η αύξηση του κόστους των επιχειρήσεων, καθώς αναγκάστηκαν να δαπανήσουν ένα σημαντικό ποσό για την ενίσχυση της ασφάλειας των συστημάτων τους. Αυτό, και σε συνδυασμό με τις αυξημένες κυβερνοεπιθέσεις οδήγησαν πολλές επιχειρήσεις στο να έρθουν αντιμέτωπες με σημαντικά οικονομικά προβλήματα, ενώ αρκετές από αυτές δεν ήταν ικανές να αντέξουν την οικονομική πίεση και εν τέλει οδηγήθηκαν σε κλείσιμο. Επιπρόσθετα, ένα από τα

μεγαλύτερα λάθη των οργανισμών κατά την περίοδο αυτή ήταν η μη ορθή ενημέρωση του προσωπικού τους σχετικά με θέματα ασφάλειας. Οι πλείστες επιχειρήσεις θεώρησαν σημαντικότερο να εξοπλιστούν με λογισμικά και συστήματα τελευταίας τεχνολογίας, αφού έκριναν πως αποτελούν πιο αποτελεσματικό τρόπο προστασίας και απόκρουσης των κυβερνοεπιθέσεων.

Έρευνα που διεξήχθη από το παγκόσμιο οικονομικό forum, κατέδειξε ότι το 95% των παραβιάσεων της κυβερνοασφάλειας οφείλεται σε ανθρώπινα λάθη. Εύλογα λοιπόν αντιλαμβανόμαστε πως επειδή οι οργανισμοί επικέντρωσαν τις προσπάθειες και τους πόρους τους προς μία μόνο κατεύθυνση, αδυνατούσαν να αντιμετωπίσουν τέτοιου είδους περιστατικά. Μερικές προβλέψεις που πραγματοποιήθηκαν, υπολογίζουν ότι τα επόμενα χρόνια το κυβερνοέγκλημα θα επιφέρει τεράστιο κόστος στις εταιρείες, ποσό το οποίο θα παρουσιάζει αύξηση 15% χρόνο με το χρόνο (Mike Mclean, 2023).

1.7 Cloud computing εν καιρώ πανδημίας

Το cloud είναι ένα πολύ χρήσιμο εργαλείο το οποίο διευκολύνει σε μεγάλο βαθμό την καθημερινότητα των χρηστών του διαδικτύου. Αποτελεί ένα σύνολο διακομιστών που μπορεί να βρίσκονται οπουδήποτε στον κόσμο, παρέχοντας υπηρεσίες αποθήκευσης αρχείων και παράδοσης πόρων πληροφορικής μέσω διαδικτύου. Επομένως, αντί οι επιχειρήσεις να διατηρούν φυσικούς πόρους αποθήκευσης δεδομένων, με το cloud τους δίνεται η δυνατότητα να έχουν πρόσβαση σε εικονικούς χώρους αποθήκευσης. Αντίστοιχα, οι χρήστες δύναται να αποθηκεύουν φωτογραφίες, βίντεο κλπ., χωρίς να επιβαρύνουν τον αποθηκευτικό χώρο της συσκευής τους, αφού αυτά θα βρίσκονται στους απομακρυσμένους servers (Mansoor Alaali, 2022).

Κατά την περίοδο της πανδημίας παρατηρήθηκε θεαματική στροφή του πληθυσμού στη χρήση του cloud. Σε έρευνα που πραγματοποιήθηκε το 2021 από την αμερικάνικη εταιρεία Flexera η οποία ασχολείται με λογισμικά υπολογιστών Cloud, σημειώνει πως 9 στους 10 οργανισμούς εν καιρώ πανδημίας χρησιμοποιούσαν δημόσιο ή ιδιωτικό cloud, λόγω της αυξανόμενης διαδικτυακής χρήσης. Παραδείγματα δημόσιου cloud που χρησιμοποιήθηκαν περισσότερο ήταν της Google, AWS και Azure (Kevin Miller, 2021).

Αναντίρρητα, το γεγονός πως όλο και περισσότερα άτομα και οργανισμοί υιοθετούν τη χρήση του cloud, καταδεικνύει το μέγεθος των πλεονεκτημάτων που προσφέρει. Αρχικά,

εάν μια επιχείρηση στραφεί προς τη χρήση cloud θα καταφέρει να μειώσει τα πάγια κόστη της, καθώς δεν θα διατηρεί ιδιωτικούς servers, εξοικονομώντας έτσι έξοδα που σχετίζονται με αυτούς. Το cloud δίνει τη δυνατότητα στο χρήστη να πληρώνει ένα χρηματικό ποσό ανάλογα με τη χρήση και τον αποθηκευτικό χώρο που χρειάζεται.

Επιπρόσθετα, παρέχει μεγάλη ευελιξία και πρόσβαση σε σωρεία τεχνολογιών, γεγονός που επιτρέπει συνεχή καινοτομία και ανανέωση του αποθηκευτικού χώρου. Έτσι, οι επιχειρήσεις και οι χρήστες έχουν τη δυνατότητα να προσαρμοστούν ταχύτατα στις νέες τους ανάγκες, στοιχείο που τους δίνει την ευκαιρία να πειραματιστούν και να διαφοροποιηθούν. Ταυτόχρονα, το γεγονός ότι το cloud λειτουργεί επιτυχώς καθημερινά ολόκληρο τον χρόνο με μηδαμινά τεχνικά προβλήματα ενισχύει σε μεγάλο βαθμό την αξιοπιστία του. Ένα ακόμη σημαντικό πλεονέκτημα του clouds είναι η ευκολία διαχείρισής του, καθώς δεν περιλαμβάνει περίπλοκες εντολές και ρυθμίσεις. Οι λειτουργίες του αναβαθμίζονται αυτόματα οπότε υπάρχει διαθέσιμη ενημέρωση και έτσι ο χρήστης να δουλεύει με εργονομικό τρόπο χωρίς διακοπές και καθυστερήσεις.

Ένας άλλος λόγος που ωθεί τις επιχειρήσεις προς τη χρήση cloud είναι η ανάγκη για ενίσχυση της περιβαλλοντικής βιωσιμότητας στα πλαίσια της εταιρικής κοινωνικής ευθύνης. Είναι κοινώς αποδεκτό ότι οι σύγχρονοι οργανισμοί δίνουν μεγαλύτερη βαρύτητα σε θέματα που αφορούν την εταιρική κοινωνική ευθύνη και μεριμνούν ούτως ώστε να την ενισχύσουν. Μέσα σε αυτά τα πλαίσια οδηγούνται στην υιοθέτηση δημόσιου cloud, η οποία έχει ως αποτέλεσμα να μειώσει τον αντίκτυπο χρήσης του άνθρακα. Αντίθετα, τα παραδοσιακά συστήματα αποθήκευσης δεδομένων απαιτούν τόνους ηλεκτρικής ενέργειας, ψυκτικούς μηχανισμούς και συνεχόμενη κοστοβόρα συντήρηση, στοιχεία τα οποία προκαλούν τεράστιες επιπτώσεις στο περιβάλλον (Jamie Morgan, 2015). Επίσης, η στροφή των εταιρειών σε μια πιο οικολογική συνείδηση τυγχάνει αναγνώρισης και επιβράβευσης από τους καταναλωτές, οι οποίοι τα τελευταία χρόνια τις στηρίζουν όλο και περισσότερο.

Τέλος, ένας από τους σημαντικότερους λόγους που στράφηκαν οι επιχειρήσεις προς τη χρήση cloud είναι η αυξημένη ασφάλεια και η προστασία των δεδομένων που παρέχει. Ο αριθμός των κυβερνοεπιθέσεων τα τελευταία δύο χρόνια ξεπέρασε κάθε προηγούμενο με τις επιθέσεις στο διαδικτυακό χώρο να διαδέχονται η μία την άλλη. Επομένως, το cloud θεωρείται πλέον η πιο αξιόπιστη λύση για την προστασία της ιδιωτικότητας και της ασφάλειας προσωπικών δεδομένων. Συγκεκριμένα, το cloud κρυπτογραφεί τα δεδομένα

χρησιμοποιώντας το μοντέλο στρατιωτικής ποιότητας AES 256 που αποτρέπει τους hackers να διαβάσουν και να κλέψουν δεδομένα (Jamie Morgan, 2015). Δεν μπορεί επίσης, να μην σημειωθεί ότι το cloud έχει ικανό εργατικό δυναμικό το οποίο παρακολουθεί το σύστημα όλο το 24ώρο, ώστε να αντιληφθεί πιθανές ευπάθειες ή κινδύνους που μπορεί να εμφανιστούν.

Εν κατακλείδι, αν και αργοπορημένα, ο κόσμος αρχίζει να αντιλαμβάνεται τη μεγάλη σημασία που έχει η προστασία των πληροφοριών και των δεδομένων στις μέρες μας. Διάφορες προβλέψεις που πραγματοποιήθηκαν κάνουν λόγο πως τα επόμενα χρόνια το cloud computing θα χρησιμοποιείται από την πλειοψηφία. Επομένως, υπάρχει ελπίδα πως με την αυξημένη του χρήση ο κόσμος θα απολαμβάνει τόσο τα οφέλη και τις διευκολύνσεις τις οποίες παρέχει, ενώ ταυτόχρονα θα είναι και πιο ασφαλής από ενδεχόμενες κυβερνοεπιθέσεις.

Κεφάλαιο 2

2. Κυβερνοασφάλεια

2.1 Πώς ορίζεται η Κυβερνοασφάλεια

Η ευκολία και η συχνότητα με την οποία πραγματοποιούνται κυβερνοεπιθέσεις ανά το παγκόσμιο προβληματίζουν σε μεγάλο βαθμό κυβερνήσεις, επιχειρήσεις και οργανισμούς. Οι ζημιές που προκαλούνται από τέτοιου είδους επιθέσεις μπορεί να είναι καταστροφικές και μη ανατρέψιμες. Επομένως, επιτακτική ανάγκη αποτελεί η υιοθέτηση μιας νοοτροπίας στην οποία οι πολίτες θα είναι ευαισθητοποιημένοι σε θέματα που αφορούν την ιδιωτικότητά τους και την προστασία των προσωπικών τους δεδομένων.

Αρχικά, τα άτομα επιβάλλεται να εμπλουτιστούν με γνώσεις και πληροφορίες που θα τους βοηθήσουν να κατανοήσουν τη σημαντικότητα της διαδικτυακής τους ασφάλειας. Ταυτόχρονα, είναι σημαντικό να προβούν σε ενέργειες που θα μειώσουν το ρίσκο τέτοιου είδους επιθέσεων και θα ενισχύσουν σημαντικά την προστασία τους από τους κυβερνοεγκληματίες. Για την επίτευξη όλων αυτών χρειάζεται συλλογική προσπάθεια, σοβαρότητα και θέληση. Μόνο με τον τρόπο αυτό θα μπορεί ο κάθε πολίτης να αντιληφθεί την έννοια της κυβερνοασφάλειας, ώστε να εκτελεί τις καθημερινές του διαδικτυακές δραστηριότητες με ασφάλεια χωρίς να κινδυνεύει από επιθέσεις.

Τα συστήματα δικτύου των κυβερνήσεων, των επιχειρήσεων και των απλών ανθρώπων έχουν ιδιαίτερη σημασία, γι’ αυτό και επιβάλλεται η προστασία τους, η οποία επιτυγχάνεται με την κυβερνοασφάλεια. Η κυβερνοασφάλεια αποτελεί όλες τις διαδικασίες και τεχνικές που σχετίζονται με την προστασία των δικτύων, των συσκευών και των ευαίσθητων δεδομένων από πιθανές ψηφιακές απειλές. Πιο συγκεκριμένα, αποσκοπεί στην ανίχνευση, ανάλυση και πρόβλεψη πιθανών ηλεκτρονικών απατών, με σκοπό να αποφευχθούν και να αντιμετωπιστούν έγκαιρα και αποτελεσματικά (Godwin Thomas & Mary-Jane Sule, 2021).

Ακόμη, ορίζεται και ως το μέσο διατήρησης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας στον κυβερνοχώρο (Basie Von Solms & Rossouw Von Solms, 2017). Η έλλειψη της απαραίτητης προστασίας και λήψης μέτρων για αντιμετώπιση ηλεκτρονικών επιθέσεων, επιτρέπει στους hackers να πραγματοποιούν στοχευμένες επιθέσεις με μεγαλύτερη ευκολία. Έτσι, προκαλούν σοβαρές ζημιές σε διάφορους τομείς της ζωής μας, όπως η υγεία, η οικονομία και η εκπαίδευση.

Είναι γεγονός ότι με το πέρασμα των χρόνων σημειώνεται δραματική αύξηση ηλεκτρονικών επιθέσεων με στόχο την απόκτηση πληροφοριών και δεδομένων (Hamid Jahankhani, Arshad Jamal & Shaun Lawson, 2021). Παρόλο που μεγάλες εταιρείες και οργανισμοί λαμβάνουν μέτρα για την κυβερνοασφάλεια, αρκετές από αυτές αδυνατούν να αντιμετωπίσουν κακόβουλες ενέργειες εναντίον τους. Η αύξηση της συχνότητας και οι εντάσεις των κυβερνοεπιθέσεων προβληματίζουν σε μεγάλο βαθμό, γι’ αυτό και χρειάζεται να βρίσκονται πάντα σε εγρήγορση, ώστε να αποκρούσουν όσο το δυνατό περισσότερες μπορούν. Επομένως, η κυβερνοασφάλεια διαδραματίζει καθοριστικό ρόλο για την προστασία και την εξάλειψη αυτών των επιθέσεων, μέσα από την υιοθέτηση των βέλτιστων πρακτικών.

2.2 Οργανισμός ENISA

Ο ENISA αποτελεί τον ευρωπαϊκό οργανισμό για την κυβερνοασφάλεια, ο οποίος ιδρύθηκε το 2004 και έχει ως έδρα το Ηράκλειο στην Ελλάδα. Η σύστασή του έγινε με σκοπό τη δημιουργία μιας πολιτικής στην ΕΕ, η οποία θα διασφαλίζει την προστασία και την ασφάλεια των δικτύων προς όφελος των πολιτών και των επιχειρήσεων. Οι προσπάθειες του οργανισμού βασίζονται στη δημιουργία μιας σχέσης εμπιστοσύνης με το κοινό χρησιμοποιώντας προηγμένο εξοπλισμό και λογισμικά, ενισχύοντας έτσι την αξιοπιστία του. Ο συνδυασμός των ικανοτήτων του προσωπικού, αλλά και οι συμμαχίες με μεγάλες επιχειρήσεις του κλάδου, καθιστούν τον ENISA ως ένα κολοσσό, ο οποίος έχει καταφέρει να διατηρήσει την ηλεκτρονική ασφάλεια στους πολίτες της ΕΕ. Χαρακτηρίζεται από ευελιξία και καινοτομία και αναμφίβολα αποτελεί κλειδί στον χώρο της κυβερνοασφάλειας στην ΕΕ.

Ο οργανισμός παρέχει τόσο συμβουλευτικές όσο και συντονιστικές υπηρεσίες για την ασφάλεια και ανάλυση δεδομένων. Η υψηλή εξειδίκευση, καθώς και η εμπειρογνωμοσύνη των ατόμων που απαρτίζουν τον οργανισμό, ενθαρρύνει τα κράτη μέλη της ΕΕ να ζητούν συμβουλές για τεχνικά θέματα ασφαλείας. Επιπρόσθετα, ο ENISA προσπαθεί να προβλέψει πιθανούς κινδύνους μέσα από τη συλλογή και την επεξεργασία δεδομένων, ώστε να προτείνει εφαρμόσιμες λύσεις για την διαχείριση τους. Έτσι, αποτελεί μια σταθερή αξία στο χώρο της κυβερνοασφάλειας, αφού έχει αποδείξει την ικανότητα να προσφέρει αποτελεσματικές λύσεις σε προβλήματα που παρουσιάστηκαν στον κυβερνοχώρο.

