

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



- Πτυχιακή Εργασία -

Ηλεκτρονικό ψάρεμα – Phishing

Νουβάκη Ελένη

Επιβλέπων καθηγητής : Χριστόφορος Νταντογιάν

Σεπτέμβριος 2023

Περίληψη

Το ηλεκτρονικό ψάρεμα (phishing) είναι μία μορφή ηλεκτρονικού εγκλήματος στο οποίο χρησιμοποιείται η τεχνική της κοινωνικής μηχανικής. Με τους ρυθμούς ανάπτυξης της τεχνολογίας, εκτός από όλα τα οφέλη που προσφέρει, δημιουργεί και κακόβουλες ενέργειες. Κατά τη διάρκεια της πανδημίας του κορονοϊού που ξέσπασε το 2019, αφότου άρχισε ο εγκλεισμός της καραντίνας (2020), παρατηρήθηκε αύξηση στις επιθέσεις αλλά και στα θύματα phishing. Στην παρούσα πτυχιακή εργασία θα μελετηθούν έρευνες και ορισμοί για το ηλεκτρονικό έγκλημα και πιο συγκεκριμένα για το ηλεκτρονικό ψάρεμα. Στόχος, είναι η πληροφόρηση των χρηστών για τους κινδύνους που εγκυμονεί το διαδίκτυο καθώς και η ενημέρωση τους όσον αφορά το κομμάτι της πρόληψης για την αποφυγή του ηλεκτρονικού ψαρέματος. Πάνω στον προαναφερόμενο στόχο, διεκπεραιώθηκε μια ποσοτική έρευνα με την χρήση ερωτηματολογίου, που αποσκοπούσε στο να διαπιστωθεί το ποσοστό ενημερότητας των ανθρώπων που χρησιμοποιούν το διαδίκτυο αλλά και για να εντοπιστούν οι ευπάθειες των θυμάτων. Τα αποτελέσματα επιβεβαίωσαν την αξιοπιστία των προηγούμενων επιστημονικών ερευνών σχετικά με τα δημογραφικά χαρακτηριστικά των θυμάτων. Παρόλα αυτά, η έρευνα μας φέρνει στο προσκήνιο νέα ευρήματα, τα οποία είναι ιδιαίτερα σημαντικά όσον αφορά την ασφαλή πλοήγηση στο διαδίκτυο. Ένα από αυτά είναι πως ακόμη κι αν κάποιος δεν πραγματοποιεί online αγορές, δεν σημαίνει ότι δεν μπορεί να πέσει θύμα phishing. Επίσης, από τα συμπεράσματα της έρευνας, διαφαίνεται η σημασία της εκπαίδευσης και της ενημέρωσης για την ασφαλή χρήση του διαδικτύου, καθώς αναδεικνύεται και η σημασία της ενεργούς επίβλεψης από τους γονείς και τους κηδεμόνες σχετικά με τις δραστηριότητες των παιδιών τους στο διαδίκτυο. Η παρούσα πτυχιακή εργασία συντάχθηκε με σκοπό την προφύλαξη των χρηστών του διαδικτύου από ηλεκτρονικά εγκλήματα, αλλά κυρίως από επιθέσεις ηλεκτρονικού ψαρέματος.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Χριστόφορο Νταντογιάν, επίκουρο καθηγητή στο τμήμα Πληροφορικής του Ιονίου Πανεπιστημίου, για την καθοδήγηση που μου πρόσφερε και τον χρόνο που διέθεσε δίνοντάς μου χρήσιμες συμβουλές και οδηγίες για την ολοκλήρωση της πτυχιακής μου εργασίας. Στο ίδιο πλαίσιο ευγνωμοσύνης, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του τμήματος Πληροφορικής για την συμβολή τους στην επιστημονική και τεχνολογική μου συγκρότηση στα χρόνια φοίτησής μου στο Τμήμα, καθώς και την έμπνευση που μου προσέφεραν από τις διαλέξεις τους πάνω στην έρευνα μου.

Οφείλω επίσης ένα μεγάλο ευχαριστώ σε όλους εκείνους που συνέβαλαν είτε πρακτικά (π.χ. συμπλήρωση ερωτηματολογίου) είτε ψυχικά (βοήθεια και παραινέσεις) στην ολοκλήρωση των σπουδών μου.

Τέλος, ένα μεγάλο ευχαριστώ στους γονείς μου για την οικονομική τους υποστήριξη, καθώς και τους συγγενείς και τους φίλους για την ηθική και ψυχολογική υποστήριξη σε όλο το διάστημα των σπουδών μου.

Περιεχόμενα

Περίληψη.....	i
Ευχαριστίες.....	ii
Εισαγωγή.....	1
Κεφάλαιο 1°.....	2
Ορισμοί.....	2
1. Ορισμός Διαδικτύου.....	2
2. Ορισμός Ηλεκτρονικού Εγκλήματος.....	3
Hacking/Cracking.....	4
Επιθέσεις άρνησης Εξυπηρέτησης.....	4
Κακόβουλο Λογισμικό.....	5
Spamming.....	6
Επιθέσεις σε Site.....	6
Πειρατεία Λογισμικού.....	6
Νιγηριανά Μηνύματα.....	6
Πλαστοπροσώπια.....	7
Διακίνηση παιδικού πορνογραφικού υλικού.....	7
Cyberbullying.....	8
Διαδικτυακή τρομοκρατία.....	8
Ηλεκτρονικό Ψάρεμα-Phishing.....	9
Κεφάλαιο 2ο.....	10
Ηλεκτρονικό Ψάρεμα.....	10
1. Ορισμός Ηλεκτρονικού Ψαρέματος.....	10
2. Ιστορία.....	11
3. Μορφές Ηλεκτρονικού Ψαρέματος (Phishing).....	11
4. Χαρακτηριστικά Θυμάτων.....	14
5. Phishing στην περίοδο του Covid-19.....	16
6. Τρόποι αντιμετώπισης.....	18
Κεφάλαιο 3ο.....	21
Σχετικά με την Νομοθεσία του Ηλεκτρονικού Εγκλήματος.....	21
Παγκόσμια Νομοθεσία για το Ηλεκτρονικό Έγκλημα.....	21
Ελληνική Νομοθεσία Ηλεκτρονικού Εγκλήματος.....	23

Κεφάλαιο 4ο.....	28
Ανάλυση Ερευνών.....	28
Παραδείγματα από θύματα και απάτες.....	31
Κεφάλαιο 5ο.....	36
Μεθοδολογία Έρευνας.....	36
Αποτελέσματα έρευνας και ανάλυση δεδομένων.....	37
Συμπεράσματα.....	42
Παράρτημα.....	43
Ερωτηματολόγιο.....	43
Γραφήματα Ερωτηματολογίου.....	49
Βιβλιογραφία.....	62

Περιεχόμενα Γραφημάτων

Γράφημα 1: Μορφωτικό επίπεδο ερωτηθέντων της έρευνας.....	35
Γράφημα 2: Εύρος ηλικίας ερωτηθέντων της έρευνας.....	35
Γράφημα 3: Ποιές ηλεκτρονικές αγορές έχουν στην κατοχή τους.....	36
Γράφημα 4: Εάν έχουν πέσει θύμα Phishing και γνωρίζουν αν μια ιστοσελίδα είναι αξιόπιστη για ηλεκτρονικές αγορές.....	36
Γράφημα 5: Πόσοι από τους ερωτηθέντες έχουν λάβει Phishing Email.....	37
Γράφημα 6: Πόσοι από τους ερωτηθέντες έχουν λάβει Phishing SMS.....	37
Γράφημα 7: Μορφωτικό επίπεδο θυμάτων Phishing.....	38
Γράφημα 8: Πόσες ώρες χρησιμοποιούν το διαδίκτυο όσοι έπεσαν θύμα phishing;.....	38
Γράφημα 9: Σύγκριση αν οι χρήστες γνωρίζουν το Phishing και ποια είναι ο κύριος λόγος χρήσης του διαδικτύου (ψυχαγωγία ή εργασία/εκπαίδευση).....	39
Γράφημα 10: Ποσοστά ανηλίκων που ζητάνε άδεια ενήλικα για την πραγματοποίηση ηλεκτρονικών αγορών.....	40

Περιεχόμενα Εικόνων

Εικόνα 1: Παράδειγμα Phishing SMS κατά την διάρκεια της πανδημίας του κορονοϊού.....	17
Εικόνα 2: Phishing Μήνυμα από Ελτά για επιβεβαίωση παράδοσης.....	31
Εικόνα 3: Phishing Μήνυμα από ACS Κύπρου για επαλήθευση τοποθεσίας.....	31
Εικόνα 4: Phishing Email με αλλαγή της ονομασίας ελάχιστα. Από ΕΛΤΑ, σε ΕΑΤΑ.....	31
Εικόνα 5: Phishing SMS από μεταφορική εταιρεία για επιβεβαίωση παράδοσης.....	32
Εικόνα 6: Phishing SMS κατά σειρά, με απειλή χρέωσης τελωνείου εάν δεν προβεί στην επίσκεψη του συνδέσμου ή την πληρωμή μέσω αυτού.....	32
Εικόνα 7: Phishing μήνυμα εικονικά από την κυβέρνηση.....	33
Εικόνα 8: Phishing μήνυμα για μισθωτήριο ακίνητης περιουσίας.....	33
Εικόνα 9: Phishing SMS από το Netflix με απειλή απενεργοποίηση λογαριασμού.....	34

Εισαγωγή

Σήμερα ζούμε σε μια εποχή όπου η τεχνολογία έχει εντυφώσει στην καθημερινή μας ζωή, είτε την αποδεχόμαστε είτε όχι. Διάφορες πτυχές, όπως τα κινητά τηλέφωνα και η αυτοματοποίηση των τραπεζικών συναλλαγών, μέσω της υποχρεωτικής αποδοχής τραπεζικών καρτών σε κάθε είδους καταστήματα (τόσο εμπορικά όσο και εστίασης), έχουν γίνει αναπόσπαστα στοιχεία της ρουτίνας μας. Επιπλέον, οι πλατφόρμες κοινωνικής δικτύωσης έχουν ενταχθεί με τέτοιο τρόπο στην καθημερινή ζωή των ανθρώπων, ανεξαρτήτως ηλικίας, με αποτέλεσμα να είναι πλέον σπάνιο να συναναστραφεί κανείς με ανθρώπους απομονωμένους από το κόσμος του διαδικτύου.

Οι προαναφερθείσες περιπτώσεις αποτελούν παράδειγμα της προοδευτικής ενσωμάτωσης της τεχνολογίας στην καθημερινή ζωή των ανθρώπων, οδηγώντας σε μια πιο ψηφιακή και αυτοματοποιημένη ύπαρξη. Ωστόσο, αυτή η μεταμόρφωση έχει προκαλέσει ένα ανησυχητικό ζήτημα -το έγκλημα στον κυβερνοχώρο- το οποίο παρουσιάζει αυξητική τάση από την αρχή της εμφάνισης του διαδικτύου. Μια εξέχουσα μορφή εγκλήματος στον κυβερνοχώρο είναι το ηλεκτρονικό ψάρεμα (Phishing), ιδιαίτερα διαδεδομένη στις διαδικτυακές απάτες.

Πρωταρχικός μας στόχος είναι να διερευνήσουμε την έννοια του ηλεκτρονικού ψαρέματος - Phishing, εξετάζοντας τις διάφορες εκφάνσεις αυτού του είδους εγκλήματος. Στόχος μας είναι να εντοπίσουμε τα άτομα που είναι πιο επιρρεπή στο να πέσουν θύματα και θα διερευνήσουμε επίσης τις τακτικές που χρησιμοποιούν οι δράστες, με σκοπό να ευαισθητοποιήσουμε τους χρήστες και ενδεχομένως να τους βοηθήσουμε να αποφύγουν τέτοιου είδους επιθέσεις. Επιπλέον, θα εμβαθύνουμε στα νομοθετικά μέτρα που ισχύουν για την αντιμετώπιση αυτής της μορφής εγκλήματος, όχι μόνο σε παγκόσμιο αλλά κυρίως σε εθνικό επίπεδο.

Στο πρώτο κεφάλαιο θα αναφέρουμε μερικούς ορισμούς από το υπόβαθρο του ηλεκτρονικού ψαρέματος, όπως τι είναι το διαδίκτυο και τι ορίζεται ως ηλεκτρονικό έγκλημα. Στο δεύτερο κεφάλαιο θα αναλύσουμε το ηλεκτρονικό ψάρεμα εκτενώς, δηλαδή εκτός από τον ορισμό του, θα παραθέσουμε τις κατηγορίες που απαρτίζουν το ηλεκτρονικό ψάρεμα, τους τρόπους που διαλέγουν οι θύτες να επιτεθούν στον χρήστη, τα χαρακτηριστικά ενός θύματος που θα πέσει στις “καλοφτιαγμένες παγίδες” του θύτη, αλλά και την επιρροή που είχε η πανδημία Covid-19 στο Phishing. Στο τρίτο κεφάλαιο θα παραθέσουμε την νομοθεσία που καλύπτει τα εγκλήματα στον κυβερνοχώρο, θα παρουσιάσουμε τα άρθρα του ποινικού κώδικα που το καλύπτουν νομοθετικά. Στο τέταρτο κεφάλαιο θα σχολιάσουμε τα στοιχεία από άλλες έρευνες που έχουν περατωθεί σχετικές με το θέμα αυτό και θα δώσουμε μερικά παραδείγματα ηλεκτρονικού ψαρέματος που έχουν πραγματοποιηθεί σε βάθος χρόνου. Στο πέμπτο κεφάλαιο θα παρουσιάσουμε την έρευνα που περατώθηκε στα πλαίσια της πτυχιακής εργασίας σχετικά με το ηλεκτρονικό ψάρεμα, την συχνότητα που παρουσιάζει το φαινόμενο αυτό στις μέρες μας.

Κεφάλαιο 1°

Ορισμοί

Σε αυτό το κεφάλαιο παρουσιάζονται μερικοί ορισμοί με χρήσιμους όρους για την κατανόηση του ηλεκτρονικού ψαρέματος (Phishing). Οι παρακάτω ορισμοί κάνουν εισαγωγή για την ανάλυση του Phishing, διότι είτε είναι κατηγορίες στις οποίες ανήκει, είτε πυλώνες για την περαιτέρω συζήτηση του θέματος της παρούσας πτυχιακής εργασίας.

1. Ορισμός Διαδικτύου

“Το διαδίκτυο, ή αλλιώς internet, είναι ένα παγκόσμιο δίκτυο μέσω του οποίου συνδέονται υπολογιστές και δίκτυα υπολογιστών που είναι εγκατεστημένα σε πανεπιστήμια, βιβλιοθήκες, επιχειρήσεις, ιδρύματα και οργανισμούς και επιτυγχάνεται η μεταξύ τους επικοινωνία καθώς και η παροχή στον χρήστη διαφόρων υπηρεσιών”, είναι ο ορισμός που δίνει για τον όρο διαδίκτυο ο κ.Μπαμπινιώτης στο λεξικό της ελληνικής γλώσσας. (Bampiniotis, 2002) Το διαδίκτυο χρησιμοποιείται πλέον σε κάθε νοικοκυριό αλλά και σε φορητές συσκευές όπως είναι τα smartphones και τα tablets. Ανήκει στην καθημερινότητα του μέσου ανθρώπου αλλά και σε ακραίες περιπτώσεις η ανεξέλεγκτη χρήση του μπορεί να προκαλέσει και εθισμό. Με λίγα λόγια, η χρήση του διαδικτύου απαρτίζει ένα μέρος της ζωής του ανθρώπου και είναι αμέσως επόμενο να αναπτυχθούν όλων των ειδών οι συνήθειές του σε αυτό. Παράδειγμα αποτελούν τα διάφορα είδη εξαπάτησης που έχουν δημιουργηθεί μέσω του διαδικτύου.

Παρόλο που το διαδίκτυο έχει δημιουργήσει αρκετά προβλήματα, έχει λύσει άλλα τόσα. Η ένταξη του διαδικτύου στην ζωή του ανθρώπου ήρθε για διαφορετικούς σκοπούς χρήσης. Ενώ σήμερα το διαδίκτυο χρησιμοποιείται κατά κύρια βάση για την επικοινωνία, το εμπόριο και την ψυχαγωγία, η απόκτηση της ιδέας τού ήταν κατά την περίοδο του Ψυχρού πολέμου στις ΗΠΑ, όπου είχε τεθεί το ερώτημα εάν θα καταρρεύσει η επικοινωνία του αμερικανικού πενταγώνου, μετά την ανακάλυψη των ατομικών όπλων. Με αυτή την ιστορική αναδρομή για την δημιουργία του διαδικτύου, μπορούμε να αντιληφθούμε ότι ο σκοπός του διαδικτύου τότε ήταν αποκλειστικά για την επικοινωνία σε τυχόν πόλεμο μεταξύ των ανώτερων δυνάμεων. (Μυλωνάς, 2009)

Σε γενικές γραμμές, το διαδίκτυο έχει την δική του ξεχωριστή θέση στην ρουτίνα του ανθρώπου και σχεδόν ποτέ δεν απουσιάζει από αυτή. Ο άνθρωπος το αποδέχτηκε με τα χρόνια και επένδυσε σε αυτό, αντιλαμβανόμενος την θετική επιρροή που έχει στις καθημερινές δραστηριότητες και την ελαχιστοποίηση του χρόνου διεκπεραίωσης τους. Το πρόβλημα ξεκινάει όταν εξαρτάται από αυτό ο άνθρωπος, όπως για παράδειγμα ένα πρόσφατο δημιούργημα της εποχής, το ChatGPT. Η νέα ανακάλυψη της τεχνητής νοημοσύνης είναι τόσο αξιοθαύμαστη έως και ανησυχητικά απειλητική για τον άνθρωπο, δίνοντας του την ευχέρεια να έχει έτοιμη πληροφορία σε οποιοδήποτε τομέα αναζητάει. Αυτό μπορεί να προκαλέσει σοβαρά προβλήματα στην εξέλιξη του ανθρώπου, γι'αυτό καλό είναι να γίνει έλεγχος της χρήσης του. Η ραγδαία εξέλιξη της τεχνολογίας μέχρι σήμερα, παρόλο που έχει συντελέσει τόσο θετικά τόσο και αρνητικά, παραμένει κατά κύριο λόγο για την διευκόλυνση των δραστηριοτήτων του ανθρώπου, είτε για κοινωνικές

σχέσεις, είτε για αυτοματοποίηση της εργασίας. Τέλος, αξίζει να σημειωθεί πως το διαδίκτυο έχει ενώσει τον κόσμο ολόκληρης της υφηλίου και έχει δώσει την δυνατότητα να διευρυνθούν οι ορίζοντες σε όλους τους τομείς του ανθρώπου.

2. Ορισμός Ηλεκτρονικού Εγκλήματος

Από τις αρχές της επαφής του ανθρώπου με το διαδίκτυο ξεκίνησε η επινόηση τρόπων εξαπάτησης των υπόλοιπων χρηστών. Στις αρχές, πολλές φορές, δεν αποσκοπούσε στην καταστροφή δεδομένων ή περιουσίας, αλλά κυρίως για την επίδειξη της ικανότητας χρήσης του ηλεκτρονικού υπολογιστή. Δεν υπάρχει ένας κοινός ορισμός που να καθορίζει το ηλεκτρονικό έγκλημα. Παρόλα αυτά, ένας εύστοχος ορισμός που θα μπορούσε να διατυπωθεί ορίζει το Ηλεκτρονικό έγκλημα ως τις αξιόποινες εγκληματικές πράξεις που τελούνται με την χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία”. Χωρίζεται σε δύο κατηγορίες, με γνώμονα την νομοθεσία και την τέλεσή του, σε Computer Crimes -για τα εγκλήματα που πραγματοποιούνται με την χρήση ηλεκτρονικού υπολογιστή και σε Κυβερνοεγκλήματα (Cyber Crimes) - όταν πραγματοποιούνται μέσω του διαδικτύου. (Λυκούρεσης & Φραντζέσκου, n.d.) Άλλοι ορισμοί περιγράφουν το ηλεκτρονικό έγκλημα ως το έγκλημα που σχετίζεται με υπολογιστή, δίκτυο ή τεχνολογία πληροφοριών, ή τις επιβλαβείς πράξεις που διαπράττονται από έναν υπολογιστή ή ένα δίκτυο. Σε γενικές γραμμές, ο πιο ολοκληρωμένος ορισμός πάνω στο ηλεκτρονικό έγκλημα το καθιστά ως παράνομη, ανήθικη ή μη εγκεκριμένη συμπεριφορά που σχετίζεται με την αυτόματη επεξεργασία και διαβίβαση δεδομένων. (Μπενέτου, 2021)

Το ηλεκτρονικό έγκλημα θεωρείται ένας όρος πολυδιάστατος, διότι έχει πολλά χαρακτηριστικά στα οποία μπορεί ο θύτης να βασιστεί ώστε να δράσει ανενόχλητος. Αρχικά, τον καλύπτει σε πολλές περιπτώσεις η ανωνυμία. Είναι γνωστό ότι με λίγες γνώσεις στην χρήση του διαδικτύου, μπορεί κανείς να πλοηγείται χωρίς να αφήνει τα “ίχνη” του. Από αυτό επωφελούνται οι εγκληματίες, δίνοντάς τους την ελευθερία να διαπράττουν κάθε είδους απάτη. Ένα άλλο χαρακτηριστικό του διαδικτύου είναι η διεθνής χρήση του. Οι χρήστες μπορούν να επικοινωνούν μεταξύ τους από κάθε άκρη της Γης. Με αυτόν τον τρόπο, καθίσταται δύσκολος ο εντοπισμός του θύτη -εγκληματία, εφόσον θα μπορούσε και ο ίδιος να βρίσκεται σε οποιοδήποτε άκρο της Γης. Από την άλλη πλευρά και για τους εγκληματίες του διαδικτύου υπάρχει μία δυσκολία παραπάνω στην επίτευξη της απάτης, εφόσον αναπτύσσονται συνεχώς μέτρα ασφαλείας, ώστε να προληφθούν τέτοιες ενέργειες. Αυτό όμως δεν τους εμποδίζει. Αντιθέτως, συνεργάζονται μεταξύ τους ώστε να χωρίσουν το “φόρτο” εργασίας τους αλλά και να μοιραστούν τις γνώσεις τους για τους ηλεκτρονικούς υπολογιστές. Η γνώση αυτή τους είναι απαραίτητη ώστε να καταφέρουν οποιαδήποτε απάτη στο διαδίκτυο.

Το ηλεκτρονικό έγκλημα αναπτύχθηκε μετά την εμφάνιση του πρώτου σύγχρονου υπολογιστή, Arpanet. Ο Bob Thomas, το 1971, δημιούργησε το πρώτο λογισμικό για την καταπολέμηση ιού, το Creeper. Ο ίδιος δεν είχε καμία πρόθεση να πραγματοποιήσει κακόβουλες ενέργειες. Εν αντιθέσει, το πρώτο έγκλημα στον κυβερνοχώρο εμφανίστηκε το 1820, όταν ο Joseph-Marie Jacquard εφηύρε τον αργαλειό και οι υπάλληλοί του προσπάθησαν να τον σαμποτάρουν, με τον φόβο ότι θα χάσουν την δουλειά τους από αυτό

το μηχανήμα. Λόγω της ελλιπούς ενημέρωσης του χρήστη για το τι ορίζεται ως ηλεκτρονικό έγκλημα και με ποιον τρόπο διαπράττεται, καθώς και το γεγονός ότι οι ταινίες επιστημονικής φαντασίας παρουσιάζουν κινηματογραφικά επιτελεσμένους τρόπους εγκλήματος, η φαντασία του ανθρώπου πλάθει διάφορους μύθους για αυτό. (Μπενέτου, 2021)

Μορφές Κυβερνοεγκλήματος

Το Ηλεκτρονικό Έγκλημα κατηγοριοποιείται με βάση την νομοθεσία σε εγκλήματα κοινού ποινικού δικαίου και σε εγκλήματα του κυβερνοχώρου. Στην πρώτη κατηγορία ανήκουν τα εγκλήματα που μπορούν να λάβουν χώρα τόσο σε φυσικό όσο και διαδικτυακό περιβάλλον, ενώ στην δεύτερη κατηγορία είναι τα γνήσια ηλεκτρονικά εγκλήματα που διαπράττονται αποκλειστικά με την χρήση του διαδικτύου. Παρακάτω αναλύονται μερικές γνωστές μορφές του ηλεκτρονικού εγκλήματος που είναι απαραίτητες να γνωρίζει ο κάθε χρήστης τόσο του Η/Υ αλλά και του διαδικτύου.

Hacking/Cracking

Το Hacking και το Cracking αφορούν την παραβίαση ενός συστήματος χωρίς να έχει εξουσιοδοτηθεί. Με άλλα λόγια είναι η απόκτηση πρόσβασης σε ένα σύστημα (σε έναν Η/Υ ή ακόμη και δίκτυο υπολογιστών) χωρίς να υπάρχει άδεια πρόσβασης σε αυτό. Η διαφορά των δύο εννοιών έρχεται στο επόμενο βήμα της μη εξουσιοδοτημένης χρήσης. Πιο συγκεκριμένα, οι “θύτες” μετονομάζονται crackers (cracking) στην περίπτωση που επιδιώξουν να προσθέσουν, αφαιρέσουν ή παραποιήσουν γενικότερα τα δεδομένα προς όφελός τους, αφότου αποκτήσουν πρόσβαση στο σύστημα. Εάν όμως έχουν σκοπό να παραβιάσουν ένα σύστημα ώστε να αποδείξουν τις ευπάθειες του και να προστατέψουν τον χρήστη ενημερώνοντας τον για αυτές, στην περίπτωση αυτή ονομάζονται hackers (hacking). Τους hackers πολλές φορές τους αναθέτουν οι ίδιες οι εταιρείες να προσπαθήσουν να παραβιάσουν το σύστημά τους, με σκοπό να ανακαλύψουν τα κενά ασφαλείας και να τα διορθώσουν.

