ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΣΥΜΠΕΡΙΦΟΡΑ ΤΩΝ ΧΡΗΣΤΩΝ ΤΟΥ «ΙΝΤΕΡΝΕΤ» ΣΕ ΑΠΟΠΕΙΡΕΣ PHISHING

Σμέου Μαρία/ Α.Μ: eco21390

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων Καθηγητής: Οικονομίδης Αναστάσιος, Καθηγητής Τμήματος Οικονομικών Επιστημών

Αναπληρωματικός Επιβλέπων Καθηγητής: Παναγιωτίδης Θεόδωρος, Καθηγητής Τμήματος Οικονομικών Επιστημών

ΘΕΣΣΑΛΟΝΙΚΗ, ΣΕΠΤΕΜΒΡΙΟΣ 2023

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση αυτής της διπλωματικής εργασίας θα ήθελα να ευχαριστήσω όλους όσους με βοήθησαν στην περάτωσή της.

Πρώτα από όλα, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή, κ. Αναστάσιο Οικονομίδη, καθηγητή του Τμήματος Οικονομικών Επιστημών του Πανεπιστημίου Μακεδονίας, όχι μόνο για την εμπιστοσύνη που μου έδειξε και την ευκαιρία που μου έδωσε να εκπονήσω τη διπλωματική μου εργασία, αλλά και για τις συμβουλές του καθ' όλη τη διάρκεια της διπλωματικής μου εργασίας και το χρόνο που διέθεσε για τη βαθμολόγηση της παρούσας εργασίας.

Ευχαριστώ πολύ τον πρόεδρο και καθηγητή του Τμήματος Οικονομικών Επιστημών του Πανεπιστημίου Μακεδονίας, κ. Θεόδωρο Παναγιωτίδη, για τη προθυμία του να δεχτεί την επίβλεψη της παρούσας εργασίας και για τον χρόνο που διέθεσε για τη βαθμολόγησή της.

Ευχαριστώ θερμά τη κ. Μαρία Περηφάνου, διδάσκουσα του Τμήματος Ιταλικής Γλώσσας και Φιλολογίας του Αριστοτελείου Πανεπιστημίου για τη βοήθεια της στη σύνθεση του ερωτηματολογίου μου και τη παρακολούθηση της πορείας της διπλωματικής μου εργασίας.

Κλείνοντας, οφείλω να ευχαριστήσω τους γονείς μου, Δαμιανό και Γεωργία για τη στήριξή τους και την ανεξάντλητη υπομονή και αγάπη τους.

Σας ευχαριστώ όλους και τον καθένα ξεχωριστά.

ΠΕΡΙΛΗΨΗ

Η εργασία πραγματεύεται τη συμπεριφορά των χρηστών του διαδικτύου σε απόπειρες «phishing». Κάθε «phishing» email που αποστέλλει ένας «phisher» και κάθε «phishing» ιστότοπος που δημιουργεί, έχει ως στόχο να εξαπατήσει τους χρήστες του κυβερνοχώρου με διάφορους τρόπους και να αποσπάσει από αυτούς χρηματικά ποσά. Παρακάτω, θα αναλυθούν μεταξύ άλλων θέματα που σχετίζονται με τους μηχανισμούς που χρησιμοποιούν οι «phishers» για να εξαπατήσουν τα θύματά τους, τις μορφές «phishing» που υπάρχουν, τα χαρακτηριστικά που βοηθούν τους χρήστες του Ίντερνετ να αναγνωρίσουν μια επίθεση «phishing», τους λόγους για τους οποίους οι χρήστες πέφτουν θύματα «phishing», καθώς και τρόποι που συμβάλουν στην αντιμετώπιση του «phishing». Σε συνέχεια της βιβλιογραφικής ανασκόπησης, συντάχθηκε ερωτηματολόγιο που αποσκοπούσε στην απάντηση τριών ερευνητικών ερωτημάτων. Τα δύο εκ των τριών, εξετάζουν αν η ικανότητα των χρηστών του διαδικτύου να αναγνωρίσουν ένα «phishing» email ή μια «phishing» ιστοσελίδα που προέρχεται από τη τράπεζα επηρεάζεται από τα μέσα που υπάρχουν για να προστατέψουν τους χρήστες του διαδικτύου από το «phishing», ενώ το τρίτο αναφέρεται στους παράγοντες που ωθούν τους χρήστες του Ίντερνετ να κάνουν κλικ σε «phishing link» που προέρχονται από τη «τράπεζα». Τα αποτελέσματα της έρευνας, έπειτα της στατιστικής ανάλυσης που επιδέχτηκαν οι απαντήσεις των συμμετεχόντων του ερωτηματολογίου, έδειξαν ότι ορισμένα από τα μέσα που υπάρχουν για να προστατέψουν τους χρήστες του κυβερνοχώρου από το «phishing» είναι αποτελεσματικά, ενώ άλλα όχι και επιπλέον αναδείχθηκαν οι παράγοντες που ωθούν τους χρήστες να πέσουν θύματα επιθέσεων «phishing».

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Το διαδίκτυο (Internet) αποτελεί ένα τεράστιο δίκτυο με άπειρες δυνατότητες, οι οποίες μετατρέπονται σε απειλές για τους ανεκπαίδευτους χρήστες του (Kim et al., 2015). Η τεχνολογία του διαδικτύου έχει επεκταθεί σε όλο το κόσμο, με αποτέλεσμα οι καθημερινές ενέργειες του «σύγχρονου» κόσμου να εξαρτώνται από αυτή. Χαρακτηριστικό παράδειγμα αποτελούν οι εργαζόμενοι, οι οποίοι έχουν τη δυνατότητα να εργάζονται από το σπίτι τους. Αυτή η ενέργεια ευνοεί τους χακερ. Σε αντίθεση με τους εργαζόμενους που δουλεύουν στο χώρο εργασία τους, οι εργαζόμενοι από το σπίτι είναι απίθανο να διαθέτουν τη κατάλληλη υποδομή πληροφορικής για να προστατευθούν από τα κυβερνοεγκλήματα. Όσο προοδεύει η τεχνολογία αντίστοιχα πρέπει να εξελίσσονται και οι διαδικασίες που χρησιμοποιούν οι άνθρωποι για να αποτρέψουν τη διάδοση των προσωπικών τους πληροφοριών. Πιο συγκεκριμένα, η διάδοση των προσωπικών πληροφοριών επιτυγχάνεται μέσω του χακαρίσματος (hacking) και του ηλεκτρονικού ψαρέματος (Phishing) που προέρχεται από ανθρώπους που επιθυμούν να αποκτήσουν είτε οικονομικό είτε κοινωνικό κέρδος.

Με τον όρο ηλεκτρονικό ψάρεμα (Phishing) αναφερόμαστε σε μία κυβερνοεπίθεση που έχει ως σκοπό την κλοπή των προσωπικών και οικονομικών πληροφοριών από τους χρήστες του κυβερνοχώρου, όπως για παράδειγμα κωδικούς πρόσβασης και στοιχεία ηλεκτρονικής τραπεζικής. Οι χρήστες του internet πέφτουν θύματα είτε μέσω κακόβουλων συνδέσμων είτε μέσω μηνυμάτων που δέχονται στο ηλεκτρονικό ταχυδρομείο με αποτέλεσμα την απόσπαση διάφορων χρηματικών ποσών. Συνήθως, οι «hackers» φτιάχνουν ψεύτικες ιστοσελίδες που μοιάζουν πολύ με τις νόμιμες ιστοσελίδες και ζητούν από τα θύματα να συμπληρώσουν τα στοιχεία τους. Σύμφωνα με τη Google καθημερινά μπαίνουν στη μαύρη λίστα 9500 ιστότοποι (Goodin, 2012).

Στις μέρες μας, η χρήση κινητών τηλεφώνων έχει επεκταθεί σε όλες τις ηλικιακές ομάδες. Αυτό οφείλεται στο μέγεθος της συσκευής το οποίο είναι μικρό, εύκολο στη μετακίνηση σε εξωτερικούς χώρους και με μεγάλη διάρκεια μπαταρίας (Foozy et al., 2013). Το αυξημένο εύρος ηλικίας που χρησιμοποιεί κινητά τηλέφωνα, οδήγησε σε αύξηση των επιθέσεων «phishing». Οι «phishers» στέλνουν στα θύματα μηνύματα με συνδέσμους που τους οδηγούν σε ιστοσελίδες «phishing» και ζητούν τα προσωπικά τους στοιχεία (CAPEC, 2017). Συγκριτικά με όσους χρησιμοποιούν επιτραπέζιους υπολογιστές, οι χρήστες των κινητών τηλεφώνων διακατέχουν τρεις φορές μεγαλύτερο κίνδυνο να πέσουν θύματα «phishing» (Kessem, 2012). Ένας από τους λόγους που συμβαίνει αυτό αφορά τη μικρή οθόνη του κινητού που εμποδίζει τον χρήστη να δει όλες τις λεπτομέρειες του μηνύματος. Οι «phishers» εκμεταλλεύονται τις αρνητικές συνέπειες που επιφέρουν οι μικρές συσκευές τηλεφώνων, την απερίσκεπτη συμπεριφορά και την ελλιπή γνώση των χρηστών κινητών τηλεφώνων σχετικά με τις επιθέσεις «phishing» (Tewari et al., 2016). Οι

επιθέσεις «phishing» επιδρούν αρνητικά στην οικονομία, εξαιτίας της απώλειας χρηματικών ποσών τόσο των επιχειρήσεων όσο και των ατόμων γενικότερα (Gupta et al., 2017).

Προκειμένου να προστατευθούν οι χρήστες του διαδικτύου από επιθέσεις «phishing» προτείνονται διάφοροι τρόποι αντιμετώπισης, με σκοπό την εύρεση στοιχείων που παραπέμπουν σε απειλή από «phishers» και την πρόληψη των χρηστών από την εξαπάτηση. Για την εύρεση αυτών των στοιχείων οι χρήστες του Ίντερνετ προμηθεύονται από την αγορά κατάλληλα λογισμικά εντοπισμού του «phishing» που διαθέτουν «Blacklist». Ωστόσο, η «Blacklist» έχει το ελάττωμα να μην ανιχνεύει τις επιθέσεις «phishing» μηδενικής ημέρας (Chorghe and Shekokar, 2016). Πληθώρα ιστοτόπων ηλεκτρονικού ψαρέματος δημιουργούνται και λήγουν καθημερινά. Σύμφωνα με το Anti-Phishing Working Group(APWG), ένας «phishing» ιστότοπος είναι ενεργός περίπου 4,5 ημέρες στον κυβερνοχώρο ή ορισμένες φορές διατηρείται για ελάχιστες μόνο ώρες (Cranor et al.,2007).

Ο μηχανισμός του «Phishing email»

Οι «phishers» έχουν ως στόχο την εξαπάτηση των χρηστών του διαδικτύου και για αυτόν το λόγο αποστέλλουν μαζικά ανεπιθύμητα μηνύματα στην ηλεκτρονική διεύθυνση αλληλογραφίας (phishing emails) με πλαστούς συνδέσμους URL. Η ενέργεια αυτή περιγράφει το «phishing» μέσω email, το οποίο είναι παράνομο, καθώς προσποιείται ότι προέρχεται από μία νόμιμη και δημοφιλή εταιρία (Nguyen et al., 2014). Παρόλα αυτά τα «phishing emails», δεν πρέπει να μοιάζουν με πλαστά μηνύματα, καθώς οι χρήστες πιθανώς να υποψιαστούν ότι πρόκειται να «πέσουν θύματα επίθεσης» και να μην πράξουν όπως αναμένουν οι εισβολείς, για να είναι επιτυχές το «phishing» (Moore & Clayton, 2007).

Τα «phishing emails» θα πρέπει να περιλαμβάνουν κάποια χαρακτηριστικά, έτσι ώστε να είναι ικανά να εξαπατήσουν τον χρήστη. Αρχικά, στο κείμενο του «phishing email» θα πρέπει να υπάρχει ένας «ψεύτικος σύνδεσμος» και να είναι κατάλληλα διαμορφωμένο, ώστε να παρακινεί τον αναγνώστη να κάνει «κλικ» σε αυτό για να πραγματοποιήσει μία ενέργεια, όπως είναι η πληρωμή μιας συνδρομής σε μια πλατφόρμα συνδρομητικών διαδικτυακών τηλεοπτικών υπηρεσιών για παράδειγμα στο Netflix (Moore & Clayton, 2007) ή να ενημερώσει τα στοιχεία του τραπεζικού του λογαριασμού (Moore & Clayton, 2007; Nguyen et al., 2014). Μόλις το θύμα πατήσει στο σύνδεσμο, είτε θα οδηγηθεί σε μια «phishing ιστοσελίδα» είτε θα «κατεβάσει», εν αγνοία του, έναν ιό. Οι επιτήδειοι προκειμένου να πείσουν τα θύματά τους ότι το email προέρχεται από έγκυρη πηγή και να αντλήσουν από αυτούς χρήσιμες πληροφορίες για να τους εξαπατήσουν, χρησιμοποιούν τεχνικές της κοινωνικής μηχανικής. (Nguyen et al., 2014)

Για να επιτευχθεί ο στόχος των «phishers» θα πρέπει το «phishing email» να μην αναγνωρίζεται από τις «μαύρες λίστες» (blacklist) που έχουν πρόσβαση τα «φίλτρα ανεπιθύμητης αλληλογραφίας» και διακρίνουν το «πλαστό ιστότοπο» από το «νόμιμο ιστότοπο» (Moore & Clayton, 2007). Εφόσον το πρόγραμμα περιήγησης δεν χαρακτηρίσει τη σελίδα ως «σελίδα ηλεκτρονικού ψαρέματος», ο χρήστης θα συνδεθεί με μία σελίδα απολύτως όμοια με τη γνήσια της εταιρείας. Έτσι, ο χρήστης θα αισθανθεί ασφαλής και θα πληκτρολογήσει τα προσωπικά του στοιχεία με αποτέλεσμα να πέσει «θύμα ηλεκτρονικής απάτης». Τα παραβιασμένα δεδομένα συνήθως στέλνονται μέσω email σε μια διεύθυνση webmail, όμως κάποιες άλλες φορές αποθηκεύονται σε μορφή αρχείου απλού κειμένου στον «phishing ιστότοπο» με σκοπό να καταλήξουν στον «phisher». Τέλος, αφού ο αρχικός σκοπός επιτεύχθηκε, ο «phisher» σβήνει τον ιστότοπο και στη συνέχεια αφαιρεί χρηματικά ποσά από τον λογαριασμό του θύματος (Moore & Clayton, 2007).

Spear phishing

Ένα καινοτόμο είδος «phishing email» είναι το «spear phishing», στο οποίο ο «phisher» επικεντρώνεται στην εξαπάτηση συγκεκριμένων ανθρώπων, οργανισμών ή

επιχειρήσεων. Σύμφωνα με τους Moore & Clayton (2007), έχει αποδειχθεί πως το «spear phishing» επιτυγχάνει το στόχο του, δηλαδή να παραπλανήσει τον δέκτη του email, καθώς το 70% των αποδεκτών ανοίγει το email και σε διάστημα μίας ώρας το 50% αυτών πατούν στο σύνδεσμο που αναγράφεται στο email» (Moore & Clayton, 2007). Στο «spear phishing» ο αποστολέας του email φέρει το όνομα μιας διάσημης εταιρίας ή κάποιου οργανισμού όπου έχει λογαριασμό ο χρήστης του διαδικτύου και τον εμπιστεύεται επειδή έχει συνομιλήσει με αυτόν (Moore & Clayton, 2007; Al-Hamar et al., 2021). Ακόμη, ο «phisher» μπορεί να μιμηθεί τη ταυτότητα φίλων και συνεργατών του θύματος (Al-Hamar et al., 2021). Η επιτυχία του «spear phishing» οφείλεται όχι μόνο στην αξιόπιστη πηγή που φαίνεται να έχει το email αλλά και στο εύστοχο περιεχόμενο του, αφού ο «phisher» έχει συλλέξει πληροφορίες για το θύμα και έχει συντάξει το email αποκλειστικά για αυτόν (Moore & Clayton, 2007; Al-Hamar et al., 2021).

Whaling

Το Whaling αποτελεί μια κατηγορία «phishing» που εστιάζει σε μεγάλες εταιρίες και υψηλόβαθμα στελέχη, τα οποία διαχειρίζονται πολύτιμες πληροφορίες (Pienta et al., 2020). Ο απώτερος σκοπός της επίθεσης εξαρτάται από την εξουσία που κατέχει ο δέκτης του παραπλανητικού email στην εταιρία (Goel & Jain, 2018). Για να οργανώσουν την επίθεσή τους οι «Whalers» παρατηρούν τις δραστηριότητες των θυμάτων τους όχι μόνο στα μέσα κοινωνικής δικτύωσης ώστε να αντλήσουν πληροφορίες που σχετίζονται με τη προσωπική τους ζωή αλλά και τις ιστοσελίδες της επαγγελματικής τους δραστηριότητας για να αποκομίσουν πληροφορίες που αναφέρονται στην επαγγελματική τους απασχόληση (Pienta et al., 2020). Οι πληροφορίες αυτές, σε συνδυασμό με τη κοινωνική μηχανική συμβάλλουν στην οργάνωση πολύ πειστικών επιθέσεων (Pienta et al., 2020). Δεδομένου ότι τα κέρδη που εισπράττουν οι «Whalers» από αυτές τις επιθέσεις είναι μεγάλα, αφιερώνουν πολύ χρόνο για να κατασκοπεύσουν το προφίλ του θύματος, ώστε η επίθεσή τους να είναι επιτυχημένη και δύσκολα ανιχνεύσιμη από τα συστήματα ασφαλείας (Shankar et al., 2019).