2.3 Τρόποι ενίσχυσης προστασίας από κυβερνοεπιθέσεις

Όπως αναφέρθηκε και πιο πάνω επικρατεί υποτίμηση προς τους κινδύνους που κρύβονται στο διαδικτυακό κόσμο. Ωστόσο, παρατηρούμε πως παρόλο που αρκετοί αντιλαμβάνονται το ζήτημα αυτό δεν υιοθετούν τα κατάλληλα μέτρα προστασίας (Jacob Wirth, Christian Maier, Sven Laumer & Tim Weitzel, 2019). Επιβάλλεται η ευαισθητοποίηση σε θέματα ασφαλείας και απορρήτου να ενισχυθεί, για να αποφευχθούν πιθανές μελλοντικές ζημιές. Έτσι, το φαινόμενο του privacy paradox θα αντιμετωπιστεί σε κάποιο βαθμό, θα αυξηθεί η υπευθυνότητα των πολιτών και θα ληφθούν δραστικά μέτρα για απόκρουση οποιασδήποτε διαδικτυακής απειλής εμφανιστεί.

Για την υιοθέτηση μιας κουλτούρας η οποία θα βασίζεται σε αρχές που θα διασφαλίζουν την ιδιωτικότητα των ατόμων και την προστασία των προσωπικών τους δεδομένων, θα πρέπει να δοθεί ιδιαίτερη σημασία στα πιο κάτω:

2.3.1 Passwords

Η προστασία των προσωπικών δεδομένων ξεκινά από την εφαρμογή ισχυρών κωδικών πρόσβασης. Μεγάλη έμφαση θα πρέπει να δοθεί στη συνεχή ενημέρωση των ατόμων για τη σημαντικότητα των κωδικών πρόσβασης. Ας μη ξεχνάμε πως οι κωδικοί μας θεωρούνται ως ένα μέσο επαλήθευσης της ταυτότητας που επιτρέπει τη χρήση μιας εφαρμογής ή δικτύου (Joakim Kävrestad, Fredrik Eriksson & Marcus Nohlberg, 2018). Καταλαβαίνουμε λοιπόν, πως η εφαρμογή τους γίνεται ώστε να εμποδίζουν την πρόσβαση σε μη εξουσιοδοτημένα άτομα και την απόκτηση ευαίσθητων πληροφοριών. Βάσει των πιο πάνω, μπορούμε να υποστηρίξουμε την ανάγκη για δημιουργία μιας πολιτικής διαχείρισης κωδικών πρόσβασης που θα εφαρμόζεται από τους πολίτες, για να εκτελούν με ασφάλεια τις καθημερινές τους διαδικτυακές δραστηριότητες.

Αρχικά, οι περισσότεροι ειδικοί προτείνουν πως για να είναι ισχυρός ένας κωδικός, είναι καλό να αποτελείται από τουλάχιστον 10-12 χαρακτήρες. Αυτό ενισχύει τη δυσκολία παραβίασής τους, αφού όσοι περισσότεροι χαρακτήρες χρησιμοποιούνται, τόσο πιο περίπλοκος γίνεται ένας κωδικός (Pat Langdon, Jonathan Lazar, Ann Heylighen & Hua Dong, 2018). Όπως αναφέρει και το επιστημονικό περιοδικό Scientific American, ένας κωδικός πρόσβασης που περιέχει 12 χαρακτήρες είναι 62 τρισεκατομμύρια φορές πιο δύσκολο να

παραβιαστεί από ένα κωδικό με 6 χαρακτήρες. Συμπερασματικά, αντιλαμβανόμαστε πόσο σημαντικό είναι το μέγεθος των κωδικών, αφού αυτό καθορίζει την ισχυρότητά τους και μειώνει δραματικά την πιθανότητα παραβίασής τους (Scientific American, 2019).

Ένα άλλο στοιχείο που ενισχύει την πολυπλοκότητα των κωδικών πρόσβασης είναι το περιεχόμενό τους. Είναι απαραίτητο να χρησιμοποιείται ένας συνδυασμός από αριθμούς, σύμβολα, κεφαλαία και μικρά γράμματα. Οι κωδικοί που έχουν αυτή την πολυμορφία, δεδομένα αποτελούν ένα σημαντικό εργαλείο άμυνας. Εντούτοις, εξίσου σημαντικό είναι να αποφεύγεται η χρήση προσωπικών στοιχείων του χρήστη όπως όνομα, επίθετο, ημερομηνία γέννησης ή διεύθυνση. Η εφαρμογή αυτών των πληροφοριών εντός των κωδικών τους καθιστά προβλέψιμους, αφού ένας έμπειρος hacker μπορεί αντιληφθεί και να παραβιάσει εύκολα τέτοιου είδους κωδικών (Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis & Sotiris Ioannidis, 2018).

Επιπρόσθετα, κάθε άτομο δεν πρέπει να περιορίζεται σε ένα μόνο κωδικό, αλλά να διατηρεί μοναδικούς κωδικούς πρόσβασης για κάθε εφαρμογή ή δραστηριότητα που πραγματοποιεί. Οπωσδήποτε, οι χρήστες πρέπει κάθε φορά να πληκτρολογούν τους κωδικούς και να μην τους αποθηκεύουν στη μνήμη των συσκευών τους. Παράλληλα, θα ήταν αφελές να παραλείψουμε και πόσο σημαντική είναι η σωστή αποθήκευση των κωδικών, σε μέρη που δεν θα είναι εύκολη η πρόσβαση από τρίτους. Τέλος, όλοι καλούμαστε να κατανοήσουμε τη σημασία της προστασίας των προσωπικών δεδομένων, γι’ αυτό και δεν πρέπει να μοιραζόμαστε με κανένα τους κωδικούς μας, είτε είναι συγγενείς είτε φίλοι. Έτσι, θα διασφαλιστεί η ιδιωτικότητά και οι ευαίσθητες πληροφορίες θα παραμείνουν άθικτες.

2.3.2 Antivirus

Ακόμη ένας τρόπος με τον οποίο ενισχύεται το privacy awareness στον πληθυσμό είναι η κατανόηση της σημαντικότητας των λογισμικών antivirus. Πολλοί θεωρούν τα antivirus αχρείαστα επειδή δεν αντιλαμβάνονται τα οφέλη που παρέχουν στις συσκευές που είναι εγκατεστημένα. Επομένως, είναι αναγκαία η λεπτομερής ενημέρωση του κοινού για τα πλεονεκτήματα του, ώστε να πειστεί ο καθένας ξεχωριστά για την αναγκαιότητά τους.

Ένα πρόγραμμα antivirus έχει ως στόχο τον εντοπισμό ιών και κακόβουλων λογισμικών τα οποία προκαλούν ζημία στις συσκευές των χρηστών. Οι λειτουργίες του λογισμικού είναι τέτοιες ώστε να εντοπίζει πρόωρα και να αποκρούει τέτοιου είδους κακόβουλες ενέργειες, διασφαλίζοντας την προστασία του συστήματος (Farrokh Mamaghani, 2002).

Ένα από τα σημαντικότερα πλεονεκτήματα του λογισμικού είναι η διαρκής προστασία των συσκευών από ιούς που αναπτύσσονται ή τροποποιούνται με στόχο να μολύνουν τα συστήματα. Ένα από τα πιο ήπια προβλήματα που προκαλεί ένας ιός είναι η δραματική μείωση της ταχύτητα των συσκευών μας (Sidney M. L. Lima, Sthéfano H. M. T. Silva, Washington W. A. da Silva & Wellington P. dos Santos, 2022). Ωστόσο, υπάρχουν και είδη ιών που μπορεί να προκαλέσουν σοβαρή ζημιά στις συσκευές, όπως η μόνιμη διαγραφή σημαντικών αρχείων και προγραμμάτων. Αντιλαμβανόμαστε λοιπόν, πως βάσει του ιού που εισέρχεται στις συσκευές μας, οι ζημιές που πραγματοποιούνται διαφέρουν, ενώ σε κάποιες περιπτώσεις μπορεί να είναι και μη αναστρέψιμες.

Επιπλέον, ένα antivirus ενημερώνει διαρκώς το χρήστη για την επικινδυνότητα κάποιων ιστοσελίδων ή διαδικτυακών δραστηριοτήτων ώστε να τις αποφεύγει. Το πλεονέκτημα αυτό είναι εξαιρετικά σημαντικό ιδίως για τους γονείς, καθώς αποτελεί ένα μέτρο ελέγχου για τα μικρά παιδιά ώστε να τους απαγορεύεται η είσοδος σε ιστοσελίδες με ακατάλληλο υλικό (Harshit Gupta, 2022). Συνεπώς, το antivirus μπορεί να αποτελέσει ένα χρήσιμο εργαλείο για τους γονείς, το οποίο θα διασφαλίζει ότι τα παιδιά τους δεν θα χρησιμοποιούν την σκοτεινή πλευρά του διαδικτύου.

Όπως είναι γνωστό, οι hackers επιτίθονται σε συστήματα τα οποία παρουσιάζουν ευπάθειες και δεν έχουν εγκατεστημένο λογισμικό antivirus. Μέσα από ύπουλες τεχνικές εκμεταλλεύονται την αδυναμία των συστημάτων και επιτυγχάνουν πρόσβαση σε συσκευές

ανυποψίαστων ατόμων, με αποτέλεσμα την υποκλοπή των προσωπικών τους δεδομένων. Έτσι, τα θύματα μπορεί να χάσουν για πάντα τις προσωπικές τους πληροφορίες και σε κάποιες περιπτώσεις να έχουν οικονομικές απώλειες. Άρα, κρίνεται απαραίτητο κάθε άτομο να μεριμνά ώστε να έχει πάντοτε εγκατεστημένο ένα ισχυρό πρόγραμμα antivirus σε κάθε συσκευή του.

Ταυτόχρονα, ο κόσμος θα πρέπει να σταματήσει να χρησιμοποιεί τις δωρεάν εκδόσεις των λογισμικών antivirus. Οι συγκεκριμένες εκδόσεις, παρόλο που προσφέρουν κάποια προστασία, παρουσιάζουν αρκετές ευπάθειες που μπορεί να ευνοήσουν πιθανότητες μόλυνσης των συστημάτων. Επομένως, κρίνεται απαραίτητη η εγκατάσταση λογισμικών τα οποία, αν και έχουν οικονομικό αντίτιμο, προσφέρουν επιπρόσθετες ρυθμίσεις που διατηρούν την ασφάλεια των συσκευών μας (Darren Allan, 2020). Μερικές από αυτές είναι η προστασία από άγνωστες απειλές, αποκλεισμός επικίνδυνων ιστοσελίδων, προληπτικά μέτρα ασφαλείας, αλλά και τμήμα υποστήριξης πελατών.

2.3.3 Ενθάρρυνση για ανώνυμη περιήγηση

Ένα ακόμη στοιχείο το οποίο αυξάνει την προστασία της ιδιωτικότητας των ατόμων τους είναι η ενθάρρυνση χρήσης της ανώνυμης περιήγησης. Η ανώνυμη περιήγηση, γνωστή και ως Incognito, παρέχει προστασία σε θέματα απορρήτου, καθώς ο χρήστης μπορεί να εκτελεί τις διαδικτυακές του δραστηριότητες χωρίς να αφήνει πίσω του ίχνη που προδίδουν τα προσωπικά στοιχεία και τις προτιμήσεις του (Rahat Masood, Dinusha Vatsalan & Muhammad Ikram, 2018).

Τα τελευταία χρόνια παρατηρήθηκε ότι επιχειρήσεις και ιστοσελίδες συγκεντρώνουν ευαίσθητες πληροφορίες και δεδομένα των χρηστών που τις επισκέπτονται. Η συλλογή των δεδομένων γίνεται με στόχο να δημιουργηθεί ένα προφίλ για τον καθένα ξεχωριστά, βάσει των προτιμήσεων και των συνηθειών του. Έτσι, τοποθετούνται στοχευμένες διαφημίσεις στις συσκευές των ατόμων ανάλογα με τα στοιχεία που έχουν συλλέξει, ώστε να προβάλουν τα προϊόντα και τις υπηρεσίες τους. Αντιλαμβανόμαστε λοιπόν, πως τα ψηφιακά ίχνη που αφήνει κάθε άτομο από τις περιηγήσεις τους ωφελεί τους hackers, αφού έχουν τη δυνατότητα να αντλήσουν σημαντικά στοιχεία για τα πιθανά τους θύματα και να

τα εξαπατήσουν (Joaquin Garcia-Alfaro, Georgios Lioudakis, Nora Cuppens-Boulahia, Simon Foley & William M. Fitzgerald, 2013).

Ιστότοποι που δίνουν τη δυνατότητα χρήσης ανώνυμης περιήγησης είναι το Internet Explorer, Chrome και Firefox (Nor Azizah Yacob, Nur Asmaliza Mohd Noor, Nor Yuziah Mohd Yunus, Rahmanh Lob Yussof & Shaik Adbul Zakaria, 2016). Το μεγαλύτερο πλεονέκτημα που παρέχει η ανώνυμη περιήγηση είναι ότι δεν αποθηκεύονται προσωπικά στοιχεία όπως όνομα, διεύθυνση, κωδικοί πρόσβασης και τραπεζικοί λογαριασμοί. Επίσης, δεν αποθηκεύεται ούτε το ιστορικό περιήγησης κάνοντας ουσιαστικά τους χρήστες αόρατους. Όλα αυτά, βοηθούν σε μεγάλο βαθμό να μειωθεί δραματικά η πιθανότητα εκδήλωσης κάποιας απάτης και να πραγματοποιούνται με ασφάλεια διαδικτυακές αγορές.

Ωστόσο, η ανώνυμη περιήγηση δεν εξασφαλίζει από μόνη της την ασφάλεια των χρηστών στο διαδίκτυο. Για να είναι αποτελεσματική και ωφέλιμη η χρήση του, επιβάλλεται να συνοδεύεται πάντα με το κατάλληλο λογισμικό antivirus που θα λειτουργεί σαν ασπίδα προστασίας από τυχόν κακόβουλες επιθέσεις. Ακόμη, καλό θα ήταν να χρησιμοποιείται και το εικονικό ιδιωτικό δίκτυο VPN το οποίο αποκρύπτει την ηλεκτρονική διεύθυνση IP του ατόμου προστατεύοντας τα προσωπικά του δεδομένα και την τοποθεσία του.

Καταληκτικά, η ενημέρωση περί ανώνυμης περιήγησης στο κοινό θα οδηγήσει στην ενίσχυση της ασφάλειας των πολιτών, γι' αυτό και οι αρμόδιοι πρέπει να αναλάβουν δράση, ώστε να προωθηθεί και να υιοθετηθεί από όλους.

2.3.4 Social Media

Κανείς δεν μπορεί να αμφισβητήσει το γεγονός πως τα social media αποτελούν πλέον ένα αναπόσπαστο μέρος της ζωής μας. Όλο και περισσότερα άτομα από όλες τις ηλικιακές ομάδες, χρησιμοποιούν έστω και μια πλατφόρμα των social media. Αυτό συμβαίνει λόγω της ανάγκης που έχουν οι άνθρωποι να επικοινωνούν και να ψυχαγωγούνται μέσω της αλληλεπίδρασης τους με άλλα άτομα, γεγονός που έχει καταστήσει τα social media σημαντικό κομμάτι στην καθημερινότητά τους. Αυτό αποδεικνύεται και μέσα από έρευνα της Statista, η οποία αναφέρει ότι ο μέσος άνθρωπος παγκόσμια ξοδεύει ημερησίως περίπου 147 λεπτά στα social media. Επομένως, καταλαβαίνουμε πως ο χρόνος που

αφιερώνεται σε αυτές τις πλατφόρμες είναι αρκετά μεγάλος, άρα πρέπει να υπάρξει και η κατάλληλη πληροφόρηση για σωστή χρήση τους.

Αδιαμφισβήτητα, η ενημέρωση περί σωστής διαχείρισης των μέσων κοινωνικής δικτύωσης θα ενισχύσει την ευαισθητοποίηση των χρηστών σε θέματα απορρήτου (Clare Stouffer, 2021). Πρέπει να γίνει σε όλους κατανοητό ότι η διασφάλιση της ιδιωτικότητας αποτελεί επιτακτική ανάγκη για κάθε άτομο. Ένα από τα μεγαλύτερα λάθη που γίνονται είναι ότι οι χρήστες δημοσιεύουν πληροφορίες όπως ο τόπος διαμονής, email, επάγγελμα κ.α. στα προφίλ τους. Ταυτόχρονα, όχι μόνο μοιράζονται προσωπικές τους πληροφορίες, αλλά διατηρούν και δημόσια προφίλ, στα οποία ο καθένας έχει πρόσβαση και παρακολουθεί τον λογαριασμό τους. Για προστασία λοιπόν της ιδιωτικότητας, τα άτομα θα πρέπει να σταματήσουν να μοιράζονται σε πλατφόρμες όπως το Facebook, Instagram, Twitter και Tik Tok προσωπικές τους πληροφορίες.