Επιθέσεις άρνησης Εξυπηρέτησης

Οι επιθέσεις άρνησης εξυπηρέτησης πραγματοποιούνται από τον θύτη με σκοπό να υπερφορτώσουν σε εργασίες το σύστημα (υπολογιστής/ιστοσελίδα) ώστε να μην μπορεί να εξυπηρετεί τους χρήστες του ή για να καταρρεύσει. Τέτοιου είδους είναι οι επιθέσεις Denial of Service - DoS στις οποίες είτε πολλοί χρήστες στέλνουν μαζικά αιτήματα χρήσης του συστήματος, είτε ένας θύτης (ή σε συνεργασία με άλλους) στέλνει εικονικά ή και πολλαπλά αιτήματα στο σύστημα, με αποτέλεσμα την υπερφόρτωση του. Ένα γνωστό παράδειγμα επίθεσης άρνησης εξυπηρέτησης συνέβη τον Ιούνιο 2023 στην Microsoft, η οποία επιβεβαίωσε πως δέχτηκε επίθεση DoS επιπέδου 7. Μία επίθεση άρνησης εξυπηρέτησης επιπέδου 7 είναι όταν οι απειλητικοί φορείς στοχεύουν στο επίπεδο της εφαρμογής, κατακλύζοντας τις υπηρεσίες με τεράστιο όγκο αιτημάτων, προκαλώντας έτσι την παύση λειτουργίας των υπηρεσιών, με αποτέλεσμα την αδυναμία

επεξεργασίας όλων των δεδομένων. (Lawrence, 2023) Μια αξιοσημείωτη και αξέχαστη επίθεση DDos (Distributed Denial of Service) ήταν η επίθεση των Ανώνυμων το 2010, οι οποίοι επιτέθηκαν την PayPal, την MasterCard και την Visa ως αντίποινα που σταμάτησαν να πραγματοποιούν δωρεές προς την ομάδα WikiLeaks. Το αντίκτυπο της επίθεσης αυτής ήταν αρκετά δυσμενές, αφού μόνο για την PayPal η ζημία υπολογίστηκε στα 5,5 εκατομμύρια δολάρια των Ηνωμένων Πολιτειών (USD). Επίσης, τον Απρίλιο του 2018 αναφέρθηκε πως η πρόσβαση σε έναν ιστότοπο προσφερόταν έναντι 14,99USD σε όποιον επιθυμούσε να πραγματοποιήσει επίθεση DDoS. (Sarre et al., 2018)

Κακόβουλο Λογισμικό

Οι επιθέσεις με κακόβουλο λογισμικό (Malware) είναι ένα φαινόμενο που πλήττει τους χρήστες των Η/Υ. Πλέον τα λογισμικά αυτά μεταδίδονται και στα κινητά τηλέφωνα (Smartphones). Ο σκοπός αυτού του είδους λογισμικού είναι κυρίως για λόγους οικονομικού σφετερισμού. Τα κακόβουλα λογισμικά έχουν πολλές μορφές, τις οποίες ο άνθρωπος τις έχει ονοματίσει με βάση την συμπεριφορά τους. Παράδειγμα αποτελούν οι δούρειοι ίπποι (Trojan horses), οι ιοί (viruses), τα σκουλήκια (worms) και τα λογισμικά υποκλοπής (Spyware). Κάθε ένα από αυτά παραβιάζει την ασφάλεια του Η/Υ του χρήστη με ή χωρίς την άδειά του. Τις περισσότερες φορές, όταν ο χρήστης δίνει την άδεια στο κακόβουλο λογισμικό να εγκατασταθεί στον υπολογιστή του, γίνεται εν αγνοία του. Αυτό συμβαίνει διότι παρουσιάζεται σαν ένα γνωστό/“νόμιμο” πρόγραμμα αποκτώντας την εμπιστοσύνη του χρήστη. [22]

Οι δούρειοι ίπποι (Trojan horses) είναι ένα κακόβουλο λογισμικό που παρουσιάζεται σαν να μην είναι βλαβερό στον υπολογιστή. Το όνομά τους το προκύπτει από τον Δούρειο ίππο που είχε σταλεί στην Τροία από τον Οδυσσέα σαν δώρο ειρήνης. Έτσι και αυτό το λογισμικό παρουσιάζεται στον χρήστη σαν ένα πρόγραμμα, φαινομενικά έμπιστο, αλλά στην πορεία εισβάλλει στα αρχεία και στα δεδομένα του υπολογιστή τα οποία ενδεχομένως και να τα καταστρέψει.

Οι ιοί (viruses) είναι προγράμματα τα οποία προσκολλώνται σε άλλα προγράμματα ή και στα αρχεία του υπολογιστή και μεταδίδονται μέσω δικτύου ή από συσκευές αποθήκευσης (Usb stick, σκληρός δίσκος κ.α.). Η λειτουργία τους μοιάζει με τους ιούς που έχει να διαχειριστεί και ο ανθρώπινος οργανισμός. Όπως δηλαδή μπορεί ένας άνθρωπος να κολλήσει μία ίωση και να αρχίσει να καταρρέει ολόκληρο το ανοσοποιητικό του σύστημα, έτσι και με τον υπολογιστή του χρήστη. Όταν εισβάλλει το κακόβουλο λογισμικό, ένας ιός, μπορεί να διαγραφούν αρχεία, να αλλοιωθούν δεδομένα, ακόμη και να διαταραχτεί η λειτουργία του συστήματος.

Τα σκουλήκια ή αλλιώς worms, μοιάζουν αρκετά με τους ιούς γιατί και αυτά μεταδίδονται από υπολογιστή σε υπολογιστή. Τα worms μπορούν να αναπαραχθούν στο σύστημα που είναι εγκατεστημένα αλλά και να μεταδοθούν όλα μαζί στο επόμενο σύστημα. Το πρόβλημα που δημιουργεί αυτό το κακόβουλο λογισμικό είναι να γεμίζει ο χώρος μνήμης του υπολογιστή αλλά και πολλές φορές και το bandwidth (εύρος ζώνης δεδομένων) με αποτέλεσμα να μην μπορεί να εκτελεστεί η φυσιολογική λειτουργία του υπολογιστή, του web server ή του network server.

Spamming

Το spam είναι η διαδικασία αποστολής μαζικών ή μεμονωμένων μηνυμάτων, διαφημιστικού περιεχομένου, τα οποία ο χρήστης δεν έχει ζητήσει αλλά ούτε έχει επιβεβαιώσει την συνδρομή του σε αυτά. Ως “spamming” θεωρείται και η συνεχόμενη αποστολή μηνυμάτων με οποιοδήποτε μέσω, όχι απαραίτητα διαφημιστικό ή παραπλανητικό, το οποίο ο παραλήπτης δεν επιθυμεί ή/και θεωρεί ενοχλητικό. Πολλές φορές, το περιεχόμενο αυτών των μηνυμάτων δεν είναι έμπιστο (μπορεί να παραμονεύει τυχόν άλλη ηλεκτρονική επίθεση). Ένα τρανταχτό παράδειγμα χρήσης spamming μηνυμάτων για κυβερνοεπίθεση είναι το ηλεκτρονικό ψάρεμα -phishing.

Επιθέσεις σε Site

Οι επιθέσεις σε ιστοσελίδες γίνονται για να δυσφημίσουν ή να καταστρέψουν το περιεχόμενο τους. Ο κυριότερος λόγος που πραγματοποιούνται αυτού του είδους επιθέσεις, είναι για να χαθεί η εμπιστοσύνη των χρηστών για την ιστοσελίδα και κατ’ επέκταση για όλη την επιχείρησης (πχ στο e-banking μίας τράπεζας). Συνήθως πραγματοποιούνται με τη χρήση ενός κακόβουλου κώδικα που μπορεί να αποσταλεί στον ιστότοπο μέσω του URL και να εκτελεστεί μόλις τρέξει η σελίδα στον χρήστη. Στην ουσία, ο χρήστης πρέπει να γίνει “συνένοχος” σε αυτήν την επίθεση, κάνοντας κλικ στον σύνδεσμο της ιστοσελίδας.

Πειρατεία Λογισμικού

Η πειρατεία λογισμικού μπορεί να πραγματοποιηθεί σχεδόν από τον μισό πληθυσμό που τυγχάνουν να είναι απλοί χρήστες ηλεκτρονικού υπολογιστή. Ως πειρατεία λογισμικού ορίζεται η αντιγραφή/κοινή χρήση της άδειας του λογισμικού σε περισσότερες συσκευές από αυτές που έχει ορίσει η υπάρχουσα άδεια χρήσης. Πολλές φορές δεν διαμοιράζεται μόνο το λογισμικό, αλλά μεταπωλείται. Δεν είναι λίγοι οι χρήστες οι οποίοι μπαίνουν σε “πειρατικές” ιστοσελίδες για να βρουν τα “σπασμένα” λογισμικά που επιθυμούν. “Σπασμένα” ονομάζονται τα λογισμικά τα οποία μπορούν να εγκατασταθούν χωρίς άδεια χρήσης. Στην πραγματικότητα, όσοι εγκαθιστούν ένα λογισμικό χωρίς να έχουν την άδεια χρήσης ή η άδεια χρήσης που έχουν δεν εγκρίνει τον αριθμό υπολογιστών στους οποίους το έχουν εγκαταστήσει, παραβαίνουν τον νόμο και τα πνευματικά δικαιώματα των δημιουργών.

Νιγηριανά Μηνύματα

Η συγκεκριμένη απάτη αφορά έναν θύτη που αποσκοπεί στην οικονομική χρέωση του θύματος με την παραπλάνηση του μέσω μηνυμάτων. Πιο συγκεκριμένα, ο θύτης παρουσιάζει μία ιστορία στο θύμα μέσω μηνύματος στην οποία παρουσιάζεται ο ίδιος να μην έχει άλλη επιλογή. Ζητάει λοιπόν από το θύμα να τον εξυπηρετήσει μεταφέροντας του κάποιο χρηματικό ποσό σε έναν άλλον τραπεζικό λογαριασμό. Τα

θύματα συνήθως πέφτουν στην παγίδα επειδή τους υπόσχονται κάποια αμοιβή σε αντάλλαγμα της εξυπηρέτησης. Έτσι είτε δίνουν τα στοιχεία του τραπεζικού τους λογαριασμού είτε κάνουν οι ίδιοι την μεταφορά των χρημάτων, με αποτέλεσμα ο θύτης αμέσως μετά να κόψει την επικοινωνία έχοντας πάρει αυτό που επιθυμεί. Στην περίπτωση που έχουν δώσει τα θύματα τα στοιχεία του τραπεζικού λογαριασμού, ο θύτης προσπαθεί να κάνει ανάληψη όσο δυνατόν μεγαλύτερο χρηματικό ποσό του επιτρέπεται.

Πλαστοπροσωπία

Η πλαστοπροσωπία δεν θεωρείται πρόσφατο αδίκημα, μιας και είναι συχνό φαινόμενο εδώ και πολλές δεκαετίες. Ένα τρανταχτό και συνάμα ιστορικό παράδειγμα πλαστοπροσωπίας αφορά την αμφίεση ενός θύτη σε αστυνομικό, με σκοπό την παράδοση αντικειμένων ή την υποκλοπή προσωπικών δεδομένων. Στο σημερινό πλαίσιο, το διαδίκτυο παρουσιάζει ένα παρόμοιο τοπίο. Με βάση διάφορες αναφορές σχετικά με την πλαστοπροσωπία, μπορούμε να συμπεράνουμε ότι πρόκειται για τη μη εξουσιοδοτημένη χρήση των προσωπικών πληροφοριών κάποιου άλλου για τη συμμετοχή σε εγκληματικές δραστηριότητες. Η εμφάνιση της πλαστοπροσωπίας μέσω διαδικτύου μπορεί να εντοπιστεί στα μέσα της δεκαετίας του 1990.

Η πλαστοπροσωπία μπορεί να λάβει διάφορες μορφές. Οι μέθοδοι που χρησιμοποιούνται για την κλοπή προσωπικών δεδομένων μπορούν να κατηγοριοποιηθούν σε δύο ομάδες: εκείνες που δεν απαιτούν προηγμένη τεχνολογία και εκείνες που εκτελούνται μέσω επιθέσεων στο διαδίκτυο. Τα ακόλουθα είναι παραδείγματα αυτών των κατηγοριών:

Μέθοδοι χαμηλής τεχνολογίας: Οι προσεγγίσεις αυτές δεν βασίζονται σε εξελιγμένη τεχνολογία. Περιλαμβάνουν δραστηριότητες όπως το ψάξιμο στα σκουπίδια του θύματος για τον εντοπισμό αποδείξεων τραπεζικών καρτών ή αρχείων πληρωμών δανείων που περιέχουν αριθμούς τραπεζικών καρτών. Μια άλλη περίπτωση είναι η υποκλοπή προσωπικών συνομιλιών για τη συλλογή ευαίσθητων πληροφοριών, η κλοπή αλληλογραφίας από γραμματοκιβώτια ή πιο προηγμένες τακτικές όπως η αλλαγή της εγγεγραμμένης διεύθυνσης του θύματος.

Μέθοδοι υψηλότερης τεχνολογίας: Για τους εγκληματίες που έχουν κλίση στην τεχνολογία, υπάρχουν προηγμένες τεχνικές για την απόκτηση προσωπικών δεδομένων. Αυτό περιλαμβάνει την αναζήτηση σε δημόσιες βάσεις δεδομένων, την εξαγωγή πληροφοριών από φυσικά καταστήματα και ΑΤΜ με τη χρήση εξωτερικών σκληρών δίσκων.

Αυτές οι διαφορετικές τεχνικές χρησιμοποιούνται από τους επιτήδειους για να πραγματοποιήσουν τις παράνομες δραστηριότητές τους, στοχεύοντας ανυποψίαστα άτομα και εκμεταλλευόμενοι τις προσωπικές τους πληροφορίες για κακόβουλους σκοπούς. (Tajpour et al., 2010)

Διακίνηση παιδικού πορνογραφικού υλικού

Μια ακόμα μορφή του ηλεκτρονικού εγκλήματος είναι η διακίνηση παιδικού πορνογραφικού υλικού. Σύμφωνα με το πρόσθετο Πρωτόκολλο της Σύμβασης του ΟΗΕ για τα δικαιώματα του παιδιού, ως

παιδική πορνογραφία ορίζεται οποιαδήποτε αναπαράσταση παιδιού, με οποιοδήποτε μέσο, εμπλεκόμενου σε πραγματικές ή εικονικές ρητές σεξουαλικές δραστηριότητες, ή κάθε απεικόνιση των γενετήσιων οργάνων παιδιού με σεξουαλικούς σκοπούς. (Αγγελάκης & Ιωσηφέλλη, 2018) Η διαδικασία που ακολουθούν ώστε να αποφύγουν τον εντοπισμό του διαμοιρασμού πορνογραφικού υλικού ανηλίκων από τις μηχανές αναζήτησης, είναι η χρήση “καμουφλαρισμένων” ιστοσελίδων, ομαδικές συνομιλίες (chat rooms), ομαδικές σελίδες (group sites) αλλά και μονταρισμένο παιδικό πορνογραφικό υλικό στο οποίο έχει ενταχθεί σε πορνογραφικό υλικό ενηλίκων.

Cyberbullying

Το Cyberbullying είναι σύνθετη λέξη και αναφέρεται στο bullying που διαπράττεται μέσω του διαδικτύου. Ο όρος bullying μεταφράζεται ως σχολικός εκφοβισμός και εκφράζει την σωματική και την ψυχολογική κακοποίηση με σκοπό την επιβολή αλλά και τον σωματικό και ψυχολογικό πόνο στο θύμα. Το φαινόμενο παρουσιάστηκε για πρώτη φορά περίπου πριν δύο δεκαετίες, όπως και η χρήση του όρου αυτού σε αντίστοιχα περιστατικά, η οποία χρησιμοποιείται πλέον και στο διαδίκτυο. Μέσω του κινητού τηλεφώνου, του υπολογιστή ή άλλων φορητών ηλεκτρονικών συσκευών που έχουν πρόσβαση στο Internet, ο “θύτης” επιλέγει το θύμα του, το οποίο βρίσκεται στον κοινωνικό του περίγυρο, και ξεκινάει να επιτίθεται σε αυτό. Οι επιθέσεις πραγματοποιούνται μέσω e-mails, μηνυμάτων στο κινητό, chat-rooms αλλά και ιστοσελίδες και πλατφόρμες κοινωνικής δικτύωσης, στις οποίες αποστέλλεται το υβριστικό ή/και ταπεινωτικό περιεχόμενο που αποσκοπεί στην εκφόβιση του θύματος. Είναι πολλά τα περιστατικά στα οποία μαθήτριες στο σχολείο δημιουργούν chat-room για να χλευάσουν ενδεχομένως κάποια άλλη συμμαθήτρια, ή τα αγόρια για να εκφοβίσουν κάποιον/α συμμαθητή/τρια μιλώντας τους υποτιμητικά και απειλώντας ότι θα ανεβάσουν κάποια ταπεινωτική φωτογραφία ή είδηση ώστε να τον φοβερίσουν.

Διαδικτυακή τρομοκρατία

Σύμφωνα με τον κ. Μπαμπινιώτη, η τρομοκρατία είναι ένα σύνολο ενεργειών για την επιβολή του τρόμου με την χρήση βίας-σωματικής/ψυχολογικής. Επίσης ορίζεται και ως ένας τρόπος διακυβέρνησης του λαού από μικρή μειοψηφία ασκώντας αυστηρά και βίαια μέτρα. (Bampiniotis, 2002) Ωστόσο, η διαδικτυακή τρομοκρατία δεν διαφέρει πολύ. Με την χρήση του διαδικτύου, συνήθως απειλείται η κυβέρνηση και δομές που θα δημιουργήσουν σοβαρό πλήγμα στην λειτουργία της καθημερινής ζωής του ανθρώπου, όπως νοσοκομεία, τράπεζες, Μέσα Μαζικής Μεταφοράς και βιομηχανίες. Τα προαναφερόμενα, διαλέγονται με σκοπό τον πανικό του λαού αλλά και ταυτόχρονα την εξόργιση που δεν διευθετούν τα αιτήματά των τρομοκρατών για να συνεχίσουν τις διαδικασίες τους στις υπηρεσίες. Η διαδικτυακή τρομοκρατία είναι μία σοβαρή μορφή ηλεκτρονικού εγκλήματος, διότι μπορεί να συμβεί μεμονωμένα σε ένα άτομο ή σε μικρή ομάδα ανθρώπων, αποσκοπώντας στην αποδυνάμωση της ψυχολογίας ή έχοντας χρηματικό κίνητρο. Στην

περίπτωση όμως που η τρομοκρατία αφορά κυβερνήσεις, το έγκλημα πλήττει ολόκληρη εθνικότητα σε ψυχολογικό, οικονομικό ή/και κοινωνικό επίπεδο.(Furnell & Warren, 1999; Jones, 2005)

Ηλεκτρονικό Ψάρεμα - Phishing

Το ηλεκτρονικό ψάρεμα, γνωστό και ως phishing, είναι μια αρκετά διαδεδομένη διαδικτυακή επίθεση που δέχονται καθημερινά οι άνθρωποι σε όλο τον κόσμο. Θα μπορούσαμε να την συγκρίνουμε με την πλαστοπροσωπία και τις επιθέσεις σε site. Με την πλαστοπροσωπία έχουν το κοινό της παραπλανητικής ταυτότητας και του ψεύτικου περιεχομένου. Με τις επιθέσεις στις ιστοσελίδες είναι όμοιες διότι όπως και στο Phishing όταν η επίθεση γίνεται με πανομοιότυπη ιστοσελίδα γνωστής υπηρεσίας, ο χρήστης του διαδικτύου χάνει την εμπιστοσύνη και την εκτίμησή του στην υπηρεσία, κάτι που λειτουργεί σαν δυσφήμιση. Στο επόμενο κεφάλαιο θα γίνει περαιτέρω ανάλυση της συγκεκριμένης μορφής διαδικτυακής επίθεσης.

Κεφάλαιο 2ο

Ηλεκτρονικό Ψάρεμα

1. Ορισμός Ηλεκτρονικού Ψαρέματος

Όπως έχει προαναφερθεί, το phishing είναι μια μορφή διαδικτυακού εγκλήματος που αποσκοπεί στην παράνομη απόκτηση προσωπικών δεδομένων, συμπεριλαμβανομένων αριθμών τραπεζικών καρτών και κωδικών πρόσβασης (που συχνά σχετίζονται με τις ηλεκτρονικές τραπεζικές συναλλαγές). Αυτός ο τύπος επίθεσης χρησιμοποιεί αυτοματοποιημένες τεχνικές για να αυξήσει το ποσοστό επιτυχίας των παραπλανητικών μηνυμάτων που αποστέλλονται από τους δράστες. Πολλές φορές οι χρήστες του διαδικτύου συνδέουν το Phishing με τα ανεπιθύμητα μηνύματα στο ηλεκτρονικό ταχυδρομείο, τα οποία έρχονται επανειλημμένα, αναζητώντας επιβεβαίωση στοιχείων σύνδεσης.(Hota et al., 2018) Το Phishing είναι κάθε ενέργεια αποστολής email σε έναν χρήστη, ισχυριζόμενοι ψευδώς την αξιόπιστη ταυτότητα μίας νόμιμης επιχείρησης, με σκοπό την εξαπάτηση του χρήστη, που θα τον ωθήσει να μοιραστεί προσωπικές πληροφορίες που θα χρησιμοποιηθούν ως πλαστοπροσωπία. Η έρευνα (Steyn et al., 2007) ορίζει επίσης το ηλεκτρονικό ψάρεμα ως ένα έγκλημα στο οποίο ο απατεώνας αποκτά βασικές προσωπικές πληροφορίες και τις χρησιμοποιεί προς όφελός του.

Οι (Darwish et al., 2012) ορίζουν το Phishing ως μία μορφή επίθεσης κοινωνικής μηχανικής κατά την οποία οι phishers, δηλαδή οι εισβολείς, εξαπατούν το θύμα για να αποκτήσουν δόλια ιδιωτικές πληροφορίες. Ως μια μορφή διαδικτυακής δραστηριότητας κατά την οποία ο επιτιθέμενος στοχεύει στην κλοπή ευαίσθητων πληροφοριών του θύματος, παρουσιάζεται στην έρευνα των (Mayuri et al., 2012) . Ο ορισμός που γενικεύει το ηλεκτρονικό ψάρεμα είναι από την πτυχιακή εργασία (Μπενέτου, 2021), στην οποία αναφέρεται πως είναι η πράξη κλοπής των ψηφιακών διαπιστευτηρίων ενός ανθρώπου, όπως για παράδειγμα κωδικοί πρόσβασης στον τραπεζικό λογαριασμό στο διαδίκτυο, τα στοιχεία της τραπεζικής κάρτας κα. Άλλος ένας ορισμός για το Phishing αναφέρει, “Η επίθεση ηλεκτρονικού ψαρέματος είναι μία τεχνική κοινωνικής μηχανικής που αποσκοπεί στην υποκλοπή των ευαίσθητων πληροφοριών ενός χρήστη ή/και για την τέλεση άλλων μορφών επιθέσεων όπως το λογισμικό λύτρων (ransomware). Το ransomware είναι μία κατηγορία κακόβουλων λογισμικών στην οποία απαιτούνται χρήματα σε αντάλλαγμα των αποκλεισμένων λειτουργιών, αρχείων κα. (Abroshan et al., 2021; Popoola et al., 2017)

Το ηλεκτρονικό ψάρεμα ανήκει στην κατηγορία επιθέσεων της κοινωνικής μηχανικής. Αυτή η κατηγορία επιθέσεων βασίζεται στον ανθρώπινο παράγοντα της αλυσίδας της ασφάλειας. Γενικότερα, ο άνθρωπος είναι ο πιο αδύναμος κρίκος στην αλυσίδα της ασφάλειας, ένα παραπάνω όμως στην ασφάλεια στο διαδίκτυο. Η κοινωνική μηχανική στηρίζεται στην ευπιστία του ανθρώπου, Πιο συγκεκριμένα, βασίζεται στο ότι θα καταφέρει να πείσει τον χρήστη να δώσει τα ευαίσθητα προσωπικά του δεδομένα, με σκοπό πάντα την οικονομική εκμετάλλευση. Σε αυτήν την τεχνική, ο επιτιθέμενος ακολουθεί τέσσερα βήματα. Πρώτα, ξεκινάει να συλλέγει πληροφορίες ώστε να σχηματίσει μία ολοκληρωμένη εικόνα και να μπορεί να

επιλέξει σωστά τον τρόπο που θα επιτεθεί. Στην συνέχεια, πρέπει να θεμελιώσει την εμπιστοσύνη με το θύμα, κάθε ένα ξεχωριστά. Αυτό μπορεί να το πετύχει με ένα απλό κοίταγμα, ένα ψεύτικο προφίλ στο διαδίκτυο ή ακόμα και ανταλλαγή πληροφοριών. Ως αποτέλεσμα, αργότερα το θύμα θα του εμπιστευτεί προσωπικές πληροφορίες ή απλά θα πατήσει κατά λάθος σε κάποιο κακόβουλο link. Το συγκεκριμένο βήμα είναι αρκετά χρονοβόρο, διότι πρέπει να γίνει ξεχωριστά για κάθε στοχευμένο θύμα. Στο τρίτο βήμα, ο επιτιθέμενος πλέον εκμεταλλεύεται την εμπιστοσύνη που κέρδισε στο προηγούμενο στάδιο και χρησιμοποιεί τις πληροφορίες που έχει συλλέξει στο πρώτο βήμα. Στο τελευταίο στάδιο, επιτίθεται με την μέθοδο που επέλεξε στα προηγούμενα βήματα. (Γιαμπουλάκης, 2017)

2. Ιστορία

Το phishing ως τεχνική ηλεκτρονικού εγκλήματος εμφανίστηκε γύρω στα μέσα της δεκαετίας του 1990. Ένα πρώιμο παράδειγμα επίθεσης ηλεκτρονικού ψαρέματος σημειώθηκε στις Ηνωμένες Πολιτείες, συγκεκριμένα στο πλαίσιο της America Online (AOL), μιας δημοφιλής εφαρμογής εξυπηρέτησης χρηστών. Το 1994, μια ομάδα αυτοαποκαλούμενων "χάκερ" ξεκίνησε μια εκστρατεία phishing με στόχο νέους χρήστες, τους οποίους αποκαλούσαν "ψάρια". Αυτοί οι επιτιθέμενοι έστειλαν απατηλά μηνύματα παριστάνοντας τους διοικητικούς εκπροσώπους της εταιρείας. Τα μηνύματα ζητούσαν από τους χρήστες να επαληθεύσουν τα στοιχεία του λογαριασμού τους, όπως κωδικούς πρόσβασης ή αριθμούς τραπεζικών καρτών, με το πρόσχημα ότι θα απένεργον την απενεργοποίηση των λογαριασμών τους. Για τη βελτιστοποίηση της λειτουργίας τους, οι επιτιθέμενοι χρησιμοποιούσαν αυτοματοποιημένες εφαρμογές ανταλλαγής μηνυμάτων και αποθήκευαν τις απαντήσεις των χρηστών στους υπολογιστές τους. Αυτό επέτρεπε στους επιτιθέμενους να ανακτούν τις πληροφορίες ακόμη και αν τα μέτρα ασφαλείας του ιστότοπου εντόπιζαν και αφαιρούσαν τα μηνύματα μετά από σύντομο χρονικό διάστημα. (Rekouché, 2011)

Η ιστορία του ηλεκτρονικού ψαρέματος σχετίζεται στενά με την εξέλιξη του διαδικτύου και των ψηφιακών επιθέσεων. Ο όρος phishing πρόκειται για μια παραλλαγή του όρου ψαρέματος (fishing – ψάρεμα κωδικών πρόσβασης) και επηρεάζεται από τον όρο phreaking (εκμετάλλευση των τηλεφωνικών συστημάτων). (Steyn et al., 2007)

3. Μορφές Ηλεκτρονικού Ψαρέματος (Phishing)

Το phishing έχει αρκετές μορφές που πραγματοποιείται. Σε κάθε μορφή ακολουθούνται τα ίδια τέσσερα βήματα που αναφέρθηκαν παραπάνω, προσαρμοσμένα στην έκτοτε περίπτωση. Ανάλογα όμως τον παράγοντα που θέλουμε να κατηγοριοποιήσουμε την επίθεση, διαφέρουν και οι κατηγορίες. Εδώ θα αναλύσουμε τις κατηγορίες σε συνάρτηση με το στόχο που θέτει ο επιτιθέμενος. Οι παρακάτω κατηγορίες είναι η εξέλιξη του Phishing.