Συνοψίζοντας, το «Whaling» διαφέρει από το «phishing email» και το «spear phishing». Σε κάθε περίπτωση οι επιτιθέμενοι θέλουν να εξαπατήσουν διαφορετικές ομάδες ανθρώπων. Για παράδειγμα, ενώ το «Whaling» εστιάζει σε υψηλόβαθμα στελέχη μιας τράπεζας, το «phishing email» επικεντρώνεται σε όλους τους χρήστες που έχουν λογαριασμό Gmail. Από την άλλη μεριά, το «spear phishing» προσανατολίζεται σε συγκεκριμένες ομάδες ανθρώπων όπως είναι για παράδειγμα η ομάδα του λογιστηρίου ενός χρηματοπιστωτικού ιδρύματος (Pienta et al., 2020).

Hacking

Ο όρος «hacking» αναφέρεται σε κάθε τεχνική προσπάθεια από έναν «hacker» για την εκμετάλλευση αδυναμιών του συστήματος ή του δικτύου του υπολογιστή που χρησιμοποιούν οι χρήστες του διαδικτύου με σκοπό να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αυτά (Desolda et al., 2022). Οι «hackers»

δημιουργούν επιθέσεις μέσω κακόβουλων προγραμμάτων στο διαδίκτυο, αντιμετωπίζοντας το hacking, ως κίνητρο για κέρδος. Για την εύρεση των τρωτών σημείων των δικτύων του υπολογιστή, οι «hackers» χρησιμοποιούν σαρωτή ευπάθειας και σαρωτή θυρών (Desolda et al., 2022).

Από τη μια μεριά, ο «σαρωτής ευπαθειών» (vulnerability scanning) επιτρέπει στους «hackers» να συνδεθούν με το δίκτυο του υπολογιστή ενός θύματος και να ελέγξει για πιθανές ευπάθειες, όπως είναι τα σφάλματα στις ρυθμίσεις του δικτύου (Yash et al., 2022). Ένα από τα δημοφιλέστερα εργαλεία σάρωσης ευπαθειών είναι το Nessus, το οποίο χρησιμοποιείται σε Linux και Windows (Yash et al., 2022). Από την άλλη μεριά, ο «σαρωτής θυρών» (port scanning) στο «hacking» αποτελεί λογισμικό, το οποίο σαρώνει ένα δίκτυο ή σύστημα για να βρει ανοιχτές θύρες (Yash et al., 2022). Μέσω των θυρών οι «hackers» μπορούν να αποκτήσουν πρόσβαση στα συστήματα των θυμάτων τους. Πιο αναλυτικά, οι «hackers» αρχικά εντοπίσουν τη διεύθυνση IP του συστήματος που θέλουν να εισβάλλουν και στη συνέχεια σαρώνουν τις θύρες του (Yash et al., 2022). Το πιο διάσημο εργαλείο που χρησιμοποιείται στη σάρωση θυρών για Linux και Windows είναι το Nmap (Yash et al., 2022). Το Nmap σαρώνει διάφορες λειτουργίες του συστήματος και παρέχει στους «hackers» πληροφορίες για αυτό. Για παράδειγμα, εντοπίζει τους διαθέσιμους υπολογιστές του δικτύου ανάλογα με τις διευθύνσεις IP που απαντούν στα αιτήματα του συστήματος (Yash et al., 2022).

Μία ευρέως γνωστή τεχνική που χρησιμοποιείται από τους εισβολείς είναι η επίθεση «Brute Force» κατά την οποία επιδιώκεται το «σπάσιμο ενός κωδικού πρόσβασης» (Bošnjak et al., 2018). Οι «hackers» δοκιμάζουν όλους τους πιθανούς συνδυασμούς από διάφορους κωδικούς πρόσβασης και λέξεις, όπως είναι τα ονόματα ποδοσφαιρικών ομάδων μέχρι να βρουν τον σωστό κωδικό και να αποκτήσουν πρόσβαση στα συστήματα των θυμάτων τους (Bošnjak et al., 2018).

Κοινωνική μηχανική

Η κοινωνική μηχανική αποτελεί μία επιθετική τακτική που χρησιμοποιείται από τους «phishers» και στοχεύει στη παραπλάνηση και εκμετάλλευση των ανθρώπων με σκοπό την άντληση των προσωπικών τους δεδομένων. Σε αυτή τη μορφή επίθεσης, οι «phishers» είναι εξειδικευμένοι σε κάποιον τομέα γνώσης ή τεχνολογίας και αναζητούν τον πιο αδύναμο κρίκο που θα έχει ελλιπή πληροφόρηση της κοινωνικής μηχανικής για να επιτεθούν σε αυτόν. Η κοινωνική μηχανική δεν στοχεύει στην πρόσβαση των δεδομένων των χρηστών μέσω συστημάτων αλλά στη παραπλάνηση των ανθρώπων ώστε οι ίδιοι να προβούν στην αποκάλυψη των προσωπικών τους πληροφοριών (π.χ. κωδικούς πρόσβασης). Αξίζει να σημειωθεί πως οι άνθρωποι αμφισβητούν τις ικανότητες των «phishers», και πιστεύουν ότι δεν θα έπεφταν θύματα τους μέσω της κοινωνικής μηχανικής. Επίσης, οι επιθέσεις κοινωνικής μηχανικής εξελίσσονται διαρκώς και προσαρμόζονται όχι μόνο στις εξελίξεις της πληροφορικής αλλά και στις μορφές επικοινωνίας που χρησιμοποιούν οι άνθρωποι, όπως για παράδειγμα είναι οι τηλεφωνικές κλήσεις και τα ηλεκτρονικά μηνύματα.

Οι πέντε αρχές της πειθούς στην κοινωνική μηχανική(PPSE)

Οι αρχές πειθούς στην κοινωνική μηχανική (PPSE) που χρησιμοποιούν οι «phishers» είναι η επίκληση στην αυθεντία, η κοινωνική απόδειξη, η αρχή της συμπάθειας, ομοιότητας και εξαπάτησης, η αρχή της δέσμευσης, ανταπόδοσης και συνέπειας και η παραπλάνηση/ διάσπαση προσοχής.

Επίκληση στην αυθεντία

Οι άνθρωποι εκπαιδεύονται να εμπιστεύονται τα άτομα που έχουν την αυθεντία και να πράττουν αντίστοιχα με αυτά που τους ζητούν. Με άλλα λόγια, η κοινωνία διδάσκει τους ανθρώπους να μην αμφισβητούν την εξουσία/αυθεντία των ειδικών και να υπακούν σε αυτήν. Οι «phishers» προκειμένου να εξαπατήσουν τους ανθρώπους προσπαθούν να τους πείσουν επιβεβαιώνοντας το λόγο τους με αναφορά σε αξιόπιστες εταιρίες και ιστοσελίδες (Sharevski & Jachim, 2022). Για να επιτευχθεί αυτό, οι «phishers» χρησιμοποιούν λέξεις ή λογότυπα που υποδηλώνουν την εξουσία του αποστολέα και ονόματα από γνωστές και αξιόπιστες εταιρίες, όπως για παράδειγμα το λογότυπο της «Amazon» (Sharevski & Jachim, 2022). Επιπλέον, οι «phishers» για να ισχυροποιήσουν το λόγο τους χρησιμοποιούν επείγουσες λέξεις που υποδηλώνουν φόβο. Πιο συγκεκριμένα συναντάμε εκφράσεις όπως «Κάντε κλικ εδώ», «Θα πρέπει να επιβεβαιώσετε άμεσα τα στοιχεία σας, διαφορετικά ο λογαριασμός σας θα αποκλειστεί εντός 48 ωρών» (Sharevski & Jachim, 2022). Ακόμη, επίκαιρο παράδειγμα πλαστών email με επίκληση στην αυθεντία αποτελούν αυτά που ισχυρίζονται ότι προέρχονται από τον Παγκόσμιο Οργανισμό Υγείας και προτρέπουν τους παραλήπτες να κατεβάσουν ένα έγγραφο με μέτρα ασφαλείας κατά της πανδημίας του COVID-19 (Sharevski & Jachim, 2022). Για το λόγο ότι το κοινό εμπιστεύεται τον Παγκόσμιο Οργανισμό Υγείας και επιθυμεί να ενημερωθεί για τον φονικό ιό, πραγματοποιεί τη λήψη του εν λόγω εγγράφου με αποτέλεσμα να πέσει θύμα απάτης. Συνεπώς, όταν οι άνθρωποι λαμβάνουν ένα email που φέρει τα παραπάνω χαρακτηρίστηκα υπάρχει μεγάλη πιθανότητα να υπακούσουν σε αυτό και να πέσουν θύματα επίθεσης (Sharevski & Jachim, 2022).

Κοινωνική Απόδειξη

Οι άνθρωποι ακολουθούν μία τάση μίμησης ανάλογα με τη συμπεριφορά των υπόλοιπων ανθρώπων της κοινωνίας στην οποία είναι μέλη. Αναλυτικότερα, βλέποντας ότι οι υπόλοιποι άνθρωποι του κοινωνικού συνόλου στο οποίο ανήκουν, δεν είναι καχύποπτοι σχετικά με τα email που δέχονται, ακολουθούν και αυτοί την ίδια συμπεριφορά, παραβλέποντας τους κινδύνους που μπορεί να κρύβει το email (Ferreira et al., 2015). Με αυτό το τρόπο, δεν αισθάνονται αποκλειστικά υπεύθυνοι για τις πράξεις τους, επειδή ακολουθούν την ίδια συμπεριφορά με τους συνανθρώπους τους και έρχονται αντιμέτωποι με τους ίδιους κινδύνους (Ferreira et al., 2015).

Πιο συγκεκριμένα, οι χρήστες του κυβερνοχώρου δείχνουν εμπιστοσύνη στα άτομα που γνωρίζουν, όπως για παράδειγμα είναι οι φίλοι τους ή τους συναδέλφους που απεικονίζονται στο εικονίδιο του email ή υπογράφουν με το όνομά τους στο τέλος του email (Ferreira & Teles, 2019). Παράδειγμα επίκλησης στην κοινωνική απόδειξη

μπορεί να αποτελέσει ένα email που εκ πρώτης όψεως φαίνεται να προέρχεται από το διαχειριστή του συστήματος που εργάζεται ο παραλήπτης του email (Ferreira & Teles, 2019). Σε αυτή τη περίπτωση η διεύθυνση του email θα είναι πανομοιότυπη με τη γνήσια διεύθυνση της εταιρίας και θα ζητάει από τον παραλήπτη να προβεί σε μια ενέργεια που έχουν ακολουθήσει και οι συνεργάτες του, λόγου χάρη να ελέγξει τη λειτουργία ενός συνδέσμου, ο οποίος έχει ήδη δοκιμαστεί και από τους συνεργάτες του (Ferreira & Teles, 2019).

Συνεπώς, όταν οι άνθρωποι λαμβάνουν ένα email από γνωστό τους πρόσωπο, ακόμα κι αν αυτό έχει σημάδια που υποδηλώνουν τη πιθανή εξαπάτησή τους, τείνουν να το εμπιστεύονται λόγω του ότι το εμπιστεύονται και άλλα μέλη του κοινωνικού συνόλου στο οποίο ανήκουν.

Συμπάθεια, Ομοιότητα και Εξαπάτηση

Οι «phishers» πολλές φορές σχεδιάζουν τα email τους σύμφωνα με την αρχή της συμπάθειας, της ομοιότητας και της εξαπάτησης. Η συμπάθεια, θα προσελκύσει τον παραλήπτη και θα εξασφαλίσει την ανάπτυξη μιας καλής σχέσης με τον αποστολέα, ενώ η ομοιότητα θα δημιουργήσει μια αίσθηση ταύτισης του χρήστη με το περιεχόμενο του email με αποτέλεσμα ο χρήστης να εμπιστευτεί το μήνυμα και τελικά να πέσει θύμα εξαπάτησης (Ferreira et al., 2015).

Οι άνθρωποι είναι γνωστό ότι έλκονται από εταιρίες που προσποιούνται ότι είναι οι γνήσιες και εμπιστεύονται όποιον νομίζουν ότι γνωρίζουν. Ειδικότερα, όπως και στη περίπτωση της επίκλησης στην αυθεντία οι «phishers» χρησιμοποιούν λογότυπα και φωτογραφίες από διάσημους οργανισμούς που φέρουν ομοιότητα με τα χαρακτηριστικά των γνήσιων οργανισμών, προκειμένου να εξαπατήσουν τον δέκτη του email (Ferreira & Teles, 2019). Αξιοσημείωτο παράδειγμα αποτελεί η χρήση του λογότυπου «NBG» που ανήκει στην Εθνική Τράπεζα Ελλάδος (Ferreira & Teles, 2019). Επίσης, οι «phishers» προκειμένου να γίνουν πιο συμπαθείς και να αποτρέψουν την καχυποψία του αναγνώστη μερικές φορές χρησιμοποιούν κινούμενα γραφικά και λέξεις που δηλώνουν ευγένεια και σεβασμό (Ferreira & Teles, 2019). Για παράδειγμα, μπορούν να χρησιμοποιήσουν ένα κινούμενο εικονίδιο, όπως μια κινούμενη καρδιά ή εκφράσεις όπως είναι «Αγαπητέ πελάτη», «Αγαπητέ συνεργάτη» (Ferreira & Teles, 2019). Επιπλέον, οι αποστολείς του email για να επιτύχουν την εξαπάτηση ενός χρήστη του κυβερνοχώρου μπορούν να χρησιμοποιήσουν πανομοιότυπες διευθύνσεις email με τους φίλους τους προκειμένου να ενισχύσουν την αξιοπιστία τους (Ferreira & Teles, 2019). Αφού εκ πρώτης όψεως φαίνονται αξιόπιστοι, μπορούν για παράδειγμα να αποστείλουν ένα σύνδεσμο και να ισχυριστούν ότι θα τους οδηγήσει σε μία ενδιαφέρουσα ιστοσελίδα που θα τους ενημερώσει για την επικαιρότητα ή θα τους οδηγήσει σε κάποιο εύθυμο βίντεο που θα τους ψυχαγωγήσει. Ωστόσο, είναι σημαντικό να γνωρίζουν οι χρήστες του διαδικτύου ότι τα μηνύματα που δέχονται δεν αντιπροσωπεύουν απαραίτητα αυτά που ισχυρίζονται (Ferreira & Teles, 2019).

Δέσμευση, Ανταπόδοση και Συνέπεια

Οι άνθρωποι πολλές φορές καταφεύγουν στη δέσμευση για να αισθάνονται σιγουριά για την απόφασή τους. Η δέσμευση μπορεί να πραγματοποιείται σε εργασιακό επίπεδο ή μπορεί να αποτελεί τον συνδετικό κρίκο σε μία ενέργεια που δεν είναι νόμιμη. Για το λόγο ότι οι άνθρωποι θέλουν να είναι συνεπείς με τη δέσμευσή τους όταν συναντούν επείγουσες εκφράσεις, από κάποιον που νομίζουν ότι τον ξέρουν, απαντούν χωρίς δεύτερη σκέψη (Ferreira & Teles, 2019). Ένα παράδειγμα που θα μπορούσε να χρησιμοποιηθεί η αρχή της δέσμευσης είναι όταν ο αποστολέας του email κατέχει εκ των προτέρων τη γνώση ότι ο παραλήπτης αναζητά ένα σπίτι για αγορά. Σε αυτή τη περίπτωση, ο αποστολέας προσφέρει μια εξαιρετικά προσιτή τιμή για το σπίτι με τις προδιαγραφές που επιθυμεί ο παραλήπτης, λόγου χάρη κεντρική τοποθεσία, απαιτώντας όμως την άμεση προκαταβολή από τη μεριά του για να δεσμεύσει το ακίνητο. Ο παραλήπτης του email καταβάλλει άμεσα τη προκαταβολή για να εξασφαλίσει τη «τιμή ευκαιρία», παραβλέποντας την εξακρίβωση της ταυτότητας του αποστολέα με αποτέλεσμα να πέσει θύμα επίθεσης «phishing» (Ferreira & Teles, 2019).

Παραπλάνηση/ Διάσπαση Προσοχής (Distraction)

Οι άνθρωποι, τις περισσότερες φορές, όταν λαμβάνουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου εστιάζουν στα οφέλη που μπορούν να αποκομίσουν από αυτό. Επηρεασμένοι από τα πολλαπλά οφέλη, όμως, παραβλέπουν εξίσου σημαντικά ζητήματα που θα έπρεπε να συλλογιστούν πριν λάβουν μια απόφαση. Για παράδειγμα ένας χρήστης του διαδικτύου θα μπορούσε να δεχτεί ένα email από τον Οργανισμό Προγνωστικών Αγώνων Ποδοσφαίρου(ΟΠΑΠ) που τον συγχαίρει για τα χρήματα που κέρδισε από τη κλήρωση του λαχείου που αγόρασε (Ferreira & Teles, 2019). Σε αυτή τη περίπτωση αν ο «ΟΠΑΠ» ζητούσε από τον χρήστη τα στοιχεία του τραπεζικού του λογαριασμού για την άμεση παραλαβή των χρημάτων του, ο χρήστης πιθανόν να τα έδινε (Ferreira & Teles, 2019). Αυτό θα συνέβαινε διότι εκείνη τη στιγμή το μόνο που θα ενδιέφερε τον χρήστη θα ήταν η άμεση πρόσβασή του στα χρήματα και όχι άλλες λεπτομέρειες, όπως για παράδειγμα ότι αυτός δεν αγόρασε ποτέ λαχείο (Ferreira & Teles, 2019).