Η μη ορθή χρήση των social media και η απερίσκεπτη προβολή προσωπικών πληροφοριών, αποτελούν πρόσφορο έδαφος για τους κυβερνοεγκληματίες, καθώς έχουν τη δυνατότητα να συλλέξουν τα δεδομένα που χρειάζονται και να φέρουν στην κατοχή τους λογαριασμούς των χρηστών. Αυτός θεωρείται ένας σημαντικός λόγος για τους πολίτες να διατηρούν ιδιωτικούς λογαριασμούς και να μοιράζονται πληροφορίες και υλικό το οποίο δεν θα αποκαλύπτει την ταυτότητα τους (Clare Stouffer, 2021). Σε καμία περίπτωση δεν πρέπει να δίνουν την ευκαιρία σε άγνωστα άτομα να έχουν πρόσβαση στα προφίλ που έχουν στα social media, αφού οι κίνδυνοι που κρύβονται είναι πάρα πολλοί.

Με βάση τα πιο πάνω κατανοούμε πως πρέπει να διασφαλιστεί κατάλληλη επιμόρφωση του κοινού για σωστή χρήση των μέσω κοινωνικής δικτύωσης. Τα μέσα αυτά αποτελούν ένα σημαντικό εργαλείο για τη σύγχρονη κοινωνία, αφού η επίδρασή τους είναι τεράστια παγκόσμια. Ως εκ τούτου, θα πρέπει να γίνουν οι κατάλληλες ενέργειες ώστε με τη χρήση τους να διασφαλιστεί το κοινό καλό και να προστατευτεί η ιδιωτικότητα των ατόμων.

2.3.5 Σχολείο, πολιτεία, επαγγελματικό περιβάλλον

Εξίσου σημαντικό μερίδιο ευθύνης στην ευαισθητοποίηση των πολιτών για θέματα απορρήτου και ασφάλειας στο διαδίκτυο κατέχουν η πολιτεία, τα εκπαιδευτικά ιδρύματα και το επαγγελματικό περιβάλλον. Οι φορείς αυτοί οφείλουν να αποτελέσουν οδηγό για τον πληθυσμό και πηγή γνώσεων, μεταφέροντας του όλα όσα πρέπει να γνωρίζει για την προστασία της ιδιωτικότητάς του.

Καίριο ρόλο στην καλλιέργεια των ατόμων για υπεύθυνη χρήση του διαδικτύου αποτελούν τα σχολεία. Το διαδίκτυο αποτελεί μια από τις μεγαλύτερες τάσεις και προκλήσεις της σύγχρονης εποχής, γι' αυτό και τα εκπαιδευτικά ιδρύματα όλων των βαθμίδων πρέπει να δώσουν μεγαλύτερη έμφαση στην εκμάθηση των μαθητών για τους κινδύνους του διαδικτύου, αλλά και για τρόπους προστασίας στον ψηφιακό κόσμο. Τα σχολεία θα ήταν καλό να εντάξουν στο εκπαιδευτικό τους πρόγραμμα μαθήματα που αφορούν στο διαδίκτυο και την ιδιωτικότητα, ώστε να τους μεταφέρουν από μικρή ηλικία τους κινδύνους που εμπεριέχει και τους τρόπους προστασίας από αυτούς. Έτσι, τα άτομα θα αφομοιώσουν τις γνώσεις αυτές από μικρή ηλικία και θα αποκτήσουν τα απαραίτητα εφόδια, ώστε να είναι ικανοί να αντιμετωπίσουν τυχών διαδικτυακούς κινδύνους.

Από την πλευρά της η πολιτεία θα πρέπει να ωθήσει όλες τις ηλικιακές ομάδες να υιοθετήσουν μια κουλτούρα βασισμένη στην προστασία της ιδιωτικότητας. Για να γίνει αυτό όμως, η πολιτεία οφείλει να ενημερώνει σε βάθος τους πολίτες της για αυτά τα θέματα. Ένας τρόπος που δύναται να το πράξει αυτό είναι μέσω εκδηλώσεων για θέματα ιδιωτικότητας και κινδύνων στον ψηφιακό κόσμο από εξειδικευμένο ανθρώπινο δυναμικό. Μέσα από διαδραστικές παρουσιάσεις οι πολίτες θα λαμβάνουν χρήσιμες πληροφορίες σχετικά με το απόρρητο και άλλα θέματα ασφαλείας που χρήζουν σημασίας. Ωστόσο, για να είναι επιτυχημένη μια τέτοια εκδήλωση, η πολιτεία θα πρέπει να βρει τρόπο να προσελκύσει κόσμο να παρευρεθεί σε αυτές. Ταυτόχρονα, η ευαισθητοποίηση των πολιτών μπορεί να ενισχυθεί μέσα από διαφημίσεις στα μέσα μαζικής ενημέρωσης και σε μεγάλες ταμπέλες στο δρόμο. Οι διαφημίσεις πρέπει να είναι δομημένες με τέτοιο τρόπο, ώστε να μεταφέρουν δυνατά μνήματα που θα τονίζουν τη σημασία της ιδιωτικότητας στους τηλεθεατές. Οι περισσότερες διαφημίσεις όμως, θα πρέπει να προβάλλονται στο

διαδίκτυο, καθώς αποτελεί ένα μέσο στο οποίο η πλειοψηφία του κόσμου αφιερώνει σημαντικό χρόνο της καθημερινότητάς του.

Τέλος, το επαγγελματικό περιβάλλον του καθενός επιβάλλεται να συμβάλει στη δημιουργία συνειδητοποιημένων εργαζομένων όσον αφορά την προστασία των προσωπικών τους πληροφοριών. Απαραίτητη προϋπόθεση γι' αυτό είναι η δημιουργία μιας κουλτούρας που θα βασίζεται στην ιδιωτικότητα. Οι ηγέτες και τα υψηλόβαθμα στελέχη μέσα από κανόνες και πολιτικές οφείλουν να ευθυγραμμίσουν το απόρρητο με τους επιχειρηματικούς τους στόχους και αξίες. Αρχικά, κάθε επιχείρηση οφείλει να διαθέτει έμπειρο προσωπικό που ειδικεύεται σε θέματα ασφαλείας, ώστε να μπορούν να μεταλαμπαδεύσουν τις γνώσεις στους υπόλοιπους υπαλλήλους. Επίσης, κρίνεται απολύτως απαραίτητο οι εταιρείες να διοργανώνουν τακτικά trainings, μέσα από τα οποία οι υπάλληλοι θα αποκτούν ολοκληρωμένη πληροφόρηση. Ωστόσο, για να διασφαλιστεί η επιτυχής μεταφορά και πλήρης αφομοίωση των γνώσεων θα πρέπει να διοργανώνονται γραπτές ή και προφορικές εξετάσεις για να βεβαιωθεί ο οργανισμός ότι οι υπάλληλοι παρακολούθησαν με σοβαρότητα τα trainings. Επιπρόσθετα, το προσωπικό των επιχειρήσεων οφείλει ανά τακτά χρονικά διαστήματα να παρευρίσκεται σε σεμινάρια περί ιδιωτικότητας και ασφαλείας που πραγματοποιούνται από πιστοποιημένα άτομα. Ζώντας σε ένα συνεχώς μεταβαλλόμενο κόσμο η μάθηση και η ανανέωση της γνώσης δεν πρέπει να σταματά ποτέ. Επομένως, η παρακολούθηση τέτοιων σεμιναρίων θα παρέχει την ευκαιρία για επιπρόσθετες γνώσεις ή ανανέωσή των υπάρχοντων όσον αφορά το θέμα αυτό.

Συνοψίζοντας τα πιο πάνω, γίνεται κατανοητή η αδήριτη ανάγκη για εφαρμογή κατάλληλων μέτρων προστασίας έναντι των ηλεκτρονικών επιθέσεων. Η έγκαιρη εφαρμογή τους θα λειτουργήσει προς όφελος των χρηστών του διαδικτύου, καθώς θα έχουν μια επιπλέον ασπίδα ασφαλείας. Όλα τα μέτρα προστασίας στα οποία έγινε αναφορά νωρίτερα θεωρούνται άκρως αποτελεσματικά, γι' αυτό και επιβάλλεται όλοι μας να τα υιοθετήσουμε. Τέλος, εξίσου σημαντική είναι η συνεχής ενημέρωση των ατόμων για τους κινδύνους του διαδικτύου, ούτως ώστε να γνωρίζουν τις νέες απειλές που εμφανίζονται και να ανανεώνουν τα μέτρα προστασίας τους για να είναι ακόμη πιο ασφαλείς.

Κεφάλαιο 3

3. Διεξαγωγή Έρευνας

3.1 Privacy awareness και Privacy paradox

Όπως προαναφέρθηκε, παρατηρείται ραγδαία αύξηση στις κυβερνοεπιθέσεις τα τελευταία χρόνια με όλο και περισσότερα άτομα να πέφτουν θύματα ηλεκτρονικών απατών. Έχοντας λοιπόν υπόψη την σημασία της κυβερνοασφάλειας και την ανάγκη για προστασία από τέτοιες επιθέσεις, πραγματοποιήθηκε έρευνα η οποία εξετάζει κατά πόσο είναι ενήμερος ο πληθυσμός για θέματα που αφορούν το privacy awareness.

Μελετήθηκαν οι συνήθειες και η δράση των ατόμων στο διαδικτυακό χώρο, ώστε να αντιληφθούμε κατά πόσο είναι ευαισθητοποιημένοι σε θέματα ασφάλειας και εάν λαμβάνουν κατάλληλα μέτρα για προστασία της ιδιωτικότητάς τους. Εξετάστηκε επίσης, κατά πόσο υπάρχει και το φαινόμενο παραδόξου του απορρήτου, δηλαδή πιθανή ασυμφωνία μεταξύ των ανησυχιών των χρηστών και της πραγματικής τους συμπεριφοράς στο ψηφιακό κόσμο.

Privacy awareness

Η ευαισθητοποίηση των πολιτών σε θέματα ιδιωτικότητας και ασφάλειας δεδομένων αποτελεί ένα σημαντικό κομμάτι που εξετάζεται όλο και περισσότερο από την πολιτεία και την επιστημονική κοινότητα (Michele Bezzi, Penny Duquenoy, Marit Hansen & Ge Zhang, 2009). Τα τελευταία 10 χρόνια εντείνονται όλο και περισσότερο οι έρευνες γύρω από το privacy awareness, αφού τόσο η δραματική αύξηση του ηλεκτρονικού εγκλήματος όσο και η ανάγκη για ασφαλή περιήγηση στο διαδίκτυο, ωθούν τους ειδικούς να μελετούν σε βάθος το θέμα αυτό. Αρκετοί είναι οι ορισμοί που έχουν αποδοθεί για το τι σημαίνει privacy awareness. Ένας από αυτούς το παρουσιάζει ως την ικανότητα του ατόμου να μπορεί να αντιλαμβάνεται με ακρίβεια πιθανές απειλές που δύναται να προκαλέσουν ζημιά στην ιδιωτική του ζωή και τα προσωπικά του δεδομένα (Konings, 2013). Ταυτόχρονα,

ορίζεται και ως ο μηχανισμός μέσα από τον οποίο τα άτομα είναι ικανά να ανιχνεύσουν πιθανούς κινδύνους που υφίστανται στο ψηφιακό κόσμο, έχοντας ωστόσο και τις εφαρμόσιμες προστατευτικές λύσεις για αντιμετώπισή τους (Rena Lavranou & Aggeliki Tsohou, 2019).

Privacy paradox

Η ευαισθητοποίηση σε θέματα απορρήτου και προστασίας δεδομένων οδηγεί τους ανθρώπους στο να είναι προδραστικοί, λαμβάνοντας λογικές αποφάσεις που διασφαλίζουν την ιδιωτικώτητά τους. Μεγάλη μερίδα του πληθυσμού αντιλαμβάνεται ότι οι πληροφορίες και τα δεδομένα αποτελούν πόλο έλξης για τους κυβερνοεγκληματίες, γι' αυτό και λαμβάνουν μέτρα ώστε να αποκρούσουν τυχόν επιθέσεις. Ωστόσο μελέτες και έρευνες έχουν παρατηρήσει ένα φαινόμενο το οποίο χαρακτηρίζεται αντιφατικό, γνωστό ως το Privacy paradox. Συγκεκριμένα, το φαινόμενο αυτό ορίζεται ως η ασυμφωνία που υφίσταται ανάμεσα στις ανησυχίες των χρηστών και της πραγματικής τους συμπεριφοράς (Vashek Matyas, Simone Fischer-Hubner, Daniel Cvrcek & Petr Svenda, 2008). Πολλά είναι τα άτομα που γνωρίζουν τους κινδύνους του διαδικτύου και τις ζημίες που μπορεί να προκαλέσει μια ηλεκτρονική επίθεση. Εντούτοις, παρά τις ανησυχίες αυτές, παρατηρείται χαλαρότητα και αδράνεια στην ηλεκτρονική τους συμπεριφορά, εξακολουθώντας να είναι απρόσεκτοι και να μην λαμβάνουν τα απαραίτητα μέτρα ασφαλείας (Spyros Kokolakis, 2015).

3.2 Περιγραφή Έρευνας

3.2.1 Μεθοδολογία έρευνας και δειγματοληψία

Στα πλαίσια της μεταπτυχιακής διατριβής πραγματοποιήθηκε έρευνα μέσω ενός σύντομου ερωτηματολογίου το οποίο περιείχε ερωτήσεις περί προστασίας δεδομένων και ιδιωτικότητας των πολιτών. Όπως γνωρίζουμε, το ερωτηματολόγιο αποτελεί ένα από τα πιο διαδεδομένα ερευνητικά εργαλεία, μέσα από το οποίο μπορούμε να αντλήσουμε χρήσιμες πληροφορίες και να εξάγουμε συμπεράσματα. Η μέθοδος αυτή είναι αρκετά απλή και αποτελεσματική, αφού επιτυγχάνει τόσο εξοικονόμηση χρήματος όσο και χρόνου.

Το ερωτηματολόγιο δόθηκε προσωπικά σε κάθε συμμετέχοντα, ώστε να απαντηθεί με πλήρη σοβαρότητα και ειλικρίνεια. Για τη λήψη πληροφοριών και την εξαγωγή ορθών συμπερασμάτων επιλέχθηκε ένα υποσύνολο 150 ατόμων, ώστε να εκτιμηθούν χαρακτηριστικά που αφορούν όλο τον πληθυσμό. Όλοι οι συμμετέχοντες του ερωτηματολογίου ήταν πολίτες της Κυπριακής Δημοκρατίας ηλικίας 12 - 65 ετών. Απαραίτητη προϋπόθεση για συμμέτοχη στην έρευνα ήταν η καθημερινή χρήση του διαδικτύου για διάφορους σκοπούς. Τέλος, επιλέχθηκαν άτομα από διάφορες επαρχίες της Κύπρου, ώστε η έρευνα να γίνει πιο αξιόπιστη.

3.2.2 Δομή

Το ερωτηματολόγιο συντάχτηκε ηλεκτρονικά, ωστόσο δόθηκε στους συμμετέχοντες σε έντυπη μορφή. Περιλαμβάνει 20 ερωτήσεις κλειστού τύπου για καλύτερη οργάνωση και επεξεργασία των δεδομένων. Δόθηκε μεγάλη έμφαση στην έκτασή του ώστε να μην είναι κουραστικό για τον αναγνώστη και να αποφευχθούν τυχόν βιαστικές ή τυχαίες απαντήσεις . Ο εκτιμώμενος χρόνος για την συμπλήρωση του ερωτηματολογίου είναι περίπου 5 - 7 λεπτά.

Όσο αφορά το λεξιλόγιο, χρησιμοποιήθηκαν πολύ απλές λέξεις και αποφεύχθηκαν περίπλοκες έννοιες που μπορεί να προκαλούσαν σύγχυση και να επηρεάσουν τις απαντήσεις των συμμετεχόντων. Ταυτόχρονα, δεν έγινε χρήση διφορούμενών ή αρνητικών

ερωτήσεων, καθώς σύμφωνα με μελέτες προκαλούν μπέρδεμα στο κοινό, αλλοιώνοντας πολλές φορές τα αποτελέσματα της έρευνας.