Spear Phishing: περιλαμβάνει την αποστολή στοχευμένων μηνυμάτων “δόλωμα” σε μικρές ομάδες χρηστών που θεωρούνται πιο ευάλωτοι σε τέτοιου είδους επιθέσεις. Με το spear phishing ο επιτιθέμενος μπορεί να αποσπάσει προσωπικά δεδομένα χωρίς να βασίζεται σε phishing ιστότοπους που θα μπορούσαν

ενδεχομένως να εντοπιστούν από το ευρύτερο κοινό. Επομένως, η δραστηριότητα του επιτιθέμενου παραμένει διακριτική, καθώς δεν αποστέλλεται μαζικό μήνυμα σε άτομα που θα μπορούσαν να εντοπίσουν το ύποπτο ιστότοπο.

Whaling: το whale-phishing είναι η ίδια μέθοδος επίθεσης με το spear phishing απλώς ο στόχος γίνεται ακόμα πιο συγκεκριμένος. Στο whaling ο επιτιθέμενος επιθυμεί το θύμα να είναι ιστάμενο σε κάποια εταιρεία, με απώτερο σκοπό, να έχει πληροφορίες και πρόσβαση σε δεδομένα και αρχεία ολόκληρης της εταιρείας. Σε αυτήν την μέθοδο είναι εξίσου δύσκολο να εντοπιστεί η επίθεση, διότι είναι αρκετά συγκεκριμένη σε μικρή ομάδα ανθρώπων, με αποτέλεσμα να πέφτουν στην παγίδα πολλά θύματα.

Tabnapping: το Tabnapping είναι μία τεχνική, εξέλιξη του phishing. Ο τρόπος που λειτουργεί είναι να παρακολουθεί την περιήγηση του χρήστη σε μία ιστοσελίδα και μόλις αναγνωρίσει ότι το θύμα έχει αφήσει ανοιχτή την καρτέλα στον περιηγητή, αλλάζει το περιεχόμενο της ιστοσελίδας, συνήθως με κάποια φόρμα συμπλήρωσης (log in). Εάν ο χρήστης δεν παρατηρήσει την αλλαγή του περιεχομένου της ιστοσελίδας, θα στείλει τα διαπιστευτήριά του στο επιτιθέμενο.

Pharming: Ακόμη μία εξέλιξη του Phishing, το οποίο στοχεύει στις ιστοσελίδες που χρησιμοποιεί ο χρήστης. Ο επιτιθέμενος προσπαθεί να ανακατευθύνει τον χρήστη σε μία ιστοσελίδα, πανομοιότυπη με την αυθεντική, η οποία όμως ελέγχεται από τον θύτη. Συνήθως η συγκεκριμένη επίθεση αποτελεί σοβαρή απειλή, εφόσον είναι δύσκολο να εντοπιστεί ακόμη και από κάποιο anti-virus λογισμικό.

Vishing: Το Vishing είναι σύνθετη λέξη από το voice και το phishing. Σε αυτήν την επίθεση χρησιμοποιείται η φωνή και το ηλεκτρονικό ψάρεμα. Οι εγκληματίες καλούν το θύμα, συνήθως με ηχογραφημένο μήνυμα, και το καθοδηγούν να καλέσει ένα άλλο νούμερο ώστε να δώσει τον αριθμό του τραπεζικού λογαριασμού ή τα στοιχεία της τραπεζικής κάρτας. Κάποιες φορές το θύμα λαμβάνει κανονικό phishing email, στο οποίο, αντί να τους ανακατευθύνει σε κάποιο διαδικτυακό site, τους ζητούνται ευαίσθητες πληροφορίες δια μέσω τηλεφώνου. Για να ξεγελάσει το θύμα ο επιτιθέμενος, στην τηλεφωνική κλήση υποδύεται κάποιον προϊστάμενο σε κάποιον οργανισμό, κάποιον τεχνικό τηλεφωνικής υποστήριξης ή ακόμη και κάποιον συνάδελφο ώστε να εκμαιεύσει τα προσωπικά δεδομένα.

SMiShing: Το SmiShing είναι συνδυασμός του SMS και του phishing. Εφόσον τα smartphones είναι αναπόσπαστο κομμάτι για την καθημερινότητα του ανθρώπου, σε αυτήν την μορφή επίθεσης, αποστέλλεται ένα SMS στο κινητό του θύματος με κάποιον κακόβουλο επισυναπτόμενο ιστότοπο ώστε το θύμα να το “ανοίξει” και να συνδεθεί στον λογαριασμό του. Για να στεφθεί με επιτυχία αυτή η επίθεση, στο μήνυμα υπάρχει ένα κείμενο το οποίο παροτρύνει τον χρήστη να συνδεθεί άμεσα, διότι σε διαφορετική περίπτωση θα κλειδώσει ή θα κλείσει ο λογαριασμός του.

Wi-Phishing: Αυτή η μορφή phishing σχετίζεται με το ασύρματο δίκτυο (Wifi). Οι χρήστες του διαδικτύου, πολλές φορές συνδέονται σε ασύρματα δίκτυα που έχουν δημιουργηθεί από απατεώνες. Αυτό διευκολύνει τους εγκληματίες να κλέψουν τους κωδικούς πρόσβασης αλλά και άλλες προσωπικές πληροφορίες, με σκοπό να τις εκμεταλλευτούν εις βάρος του θύματος.

(Tajpour et al., 2010; Γιαμπουλάκης, 2017)

Οι επιτιθέμενοι γενικά ακολουθούν μια κοινή μεθοδολογία για να εξαπατήσουν πειστικά τα θύματα και να αποκτήσουν τα προσωπικά τους δεδομένα. Μια αποτελεσματική προσέγγιση που χρησιμοποιούν οι επιτιθέμενοι για να διατηρήσουν την ανωνυμία τους και να μειώσουν τον κίνδυνο εντοπισμού είναι η δημιουργία εργαλειοθηκών phishing. Διανέμοντας σε αυτές τις εργαλειοθήκες, οι επιτιθέμενοι μπορούν να συλλέγουν όλα τα δεδομένα που αποκτούν όσοι τις χρησιμοποιούν, παρέχοντας στον δημιουργό της εργαλειοθήκης πρόσβαση στις συλλεγμένες πληροφορίες. Ένα βασικό χαρακτηριστικό των επιθέσεων phishing είναι η χρήση σχεδόν πανομοιότυπων ιστοτόπων με τους νόμιμους αντίστοιχους.

Συνήθως, οι επιτιθέμενοι δημιουργούν ιστοτόπους με ελαφρώς τροποποιημένα domain names, όπως η αντικατάσταση ενός γράμματος με έναν οπτικά παρόμοιο χαρακτήρα (π.χ. η χρήση ενός μεγάλου "i" αντί για ένα μικρό "l" στο "Alphabank" για να δημιουργηθεί το "Alphabank"). Εναλλακτικά, οι επιτιθέμενοι μπορεί να επιχειρήσουν να παραβιάσουν τον διακομιστή της στοχευμένης εταιρείας. Όταν το θύμα αποκτά πρόσβαση στον γνήσιο ιστότοπο, ανακατευθύνεται σε μια παρόμοια σελίδα με διαφορετική διεύθυνση IP. Σε αυτές τις περιπτώσεις, ακόμη και αν το θύμα ελέγξει το domain name, ενδέχεται να μην παρατηρήσει καμία διαφορά, καθώς η διαφορά έγκειται στη διεύθυνση IP στην οποία αποστέλλονται τα δεδομένα.

Επιπλέον, οι καλά σχεδιασμένοι ιστοτόποι phishing είναι αποτελεσματικοί στο να τραβούν την προσοχή του θύματος, ενώ παράλληλα αποφεύγουν την ανίχνευση μέσω διαφόρων κόκκινων σημαιών. Ωστόσο, καθώς οι επιθέσεις phishing έχουν γίνει ευρύτερα γνωστές, έχουν αναπτυχθεί εφαρμογές και πρόσθετα για το φιλτράρισμα ιστοσελίδων και δεδομένων στα οποία οι χρήστες επιχειρούν να αποκτήσουν πρόσβαση. Σε απάντηση, οι phishers έχουν επινοήσει μεθόδους για την παράκαμψη αυτών των φίλτρων, όπως η αντικατάσταση του γραπτού κειμένου με εικόνες στις σελίδες ή τα μηνύματα ηλεκτρονικού ταχυδρομείου τους. (Darwish et al., 2012)

Με βάση την έρευνα στο επιστημονικό άρθρο (Basit et al., 2020) το ηλεκτρονικό ψάρεμα μπορεί να κατηγοριοποιηθεί σε τρεις μορφές σε συνάρτηση με τον τρόπο επίθεσης. Κατά την πρώτη κατηγορία, το ηλεκτρονικό ψάρεμα, στο οποίο σε μια ιστοσελίδα πραγματοποιείται ένα πιστό αντίγραφο μιας επίσημης σελίδας ώστε να παραπλανήσει τους πελάτες να υποβάλλουν σημαντικά δεδομένα. Άλλη κατηγορία είναι το Phishing μέσω του ηλεκτρονικού ταχυδρομείου (email). Σε αυτήν την περίπτωση ο επιτιθέμενος στέλνει ένα μήνυμα σε πολλούς πελάτες υποστηρίζοντας ότι υπάρχει κάποιο πρόβλημα με τα καταγεγραμμένα δεδομένα. Τέλος, η τρίτη κατηγορία αποτελείται από το phishing που βασίζεται σε κακόβουλο λογισμικό. Αναλυτικότερα, ύποπτος κώδικας εισάγεται σε έμπιστα site και μόλις ο χρήστης επισκεφτεί την ιστοσελίδα, το κακόβουλο λογισμικό εισχωρεί στο σύστημα του πελάτη.

4. Χαρακτηριστικά Θυμάτων

Σύμφωνα με μια μελέτη [(Darwish et al., 2012)], τα θύματα των επιθέσεων phishing παρουσιάζουν συχνά κοινά χαρακτηριστικά. Έχει διαπιστωθεί πως, οι νεότεροι χρήστες του διαδικτύου, συγκεκριμένα εκείνοι που βρίσκονται στην ηλικιακή κλίμακα 18-25 ετών ή ακόμη και νεότεροι, είναι πιο ευάλωτοι σε τέτοιου είδους επιθέσεις. Ωστόσο, είναι σημαντικό να σημειωθεί ότι υπάρχουν περιπτώσεις νεαρών ατόμων που έχουν αποφύγει επιτυχώς τέτοιες επιθέσεις, καθώς και μεγαλύτερων σε ηλικία χρηστών του διαδικτύου που έχουν πέσει θύματα των δραστών.

Επιπλέον, από την έρευνα έγινε διάκριση του φύλου και των διαδικτυακών δραστηριοτήτων ως βασικοί παράγοντες. Αποφάνθηκε πως οι γυναίκες, ιδίως όσες ασχολούνται με το ηλεκτρονικό εμπόριο και τις ηλεκτρονικές αγορές, τείνουν να πέφτουν στην παγίδα των παραπλανητικών μηνυμάτων, ενώ οι άνδρες χρησιμοποιούν το διαδίκτυο κυρίως για την επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου και τη βασική περιήγηση.

Μια άλλη σημαντική πτυχή που καθορίζει την ευαισθησία σε επιθέσεις είναι ο συνδυασμός των χαρακτηριστικών της προσωπικότητας και της εκπαίδευσης σχετικά με τις εν λόγω απειλές. Η έρευνα έδειξε πως τα άτομα που χαρακτηρίζονται ως εξωστρεφείς, συνεργάσιμοι, ευχάριστοι ή κοινωνικοί, είναι πιο ευάλωτοι σε σύγκριση με εκείνους που είναι νευρικοί, ευσυνείδητοι και ειλικρινείς. Ωστόσο, ανεξάρτητα από το αν κάποιος εμπίπτει σε μια ευάλωτη κατηγορία ή όχι, η ολοκληρωμένη κατανόηση του τρόπου λειτουργίας αυτών των επιθέσεων και της ύπαρξής τους μπορεί να μειώσει σημαντικά την ευπάθεια.

Σύμφωνα με μία έρευνα που πραγματοποίησαν οι (Abroshan et al., 2021) μέσω της πληθοποριστικής αγοράς (crowdsourcing marketplace), του Amazon Mechanical Turk, αναζητούσαν το μέγεθος της επιρροής του ανθρώπου με βάση την συμπεριφορά, τον χαρακτήρα αλλά και τα δημογραφικά χαρακτηριστικά. Ως παράγοντα τη έρευνας έθεσαν την επιρροή της έξαρσης της πανδημίας του κορονοϊού. Σύμφωνα με τους συμμετέχοντες, και τα αποτελέσματα της έρευνάς τους, εάν ο χρήστης έχει άγχος και ψυχαναγκαστικό στρες για τον Covid-19 είναι πιο επιρρεπείς να πέσει θύμα, τόσο σε επιθέσεις ηλεκτρονικού ψαρέματος σχετικά με την πανδημία όσο και σε γενικού χαρακτήρα phishing μηνύματα. Εάν όμως ο χρήστης έχει φόβο ή νιώθει τον κίνδυνο για μόλυνση από τον κορονοϊό, τότε είναι πιθανό να πέσει θύμα σε επιθέσεις με θέμα την πανδημία, σε αντίθεση με τις γενικές phishing επιθέσεις. Όσον αφορά την συμπεριφορά του ανθρώπου, εάν παίρνει ρίσκο γενικά, στον τομέα της ηθικής επηρεάζεται αρνητικά και στις δύο μορφές επιθέσεων, ενώ στον κοινωνικό τομέα αυξάνεται η πιθανότητα στις επιθέσεις με θέμα τον ιό. Τέλος, για τα δημογραφικά χαρακτηριστικά παρατηρήθηκε πως δεν επηρεάζει το γένος, η ηλικία και η καταγωγή στην ευαισθησία του χρήστη να πέσει θύμα, αλλά στην έρευνά τους φάνηκε πως το υψηλό μορφωτικό επίπεδο επηρεάζει την πιθανότητα στοχοποίησης του θύματος.

Σε μία άλλη έρευνα, η οποία πραγματοποιήθηκε στο πανεπιστήμιο της Ιντιάνας, το συμπέρασμα είναι πως το γυναικείο φύλο είναι πιο ευάλωτο και πιο εύκολα γίνεται θύμα ηλεκτρονικού εγκλήματος. Παρόλα αυτά, τα ποσοστά ανάμεσα στα δύο φύλα δεν αποκλίνουν πολύ, οπότε δεν διαφέρει σημαντικά η

πιθανότητα να απαντήσουν σε παραπλανητικό μήνυμα με παράγοντα το φύλο. Σε συνάρτηση με τον ηλικιακό παράγοντα, διαπιστώθηκε πως τα άτομα 18 – 25 είναι πιο ευάλωτα σε επιθέσεις phishing. Στην βιβλιογραφική ανασκόπηση της ίδιας μελέτης, παρατηρήθηκε μέσω ενός πειράματος ρόλων, ότι το ανδρικό φύλο αναγνωρίζει ευκολότερα τα παραπλανητικά μηνύματα και είναι πιο πιθανό να αποφύγει τις παγίδες του ηλεκτρονικού ψαρέματος σε σύγκριση με το γυναικείο. Σαν συμπέρασμα, η μελέτη καταλήγει πως το γυναικείο φύλο, συνολικά από διάφορες έρευνες, παρουσιάζεται πιο εύπιστο στα παραπλανητικά μηνύματα και εμπιστεύεται ευκολότερα να δώσει τα προσωπικά δεδομένα σε μηνύματα ηλεκτρονικού ψαρέματος. (Sheng et al., 2010)

Σε μία παλιότερη έρευνα που συμμετείχα, με θέμα το ηλεκτρονικό έγκλημα, πραγματοποιήθηκε μία δημοσκοπήση με την μορφή ερωτηματολογίου, στο οποίο εντάχθηκε δύο φορές σε διαφορετικά σημεία της δομής, η ερώτηση εάν έχουν πέσει θύμα ηλεκτρονικού ψαρέματος. Τα αποτελέσματα ήταν διαφορετικά στις δυο ερωτήσεις, αφού στην πρώτη υπήρχε θετική απάντηση ύψους 2,7% ενώ στην δεύτερη 8%. Το συμπέρασμα ήταν πως δεν υπήρχε ολοκληρωμένη ενημέρωση των χρηστών για την επίθεση ηλεκτρονικού ψαρέματος στην πρώτη ερώτηση, εφόσον πριν την δεύτερη είχαν παρουσιαστεί ο ορισμός και κάποια παραδείγματα. Όσον αφορά το γένος και την ηλικία, οι άντρες και οι γυναίκες ήταν με μικρή απόκλιση στα ίδια ποσοστά θύματα σε phishing επιθέσεις, ενώ φάνηκαν πιο επιρρεπείς όσοι βρίσκονταν ηλικιακά ανάμεσα στα 18-25 έτη.

Στην έρευνα των (Lain et al., 2022) πραγματοποιήθηκε μια μακροπρόθεσμη (15 μήνες) και μεγάλης κλίμακας (πάνω από 14 χιλιάδες συμμετέχοντες) έρευνα για τα phishing emails. Στην συγκεκριμένη μελέτη, έστειλαν phishing emails στους συμμετέχοντες με σκοπό την παρατήρηση της συμπεριφοράς τους απέναντι σε αυτά και κατά πόσο θα εμπιστευτούν τα παραπλανητικά μηνύματα και θα πατήσουν πάνω στα κακόβουλα link. Διαπιστώθηκε πως οι υπάλληλοι που είναι εξειδικευμένοι στους υπολογιστές πάτησαν περισσότερες φορές πάνω σε παραπλανητικούς συνδέσμους αλλά και κινήθηκαν σε επικίνδυνες ενέργειες (όπως την καταχώρηση στοιχείων). Σε αντίθεση με αυτό, οι υπάλληλοι που είχαν συχνή ή σπάνια χρήση του υπολογιστή, είχαν χαμηλότερες τιμές. Αυτό το δικαιολόγησαν πως οι εξειδικευμένοι υπάλληλοι υπολογιστών αναμένουν να αλληλεπιδράσουν με email ενώ οι υπάλληλοι που είχαν σπάνια χρήση του υπολογιστή φάνηκαν πιο καχύποπτοι. Συνολικά από τους συμμετέχοντες, το 30,6% πάτησε παραπάνω από δυο φορές στα παραπλανητικά μηνύματα, ενώ το 23,9% πραγματοποίησε κάποια επικίνδυνη δραστηριότητα τουλάχιστον δύο φορές. Συγκεκριμένα, ένας από τους συμμετέχοντες έπεσε θύμα στις 6 από τις 8 επιθέσεις. Επίσης παρατηρήθηκε πως η ομάδα νεώτερων υπαλλήλων (18 – 19 ετών) ήταν πιο πιθανόν να πατήσουν σε έναν σύνδεσμο πάνω από μία φορά. Τέλος, στην συνεχόμενη έκθεση σε phishing μηνύματα το 32,1% πάτησε τουλάχιστον μία φορά έναν σύνδεσμο ή ένα συνημμένο αρχείο, ενώ το 25,4% προέβη σε επικίνδυνες δραστηριότητες.

5. Phishing στην περίοδο του Covid-19

Το ηλεκτρονικό έγκλημα έχει τρεις παραμέτρους. Το θύμα, το οποίο είναι ο στόχος της επίθεσης, το κίνητρο, το οποίο είναι η πρόθεση του εγκληματία να διαπράξει την επίθεση και η ευπάθεια ή η ευκαιρία που επιτρέπει το έγκλημα να διαπραχθεί. Εφόσον καθημερινά οι χρήστες του διαδικτύου αυξάνονται, οι δύο πρώτες παράμετροι δημιουργούνται σχεδόν αυτόματα. Ανάλογα τις συγκυρίες επηρεάζεται ο τρίτος παράγοντας. Στις επιθέσεις ηλεκτρονικού εγκλήματος οι επιτιθέμενοι εκμεταλλεύονται τις περιόδους πίεσης, ανάγκης και αντιπερισπασμού. Με άλλα λόγια, όταν υπάρχει ένα γεγονός που επηρεάζει μεγάλο αριθμό ανθρώπων, συνεπώς χρηστών του διαδικτύου, οι εγκληματίες αρπάζουν την ευκαιρία και ξεκινούν τις επιθέσεις. Μία τέτοια αφορμή είναι οι πανδημίες. Για παράδειγμα, όταν το 2016 είχε ξεσπάσει ο ιός Έμπολα, οι επιτιθέμενοι έστελναν phishing emails σε ομάδες ανθρώπων που επηρεάζοντουσαν από τον ιό. Το ίδιο συνέβη και με την πυρκαγιά στην Αυστραλία το 2019, όπου οι εγκληματίες υποστήριζαν πως είναι από κάποια φιλανθρωπική οργάνωση, μεγάλους οργανισμούς ή ακόμα και από την κυβέρνηση, παραπλανώντας τους χρήστες να δωρίσουν κάποια χρήματα ή ακόμα και να δώσουν προσωπικά δεδομένα. Με την εμφάνιση της πανδημίας του Covid-19, δεν έχασαν την ευκαιρία οι επιτιθέμενοι να ξεκινήσουν να ξεγελούν τους χρήστες στο διαδίκτυο με phishing μηνύματα αλλά και με άλλων ειδών ηλεκτρονικής απάτης. (Bitaab et al., 2020)

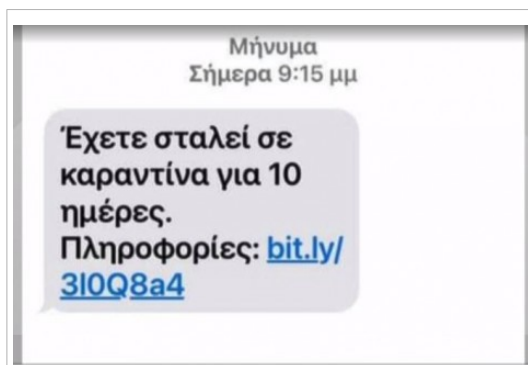
Η πανδημία του κορονοϊού προκάλεσε παγκοσμίως πανικό και φόβο και σε συνδυασμό τα περιοριστικά μέτρα και τον εγκλεισμό της καραντίνας, ο κόσμος άρχισε να αναζητά στο διαδίκτυο πληροφορίες σχετικά με τον ιό. Σε όλη αυτή την κατάσταση πανικού και άγχους, εντάχθηκε και στην καθημερινότητα η εργασία από το σπίτι (remote control work), η τηλεεκπαίδευση αλλά το πιο βασικό οι ηλεκτρονικές αγορές.

Σύμφωνα με την έρευνα στο άρθρο [3] παραθέτονται μερικά παραδείγματα των επιθέσεων Phishing κατά την διάρκεια της πανδημίας. Καθώς ο ιός μεταδίδεται πολύ εύκολα, ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) συνιστούσε την χρήση μάσκας. Στις αρχές της έξαρσης της πανδημίας, τα αποθέματα масκών αλλά και γενικότερα του εξοπλισμού προσωπικής προστασίας από τον ιό ήταν λίγα και εξαντλήθηκαν γρήγορα. Εκτός από αυτό, εφόσον υπήρχε μεγάλη ζήτηση, αυξήθηκε και το κόστος τους. Έτσι οι καταναλωτές, εφόσον τα αναζητούσαν απεγνωσμένα και τα διαδεδομένα site πωλήσεων δεν είχαν αποθέματα ή καθυστερούσαν την αποστολή λόγω όγκου παραγγελιών, εμπιστεύτηκαν άλλες ιστοσελίδες καταστημάτων για την αγορά προστατευτικής μάσκας, αντισηπτικού και γαντιών με αποτέλεσμα να πέσουν σε ιστοσελίδες απάτη και να χάσουν τα χρήματά τους. Σε αυτό βοήθησαν οι εγκληματίες, επειδή προσαρμόστηκαν άμεσα στα δεδομένα της πανδημίας. Παρατήρησαν γρήγορα τις νέες προσθήκες στην πολιτική των ηλεκτρονικών επιχειρήσεων και διαμόρφωσαν τα καταστήματα απάτη αντίστοιχα ή ακόμα πρόσθεταν την ετικέτα “δωρεάν μεταφορικά”, πράγμα που προσέλκυε περισσότερους καταναλωτές να επισκεφτούν αλλά και να πραγματοποιήσουν αγορές.

Άλλος ένας τρόπος παγίδευσης του χρήστη από τους εγκληματίες ήταν, με αφορμή τις κρατικές επιδοτήσεις ή οποιαδήποτε χρηματοδότηση εισέπρατταν λόγω της πανδημίας, οι επιτιθέμενοι εκμεταλλευτήκαν την ανησυχία των πολιτών για την “ημέρα πληρωμής”. Ως εκ τούτου, ο κόσμος αναζητούσε στους διαδικτυακούς περιηγητές για την ημερομηνία κατάθεσης των χρημάτων τους, αλλά οι επιτιθέμενοι τους “προλάβαιναν” με phishing email στο οποίο αναγραφόταν πως λήγει σε μερικές μέρες η προθεσμία επιβεβαίωσης στοιχείων (1 με 2 συνήθως, ώστε να βιαστούν οι χρήστες να συνδεθούν) και ζητούσαν να συνδεθούν σε εικονικές πλατφόρμες για την επιδότηση ή να στείλουν στοιχεία του τραπεζικού λογαριασμού. (Bitaab et al., 2020)

Οι επιτιθέμενοι, για να έχουν επιτυχία στα phishing μηνύματα, στοχεύουν σε ομάδες ανθρώπων ή οργανισμούς που είναι πιο ευάλωτοι στις επιθέσεις. Κατά την πανδημία του κορονοϊού, το ηλεκτρονικό ψάρεμα και οι απάτες ήταν τα πιο κοινά και αποτελεσματικά ηλεκτρονικά εγκλήματα που διαπράχθηκαν. Πιο συγκεκριμένα, μία phishing επίθεση έχει τουλάχιστον κατά 30% και πάνω επιτυχία. Στο πρώτο τρίμηνο του 2020 υπήρχε αύξηση των phishing emails που σχετίζονταν με τον Covid-19 κατά 600%. Επίσης, το 75% από τα κακόβουλα site έχουν προσθέσει SSL (πρωτόκολλο για την ασφαλή μετάδοση δεδομένων στο διαδίκτυο). (Pranggono & Arabo, 2020) Σύμφωνα με τα φίλτρα προστασίας της τεχνητής νοημοσύνης της Google, παρατηρήθηκαν πάνω από 18 εκατομμύρια ηλεκτρονικού ψαρέματος και κακόβουλου λογισμικού επιθέσεις με θέμα τον Covid-19 κατά σε μία εβδομάδα του Απριλίου του 2020. (Akdemir & Yenal, 2021)

Συμπεραίνοντας, η πανδημία του Covid-19 κινητοποίησε και ενέπνευσε τους επιτιθέμενους του ηλεκτρονικού εγκλήματος και ιδίως του ηλεκτρονικού ψαρέματος. Ήταν μία περίοδος που έσπειρε στους ανθρώπους το άγχος, την αμφιβολία και την αβεβαιότητα για την καθημερινότητα προκαλώντας τους πανικό και σύγχυση, με αποτέλεσμα να είναι πιο ευάλωτοι σε επιθέσεις phishing. Ανεξαρτήτως της οικονομικής κατάστασης που επικρατεί παγκοσμίως, η πανδημία έφερε στο προσκήνιο την αξία της κυβερνοασφάλειας και μας έκανε να συνειδητοποιήσουμε ότι η επιμέλεια της κυβερνοασφάλειας πρέπει να αποτελεί προτεραιότητα και δεν μπορεί να τίθεται ως “δεύτερη σκέψη”.