Όπως είναι φανερό, οι άνθρωποι παραβλέπουν τους κινδύνους που μπορεί να κρύβει ένα email και επηρεασμένοι από τη στιγμιαία τους χαρά πέφτουν θύματα επίθεσης «phishing». Η επιτυχημένη παραπλάνηση, μεταξύ άλλων, προϋποθέτει τη χρήση λογότυπων, εικόνων, χρήση στοιχείων που ανήκουν στις νόμιμες εταιρίες, και πλαστούς συνδέσμου που οπτικά φαίνονται νόμιμοι (Ferreira & Teles, 2019). Όλα αυτά ενισχύουν την ορθότητα του email και πείθουν τον χρήστη να υπακούσει σε αυτό (Ferreira & Teles, 2019).

Επιλογή της κατάλληλης αρχής πειθούς.

Ανάλογα με το στόχο που θέλουν να πετύχουν οι «phishers» χρησιμοποιούν και τις κατάλληλες αρχές πειθούς κοινωνικής μηχανικής. Αρχικά, αν θέλουν να κλέψουν τα δεδομένα του χρήστη χρησιμοποιώντας μία αρχή, αυτή θα είναι η ομοιότητα (Ferreira & Teles, 2019). Αν θέλουν να χρησιμοποιήσουν δύο αρχές για να

ενισχύσουν την αποτελεσματικότητα μπορούν να χρησιμοποιήσουν την αρχή της ομοιότητας και την επίκληση στην αυθεντία (Ferreira & Teles, 2019). Κατά δεύτερον, αν οι «phishers» επιθυμούν να προσβάλουν τον χρήστη με ένα κακόβουλο λογισμικό μπορούν να χρησιμοποιήσουν την αρχή της ομοιότητας ή τον συνδυασμό της με την παραπλάνηση/ διάσπαση προσοχής (Ferreira & Teles, 2019). Τρίτον, αν οι εισβολείς θέλουν να εξαπατήσουν τον δέκτη του email μπορούν είτε να χρησιμοποιήσουν την ομοιότητα είτε να συνδυάσουν την αρχή της δέσμευσης, ανταπόδοσης και συνέπειας με την παραπλάνηση/ διάσπαση προσοχής. Σε κάθε περίπτωση η τριπλέτα που προσφέρει το πιο παραπλανητικό email είναι ο συνδυασμός της επίκλησης στην αυθεντία με την δέσμευση, ανταπόδοση, συνέπεια και της παραπλάνησης/ διάσπαση προσοχής (Ferreira & Teles, 2019).

Μορφές επίθεσης phishing

Στη σύγχρονη εποχή οι επιθέσεις «phishing» χωρίζονται σε κατηγορίες ανάλογα με το μέσο και το τρόπο που χρησιμοποιούν οι «phishers» για να εξαπατήσουν τα θύματά τους (Ferreira & Lenzini, 2015).

Επίθεση phishing μέσω SMS(Smishing)

Μία από τις πιο διαδεδομένες μεθόδους πραγματοποίησης επιθέσεων «phishing» στα κινητά τηλεφώνα είναι μέσω «Short Message Service» (SMS) (Yeboah-Boateng & Amanor, 2014). Η μέθοδος αυτή ακολουθεί παρόμοιο τρόπο λειτουργίας με τις επιθέσεις «phishing» μέσω ηλεκτρονικού ταχυδρομείου (phishing emails) στοχεύοντας στο «κλέψιμο» των προσωπικών και οικονομικών δεδομένων από τα κινητά τηλέφωνα των θυμάτων τους (Syafitri et al., 2022).

Τα «SMS» που δέχονται οι χρήστες των κινητών περιλαμβάνουν ένα κείμενο το οποίο υποστηρίζει ότι προέρχεται από έγκυρη πηγή όπως για παράδειγμα είναι η εθνική τράπεζα μαζί με ένα σύνδεσμο (Yeboah-Boateng & Amanor, 2014). Πατώντας πάνω στο σύνδεσμο ο χρήστης είτε μεταφέρεται σε ένα πλαστό ιστότοπο είτε ένα κακόβουλο πρόγραμμα εγκαθίσταται στο κινητό του. Και στις δύο περιπτώσεις μέσα από το «Smishing», το οποίο βασίζεται στη κοινωνική μηχανική, οι «phishers» καταφέρνουν να αποκτήσουν πρόσβαση στο κινητό του χρήστη και να παρακολουθούν όχι μόνο τις επαφές και τα εισερχόμενα μηνύματά του αλλά και τις εφαρμογές που έχει εγκαταστημένες στη συσκευή του με αποτέλεσμα να του αποσπάσουν σημαντικές προσωπικές πληροφορίες και χρήματα (Yeboah-Boateng & Amanor, 2014). Για την αντιμετώπιση του «Smishing» έχουν γίνει πολλές προσπάθειες (Yeboah-Boateng & Amanor, 2014). Ωστόσο, για τον λόγο ότι η επίθεση του «smishing» κατέχει πιο προσωπικό χαρακτήρα, επειδή τα SMS αποστέλλονται στο προσωπικό κινητό του θύματος, καθιστά τα θύματα λιγότερο προσεκτικά και επιφυλακτικά (Syafitri et al., 2022). Ακόμη, λόγω του ότι οι σύνδεσμοι που χρησιμοποιούνται στα «SMS» αλλάζουν συνεχώς η ανίχνευσή τους γίνεται όλο και πιο δύσκολη (Yeboah-Boateng & Amanor, 2014).

Επίθεση phishing μέσω Voice over Internet (Vishing)

Το «vishing» υποδηλώνει μια μορφή «phishing» η οποία εστιάζει στις τηλεπικοινωνίες και χρησιμοποιεί τηλεφωνικά μέσα για να εξαπατήσει τους ανθρώπους (Yeboah-Boateng & Amanor, 2014). Οι κακόβουλοι χρήστες χρησιμοποιούν πληθώρα ψυχολογικών τεχνικών, για παράδειγμα προκαλούν ανησυχία στους ανθρώπους για κάποιο θέμα, με απώτερο σκοπό να αποσπάσουν προσωπικές πληροφορίες, όπως είναι οι κωδικοί e-banking από αυτούς χωρίς να το αντιληφθούν (Yeboah-Boateng & Amanor, 2014).

Για να επιτευχθεί το «vishing» χρησιμοποιούνται δύο δημοφιλείς μέθοδοι. Η μία αναφέρεται στη προσομοίωση του τμήματος υποστήριξης (Impersonation on Help Desk, IHD) κατά την οποία οι εισβολείς προσποιούνται ότι είναι υπάλληλοι τμήματος υποστήριξης μιας εταιρείας ή ενός οργανισμού (Yeboah-Boateng & Amanor, 2014). Σε αυτή τη περίπτωση οι απατεώνες προσπαθούν να πείσουν τα θύματα ότι δίνοντας τις προσωπικές τους πληροφορίες συμβάλλουν σε ένα πρόβλημα ή σε μία διαδικασία εξυπηρέτησης πελατών (Syafitri et al., 2022). Αυτή η επίθεση επιτυγχάνεται μέσω τηλεφώνου, email ή άλλων μέσων επικοινωνίας (Yeboah-Boateng & Amanor, 2014). Η δεύτερη δημοφιλέστερη μέθοδος με την οποία επιτυγχάνεται το «vishing» είναι μέσω «Robocalls» (Yeboah-Boateng & Amanor, 2014). Σε αυτή τη τακτική παρατηρούνται ανεπιθύμητες κλήσεις από κακόβουλους χρήστες, οι οποίοι πολλές φορές εικάζονται ότι πωλούν προϊόντα για να αντλήσουν ευαίσθητα δεδομένα από τους χρήστες και να τους εξαπατήσουν (Yeboah-Boateng & Amanor, 2014). Αυτή η μέθοδος στοχεύει σε σταθερά, κινητά τηλέφωνα και τηλέφωνα γραφείων (Syafitri et al., 2022). Η μόνη διαφορά ανάμεσα στο «Vishing» και στο «Phishing» είναι ότι το «Vishing» για να καταφέρει να εξαπατήσει τους ανθρώπους χρησιμοποιεί τεχνολογία φωνής (Yeboah-Boateng & Amanor, 2014).

Επιθέσεις «Pharming»

Το «pharming» είναι μια εξελιγμένη μορφή «phishing», η οποία είναι ικανή να εγκαταστήσει κρυφά κακόβουλο λογισμικό ή ιό σε μια συσκευή, όταν χρησιμοποιείται. Το «pharming» ανακατευθύνει τους χρήστες του διαδικτύου σε ένα πλαστό ιστότοπο, χωρίς τη συγκατάθεσή τους, αφού οι χρήστες έχουν πληκτρολογήσει στη μηχανή αναζήτησης τη νόμιμη διεύθυνση της ιστοσελίδας. (Brody et al., 2007; Alkhalil et al., 2021)

Οι «pharmers» δημιουργούν ιστοτόπους «pharming» που μοιάζουν οπτικά πολύ με τους νόμιμους αποσκοπώντας στη παραπλάνηση όλο και περισσότερων θυμάτων (Gastellier-Prevost, et al., 2011). Η πιο γνωστή τεχνική που χρησιμοποιούν οι «pharmers» για να κατευθύνουν τους χρήστες του διαδικτύου σε έναν ιστότοπο που αποτελεί απομίμηση του γνήσιου, είναι η αλλαγή της λίστας διευθύνσεων του Domain Name System (DNS). Με αυτό το τρόπο, οι εισβολείς αντλούν τις πληροφορίες που έχει πληκτρολογήσει ο χρήστης στον «pharming» ιστότοπο (π.χ. όνομα πατέρα, πληροφορίες πιστωτικών καρτών) και πραγματοποιούν πολυάριθμες απάτες χωρίς να είναι απαραίτητο να έχει προηγηθεί «κλικ» σε κάποιο «phishing» URL (Brody et al., 2007). Βέβαια, το «pharming» είναι πιο αποτελεσματικό όταν

συνδέεται με κακόβουλες επιθέσεις όπως είναι οι επιθέσεις «phishing». Σε αυτή περίπτωση οι χρήστες του διαδικτύου κάνουν «κλικ» σε ένα σύνδεσμο και με τη παρέμβαση του DNS κατευθύνονται σε πλαστούς ιστοτόπους που μοιάζουν οπτικά με τους γνήσιους (Brody et al., 2007)

Επίθεση phishing μέσω ιστότοπου

Το «phishing» μέσω ιστότοπου έχει ως σκοπό τη παραπλάνηση των ατόμων ενός συστήματος. Οι «phishers» ακολουθούν συγκεκριμένα βήματα για να εξαπατήσουν τα θύματά τους.

Πρώτα από όλα, ο εισβολέας δημιουργεί μία πλαστή ιστοσελίδα που έχει κοινά στοιχεία με την αντίστοιχη γνήσια (Basit et al., 2020). Στη συνέχεια, οι «phishers» αποστέλλουν τη διεύθυνση URL της ιστοσελίδας στα θύματά τους ελπίζοντας να τους κινήσουν το ενδιαφέρον και να κάνουν «κλικ» στο σύνδεσμο, καταχωρώντας τα προσωπικά τους δεδομένα (Basit et al., 2020). Για τους εισβολείς είναι πολύ εύκολο να δημιουργήσουν ένα πλαστό ιστότοπο ο οποίος να μοιάζει σε μεγάλο βαθμό με τον γνήσιο ιστότοπο (Wenyin et al., 2011). Οι «phishers» εστιάζουν στη δημιουργία ευρέως γνωστών ιστοσελίδων όπως για παράδειγμα είναι το eBay, PayPal με σκοπό να αντλήσουν οικονομικές και προσωπικές πληροφορίες από τους χρήστες του κυβερνοχώρου (Basit et al., 2020; Wenyin et al., 2011). Ο ιστότοπος μπορεί να είναι μια νόμιμη ιστοσελίδα, η οποία δέχεται επεξεργασία και αποκτά «phishing» περιεχόμενο ή μπορεί να είναι μία ιστοσελίδα που ανήκει στον «phisher» (Basit et al., 2020; Wenyin et al., 2011). Η επιτυχής εξαπάτηση των θυμάτων οφείλεται στο ότι τα θύματα δεν μπορούν να γνωρίζουν εκ των προτέρων το ακριβές περιεχόμενο της ιστοσελίδας που θα μεταφερθούν κάνοντας «κλικ» σε μία διεύθυνση URL (Wenyin et al., 2011).

Τεχνικές phishing

Οι «phishers» προκειμένου να εξαπατήσουν τους χρήστες του διαδικτύου χρησιμοποιούν πληθώρα τεχνικών. Οι τεχνικές «phishing» έχουν κοινά στοιχεία με τις μεθόδους «phishing» και τους τρόπους που χρησιμοποιούν οι «phishers» για να επιτύχουν το στόχο τους. Παρακάτω αναλύονται μερικές από τις πιο γνωστές τεχνικές «phishing».

Πλαστή άγκυρα

Οι «phishers» πολλές φορές , αξιοποιούν το «Hyper Text Markup Language» (HTML), το οποίο είναι μια γλώσσα προγραμματισμού μέσω της οποίας δημιουργούνται και σχεδιάζονται ιστοσελίδες στον Παγκόσμιο Ιστό (Fette et al., 2007). Οι κυβερνοεγκληματίες χρησιμοποιούν τα μηνύματα του ηλεκτρονικού ταχυδρομείου για να «ψαρέψουν» τις προσωπικές πληροφορίες των θυμάτων τους (Fette et al., 2007).

Με τη χρήση του ηλεκτρονικού ταχυδρομείου οι «phishers» μπορούν να παραπλανήσουν τους χρήστες του διαδικτύου, γιατί ο σύνδεσμος που εμφανίζεται

στο email μπορεί να κατευθύνει τους χρήστες σε τελείως διαφορετικό ιστότοπο. Πιο συγκεκριμένα, αν ένας χρήστης δεχτεί στο email το σύνδεσμο (link) «paypal.com» και κάνει κλικ σε αυτό μπορεί να συνδεθεί άθελά του στο badsite.com (Fette et al., 2007). Αυτό συμβαίνει γιατί ο κώδικας HTML που κρύβεται από πίσω είναι paypal.com (Fette et al., 2007). Αναλύοντας το κώδικα HTML διαπιστώνουμε ότι το χαρακτηριστικό href καθορίζει τον προορισμό του χρήστη, όταν κάνει κλικ στον σύνδεσμο, ενώ το paypal.com υποδηλώνει το κείμενο του συνδέσμου που αντικρίζει ο χρήστης στο email και πατάει πάνω σε αυτό για να κατευθυνθεί στον ιστότοπο. Στη προκειμένη περίπτωση ο κώδικας θα δείξει στο πρόγραμμα περιήγησης του χρήστη το badsite.com (Fette et al., 2007).

Επίσης, η δύναμη της πλαστής άγκυρας ενισχύεται και με την ασυνέπεια ονόματος τομέα, κατά την οποία οι απατεώνες αντικαθιστούν γράμματα που είναι οπτικά πανομοιότυπα μεταξύ τους και οι χρήστες του διαδικτύου μπορεί να τα παραβλέψουν (Dhamija et al., 2006). Χαρακτηριστικό παράδειγμα αποτελεί το www.paypa1.com κατά το οποίο παρατηρείται αντικατάσταση του αριθμού «1» με το γράμμα «l» που εκ πρώτης όψεως μοιάζουν (Dhamija et al., 2006).

Ψεύτικο πιστοποιητικό SSL(Secure Sockets Layer)/ TLS(Transport Layer Security):

Οι επιθέσεις ηλεκτρονικού ψαρέματος επιτυγχάνονται με τη δημιουργία παράνομων ιστοσελίδων. Αν και η νόμιμη ιστοσελίδα ενός ιστότοπου ταυτίζεται σε μεγάλο βαθμό με τη παράνομη ιστοσελίδα του ιστότοπου, υπάρχουν διαφορές μεταξύ τους (Goel & Kumar Jain, 2017).

Μία από τις πιο βασικές διαφορές είναι ότι μία νόμιμη ιστοσελίδα πρέπει υποχρεωτικά να φέρει το πιστοποιητικό SSL/TLS για να προσφέρει ασφάλεια των προσωπικών δεδομένων του επισκέπτη της ιστοσελίδας (Goel & Kumar Jain, 2017). Το πρωτόκολλο TLS αποτελεί τη νεότερη έκδοση του πρωτοκόλλου SSL. Το πρωτόκολλο SSL/TLS δημιουργεί μια κρυπτογραφική σύνδεση μεταξύ του web server και του browser του χρήστη ενισχύοντας την ασφαλή ανταλλαγή πληροφοριών(π.χ. κωδικοί τράπεζας) (Goel & Kumar Jain, 2017).

Πιο συγκεκριμένα το SSL/TLS ελέγχει και πιστοποιεί τη ταυτότητα του διακομιστή βεβαιώνοντας τον πελάτη ότι η ιστοσελίδα είναι νόμιμη και τα προσωπικά του δεδομένα δεν κινδυνεύουν να κλαπούν από κακόβουλους χρήστες (Freier et al., 2011).