Πριν την ολοκλήρωση της τελικής μορφής του ερωτηματολογίου πραγματοποιήθηκαν όλες οι απαραίτητες ενέργειες για σωστό σχεδιασμό και έλεγχο. Αρχικά, δημιουργήθηκε ένα πρόχειρο ερωτηματολόγιο που δοκιμάστηκε τόσο από ένα μικρό δείγμα ερωτώμενων όσο και από εμένα τον ίδιο, σε μια προσπάθεια να εντοπιστούν αδυναμίες και να πραγματοποιηθούν οι απαραίτητες βελτιώσεις. Έτσι, οι ερωτήσεις τοποθετήθηκαν σε σωστή σειρά, με στόχο να υπάρχει συνεχόμενη ροή και η συμπλήρωσή του να είναι μια ευχάριστη εμπειρία για τους συμμετέχοντες.

3.2.3 Μέρη ερωτηματολογίου

Το πρώτο μέρος του ερωτηματολογίου περιλαμβάνει 3 ερωτήσεις δημογραφικού χαρακτήρα, οι οποίες αφορούσαν το φύλο, την ηλικία και το μορφωτικό επίπεδο των ατόμων. Στόχος τους είναι η άντληση δεδομένων για να κατανοήσουμε πως συμπεριφέρεται η κάθε ομάδα του πληθυσμού σε διάφορες καταστάσεις που αφορούν το διαδίκτυο.

Στο δεύτερο μέρος συμπεριλαμβάνονται ερωτήσεις που επικεντρώνονται στις συνήθειες του πληθυσμού, εξετάζοντας εάν λαμβάνουν κατάλληλα μέτρα προστασίας για τους κινδύνους που κρύβει το διαδίκτυο. Οι ερωτήσεις είναι βαθμονομημένες σε αύξουσα σειρά με βάση την συχνότητα, και οι επιλογές αποτελούνται από: «Ποτέ», «Σπάνια», «Μερικές φορές», «Συχνά» και «Πάντα». Οι απαντήσεις των συμμετεχόντων θα φανερώνουν κατά πόσο τα άτομα είναι ευαισθητοποιημένα σε θέματα ιδιωτικότητας και ασφάλειας των προσωπικών τους δεδομένων. Πιο συγκεκριμένα οι ερωτήσεις αφορούν τη δομή και τη διαχείριση των κωδικών πρόσβασης των χρηστών, καθώς και τη λήψη ή άνοιγμα συνδέσμων URL. Επίσης, υπάρχουν ερωτήσεις σχετικά με το λογισμικό antivirus και τη δράση διάφορων φορέων σχετικά με θέματα ιδιωτικότητας.

Το τρίτο μέρος αποτελείται από ερωτήσεις που εξετάζουν κατά πόσο υπάρχει το φαινόμενο παραδόξου του απορρήτου. Η συμπλήρωση τους θα υποδείξει κατά πόσο οι συμπεριφορές των πολιτών στο ψηφιακό κόσμο είναι ανάλογες με τις ανησυχίες τους για τους κινδύνους που κρύβονται στο διαδίκτυο. Οι ερωτήσεις είναι διαμορφωμένες με βάση

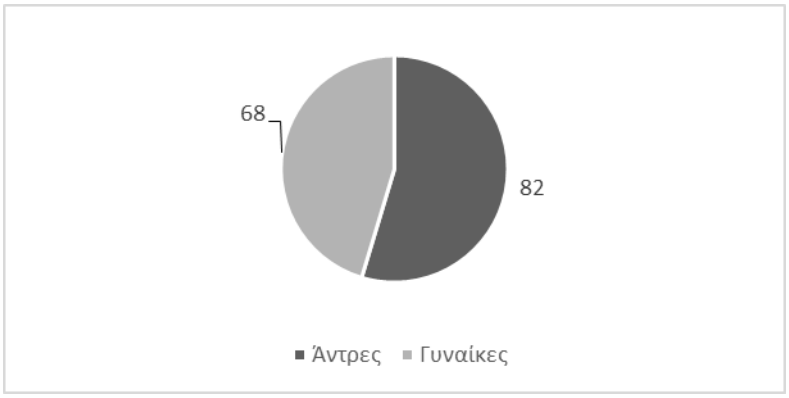
την κλίμακα Likert και αφορούν το βαθμό πιθανότητας εκδήλωσης κάποιων καταστάσεων. Η βαθμονόμηση περιλαμβάνει τις επιλογές: «Καθόλου», «Μικρό βαθμό», «Μέτριο βαθμό», «Μεγάλο βαθμό», «Πολύ μεγάλο βαθμό».

3.3 Ανάλυση δεδομένων

Μέρος Α: Δημογραφικά στοιχεία

- Διάγραμμα 1:

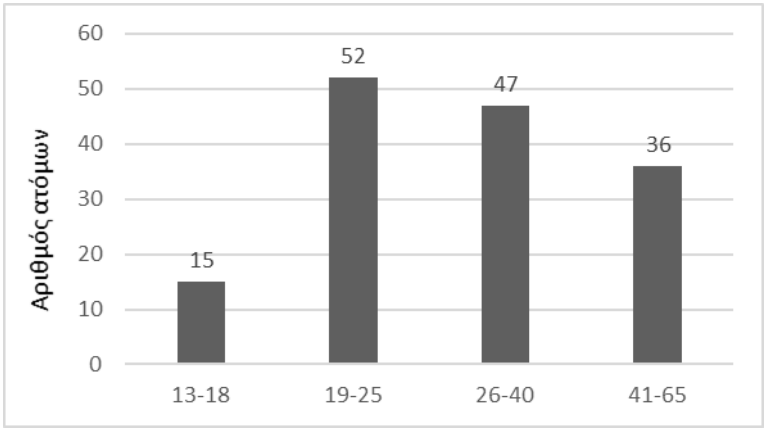
Φύλο



Όπως προαναφέρθηκε, στην έρευνα έλαβαν μέρος 150 άτομα από όλη την Κύπρο, ανάμεσά τους 82 άνδρες και 68 γυναίκες. Έγινε προσπάθεια να μην υπάρχει μεγάλη διαφορά στον αριθμό μεταξύ ανδρών και γυναικών που συμμετείχαν, ώστε να διασφαλιστεί μεγαλύτερη αξιοπιστία. Είναι γνωστό ότι τα δύο φύλα συμπεριφέρονται με διαφορετικό τρόπο σε αρκετές καταστάσεις. Επομένως, μια μεγάλη διαφορά στον αριθμό των ατόμων ανά φύλο θα μπορούσε να επηρεάσει τα αποτελέσματα.

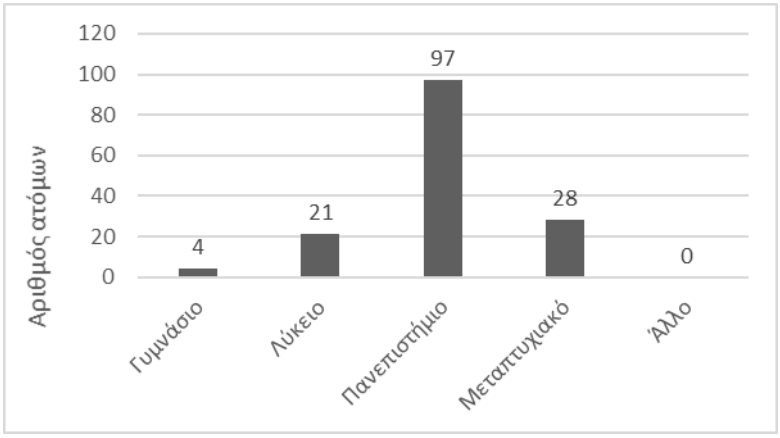
- Διάγραμμα 2:

Ηλικία



Το πιο πάνω διάγραμμα απεικονίζει τις ηλικίες των ατόμων που έλαβαν μέρος στο ερωτηματολόγιο. Το δείγμα αποτελείτο από άτομα διάφορων ηλικιακών ομάδων, με στόχο να εντοπιστούν τυχών διαφορές στη συμπεριφορά της καθεμιάς. Οι περισσότεροι συμμετέχοντες ήταν ηλικίας 19-25 ετών (52 άτομα), ωστόσο αρκετοί ήταν και οι αυτοί ηλικίας 26-40 ετών (47 άτομα). Η μειοψηφία του δείγματος ήταν τα άτομα ηλικίας 13-18 ετών (15 άτομα).

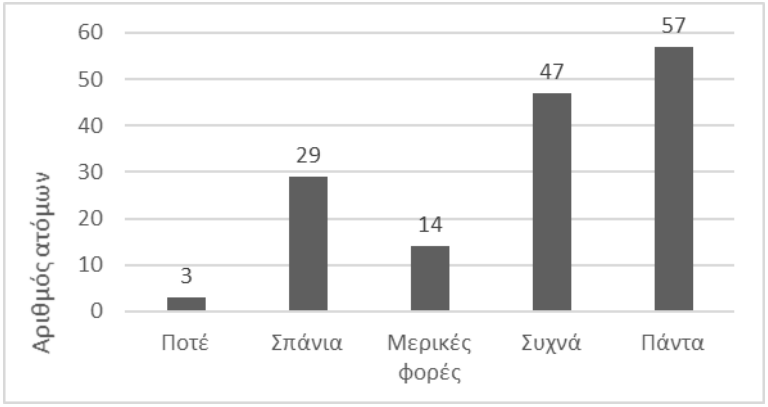
- <u>Διάγραμμα 3: Μορφωτικό επίπεδο</u>



Το μορφωτικό επίπεδο των συμμετεχόντων φαίνεται να βρίσκεται σε ψηλό επίπεδο, αφού η συντριπτική πλειοψηφία κατέχει πανεπιστημιακό δίπλωμα (97 άτομα). Επίσης, 28 άτομα κατέχουν μεταπτυχιακό δίπλωμα, ενώ 25 άτομα βρίσκονται ακόμη στη μέση εκπαίδευση, με τους 21 από τους ερωτώμενους να είναι στο λύκειο και μόλις 4 να είναι στο γυμνάσιο.

Μέρος Β: Κωδικοί πρόσβασης / συνθηματικά (passwords)

- Διάγραμμα 4: Αποθηκεύετε τους κωδικούς πρόσβασης σας στις συσκευές που

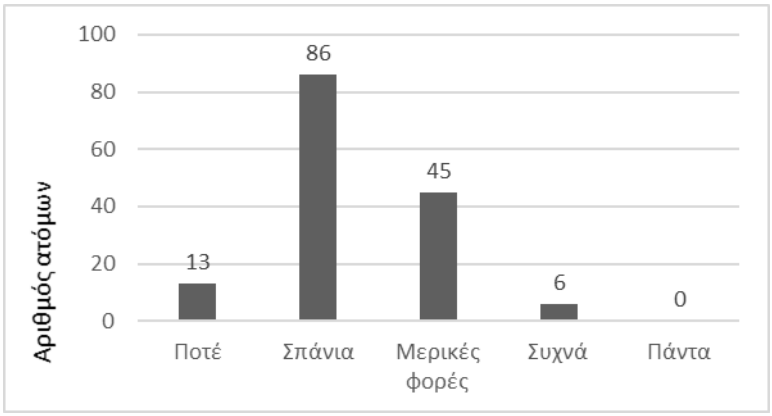


χρησιμοποιείτε;

Από το σύνολο των συμμετεχόντων τα 104 άτομα αποθηκεύουν συχνά ή πάντα τους κωδικούς πρόσβασης τους στη μνήμη των συσκευών τους. Αυτό ίσως συμβαίνει για να αποφύγουν το ενδεχόμενο να ξεχάσουν τους κωδικούς τους και για να εξοικονομούν χρόνο κάθε φορά που επιθυμούν να αποκτήσουν πρόσβαση στους λογαριασμούς τους. Επίσης, 43 άτομα απάντησαν πως μερικές φορές ή σπάνια επιλέγουν να αποθηκεύουν τους κωδικούς πρόσβασης τους στη μνήμη των συσκευών τους. Τα συγκεκριμένα άτομα, φαίνεται να επιλέγουν την πληκτρολόγηση μόνο για κωδικούς πρόσβασης υψηλής σημαντικότητας που περιλαμβάνουν ευαίσθητες πληροφορίες των ιδίων. Τέλος, μόνο 3

άτομα δεν αποθηκεύουν ποτέ τους κωδικούς πρόσβασης τους, πληκτρολογώντας τους κάθε φορά για μεγαλύτερη ασφάλεια.

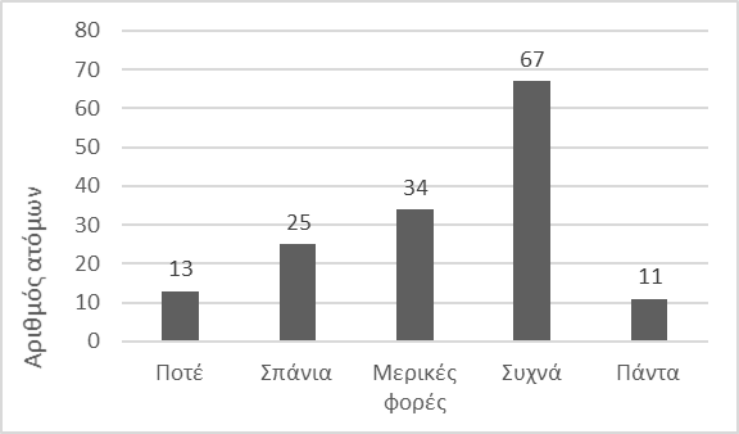
- Διάγραμμα 5: Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για τις ιστοσελίδες και τις διάφορες εφαρμογές με τις οποίες αλληλεπιδράτε;



Στο πιο πάνω διάγραμμα βλέπουμε ότι 86 άτομα σπάνια χρησιμοποιούν διαφορετικούς κωδικούς για τις διαδικτυακές δραστηριότητες, ενώ ένα επίσης μεγάλο μέρος του δείγματος αναφέρει ότι χρησιμοποιεί μερικές φορές διαφορετικούς κωδικούς. Οι συνήθειες των 2 αυτών κατηγοριών είναι άκρως ανησυχητικές, αφού φαίνεται να μην

αντιλαμβάνονται τη σημαντικότητα της διατήρησης διαφορετικών κωδικών πρόσβασης για κάθε ηλεκτρονική υποχρέωση. Μόλις 6 άτομα χρησιμοποιούν συχνά διαφορετικούς κωδικούς πρόσβασης ως μια προσπάθεια ενίσχυσης της προστασίας των προσωπικών τους δεδομένων. Αντίθετα 13 άτομα υποστηρίζουν ότι έχουν ένα μοναδικό κωδικό πρόσβασης με τον οποίο εκτελούν όλες τις καθημερινές τους λειτουργίες. Αυτή η συνήθεια εμπεριέχει τεράστιο ρίσκο, αφού αν ένας κυβερνοεγκληματίας καταφέρει να υποκλέψει τον κωδικό τους, τότε θα μπορεί να αποκτήσει πρόσβαση σε όλους τους λογαριασμούς που διατηρούν.