Εικόνα 1: Παράδειγμα Phishing SMS κατά την διάρκεια της πανδημίας του κορονοϊού
(<https://www.ertnews.gr/eidiseis/ellada/nea-apatimeso-sms-echete-stalei-se-karantina-gia-10-imeres-prosochi-sta-minymata-covid19-video/>)

6. Τρόποι αντιμετώπισης

Οι ιοί του υπολογιστή μεταδίδονται με την ίδια ευκολία που μεταδίδονται και οι ανθρώπινοι ιοί. Για αυτό, όπως αποφεύγουμε την επαφή αντικειμένων και επιφανειών που δεν είναι καθαρές, έτσι πρέπει να αποφεύγουμε να ανοίγουμε τα email από παραλήπτες αγνώστου ταυτότητας ή να μην επισκεπτόμαστε αναξιόπιστες ιστοσελίδες. Πολλές φορές αυτό όμως είναι δύσκολο να εντοπιστεί, διότι οι επιτιθέμενοι δημιουργούν πιστά αντίγραφα ιστοσελίδων ή χρησιμοποιούν περίτεχνα τεχνάσματα στα email για να ξεγελάσουν τους χρήστες. Για να αποφευχθεί η απάτη πρέπει να ακολουθηθούν κάποια μέτρα προστασίας.

Στην έρευνα που πραγματοποίησαν οι (Mayuri et al., 2012) αναφέρουν πως μία καλή τακτική πρόληψης των επιθέσεων ηλεκτρονικού ψαρέματος είναι η χρήση του AntiPhish plugin στον περιηγητή και το DOMAntiPhish extension. Αυτά τα δύο εργαλεία, μπορούν να προειδοποιήσουν τον χρήστη για τις αναξιόπιστες ιστοσελίδες αλλά και για τα ύποπτα email που λαμβάνει. Αρχικά, το AntiPhish έχει την δυνατότητα να εντοπίζει τις ευαίσθητες πληροφορίες που συνηθίζει να συμπληρώνει ο χρήστης και αντιλαμβάνεται τότε πρόκειται να τις μεταβιβάσει σε κάποια άλλη ιστοσελίδα. Ο χρήστης θα ενημερωθεί εάν η σελίδα δεν θεωρείται έμπιστη. Επίσης, έχει την ικανότητα να απομνημονεύει τα δεδομένα που υποβάλλει ο χρήστης αλλά και να αποθηκεύει σε ποιο Domain τα έχει αποστείλει, σύμφωνα με το URL. Επιπλέον, η ασφάλεια έναντι των απειλών στον κυβερνοχώρο παρέχεται σε διάφορα επίπεδα (λειτουργικό σύστημα, λογισμικό εφαρμογών κλπ). Τα τελευταία λειτουργικά συστήματα και τα προγράμματα περιήγησης στο διαδίκτυο διαθέτουν ενσωματωμένο χαρακτηριστικό ασφάλειας που προστατεύει τους χρήστες από τις απειλές στον κυβερνοχώρο. Αλλά αυτά δεν επαρκούν, διότι οι Phishers αλλάζουν συνεχώς το στόχο τους με νέα εργαλεία και τεχνικές, με δυναμικό τρόπο, επομένως οι ειδικοί σε θέματα ασφαλείας πρέπει να αναπτύσσουν νέα εργαλεία λογισμικού για την καταπολέμηση των απειλών στον κυβερνοχώρο. (Hota et al., 2018)

Γενικότερα, προτείνεται η χρήση εργαλειοθηκών στον περιηγητή (Toolbars web browser), από φίλτρα κατά του phishing (Anti-Phishing filters) και παγίδων κατά του ηλεκτρονικού ψαρέματος (Anti-Phishing honeypots). Η χρήση της παγίδας ηλεκτρονικού ψαρέματος δεν είναι τελείως αποτελεσματική, διότι για να λειτουργήσει χρειάζεται κάποιο χρονικό περιθώριο προκειμένου να εντοπίσει και να επεξεργαστεί τα δεδομένα, αφήνοντας εκείνες τις ώρες τον χρήστη εκτεθειμένο σε επιθέσεις. Οι επιτιθέμενοι, γνωρίζοντας για τα Anti-phishing φίλτρα, έχουν βρει τρόπο ώστε να μπορούν να παρακάμψουν τα φίλτρα. Τα συγκεκριμένα φίλτρα, ελέγχουν το περιεχόμενο της ιστοσελίδας και των μηνυμάτων. Για αυτό δημιουργούν οι επιτιθέμενοι ιστοσελίδες με εικόνα από το περιεχόμενο, ώστε τα φίλτρα να μην μπορούν να αναγνωρίσουν το κακόβουλο περιεχόμενο. Επίσης τα φίλτρα ελέγχουν αν το Domain name είναι στην λίστα με τις ιστοσελίδες που έχουν κάνει αναφορά για επιθέσεις ηλεκτρονικού ψαρέματος. Εάν η επισκεπτόμενη σελίδα ανήκει σε αυτήν την λίστα, τότε είτε μπλοκάρει (δεν επιτρέπει την πρόσβαση) την ιστοσελίδα στον χρήστη, είτε τον ενημερώνει με ένα προειδοποιητικό μήνυμα. Όσο για τις εργαλειοθήκες του περιηγητή, είναι σχεδιασμένες να δείχνουν στοιχεία ασφαλείας για τις ιστοσελίδες που επισκέπτεται ο χρήστης, όπως η

παροχή νόμιμης ψηφιακής πιστοποίησης και SSL κρυπτογράφησης. Μόλις παρατηρηθεί η απουσία τους, ειδοποιείται ο χρήστης με ένα μήνυμα, ότι η ιστοσελίδα μπορεί να είναι κακόβουλη. Σύμφωνα με έρευνες που πραγματοποιήθηκαν σχετικά με τα toolbars, βρήκαν πως δεν είναι αποτελεσματικά για τις επιθέσεις phishing. Πολλές φορές οι χρήστες παραβλέπουν τα προειδοποιητικά μηνύματα, εν αγνοία τους για τις επιθέσεις ηλεκτρονικού ψαρέματος.(Darwish et al., 2012)

Μπορούμε να αντιληφθούμε πως τα εργαλεία προφύλαξης του χρήστη από τις επιθέσεις phishing, μπορεί στην αρχή να ήταν αποτελεσματικά, αλλά στην πορεία βρέθηκαν τρόποι να τα παραβιάσουν προσπερνώντας τα από τους επιτιθέμενους, επιστρέφοντας πάλι στην ίδια θέση για τον κίνδυνο του χρήστη να πέσει θύμα. Ένας αποτελεσματικός τρόπος για την αποφυγή επιθέσεων ηλεκτρονικού ψαρέματος είναι η ευαισθητοποίηση του χρήστη. Ένας χρήστης του διαδικτύου, οφείλει να γνωρίζει τους κινδύνους που μπορεί να αντιμετωπίσει αλλά και τον τρόπο που πρέπει να τους διαχειριστεί. Για να επιτευχθεί αυτό πρέπει να γίνουν ενημερωτικά σεμινάρια και εκπαιδεύσεις ώστε όχι μόνο να μάθουν στην θεωρία τις επιθέσεις που μπορεί να δεχτούν, αλλά και να δουν στην πράξη πως μπορεί να μοιάζει μία επίθεση.

Σε ένα πείραμα που διεξήγαγαν οι ερευνητές (Darwish et al., 2012), δύο ομάδες συμμετεχόντων υποβλήθηκαν σε "διαδραστικά" και "μη διαδραστικά" περιβάλλοντα μάθησης. Η ομάδα που υποβλήθηκε σε "διαδραστική" μάθηση, όπου εκτέθηκαν σε μια επίθεση phishing μέσω ενός προσομοιωμένου μηνύματος "δόλωμα" πριν εκπαιδευτούν σχετικά με το phishing, παρουσίασε ισχυρότερη εσωτερική ευαισθητοποίηση των κόκκινων σημαιών που σχετίζονται με τέτοιες επιθέσεις. Αντίθετα, η ομάδα "μη διαδραστικής" μάθησης, η οποία έλαβε γενικές προειδοποιήσεις σχετικά με τις κόκκινες σημαίες και το phishing πριν εκτεθεί στο δικό της μήνυμα, επέδειξε σχετικά ασθενέστερη κατανόηση των σχετικών κινδύνων.

Το τεχνολογικό κομμάτι μπορεί να βοηθήσει σημαντικά στον μετριασμό των επιθέσεων ηλεκτρονικού ψαρέματος. Αρχικά, σε κλήσεις (vishing) και μηνύματα (είτε email είτε SMS), η καταγραφή του αποστολέα και του περιεχομένου και η αποστολή του στα εργαλεία ασφάλειας θα απέτρεπε επιθέσεις με τον αποκλεισμό ίδιας ή ακόμη και παρόμοιας απόπειρας. Επίσης, πρέπει να επιδιορθώνεται συχνά το δίκτυο αλλά και να αναλύεται και να εξελίσσεται από επαγγελματίες κυρίως για τις επιχειρήσεις με πολύτιμα δεδομένα (όπως τράπεζες, νοσοκομεία κ). Όσον αφορά το διαδίκτυο, συνιστάται να αναζητούνται και να μπλοκάρονται οι παραπλανητικές ειδήσεις. Με αυτόν τον τρόπο, οι χρήστες θα είναι ελαφρώς πιο προστατευμένοι από τις κακόβουλες ενέργειες των επιτιθέμενων.

Οι χρήστες για να μπορέσουν να ελέγξουν μόνοι τους πιθανές επιθέσεις θα πρέπει να είναι αρκετά καχύποπτοι στις ιστοσελίδες που επισκέπτονται αλλά και στα email που λαμβάνουν. Για αυτόν τον λόγο συστήνεται η αυτοματοποίηση των παρακάτω ενεργειών από τους περιηγητές που χρησιμοποιούν οι χρήστες για την επίσκεψη ιστοσελίδων αλλά και τους διακομιστές των ηλεκτρονικών ταχυδρομείων.

1. Το περιεχόμενο μιας ιστοσελίδας θα πρέπει να αναλύεται και να φιλτράρεται, ώστε να αναγνωρίζονται οι παραπλανητικές ιστοσελίδες με ψεύτικο περιεχόμενο.
2. Το URL μια ιστοσελίδας θα πρέπει να ελέγχεται για πιθανούς αναγραμματισμούς. Πολύ συχνά, για να παραπλανήσουν τον χρήστη να επισκεφτεί την phishing ιστοσελίδα, χρησιμοποιούν μία έμπιστη

ιστοσελίδα με έναν αναγραμματισμό ή παραποίηση των γραμμάτων με τέτοιο τρόπο ώστε να μην είναι αντιληπτό με γυμνό μάτι. Έχει αναφερθεί πως η Microsoft (www.microsoft.com) έχει κερδίσει σε δικαστικές αγωγές εναντίον των ατόμων που χρησιμοποιούσαν ιστοσελίδες με παρόμοιο URL με αυτήν. (www.micosoft.com)

3. Η ηλικία της ιστοσελίδας θα πρέπει να λαμβάνεται υπόψιν στις δικλίδες ασφαλείας, εφόσον τα κακόβουλα site έχουν την τάση μικρής διάρκειας “ζωής”.
4. Η εγκυρότητα του αποστολέα στο ηλεκτρονικό ταχυδρομείο. Είναι σημαντικό να ταυτοποιείται ο αποστολέας του μηνύματος και να συγκρίνεται με προηγούμενες αναφορές από επιθέσεις ηλεκτρονικού ψαρέματος. (Al-Qahtani & Cresci, 2022; Rameem Zahra et al., 2022)

Οι (Mao et al., 2017) προτείνουν μία μέθοδο ανίχνευσης ιστοσελίδες ηλεκτρονικού ψαρέματος, το Phishing-Alarm. Χρησιμοποιεί χαρακτηριστικά που είναι δύσκολο να τα παρακάμψουν οι επιτιθέμενοι για να ποσοτικοποιήσει τον βαθμό επικινδυνότητας των σελιδών, με βάση την εμφανισιακή ομοιότητα μεταξύ τους. Η συγκεκριμένη μέθοδος χρησιμοποιεί CSS και είναι αποτελεσματική επειδή βασίζεται σε θεμελιώδη οπτικά χαρακτηριστικά των ιστοσελίδων και δεν απαιτεί πολύπλοκους αλγορίθμους μηχανικής μάθησης ή μεγάλα σύνολα δεδομένων εκπαίδευσης. Η μέθοδος αυτή αξιολογήθηκε σε μεγάλο αριθμό δεδομένων από ιστοσελίδες Phishing αλλά και νόμιμες ιστοσελίδες, και τα αποτελέσματα δείχνουν ότι ξεπερνά αρκετές σύγχρονες μεθόδους ανίχνευσης ηλεκτρονικού ψαρέματος, από άποψη ακρίβειας και αποτελεσματικότητας.

Όσον αφορά το θέμα της ασφάλειας γύρω από το διαδίκτυο και της αποφυγής επιθέσεων ηλεκτρονικού ψαρέματος, έχει δημιουργηθεί εκπαιδευτικό υλικό του οποίου η συνεισφορά είναι ιδιαίτερα σημαντική, μιας και έχει αποδειχθεί πως βελτιώνει την ικανότητα των χρηστών να αποφύγουν τις επιθέσεις phishing. Το εκπαιδευτικό υλικό απαρτίζεται από:

1. Την εκπαίδευση με βάση τα συμφραζόμενα. Αποστολή προσωποποιημένων μηνυμάτων από τους πειραματιστές με σκοπό να μάθουν οι χρήστες να εντοπίζουν τυχόν ηλεκτρονικού ψαρέματος.
2. Ενσωματωμένη εκπαίδευση. Ο εκπαιδευτής στέλνει μηνύματα ηλεκτρονικού ψαρέματος και αν οι χρήστες κάνουν κλικ στους παραπλανητικούς συνδέσμους, τους παρουσιάζεται μία παρέμβαση που είναι σχεδιασμένη καταλλήλως με σκοπό να τους εκπαιδεύσει στο πως να αποφύγουν παρόμοιες παγίδες.
3. Διαδικτυακό παιχνίδι Anti-phishing Phil. Είναι ένα παιχνίδι σχεδιασμένο από τους Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (Sheng et al., 2007) Σκοπός του παιχνιδιού είναι να μάθουν οι χρήστες να αποφεύγουν επιθέσεις phishing και να είναι σε θέση να εντοπίζουν δόλιους ιστότοπους. (Sheng et al., 2010)

Επομένως καταλήγουμε στο συμπέρασμα ότι υπάρχουν αρκετοί τρόποι να αντιμετωπιστεί το ηλεκτρονικό ψάρεμα. Ακόμη μία λύση θα ήταν η διασυνωριακή συνεργασία των κρατών σχετικά με το ζήτημα. Υπάρχουν πολλαπλοί τρόποι για την ανέγερση ενός τοίχου προστασίας, με την δυνατότητα να αναπτυχθεί από πολλαπλές κατευθύνσεις, συμπεριλαμβανομένου του τελικού χρήστη. Σε καμία περίπτωση όμως δεν θα έπρεπε να επιβαρύνεται ο ίδιος ο χρήστης το μερίδιο ευθύνης που εξαπατήθηκε.

Κεφάλαιο 3ο

Σχετικά με την Νομοθεσία του Ηλεκτρονικού Εγκλήματος

Το ηλεκτρονικό έγκλημα, όπως παρουσιάστηκε νωρίτερα, έχει εισχωρήσει στην καθημερινότητα των ανθρώπων και πλήττονται καθημερινά αρκετοί χρήστες του διαδικτύου από αυτό. Αμέσως επόμενο είναι η απαίτηση από την κοινωνία να λάβει μέρος και η δικαιοσύνη σε αυτά τα εγκλήματα. Το πρόβλημα με τέτοιου είδους εγκλήματα που αντιμετωπίζεται είναι η γεωγραφική τοποθεσία. Ο τόπος του ηλεκτρονικού εγκλήματος δεν μπορεί να οριστεί εύκολα. Το διαδίκτυο έχει δώσει την πρόσβαση σε κάθε χρήστη να αναζητεί, να κοινοποιεί και να αποκτά πρόσβαση από κάθε μέρος του πλανήτη. Ένα ηλεκτρονικό έγκλημα μπορεί να διαπραχθεί σε διαφορετικές πόλεις ταυτόχρονα, εκεί όπου βρίσκονται και οι υπολογιστές που το εκτελούν. Υπάρχουν τέσσερις διαφορετικές θεωρίες όπου ορίζουν τον τόπο τέλεσης του ηλεκτρονικού εγκλήματος.

1. Ο τόπος ενέργεια, ορίζεται ο τόπος που τελέστηκε η ενέργεια που οδήγησε στην άδικη πράξη. Αυτήν την θεωρία την χρησιμοποιούν τα περισσότερα κράτη, παίρνοντας ως γνώμονα τον τόπο που ολοκληρώθηκε το έγκλημα.
2. Ο τόπος αποτελέσματος. Σε αυτήν την θεωρία ορίζεται ως τόπος του εγκλήματος η τοποθεσία στην οποία εκδηλώθηκε το ζημιογόνο αποτέλεσμα.
3. Μικτή θεωρία, όπου συνδυάζεται ο τόπος ενέργεια και ο τόπος αποτελέσματος και δίνεται το δικαίωμα επιλογής στον παθόντα να διαλέξει.
4. Ο βαρύνοντας τόπος. Σε αυτήν την θεωρία, ο τόπος του αδικήματος εντοπίζεται στο κράτος που εκδηλώθηκε ως γενική εικόνα. Σε αυτήν την θεωρία, είναι δύσκολο να οριστεί ο βαρύνοντας τόπος του διαδικτυακού εγκλήματος για την τέλεση της δικαιοσύνης. Αυτή η θεωρία επικρατεί στην Ευρώπη και στην χώρα μας. (Μαυρομάτη & Γατσούλα, 2013)

Παγκόσμια Νομοθεσία για το Ηλεκτρονικό Έγκλημα

Η παγκόσμια νομοθεσία του ηλεκτρονικού εγκλήματος αποτελεί έναν κεντρικό πυλώνα στη σύγχρονη νομική τοποθέτηση που αντιμετωπίζει τις προκλήσεις της ψηφιακής εποχής. Αυτή η νομοθεσία αποσκοπεί στον προσδιορισμό, στην πρόληψη και στην τιμωρία εγκλημάτων που διαπράττονται στον κυβερνοχώρο, όπως η κλοπή δεδομένων, η κυβερνοεπίθεση, η διαδικτυακή απάτη και άλλα. Η παγκόσμια νομοθεσία ενθαρρύνει τη συνεργασία μεταξύ χωρών και διεθνών οργανισμών για τον εντοπισμό και τη δίωξη των δραστών αυτών των εγκλημάτων, προστατεύοντας τα θύματα και εξασφαλίζοντας την ψηφιακή προστασία. Ως ένας αναπτυσσόμενος τομέας, η παγκόσμια νομοθεσία του ηλεκτρονικού εγκλήματος συνεχίζει να προσαρμόζεται στις νέες τεχνολογίες και τις αναδυόμενες απειλές, προσφέροντας ένα πλαίσιο για την εφαρμογή της νομοθεσίας σε αυτόν τον δυναμικό και συνεχώς εξελισσόμενο τομέα.

Οι νόμοι που αντιμετωπίζουν το ηλεκτρονικό έγκλημα διαφέρουν από χώρα σε χώρα, αλλά υπάρχουν κάποιοι κοινοί τύποι νόμων που εφαρμόζονται σε παγκόσμιο επίπεδο. Ορισμένοι από αυτούς περιλαμβάνουν:

1. Νόμοι για την Κυβερνοασφάλεια (Cybersecurity Laws)
2. Νόμοι περί Παραβίασης Δεδομένων (Data Breach Laws)
3. Νόμοι περί Ηλεκτρονικής Απάτης (Cyber Fraud Laws)
4. Νόμοι για την πνευματική ιδιοκτησία (Intellectual Property Laws)
5. Νόμοι για τον Κυβερνοχώρο (Cybercrime Laws)
6. Νόμοι περί προστασίας Ιδιωτικότητας (Privacy Laws)
7. Συμφωνίες Εξουσιοδότησης (Extradition Agreements)

Οι Ηνωμένες Πολιτείες ξεκίνησαν τις προσπάθειές τους κατά του κυβερνοεγκλήματος το 2001, με αφορμή τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου, οι οποίες οδήγησαν στην αναγνώριση του κυβερνοχώρου ως κρίσιμου αγαθού με επιπτώσεις στην εθνική ασφάλεια. Το 2006 το αμερικανικό Υπουργείο Εξωτερικών Υποθέσεων ίδρυσε την Παγκόσμια Ομάδα Δράσης για την Ελευθερία του Διαδικτύου, με σκοπό την αντιμετώπιση των παγκόσμιων προκλήσεων που σχετίζονται με την ελευθερία της έκφρασης και την ελεύθερη ροή πληροφοριών στο διαδίκτυο. Η πρωτοβουλία αυτή έθεσε τα θεμέλια για μια ολοκληρωμένη παγκόσμια στρατηγική με στόχο τη διασφάλιση της ελευθερίας του διαδικτύου.

Τα επόμενα χρόνια, οι Ηνωμένες Πολιτείες εφάρμοσαν περαιτέρω μέτρα για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Τον Απρίλιο του 2011, η κυβέρνηση Ομπάμα παρουσίασε την Εθνική Στρατηγική για αξιόπιστες ταυτότητες στον κυβερνοχώρο, η οποία πρότεινε ένα "οικοσύστημα ταυτότητας" που θα βασίζεται στον τυποποιημένο έλεγχο των διαδικτυακών ταυτοτήτων από όλους τους χρήστες. Η κυβέρνηση παρουσίασε επίσης τη διεθνή στρατηγική για τον κυβερνοχώρο: Prosperity, Security, and Honesty in a Connected World (Ευημερία, ασφάλεια και ειλικρίνεια σε έναν συνδεδεμένο κόσμο) τον Μάιο του 2011, τονίζοντας τη δέσμευση της χώρας να συνεργαστεί με διεθνείς εταίρους για την αντιμετώπιση ζητημάτων του κυβερνοχώρου, συμπεριλαμβανομένου του κυβερνοεγκλήματος.

Τον Ιούλιο του 2011, οι Ηνωμένες Πολιτείες ανακοίνωσαν δύο πρόσθετες στρατηγικές για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η πρώτη ήταν η στρατηγική του Υπουργείου Άμυνας, η οποία επικεντρώθηκε σε ολοκληρωμένα μέτρα κυβερνοασφάλειας. Η πιο πρόσφατη στρατηγική που εισήχθη στις Ηνωμένες Πολιτείες αποσκοπεί στην καταπολέμηση του οργανωμένου εγκλήματος στον κυβερνοχώρο και στην αντιμετώπιση των αναδυόμενων απειλών για την εθνική ασφάλεια. Η στρατηγική αυτή προσδιορίζει δέκα κύριες κατηγορίες απειλών και περιγράφει έξι βασικές δράσεις για την αντιμετώπισή τους.

Είναι σημαντικό να σημειωθεί ότι έχουν γίνει συζητήσεις σχετικά με τη θέσπιση ενός παγκόσμιου προτύπου, όπως μια Σύμβαση ή άλλος διεθνής οργανισμός, για την ενίσχυση της παγκόσμιας αντίδρασης στο έγκλημα στον κυβερνοχώρο. Η ύπαρξη συνεπούς νομοθεσίας σε όλες τις χώρες θα διευκόλυνε

σημαντικά τη διεθνή συνεργασία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. (Finklea & Theohary, 2013; Weber, 2003)

Στη Σαουδική Αραβία η νομοθεσία τους για τα εγκλήματα στον κυβερνοχώρο στο Άρθρο 6 παραθέτει:

“Κάθε πρόσωπο που διαπράττει ένα από τα ακόλουθα εγκλήματα στον κυβερνοχώρο τιμωρείται με φυλάκιση που δεν υπερβαίνει τα πέντε έτη και με χρηματική ποινή που δεν υπερβαίνει τα τρία εκατομμύρια ριάλ ή με οποιαδήποτε από τις δύο ποινές:

- α. Παραγωγή, προετοιμασία, μετάδοση ή αποθήκευση υλικού που προσβάλει την δημόσια τάξη, τις θρησκευτικές αξίες, τα δημόσια ήθη και την ιδιωτική ζωή, μέσω του δικτύου πληροφοριών ή των ηλεκτρονικών υπολογιστών.
- β. Η κατασκευή ή δημοσιοποίηση ιστοσελίδας στο δίκτυο πληροφοριών ή σε υπολογιστή για την προώθηση ή τη διευκόλυνση της εμπορίας ανθρώπων.
- γ. Η προετοιμασία, δημοσίευση και προώθηση υλικού για ιστοσελίδες πορνογραφικού περιεχομένου ή τυχερών παιχνιδιών που παραβιάζουν τα δημόσια ήθη.
- δ. Η κατασκευή ή δημοσιοποίηση ιστοσελίδας στο δίκτυο πληροφοριών ή στον ηλεκτρονικό υπολογιστή για την εμπορία, διανομή, επίδειξη μεθόδου χρήσης ή διευκόλυνση της εμπορίας ναρκωτικών και ψυχοτρόπων φαρμάκων. (https://sherloc.unodc.org/cld/en/legislation/sau/anti_cyber_crime_law/article_6/article_6.html)

Σύμφωνα με τον Συνέδριο Ηνωμένων Εθνών για το εμπόριο και την ανάπτυξη (United Nations Conference on Trade and Development-UNCTAD), το 80% των κρατιδίων παγκοσμίως έχουν στην νομοθεσία άρθρα για το ηλεκτρονικό έγκλημα, ενώ το 5% υπάρχει ήδη το σχέδιο της νομοθεσίας αλλά δεν έχει εγκριθεί ακόμα. Από την άλλη, το 13% των χωρών στην υφήλιο δεν έχουν θεσπίσει νόμους για τον έλεγχο του ηλεκτρονικού εγκλήματος. (<https://unctad.org/page/cybercrime-legislation-worldwide>)

Ελληνική Νομοθεσία Ηλεκτρονικού Εγκλήματος

Στην ελληνική νομοθεσία έχουν ενταχθεί μέτρα για τις επιθέσεις που πραγματοποιούνται μέσω πληροφορικών συστημάτων, καθώς και στον ποινικό κώδικα. Ο Νόμος 4411/2016 “ Ελληνικό Δίκαιο για το Κυβερνοέγκλημα” στο οποίο στο Μέρος Δεύτερο του Νόμου γίνεται μεταφορά στο Ελληνικό Δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Του Συμβουλίου για τις επιθέσεις κατά Συστημάτων Πληροφοριών η οποία καταλαμβάνει και τα εργαλεία που χρησιμοποιούνται για την τέλεση των σχετικών με τις επιθέσεις κατά συστημάτων πληροφοριών εγκλημάτων.