Η ύπαρξη του πρωτοκόλλου SSL/TLS σε μία ιστοσελίδα μπορεί να γίνει αντιληπτό από τον επισκέπτη με δύο τρόπους. Αρχικά, η ιστοσελίδα θα πρέπει να φέρει το εικονίδιο του λουκέτου στη γραμμή διευθύνσεως του browser και η διεύθυνση URL θα πρέπει να ξεκινάει με το πρόθεμα “https”(Hypertext Transfer Protocol Secure) (Conrad & Feldman, 2017).

Για το λόγο ότι ορισμένοι χρήστες του διαδικτύου αντιλαμβάνονται μόνο το σημασιολογικό ρόλο του εικονιδίου δημιουργείται σύγχυση όταν οι απατεώνες

τοποθετούν πλαστά εικονίδια κλειδαριάς μέσα στο περιεχόμενο μιας ιστοσελίδας. (Dhamija et al., 2006)

Ένας τρόπος που συμβάλλει στη διάκριση της πλαστής από την αληθινή κλειδαριά είναι το «κλικ» στο εικονίδιο της κλειδαριάς, το οποίο θα πρέπει να εμφανίζει πληροφορίες σχετικά με το πιστοποιητικό SSL (Ye et al., 2005).

Αν και τα προγράμματα περιήγησης προειδοποιούν τους χρήστες όταν εντοπίζουν ασυνέπεια στα πεδία του πιστοποιητικού ασφαλείας (π.χ. όνομα εκδότη και ημερομηνία λήξης), οι χρήστες δεν κατέχουν τη γνώση ελέγχου των πιστοποιητικών και αγνοούν τις προειδοποιήσεις των συστημάτων ασφαλείας.

Χρήση υποτομέα

Οι ιστοσελίδες «phishing» χρησιμοποιούν διευθύνσεις URL που οπτικά φαίνονται εν μέρη αξιόπιστες (Fette et al., 2007). Για το λόγο ότι οι απατεώνες δεν μπορούν να χρησιμοποιήσουν αυτούσια τις νόμιμες διευθύνσεις URL κάνουν ορθογραφικά λάθη προκειμένου να δημιουργήσουν πλαστά URL για να ξεγελάσουν τα θύματά τους (Nguyen et al., 2014).

Αναλυτικότερα, στη νόμιμη διεύθυνση URL http://www.apple.attack.com, το «http» υποδηλώνει το πρωτόκολλο επικοινωνίας στον Παγκόσμιο Ιστό (World Wide Web), το «apple» είναι ένας υποτομέας που απαρτίζεται από ποικίλους τύπους ανάλογα με τις υπηρεσίες της σελίδας του τομέα, ο πρωτεύον τομέας είναι το «attack» και το Top-Level-Domain (TLD) το οποίο καθορίζει το τύπο οργανισμού ή τη χώρα στην οποία ανήκει ο ιστότοπος είναι το com (Nguyen et al., 2014). Ομοίως, αν ο νόμιμος ιστότοπος της εθνικής τράπεζας είναι www.nbg.gr, ένας «phisher» μπορεί να επιλέξει ως πλαστό URL της σελίδας το www.ngb.gr το οποίο απαρτίζεται από ένα μέρος νόμιμης και ένα παράνομης διεύθυνσης URL (Fette et al., 2007).

Αναγνώριση phishing email

Κάθε μήνα όλο και περισσότερες επιθέσεις «phishing email» παρατηρούνται στο κυβερνοχώρο. Οι επιθέσεις αυτές στοχεύουν να πείσουν τους χρήστες του διαδικτύου ότι αλληλοεπιδρούν με μια έμπιστη οντότητα και έχουν ως απώτερο σκοπό να «ψαρέψουν» τις προσωπικές πληροφορίες του λογαριασμού τους, τα διαπιστευτήρια σύνδεσής τους και τις πληροφορίες της ταυτότητάς τους γενικότερα (Fette et al., 2007). Έχουν εντοπιστεί κάποια σημάδια, τα οποία μπορούν να συμβάλλουν, έως ένα βαθμό, στην αναγνώριση των phishing email και παραθέτονται παρακάτω.

1. Χρήση επειγουσών λέξεων: Οι «phishers» προκειμένου να δημιουργήσουν άγχος στον αναγνώστη του email χρησιμοποιούν λέξεις που δηλώνουν επείγον με σκοπό να κινητοποιήσουν τα θύματα να προβούν άμεσα στην ενέργεια που αναγράφουν στο email (Longfei et al., 2014).
2. Αίτημα για προσωπικά δεδομένα: Αρχικά οι εισβολείς προσπαθούν να κερδίσουν την εμπιστοσύνη των θυμάτων τους (π.χ. χρησιμοποιούν την αρχή

της αυθεντίας) και στη συνέχεια τους ζητούν προσωπικές πληροφορίες (π.χ. κωδικούς πρόσβασης) (Longfei et al., 2014).

3. Άγνωστος αποστολέας: Ο εισβολέας προσποιείται ότι ανήκει σε ένα μεγάλο οργανισμό και αυτός ο οργανισμός φαίνεται και ως όνομα αποστολέα. Έτσι, ο δέκτης του email εμπιστεύεται τον οργανισμό χωρίς να γνωρίζει τη ταυτότητα του αποστολέα και πέφτει θύμα επίθεσης (Longfei et al., 2014).
4. Πλαστός υπερσύνδεσμος: Τα phishing email περιλαμβάνουν και phishing υπερσυνδέσμους οι οποίοι οδηγούν τους χρήστες του διαδικτύου σε πλαστές ιστοσελίδες. Χαρακτηριστικό παράδειγμα αποτελεί η αντικατάσταση των γραμμάτων της διεύθυνσης URL και πιο συγκεκριμένα του μικρού λατινικού γράμματος «λάμδα»(l) από το κεφαλαίο λατινικό χαρακτήρα «ιώτα»(του «I» από το κεφαλαίο (i) τα οποία έχουν πολύ μικρή διαφορά ύψους που δεν μπορεί να γίνει αντιληπτή από τα ανθρώπινα μάτια (Longfei et al., 2014).
5. Ορθογραφικά και γραμματικά λάθη: Τα μηνύματα ηλεκτρονικού ψαρέματος χαρακτηρίζονται από «κακή» χρήση της γλώσσας. Αυτό θα πρέπει να ανησυχεί τον αναγνώστη, διότι τα μηνύματα που αποστέλλονται από μέλη μεγάλων οργανισμών (π.χ. τράπεζες) ελέγχονται για ορθογραφικά και γραμματικά λάθη (Longfei et al., 2014).

Εκπαίδευση χρηστών

Το «phishing» αποτελεί ένα πρόβλημα μείζονος σημασίας το οποίο βλάπτει τους ανθρώπους και εξελίσσεται με ραγδαίους ρυθμούς. Η ενημέρωση των ανθρώπων για τις απειλές του «phishing» επιτυγχάνεται μέσα από την εκπαίδευσή τους. Η εκπαίδευσή αυτή μπορεί να περιλαμβάνει την ένδειξη προειδοποιήσεων στην οθόνη του κινητού ή του υπολογιστή και την εκπαίδευσή τους μέσα από παιχνίδια ειδικών προδιαγραφών.

Ενεργητικές και παθητικές προειδοποιήσεις

Πρώτα από όλα, η ένδειξη προειδοποίησης στην οθόνη του κινητού ή του υπολογιστή προϋποθέτει την ανάλογη ενεργοποίηση στο πρόγραμμα περιήγησης ιστού από τον χρήστη. Η προειδοποίηση μπορεί να είναι είτε παθητική (passive warning) είτε ενεργητική (active warning). Η παθητική προειδοποίηση απεικονίζει αποκλειστικά τη προειδοποίηση και δίνει τη δυνατότητα στο χρήστη να την δεχτεί και να μη πάει παρακάτω ή να την απορρίψει και να συνεχίσει με δική του ευθύνη. Αντίθετα, η ενεργητική προειδοποίηση πράττει η ίδια, δηλαδή δεν επιτρέπει τον χρήστη να συνεχίσει παρακάτω αν κρίνει πως το περιεχόμενο δεν είναι ασφαλές. Δεδομένου ότι οι χρήστες δεν δίνουν την απαιτούμενη προσοχή στις ενδείξεις άγεται το συμπέρασμα πως οι ενεργές ενδείξεις έχουν μεγαλύτερη αποτελεσματικότητα συγκριτικά με την παθητικές ενδείξεις. Σύμφωνα με τους Egelman et al. (2018), η αποτελεσματικότητα των «active warnings» αποδεικνύεται από την έρευνα που συμμετείχαν 60 άτομα και το 79% των συμμετεχόντων, σε αντίθεση με τις «passive warnings», επωφελήθηκε από αυτές και δεν έπεσε θύμα ηλεκτρονικού ψαρέματος (Egelman et al., 2018).

Εκπαίδευση μέσω παιχνιδιών κινητού

Η εκπαίδευση των χρηστών κινητού τηλεφώνου αποτελεί μία από τις κυριότερες μεθόδους για την αναγνώριση όχι μόνο των νόμιμων ιστοσελίδων, αλλά και των αξιόπιστων email που θα συμβάλλουν στην αποφυγή της εξαπάτησής τους από «phishers» (Alghamdi , 2017). Η ταχύτατη ανάπτυξη της τεχνολογίας και η χρήση του διαδικτύου από ανεκπαίδευτους χρήστες, οδήγησε πολλούς κατόχους κινητών τηλεφώνων να πέσουν θύματα «phishing» (Alghamdi , 2017). Η εκπαίδευση των χρηστών του διαδικτύου μπορεί να γίνει μέσω της εννοιολογικής γνώσης του «phishing» και μέσα από διαδραστικά παιχνίδια κινητών τηλεφώνων, μειώνοντας την αποτελεσματικότητα των επιθέσεων «phishing» (Alghamdi , 2017). Για το λόγο ότι τα κινητά τηλέφωνα είναι φορητά, οι άνθρωποι έχουν τη δυνατότητα να τα χρησιμοποιήσουν όποια στιγμή θέλουν (Alghamdi , 2017). Για παράδειγμα, οι χρήστες των κινητών που επιθυμούν να προστατευθούν από το «phishing» μπορούν να παίζουν το παιχνίδι καθώς περιμένουν στην ουρά του σουπερ μαρκετ ή ενώ ταξιδεύουν με το λεωφορείο (Alghamdi , 2017). Παράδειγμα παιχνιδιών κατά του «phishing» είναι το Anti-Phishing Phill και το PhishGuru (Alghamdi , 2017).

Τα παιδιά και οι έφηβοι έχουν τα κατάλληλα εφόδια για να εντοπίζουν επιθέσεις «phishing»;

Στις μέρες μας η ανάπτυξη της τεχνολογίας έχει οδηγήσει όλο και μικρότερες ηλικίες στον δυτικό κόσμο να χειρίζονται κινητά τηλέφωνα, tablet και κονσόλες παιχνιδιών πολλές φορές χωρίς την επίβλεψη των γονέων τους. Στην ηλικία των τεσσάρων πολλά παιδιά αποκτούν τη πρώτη τους κινητή συσκευή και στην ηλικία των 5-15 έχουν πρόσβαση στον κυβερνοχώρο για τουλάχιστον 8 ώρες τη βδομάδα. Πιο συγκεκριμένα, τα παιδιά χρησιμοποιούν το διαδίκτυο για να επικοινωνούν με τους φίλους τους μέσω των μέσων κοινωνικής δικτύωσης, να παίζουν παιχνίδια και να παρακολουθούν βίντεο στο Youtube (Nicholson et al., 2020). Λόγω της αυξημένης ενασχόλησης των μικρών ηλικιακών ομάδων με το διαδίκτυο, απαιτείται η ένταξη εκπαιδευτικών μεθόδων κατά του «phishing» στην εκπαίδευση. Σύμφωνα με τους Nicholson et al. (2020), αξιοσημείωτο παράδειγμα αποτελεί το γεγονός που διαδραματίστηκε το 2017 στις ΗΠΑ, όπου περισσότερα από 1 εκατομμύρια παιδία ηλικίας κάτω από 17 έπεσαν θύματα κλοπής ταυτότητας με κόστος 2,6 δισεκατομμύρια δολάρια (Nicholson et al., 2020)

Το ηλεκτρονικό ψάρεμα δεν στοχεύει στη θυματοποίηση μόνο των ενηλίκων αλλά και των παιδιών (Nicholson et al., 2020). Οι «phishers» εκμεταλλευόμενοι το γεγονός ότι τα παιδιά δημιουργούν απλούς κωδικούς πρόσβασης στους λογαριασμούς τους χρησιμοποιώντας το όνομα ή την ηλικία τους, πολλές φορές επιδιώκουν την εξαπάτηση των μικρών παιδιών με απώτερο σκοπό να μάθουν πληροφορίες για τους γονείς τους. Πιο συγκεκριμένα, για το λόγο ότι πολλοί ενήλικες, δεν έχουν την ευχέρεια διαχείρισης του διαδικτύου απευθύνονται στα παιδιά και έτσι αν ο «phisher» αποκτήσει πρόσβαση στο λογαριασμό του παιδιού αυτομάτως μπορεί να αντλήσει πληροφορίες και για κάποιον ενήλικα (Nicholson et al., 2020).

Με την ένταξη μαθημάτων κατά του «phishing» στην εκπαίδευση και την κατάλληλη διδασκαλία του ανάλογα με την ηλικιακή ομάδα των παιδιών το φαινόμενο του «phishing» θα περιοριστεί σε μεγάλο βαθμό. Αρχικά, για τα παιδιά ηλικίας 9-12 ετών η εκπαίδευση μπορεί να αρχίσει μέσα από αφηγήσεις από τους δασκάλους τους (Nicholson et al., 2020). Βέβαια αυτή η διαδικασία θα πρέπει να επαναλαμβάνεται σε τακτικά χρονικά διαστήματα γιατί μετά από 2 με 4 εβδομάδες το παιδί αρχίζει να ξεχνάει αυτά που αποκόμισε (Nicholson et al., 2020). Για τις μεγαλύτερες ηλικίες η εκπαίδευση των εφήβων μπορεί να γίνει μέσω κόμικ ή εφαρμογών. Και σε αυτή τη περίπτωση βέβαια η διαδικασία θα πρέπει να επαναλαμβάνεται τακτικά για να μη ξεχνιέται η πληροφορία. Ακόμη, επειδή οι δάσκαλοι σε αυτή την ηλικία αποτελούν πρότυπο για τον νέο, όχι μόνο οι απόψεις τους για την τεχνολογία αλλά και η συμπεριφορά τους μπορεί να αντιγραφεί (Nicholson et al., 2020).

Οι Kumaraguru et al. (2010) σχεδίασαν το διαδικτυακό παιχνίδι «Anti-Phishing Phill» και «PhishGuru» (Sheng et al., 2007; Kumaraguru et al., 2010). Τόσο το «Anti-Phishing Phill» όσο και το «PhishGuru» μπορούν να χρησιμοποιηθούν από σχολικές μονάδες προκειμένου να εκπαιδεύσουν τους χρήστες με τρόπους προστασίας από επιθέσεις «phishing» (Nicholson et al., 2020)

Anti-Phishing Phill

Ο βασικός ήρωας του διαδικτυακού παιχνιδιού “Anti-Phishing Phill” είναι ο Phill, ένα νεαρό ψαράκι που ζει στο Interweb Bay (Sheng et al., 2007). Ο Phill για να μεγαλώσει πρέπει να τρώει αληθινά σκουλήκια και να απορρίπτει τα ψεύτικα σκουλήκια (δολώματα) που του ρίχνουν οι ψαράδες για να τον ψαρέψουν, πριν τελειώσει ο χρόνος (Sheng et al., 2007). Τα αληθινά σκουλήκια αντιπροσωπεύουν τις διευθύνεις URL των γνήσιων ιστοσελίδων, ενώ τα ψεύτικα σκουλήκια αντιπροσωπεύουν τις διευθύνσεις URL των ιστοσελίδων phishing (Sheng et al., 2007). Στο παιχνίδι συναντάμε και τον πατέρα του Phill ο οποίος συμβουλεύει τον γιο του πως να αναγνωρίζει τα δολώματα των ψαράδων, δηλαδή τις ιστοσελίδες phishing (Sheng et al., 2007). Ο στόχος του παιχνιδιού είναι να διδάξει τους παίκτες πώς να ξεχωρίζουν τις νόμιμες διευθύνσεις URL από τις πλαστές διευθύνσεις URL όταν τις συναντούν στη γραμμή διεύθυνσης ενός ιστότοπου αλλά και στο εσωτερικό κάποιου email (Sheng et al., 2007).

PhishGuru

Οι χρήστες δέχονται σε τακτά χρονικά διαστήματα εκπαιδευτικά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία έχουν μορφή «phishing email» και προέρχονται είτε από τον διαχειριστή του συστήματος «phishing» είτε από κάποια εταιρεία εκπαίδευσης (Kumaraguru et al., 2010). Καθώς οι χρήστες ελέγχουν τα εισερχόμενα μηνύματα τους στο ηλεκτρονικό ταχυδρομείο, έχουν πρόσβαση και στο email εκπαιδευτικού περιεχομένου. Τα εκπαιδευτικά μηνύματα έχουν απόλυτη ταύτιση με τα «phishing email», δηλαδή προτρέπουν τους χρήστες να κάνουν «κλικ» σε κάποιο σύνδεσμο και να προβούν σε κάποιες συγκεκριμένες ενέργειες. Αν ο δέκτης του email δεν καταλάβει ότι το email αποτελεί απάτη και πέσει θύμα, δηλαδή αν κάνει «κλικ»

στο σύνδεσμο τότε εμφανίζεται ένα μήνυμα παρέμβασης που προειδοποιεί τον χρήστη ότι είναι ευάλωτος σε επιθέσεις phishing και του προτείνει τρόπους προστασίας από επιθέσεις «phishing» (Kumaraguru et al., 2010).