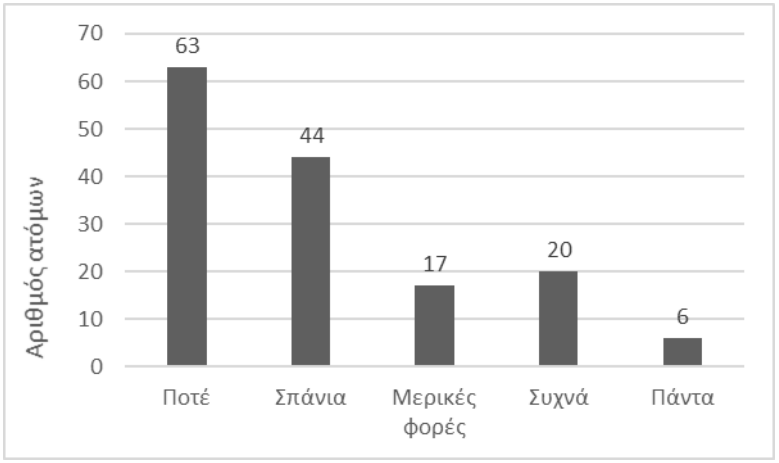
- <u>Διάγραμμα 6: Χρησιμοποιείτε κωδικούς πρόσβασης που σχετίζονται με προσωπικά σας στοιχεία;</u>



Το πιο πάνω διάγραμμα καταδεικνύει πως 67 από τα 150 άτομα που ερωτήθηκαν χρησιμοποιούν συχνά προσωπικά τους στοιχεία εντός των κωδικών πρόσβασης τους, αριθμός που είναι αρκετά μεγάλος και προβληματίζει. Ωστόσο, υπάρχουν και 11 άτομα τα οποία δήλωσαν πως οι κωδικοί πρόσβασής τους περιλαμβάνουν πάντοτε στοιχεία όπως

όνομα, ημερομηνία γέννησης, διεύθυνση κλπ. Αυτό ευνοεί αρκετά έναν hacker, καθώς μπορεί εύκολα να προβλέψει τους κωδικούς και να τους πάρει στην κατοχή του. Επιπλέον, 59 άτομα χρησιμοποιούν μερικές φορές ή σπάνια προσωπικά τους στοιχεία εντός των κωδικών πρόσβασης τους. Τα συγκεκριμένα άτομα επιλέγουν τη συμπερίληψη αυτών των στοιχείων εντός των κωδικών τους ανάλογα με το περιεχόμενο και τη σημαντικότητα των ιστοσελίδων που επισκέπτονται. Τέλος, 13 ερωτηθέντες υποστηρίζουν ότι σε καμία περίπτωση οι κωδικοί πρόσβασης τους δεν περιέχουν στοιχεία που αφορούν την ταυτότητα τους ή άλλα προσωπικά τους στοιχεία. Με τον τρόπο αυτό μειώνουν δραματικά την πιθανότητα να δεχτούν οποιασδήποτε μορφής κακόβουλη επίθεση.

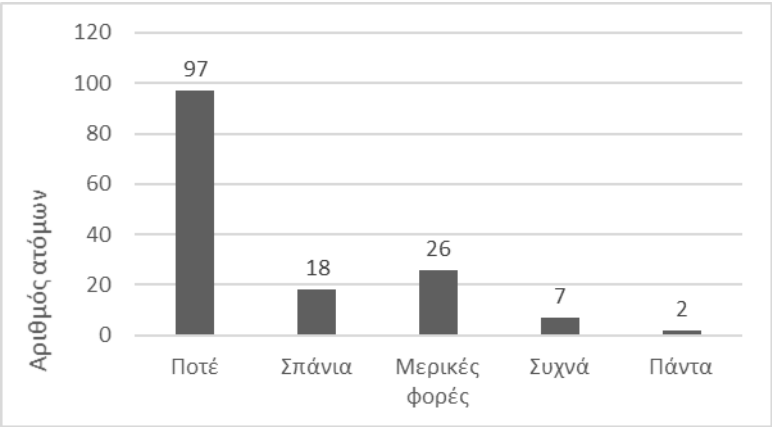
- Διάγραμμα 7: Οι κωδικοί πρόσβασης σας περιέχουν συνδυασμό από αριθμούς, σύμβολα και κεφαλαία γράμματα;



Στην πιο πάνω ερώτηση 63 άτομα απάντησαν πως δεν περιλαμβάνουν ποτέ συνδυασμό συμβόλων, γραμμάτων και αριθμών στους κωδικούς πρόσβασής τους. Κύριος λόγος για την

επιλογή αυτή είναι η πολυπλοκότητα που δημιουργείται στον κωδικό και ο χρόνος πληκτρολόγησης που χρειάζεται με τέτοιους συνδυασμούς. Ταυτόχρονα, κάποιοι θεωρούν και δύσκολη την απομνημόνευσή τους, γι' αυτό και προτιμούν πιο απλούς κωδικούς. Επίσης, 61 άτομα δήλωσαν πως σπάνια ή μερικές φορές χρησιμοποιούν περίπλοκους κωδικούς και πως όταν το πράττουν γίνεται επειδή τους το επιβάλλει μια ιστοσελίδα, η οποία θέτει σαν προϋπόθεση τέτοιους συνδυασμούς για να παρέχει τις υπηρεσίες της. Δεν είναι λίγες οι εταιρείες οι οποίες ενθαρρύνουν τους πολίτες να έχουν ισχυρούς κωδικούς με αποτέλεσμα να τους ''αναγκάζουν'' να τοποθετούν συνδυασμό συμβόλων και αριθμών για να έχουν την απαιτούμενη πρόσβαση. Τέλος, ένας μικρός αριθμός 6 ατόμων φροντίζει να έχει πάντοτε περίπλοκους κωδικούς που δύσκολα παραβιάζονται, αποδεικνύοντας ότι αντιλαμβάνονται τη σημαντικότητα διατήρησης ισχυρών κωδικών.

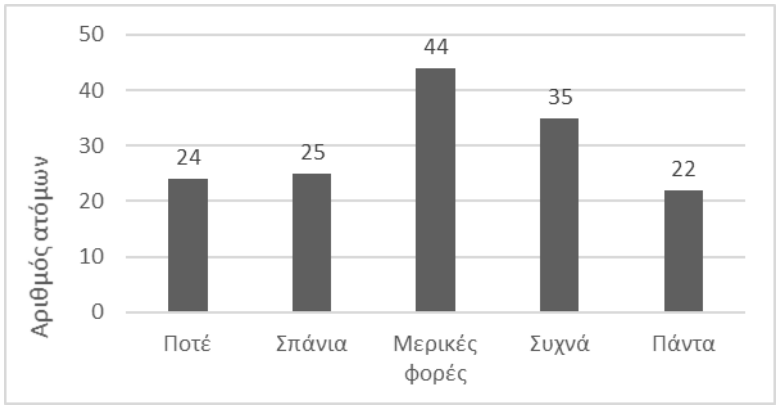
- <u>Διάγραμμα 8: Μοιράζεστε τους κωδικούς πρόσβασης με άλλα άτομα όπως φίλους, συγγενείς και συναδέλφους;</u>



Στην ερώτηση αν οι συμμετέχοντες μοιράζονται τους κωδικούς πρόσβασης τους με άλλα άτομα, η πλειοψηφία (97 άτομα) δεν το κάνει ποτέ, καθώς οι κωδικοί πρόσβασης αποτελούν το κλειδί διατήρησης της ιδιωτικότητάς τους. Αντίστοιχα, 44 άτομα ανέφεραν

πως μοιράζονται τους κωδικούς τους σπάνια ή μερικές φορές, υποθέτοντας πως αυτό συμβαίνει μόνο με στενούς συγγενείς ή φίλους για λογαριασμούς που δε θεωρούν σημαντικούς. Τέλος, 2 άτομα φαίνεται να μην έχουν κανένα πρόβλημα να μοιράζονται πάντα τους κωδικούς τους με άτομα του στενού τους κύκλου, αφού πιθανότατα υπάρχει απόλυτη εμπιστοσύνη μεταξύ τους.

- Διάγραμμα 9: Πόσο συχνά καταγράφετε τους κωδικούς πρόσβασης σε χαρτί ή κάποιο sticky note ή σε αρχείο στον υπολογιστή σας;

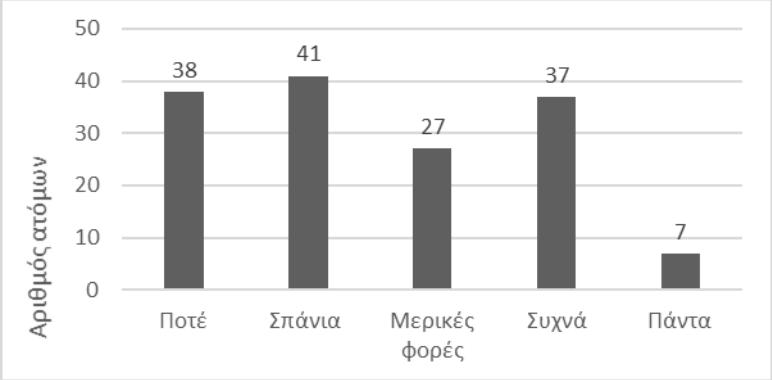


Στην πιο πάνω ερώτηση οι απαντήσεις που δόθηκαν από τους ερωτώμενους ήταν αρκετά ισορροπημένες. Αρχικά, 44 άτομα δήλωσαν ότι μερικές φορές γράφουν τους κωδικούς τους σε χαρτί για να τους θυμούνται, ενώ 35 άτομα ακολουθούν συχνά αυτή την τεχνική. Η

συνήθεια αυτή μπορεί να γίνεται επειδή θεωρούν πως είναι μια εύκολη λύση με την οποία έχουν τη δυνατότητα να ανατρέξουν γρήγορα σε αυτά εάν ξεχάσουν κάποιο κωδικό. Αρνητικό είναι το γεγονός πως 22 άτομα έχουν όλους τους κωδικούς πρόσβασής τους γραμμένους σε κάποιο χαρτί η sticky note, κάτι που εμπεριέχει τεράστιο κίνδυνο, αφού υπάρχει πιθανότητα να περάσουν σε λάθος χέρια. Από την άλλη, 24 άτομα δεν γράφουν ποτέ τους κωδικούς τους σε χαρτί με στόχο να ενισχύσουν την ασφάλεια τους και να αποφύγουν να βρεθούν αντιμέτωποι με ανεπιθύμητες καταστάσεις.

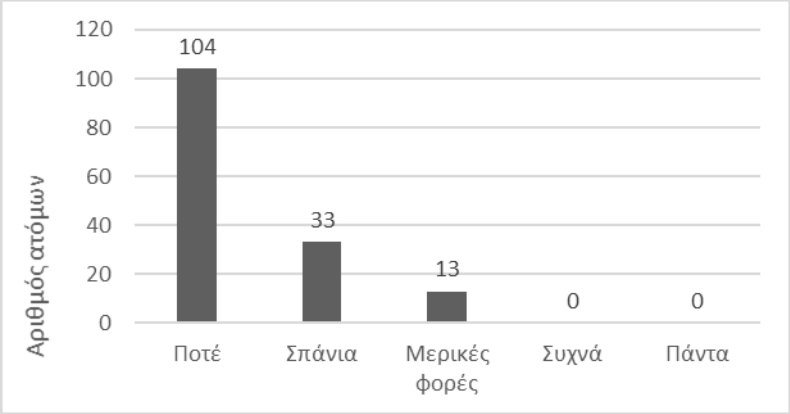
Μέρος Γ - Λήψη email και συνδέσμων (url)

- Διάγραμμα 10: Ανοίγετε emails και συνδέσμους (links) από άγνωστους αποστολείς;



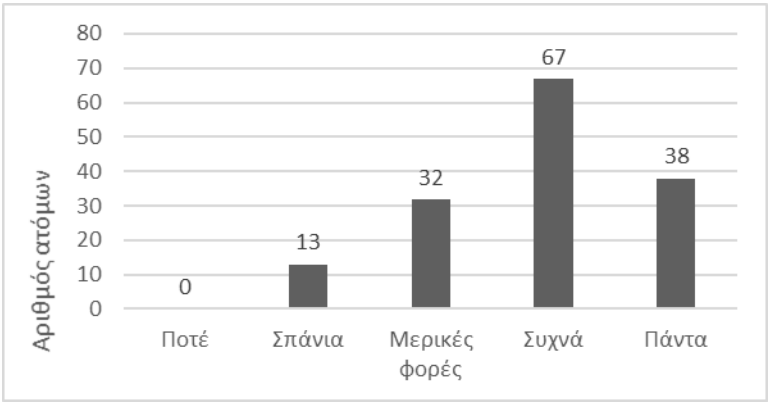
Το πιο πάνω ιστόγραμμα φανερώνει ότι συνολικά 112 άτομα ανοίγουν emails και συνδέσμους από άγνωστες πηγές. Αναλυτικότερα, 27 άτομα δήλωσαν ότι ανοίγουν μερικές φορές τέτοιου είδους μηνύματα, υποδηλώνοντας πως η επιλογή τους αυτή γίνεται μόνο όταν κρίνουν ότι είναι ακίνδυνα, γι' αυτό και τα διαβάζουν. Ακόμη, 41 άτομα αναφέρουν ότι ελάχιστες φορές μπαίνουν στον πειρασμό να ελέγξουν τέτοιου είδους συνδέσμους και emails. Σχεδόν το 1/5 των ερωτώμενων απάντησαν πως σε καμία περίπτωση δεν ανοίγουν πηγές από άγνωστους αποστολείς, αφού πιθανολογούν πως ενδέχεται να περιέχονται κακόβουλα λογισμικά εντός των μηνυμάτων τα οποία θα μεταφέρουν ιούς και θα προκαλέσουν ζημιά στις συσκευές τους. Ωστόσο, περίπου το 30% των συμμετεχόντων (44 άτομα) δήλωσαν πως ανοίγουν συχνά ή πάντα ληφθέντα αρχεία από αγνώστους, αφού η περιέργεια σε συνδυασμό με την άγνοια κινδύνου που τους διακατέχει, δεν τους επιτρέπει να αναλογιστούν το ρίσκο της πράξης τους.

- Διάγραμμα 11: Όταν σας σταλεί ένα email ή σύνδεσμος (link) από κάποιο γνωστό σας, αναρωτιέστε αν μπορεί να περιέχει κακόβουλο λογισμικό;



Ενδιαφέρον παρουσιάζουν τα αποτελέσματα της πιο πάνω ερώτησης, όπου περίπου το 70% των ερωτώμενων απάντησαν πως ποτέ δεν υποψιάστηκαν ότι κάποιο μήνυμα από κοντινά τους άτομα μπορεί να περιέχει επικίνδυνο υλικό. Αυτό μάλλον συμβαίνει λόγω της εμπιστοσύνης που έχουν προς τους φίλους, συγγενείς και συναδέλφους τους, γεγονός που τους οδηγεί στο να ανοίγουν οποιοδήποτε αρχείο ή μήνυμα τους σταλεί. Από την άλλη, 46 άτομα δήλωσαν ότι σπάνια ή μερικές φορές αισθάνθηκαν ότι μηνύματα ή αρχεία που στάλθηκαν από γνωστούς τους είναι ύποπτα ή ασυνήθιστα. Αξιοσημείωτο είναι το γεγονός πως κανένα άτομο δεν υποψιάζεται μηνύματα που στέλνονται από οικεία τους άτομα για πιθανούς κινδύνους. Αξίζει να σημειωθεί πως η οικειότητα και οι σχέσεις των ανθρώπων μπορεί να θεωρηθούν ως ευάλωτο σημείο, το οποίο οι hackers καταβάλλουν προσπάθεια να εκμεταλλευτούν για να πραγματοποιήσουν τις επιθέσεις τους.

- Διάγραμμα 12: Όταν σας σταλεί email ή σύνδεσμος (link) από κάποιο άγνωστο, αναρωτιέστε αν μπορεί να περιέχει κακόβουλο λογισμικό;

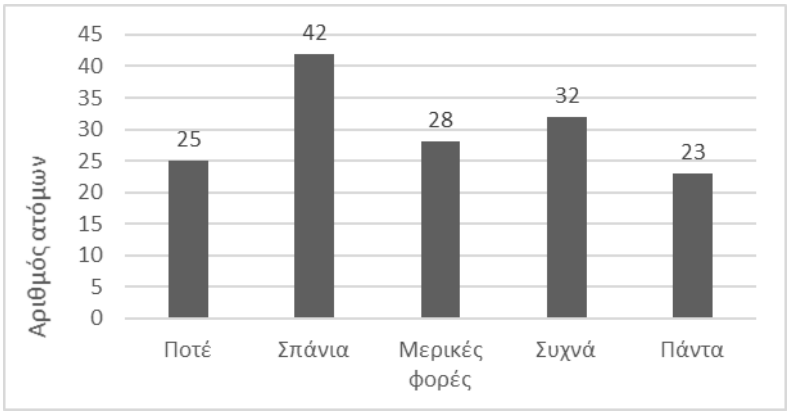


Το πιο πάνω διάγραμμα φανερώνει πως συνολικά 105 άτομα, που αναλογεί στο 70% των ερωτώμενων, υποψιάζονται συχνά ή πάντα πως emails και σύνδεσμοι από άγνωστες πηγές είναι επικίνδυνα. Τα συγκεκριμένα άτομα ενδεχομένως συνδέουν τη λήψη αρχείων με την πιθανότητα ύπαρξης κακόβουλου λογισμικού που μπορεί να έχει ως επακόλουθο την παραβίαση των προσωπικών τους δεδομένων. Σε μικρότερο βαθμό, 45 άτομα υποψιάζονται πως τέτοια μηνύματα πιθανόν να περιέχουν ιούς, κυρίως λόγω της δομής των συνδέσμων η οποία τους δίνει μια αρνητική εντύπωση. Εν κατακλείδι, οφείλουμε να αναφέρουμε το γεγονός ότι όλοι οι ερωτώμενοι έχουν υποψιαστεί και συνδέσει έστω και σε ελάχιστο βαθμό πως μηνύματα ή σύνδεσμοι από άγνωστες πηγές μπορεί να είναι επικίνδυνες και ζημιογόνες.