Σχετικά με την νομοθεσία για τα πληροφοριακά συστήματα και ψηφιακά δεδομένα ο Νόμος παραθέτει τους σχετικούς όρους :

Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η' και θ' ως εξής:

«η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών

δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό την λειτουργία, την χρήση, την προστασία και την συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσία γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακά συστήματα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία». (ΦΕΚ – 142/Α/3-8-2016, ν. 4411/2016 Μέρος Δεύτερο)

Άλλα άρθρα του Ποινικού Κώδικα που αναφέρονται στα εγκλήματα στο διαδίκτυο είναι το 292B, 292Γ, 370Α, 370Β, 370Γ, 381Α, 385Α, 386, 386Α, των οποίων οι σχετικοί παράγραφοι παρουσιάζονται παρακάτω. Οι δυσκολίες όμως κατά την απονομή δικαιοσύνης για το ηλεκτρονικό έγκλημα δεν εξομαλύνονται με την νομοθεσία. Το ηλεκτρονικό έγκλημα αποτελεί συνδυασμό εξειδικευμένων γνώσεων του Η/Υ, τις οποίες οι νομικοί (Δικαστής, Εισαγγελέας, δικηγόρος) συνήθως δεν κατέχουν. Με αποτέλεσμα, για να απονεμηθεί η δικαιοσύνη, θα πρέπει να εξιχνιαστεί το έγκλημα ώστε να γνωρίζει ακριβώς ο νομικός σε ποιο άρθρο του ποινικού κώδικα θα βασιστεί. Σε αντίθετη περίπτωση υπάρχει κίνδυνος να απονεμηθεί λανθασμένη ποινή για το αδίκημα.

“Άρθρο:292B

Τίτλος: Παρακώλυση λειτουργίας πληροφοριακών συστημάτων (παρ. 1,2 και 3)

1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει την λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.
2. Η πράξη της πρώτης παραγράφου τιμωρείται:
 - a. με φυλάκιση από ένα έως τρία έτη, αν τελέστηκε με την χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημιές και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων,
 - b. με φυλάκιση τουλάχιστον ενός έτους, αν προκάλεσε σοβαρές ζημιές ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων,
 - c. με φυλάκιση τουλάχιστον ενός έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτική σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3. *Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών.*”

“Άρθρο:292Γ

Τίτλος: Παρακώλυση λειτουργιών πληροφοριακών συστημάτων

«Με φυλάκιση μέχρι δύο ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύει προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί:

- a. συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό διάπραξης των εγκλημάτων του άρθρου 292Β,
- b. συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με την χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

“Άρθρο:370Α

Τίτλος: Παραβίαση του Απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας

1. Όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλον τρόπο παρεμβαίνει σε συσκευή, σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού, που χρησιμοποιείται για την παροχή τέτοιων υπηρεσιών, με σκοπό ο ίδιος ή άλλος να πληροφορηθεί ή να αποτυπώσει σε υλικό φορέα το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων ή τα στοιχεία της θέσης και κίνησης της εν λόγω επικοινωνίας, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της τηλεφωνικής επικοινωνίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.
2. Όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή αποτυπώνει σε υλικό φορέα προφορική συνομιλία μεταξύ τρίτων ή αποτυπώνει σε υλικό φορέα μη δημόσια πράξη άλλου, τιμωρείται με κάθειρξη μέχρι δέκα ετών. Με την ίδια ποινή τιμωρείται η πράξη του προηγούμενου εδαφίου και όταν ο δράστης αποτυπώσει σε υλικό φορέα το περιεχόμενο της συνομιλίας του με άλλον χωρίς τη ρητή συναίνεση του τελευταίου.
3. Με κάθειρξη μέχρι δέκα ετών τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπονται στις παραγράφους 1 και 2 αυτού του άρθρου.
4. Αν ο δράστης των πράξεων των παραγράφων 1, 2 και 3 αυτού του άρθρου είναι πάροχος υπηρεσιών τηλεφωνίας ή νόμιμος εκπρόσωπος αυτού ή μέλος της διοίκησης ή υπεύθυνος διασφάλισης του απορρήτου ή εργαζόμενος ή συνεργάτης του παρόχου ή ενεργεί ιδιωτικές έρευνες ή τελεί τις πράξεις αυτές κατ' επάγγελμα ή κατά συνήθεια ή απέβλεπε στην είσπραξη αμοιβής, επιβάλλεται κάθειρξη μέχρι

δέκα ετών και χρηματική ποινή από πενήντα πέντε χιλιάδες (55.000) μέχρι διακόσιες χιλιάδες (200.000) ευρώ.

5. Αν οι πράξεις των παραγράφων 1 και 3 αυτού του άρθρου συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του κράτους ή την ασφάλεια εγκαταστάσεων κοινής ωφέλειας, τιμωρούνται κατά τα άρθρα 146 και 147 του Ποινικού Κώδικα.”

“Άρθρο:370B

Τίτλος: Παραβίαση Προγραμμάτων-Στοιχείων Ηλεκτρονικών Υπολογιστών (παρ. 1)

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.”

“Άρθρο:370Γ

Τίτλος: Παράνομη πρόσβαση σε πληροφοριακό σύστημα (παρ.1 και 2)

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.
2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.”

“Άρθρο:381Α

Τίτλος: Φθορά ηλεκτρονικών δεδομένων (παρ. 1)

1. Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιοδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.”

“Άρθρο:385Α

Τίτλος:Εκβίαση (παρ. 1)

1. Όποιος, εκτός από τις περιπτώσεις του άρθρου 380, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, εξαναγκάσει κάποιον με βία ή με απειλή σε πράξη, παράλειψη ή ανοχή από την οποία επέρχεται ζημία στην περιουσία εξαναγκασμένου ή άλλου τιμωρείται από φυλάκιση τριών μηνών έως και δέκα ετών.”

“Άρθρο:386

Τίτλος: Απάτη (παρ. 1)

1. Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώση παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών.”

“Άρθρο:386Α

Τίτλος: Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του Άρθρου 386. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα.”

Κεφάλαιο 4ο

Ανάλυση Ερευνών

Το ηλεκτρονικό έγκλημα έχει δημιουργήσει στους ανθρώπους τον φόβο κατά την χρήση του διαδικτύου. Μέχρι τώρα όμως δεν είχε προκύψει θάνατος λόγω μιας κακόβουλης επίθεσης. Συγκεκριμένα, σύμφωνα με την έρευνα των (Rameem Zahra et al., 2022) σημειώθηκε το πρώτο περιστατικό θανάτου εξαιτίας μιας Ransomware επίθεσης. Αναλυτικότερα, το 2020, εν μέσω την έξαρσης της πανδημίας του Covid-19, στο πανεπιστημιακό νοσοκομείο του Ντίσελντορφ της Γερμανίας, μία γυναίκα έχασε την ζωή της εξαιτίας μιας κυβερνοεπίθεσης. Ο λόγος ήταν ότι η επίθεση προκάλεσε την εκ νέου δρομολόγηση της ασθενούς σε ένα νοσοκομείο που βρισκόταν σε απόσταση τουλάχιστον 30χλμ. Οι εσωτερικοί διακομιστές (servers) του νοσοκομείου ήταν όλοι κλειδωμένοι, για αυτόν τον λόγο δεν μπορούσαν να την παραλάβουν. Επίσης, το 2015 μία επίθεση Ransomware δημιούργησε ζημία ύψους 325USD. Χρησιμοποίησαν μια εργαλειοθήκη ικανή για επιθέσεις στις ευπάθειες των λογισμικών, την CryptoWall 3.0. Η CryptoWall 3.0 αναζητούσε αρχεία στους υπολογιστές των θυμάτων, κρυπτογραφούσε τα έγγραφα και διέγραφε τα πρωτότυπα του χρήστη. Στην συνέχεια, ζητούσε από τους χρήστες να πληρώσουν χιλιάδες δολάρια σε λύτρα για να τα πάρουν πίσω. Οι υπολογιστές που μολύνθηκαν ήταν εκατοντάδες χιλιάδες σε όλο τον κόσμο. (Sarre et al., 2018) Πριν από αυτό, τον Μάιο του 2000 εκτέθηκαν πολλοί υπολογιστές στον ιό “Love Bug”. Μεταξύ των μολυσμένων συστημάτων βρέθηκαν και κυβερνητικές υπηρεσίες των Ηνωμένων Πολιτειών Αμερικής και της Αγγλίας. Για την συγκεκριμένη επίθεση κατηγορήθηκε ένας φοιτητής από τις Φιλιππίνες, του οποίου οι κατηγορίες αποσύρθηκαν, εφόσον δεν υπήρχε νομοθεσία για το ηλεκτρονικό έγκλημα στις Φιλιππίνες. Στη συνέχεια, όπως αναφέρεται στην ίδια έρευνα (Μπενέτου, 2021), τον Ιούλιο του 2016, στο Ντάλας του Τέξας, η αστυνομία αναζητούσε για να εξαλείψει με την χρήση ενός ρομπότ έναν ελεύθερο σκοπευτή, ο οποίος ευθυνόταν για τον θάνατο πέντε αστυνομικών. Μάλιστα, ενώ η χρήση ρομπότ για δολοφονία υπόπτου δεν είναι συνηθισμένη, χρησιμοποιούνται συχνά τηλεκατευθυνόμενα ή μη επανδρωμένα αεροσκάφη με σκοπό την απενεργοποίηση ή πυροδότηση εκρηκτικού μηχανισμού. Σε συνέχεια της παράθεσης των ηλεκτρονικών εγκλημάτων, το 2009 ο 21χρονος Αυστραλός διέδωσε έναν ιό (worm) στα κινητά τηλέφωνα, iPhone, αλλάζοντας την ταπετσαρία οθόνης με μία φωτογραφία του Rick Astley και εμφάνιζε το μήνυμα “IKEE is never gonna give you up”. Μετά από αυτό, η εταιρεία προσέλαβε τον Αυστραλό προγραμματιστή στο παράρτημα της στην Αυστραλία. (Tajpour et al., 2010)

Κατά την διάρκεια της πανδημίας, εξελίχθηκαν αρκετά οι επιθέσεις ηλεκτρονικού εγκλήματος και κυρίως του ηλεκτρονικού ψαρέματος. Πράγματι, στην έρευνα (Bitaab et al., 2020) αναφέρεται ότι δημιουργήθηκαν ιστοσελίδες πανομοιότυπες με φιλανθρωπικών οργανισμών, οι οποίες αποζητούσαν δωρεές για το Κέντρο Ελέγχου Ανταπόκρισης Ασθενειών της Αμερικής για τον κορονοϊό. Και ενώ οι χρήστες νόμιζαν ότι έκαναν κάποια δωρεά για φιλανθρωπικό σκοπό, στην πραγματικότητα έδιναν ευαίσθητα προσωπικά δεδομένα, εφόσον οι επιτιθέμενοι κρατούσαν τα στοιχεία της κάρτας και δεν πραγματοποιούσαν η δωρεά. Η έρευνα των (Akdemir & Yenal, 2021) αναφέρει πως κατά την διάρκεια του εγκλεισμού, οι

άνθρωποι περνούσαν περισσότερο χρόνο στο διαδίκτυο, γεγονός που τους έκανε πιο πιθανό να συναντήσουν παραβάτες με κίνητρα. Μερικοί άνθρωποι άρχισαν να παρακολουθούν δωρεάν ταινίες σε ιστότοπους που δεν είναι ασφαλείς, ένα γεγονός που αύξησε την ευπάθεια των υπολογιστών τους στην μολυσματική επίθεση. Ορισμένες μελέτες λένε ότι η καραντίνα της πανδημίας δεν έκανε τους ανθρώπους να αλλάξουν τον τρόπο που χρησιμοποιούν το διαδίκτυο, οπότε δεν διέτρεχαν μεγαλύτερο κίνδυνο να πέσουν θύματα ηλεκτρονικού εγκλήματος. Οι διαφορές μεταξύ των μελετών μπορεί να οφειλόταν στο γεγονός ότι οι άνθρωποι έκαναν διαφορετικά πράγματα στο διαδίκτυο κατά την διάρκεια του εγκλεισμού. Η μία μελέτη έδειξε ότι οι άνθρωποι έκαναν επικίνδυνα πράγματα, ενώ μία άλλη παρουσίασε πως οι άνθρωποι δεν άλλαξαν τον τρόπο με τον οποίο ενεργούσαν στο διαδίκτυο. Συγκεντρωτικά, οι μελέτες αυτές δείχνουν ότι το να κάνεις επικίνδυνα πράγματα στο διαδίκτυο αυξάνει τις πιθανότητες να πέσεις θύμα εγκλήματος στον κυβερνοχώρο.

Το 2005 προτάθηκε ένα πλαίσιο για την μέτρηση των επιπέδων ευαισθητοποίησης του προσωπικού στον τομέα της ασφάλειας. Σε ένα πανεπιστήμιο της Νότιας Αφρικής διεξήχθη ένα τεστ Phishing για την ευαισθητοποίηση του προσωπικού στον τομέα της κλοπής ταυτότητας (πλαστοπροσωπίας - identity theft). Στόχος του πειράματος ήταν να μετρηθεί η αντίδραση του προσωπικού στην κλοπή ταυτότητας και να αυξηθεί η ευαισθητοποίηση στον τομέα της ασφάλειας σχετικά με τους διαδικτυακούς κινδύνους. Αποφασίστηκε να χρησιμοποιηθεί μόνο ένα δείγμα μελών του προσωπικού. Η μελέτη διεξήχθη σε τρεις φάσεις, δύο δοκιμές και μία τελική δοκιμή. Το μήνυμα ηλεκτρονικού ταχυδρομείου στάλθηκε σε τυχαία επιλεγμένη ομάδα μελών του προσωπικού απαρτιζόμενη από 400 άτομα. Εφόσον έστειλαν το μήνυμα στο δείγμα του πειράματος, άφησαν περιθώριο επτά ημερών για να ξεκινήσουν να αναλύουν τα αποτελέσματα. Το ποσοστό ανταπόκρισης ανήλθε περίπου στο 80% και περισσότερα από τα μισά μέλη του προσωπικού ήταν πρόθυμα να δώσουν τους κωδικούς τους. (Steyn et al., 2007)

Επιπλέον, αναφορικά με την μέτρηση της ευαισθησίας των χρηστών, εξετάστηκαν δύο είδη σφαλμάτων των χρηστών του διαδικτύου με σκοπό την μέτρηση των ατόμων να πέσουν θύματα ηλεκτρονικού ψαρέματος.

1. Ψευδώς θετικό αποτέλεσμα. Στη περίπτωση αυτή ο χρήστης κρίνει εσφαλμένα ένα νόμιμο μήνυμα στο ηλεκτρονικό ταχυδρομείο ή έναν ιστότοπο ως phish και αρνείται να προβεί στις απαραίτητες επιθυμητές ενέργειες.
2. Πτώση στο phish. Όταν ένα μήνυμα στο ηλεκτρονικό ταχυδρομείο ή ένας ιστότοπος phishing κρίνεται ως νόμιμο και ωθεί τους χρήστες να κάνουν κλικ σε κακόβουλους συνδέσμους ή υποβάλλουν πληροφορίες στην ιστοσελίδα.

Σύμφωνα με την μελέτη (Sheng et al., 2010) το 50% των συμμετεχόντων θα έκαναν κλικ σε συνδέσμους phishing και έπειτα το 40% θα προχωρούσε και στην παροχή ευαίσθητων προσωπικών δεδομένων.

Μία αξιολογημένη μελέτη πραγματοποίησαν οι (Λιοντήρης & Μπάκας, 2016), οι οποίοι τέλεσαν για την πτυχιακή τους εργασία μία προσομοίωση των επιθέσεων ηλεκτρονικού εγκλήματος με παραπλανητικές ιστοσελίδες και κακόβουλα μηνύματα στο ηλεκτρονικό ταχυδρομείο. Οι ιστοσελίδες που έφτιαξαν είναι φαινομενικά ίδιες με τις νόμιμες (πρωτότυπες). Χρησιμοποίησαν μία ιστοσελίδα από τα μέσα κοινωνικής δικτύωσης, το Facebook, την ιστοσελίδα ηλεκτρονικών συναλλαγών μιας τράπεζας, την Eurobank, καθώς και μια ιστοσελίδα ηλεκτρονικού εμπορίου, την Amazon. Προγραμμάτισαν τις ιστοσελίδες ώστε να είναι αμελητέες οι διαφορές τους από τις αυθεντικές, ώστε να μπορεί να τις εμπιστευτεί ο χρήστης. Επίσης, σε κάθε ιστοσελίδα, μετά την συμπλήρωση των στοιχείων σύνδεσης και πατώντας το κουμπί υποβολής, ανακατευθυνόντουσαν στον αυθεντικό ιστότοπο με το μήνυμα λανθασμένων στοιχείων σύνδεσης. Αυτήν την τακτική την δημιούργησαν στις ιστοσελίδες του Facebook, και της Eurobank. Κατά την εκτέλεση της επίθεσης, η οποία πραγματοποιήθηκε δοκιμαστικά στο τοπικό τους δίκτυο, αντιλήφθηκαν ότι, ενώ με το Facebook η ροή των απατηλών ενεργειών κυλούσε ομαλά, με αποτέλεσμα να μην υποψιαστεί το χρήστης ότι έπεσε θύμα υποκλοπής στοιχείων σύνδεσης, στην ιστοσελίδα της Eurobank, όταν γινόταν η ανακατεύθυνση στην ιστοσελίδα της τράπεζας, έβγαζε ένα μήνυμα προειδοποίησης στον χρήστη, γεγονός που τον προειδοποιεί να αντιληφθεί ότι έπεσε θύμα, με αποτέλεσμα να αχρηστευτούν τα στοιχεία σύνδεσης που αποκόμισε ο επιτιθέμενος.

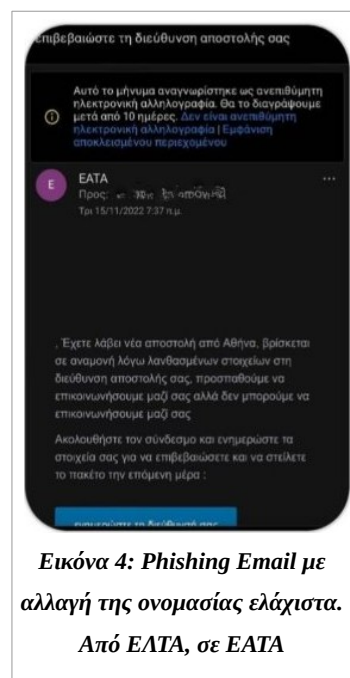
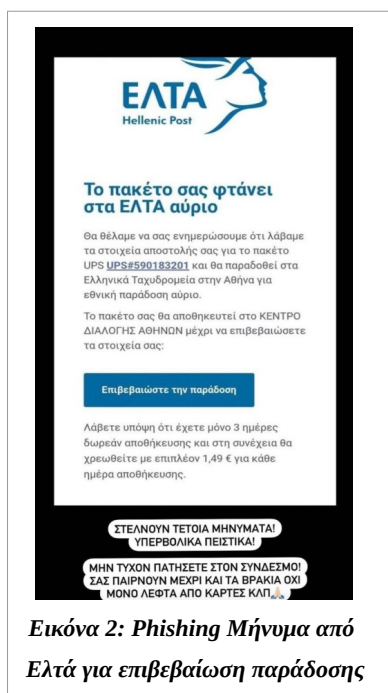
Στο δεύτερο μέρος της έρευνάς τους, προσομοίωσαν ένα ολοκληρωμένο σενάριο ηλεκτρονικού ψαρέματος. Δημιούργησαν ένα πρόγραμμα μαζικής αποστολής email και στην συνέχεια συνέταξαν τον μήνυμα Phishing που θα έστελναν. Το μήνυμα παρουσίαζε κάποιο σφάλμα στα στοιχεία σύνδεσης του λογαριασμού και ζητούσε από τον χρήστη να ακολουθήσει τον σύνδεσμο και να συνδεθεί. Σε αυτή τη μελέτη χρησιμοποιήθηκε ξανά η ιστοσελίδα του Facebook αλλά και της Amazon. Στον ψεύτικο ιστότοπο του Facebook πρόσθεσαν ένα μήνυμα που ζητούσε επιβεβαίωση των στοιχείων σύνδεσης του χρήστη, με σκοπό να γίνει πειστικό. Για την ιστοσελίδα της Amazon, του ζητούσε να συνδεθούν στον λογαριασμό τους και στην συνέχεια να δώσουν τα στοιχεία της κάρτας τους για να κερδίσουν κάποιες προσφορές και εκπτώσεις σε μερικά προϊόντα. Για να διαπιστώσουν εάν θα είναι πετυχημένες οι παραπλανητικές ιστοσελίδες και τα μηνύματα phishing που δημιούργησαν, έκαναν δοκιμές σε φίλους τους. Παρατήρησαν ότι σχεδόν όλοι έδωσαν τα στοιχεία σύνδεσης του λογαριασμού τους στην πλατφόρμα του Facebook. Για λόγους προσωπικών δεδομένων δεν στάλθηκαν τα email για την ιστοσελίδα της Amazon διότι μπορεί κάποιος να έστελνε τα στοιχεία της κάρτας του. Τους ρώτησαν όμως υποθετικά, τι θα έκαναν αν δεχόντουσαν αυτό το email και οι περισσότεροι απάντησα πως δεν θα έδιναν τα στοιχεία της κάρτας εάν δεν πραγματοποιούσαν εκείνη την ώρα κάποια αγορά.

Οι (Mayuri et al., 2012) δημιούργησαν μία αποτελεσματική προσέγγιση εντοπισμού του Phishing εμπνευσμένοι από δύο άλλα εργαλεία, το DOMAntiPhish και το AntiPhish, στο οποίο μέσω της σύγκρισης ομοιότητας από κείμενο, ενσωματωμένες εικόνες και την γενική απεικόνιση, εντόπιζαν τις phishing ιστοσελίδες. Είναι γνωστό πως ο χρήστης εμπιστεύεται με το πως φαίνεται και αν τον αισθάνεται οικείο έναν ιστότοπο, γι' αυτό και οι δράστες προσπαθούν να δημιουργούν “καλοφτιαγμένα” site. Το συγκεκριμένο

εργαλείο εκτέθηκε σε 41 phishing ιστοσελίδες, από τις οποίες για καμία δεν υπήρχε λανθασμένος συναγερμός (να ήταν η νόμιμη ιστοσελίδα και να την θεώρησε ως παραπλανητική ή κακόβουλη) και μόνο δύο απόπειρες ηλεκτρονικού ψαρέματος, οι οποίες δεν έμοιαζαν με την νόμιμη ιστοσελίδα, δεν ανιχνεύτηκαν.

Παραδείγματα από θύματα και απάτες

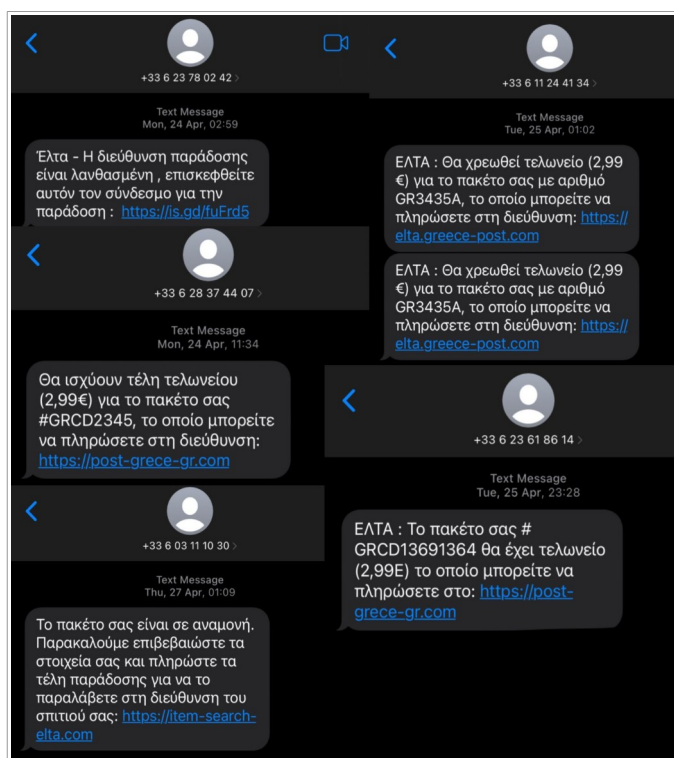
Κατά την διάρκεια της συγγραφής της πτυχιακής μου εργασίας, συγκέντρωσα υλικό από επιθέσεις ηλεκτρονικού ψαρέματος. Το υλικό είναι είτε από επιθέσεις που αποστέλλαν το μήνυμα σε προσωπικές μου συσκευές, είτε από γνωστούς και φίλους που κοινοποιούσαν το στιγμιότυπο οθόνης, βοηθώντας τον περίγυρό τους να αποφύγει τις επιθέσεις.



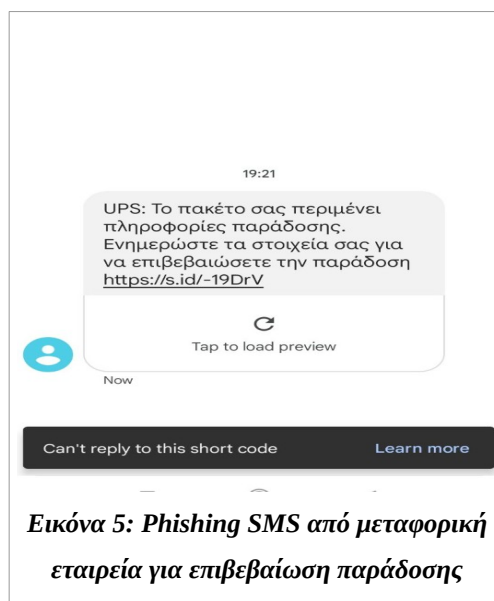
Παρατηρήθηκε από την περίοδο της πανδημίας που επικρατούσε ο εγκλεισμός στα σπίτια, η αύξηση των διαδικτυακών αγορών. Ένα διάστημα μάλιστα είχαν τεράστιο φόρτο εργασία οι μεταφορικές εταιρείες και δυσκολευόντουσαν στην αποθήκευση των πακέτων αλλά και στην κατανομή τους. Αυτό δημιούργησε άγχος στο προσωπικό και αύξηση των λαθών αλλά και των καθυστερήσεων. Κυρίως όμως ξεκίνησε ο καταναλωτής τα παράπονα. Δεν ήταν όμως αυτή η αφορμή πολλών ανθρώπων να πέσουν θύματα ηλεκτρονικού ψαρέματος. Οι εγκληματίες του διαδικτύου βρήκαν αφορμή να “ψαρέσουν” τους ανθρώπους στέλνοντας μηνύματα στα οποία παρίσταναν τις μεταφορικές εταιρείες (courier) και ζητούσαν επιβεβαίωση στοιχείων. Σε κάποιες περιπτώσεις χρησιμοποιούσαν την απειλή επιπλέον χρέωσης στους παραλήπτες για την αποθήκευση του πακέτου στις αποθήκες της μεταφορικής, αλλά το πιο συνηθισμένο ήταν να ζητάνε την επιβεβαίωση των στοιχείων ώστε ο παραλήπτης να εξασφαλίσει την άφιξη του πακέτου του στην σωστή διεύθυνση.