Η εκπαίδευση των παιδιών σχετικά με τις επιθέσεις «phishing» από τα σχολεία τους δεν θα τους ωφελήσει μόνο στη παιδική τους ηλικία αλλά και μελλοντικά. Για παράδειγμα, θα τους ωφελήσει στον εργασιακό τους τομέα. Πιο συγκεκριμένα, όταν ένας εργαζόμενος δεχτεί ένα email από τη τράπεζά που συνεργάζεται ο οργανισμός που δουλεύει θα πρέπει να είναι σε θέση να αναγνωρίσει αν είναι γνήσιο ή «phishing». Αν δεν μπορεί να ξεχωρίσει ένα γνήσιο από ένα παράνομο email ο εργαζόμενος, θα αγνοήσει το email που δέχτηκε από τη τράπεζα και αυτό μπορεί να επιφέρει απώλεια χρημάτων στον οργανισμό ή/και πρόστιμα.

Λόγοι για τους οποίους οι άνθρωποι πέφτουν θύματα σε επιθέσεις phishing

Χρήση κινητών τηλεφώνων αφής

Οι άνθρωποι κατά την ενασχόλησή τους με τον κυβερνοχώρο χρησιμοποιούν τόσο τους επιτραπέζιους υπολογιστές όσο και τα κινητά τους τηλέφωνα. Όμως, τα περισσότερα θύματα «phishing» εξαπατώνται κατά τη διάρκεια χρήσης των κινητών τηλεφώνων.

Τα τελευταία χρόνια τα κινητά αφής έχουν γίνει κυρίαρχα στις αγορές τηλεφώνων. Όμως, οι χρήστες των κινητών, ειδικά όσοι είναι μεγαλύτερης ηλικίας τους φαίνεται δυσκολότερο να πληκτρολογούν στο εικονικό πληκτρολόγιο του κινητού από ότι στο φυσικό πληκτρολόγιο ενός υπολογιστή (Longfei et al., 2014). Αυτό είναι εντονότερο όταν ο χρήστης του κινητού οδηγεί ή περπατάει στο δρόμο (Longfei et al., 2014). Για αυτό το λόγο, οι χρήστες των κινητών δελεάζονται να πατήσουν στο link μιας ιστοσελίδας ή ενός email παρά να το πληκτρολογήσουν, ειδικά όταν συναντούν επείγουσες λέξεις που τους προκαλούν άγχος (Longfei et al., 2014). Ακόμη, αν οι χρήστες δέχονται συνήθως νόμιμα email και συνδέσμους που τους προτρέπουν να χρησιμοποιήσουν τα προσωπικά τους στοιχεία, όταν λάβουν ένα «phishing email» θα παραβλέψουν να ελέγξουν την αξιοπιστία του email και από συνήθεια θα εισάγουν τα προσωπικά τους στοιχεία με αποτέλεσμα να πέσουν θύματα «phishing» (Longfei et al., 2014).

Ακόμη, η εξαπάτηση των χρηστών μέσω διαδικτύου είναι πιο αποτελεσματική μέσω του κινητού τηλεφώνου, επειδή οι «phishers» εκμεταλλεύονται μεταξύ άλλων τη μικρή έκταση της οθόνης του κινητού τους (Longfei et al., 2014; Longfei et al., 2016). Αναλυτικότερα, όσον αφορά τις ιστοσελίδες για κινητά τηλέφωνα παρατηρείται ότι διαφέρουν από αυτές που είναι για τους υπολογιστές όσον αφορά το περιεχόμενο, τη διάταξη και τη λειτουργικότητά τους (Longfei et al., 2014). Έτσι, λοιπόν, όταν ένας χρήστης του διαδικτύου συνδεθεί μέσω κινητού σε μια ιστοσελίδα παρατηρείται σύντμηση της διεύθυνσης URL αποκρύπτοντας σημαντικές πληροφορίες. Για παράδειγμα, όταν κάποιος θέλει να συνδεθεί στην ιστοσελίδα «Bank of America» και

συνδέεται μέσω κινητού τηλεφώνου αντικρίζει τη περικομμένη διεύθυνση URL “Bank of America” και ενώ εκ πρώτης όψεως μοιάζει γνήσια μπορεί στη πραγματικότητα να μην είναι. Έτσι, αν η πλήρης διεύθυνση URL είναι https://secure.bankofamerica.com.phishing.com, ο χρήστης του κινητού τηλεφώνου, δεδομένου ότι την βλέπει περικομμένη, αν δε κάνει χειροκίνητη κύλιση μέχρι το τέλος της διεύθυνσης URL θα παραπλανηθεί από την ομοιότητα του πλαστού με τον γνήσιο ιστότοπο και θα έχει πέσει θύμα επίθεσης «phishing» (Longfei et al., 2014; Longfei et al., 2016).

Άγχος

Οι άνθρωποι πέφτουν θύματα σε επιθέσεις «phishing», εξαιτίας του άγχους που τους προκαλούν τα μηνύματα αυτά όταν τα διαβάζουν. Πολλοί άνθρωποι πέφτουν θύματα σε τέτοιου είδους επιθέσεις, επειδή δε γνωρίζουν ποιους πρέπει να εμπιστεύονται και ποιους όχι στο διαδίκτυο. Έτσι, όταν λάβουν ένα μήνυμα που αποτελεί επίθεση «phishing», δε μπορούν να διαχωρίσουν το αν είναι όντως μήνυμα απάτης ή πρέπει να κάνουν όσα τους λέει για να προστατευτούν. Σύμφωνα με ψυχολογικές μελέτες, φαίνεται πως όταν ένας χρήστης κυριεύεται από άγχος δεν είναι ικανός να σκεφτεί τις εναλλακτικές επιλογές που του δίνονται, αλλά λαμβάνει επιπόλαιες αποφάσεις. Για παράδειγμα, μια στρεσογόνα κατάσταση είναι η είσοδος στο ηλεκτρονικό ταχυδρομείο εν ώρα εργασίας, διότι ο παραλήπτης του email βλέποντας τη στιγμή εκείνη, φράσεις με επείγουσες λέξεις, πράττει χωρίς δεύτερη σκέψη, με αποτέλεσμα να πέφτει θύμα σε επιθέσεις «phishing» (Sharevski & Jachim, 2022). Ακόμη, οι «phishers» εκμεταλλευόμενοι το άγχος που προκαλούν επίκαιρα γεγονότα στα μέλη της κοινωνία όπως για παράδειγμα είναι η πανδημία του COVID-19 δημιουργούσαν email τα οποία θα ενημέρωναν τους παραλήπτες για μέτρα προστασίας κατά αυτού. Στη πραγματικότητα, όμως, θα τους εξαπατούσαν (Sharevski & Jachim, 2022).

Έλλειψη γνώσης

Οι άνθρωποι πέφτουν θύματα σε επιθέσεις «phishing» λόγω της ελλιπούς γνώσης τους σχετικά με τον τρόπο λειτουργίας του «phishing» και των κινδύνων που ενέχει. Παρακάτω αναλύονται δύο από τις ομάδες ανθρώπων στις οποίες επικεντρώνονται οι «phishers» για να εξαπατήσουν.

Αρχικά, οι κυβερνοεγκληματίες στοχεύουν στην εξαπάτηση των ηλικιωμένων (Alwanain, 2020). Οι «phishers» εκμεταλλεύονται τους ηλικιωμένους, επειδή δεν γνωρίζουν ότι τα προσωπικά τους δεδομένα μπορούν να στοχοποιηθούν στο διαδίκτυο και να κλαπούν (Alwanain, 2020; Longfei et al., 2014). Επίσης, τα υψηλά όρια ανάληψης που έχουν συνήθως οι ηλικιωμένοι στις πιστωτικές τους κάρτες σε συνδυασμό με την άγνοια που έχουν σχετικά με τους αρμόδιους που πρέπει να απευθυνθούν σε περίπτωση επίθεσης «phishing», τους καθιστούν εύκολο «στόχο» για τους «phishers» (Alwanain, 2020). Αν και οι ηλικιωμένοι έχουν συστήματα ασφαλείας κατά του «phishing» η ελλιπής γνώση για στοιχειώδη πράγματα σχετικά με τις ενδείξεις του υπολογιστή που χρησιμοποιούνται για την ασφάλειά τους έχει ως αποτέλεσμα την εξαπάτηση τους από την ομάδα των «phishers» (Alwanain, 2020).

Επιπρόσθετα, η ελλιπής γνώση σε κάποια τεχνικά θέματα ορισμένες φορές χαρακτηρίζει τους χρήστες που είναι μέλη ενός οργανισμού. Αυτό έχει ως αποτέλεσμα οι «phishers» να προσποιούνται κάποιον «ειδικό» και να ευνοούνται με την άντληση πληροφοριών και χρηματικών ποσών. Για παράδειγμα, όταν το μέλος ενός οργανισμού αντιμετωπίζει κάποιο πρόβλημα και πρέπει να επικοινωνήσει με κάποιον «ειδικό» για την αντιμετώπισή του, συνήθως τον εμπιστεύεται και ακολουθεί βήμα-βήμα όσα του λέει πέφτοντας θύμα επίθεσης «phishing» (Alwanain, 2020).

Οπτική εξαπάτηση

Οι κυβερνοεγκληματίες χρησιμοποιούν στα «phishing email» τους οπτικά παραπλανητικό κείμενο, όπως για παράδειγμα η αντικατάσταση του «l» με το «1» στη λέξη «paypal» και παραπλανητικές εικόνες και λογότυπα, όπως είναι το λογότυπο της εθνικής τράπεζας «NBG» (Dhamija et al., 2006).

Τρόποι Αντιμετώπισης

Αρχικά, ο χρήστης μπορεί να προστατευθεί από τα μηνύματα ηλεκτρονικού ψαρέματος θέτοντας μια σειρά ερωτήσεων στον εαυτό του. Σε κάθε ερώτηση ο χρήστης θα πρέπει να απαντάει με «Ναι» ή «Όχι» και να πράττει ανάλογα μέχρι να φτάσει στη τελευταία (Goel & Jain, 2017).

Η πρώτη ερώτηση η οποία καλείται να απαντήσει είναι, «*αν ο αποστολέας του email, ζητάει από αυτόν προσωπικές ή ευαίσθητες πληροφορίες*». Δεύτερη ερώτηση είναι «*αν ο σύνδεσμος που αναγράφεται στο email ενδέχεται να μη παραπέμπει εκεί που θα έπρεπε*». Στην περίπτωση αυτή ο χρήστης, πρέπει να παρατηρήσει, μεταξύ άλλων, αν ο υπερ-σύνδεσμος γράφει ορθά τον ιστότοπο που θα παραπεμφθεί, αν αυτός ξεκινάει με το «https» και αν υπάρχουν αριθμοί που στρεβλώνουν τον σύνδεσμο. Τρίτη ερώτηση είναι «*αν εντοπίζονται επείγουσες λέξεις στο email*» και τέταρτη, «*αν ο αποστολέας του e-mail χρησιμοποιεί γενικό χαιρετισμό», όπως για παράδειγμα «Αγαπητέ πελάτη»*. Πέμπτη ερώτηση που καλείται να απαντήσει ο χρήστης είναι «*αν το email αποτελείται απλά από μία εικόνα*». Ως έκτη και τελευταία ερώτηση ο χρήστης πρέπει να ρωτήσει τον εαυτό του «*αν γνωρίζει τον αποστολέα του email»*. (Goel & Jain, 2017)

Στις παραπάνω ερωτήσεις, αν η απάντηση είναι «ναι», ο χρήστης θα πρέπει τότε να παρατηρήσει «*αν υπάρχουν γραμματικά ή συντακτικά λάθη στο email»* και αν η απάντηση είναι «όχι» ο χρήστης περνά στην επόμενη ερώτηση, όπου και θα πρέπει να σκεφτεί ξανά την απάντηση για αυτήν. Στην περίπτωση που στο email εντοπίζονται γραμματικά ή συντακτικά λάθη τότε υπάρχει μεγάλη πιθανότητα το email να αποτελεί επίθεση «phishing». Διαφορετικά, υπάρχει μεσαίος κίνδυνος το email να προέρχεται από κάποιον «phisher». Αν η απάντηση είναι όχι και αφού ο χρήστης έχει απαντήσει με «όχι» και σε όλες τις παραπάνω ερωτήσεις, το email έχει ισχυρές ενδείξεις ασφάλειας και ο χρήστης μπορεί να προβεί στις ενέργειες που αναγράφονται σε αυτό (Goel & Jain, 2017).

Στοιχεία που συμβάλλουν στην ανίχνευση ιστοσελίδων «phishing»

Οι επιθέσεις «phishing» μέσω ιστότοπου, τις οποίες οργανώνουν οι «phishers», έχουν ως στόχο τους ίδιους τους χρήστες του διαδικτύου και όχι τα συστήματα. Ειδικότερα, στις επιθέσεις αυτές η δημιουργία των ιστοτόπων είναι εύκολη, ωστόσο η αναγνώριση ενός «phishing ιστοτόπου» είναι δύσκολη, εξαιτίας της μεγάλης ταύτισης που υπάρχει μεταξύ του νόμιμου και του πλαστού ιστοτόπου. Κάποιοι τρόποι οι οποίοι συμβάλλουν στην ανίχνευση τέτοιου είδους ιστοσελίδων είναι η ανίχνευση βάσει χαρακτηριστικών, μέσω KAYO, μαύρων και λευκών λιστών.

Ανίχνευση βάσει χαρακτηριστικών

Η ανίχνευση ιστοσελίδων phishing γίνεται ανάλογα με τα χαρακτηριστικά τους και είναι μία ιδέα που πρότειναν οι Tripanthi και Gangwani (2017). Αρχικά, η ιδέα αυτή κάνει χρήση του εργαλείου Optical Character Recognition (OCR), το οποίο μετατρέπει το στιγμιότυπο της οθόνης σε ιστοσελίδα κειμένου. Κάθε φορά που ένας χρήστης διαδικτύου εισάγει το μονοπάτι/διεύθυνση URL, το σύστημα κάνει ανάλυση του κώδικα HTML, το περιεχόμενο JavaScript και προσπαθεί να ελέγξει την ορθότητα του ιστότοπου. Έπειτα, γίνεται έλεγχος του τομέα δεύτερου επιπέδου. Αν ο τομέας αυτός υπάρχει στο κείμενο, το οποίο προκύπτει από την μετατροπή του στιγμιότυπου οθόνης σε κείμενο, τότε η ιστοσελίδα είναι νόμιμη. Η τεχνική αυτή συμβάλει στον ακριβέστερο διαχωρισμό των ιστοσελίδων.

KAYO

Το KAYO είναι μία επέκταση προγράμματος περιήγησης το οποίο σχεδιάστηκε από τους Amrutkar et al. (2017). Το KAYO είναι υπεύθυνο να ανιχνεύει κακόβουλες κινητές ιστοσελίδες (Amrutkar et al., 2017). Πιο συγκεκριμένα, το KAYO δραστηριοποιείται στο διαχωρισμό των ιστοσελίδων που έχουν σχεδιαστεί με ειδικές προδιαγραφές για να είναι λειτουργικές όταν προβάλλονται από τις κινητές συσκευές σε γνήσιες ή «phishing» (Amrutkar et al., 2017). Αρχικά, ο χρήστης του διαδικτύου εισάγει τη διεύθυνση URL που θέλει να ελέγξει στη γραμμή εργαλείων επέκτασης και με τη σειρά της αυτή στέλνει το URL μέσω Hyper Text Transfer Protocol Secure (HTTPS) στον διακομιστή υποστήριξης KAYO (Amrutkar et al., 2017). Ο διακομιστής υποστήριξης KAYO εντοπίζει το μονοπάτι URL και αφού το διαχωρίσει σε γνήσια ή «phishing» ιστοσελίδα την στέλνει στο πρόγραμμα περιήγησης που χρησιμοποιεί ο χρήστης (Amrutkar et al., 2017). Αν η διεύθυνση URL είναι γνήσια τότε εμφανίζεται η ιστοσελίδα στο πρόγραμμα περιήγησης αυτόματα, διαφορετικά εμφανίζει προειδοποιητικό μήνυμα. Ο διακομιστής υποστήριξης KAYO προσφέρει 90% ακρίβεια στον διαχωρισμό της ιστοσελίδας σε καλό ή κακόβουλο (Amrutkar et al., 2017). Το ποσοστό να είναι σωστό το αποτέλεσμα, δηλαδή να είναι γνήσια η ιστοσελίδα ή «phishing» είναι 89%, ενώ το ποσοστό λανθασμένου διαχωρισμού, δηλαδή να χαρακτηρίσει μια διεύθυνση URL ως «phishing» ενώ είναι γνήσια αγγίζει το ποσοστό του 8% (Amrutkar et al., 2017). Τέλος, η τεχνική αυτή είναι αξιόπιστη και ταχεία, εντοπίζοντας νέες απειλές που η ασφαλής περιήγηση της Google δεν εντοπίζει (Amrutkar et al., 2017).