Μέρος Δ – Λογισμικό Antivirus

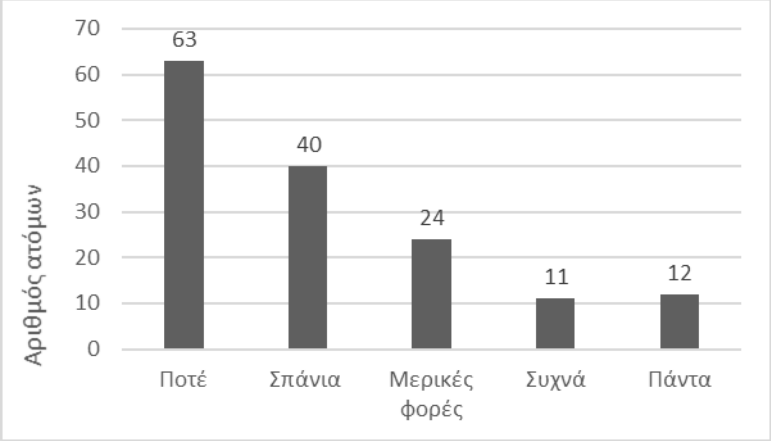
13:

- Διάγραμμα Εγκαθιστάτε λογισμικό antivirus στις συσκευές σας;



Στην πιο πάνω ερώτηση για την τοποθέτηση λογισμικού antivirus στις συσκευές των συμμετεχόντων, 67 άτομα δήλωσαν πως σπάνια ή ποτέ χρησιμοποιούν τέτοιου είδους λογισμικό. Ο κυριότερος λόγος για τον οποίο τα άτομα φαίνεται να αποφεύγουν να χρησιμοποιούν antivirus είναι το οικονομικό, αφού θεωρούν σπατάλη την πληρωμή για εγκατάστασή του. Ακόμη, πιθανόν να πιστεύουν ότι το antivirus δεν είναι τόσο αποτελεσματικό μέσο για πρόληψη και προστασία από ιούς. Επίσης, 28 άτομα απάντησαν πως χρησιμοποιούν μερικές φορές antivirus. Συνεπώς αντιλαμβανόμαστε πως σε κάποια χρονικά διαστήματα δεν το έχουν εγκατεστημένο, με αποτέλεσμα να βρίσκονται εκτεθειμένοι στο ενδεχόμενο μιας ηλεκτρονικής επίθεσης. Θετικό είναι το γεγονός πως 55 άτομα φροντίζουν συχνά ή πάντοτε η συσκευή τους να είναι προστατευμένη έχοντας ενσωματωμένο antivirus. Έτσι, νοιώθουν μεγαλύτερη ασφάλεια, αφού γνωρίζουν ότι λειτουργεί ως τείχος προστασίας από κακόβουλα λογισμικά.

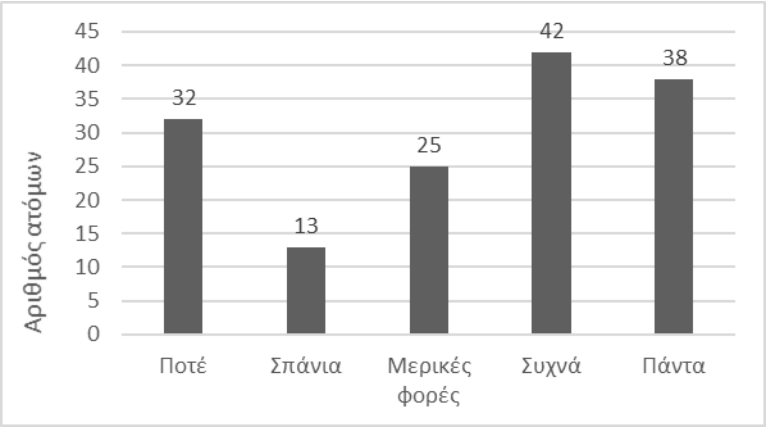
- Διάγραμμα 14: Πόσο συχνά επικαιροποιείτε (update) το λογισμικό antivirus που έχετε εγκαταστήσει;



Από τα αποτελέσματα του πιο πάνω διαγράμματος, ανησυχητικό είναι το γεγονός πως 63 άτομα δεν πραγματοποιούν ποτέ τις απαραίτητες ενέργειες για να ανανεώσουν και να επικαιροποιήσουν τα λογισμικά antivirus στις συσκευές τους. Σε αυτή την ομάδα ενδεχομένως να περιλαμβάνονται άτομα τα οποία είτε δεν έχουν καθόλου εγκατεστημένο antivirus, είτε δεν θεωρούν αναγκαίο να αναβαθμίζουν το λογισμικό τους. Βέβαια 64 άτομα δήλωσαν πως σπάνια ή μερικές φορές, προχωρούν στην επικαιροποίηση του antivirus τους. Επομένως, εύλογα συμπεραίνουμε πως τα άτομα των κατηγοριών αυτών δεν αντιλαμβάνονται τη σημαντικότητα και την αναγκαιότητα ενός update για πρόληψη και προστασία των συστημάτων τους. Με την αδράνεια τους δημιουργούν πρόσφορο έδαφος στους κυβερνοεγκληματίες να εκμεταλλευτούν την κατάσταση και να τους επιτεθούν. Τέλος, ανησυχητικό είναι πως μόλις 23 άτομα προβαίνουν συχνά ή πάντοτε σε update του

antivirus, γεγονός που δείχνει πως επιδιώκουν συνεχώς την ενίσχυση της προστασίας τους από οποιασδήποτε μορφής επικίνδυνου λογισμικού.

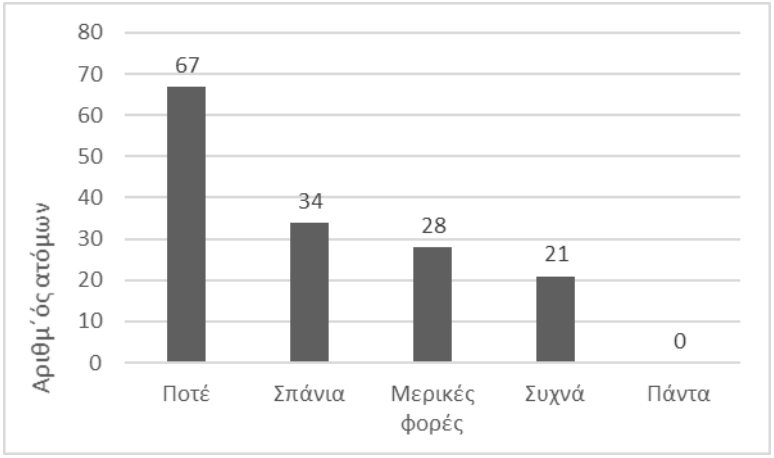
- Διάγραμμα 15: Χρησιμοποιείτε δωρεάν έκδοση κάποιου antivirus;



Στην πιο πάνω ερώτηση η πλειοψηφία των συμμετεχόντων χρησιμοποιεί, έστω και σε μικρή συχνότητα δωρεάν έκδοση antivirus. Αναλυτικότερα, 80 άτομα απάντησαν πως συχνά ή πάντοτε εγκαθιστούν δωρεάν έκδοση antivirus, καθώς φαίνεται να προτιμούν την επιλογή αυτή κυρίως για οικονομικούς λόγους. Ταυτόχρονα, θεωρούν πως το συγκεκριμένο λογισμικό έχει τις απαραίτητες προδιαγραφές που θα διασφαλίσουν την προστασία τους στο ψηφιακό κόσμο . Αντίστοιχα, 38 άτομα προτιμούν να χρησιμοποιούν δωρεάν έκδοση μερικές φορές ή σπάνια. Καταληκτικά, 32 άτομα δεν χρησιμοποιούν ποτέ δωρεάν έκδοση λογισμικού antivirus. Σε αυτή την κατηγορία πιθανόν να περιλαμβάνονται άτομα τα οποία δεν εγκαθιστούν ποτέ οποιοδήποτε λογισμικό antivirus, αλλά και άτομα που προτιμούν να πληρώσουν ένα χρηματικό ποσό για την εγκατάσταση ενός αναγνωρισμένου λογισμικού προστασίας.

Μέρος Ε – Ενημέρωση περί ιδιωτικότητας και ασφάλειας προσωπικών δεδομένων

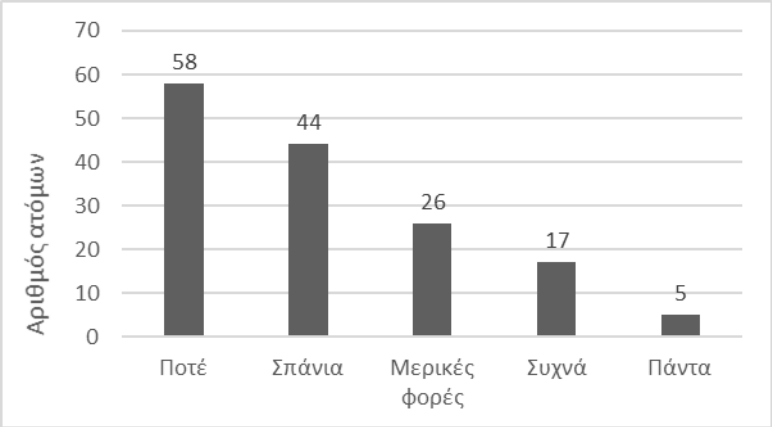
- Διάγραμμα 16: Ενημερώνεστε από την πολιτεία, το πανεπιστήμιο, το σχολείο ή το επαγγελματικό σας περιβάλλον για θέματα που αφορούν την προστασία των προσωπικών σας δεδομένων;



Άκρως ενδιαφέροντα είναι τα αποτελέσματα που προέκυψαν από την ερώτηση σχετικά με την ενημέρωση του πληθυσμού από διάφορους φορείς για θέματα που αφορούν την προστασία των προσωπικών δεδομένων. Το 45% των συμμετεχόντων (67 άτομα) δήλωσαν ότι δεν έχουν λάβει ποτέ οποιαδήποτε ενημέρωση ή εκπαίδευση για θέματα ασφάλειας στο διαδίκτυο. Αντιλαμβανόμαστε λοιπόν, πόσο σοβαρό είναι το γεγονός ότι κάποια άτομα δε λαμβάνουν την απαραίτητη πληροφόρηση από το περιβάλλον τους, ώστε να εφοδιαστούν με γνώσεις για ενίσχυση της ιδιωτικότητας και προστασίας των προσωπικών τους δεδομένων. Ωστόσο, βλέπουμε πως 62 άτομα απάντησαν πως ενημερώνονται από

κάποιους φορείς σε μικρή συχνότητα για το θέμα αυτό. Αντίθετα, 21 ερωτώμενοι υποστηρίζουν ότι λαμβάνουν συχνά ενημέρωση έστω από κάποιο φορέα που υποδείχθηκε. Επομένως, μπορούμε να υποστηρίξουμε ότι διαθέτουν τα ελάχιστα εφόδια για να κατανοήσουν περισσότερο τον ψηφιακό κόσμο και τους κινδύνους που εμπεριέχει.

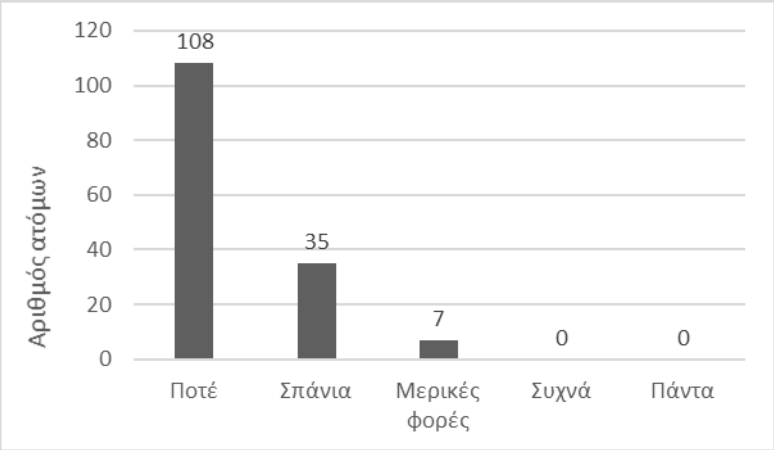
- <u>Διάγραμμα 17: Ενημερώνεστε με δικές σας πρωτοβουλίες για θέματα που αφορούν την προστασία των προσωπικών σας δεδομένων;</u>



Στη συγκεκριμένη ερώτηση εξετάζεται η συχνότητα με την οποία ενημερώνονται οι συμμετέχοντες, με δική τους πρωτοβουλία, για θέματα που αφορούν την προστασία των προσωπικών τους δεδομένων. Το γεγονός ότι 102 άτομα, δηλαδή περίπου το 70% του δείγματος μας, σπάνια ή ποτέ δεν μερίμνησαν να ενημερωθούν για θέματα ιδιωτικότητας, προκαλεί μεγάλη αίσθηση. Επιπλέον, 26 άτομα δήλωσαν πως μερικές φορές φροντίζουν να ενημερώνονται για το συγκεκριμένο θέμα, και ενδεχομένως αυτό να γίνεται όταν ήδη έχει παρουσιαστεί κάποιο πρόβλημα και όχι για προληπτικούς λόγους. Τέλος, 22 άτομα μεριμνούν συχνά ή πάντα να ενημερώνονται διαρκώς και να διαβάζουν άρθρα με σκοπό να αποκτήσουν περισσότερες γνώσεις για την ασφάλειά τους. Με αυτόν τον τρόπο είναι

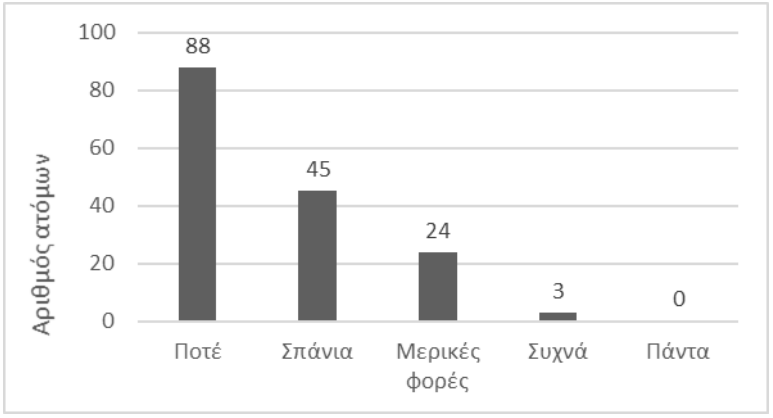
προδραστικοί, καθώς έχουν ως σκοπό να μην έρθουν αντιμέτωποι με προβλήματα παραβίασης της ιδιωτικότητάς τους.

- Διάγραμμα 18: Έχετε παρευρεθεί σε σεμινάρια ή διαλέξεις, δια ζώσης ή εξ αποστάσεως, που αφορούν θέματα σχετικά με την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων;



Το πιο πάνω διάγραμμα φανερώνει πως η πλειοψηφία των ερωτώμενων, που αντιστοιχεί περίπου στο 72%, δεν έχουν παρευρεθεί ποτέ σε σεμινάριο που αφορά την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Συνεπώς, τα άτομα αυτά πιθανόν να μην προσπαθούν να ενημερώνονται από ειδικούς ώστε να λάβουν σημαντικές πληροφορίες. Από την άλλη 35 ερωτώμενοι ισχυρίζονται πως έχουν παρευρεθεί σπάνια σε τέτοιου είδους σεμινάρια και άλλα 7 άτομα μερικές φορές, όταν τους δόθηκε η ευκαιρία και είχαν ελεύθερο χρόνο. Αξιοσημείωτο είναι το γεγονός ότι δεν υπάρχει κανείς συμμετέχοντας στην έρευνα μας που να παρακολουθεί συχνά η πάντοτε τέτοιου είδους σεμινάρια και διαλέξεις.