Μπορούμε να αντιληφθούμε ότι οι επιτιθέμενοι εκμεταλλεύτηκαν την κατάσταση άγχους και σύγχυσης της κατηγορίας ανθρώπων που ακολούθησαν την παραγγελία προϊόντων διαδικτυακά λόγω εγκλεισμού, οι οποίοι αποτελούσαν την πλειοψηφία. Δεν ήταν λίγες οι περιπτώσεις που άλλαζαν ελάχιστα τις ονομασίες των μεταφορικών εταιρειών, ώστε να παραπλανήσουν τους παραλήπτες των μηνυμάτων. Επίσης, τα μηνύματα στο κινητό (SMS) αποστέλλονται συχνά από διαφορετικό αριθμό κινητής τηλεφωνίας, αλλά είναι στρατηγικά μελετημένα ώστε να έχουν λογική συνέχεια τα μηνύματα και να αναγράφουν τον ίδιο αριθμό αποστολής και να πιέζουν την επιβεβαίωση στοιχείων με την επιπλέον χρέωση.

Η θετική πλευρά αυτών των επιθέσεων είναι ότι πολλές φορές τα μηνύματα αναγνωρίζονταν από τους διακομιστές ως παραπλανητικά ή ακόμα και ως ανεπιθύμητα, με αποτέλεσμα οι χρήστες να προειδοποιούνται για την κακόβουλη προσπάθεια των επιτιθέμενων και να αντιληφθούν πως δεν πρέπει να ακολουθήσουν τις οδηγίες από τα παραπλανητικά μηνύματα.



Εικόνα 6: Phishing SMS κατά σειρά, με απειλή χρέωσης τελωνείου εάν δεν προβεί στην επίσκεψη του συνδέσμου ή την πληρωμή μέσω αυτού.



Εικόνα 5: Phishing SMS από μεταφορική εταιρεία για επιβεβαίωση παράδοσης

Άλλος ένας φορέας που μιμήθηκαν αρκετά κατά την διάρκεια της πανδημίας είναι η κυβέρνηση. Λόγω του εγκλεισμού της καραντίνας του Κορονοϊού, οι άνθρωποι αναζητούσαν καθημερινά ενημέρωση από την κυβέρνηση του κράτους τους ώστε να βγουν από την άγνοια της νέας πανδημίας. Εν συνεχεία, κατά την διάρκεια της καραντίνας, έγινε παύση εργασίας σχεδόν σε όλους του τομείς επιχειρήσεων και υπηρεσιών, και για την οικονομική στήριξη των πολιτών, χορηγήθηκε επίδομα τόσο στους εργαζόμενους όσο και στους επιχειρηματίες. Αναμενόμενο είναι να καθυστερούν οι καταθέσεις των επιδομάτων σε όλους του πολίτες της χώρας. Αυτό ήταν αφορμή να ξεγελάσουν οι επιτιθέμενοι τους χρήστες, στέλνοντας μηνύματα παριστάνοντας την πλατφόρμα της κυβέρνησης που τους ενημερώνει για νέο επίδομα που δικαιούνται και πως πρέπει να βιαστούν να επιβεβαιώσουν τα στοιχεία ώστε να γίνει η κατάθεση στον λογαριασμό τους. Παράλληλα, γινόντουσαν μειώσεις στα μισθωτήρια των ενοικιασμένων σπιτιών εκτός του νομού κατοικίας, και οι επιτιθέμενοι δεν άργησαν να απειλήσουν με ψεύτικα μισθωτήρια στο όνομα των χρηστών, ισχυριζόμενοι πως έχει γίνει ήδη η υποβολή δήλωσης πληροφοριακών στοιχείων μίσθωσης ακίνητης περιουσίας.



**Εικόνα 7: Phishing μήνυμα
εικονικά από την κυβέρνηση**

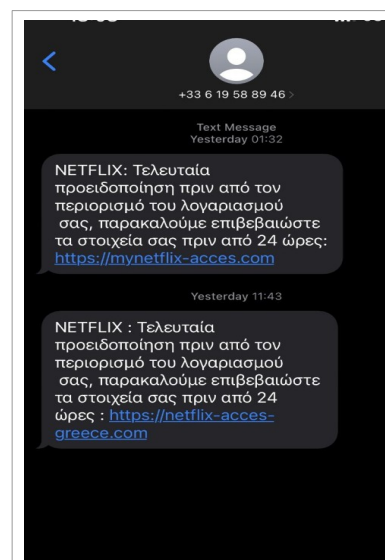
Γενικότερα, οι προαναφερόμενες απάτες δεν πραγματοποιήθηκαν μόνο κατά την περίοδο της



**Εικόνα 8: Phishing μήνυμα για
μισθωτήριο ακίνητης περιουσίας.**

πανδημίας του κορονοϊού, αλλά συνεχίστηκαν και αργότερα και σε μεγαλύτερη συχνότητα. Μετά το πέρας της έξαρσης της πανδημίας, δεν σταμάτησαν να εφευρίσκουν τρόπους να παραπλανήσουν τους χρήστες. Εκμεταλλεύονται οποιαδήποτε είδηση γίνεται γνωστή πριν τεθούν σε εφαρμογή τα μέτρα. Για παράδειγμα, είχε αναρτηθεί η είδηση για την πλατφόρμα παρακολούθησης ταινιών και τηλεοπτικών σειρών πως θα επιβάλλει καινούργια μέτρα για τον μετριασμό των αδειών για τις οθόνες για κάθε λογαριασμό. Πιο συγκεκριμένα, είχε γίνει μεγάλος ντόρος για το Netflix το οποίο είχε σκοπό να περιορίσει τις οθόνες προβολής ανά λογαριασμό χρήστη, ώστε να σταματήσει η κατάχρηση ενός λογαριασμού από πολλούς ανθρώπους. Έτσι, έστειλαν οι επιτιθέμενοι μηνύματα στα οποία απειλούσαν τον υπεύθυνο του λογαριασμού, τον χρήστη ο οποίος είχε δώσει τα στοιχεία τραπεζικού λογαριασμού ώστε να πραγματοποιείται η πληρωμή κάθε μήνα, πως πρέπει να επιβεβαιώσει τα στοιχεία πληρωμής στις επόμενες 24 ώρες ώστε

να μην περιορίσουν τον λογαριασμό (block). Τα μηνύματα έδειχναν αποστολέα έναν εννιάψηφιο αριθμό με κωδικό κλήσης χώρας +33, ο οποίος κωδικός είναι της Γαλλίας. Μέσα στο SMS υπήρχε ένα link το οποίο έπρεπε να ακολουθήσει ο χρήστης. Ένα στοιχείο πως το μήνυμα ήταν απάτη ήταν τα URL τα οποία ήταν διαφορετικά μεταξύ τους, από τον ίδιο παραλήπτη.

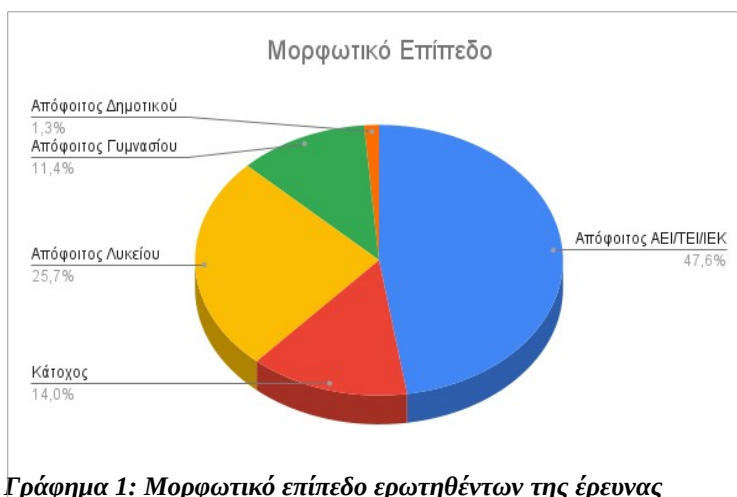


Εικόνα 9: Phishing SMS από το Netflix με απειλή απενεργοποίηση λογαριασμού

Κεφάλαιο 5ο

Μεθοδολογία Έρευνας

Στην παρούσα πτυχιακή εργασία πραγματοποιήθηκε έρευνα σε μορφή ερωτηματολογίου. Το ερωτηματολόγιο απαρτιζόταν από πέντε ενότητες, εκ των οποίων οι τρεις ήταν κοινές για όλους τους συμμετέχοντες. Στην πρώτη ενότητα υπήρχαν τρεις ερωτήσεις για τα δημογραφικά στοιχεία (Φύλο, Ηλικία, Μορφωτικό επίπεδο). Στην δεύτερη ενότητα (έξι ερωτήσεις) προωθούνταν μόνο όσοι απάντησαν πως είναι κάτω των 18 χρονών (στην προηγούμενη ενότητα) και οι ερωτήσεις ήταν σχετικές με την χρήση του διαδικτύου και τις πληρωμές που πραγματοποιούν τα ανήλικα με ή χωρίς επίβλεψη. Στην τρίτη ενότητα, οι ερωτήσεις ήταν σχετικές με την χρήση του διαδικτύου (έξι ερωτήσεις) ενώ στην τέταρτη ενότητα η θεματολογία αφορούσε την ασφάλεια στο διαδίκτυο (11 ερωτήσεις). Στην πέμπτη ενότητα κατευθύνονταν μόνο όσοι συμμετέχοντες είχαν απαντήσει θετικά στην ερώτηση αν έχουν πέσει θύμα ηλεκτρονικού ψαρέματος. Σε αυτήν την ενότητα οι ερωτήσεις ήταν σχετικές με το συμβάν (Πότε πέσατε θύμα, Πότε το αντιληφθήκατε, Με ποια μέθοδο, Χρηματικό ποσό που χάσατε κ.α.).



Γράφημα 1: Μορφωτικό επίπεδο ερωτηθέντων της έρευνας

Για την δημιουργία του ερωτηματολογίου, υπήρχε μια προεργασία. Αρχικά, σημειώθηκαν κάποια ερωτήματα στα οποία θα θέλαμε να βρούμε τις απαντήσεις από το ερωτηματολόγιο. Μερικά από αυτά ήταν, αν τα θύματα Phishing είναι κατηγοριοποιημένα σε φύλο, ηλικία και μορφωτικό επίπεδο. Επίσης, θέλαμε να ανακαλύψουμε και την γενικότερη εικόνα των χρηστών του διαδικτύου σχετικά με τις γνώσεις τους για την ασφαλή πλοήγηση. Κατά την επεξεργασία των δεδομένων, δημιουργήθηκαν επιπλέον ερωτήσεις, τις οποίες θα παρουσιαστούν παρακάτω.



Γράφημα 2: Εύρος ηλικίας ερωτηθέντων της έρευνας

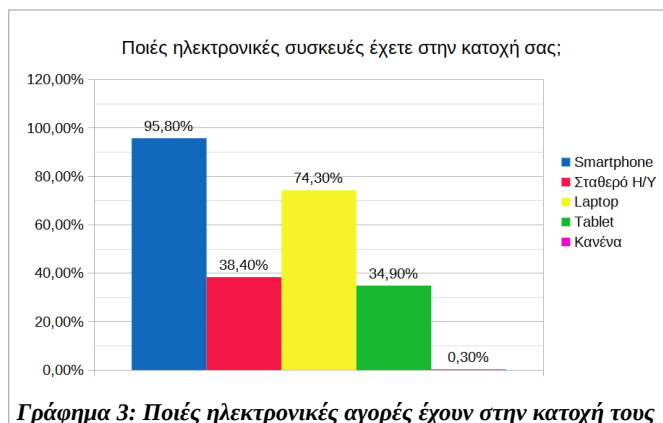
Το ερωτηματολόγιο απαντήθηκε από 307 άτομα, εκ των οποίων το 70% (215 άτομα) ήταν γυναίκες και το 30% (92 άτομα) ήταν άντρες. Οι ερωτηθέντες ήταν σε μεγάλο εύρος ηλικίας, εφόσον υπήρχαν

ανήλικοι έως και άνθρωποι άνω των 60 ετών. Στην πλειοψηφία των ερωτηθέντων ήταν απόφοιτοι τριτοβάθμιας εκπαίδευσης, δεν έλειπαν όμως και οι απόφοιτοι πρωτοβάθμιας/δευτεροβάθμιας αλλά και οι κάτοχοι μεταπτυχιακού και διδακτορικού. Οι ανήλικοι που απάντησαν το ερωτηματολόγιο ήταν 42 (13,7%) οι οποίοι το 7,1% είναι απόφοιτοι δημοτικού, το 14,3% απόφοιτοι λυκείου και το 78,6% είναι απόφοιτοι γυμνασίου. Στους ενήλικους ερωτηθέντες, το μορφωτικό επίπεδο κατά κύρια βάση είναι απόφοιτοι ΑΕΙ/ΤΕΙ/ΙΕΚ (47,6%) και στην συνέχεια είναι απόφοιτοι λυκείου (25,7%).

Αποτελέσματα έρευνας και ανάλυση δεδομένων

Κατά την επεξεργασία των δεδομένων παρουσιάστηκαν διάφορα ερωτήματα και έπειτα δημιουργήθηκαν και τα αντίστοιχα διαγράμματα. Σαν αποτέλεσμα του ερωτηματολογίου μπορούμε να βγάλουμε μερικά συμπεράσματα, τουλάχιστον για το δείγμα που πήραμε.

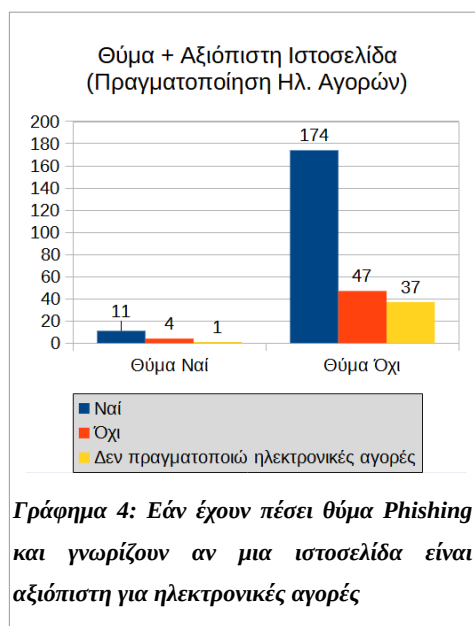
Από τα αποτελέσματα της έρευνας μπορούμε να συμφωνήσουμε ότι η τεχνολογία



έχει εντυφώσει στην καθημερινότητα του ανθρώπου, εφόσον στις ερωτήσεις για την κατοχή ηλεκτρονικών συσκευών (Smartphone, Σταθερό Η/Υ, Laptop, Tablet) μόνο ένας από τους συμμετέχοντες απάντησε πως δεν έχει καμία από αυτές τις συσκευές. Πολλές ήταν οι περιπτώσεις που είχαν παραπάνω από μία. Στην πραγματικότητα δεν μας εκπλήσσει το αποτέλεσμα, εφόσον καθημερινά προωθούμε όλοι στην αυτοματοποίηση των διαδικασιών στις επιχειρήσεις και στις υπηρεσίες.

Αμέσως επόμενο είναι και ο χρόνος που καταναλώνουν καθημερινά οι ερωτηθέντες στο διαδίκτυο. Στην πλειοψηφία απάντησαν πως πλοηγούνται στο διαδίκτυο από δύο έως τέσσερις ώρες (40,4%), το 31,6% απάντησε πως καταναλώνει παραπάνω από τέσσερις ώρες καθημερινά, ενώ μόλις το 3,9% δήλωσε πως περνάει λιγότερο από μία ώρα στο ίντερνετ.

Όσον αφορά την ασφάλεια των χρηστών στο διαδίκτυο, υπάρχουν χρήστες (2%) που δεν γνωρίζουν εάν διαθέτουν αντικό λογισμικό (antivirus) στις ηλεκτρονικές συσκευές τους ενώ το 13,7% των συμμετεχόντων της έρευνας, δεν έχει εγκαταστήσει συνειδητά κάποιο αντικό λογισμικό. Επίσης παρατηρείται πως τα τρία τέταρτα του συνόλου δηλώνει πως γνωρίζει να εντοπίζει τις ενδείξεις μίας ιστοσελίδας που την καθιστά επικίνδυνη (red flags), καθώς και το 90,6% είναι



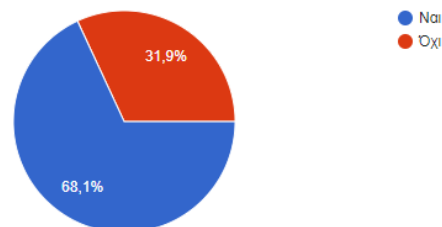
ενημερωμένο σχετικά με τα προσωπικά στοιχεία που δεν πρόκειται να τους ζητηθούν από την τράπεζα. Σχετικά με την ενημέρωση του συνόλου για το διαδίκτυο, στην ερώτηση εάν γνωρίζουν τι είναι το ηλεκτρονικό ψάρεμα (Phishing) το 81,8% απάντησε θετικά. Ενώ το 68,1% και 51,8% απάντησαν ότι έχουν λάβει email και SMS, αντίστοιχα, τα οποία θεώρησαν ότι είναι παραπλανητικά, καθώς τους ζητούσαν επιβεβαίωση στοιχείων σύνδεσης.

Το ηλεκτρονικό ψάρεμα έχει γίνει ευρέως γνωστό κυρίως από την έξαρση της πανδημίας Covid-19 και μετά. Πάνω σε αυτό, ρωτήσαμε τους συμμετέχοντες εάν γνωρίζουν τον όρο Phishing. Ενδιαφέρον είχε ο συνδυασμός της με την ερώτηση για ποιον λόγο χρησιμοποιούν το διαδίκτυο, για εργασία/εκπαίδευση ή για ψυχαγωγία. Οι περισσότεροι χρήστες του διαδικτύου που γνωρίζουν τον όρο phishing δεν χρησιμοποιούν τόσο το διαδίκτυο για την εργασία τους ή την εκπαίδευση, αλλά για ψυχαγωγία. Μόλις το 18,24% των συμμετεχόντων απάντησε πως δεν

γνώριζε τον όρο του Phishing. Στην συνέχεια, θέλαμε να διαπιστώσουμε εάν η γνώσεις των χρηστών για το διαδίκτυο παίζουν σημαντικό ρόλο στις γνώσεις για τις κυβερνοεπιθέσεις. Για αυτόν τον λόγο συνδυάσαμε τις ερωτήσεις, “πως θα χαρακτηρίζατε τις γνώσεις σας σχετικά με την χρήση του διαδικτύου;” με “γνωρίζετε τι είναι το phishing – Ηλεκτρονικό Ψάρεμα;”. Τα αποτελέσματα έδειξαν πως, όσοι δηλώνουν πως έχουν άριστες γνώσεις για την χρήση του διαδικτύου γνωρίζουν και τον όρο Phishing ενώ η πλειοψηφία που δήλωσε ότι δεν γνωρίζει τι σημαίνει το phishing, έχουν μέτριες γνώσεις χρήσης του διαδικτύου. Από τα παραπάνω μπορούμε να συμπεράνουμε πως, όσοι γνωρίζουν να χρησιμοποιούν αρκετά καλά το διαδίκτυο αλλά και όσοι το χρησιμοποιούν για ψυχαγωγικούς σκοπούς τείνουν να γνωρίζουν και τι είναι το ηλεκτρονικό ψάρεμα.

Έχετε λάβει email το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχεία σύνδεσης;

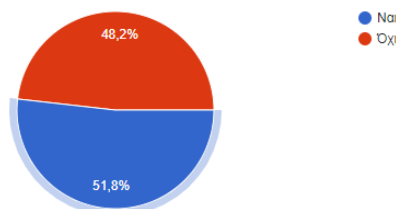
307 απαντήσεις



Γράφημα 5: Πόσοι από τους ερωτηθέντες έχουν λάβει Phishing Email

Έχετε λάβει SMS το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχεία σύνδεσης;

307 απαντήσεις



Γράφημα 6: Πόσοι από τους ερωτηθέντες έχουν λάβει Phishing SMS

Δημογραφικά Αποτελέσματα Θυμάτων

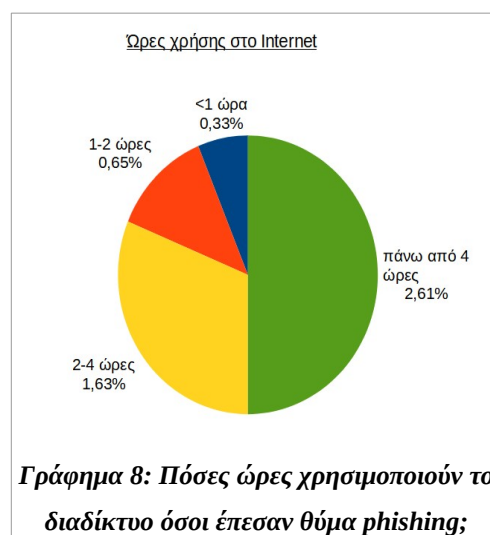
Όπως και σε άλλες έρευνες που αναζητούσαν τα δημογραφικά χαρακτηριστικά των θυμάτων, καταλήξαν ότι δεν παίζει κάποιο ρόλο το γένος, η ηλικία και το μορφωτικό επίπεδο. Και η δικιά μας έρευνα, επιβεβαιώνει τις προηγούμενες σε αυτόν τον τομέα. Από τους συμμετέχοντες που απάντησαν το ερωτηματολόγιο (307 άτομα) μόλις οι 16 δήλωσαν πως έχουν πέσει θύμα ηλεκτρονικού ψαρέματος. Αρχικά, λόγω της ανισότητας των συμμετεχόντων συγκριτικά με το φύλο (70% γυναίκες – 30% άντρες) δεν μπορούμε να βγάλουμε αξιόπιστο ποσοστό για το γένος. Παρόλα αυτά, από τα 16 άτομα που δήλωσαν ότι έχουν πέσει θύμα Phishing, το 75% των θυμάτων ήταν γυναίκες και το υπόλοιπο 25% άντρες. Με γνώμονα την ηλικία, τα θύματα κινούνται στην ηλικιακή κλίμακα 18 με 60 χρόνων, ίσα διαμοιρασμένα. Τα δεδομένα αλλάζουν για το μορφωτικό επίπεδο, στο οποίο η κλίμακα κυμαίνεται για τους απόφοιτους Λυκείου (ΓΕΛ/ΕΠΑΛ) 37,5% των θυμάτων, τους απόφοιτους ΑΕΙ/ΤΕΙ/ΙΕΚ 50% των θυμάτων και τους κατόχους Μεταπτυχιακού ή/και Διδακτορικού 12,5% των θυμάτων.

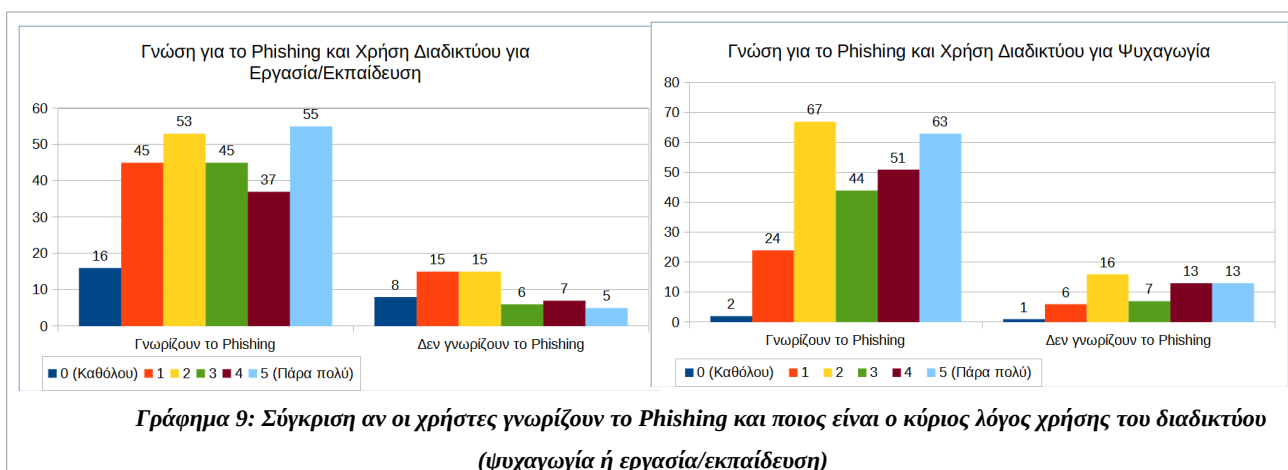


Συνήθειες Θυμάτων στο Διαδίκτυο

Σε συνάρτηση με την απόκτηση των γνώσεων για την χρήση του διαδικτύου, οι συμμετέχοντες που έχουν μάθει να χρησιμοποιούν το διαδίκτυο εμπειρικά, τείνουν στην πιθανότητα να πέσουν θύματα στο ηλεκτρονικό ψάρεμα (3,58% επί του συνόλου). Το 50% των θυμάτων απάντησαν ότι χρησιμοποιούν το διαδίκτυο παραπάνω από 4 ώρες ημερησίως, ενώ μόνο ένα θύμα απάντησε πως το χρησιμοποιεί λιγότερο από μία ώρα καθημερινά.

Επίσης, στην ερώτηση εάν γνωρίζουν τι δεν πρόκειται να τους ζητηθεί από την τράπεζα μέσω email, η συντριπτική πλειοψηφία, 87,5% των θυμάτων, απάντησε πως το γνωρίζει. Όσον αφορά την αξιοπιστία και τα σημάδια που καθιστά μια ιστοσελίδα κακόβουλη, οι περισσότεροι χρήστες που έχουν πέσει θύμα ηλεκτρονικού ψαρέματος, απάντησαν πως γνωρίζουν να ξεχωρίζουν μια ιστοσελίδα εάν έχει σημάδια που την καθιστά ύποπτη αλλά και να αναγνωρίζουν εάν μια ιστοσελίδα ηλεκτρονικού εμπορίου είναι αξιόπιστη για την πραγματοποίηση ηλεκτρονικής αγοράς.





Μία αξιοσημείωτη απάντηση ενός θύματος για την αξιοπιστία μιας ιστοσελίδας ηλεκτρονικού εμπορίου (βλ. Γράφημα 6) ήταν πως δεν πραγματοποιεί ηλεκτρονικές αγορές. Αυτό μας φέρνει το συμπέρασμα πως ακόμη και αν ένας χρήστης αποφεύγει τις ηλεκτρονικές αγορές δεν τον καθιστά ασφαλή από το ηλεκτρονικό ψάρεμα, εφόσον μπορούν να του υποκλέψουν τα στοιχεία σύνδεσης του λογαριασμού του. Στο γενικότερο σύνολο, το 56,67% μπορεί να ξεχωρίσει εάν μια ιστοσελίδα είναι αξιόπιστη ώστε να πραγματοποιήσει ηλεκτρονική αγορά και το 64,5% μπορεί να αντιληφθεί τα σημάδια μιας ιστοσελίδας που την καθιστά ύποπτη (επικίνδυνη για απάτη).