Μαύρη λίστα

Η μαύρη λίστα αποτελείται από ύποπτες διαφημίσεις, διευθύνσεις IP, διευθύνσεις URL και λέξεις κλειδιά. Η μαύρη λίστα ελέγχει τη διεύθυνση URL και τη χαρακτηρίζει ως πλαστή ή νόμιμη. Για παράδειγμα αν μια διεύθυνση URL χαρακτηριστεί ως πλαστή αυτό σημαίνει ότι χρησιμοποιείται από «phishers» με σκοπό να κλέψουν τις προσωπικές πληροφορίες των χρηστών του διαδικτύου. Για να μπορούν να εντοπιστούν οι διευθύνσεις «phishing» και IP, αυτές πρέπει να είναι καταχωρημένες στη λίστα. Αυτό βέβαια προϋποθέτει ότι η μαύρη λίστα θα πρέπει να ανανεώνεται σε τακτά χρονικά διαστήματα (Goel & Jain, 2017)

Η ανανέωση της μαύρης λίστας γίνεται είτε χειροκίνητα είτε αυτόματα από κάποιο σύστημα. Όταν η ανανέωση της λίστας γίνεται χειροκίνητα, οι χρήστες του διαδικτύου καταγράφουν τη «phishing διεύθυνση» που εντόπισαν σε μία βάση δεδομένων όπως είναι το «PhishTank» (Whittaker et al., 2010). Δεδομένου ότι πολλές από τις «phishing» σελίδες ενδέχεται να παραμείνουν ενεργές λιγότερο από μια μέρα, μία μικρή καθυστέρηση ανανέωσης της λίστας από έναν χρήστη του διαδικτύου μπορεί να καταστήσει τη μαύρη λίστα αναποτελεσματική (Whittaker et al., 2010). Από την άλλη μεριά, όταν η ενημέρωση της μαύρης λίστας γίνεται αυτόματα από κάποιο σύστημα έχει υψηλότερη ακρίβεια ανίχνευσης επιθέσεων ηλεκτρονικού ψαρέματος επειδή ανανεώνει γρηγορότερα από το περιεχόμενο των βάσεων δεδομένων της μαύρης λίστας από το χειροκίνητο τρόπο (Goel & Jain, 2017; Whittaker et al., 2010). Το αρνητικό της μαύρης λίστας είναι ότι δεν μπορεί να εντοπίσει τις επιθέσεις «phishing» μηδενικής ημέρας και κατά μέσο όρο ανιχνεύει το 20% αυτών (Goel & Jain, 2017). Η μαύρη λίστα χρησιμοποιείται από το Chrome, την αναζήτηση Google και το Gmail (Goel & Jain, 2017).

Επιθέσεις phishing μηδενικής ημέρας

Ένα ζήτημα μείζονος σημασίας είναι η ανίχνευση και η αποτροπή του «phishing» μηδενικής ημέρας. Με τον όρο «phishing» μηδενικής ημέρας, αναφερόμαστε σε επιθέσεις που δεν έχουν ξανά εμφανιστεί στο παρελθόν και οι τακτικές που έχουν ανακαλυφθεί μέχρι στιγμής από τους επιστήμονες δεν μπορούν να τις σταματήσουν. Σε αυτή την επίθεση οι «phishers» παρατηρούν τους τρόπους αντιμετώπισης των επιθέσεων «phishing» που προτείνουν οι επιστήμονες και μόλις εντοπίσουν το τρωτό σημείο της πρότασης αυτής συνθέτουν μια νέα επίθεση μηδενικής ημέρας (Bu & Cho, 2021). Το κύριο μειονέκτημα των επιθέσεων «phishing» μηδενικής ημέρας είναι ότι οι διευθύνσεις URL δημιουργούνται και σβήνονται μόλις επιτύχουν το στόχο τους οι «phishers» ή μόλις «πάνε να γίνουν αντιληπτή» από τους επιστήμονες. Για παράδειγμα μια «phishing» ιστοσελίδα διαγράφεται όταν κλαπούν οι πληροφορίες που θέλουν να συλλέξουν οι «phishers» για τα θύματά τους (Bu & Cho, 2021). Οι επιθέσεις μηδενικής ημέρας ενδέχεται να επιφέρουν εγκατάσταση κακόβουλου λογισμικού, spyware ή ανεπιθύμητη πρόσβαση στα προσωπικά δεδομένα του χρήστη (Bu & Cho, 2021).

Λευκή λίστα

Η λευκή λίστα αποτελείται από ένα κατάλογο νόμιμων και αξιόπιστων διευθύνσεων URL, οι οποίες έχουν ελεγχθεί μέσω του LUI (Login User Interfaces) (Khonji et al., 2013). Κάθε φορά που ένας χρήστης του διαδικτύου εισάγει τα διαπιστευτήριά του σε μία από τις ιστοσελίδες που βρίσκονται στη λευκή λίστα, το σύστημα δεν εμφανίζει κάποια προειδοποίηση και του επιτρέπει να συνεχίσει. Ωστόσο, αν ο χρήστης του διαδικτύου συμπληρώσει προσωπικά δεδομένα σε κάποια ιστοσελίδα που δεν βρίσκεται στη λευκή λίστα, τότε το σύστημα θα διακόψει την περιήγηση και θα προειδοποιήσει τον χρήστη για την επίθεση «phishing» (Khonji et al., 2013). Συγκριτικά με τη μαύρη λίστα, η λευκή λίστα αποδείχθηκε καλύτερη, διότι ένας νόμιμος ιστότοπος είναι δύσκολο να αλλάξει URL. Τόσο η μαύρη λίστα όσο και η λευκή λίστα πρέπει να ενημερώνονται συχνά για να λειτουργούν ορθά και αποτελεσματικά (Khonji et al., 2013).

Προκειμένου να αντιμετωπιστούν οι επιθέσεις «phishing», οι ερευνητές έχουν δώσει πολλές λύσεις. Ωστόσο, δεν έχει βρεθεί ακόμα καμία λύση που να ανιχνεύσει ή να αποτρέπει όλες τις επιθέσεις «phishing». Κάθε φορά που οι ερευνητές ανακαλύπτουν μία νέα μέθοδο αντιμετώπισης ή πρόληψης των επιθέσεων ηλεκτρονικού εγκλήματος, οι «phishers» όχι μόνο τροποποιούν τη στρατηγική που ακολουθούν αλλά βρίσκουν και τρωτά σημεία στις ήδη υπάρχουσες λύσεις (Khonji et al., 2013).

Αντι-ικά προγράμματα προστασίας Antivirus

Το anti-virus (AV), το οποίο είναι γνωστό και ως anti-malware αποτελεί μηχανισμό άμυνας του υπολογιστή και προστατεύει τα προσωπικά στοιχεία του χρήστη. Το AV είναι υπεύθυνο για τον έλεγχο της συσκευής, όπως για παράδειγμα έλεγχος για ιούς και την προειδοποίηση του χρήστη σχετικά με κακόβουλες δραστηριότητες που διαδραματίζονται στη συσκευή του. Παρακάτω αναφέρονται τα πλεονεκτήματα και τα μειονεκτήματα του αντιικού προγράμματος προστασίας Antivirus (Boja & Visoiu, 2007).

Αφενός, το λογισμικό Antivirus ανιχνεύει και διαγράφει άμεσα το λογισμικό υποκλοπής Spyware, πριν προβεί στη κλοπή των προσωπικών στοιχείων του χρήστη. Το λογισμικό κατασκοπίας (Spyware) είναι ένα κακόβουλο λογισμικό, το οποίο παρακολουθεί αόρατα τις ενέργειες του χρήστη. Διανέμεται μέσω του ηλεκτρονικού ταχυδρομείου και όχι μόνο, συλλέγει αλλά και αποστέλλει τις πληροφορίες του χρήστη σε τρίτους χωρίς την έγκριση του (Tally et al., 2004). Πιο συγκεκριμένα, το anti-virus(AV) ή anti-malware βασίζεται στη σάρωση και τον έλεγχο γνησιότητας των αρχείων του υπολογιστή. Για την σάρωση, το anti-malware σαρώνει σε τακτά χρονικά διαστήματα τα αρχεία του υπολογιστή, χωρίς να του ζητηθεί, και αν παρατηρήσει κάτι ασυνήθιστο ενημερώνει τον χρήστη. Ακόμη, το πρόγραμμα προστασίας anti-virus μπορεί να ελέγξει τα αρχεία έπειτα από εντολή του ίδιου του χρήστη και να τον ενημερώσει την ίδια στιγμή για την υγεία της συσκευής του (Boja & Visoiu, 2007). Σε κάθε περίπτωση το λογισμικό ζητάει τη συγκατάθεση του χρήστη για την εκκαθάριση των αρχείων από τους ιούς. Όσον αφορά τον έλεγχο γνησιότητας, αποτελεί μέθοδο

βασισμένη στο γεγονός ότι ένα μολυσμένο αρχείο διαφέρει από το γνήσιο, αρχικό αρχείο. Η διαφορά δεν αφορά το όνομα του αρχείου, αλλά μεταξύ άλλων, αφορά την ημερομηνία, την ώρα, το μέγεθος του αρχείο. Μόλις γίνει η εγκατάσταση του, σαρώνονται όλα τα αρχεία του υπολογιστή και δημιουργείται μια βάση δεδομένων που απαρτίζεται από τις πληροφορίες των αρχείων (Boja & Visoiu, 2007). Έτσι, κάθε φορά που γίνεται έλεγχος των αρχείων συγκρίνονται οι πληροφορίες που είναι αποθηκευμένες στη βάση δεδομένων από τη τελευταία φορά που έγινε έλεγχος με τις πληροφορίες που εμφανίζονται στη βάση δεδομένων με τον τρέχον έλεγχο και αν εντοπιστεί διαφορά η εφαρμογή ενημερώνει τον χρήστη (Boja & Visoiu, 2007). Η μέθοδος αυτή ενισχύει την αποτελεσματικότητα του AV, διότι οι πληροφορίες των αρχείων που αποθηκεύονται στη βάση δεδομένων, όπως το μέγεθος αρχείου, δεν αλλάζουν κατά τη περίοδο εκτέλεσης του περιεχομένου τους (Boja & Visoiu, 2007).

Αφετέρου, το αντι-ικό πρόγραμμα προστασίας antivirus έχει τρωτά σημεία τα οποία μπορούν να εκμεταλλευτούν από τους «phishers» για να βλάψουν τους χρήστες του διαδικτύου. Ειδικότερα, οι «phishers» εκμεταλλευόμενοι το φόβο των χρηστών του διαδικτύου σχετικά με την διέρρευση των προσωπικών τους πληροφοριών καθώς και τη καταστροφή των σημαντικών τους αρχείων έχουν δημιουργήσει απομιμήσεις των γνήσιων λογισμικών antivirus. Τα ψεύτικα antivirus υπόσχονται τη σάρωση και προστασία των συστημάτων του χρήστη από ιούς με σκοπό να τους πείσει να αγοράσουν το λογισμικό. Προκειμένου να πείσουν τους χρήστες ότι πωλούν ένα γνήσιο λογισμικό προσφέρουν και επιστροφή χρημάτων. Για αυτό οι αγοραστές θα πρέπει να είναι πολύ προσεκτικοί όταν αγοράζουν ένα αντι-ικό πρόγραμμα προστασίας (Stone-Gross et al., 2013). Επιπλέον, για να μην έχει ψευδή αποτελέσματα το λογισμικό Antivirus τα αρχεία που σαρώνει στα email του χρήστη θα πρέπει να ενημερώνονται συχνά. Τέλος, ο χρήστης έρχεται αντιμέτωπος με το κόστος του λογισμικού, αφού πρέπει να αγοράσει και να εγκαταστήσει το λογισμικό Antivirus στον υπολογιστή του. Βέβαια, είναι πρόδηλο πως οι νεότερες, επί πληρωμή εκδόσεις Antivirus είναι αποτελεσματικότερες από τις παλιότερες, δωρεάν (Tally et al., 2004).

Φιλτράρισμα των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail filtering)

Χαρακτηριστικά ενός Email

Ένα μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail), αποτελείται από δύο βασικά χαρακτηριστικά, την «κεφαλίδα» και το «κυρίως σώμα». Στην «κεφαλίδα» εντοπίζονται το θέμα του μηνύματος που σχετίζεται με το περιεχόμενό του, ο αποστολέας και ο παραλήπτης του e-mail (Dada et al., 2019). Το κυρίως μέρος του μηνύματος εντοπίζεται στο «κυρίως σώμα», το οποίο δεν έχει δεδομένα προκαθορισμένου τύπου, αλλά μπορεί να περιέχει είτε ένα απλό κείμενο, είτε ένα βίντεο, είτε μια εικόνα, άλλα και συνδυασμό αυτών (Dada et al., 2019).
Η ανάπτυξη της τεχνολογίας των μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), είναι καθοριστική και έχει σημαντική συμβολή στην επικοινωνία των ανθρώπων από απόσταση μέσω της ανταλλαγής τέτοιων μηνυμάτων, ειδικά για μηνύματα, τα οποία έχουν πιο επίσημο χαρακτήρα και ενημερωτική δράση (Gangavarapu et al., 2020). Τα παραπάνω συντέλεσαν στο να είναι μεγάλος ο αριθμός μηνυμάτων ηλεκτρονικού

ταχυδρομείου που ανταλλάσσεται καθημερινά μεταξύ των ανθρώπων, ωστόσο έχει παρατηρηθεί ότι μεγάλος όγκος αυτών των μηνυμάτων είναι ανεπιθύμητα μαζικής προώθησης e-mail (spam) (Gangavarapu et al., 2020). Τα e-mail που ανήκουν στην spam αλληλογραφία, απειλούν την ανθρώπινη ασφάλεια και την οικονομία, με χαρακτηριστικό παράδειγμα τέτοιων μηνυμάτων να είναι τα μηνύματα ηλεκτρονικού ψαρέματος (Gangavarapu et al., 2020). Αυτά, αποθηκεύουν τα προσωπικά δεδομένα των χρηστών μέσω παραπλάνησής τους με σκοπό να αποσπάσουν χρήματα από το θύμα (Gangavarapu et al., 2020). Σύμφωνα με όλα τα παραπάνω είναι αναγκαίο να θεσπιστούν και να εφαρμοστούν φίλτρα που να ανιχνεύουν αυτόματα τα ανεπιθύμητα μαζικής προώθησης e-mail (spam) (Gangavarapu et al., 2020).

Spam email filtering;

Το «spam email filtering» είναι φίλτρο το οποίο είναι υπεύθυνο για την ανίχνευση μηνυμάτων ανεπιθύμητης αλληλογραφίας και για την αποτροπή παράδοσής τους στον χρήστη (Puertas Sanz, et al., 2008). Τα μηνύματα ανεπιθύμητης αλληλογραφίας είναι γνωστά και ως «σκουπίδια email» ή «μαζικά email» ή «ανεπιθύμητα εμπορικά email» αλλά ο πιο διαδεδομένος όρος που χρησιμοποιείται για αυτά είναι το «spam» (Cormack, 2008). Μερικές από τις ιδιότητες των «spam» που συμβάλλουν στην ανίχνευσή τους είναι όχι μόνο ότι στέλνεται σε μεγάλο αριθμό χρηστών του διαδικτύου αλλά και η ταυτότητα του αποστολέα είναι άγνωστη προς τον παραλήπτη αφού συνήθως στέλνονται «spam» προς αυτόν χωρίς να το έχει ζητήσει.

Το e-mail filtering έχει την ιδιότητα να δημιουργεί «φάκελο καραντίνας», όπου παραθέτει τα ύποπτα μηνύματα. Ο χρήστης, στη συνέχεια έχει πρόσβαση στη σύνοψη των μηνυμάτων αυτών, πράγμα που σημαίνει ότι βλέπει μόνο τα πεδία, «προς», «από», «θέμα» και ενδεχομένως μια έως δύο γραμμές από το «κυρίως σώμα» του μηνύματος, ώστε να μπορεί ο παραλήπτης να διαχωρίσει το νόμιμο από το ψεύτικο μήνυμα. (Dada et al., 2019) Συνεπώς, τα φίλτρα όταν εντοπίζουν ανεπιθύμητο περιεχόμενο αποτρέπουν την παράδοσή του στον χρήστη, προστατεύοντας τον. Βέβαια, για το λόγο ότι οι «spammers» προσπαθούν να βρίσκουν συνεχώς τρόπους για να παρακάμπτουν τον έλεγχο που εκτελεί το spam email filtering ενδέχεται να παραδοθούν τελικά στον χρήστη (Cormack, 2008)

Κατηγορίες τεχνικών φιλτραρίσματος ανεπιθύμητων μηνυμάτων

Φιλτράρισμα βάσει περιεχομένου.

Μέσα από το φιλτράρισμα βάσει περιεχομένου δημιουργούνται κανόνες αυτόματου φιλτραρίσματος και ταξινομούνται τα μηνύματα ηλεκτρονικού ταχυδρομείου σε νόμιμα και παράνομα. Αυτή η τεχνική, εξετάζει τις λέξεις, την εμφάνιση και την κατανομή των λέξεων και φράσεων που αναγράφονται στο περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου (Dada et al., 2019).