- Διάγραμμα 19: Στις διάφορες ιστοσελίδες που επισκέπτεστε, πόσο συχνά διαβάζετε την πολιτική τους για τα cookies και τις πολιτικές ασφαλείας και προστασίας της ιδιωτικότητας που έχουν αναρτήσει;



Στην πιο πάνω ερώτηση παρατηρούμε ότι 88 άτομα δεν ενδιαφέρθηκαν ποτέ να διαβάσουν τις πολιτικές και τα cookies των ιστοσελίδων που επισκέπτονται. Οι συγκεκριμένοι ερωτώμενοι δίνουν απερίσκεπτα τη συγκατάθεση τους στις ιστοσελίδες που χρησιμοποιούν αποδεχόμενοι τους όρους και τις πολιτικές τους, δίνοντας έτσι δικαίωμα στον οποιοδήποτε να συγκεντρώνει προσωπικά τους δεδομένα που μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς. Αντίθετα, υπάρχουν μόλις 3 άτομα τα οποία συχνά διαβάζουν τις πολιτικές και τα cookies ορισμένων ιστοσελίδων που μπορεί να μην είναι σίγουροι για την αξιοπιστία τους. Κανένα άτομο δεν διαβάζει πάντα τις πολιτικές ασφαλείας και ιδιωτικότητας, γεγονός που προβληματίζει. Βέβαια, 69 άτομα επιλέγουν να

διαβάζουν σπάνια ή μερικές φορές τους όρους των ιστοσελίδων ανάλογα με τη σημαντικότητα των ηλεκτρονικών υποχρεώσεων που έχουν να εκτελέσουν.

- Ερώτημα: Σε ποιο βαθμό πιστεύετε ότι υπάρχει πιθανότητα να σας συμβεί ένα είδος επίθεσης κατά την περιήγηση σας στο διαδικτυακό χώρο;

Το πιο πάνω ερώτημα ήταν και το τελευταίο που οι συμμετέχοντες κλήθηκαν να απαντήσουν. Οι κατηγορίες των ειδών επιθέσεων που συμπεριλήφθηκαν στο ερώτημα ήταν: ηλεκτρονική επίθεση, πρόκληση ζημιάς στις συσκευές, κλοπή προσωπικών δεδομένων, κλοπή συνθηματικών για τραπεζικούς λογαριασμούς, μόλυνση συστημάτων από ιούς και παρακολούθηση ηλεκτρονικής δραστηριότητας από τρίτους.

Η πλειοψηφία των ερωτώμενων, και πιο αναλυτικά το 45%, πιστεύουν ότι υπάρχει μεγάλη πιθανότητα να δεχθούν ένα είδος ηλεκτρονικής επίθεσης, ενώ ένα μικρό ποσοστό 18% θεωρεί ότι οι πιθανότητες είναι ελάχιστες. Στο ενδεχόμενο πιθανής πρόκλησης ζημίας στις συσκευές τους κατά την πραγματοποίηση ηλεκτρονικών δραστηριοτήτων, το 53% των ερωτώμενων θεωρεί ότι αυτό μπορεί να συμβεί σε μέτριο βαθμό. Βέβαια υπάρχουν και αρκετοί (33%) που δίνουν αυξημένες πιθανότητες να έρθουν αντιμέτωποι με κάτι τέτοιο.

Σε πιθανή υποκλοπή ευαίσθητων πληροφοριών, το 52% του δείγματος πιστεύει πως υπάρχουν αυξημένες πιθανότητες, ωστόσο υπάρχει και μια μερίδα ατόμων που είναι πιο εφησυχασμένοι (28%), καθώς δεν θεωρούν ότι υπάρχει ιδιαίτερος κίνδυνος παραβίασης των προσωπικών τους δεδομένων. Όσον αφορά την πιθανότητα μόλυνσης των συστημάτων τους από ιούς, το 46% θεωρεί ότι είναι αρκετά πιθανό οι συσκευές τους να μολυνθούν από κακόβουλα προγράμματα, το 22% πιστεύει πως μπορεί να συμβεί σε μέτριο βαθμό, ενώ ανησυχητικό είναι πως το 32% νοιώθει σε μικρό βαθμό έως καθόλου τις συσκευές του να απειλούνται.

Στην τελευταία κατηγορία που αφορά την παρακολούθηση των ηλεκτρονικών τους δραστηριοτήτων, ένα μεγάλο ποσοστό των ερωτώμενων που ανέρχεται στο 63% θεωρεί ότι οι ηλεκτρονικές τους δραστηριότητες δεν παρακολουθούνται από τρίτα άτομα. Τέλος, σημαντικό είναι να τονιστεί πως μόλις το 12% πιστεύει ότι σε μεγάλο ή πολύ μεγάλο βαθμό υπάρχει κάποιου είδους παρακολούθηση από μη εξουσιοδοτημένα άτομα.

3.4 Συμπεράσματα που εξάχθηκαν από την έρευνα

Η συλλογή και ανάλυση των δεδομένων που λήφθηκαν στα πλαίσια της έρευνάς μας κατέδειξαν χρήσιμα συμπεράσματα τα οποία αξίζουν αναφοράς. Τα αποτελέσματα του ερωτηματολογίου ήταν αρκετά ανησυχητικά, καθώς διαφάνηκε ότι οι πολίτες δεν είναι αρκετά ευαισθητοποιημένοι σε θέματα προστασίας της ιδιωτικότητάς τους και των προσωπικών τους δεδομένων. Οι γνώσεις που παρουσιάζει η πλειοψηφία των ερωτώμενων είναι ελλιπείς, καθώς φαίνεται να έχουν λανθασμένες απόψεις για το πως πραγματικά λειτουργεί ο ψηφιακός κόσμος.

Ειδικότερα, οι απαντήσεις του ερωτηματολογίου φανέρωσαν πως ο κόσμος δεν κατανοεί τη σημαντικότητα των κωδικών πρόσβασης. Οι περισσότεροι συμμετέχοντες χρησιμοποιούν αδύναμους κωδικούς, οι οποίοι εύκολα μπορούν να παραβιαστούν. Αντιλαμβανόμαστε πως υπάρχει προτίμηση στη χρήση μικρών κωδικών σε έκταση, οι οποίοι συνήθως περιλαμβάνουν και προσωπικά τους στοιχεία (π.χ. ονόματα, ημερομηνίες γέννησης και διευθύνσεις). Με τον τρόπο αυτό αυξάνονται θεαματικά οι πιθανότητες να υποπέσουν σε μια ηλεκτρονική επίθεση.

Επίσης, παρατηρήθηκε πως μερικοί ερωτώμενοι μοιράζονται απερίσκεπτα τους κωδικούς πρόσβασής τους με φίλους και συγγενείς, γεγονός που θεωρείται αδιανόητο αν αναλογιστούμε τις αυξημένες επιθέσεις που έγιναν τα τελευταία χρόνια. Κάθε άτομο οφείλει να διατηρεί τη μυστικότητα των κωδικών του και να μην εκμυστηρεύεται σε άλλους το κλειδί για τις προσωπικές του πληροφορίες. Εξάλλου, πολλά είναι τα περιστατικά που οδήγησαν στη ρήξη σχέσεων μεταξύ φίλων ή συγγενών, οι οποίοι στη συνέχεια προχώρησαν σε ενέργειες εκδικητικού χαρακτήρα χρησιμοποιώντας τους κωδικούς των κοντινών τους ανθρώπων. Άλλη μια κακή συνήθεια που έγινε αντιληπτή μέσα από την έρευνα είναι πως αρκετοί είναι αυτοί που καταγράφουν τους κωδικούς τους πάνω σε κάποιο χαρτί ή αρχείο στον υπολογιστή τους. Κάτι τέτοιο μπορεί να δώσει εύκολη πρόσβαση σε τρίτα άτομα για απόκτηση των κωδικών, με αποτέλεσμα να υπάρχει ρίσκο να δημιουργηθούν απρόβλεπτες καταστάσεις.

Ένα άλλο συμπέρασμα που διαφάνηκε μέσα από την έρευνα είναι η άσχημη συνήθεια που διατηρούν κάποια άτομα να ανοίγουν email και συνδέσμους από άγνωστους αποστολείς. Αυτό καταδεικνύει ξεκάθαρα άγνοια κινδύνου για το τι μπορεί να περιέχεται σε τέτοια

μηνύματα, εφόσον δεν αντιλαμβάνονται ότι μπορεί να πέσουν θύματα phishing από hackers. Ταυτόχρονα, οι περισσότεροι δηλώνουν πως παρόλο που υποψιάζονται την ύπαρξη κακόβουλου λογισμικού σε emails ή συνδέσμους από κάποιον άγνωστο, δε φαίνεται να συμβαίνει το ίδιο και με emails που προέρχονται από γνωστούς τους. Συχνά ο κόσμος δέχεται μηνύματα από φίλους, συγγενείς ή συναδέλφους τα οποία στην πραγματικότητα αποστέλλονται από αγνώστους, οι οποίοι κατάφεραν να παραβιάσουν δεδομένα και να αποκτήσουν πρόσβαση στις συσκευές τους. Οι hackers εκμεταλλευόμενοι τις ανθρώπινες σχέσεις των πιθανών θυμάτων τους, προσποιούνται κάποιο γνωστό τους, ώστε να τους ξεγελάσουν και να πετύχουν τον στόχο τους. Έτσι, αν και τα μηνύματα μπορεί να φαίνονται ύποπτα, οι παραλήπτες τις περισσότερες φορές τα ανοίγουν κανονικά, καθώς θεωρούν πως ο αποστολέας είναι οικείο τους πρόσωπο.

Ακόμη, φαίνεται να υπάρχει μεγάλη υποτίμηση στη χρησιμότητα του antivirus. Αρκετοί πιστεύουν ότι δεν είναι απαραίτητη η εγκατάσταση ενός τέτοιου λογισμικού στις συσκευές τους, καθώς πιστεύουν πως οι δυνατότητες του είναι περιορισμένες. Οι πλείστοι, όπως φάνηκε, δεν είναι ενημερωμένοι για τις σύγχρονες τεχνολογίες που χρησιμοποιούν τα antivirus για την αντιμετώπιση κακόβουλων επιθέσεων όπως ransomware, cryptojacking ή phishing. Επιπλέον, αρκετοί θεωρούν πως η εγκατάσταση δωρεάν έκδοσης λογισμικού antivirus είναι άκρως αποτελεσματική. Ωστόσο, χρειάζεται να αντιληφθούν πως οι παροχές τέτοιων λογισμικών είναι περιορισμένες και πως δεν είναι ικανά να αντιμετωπίσουν όλων των ειδών κακόβουλων λογισμικών.

Χωρίς αμφιβολία η μεγαλύτερη ευθύνη για την αμάθεια και την έλλειψη γνώσεων που παρατηρείται στον πληθυσμό για θέματα προστασίας των προσωπικών δεδομένων αποδίδεται κυρίως στην πολιτεία και στα εκπαιδευτικά ιδρύματα όλων των βαθμίδων. Αρνητικό είναι το γεγονός πως οι πιο πάνω φορείς δεν αφιερώνουν τον απαραίτητο χρόνο και πόρους για την επιμόρφωση του κοινού. Αντίθετα, η εστίασή τους σε άλλα κοινωνικά θέματα, έχει ως αποτέλεσμα την υποτίμηση των κινδύνων που κρύβει το διαδίκτυο και τις ανυπολόγιστες συνέπειες που μπορεί να ακολουθήσουν.

Κρίνεται αναγκαίο, λοιπόν, η κυβέρνηση να προβεί σε όλες τις απαραίτητες ενέργειες οι οποίες θα ενισχύσουν την ευαισθητοποίηση των πολιτών, ανατρέποντας την χαώδη κατάσταση που επικρατεί και μειώνοντας παράλληλα τις πιθανότητες εκδήλωσης τέτοιων επιθέσεων. Οι κινήσεις πρέπει να είναι στοχευμένες και να προσαρμόζονται ανάλογα με

την ηλικιακή ομάδα στην οποία απευθύνονται. Επίσης, καλό θα ήταν μέσω σωστού προγραμματισμού και οργάνωσης να πραγματοποιούνται εκδηλώσεις και καμπάνιες οι οποίες θα προσελκύουν το κοινό, με στόχο τη λεπτομερή ενημέρωση για τη σημαντικότητα της διασφάλισης της ιδιωτικότητάς του.

Η επίτευξη των πιο πάνω θα είναι πιο εφικτή εάν υπάρχει κατάλληλη συνεργασία με δήμους, τράπεζες, πανεπιστήμια και εξειδικευμένο προσωπικό που έχουν τις απαραίτητες γνώσεις σχετικά με την προστασία των προσωπικών δεδομένων. Κάθε φορέας χρησιμοποιώντας τις δικές του ικανότητες και μεθόδους θα πρέπει να συμβάλει στην πλήρη ενημέρωση των πολιτών μέσα από ευχάριστες και δημιουργικές δράσεις. Έτσι θα προσελκύεται μεγαλύτερος αριθμός ατόμων, ενώ ταυτόχρονα θα υπάρχει η απαιτούμενη σοβαρότητα από τους πολίτες για την αφομοίωση όσο το δυνατόν περισσότερων γνώσεων.

Εντούτοις, παρατηρούμε πως ούτε οι ίδιοι οι πολίτες καταλαμβάνουν ατομική προσπάθεια για ενημέρωση στο συγκεκριμένο τομέα. Είναι φανερό πως ο σύγχρονος κόσμος δεν αντιλαμβάνεται ολοκληρωτικά την επικίνδυνη πλευρά του διαδικτύου και τις επιπτώσεις που μπορεί να επιφέρει μια ηλεκτρονική επίθεση. Επιπλέον, εξαιρετικά σημαντικό συμπέρασμα που διαφάνηκε από την έρευνα είναι η ύπαρξη του φαινομένου του παραδόξου. Πιο συγκεκριμένα, μεγάλο μέρος από το δείγμα συμπεριφέρεται με τρόπο που ευνοεί τέτοιες επιθέσεις, παρόλο που αντιλαμβάνονται τους κινδύνους που ελλοχεύει μια ηλεκτρονική επίθεση. Αυτό πρέπει να μας προβληματίσει, καθώς οι ανησυχίες που έχουν οι πολίτες δεν συμβαδίζουν με τον τρόπο δραστηριοποίησής τους. Ως επακόλουθο, δημιουργείται μεγάλος κίνδυνος παραβίασης των δεδομένων τους από hackers που προσπαθούν να αποσπάσουν ευαίσθητες πληροφορίες.

Συνοψίζοντας τα όσα αναφέρθηκαν πιο πάνω, το σημαντικότερο πρόβλημα που εντοπίστηκε είναι η έλλειψη ευαισθητοποίησης και ενημέρωσης για θέματα ιδιωτικότητας και προστασίας των προσωπικών τους δεδομένων. Το φαινόμενο αυτό παρουσιάζεται στα περισσότερα άτομα του δείγματος ανεξαρτήτως φύλου, ηλικίας και μόρφωσης. Επομένως, εύλογα μπορούμε να υποστηρίξουμε ότι κρίνεται εξαιρετικά σημαντικό ο καθένας από εμάς να προβεί στις απαραίτητες ενέργειες και την απόκτηση κατάλληλων γνώσεων, ώστε να μειωθεί ο κίνδυνος ηλεκτρονικών επιθέσεων.