Τρόποι Χειρισμού μετά την Επίθεση από τα Θύματα

Σε ερώτηση προς τα θύματα του ηλεκτρονικού ψαρέματος, πως διαχειρίστηκαν την κατάσταση αφότου αντιλήφθηκαν ότι έπεσαν θύματα phishing, οι κινήσεις τους ήταν να καλέσουν την τράπεζα για να αναφέρουν τον περιστατικό, να αμφισβητήσουν την τραπεζική συναλλαγή, να συμπληρώσουν μία φόρμα αναφοράς του συμβάντος στην υπηρεσία ηλεκτρονικού εγκλήματος (στην Αγγλία) και να προσλάβουν γραφείο ώστε να τρέξει την υπόθεση με την τράπεζα για να επιστραφεί το χρηματικό ποσό. Άλλες κινήσεις ήταν να απευθυνθούν στην Ένωση Εργαζομένων Καταναλωτών της Ελλάδας ή να επικοινωνήσουν άμεσα με την πλατφόρμα στην οποία έγινε η υποκλοπή των στοιχείων σύνδεσης. Μπορούμε να αντιληφθούμε ότι οι επιθέσεις ηλεκτρονικού ψαρέματος στο ερωτηματολόγιο αφορούσαν κυρίως τραπεζικές συναλλαγές, αλλά υπήρχαν και περιπτώσεις που τους έκλεψαν τα στοιχεία σύνδεσης ενός λογαριασμού. Αξίζει να σημειωθεί πως δεν ήταν λίγες οι περιπτώσεις των θυμάτων που αντιλήφθηκαν εγκαίρως την απάτη και προέβησαν σε ενέργειες αποτροπής της ζημιάς. Για αυτό και στην ερώτηση, ποιο ήταν το χρηματικό ποσό που χάσατε, η πλειοψηφία (75%) απάντησε πως δεν ζημιώθηκε οικονομικά. Στην ίδια ερώτηση το 12,5% απάντησε ότι έχασε λιγότερο από 100€ ενώ το υπόλοιπο 12,5% δήλωσε πως τα χρήματα που έχασε ήταν περισσότερα από 1000€. Παρατηρήθηκε πως τα θύματα που αντιλήφθηκαν άμεσα την παγίδα που έπεσαν ήταν μόλις το

68,8% (επί των θυμάτων), το 12,5% το αντιλήφθηκε εντός της ίδιας ημέρας, ενώ υπήρχαν άτομα που αντιλήφθηκαν μετά από 3 μήνες ή κάποιους τους ενημέρωσε η τράπεζα για την ύποπτη ενέργεια.

Χρήση Διαδικτύου και Ηλεκτρονικών Αγορών από τους Ανήλικους

Όπως αναφέρθηκε και νωρίτερα, στο ερωτηματολόγιο δεν υπήρχε κανένα θύμα που να είναι κάτω των 18 ετών. Ας δούμε όμως την χρήση του διαδικτύου από τους ανήλικους συμμετέχοντες. Αρχικά από τους ανήλικους, το 78,6% είναι απόφοιτοι γυμνασίου, το 14,3% απόφοιτοι λυκείου και το 7,1% απόφοιτοι δημοτικού. Με αυτά τα στοιχεία, αντιλαμβανόμαστε ότι υπάρχει μία σύγχυση των παιδιών για τον όρο απόφοιτος,

εφόσον στην Ελλάδα, η αποφοίτηση του λυκείου γίνεται συνήθως κατά την ολοκλήρωση του 18ου έτους ηλικίας. Οι ερωτήσεις που απευθύνονταν αποκλειστικά τους ανήλικους συμμετέχοντες, αφορούσαν τις αγορές παιχνιδιών στο διαδίκτυο, αγορές μέσα στα παιχνίδια αλλά και γενικότερες ηλεκτρονικές αγορές. Ο παράγοντας που συνδυάστηκε στις παραπάνω ερωτήσεις ήταν, εάν ζητάνε την άδεια ή ενημερώνουν τον κάτοχο της τραπεζικής κάρτας πριν πραγματοποιήσουν οποιαδήποτε ηλεκτρονική αγορά. Η εκπληκτική πλειοψηφία 88,9%, δήλωσε πως ενημερώνει κάθε φορά κάποιον ενήλικα για να ολοκληρώσει μια αγορά. Σε συνάρτηση με τις προηγούμενες απαντήσεις, μόνο ένα παιδί δήλωσε πως δεν ζητάει την άδεια για την πραγματοποίηση ηλεκτρονικής αγοράς, ο οποίος όμως δηλώνει επίσης ότι δεν έχει αγοράσει παιχνίδια στο διαδίκτυο, δεν έχει πληρώσει μέσα σε παιχνίδια αλλά και δεν έχει αγοράσει κάτι μέσω διαδικτύου μόνος του.



Συμπεράσματα

Με όσα έχουν προαναφερθεί στην παρούσα πτυχιακή εργασία, μπορούμε να καταλήξουμε στο συμπέρασμα ότι γίνονται βήματα από τις κυβερνήσεις για την νομοθετική κάλυψη του ηλεκτρονικού εγκλήματος. Το ηλεκτρονικό έγκλημα όμως παραμένει αδιάστακτο απέναντι στους χρήστες. Ως αποτέλεσμα, η λύση των επιθέσεων δεν βρίσκεται αποκλειστικά στην νομοθεσία και στα χέρια των κυβερνήσεων, αλλά στον κάθε έναν χρήστη ξεχωριστά. Το ηλεκτρονικό έγκλημα απαρτίζεται από τρεις παράγοντες, το κίνητρο του θύτη (αυτόν που πραγματοποιεί την δόλια πράξη), την ευαισθησία ή την ευκαιρία (που θα εκμεταλλευτεί ο θύτης ώστε να πραγματοποιηθεί η επίθεση) και το θύμα (που δέχεται την επίθεση και εν αγνοία του πολλές φορές συναινεί στην πράξη). Ως εκ τούτου, ο χρήστης πρέπει να προφυλαχτεί είτε αποφεύγοντας κινήσεις/ενέργειες που μπορεί να προβούν σε ζημία, είτε να μένει ενημερωμένος σχετικά με τις εξελίξεις του ηλεκτρονικού εγκλήματος. Όπως παρατηρήθηκε και από την ανάλυση των δεδομένων της έρευνάς μας, ο μέσος άνθρωπος περνάει αρκετό χρόνο καθημερινά στις ηλεκτρονικές συσκευές, πλοηγούμενος στο διαδίκτυο. Αυτό καθιστά την ενημέρωσή του ακόμη πιο απαραίτητη, εφόσον πολλές καθημερινές ενέργειες τις περατώνει μέσω του διαδικτύου.

Επίσης, διαπιστώθηκε πως οι επιθέσεις ηλεκτρονικού εγκλήματος από την εμφάνισή τους μέχρι σήμερα έχουν εξελιχθεί δραματικά και συνεχίζουν να εξελίσσονται καθημερινά, καθιστώντας δυσκολότερη την αντιμετώπισή τους. Αυτό συμβαίνει διότι έχουν αντιληφθεί οι επιτιθέμενοι πως η ευπάθεια του χρήστη είναι η μεγαλύτερη ευαισθησία που μπορούν να εκμεταλλευτούν. Για αυτόν τον λόγο, πρέπει να πραγματοποιούνται καμπάνιες ευαισθητοποίησης των χρηστών με email, φυλλάδια αλλά ακόμη καλύτερα με σεμινάρια. Έχει αποδειχθεί πως ένας άνθρωπος αντιλαμβάνεται τις επιθέσεις ηλεκτρονικού ψαρέματος, μόνο όταν έχει πέσει σε μία ιστοσελίδα phishing ή λάβει ένα παραπλανητικό email, τα οποία είναι δημιουργήματα του εκπαιδευτικού προγράμματος, και ύστερα προχωρήσουν στην εκπαίδευσή του για να κατανοήσει τα σημάδια που καθιστούν ένα μήνυμα ή μια ιστοσελίδα ύποπτα για απάτη.

Εν κατακλείδι, το διαδίκτυο δε γνωρίζει γεωγραφικά σύνορα, με αποτέλεσμα να δίνει την ευχέρεια στους χρήστες να το εκμεταλλεύονται όχι μόνο θετικά αλλά και αρνητικά. Έτσι, με τα χρόνια εισχώρησε στα θεμέλιά του και το ηλεκτρονικό έγκλημα και ως παράρτημα του και το ηλεκτρονικό ψάρεμα (phishing). Ενώ οι επιθέσεις phishing είχαν ξεκινήσει ως ένδειξη ικανοτήτων από κάποιους έφηβους, δεν άργησε να γίνει η χρήση του με οικονομικό κίνητρο. Πλέον, ο χρήστης αντί να πλοηγείται ελεύθερα και χωρίς φόβο στο διαδίκτυο, κινείται δειλά και καχύποπτα, έχοντας υπόψιν του όλες τις δόλιες ενέργειες που τον παραμονεύουν.

Παράρτημα

Ερωτηματολόγιο

Ενότητα 1 από 5

Ηλεκτρονικό Ψάρεμα "Phishing"

Το αντικείμενο της έρευνάς είναι το Ηλεκτρονικό Ψάρεμα ("Phishing")
Το συγκεκριμένο ερωτηματολόγιο συντάχθηκε από προπτυχιακή φοιτήτρια του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου στο πλαίσιο της εκπόνησης της πτυχιακής εργασίας της.
Για τη συμπλήρωση του ερωτηματολογίου απαιτείται, κατά μέσο όρο, χρόνος 5 λεπτών.
Σας ευχαριστούμε για τη συμμετοχή σας.

Φύλο

Πολλαπλές επιλογές

☐ Άρρεν

☐ Θήλυ

☐ Προσθήκη επιλογής ή προσθήκη "Άλλο"

Υποχρεωτική

Ηλικία *

☐ κάτω των 18

☐ 18 - 25

☐ 26 - 40

☐ 41 - 60

☐ άνω των 60

Μορφωτικό Επίπεδο *

☐ Απόφοιτος Δημοτικού

☐ Απόφοιτος Γυμνασίου

☐ Απόφοιτος Λυκείου (ΓΕΛ/ΕΠΑΛ)

☐ Απόφοιτος ΑΕΙ/ΤΕΙ/ΙΕΚ

☐ Κάτοχος Μεταπτυχιακού/Διδακτορικού

Χρήση Διαδικτύου Ανηλίκων



Σε αυτήν την ενότητα θα σας ζητηθούν πληροφορίες σχετικά με την επαφή σας με το διαδίκτυο και την επίβλεψη των κηδεμόνων σας.

Χρησιμοποιείτε το διαδίκτυο (σε οποιαδήποτε συσκευή) υπό την επίβλεψη κάποιου ενήλικου; *

- ☐ Ναι, πάντα
- ☐ Όχι, ποτέ
- ☐ Μερικές φορές

Παίζετε παιχνίδια με διαδικτυακή σύνδεση; *

- ☐ Ναι
- ☐ Όχι

Έχετε αγοράσει διαδικτυακά την άδεια χρήσης κάποιου παιχνιδιού; *

- ☐ Ναι
- ☐ Όχι

Έχετε κάνει κάποια αγορά μέσα στο παιχνίδι; *

- ☐ Ναι
- ☐ Όχι

Έχετε πραγματοποιήσει κάποια ηλεκτρονική αγορά χρησιμοποιώντας πιστωτική κάρτα; *

- ☐ Ναι
- ☐ Όχι

Εάν έχετε πραγματοποιήσει κάποια από τις παραπάνω αγορές, ρωτήσατε/ενημερώσατε κάποιον ενήλικα (τον κάτοχο της πιστωτικής κάρτας) για την ολοκλήρωση της αγοράς;

- ☐ Ναι, κάθε φορά
- ☐ Μερικές φορές
- ☐ Όχι, ποτέ

Χρήση Διαδικτύου



Σε αυτήν την ενότητα θα σας ζητηθούν πληροφορίες σχετικά με την επαφή σας με το διαδίκτυο.

Ποιές από τις παρακάτω ηλεκτρονικές συσκευές έχετε στην κατοχή σας ; *

- ☐ Smartphone
- ☐ Σταθερό Η/Υ
- ☐ Laptop
- ☐ Tablet
- ☐ Κανένα

Πόσο χρόνο καταναλώνετε καθημερινά στο διαδίκτυο(internet) ; *

- ☐ Λιγότερο από μία ώρα
- ☐ Μία με δύο ώρες
- ☐ Δύο με τέσσερις ώρες
- ☐ Παραπάνω από τέσσερις ώρες

Ποια υπηρεσία/ιστοσελίδα χρησιμοποιείτε περισσότερο στο διαδίκτυο; *

- ☐ Youtube
- ☐ Facebook
- ☐ Instagram
- ☐ TikTok
- ☐ Pinterest
- ☐ Google News
- ☐ Email
- ☐ Viber/Messenger/WhatsApp
- ☐ Άλλο...

Πως θα χαρακτηρίζατε τις γνώσεις σας σχετικά με την χρήση του διαδικτύου; *

- ☐ Καθόλου
- ☐ Λίγο
- ☐ Μέτρια
- ☐ Καλή
- ☐ Πολύ καλή

Η χρήση του διαδικτύου είναι κάτι που αποκτήσατε : *

- ☐ Από την εκπαίδευση
- ☐ Από την οικογένεια
- ☐ Από φίλους
- ☐ Εμπειρικά
- ☐ Άλλο...

Για ποιο λόγο χρησιμοποιείτε το Διαδίκτυο; *

	0 (Καθόλου)	1	2	3	4	5 (Πάρα πολ...
Εκπαίδευση ...	☐	☐	☐	☐	☐	☐
Ψυχαγωγία	☐	☐	☐	☐	☐	☐

Ενότητα 4 από 5

Ασφάλεια στο Διαδίκτυο



Σε αυτήν την ενότητα θα σας ζητηθούν πληροφορίες σχετικά με τις γνώσεις σας πάνω στην ασφαλή πλοήγηση στο διαδίκτυο.

Έχετε εγκαταστημένο Antivirus στις ηλεκτρονικές συσκευές σας; *

- ☐ Ναι, σε όλες (κινητά και υπολογιστές)
- ☐ Όχι, σε καμία
- ☐ Σε κάποιες
- ☐ Δεν έχω ηλεκτρονικές συσκευές
- ☐ Δεν γνωρίζω

Γνωρίζετε τις ενδείξεις μίας ύποπτης ιστοσελίδας; (Ποια χαρακτηριστικά της ιστοσελίδας την κάνουν επικίνδυνη για απάτη) *

- ☐ Ναι
- ☐ Όχι

Γνωρίζετε τι δεν πρόκειται ποτέ να σας ζητήσει με μήνυμα η τράπεζα; *

- ☐ Ναι
- ☐ Όχι

Μπορείτε να αναγνωρίσετε πριν ολοκληρώσετε μια ηλεκτρονική αγορά (δίνοντας τα στοιχεία της κάρτας σας) εάν η ιστοσελίδα είναι αξιόπιστη; *

- ☐ Ναι
- ☐ Όχι
- ☐ Δεν πραγματοποιώ ηλεκτρονικές αγορές

Γνωρίζετε τι είναι το Phishing - Ηλεκτρονικό Ψάρεμα; *

- ☐ Ναι
- ☐ Όχι

Phishing - Ηλεκτρονικό ψάρεμα

Το Phishing είναι μία απόπειρα εξαπάτησης κάποιου, ώστε να δώσει πληροφορίες μέσω διαδικτύου ή ηλεκτρονικού ταχυδρομείου που θα επιτρέψουν σε κάποιον άλλον να πάρει χρήματα από αυτόν, για παράδειγμα αφαιρώντας χρήματα από τον τραπεζικό του λογαριασμό. - Cambridge Dictionary

Έχετε λάβει email το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχεία σύνδεσης; *

- ☐ Ναι
- ☐ Όχι

Εάν απαντήσατε θετικά στην παραπάνω ερώτηση, πως χειριστήκατε την κατάσταση; *

- ☐ Δεν έχω λάβει τέτοιο email
- ☐ Αγνόησα το email
- ☐ Διέγραψα το email
- ☐ Επικοινωνώ με την υπηρεσία/ιστοσελίδα
- ☐ Επιβεβαίωσα τα στοιχεία σύνδεσης και μετά αντιλήφθηκα ότι είναι απάτη
- ☐ Άλλο...

Έχετε λάβει SMS το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχεία σύνδεσης; *

- ☐ Ναι
- ☐ Όχι

Εάν απαντήσατε θετικά στην παραπάνω ερώτηση, πως χειριστήκατε την κατάσταση; *

- ☐ Δεν έχω λάβει τέτοιο SMS
- ☐ Αγνόησα το SMS
- ☐ Διέγραψα το SMS
- ☐ Επικοινωνώ με την υπηρεσία/ιστοσελίδα
- ☐ Επιβεβαίωσα τα στοιχεία σύνδεσης και μετά αντιλήφθηκα ότι είναι απάτη
- ☐ Άλλο...

Έχετε πατήσει πάνω σε διαφήμιση και σταματήσατε την πλοήγησή σας γιατί αντιληφθήκατε ότι είναι απάτη; *

- ☐ Ναι
- ☐ Όχι

Έχετε πέσει θύμα Phishing-Ηλεκτρονικού Ψαρέματος; *

- ☐ Ναι
- ☐ Όχι
- ☐ Δεν γνωρίζω

Θύμα Phishing



Σε αυτήν την ενότητα θα σας ζητηθούν πληροφορίες σχετικά με την επίθεση ηλεκτρονικού ψαρέματος που δεχτήκατε, τον τρόπο που την διαχειριστήκατε και τις επιπτώσεις που είχατε.

Πότε πέσατε θύμα Phishing; *

- ☐ Αυτήν την χρονιά (2023)
- ☐ Την περίοδο του Covid-19 (2020-2022)
- ☐ Παλιότερα (πριν το 2020)

Πόσο γρήγορα αντιληφθήκατε ότι πέσατε θύμα; *

- ☐ Την ίδια στιγμή
- ☐ Την ίδια μέρα
- ☐ Την επόμενη μέρα
- ☐ Δεν θα το καταλάβαινα αν δεν με ενημέρωνε η υπηρεσία/ιστοσελίδα
- ☐ Άλλο...

Με ποιά μέθοδο πέσατε θύμα; *

- ☐ Με SMS
- ☐ Με email
- ☐ Με μήνυμα σε Instagram/Viber και παρόμοιων εφαρμογών
- ☐ Άλλο...

Επιλέξτε σε ποια κλίμακα ήταν το χρηματικό ποσό που χάσατε. *

- ☐ έως 100€
- ☐ 100 - 500€
- ☐ 500 - 1.000€
- ☐ περισσότερα από 1.000€
- ☐ Δεν έχασα κάποιο χρηματικό ποσό

Εάν η περιπέτειά σας δεν κατέληξε σε εξαπάτηση, πως καταφέρατε να το αποτρέψετε;

Κείμενο σύντομης απάντησης

Ποιές ήταν οι ενέργειες που ακολουθήσατε αφότου αντιληφθήκατε ότι εξαπατηθήκατε; *

Κείμενο σύντομης απάντησης

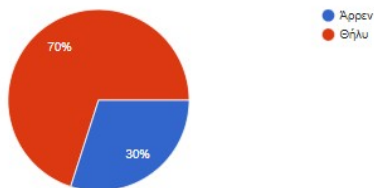
Μετά την εμπειρία σας με το phishing, είχατε την ίδια αντιμετώπιση στα μηνύματα που λαμβάνετε και στα ηλεκτρονικά καταστήματα που πραγματοποιείτε τις αγορές σας; *

- ☐ Ήμουν προσεκτικός/η για το πρώτο διάστημα (1 μήνα)
- ☐ Είμαι πιο προσεκτικός/η με τις κινήσεις μου στο διαδίκτυο από τότε
- ☐ Δεν άλλαξε κάτι στις διαδικτυακές μου συνήθειες

Γραφήματα Ερωτηματολογίου

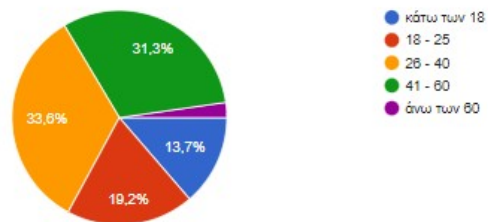
Φύλο

307 απαντήσεις



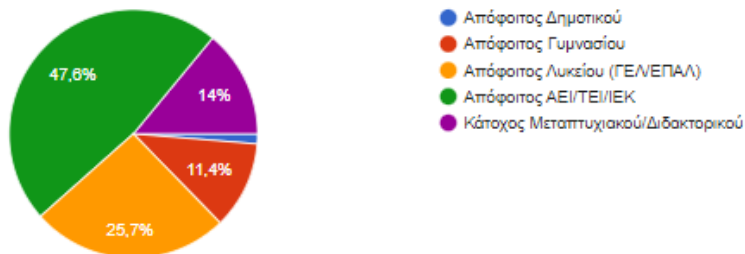
Ηλικία

307 απαντήσεις



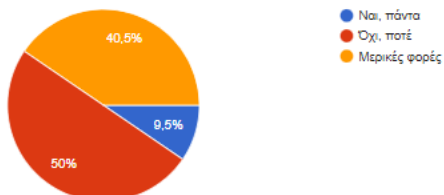
Μορφωτικό Επίπεδο

307 απαντήσεις



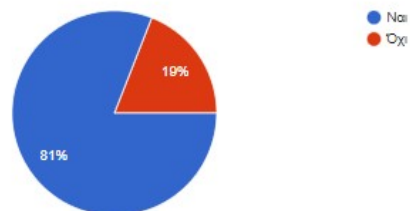
Χρησιμοποιείτε το διαδίκτυο (σε οποιαδήποτε συσκευή) υπό την επίβλεψη κάποιου ενήλικου;

42 απαντήσεις



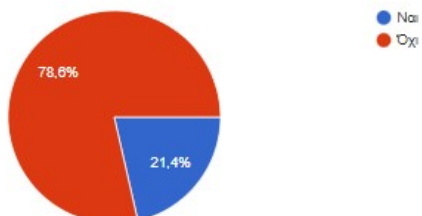
Παίζετε παιχνίδια με διαδικτυακή σύνδεση;

42 απαντήσεις



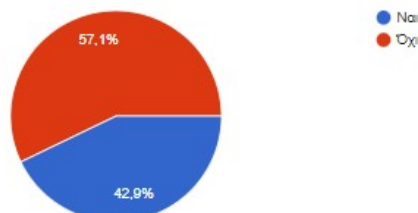
Έχετε αγοράσει διαδικτυακά την άδεια χρήσης κάποιου παιχνιδιού;

42 απαντήσεις

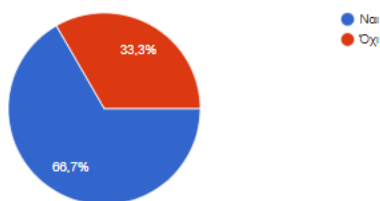


Έχετε κάνει κάποια αγορά μέσα στο παιχνίδι;

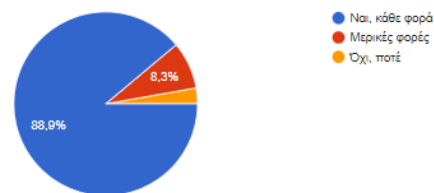
42 απαντήσεις



Έχετε πραγματοποιήσει κάποια ηλεκτρονική αγορά χρησιμοποιώντας πιστωτική κάρτα;
42 απαντήσεις

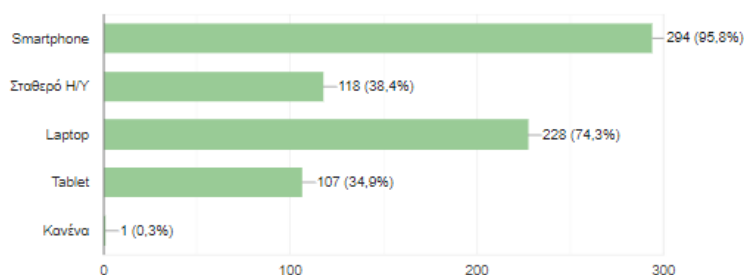


Εάν έχετε πραγματοποιήσει κάποια από τις παραπάνω αγορές, ρωτήσατε/ ενημερώσατε κάποιον ενήλικα (τον κάτοχο της πιστωτικής κάρτας) για την ολοκλήρωση της αγοράς;
36 απαντήσεις



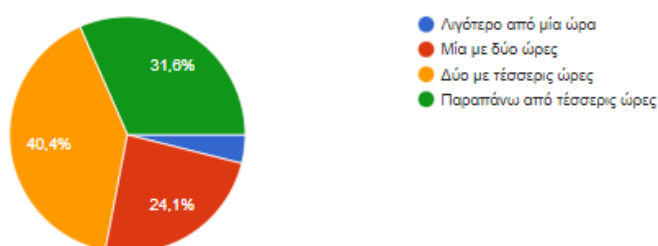
Ποιές από τις παρακάτω ηλεκτρονικές συσκευές έχετε στην κατοχή σας ;

307 απαντήσεις



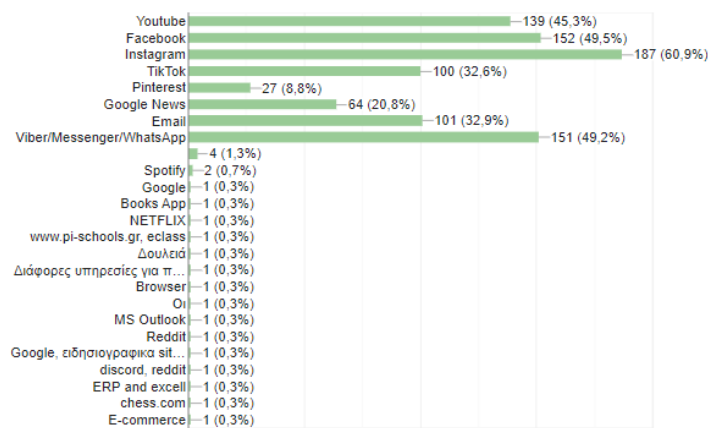
Πόσο χρόνο καταναλώνετε καθημερινά στο διαδίκτυο(internet) ;

307 απαντήσεις

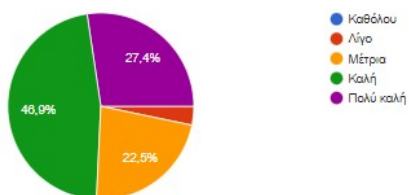


Ποια υπηρεσία/ιστοσελίδα χρησιμοποιείτε περισσότερο στο διαδίκτυο;