Φιλτράρισμα βάσει περιπτώσεων

Το φιλτράρισμα βάσει περιπτώσεων αποτελεί τεχνική φιλτραρίσματος ανεπιθύμητων μηνυμάτων (spam), κατά την οποία, τόσο τα επιθυμητά όσο και τα μη επιθυμητά μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν το ίδιο μοντέλο

συλλογής πριν αποσταλούν σε κάποιον χρήστη. Έπειτα, τα μηνύματα ηλεκτρονικού ταχυδρομείου περνούν από το στάδιο της προεπεξεργασίας και της επιλογής χαρακτηριστικών και τέλος με τη βοήθεια ενός αλγορίθμου μηχανικής εκμάθησης διαχωρίζονται σε επιθυμητά και ανεπιθύμητα μηνύματα (Dada et al., 2019).

Φιλτράρισμα βάσει κανόνων.

Το φιλτράρισμα βάσει κανόνων αξιολογεί πλήθος μοτίβων, τα οποία αποτελούνται συνήθως από εκφράσεις έναντι ενός συγκεκριμένου μηνύματος χρησιμοποιώντας ήδη υπάρχοντες κανόνες. Όσο μεγαλύτερη ομοιότητα συναντάμε ανάμεσα στα μοτίβο και στο μήνυμα, τόσο αυξάνεται η βαθμολογία του μηνύματος. Ενώ, αν δεν υπάρχει ομοιότητα ανάμεσα στο e-mail και τα μοτίβα παρατηρείται αφαίρεση βαθμολογίας (Dada et al., 2019). Όταν η βαθμολογία του μηνύματος υπερβαίνει ένα συγκεκριμένο όριο, το μήνυμα φιλτράρεται ως ανεπιθύμητο, διαφορετικά θεωρείται νόμιμο. Για την αποτελεσματικότερη ανίχνευση των spam κάποιοι κανόνες χρίζουν συνεχή ενημέρωση, ενώ άλλοι παραμένουν αξιόπιστοι χωρίς να χρειάζονται ανανέωση. Χαρακτηριστικό παράδειγμα φίλτρου ανεπιθύμητης αλληλογραφίας αποτελεί το SpamAssassin το οποίο χρησιμοποιεί κανόνες (Dada et al., 2019).

Φιλτράρισμα βάσει προηγούμενης ομοιότητας.

Το φιλτράρισμα βάσει προηγούμενης ομοιότητας ταξινομεί τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου κάνοντας χρήση των τεχνικών μηχανικής εκμάθησης, η οποία στηρίζεται στην ανάλυση και επεξεργασία προηγούμενων παραδειγμάτων (Dada et al., 2019). Πιο συγκεκριμένα, ένας τρόπος ταξινόμησης του μηνύματος είναι βάσει της ομοιότητάς του με ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προέρχεται από έναν εκπαιδευτικό, όπως για παράδειγμα είναι οι καθηγητές, λόγω του εκπαιδευτικού του περιεχομένου που το καθιστά χρήσιμο και έγκυρο (Dada et al., 2019).

Πως λειτουργούν τα φίλτρα ανεπιθύμητης αλληλογραφίας Gmail και Yahoo;

Τα φίλτρα ανεπιθύμητης αλληλογραφίας Gmail και Yahoo έχουν ως σκοπό να παραδίδουν μόνο τα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου στους χρήστες και να φιλτράρουν τα παράνομα (Dada et al., 2019). Αν και χρησιμοποιούνται διάφοροι τύποι φιλτραρίσματος για την επίτευξη του σκοπού του, ορισμένες φορές αποκλείονται λανθασμένα τα έγκυρα μηνύματα. Έχει παρατηρηθεί ότι περίπου το 20 τοις εκατό των μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται από έγκυρη πηγή δεν φτάνουν στον τελικό χρήστη (Dada et al., 2019).

Φιλτράρισμα ανεπιθύμητης αλληλογραφίας από το Gmail

Για την ταξινόμηση του e-mail σε νόμιμο ή spam, τα κέντρα δεδομένων της Google χρησιμοποιούν πλήθος κανόνων. Κάθε κανόνας περιέχει συγκεκριμένα χαρακτηριστικά ανεπιθύμητου περιεχομένου και ανάλογα με τη βαθμολογία που θα συγκεντρώσει το email χαρακτηρίζεται ως έγκυρο ή ανεπιθύμητο (Dada et al., 2019). Ακόμη, η Google κάνει χρήση υπερσύγχρονων αλγορίθμων μηχανικής εκμάθησης για να εντοπίζει τα spam, όπως για παράδειγμα είναι τα νευρωνικά δίκτυα τα οποία χρησιμοποιούνται στην εύρεση χαρακτηριστικών που παραπέμπουν σε ιστοσελίδες

«phishing» (Jakobsson, 2018; Dada et al., 2019). Επιπρόσθετα, το Gmail για να προστατεύσει τον χρήστη κάνει χρήση της οπτικής αναγνώρισης χαρακτήρων (OCR) (Jakobsson, 2018). Για τον λόγο ότι η φύση των ανεπιθύμητων μηνυμάτων εξελίσσεται συνεχώς, μέθοδοι όπως η φήμη του τομέα, δηλαδή φήμη που βασίζεται στο καλό ή κακό ιστορικό του αποστολέα και οι σύνδεσμοι στις κεφαλίδες των email, δηλαδή η διεύθυνση IP του αποστολέα, οι οποίοι δεν είναι ορατοί στους παραλήπτες μπορεί να οδηγήσουν ένα νόμιμο email στο φάκελο με τα ανεπιθύμητα (Jakobsson, 2018).

Αυτό συμβαίνει επειδή όταν ο λογαριασμός του αποστολέα είναι νέος και δεν υπάρχει καλό ιστορικό που να τον συνδέει με επιθυμητή αλληλογραφία το φίλτρο βασίζεται στο περιεχόμενο του email και το κατατάσσει στα ανεπιθύμητα (Jakobsson, 2018).

Φιλτράρισμα ανεπιθύμητης αλληλογραφίας από το Yahoo

Ο πρώτος δωρεάν παγκόσμιος πάροχος webmail είναι το Yahoo mail με περισσότερους από 320 εκατομμύρια χρήστες. Οι κύριες τεχνικές που χρησιμοποιεί για την ανίχνευση ανεπιθύμητων μηνυμάτων είναι το φιλτράρισμα URL, το περιεχόμενο του email και οι καταγγελίες ανεπιθύμητων μηνυμάτων από χρήστες. Μία βασική διαφορά που έχει από το Gmail είναι ότι τα μηνύματα του ηλεκτρονικού ταχυδρομείου δεν τα φιλτράρει κατά IP διεύθυνσης, αλλά κατά τομείς οι οποίοι είναι μοναδικοί για κάθε οργανισμό (Gangavarapu et al., 2020). Ακόμη, το Yahoo mail μέσα από ειδικούς μηχανισμούς αποτρέπει τον χαρακτηρισμό ενός έγκυρου χρήστη σε «spammer». Επιπλέον, παρέχει τη δυνατότητα στον χρήστη να καθορίσει μια λίστα αξιόπιστων χρηστών από τους οποίους θα λαμβάνει email, αποκλείοντας αυτόματα τους υπόλοιπους αποστολείς. Αυτό επιτυγχάνεται με την αξιοποίηση του λευκού πίνακα στον οποίο είναι εγγεγραμμένοι οι αξιόπιστοι χρήστες από τους οποίους ο χρήστης επιθυμεί να λαμβάνει μηνύματα και του μαύρου πίνακα που περιλαμβάνει τους μη αξιόπιστους χρήστες (Gangavarapu et al., 2020)

Πώς οι phishers εκμεταλλεύτηκαν την πανδημία του κορονοϊού;

Το πρώτο κρούσμα κορονοϊού εμφανίστηκε από τον κορονοϊό SARS-COV-2 στην πόλη Ουχάν, πρωτεύουσα της επαρχίας Χουπέι της Κίνας, τον Δεκέμβριο του 2020 και άρχισε να μεταδίδεται μεταξύ των ανθρώπων με γρήγορους ρυθμούς, ώσπου έγινε παγκόσμια απειλή και ανακηρύχθηκε ως πανδημία (Lau et al., 2020). Αυτό είχε ως αποτέλεσμα να παρθούν μέτρα για την προστασία των ανθρώπων από τον θανατηφόρο ιό. Ένα από τα αποτελεσματικά μέτρα που πήραν οι χώρες ήταν το lockdown κατά το οποίο έκλεισαν πολλά καταστήματα, εκπαιδευτικές δομές και χώροι λατρεία περιορίζοντας ακόμα και τις μετακινήσεις των πολιτών στις άκρως απαραίτητες (Lau et al., 2020).

Εκμεταλλευόμενοι τον ξαφνικό περιορισμό των ανθρώπων παγκοσμίως και την άγνοιά τους για τον νέο ιό, οι «phishers» άρχισαν να συντάσσουν «ψεύτικα» email με σκοπό να εξαπατήσουν τους ανθρώπους (Akdemir & Yenal, 2021). Για το λόγο ότι οι άνθρωποι ήθελαν να μάθουν περισσότερες πληροφορίες σχετικά με τον ιό και τους τρόπους με τους οποίους θα μπορούσαν να προστατευθούν από αυτόν παραμέριζαν

τους κινδύνους του διαδικτύου. Πολλοί χρήστες του διαδικτύου δεχόντουσαν «phishing email» και εξαιτίας της κοινωνικής μηχανικής που χρησιμοποιούσαν οι «phishers» (π.χ. λογότυπα του Παγκόσμιου Οργανισμού Υγείας) ακολουθούσαν τις ενέργειες που ήταν γραμμένες στο email (Akdemir & Yenal, 2021). Χαρακτηριστικό παράδειγμα αποτελούν τα email που ζητούσαν από τους χρήστες να δουν ή να κατεβάσουν συνημμένα έγγραφα προκειμένου να ενημερωθούν για τα μέτρα προστασίας που έχει ορίσει ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) για τον περιορισμό της εξάπλωσης του κορονοϊού (Akdemir & Yenal, 2021). Πιο συγκεκριμένα, μέσα σε μία βδομάδα τον Απρίλιο του 2020 ανιχνεύτηκαν περισσότερες από 18 εκατομμύρια επιθέσεις «phishing» σχετιζόμενες με πληροφορίες σχετικά με τον κορονοϊό και με κακόβουλο λογισμικό που κατέβαζαν οι αναγνώστες στις συσκευές τους (Akdemir & Yenal, 2021).

Κατά τη περίοδο του κορονοϊού παρατηρήθηκε αλλαγή στη τεχνική εξαπάτησης που χρησιμοποιούν οι «phishers» (Akdemir & Yenal, 2021). Πριν ξεσπάσει η πανδημία του κορονοϊού οι «phishers» προκειμένου να εξαπατήσουν ένα θύμα ζητούσαν από αυτό να κάνει κλικ σε ένα σύνδεσμο και στη συνέχεια να εισάγει στη πλατφόρμα τις προσωπικές του πληροφορίες (π.χ. κωδικούς πρόσβασης). Αντιθέτως, όταν ξέσπασε η πανδημία οι «phishers» προσάρμοσαν κατάλληλα τα email (προσποιούνταν ότι πρόσφεραν χρήσιμες οδηγίες σχετικά με τον κορονοϊό) και ζητούσαν από τα θύματα να ανοίξουν ή να κατεβάσουν κακόβουλα αρχεία για να τους βλάψουν (Akdemir & Yenal, 2021).

ΕΙΔΙΚΟ ΜΕΡΟΣ

Σκοπός

Σκοπός της παρούσας διπλωματικής εργασίας είναι να διερευνήσει τη συμπεριφορά των χρηστών του internet σε απόπειρες «phishing». Για την έρευνα αυτή, συντάχθηκε ένα ερωτηματολόγιο 18 ερωτήσεων το οποίο διανεμήθηκε μέσω των μέσων κοινωνικής δικτύωσης (Facebook, Instagram). Ειδικότερα, η διπλωματική αυτή εργασία είχε τους ακόλουθους ερευνητικούς στόχους:

1. Η ικανότητα των χρηστών του διαδικτύου να αναγνωρίσουν ένα «phishing email» που προέρχεται από τη «τράπεζα» επηρεάζεται από τα μέσα που υπάρχουν για να τους προστατέψουν από το «phishing»;

2. Η ικανότητα των χρηστών του διαδικτύου να αναγνωρίσουν μια «phishing» ιστοσελίδα που προέρχεται από τη «τράπεζα» επηρεάζεται από τα μέσα που υπάρχουν για να τους προστατέψουν από το «phishing»;

3. Παράγοντες που ωθούν τους χρήστες του διαδικτύου να κάνουν κλικ σε «phishing link» που προέρχονται από τη «τράπεζα».

Παρουσίαση ερωτηματολογίου

Το ερωτηματολόγιο απαρτίζεται από τρία μέρη και περιλαμβάνει 18 ερωτήσεις οι οποίες σχετίζονται με τη συμπεριφορά των χρηστών του internet σε απόπειρες «phishing». Στο πρώτο μέρος του ερωτηματολογίου γίνεται συλλογή όχι μόνο των προσωπικών πληροφοριών που σχηματίζουν τη ταυτότητα του κάθε συμμετέχοντα αλλά και ερωτήσεις που σχετίζονται με το χρόνο που αφιερώνει στο διαδίκτυο και τον αριθμό των μηνυμάτων email που δέχεται καθημερινά. Ακόμη, ο ερωτώμενος δηλώνει αν γνωρίζει πως να προστατευτεί από το «phishing» και υπάρχουν δύο ερωτήσεις στις οποίες καλείται να αναγνωρίσει αν η ιστοσελίδα της τράπεζας και το μήνυμα email που εκ πρώτης όψεως φαίνονται να προέρχονται από τράπεζα είναι γνήσια ή «phishing». Στη συνέχεια στο δεύτερο μέρος του ερωτηματολογίου υπάρχουν 4 ερωτήσεις που εξετάζουν αν οι χρήστες του internet μπορούν να αναγνωρίσουν αν ένα email που προέρχεται από τη τράπεζα είναι «phishing» καθώς και αν η ιστοσελίδα της τράπεζας που αντικρίζουν όταν συνδέονται στο τραπεζικό τους λογαριασμό είναι γνήσια ή «phishing». Ακόμη, υπάρχουν ερωτήσεις που ερευνούν τον βαθμό που επηρεάζουν τους συμμετέχοντες οι παράγοντες που ωθούν τους χρήστες του internet να κάνουν «κλικ» σε «phishing link» που προέρχονται από τη «τράπεζα» και τον βαθμό που τους φαίνονται αποτελεσματικοί ορισμένοι τρόποι αντιμετώπισης κατά του «phishing». Στο τρίτο, και τελευταίο μέρος, οι συμμετέχοντες καλούνται να απαντήσουν ερωτήσεις που σχετίζονται με τις ικανότητές τους να αξιολογούν έναν ιστότοπο ή ένα μήνυμα email ως προς την γνησιότητά του, ερωτήσεις που αναφέρονται στη συμβολή του κοινωνικού τους περιβάλλοντος ως προς την ενίσχυση της γνώσης τους για το «phishing» και τέλος υπάρχει μια ερώτηση για τη κατάλληλη ηλικία που θεωρεί ο κάθε ερωτώμενος κατάλληλη για να εκπαιδευτεί κάποιος για το «phishing».

ΑΠΟΤΕΛΕΣΜΑΤΑ

Αποτελέσματα στατιστικής ανάλυσης

Για την ανάλυση και τη στατιστική επεξεργασία των απαντήσεων χρησιμοποιήθηκαν δύο εργαλεία λογισμικού, το Microsoft Excel και το στατιστικό πακέτο SPSS (Statistical Package for Social Sciences). Συγκεκριμένα, χρησιμοποιήθηκε η έκδοση SPSS Statistics 28.0.0.0 (190). Με τη βοήθεια αυτών των εργαλείων, πραγματοποιήθηκε η επεξεργασία των δεδομένων από το ερωτηματολόγιο που συμπλήρωσαν οι 252 συμμετέχοντες στη μελέτη. Τα αποτελέσματα αναλύθηκαν στο SPSS για την παραγωγή στατιστικών συμπερασμάτων και την ερμηνεία των αποτελεσμάτων που προέκυψαν.