Επίλογος

Η ανθρωπότητα έχει βιώσει σημαντικές τεχνολογικές ανακαλύψεις στο πέρασμα του χρόνου. Μια αναδρομή στο χρόνο είναι αρκετή για να αποδείξει πως κάθε τεχνολογική ανακάλυψη που πραγματοποιήθηκε άλλαζε ριζικά τη ζωή των ανθρώπων. Η τεχνολογία και η αυξημένη χρήση του διαδικτύου συνέβαλαν στην ενίσχυση των ανθρώπινων σχέσεων και στην πιο αποτελεσματική ολοκλήρωση των διαδικασιών. Ωστόσο, όπως τονίστηκε και κατά τη διάρκεια της μεταπτυχιακής διατριβής, το κύριο μειονέκτημα που επέφερε η τεχνολογική εξέλιξη είναι οι κυβερνοεπιθέσεις. Χρόνο με το χρόνο όλο και περισσότεροι έρχονται αντιμέτωποι με το φόβο κλοπής των προσωπικών τους δεδομένων. Δεδομένου ότι υπάρχουν κυβερνοεγκληματίες που είναι ικανοί να σπάσουν το τείχος προστασίας τεράστιων επιχειρήσεων ή κυβερνήσεων, δημιουργείται φόβος και ανησυχία στους απλούς ανθρώπους για την προστασία της ιδιωτικότητάς τους. Παρόλες τις δυσκολίες και τον τρόμο που επικρατεί γύρω από αυτό το θέμα, ο κόσμος δε φαίνεται να είναι αρκετά ευαισθητοποιημένος, γεγονός που αποδείχθηκε και από την έρευνα που πραγματοποιήθηκε. Τόσο οι επιχειρήσεις όσο και οι χρήστες δε λαμβάνουν τα κατάλληλα μέτρα που θα τους διασφαλίσουν την προστασία από τέτοιες επιθέσεις, ενώ παράλληλα η πολιτεία και τα εκπαιδευτικά ιδρύματα δεν παρέχουν την απαραίτητη ενημέρωση στον πληθυσμό. Εάν δεν υπάρξει ριζική αλλαγή στη συμπεριφορά των ανθρώπων, τότε είναι δεδομένο πως οι κυβερνοεπιθέσεις θα αυξηθούν και οι συνέπειες θα είναι καταστροφικές. Επομένως, καθένας από εμάς είναι απαραίτητο να υιοθετήσει όλα τα απαραίτητα μέτρα προστασίας των προσωπικών δεδομένων και να ενημερώνεται συνεχώς για τους νέους κινδύνους που εμφανίζονται. Με τον τρόπο αυτό, θα μειώνονται οι πιθανότητες πραγματοποίησης κυβερνοεπιθέσεων τόσο στις επιχειρήσεις, όσο και στις συσκευές του καθενός ξεχωριστά.

Βιβλιογραφία

1. Alaali, M. (2022) Covid-19 challenges to university information technology governance
2. Alfaro, J., Lioudakis, G., Boulahia, N.,Foley, S., & Fitzgerald, W. (2013) Data privacy management and Autonomous Spontaneous Security
3. Allan, D. (2020) Paid antivirus vs free antivirus: Which should you get? https://www.techradar.com/news/paid-antivirus-vs-free-antivirus-which-should-you-get
4. Asbas, C., & Tuzlukaya, S. (2022) Conflict management in digital business: Cyberattack and Cyberwarfare strategies for business.
5. Bailey, M., Holz, T., Stamatogiannakis, M., & Ioannidis, S. (2018) Research in attacks, intrusions, and defenses
6. Bezzi, M., Duquenoy, P., Hansen, M., & Zhang, G. (2009) Privacy and identity management for life.
7. Botek, A. (2021) Office of personnel management data breach 2015 https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015)
8. Bunge, J., (2021) JBS Paid $11 Million to resolve Ransomware Attack https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
9. Cashell, B., Jickling, M., & Webel, B. (2004). The economic Impact of Cyber attacks
10. Chadd, K., (2020) The History Of Cybercrime And Cybersecurity, 1940-2020 https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/
11. Climer, S. (2018) History of cyber-attacks from the Morris worm to Exactis https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/
12. Covert, E. (2021) Case Study: TJ Maxx's Data breach https://medium.com/@edwincovert/case-study-tjx-data-breach-4ace4cc2732a

13. Dobusch, L., & Schoeneborn, D. (2015) Fluidity, Identity and organizationality: The communicative Constitution of Anonymous

14. Finnigan, P. (2018) Oracle incident response and forencics, preparing for and responding to data breaches

15. Fisher, T. (2022) What is yahoo? https://www.lifewire.com/what-is-yahoo-3483209

16. Fruhlinger, J. (2020) The OPM hacked explained: Bad security practices meet China's Captain America https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

17. Gafni, R., & Pavel, T. (2021) Cyberattacks against the health-care sectors during the COVID-19 pandemic.

18. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., & Laplante, P. (2011). Dimensions of Cyber-Attacks, social, Political, Economic, and cultural.

19. Giagkinis, I. (2017) Τρία δις. οι λογαριασμοί της Yahoo που χακαρίστηκαν https://gr.euronews.com/2017/10/04/tria-dis-oi-logariasmoi-tis-yahoo-poy-xakaristikan

20. Gregory, J. (2022) How to respond to non-malicious data threats https://securityintelligence.com/articles/how-respond-accidental-data-breach/

21. Gregory, M., & Glance, D. (2013). Security and the networked society

22. Gupta, H. (2022) 11 Advantages of using an antivirus software – importance of online security 11 Advantages of Using an Antivirus Software - Importance of Online Security (geekflare.com)

23. Hathaway, O., Crootof R., Levitz, P., Nix H., Nowlan, A., Perdue., & Spiegel, J. (2012). The law of Cyber attack

24. Huddleston, T. (2022) What is anonymous? How the infamous hacktivist group went from 4chan trolling to launching cyberattacks on Russia

https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

25. Jahankhani, H., Jamal, A., & Lawson, S. (2021) Cybersecurity, Privacy, and freedom protection in the connected world

26. James, N., (2022) The Staggering Cost of Cyberattacks: How Much Money do Businesses Actually Lose? https://www.getastra.com/blog/security-audit/cost-of-cyberattacks/

27. Kävrestad, J., Eriksson, F., & Nohlberg, M. (2018) Understanding passwords – a taxonomy of password creation strategies.

28. Khanna, A., Gupta, D., Bhattacharyya, S., Hassanien, A., Anand, S., & Jaiswal, A. (2021) International Conference on Innovative Computing and Communications

29. Kokolakis, S. (2015) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon

30. Kranenbarg, M., & Leukfeldt, R. (2021). Cybercrime in Context, The human factor in victimization, offending, and policing

31. Landahl, M., & Thornton, T. (2021) The role of law enforcement in emergency management and homeland security.

32. Langdon, P., Lazar, J., Heylighen, A., Dong, H. (2018) Breaking down barriers: Usability, accessibility, and inclusive design.

33. Lavranou, R., & Tsohou, A. (2018) Developing and validating a common body of knowledge for information privacy

34. Lehto, M., & Neittaanmäki, P. (2022) Cyber security: Critical Infrastructure protection

35. Lima, S., Silva, S., Silva, W., & Santos, W. (2022) Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack.

36. Mamaghani, F. (2002) Evaluation and selection of an antivirus and content filtering software

37. Mark, C., (2020) Understanding Cyber attacker motivations to best apply controls https://cybersecurity.att.com/blogs/security-essentials/understanding-cyber-attacker-motivations-to-best-apply-controls
38. Masood, R., Vatsalan, D., & Ikram, M. (2018) Incognito: A method for obfuscating web date
39. Matyas, V., Hubner, S., Cvrcek, D., & Svenda, P. (2008) The future of Identity in the information society
40. Mclean, M. (2023) 2023 Must-Know cyber-Attack statistics and trends https://www.embroker.com/blog/cyber-attack-statistics/
41. Miller, A. (2007) TJX Hacking Incident shows cracks in payment card systems https://www.bankinfosecurity.com/tjx-hacking-incident-shows-cracks-in-payment-card-systems-a-222
42. Miller, K. (2021) The covid pandemic's lasting impact on cloud usage https://www.infoworld.com/article/3614809/the-covid-pandemics-lasting-impact-on-cloud-usage.html
43. Morgan, J. (2015) 5 reasons why the cloud is environmentally friendly https://www.missioncloud.com/blog/5-reasons-why-the-cloud-is-environmentally-friendly
44. Morgan, S. (2020) Cybercrime to cost the world $10.5 trillion Annually by 2025 https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
45. Muncaster, P. (2022) Global Supply Chain Attacks Surge 51% in H2 2021
46. Pratt, M., (2022) What is a cyber- attack? https://www.techtarget.com/searchsecurity/definition/cyber-attack
47. Sanchez, M. (2022) Mitigating Non-malicious insider threats in a decentralized work environment https://www.spiceworks.com/it-security/vulnerability-management/guest-article/mitigating-non-malicious-insider-threats/
48. Selyukh, A. (2017) Every yahoo account that existed in Mid – 2013 was likely hacked https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked

49. Smith, S., (2015). Management models for international cybercrime

50. Solms, B., & Solms, R. (2017) Cybersecurity and information security – What goes where?

51. SonicWall. (2021) Sonicwall cyber threat report: Cyber threat intelligence for navigating today's business reality https://www.cerdant.com/wp-content/uploads/2021/09/2-2021-threat-report-midyear-summary.pdf

52. Soumelidou, A., & Tsohou, A. (2017) Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram.

53. Stoddart, K. (2022) Cyberwarfare: Threats to Critical infrastructure

54. Stouffer, C., (2021) The privacy paradox: How much privacy are we willing to give up online? https://us.norton.com/blog/privacy/how-much-privacy-we-give-up

55. Surfshark. (2021) Data breach statistics by country in 2021 Data breach statistics by country: Recap of 2021 - Surfshark

56. Thomas, G., & Sule, M. (2021) A service lens on cybersecurity continuity and management for organizations' subsistence and growth

57. Townsend, C. (2021) A brief and incomplete History of Cybersecurity https://www.uscybersecurity.net/history/

58. Warner, M., & Wang, V. (2018) Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability, and information management

59. Weber, R., & Weber, R. (2010) Internet of Things Legal Perspectives

60. Wirth, J., Maier, C., Laumer, S., & Weitzel, T. (2019) Laziness as an explanation for the privacy paradox: a longitudinal empirical investigation.

61. Wolf, A., (2022) A brief history of Cybercrime https://arcticwolf.com/resources/blog/decade-of-cybercrime/

62. Yacob, N., Noor, N., Yunus, N., Yussof, R., & Zakaria, S. (2016) Regional conference on science, Technology, and social sciences

Παράρτημα Α

Ερωτηματολόγιο Διεξαγωγής Έρευνας

Το συγκεκριμένο ερωτηματολόγιο συντάχτηκε στο πλαίσιο της μεταπτυχιακής διατριβής του **Φοίβου Χαραλάμπους**, φοιτητή του μεταπτυχιακού προγράμματος *«Διοίκηση Τεχνολογία και Ποιότητα»* του **Ανοιχτού Πανεπιστημίου Κύπρου** με θέμα:

Κυβερνοασφάλεια και ευαισθητοποίηση περί ιδιωτικότητας και προστασίας δεδομένων

Σκοπός της παρούσας έρευνας είναι να μελετηθεί κατά πόσο ο πληθυσμός είναι ενήμερος και ευαισθητοποιημένος για θέματα που αφορούν την προστασία των προσωπικών δεδομένων και τη διασφάλιση της ιδιωτικότητας του στον διαδικτυακό χώρο.

Με τον όρο ιδιωτικότητα στον διαδικτυακό χώρο εννοούμε το δικαίωμα κάθε χρήστη να μπορεί να διατηρεί τον έλεγχο των προσωπικών του δεδομένων χωρίς την παρέμβαση τρίτων ατόμων.

Το ερωτηματολόγιο είναι αρκετά σύντομο με τον εκτιμώμενο χρόνο συμπλήρωσης του να υπολογίζεται στα 5-6 λεπτά. Η συμμετοχή σας στην έρευνα είναι πάρα πολύ χρήσιμη, αφού απο τις ανώνυμες απαντήσεις σας και την επεξεργασία των δεδομένων εκτιμούμε ότι θα προκύψουν χρήσιμα συμπεράσματα σχετικά με το πόσο ευαισθητοποίημενοι είναι οι πολίτες σε θέματα ιδιωτικότητας και ασφάλειας των προσωπικών δεδομένων τους.

Για οποιεσδήποτε διευκρινίσεις ή περαιτέρω πληροφορίες σχετικά με την έρευνα, σας παρακαλώ ας επικοινωνήσετε μαζί μου.

Φοίβος Χαραλάμπους

Email: fivos.charalampous@st.ouc.ac.cy

<u>Σημειώστε με Χ την επιλογή σας στα πιό κάτω πλαίσια</u>:

<u>Μέρος Α: Δημογραφικά στοιχεία</u>

1) Φύλο

Άνδρας	Γυναίκα

2) Ηλικία

13-18	19-25	26-40	41-65

3) Μόρφωση

Γυμνάσιο	Λύκειο	Πανεπιστήμιο	Μεταπτυχιακό	Διδακτορικό

<u>Μέρος Β: Κωδικοί πρόσβασης / συνθηματικά (passwords)</u>

4) Αποθηκεύετε τους κωδικούς πρόσβασης σας στις συσκευές που χρησιμοποιείτε;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

5) Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για τις ιστοσελίδες και τις διάφορες εφαρμογές με τις οποίες αλληλεπιδράτε;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

6) Χρησιμοποιείτε κωδικούς πρόσβασης που σχετίζονται με κάποια προσωπικά σας στοιχεία;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

7) Οι κωδικοί πρόσβασης που επιλέγετε, περιέχουν συνδυασμό απο αριθμούς, γράμματα και σύμβολα;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

8) Μοιράζεστε τους κωδικούς πρόσβασης με άλλα άτομα, όπως φίλους, συγγενείς και συναδέλφους;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

9) Πόσο συχνά καταγράφετε τους κωδικούς πρόσβασης σε χαρτί ή κάποιο sticky note ή σε αρχείο στον υπολογιστή σας;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

<u>Μέρος Γ - Λήψη email και συνδέσμων (url)</u>

10) Ανοίγετε emails και συνδέσμους (links) απο άγνωστους αποστολείς;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

11) Όταν σας σταλεί ένα email ή σύνδεσμος (link) απο κάποιον γνωστό σας, αναρωτιέστε αν μπορεί να περιέχει κακόβουλο λογισμικό;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

12) Όταν σας σταλεί email ή σύνδεσμος (link) απο κάποιον άγνωστο, αναρωτιέστε αν μπορεί να περιέχει κακόβουλο λογισμικό;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

Μέρος Δ – Λογισμικό Antivirus

13) Εγκαθιστάτε λογισμικό antivirus στις συσκευές σας;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

14) Πόσο συχνά επικαιροποιείτε (update) το λογισμικό antivirus που έχετε εγκαταστήσει;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

15) Χρησιμοποιείτε δωρεάν έκδοση κάποιου antivirus ;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

Μέρος Ε – Ενημέρωση περί ιδιωτικότητας και ασφάλειας προσωπικών δεδομένων

16) Ενημερώνεστε απο την πολιτεία, το πανεπιστήμιο, το σχολείο ή το επαγγελματικό σας περιβάλλον για θέματα που αφορούν την προστασία των προσωπικών σας δεδομένων;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

17) Ενημερώνεστε με δικές σας πρωτοβουλίες για θέματα που αφορούν την προστασία των προσωπικών σας δεδομένων;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

18) Έχετε παρευρεθεί σε σεμινάρια ή διαλέξεις, δια ζώσης ή εξ αποστάσεως, που αφορούν θέματα σχετικά με την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

19) Στις διάφορες ιστοσελίδες που επισκέπτεστε, πόσο συχνά διαβάζετε για την πολιτική τους για τα cookies και για τις πολιτικές ασφαλείας και προστασίας της ιδιωτικότητας που έχουν αναρτήσει;

Ποτέ	Σπάνια	Μερικές φορές	Συχνά	Πάντα

20) Σε ποιο βαθμό πιστεύετε ότι υπάρχει πιθανότητα να σας συμβεί ένα απο τα πιο κάτω κατά την περιήγηση σας στο διαδικτυακό χώρο;

	Καθόλου	Μικρό Βαθμό	Μέτριο Βαθμό	Μεγάλο Βαθμό	Πολύ μεγάλο Βαθμό
Ηλεκτρονική επίθεση					
Πρόκληση ζημιάς στη συσκευή σας					
Κλοπή προσωπικών σας δεδομένων					
Κλοπή συνθηματικών για τους τραπεζικούς σας λογαριασμούς					
Μόλυνση του συστήματος σας απο ιούς					
Παρακολούθηση της ηλεκτρονικής σας δραστηριότητας απο τρίτους					

Σας ευχαριστούμε πολύ για τη συμμετοχή και τον χρόνο που διαθέσατε!