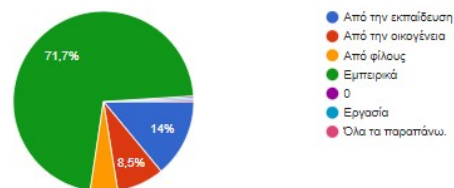
307 απαντήσεις



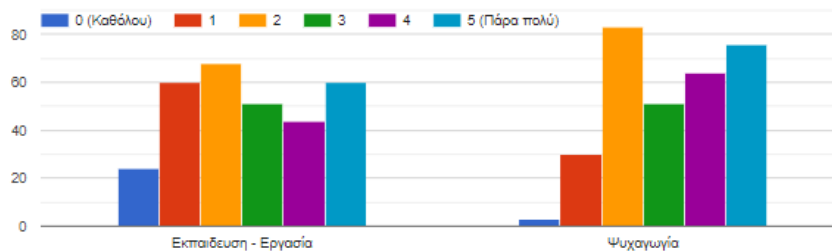
Πως θα χαρακτηρίζατε τις γνώσεις σας σχετικά με την χρήση του διαδικτύου;
307 απαντήσεις



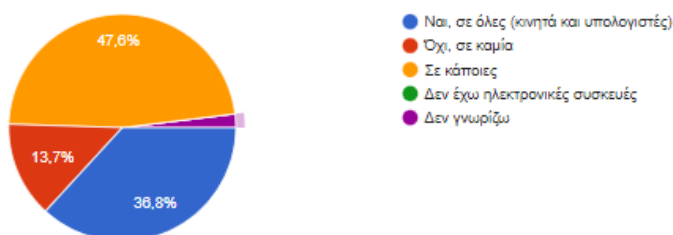
Η χρήση του διαδικτύου είναι κάτι που αποκτήσατε :
307 απαντήσεις



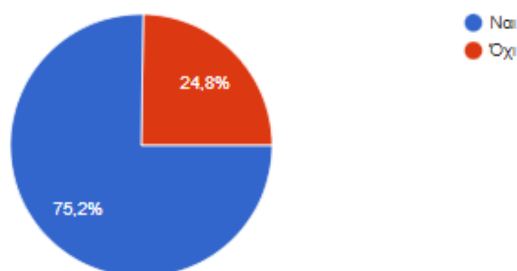
Για ποιο λόγο χρησιμοποιείτε το Διαδίκτυο;



Έχετε εγκαταστήσει Antivirus στις ηλεκτρονικές συσκευές σας;
307 απαντήσεις

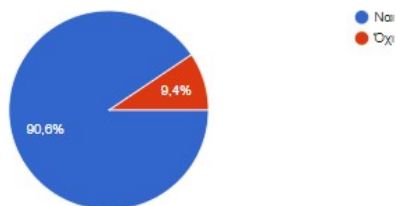


Γνωρίζετε τις ενδείξεις μίας ύποπτης ιστοσελίδας; (Ποια χαρακτηριστικά της ιστοσελίδας την κάνουν επικίνδυνη για απάτη)
307 απαντήσεις



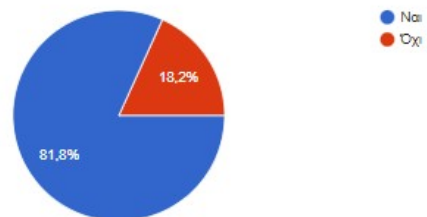
Γνωρίζετε τι δεν πρόκειται ποτέ να σας ζητήσει με μήνυμα η τράπεζα;

307 απαντήσεις



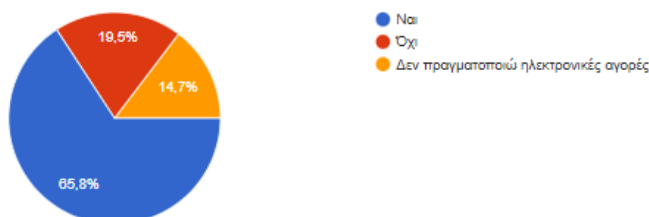
Γνωρίζετε τι είναι το Phishing - Ηλεκτρονικό Ψάρεμα;

307 απαντήσεις



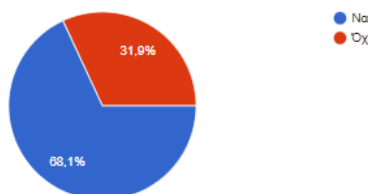
Μπορείτε να αναγνωρίσετε πριν ολοκληρώσετε μια ηλεκτρονική αγορά (δίνοντας τα στοιχεία της κάρτας σας) εάν η ιστοσελίδα είναι αξιόπιστη;

307 απαντήσεις



Έχετε λάβει email το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχείων σύνδεσης;

307 απαντήσεις



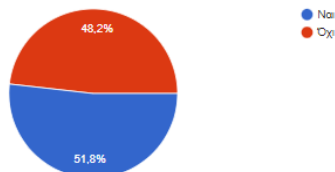
Εάν απαντήσατε θετικά στην παραπάνω ερώτηση, πως χειριστήκατε την κατάσταση;

307 απαντήσεις



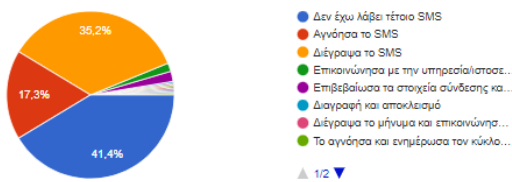
Έχετε λάβει SMS το οποίο αντιληφθήκατε ότι είναι παραπλανητικό, ζητώντας επιβεβαίωση στοιχείων σύνδεσης;

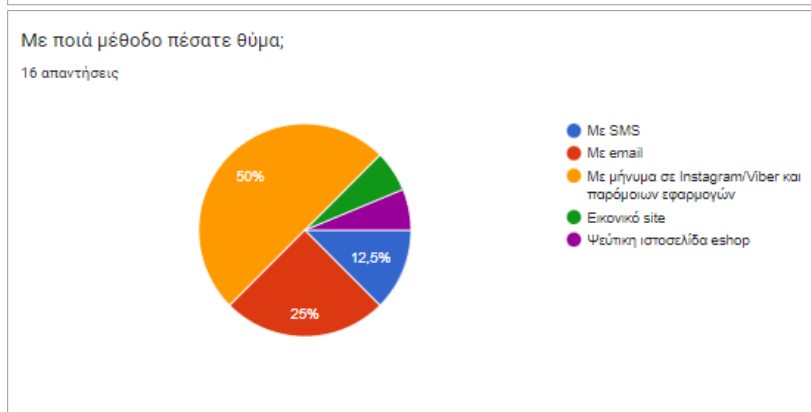
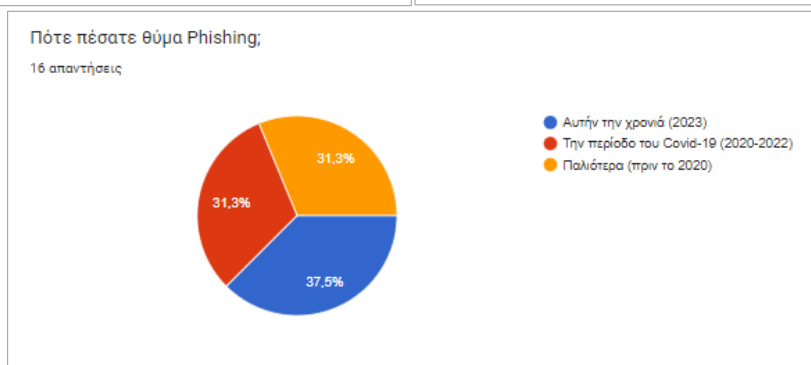
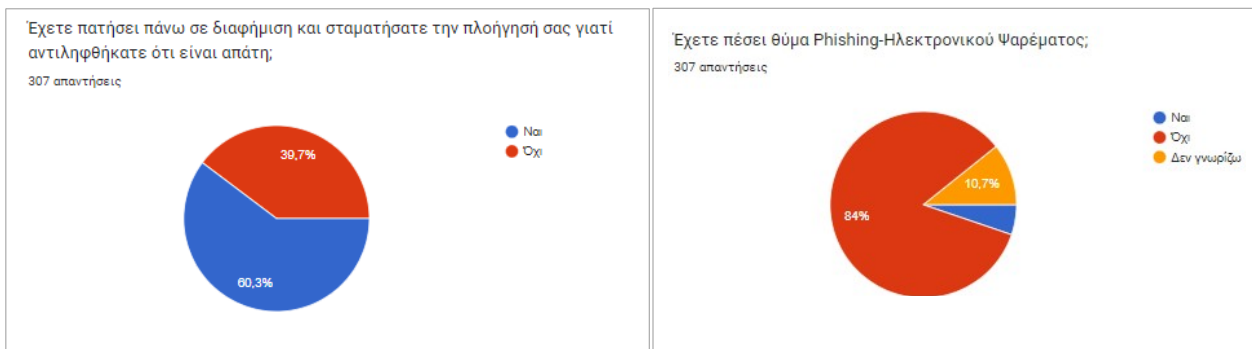
307 απαντήσεις



Εάν απαντήσατε θετικά στην παραπάνω ερώτηση, πως χειριστήκατε την κατάσταση;

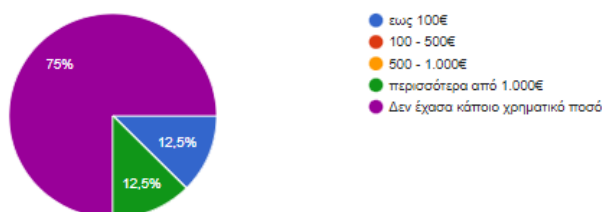
307 απαντήσεις





Επιλέξτε σε ποια κλίμακα ήταν το χρηματικό ποσό που χάσατε.

16 απαντήσεις



Εάν η περιπέτειά σας δεν κατέληξε σε εξαπάτηση, πως καταφέρατε να το αποτρέψετε;

8 απαντήσεις

Δεν ανταποκρίθηκα.

Πήρα τηλέφωνο στην τράπεζα και αμέσως μου έκλεισαν την κάρτα.

Ήμουν υποψιασμένη και έτσι διέγραψα και αγνόησα την απάτη.

Απλά δεν ασχολήθηκα

Επικοινωνία με τράπεζα

Δεν εξαπατήθηκα

Μπλοκάρισμα

Άμεση επικοινωνία με την πλατφόρμα στην οποία έγινε χακάρισμα κωδικών

Ποιές ήταν οι ενέργειες που ακολουθήσατε αφότου αντιληφθήκατε ότι εξαπατηθήκατε;

16 απαντήσεις

Πήρα τηλέφωνο στην τράπεζα και αμέσως μου έκλεισαν την κάρτα

Διέγραψα την συνομιλία και μπλόκαρι τον λογαριασμό

Συμπλήρωσα μια φόρμα με το τι συνέβη στην υπηρεσία ηλεκτρονικού εγκλήματος στην Αγγλία και προσέλαβα ένα γραφείο να τρεξει την υποθεση μου με την τραπεζα ετσι ωστε να παρω τα χρηματα μου πισω.

Διέγραψα το μήνυμα και έκανα αναφορά.

Καμια. Προσπαθησα να επικοινωνησω με την τραπεζα αλλα η συναλλαγη ειχε ήδη γινει

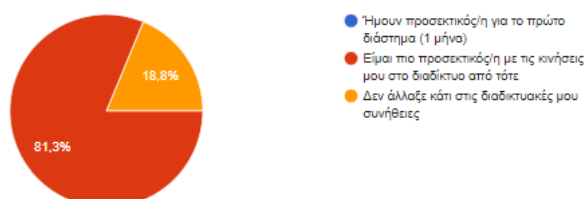
Απλά απέφυγα το ιστότοπο

Δεν εξαπατήθηκα το αντιλήφθηκα εγκαίρως

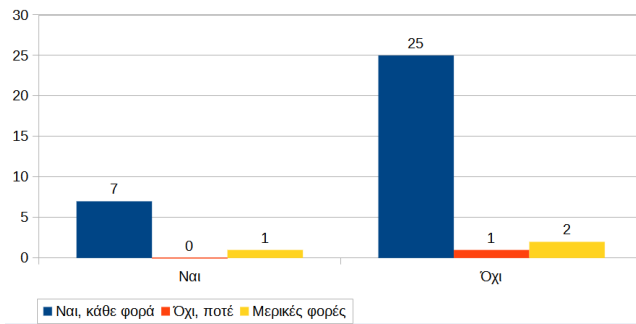
Αμφισβήτηση τραπεζικής συναλλαγής

Μετά την εμπειρία σας με το phishing, είχατε την ίδια αντιμετώπιση στα μηνύματα που λαμβάνετε και στα ηλεκτρονικά καταστήματα που πραγματοποιείτε τις αγορές σας;

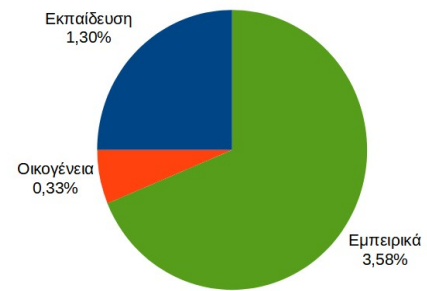
16 απαντήσεις



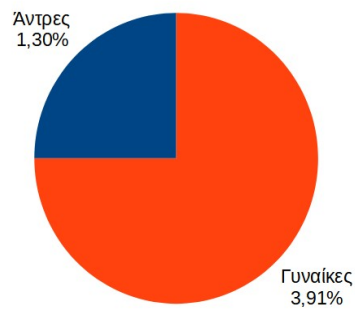
Αγορά παιχνιδιού και Κάτοχος Κάρτας



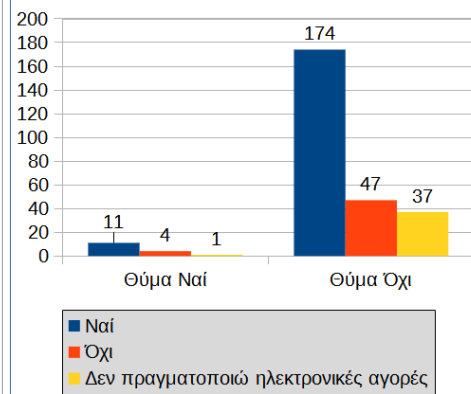
Απόκτηση γνώσης χρήσης Διαδικτύου



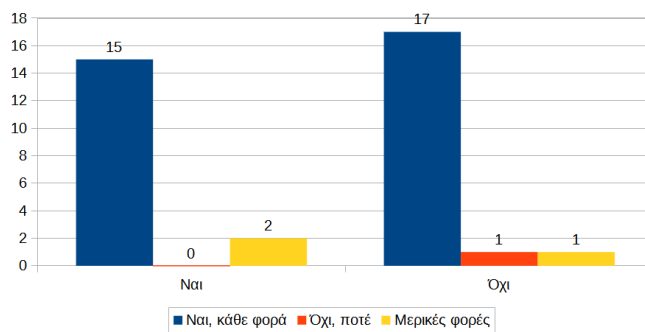
Θύματα



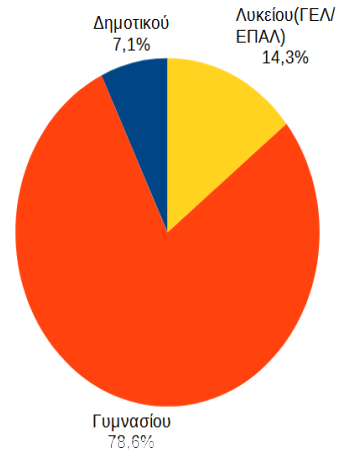
Θύμα + Αξιοπίστη Ιστοσελίδα (Πραγματοποίηση Ηλ. Αγορών)

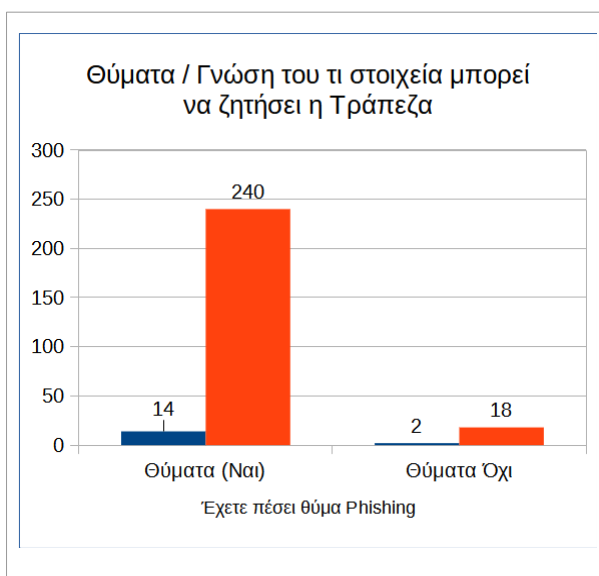
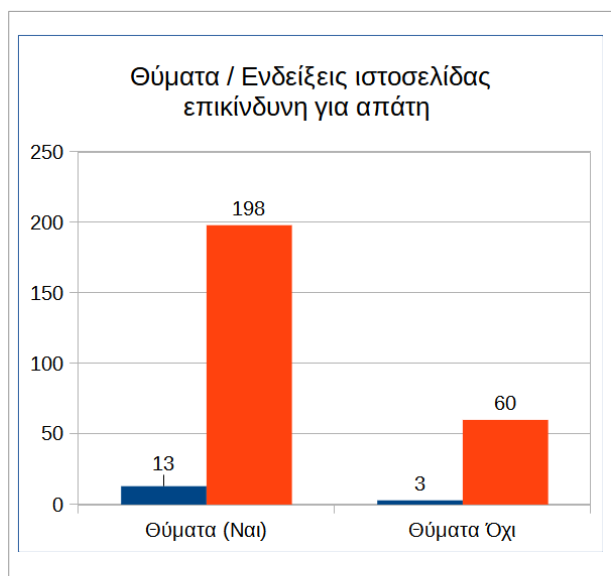
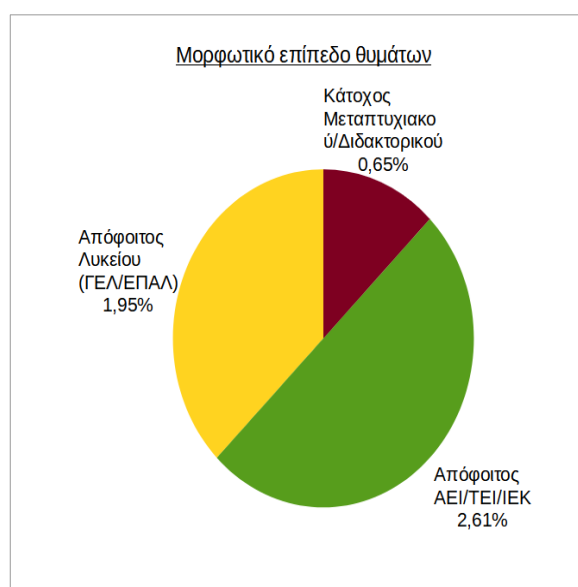
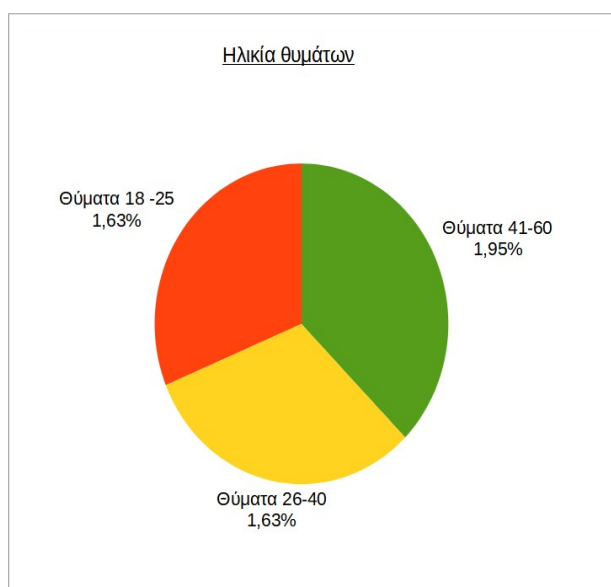
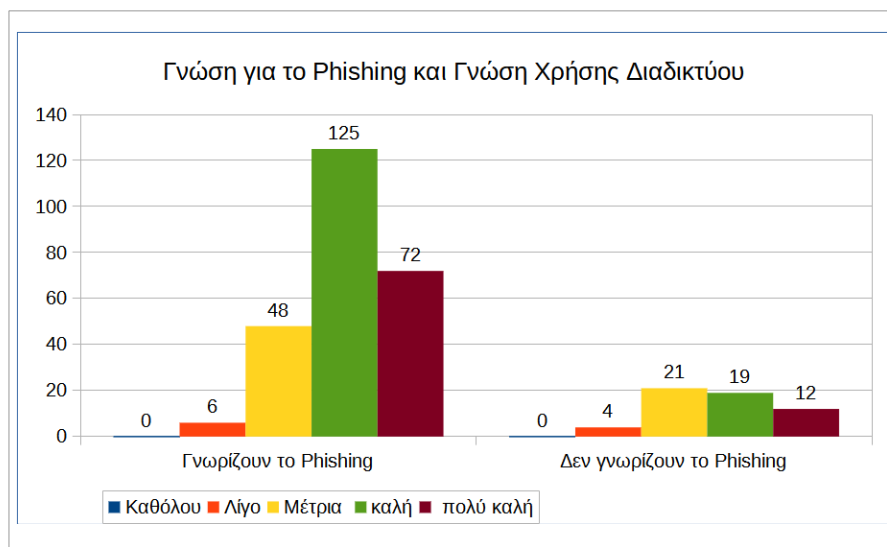


Αγορά Μέσα στο Παιχνίδι + Κάτοχος Κάρτας



Κάτω των 18





Βιβλιογραφία

1. Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts during the Pandemic. *IEEE Access*, 9, 121916–121929. <https://doi.org/10.1109/ACCESS.2021.3109091>
2. Akdemir, N., & Yenil, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, 11(3). <https://doi.org/10.1177/21582440211031879>
3. Al-Qahtani, A. F., & Cresci, S. (2022). *The COVID-19 scamdemic A survey of phishing attacks and theirXX.pdf*.
4. Bampiniotis, G. (2002). *Αεζικό Της Νέας Ελληνικής Γλώσσας*.
5. Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020, November*. <https://doi.org/10.1109/INMIC50486.2020.9318210>
6. Bitaab, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., Kim, D., Bao, T., Wang, R., Shoshitaishvili, Y., Doupe, A., & Ahn, G. J. (2020). Scam Pandemic: How Attackers Exploit Public Fear through Phishing. *ECrime Researchers Summit, ECrime, 2021-Novem*(January 2022). <https://doi.org/10.1109/eCrime51433.2020.9493260>
7. Darwish, A., Zarka, A. El, & Aloul, F. (2012). *Towards understanding phishing victims' profile _ Enhanced Reader.pdf*. 13–17.
8. Finklea, K. M., & Theohary, C. A. (2013). Cybercrime: Conceptual issues for congress and U.S. law enforcement. *Cybercrime: Conceptualized and Codified*, 1–27.
9. Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers and Security*, 18(1), 28–34. [https://doi.org/10.1016/S0167-4048\(99\)80006-6](https://doi.org/10.1016/S0167-4048(99)80006-6)
10. Hota, H. S., Shrivastava, A. K., & Hota, R. (2018). An Ensemble Model for Detecting Phishing Attack with Proposed Remove-Replace Feature Selection Technique. *Procedia Computer Science*, 132, 900–907. <https://doi.org/10.1016/j.procs.2018.05.103>
11. Jones, A. (2005). Cyber terrorism: Fact or fiction. *Computer Fraud and Security*, 2005(6), 4–7. [https://doi.org/10.1016/S1361-3723\(05\)70220-7](https://doi.org/10.1016/S1361-3723(05)70220-7)
12. Lain, D., Kostianen, K., & Capkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. *Proceedings - IEEE Symposium on Security and Privacy, 2022-May*, 842–859. <https://doi.org/10.1109/SP46214.2022.9833766>
13. Lawrence, A. (2023). *Microsoft confirms Azure, Outlook outages caused by DDoS attacks. BleepingComputer*. <https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-azure-outlook-outages-caused-by-ddos-attacks/>
14. Mao, J., Tian, W., Li, P., Wei, T., & Liang, Z. (2017). Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity. *IEEE Access*, 5, 17020–17030. <https://doi.org/10.1109/ACCESS.2017.2743528>
15. Mayuri, A. V. R., Tech, M., & Ph, D. (2012). *Phishing Detection based on Visual-Similarity*. 3(3), 1–5.
16. Popoola, S. I., Sweetwilliams, F., John, S. N., Academy, N. D., & Atayero, A. A. (2017). *Ransomware: Current Trend, Challenges, and Research Directions*. October.

17. Pranggono, B., & Arabo, A. (2020). *COVID-19 pandemic cybersecurity issues* (pp. 1–6).
18. Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, 23(2), 197–214. <https://doi.org/10.1016/j.eij.2021.12.003>
19. Rekouche, K. (2011). *Early Phishing*. 1–9. <http://arxiv.org/abs/1106.4692>
20. Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. *Police Practice and Research*, 19(6), 515–518. <https://doi.org/10.1080/15614263.2018.1507888>
21. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings*, 1(April), 373–382. <https://doi.org/10.1145/1753326.1753383>
22. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *ACM International Conference Proceeding Series*, 229(July), 88–99. <https://doi.org/10.1145/1280680.1280692>
23. Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity theft - Empirical evidence from a phishing exercise. *IFIP International Federation for Information Processing*, 232, 193–203. https://doi.org/10.1007/978-0-387-72367-9_17
24. Tajpour, A., Ibrahim, S., & Zamani, M. (2010). Identity Theft Methods and Fraud Types. *Handbook on Crime*, April, 172–190. <https://doi.org/10.1017/cbo9780511843846.006>
25. Weber, B. A. M. (2003). *THE COUNCIL OF EUROPE 'S CONVENTION ON Cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries . ' As Professor James Boyle noted , " If the king ' s writ reaches only as far as the king ' s sword , then much of the*. 446(1996).
26. Αγγελάκης, Χ., & Ιωσηφέλλη, Α. (2018). *Ηλεκτρονικό Εγκλημα : Μορφές Και Αντιμετώπιση*.
27. Γιαμπουλάκης, Χ. (2017). *Τεχνικές επιθέσεων τελικού χρήστη Client Side Attacks*. Πανεπιστήμιο Πειραιώς - Τμήμα Πληροφορικής.
28. Λιοντήρης, Α. (Τεχνολογικό Ε. Ί. Δ. Ε., & Μπάκας, Α. (Τεχνολογικό Ε. Ί. Δ. Ε. (2016). *Ζητήματα κλοπής και διαφύλαξης ταυτότητας στο διαδίκτυο*. ΤΕΙ Δυτικής Ελλάδας.
29. Λυκούρεσης, Ι., & Φραντζέσκου, Π. (n.d.). *Πτυχιακή εργασία Ηλεκτρονικό έγκλημα*.
30. Μαυρομάτη, Χ., & Γατσούλα, Θ. (2013). *Η ΔΙΕΥΘΥΝΣΗ ΔΙΩΣΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ*.
31. Μπενέτου, Α. (2021). *Το ηλεκτρονικό εγκλημα*.
32. Μυλωνάς, Π. (2009). *Διαδίκτυο Και Εξάρτηση*. 102.