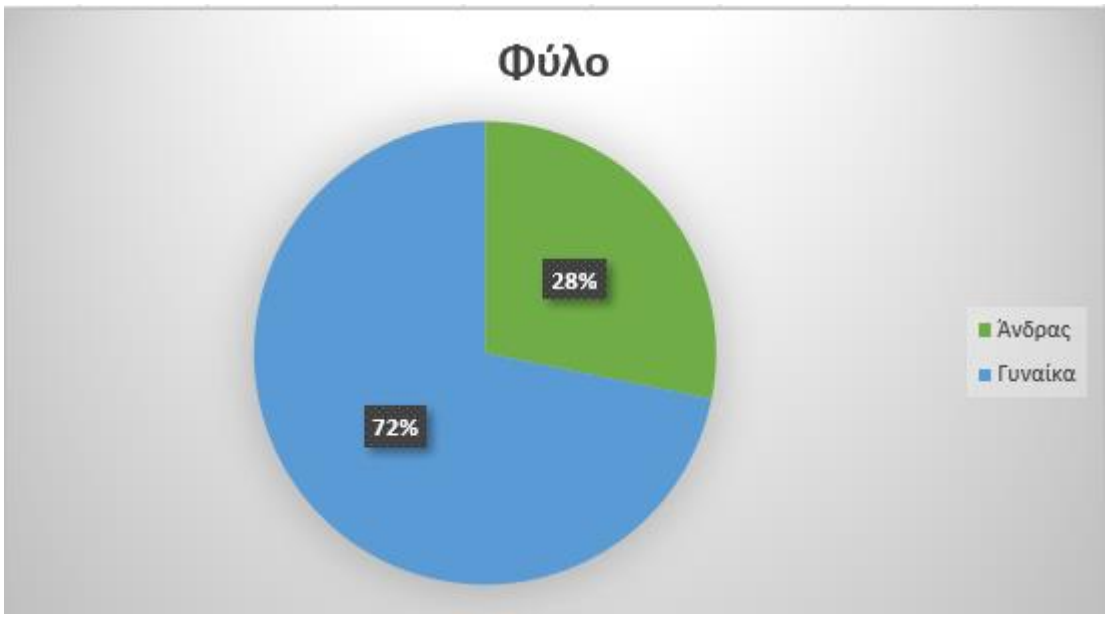
Στον παρακάτω πίνακα παρουσιάζονται οι ερωτήσεις του ερωτηματολογίου, που απαντήθηκαν από τους συμμετέχοντες στην έρευνα. Γίνεται περιγραφική στατιστική ανάλυση και έτσι, στον παρακάτω πίνακα (Πίνακας 1.) αναφέρεται η διάμεσος (Median), το ενδοτεταρτημοριακό εύρος (IQR: interquartile range) και η επικρατούσα τιμή (Mode) για μέγεθος του δείγματος (N) ίσο με 252 απαντήσεις για κάθε ερώτηση του ερωτηματολογίου μου.

Ερωτήσεις Ερωτηματολογίου	Median	IQR	Mode
1. Φύλο	1	1	1
2. Ηλικία	1	1.75	1
3. Ποιο είναι το ανώτερο επίπεδο εκπαίδευσης που έχετε ολοκληρώσει;	3	1	3
4. Ποια είναι η απασχόληση σας;	3	3	3
5. Πόσο χρόνο βρίσκεστε στο Ίντερνετ μέσω του υπολογιστή σας κάθε μέρα;	2	3	2
6. Πόσο χρόνο βρίσκεστε στο Ίντερνετ μέσω του κινητού τηλεφώνου σας κάθε μέρα;	4	3	4
7. Πόσα μηνύματα email λαμβάνετε κάθε μέρα;	2	2	2
8. Δέχεστε μηνύματα email από τη τράπεζά σας;	1.50	1	1
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	4	2	5
10. Περίπου τι ποσοστό από τα μηνύματα email που λαμβάνετε είναι phishing;	1	1	1
11. Θα βάζατε τους κωδικούς σας εδώ;	2	1	2
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	2	0	2
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. “ngb” αντί για “nbg”, “l” αντί για “I”)	4	4	1
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με “https”	5	4.75	7
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	6	4	7
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	6	3	7
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	5	4	7
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	4	4	2
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	5	4	7
14.3. Άγνωστος αποστολέας μηνύματος email	5	4.75	7
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	5	5	7
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	5	5	7
15.1. Εμπιστοσύνη στον αποστολέα του μηνύματος email (π.χ. όνομα τράπεζας)	5	4	7
15.2. Περιέργεια	3	3.75	1
15.3. Άγχος	3	4	1
15.4. Βιασύνη	3	4	1
15.5. Ελλιπής γνώση για προστασία από phishing	3	3.75	1

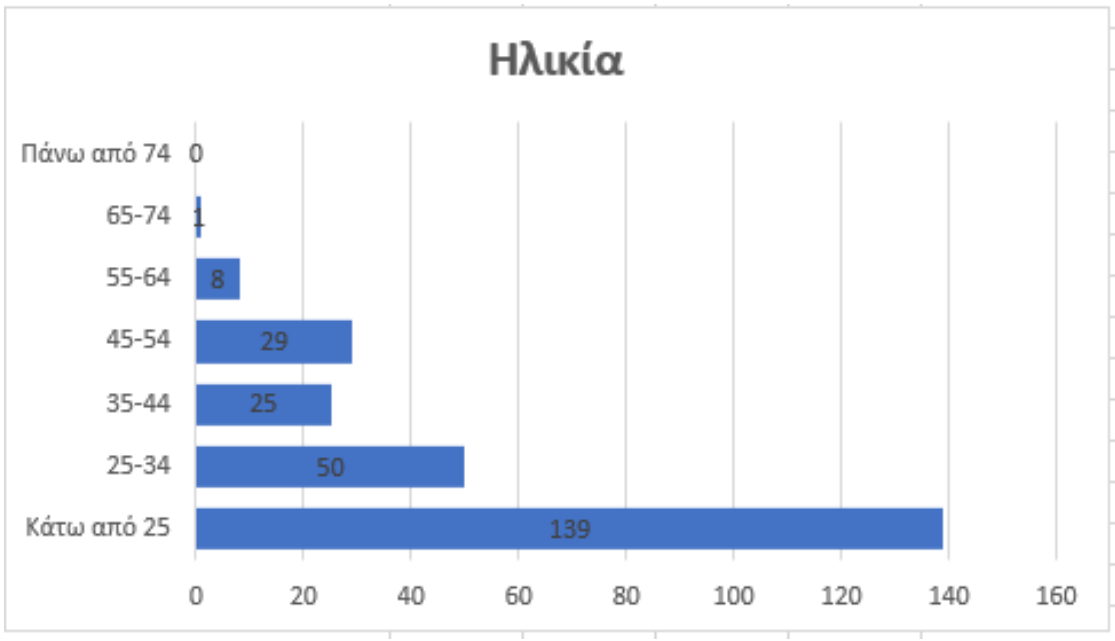
16.1. Δημιουργία Black list (με ύποπτες διευθύνσεις IP-URL, λέξεις-κλειδιά που χρησιμοποιούν οι phishers)	6	3	7
16.2. Δημιουργία White list (με νόμιμες-επίσημες διευθύνσεις URL τραπεζών κτλ.)	6	3	7
16.3. Εκπαίδευση στο σχολείο, πανεπιστήμιο, εργασία, κτλ.	6	2	7
16.4. Αυτό-εκπαίδευση από εφαρμογές (π.χ. εξειδικευμένα παιχνίδια)	6	3	7
16.5. Ενεργητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ (π.χ. αποκλεισμός δραστηριότητας χωρίς να επιτρέπει στο χρήστη να συνεχίσει)	6	2	7
16.6. Παθητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ (π.χ. προειδοποιητικό μήνυμα προς τον χρήστη και μετέπειτα πράξη με δική του ευθύνη)	6	2	7
16.7. Φιλτράρισμα μηνυμάτων email από λογισμικό	6	2	7
16.8. Εγκατάσταση Antivirus λογισμικό στις συσκευές μου	6	2	7
16.9. Απευθείας σύνδεση στον επίσημο ιστότοπο και όχι μέσω κάποιου συνδέσμου (link)	6	2	7
17.1. Μπορώ να αξιολογήσω ένα ιστότοπο με βάση την αυθεντικότητα, αξιοπιστία, εμφάνιση, περιεχόμενο του κτλ.	5	3	5
17.2. Μπορώ να αξιολογήσω εάν ένας ιστότοπος είναι ασφαλής & αξιόπιστος ή πλαστός.	5	3	5
17.3. Μπορώ να αξιολογήσω εάν ένα email είναι ανεπιθύμητο, διαφημιστικό, phishing ή απάτη.	5	2	6
17.4. Οι άνθρωποι που είναι σημαντικοί για μένα πιστεύουν ότι πρέπει να είμαι προσεκτικός με τις επιθέσεις phishing.	6	3	7
17.5. Οι δάσκαλοι ή οι συνεργάτες μου με έχουν βοηθήσει στο να μάθω σχετικά με τις επιθέσεις phishing.	3	3.75	1
17.6. Γενικά, το πανεπιστήμιο μου ή σχολείο μου ή οργανισμός μου κτλ. έχει πολιτικές και μέτρα προστασίας από επιθέσεις phishing.	3	4	1
17.7. Ξέρω πώς να ανιχνεύω απόπειρες phishing	4	4	5
17.8. Μπορώ να μάθω πώς να εντοπίζω εύκολα απόπειρες phishing	5	2.75	5
17.9. Παρακολουθώ τις εξελίξεις για απόπειρες phishing	4	3	1
17.10. Ξέρω πολλές διαφορετικές μεθόδους για να εντοπίζω απόπειρες phishing	3	3	2
17.11. Είμαι σίγουρος για τις ικανότητές μου στο να εντοπίζω απόπειρες phishing για τη λήψη πληροφοριών από τον Ιστό	4	3	5
17.12. Έχω τις τεχνικές δεξιότητες που χρειάζομαι για να εντοπίζω απόπειρες phishing	3	3	2
18. Ποια πιστεύετε ότι είναι η κατάλληλη ηλικία για να εκπαιδευτεί κάποιος για το phishing;	2	1	2

Πίνακας 1. Ερωτήσεις του ερωτηματολογίου και περιγραφική στατιστική ανάλυση αυτών ως προς το Media, IQR και Mode.

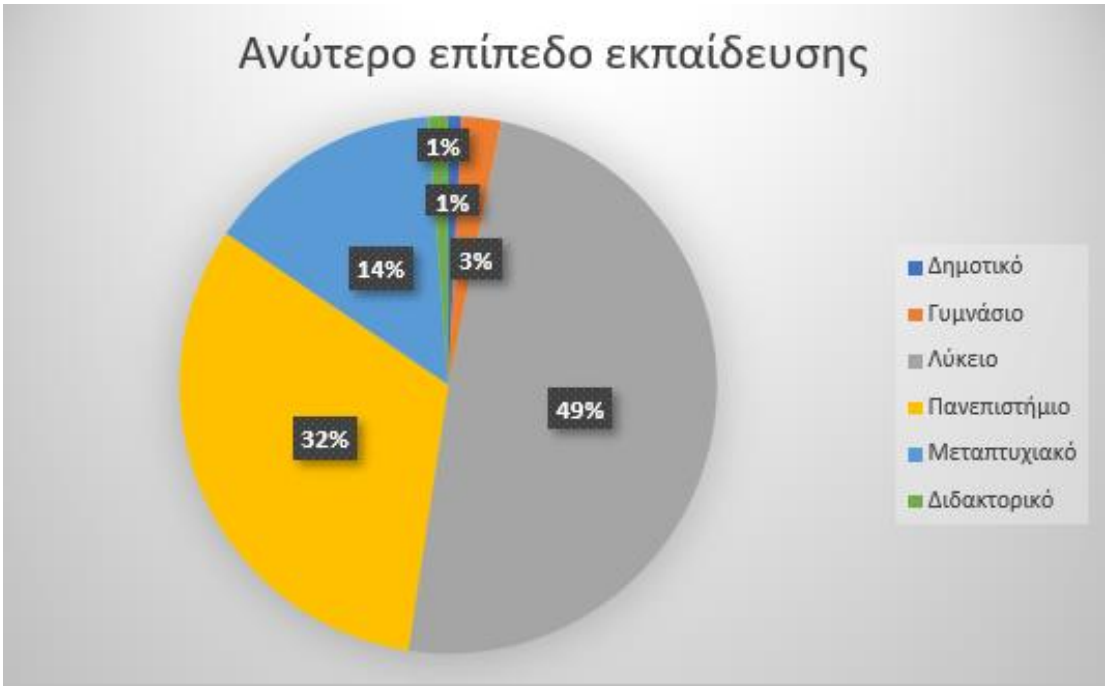
Από τη διανομή του ερωτηματολογίου συλλέχθηκαν 252 απαντήσεις εκ των οποίων όπως φαίνεται στα παρακάτω διαγράμματα το 72% αυτών ήταν Γυναίκες (181 συμμετέχοντες) και το 28% ήταν Άνδρες (71 συμμετέχοντες). Η πλειοψηφία των απαντήσεων ήταν ηλικίας κάτω από 25 χρονών (139 συμμετέχοντες), με ανώτερο επίπεδο εκπαίδευσης λύκειο (125 συμμετέχοντες) και απασχόληση φοιτητές (78 συμμετέχοντες).



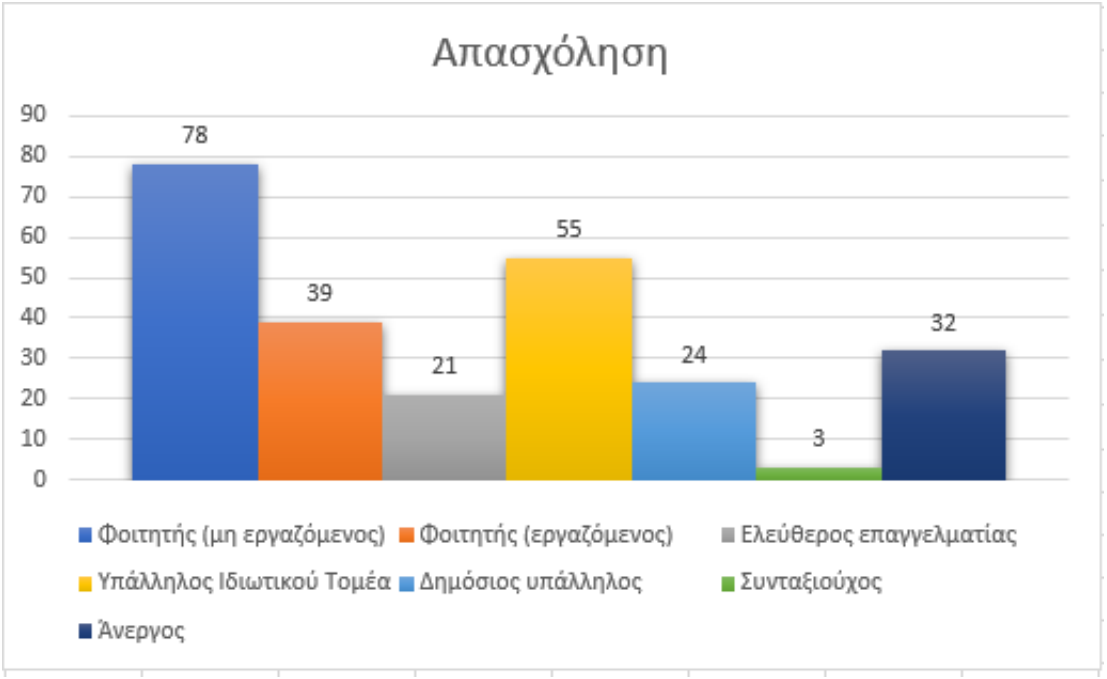
Διάγραμμα 1: Φύλο συμμετεχόντων του ερωτηματολογίου.



Διάγραμμα 2: Ηλικία συμμετεχόντων του ερωτηματολογίου.



Διάγραμμα 3: Ανώτερο επίπεδο εκπαίδευσης των συμμετεχόντων του ερωτηματολογίου.



Διάγραμμα 4: Απασχόληση των συμμετεχόντων του ερωτηματολογίου.

Στη συνέχεια, για το λόγο ότι τα δεδομένα του ερωτηματολογίου είναι ποιοτικά χρησιμοποίησα τον έλεγχο X^2 του Pearson για να ελέγξω τη συσχέτιση μεταξύ των απαντήσεων που έλαβα από τις ερωτήσεις του ερωτηματολογίου μου και συγκεκριμένων μεταβλητών. Αν η τιμή του p-value που προκύπτει από τον έλεγχο X^2 είναι μικρότερη από το επίπεδο αποδοχής (συνήθως 0,05) άγεται το συμπέρασμα ότι υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των δύο ποιοτικών μεταβλητών. Πιο συγκεκριμένα, αυτό σημαίνει ότι οι δύο μεταβλητές δεν είναι ανεξάρτητες και υπάρχει κάποια συσχέτιση μεταξύ τους. Αντίθετα, αν η τιμή του p-value που προκύπτει από τον έλεγχο X^2 είναι μεγαλύτερη από το επίπεδο αποδοχής (0,05) σημαίνει ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών.

	p-value
13.1 Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. “ngb” αντί για “nbg”, “l” αντί για “l”)	<0,001
13.2 Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με “https”	<0,001
13.3 Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	<0,001
13.4 Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	<0,001
13.5 Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	<0,001

Πίνακας 2: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 13.1 έως 13.5 και της μεταβλητής «e-banking phishing detection skills»

	p-value
14.1 Χρήση επειγουσών λέξεων στο μήνυμα email	<0,001
14.2 Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	<0,001
14.3 Άγνωστος αποστολέας μηνύματος email	<0,001
14.4 Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001
14.5 Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	<0,001

Πίνακας 3: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 14.1 έως 14.5 και της μεταβλητής «email phishing detection skills»

Στον πίνακα 2, ο οποίος αναφέρεται σε πέντε κριτήρια που υποδηλώνουν στους χρήστες του ίντερνετ ότι το email που προέρχεται από τη «τράπεζα» είναι «phishing» και στον πίνακα 3, ο οποίος περιλαμβάνει τα κριτήρια που φανερώνουν στους χρήστες του ίντερνετ αν η ιστοσελίδα της τράπεζας είναι γνήσια ή «phishing», παρατηρούμε ότι το p-value είναι μικρότερο του 0,05. Αυτό σημαίνει ότι υπάρχει συσχέτιση όχι μόνο μεταξύ των ερωτήσεων 13.1 έως 13.5 (Πίνακας 2) και της μεταβλητής «e-banking phishing detection skills», αλλά και των ερωτήσεών 14.1 έως 14.5 (Πίνακας 3) και της μεταβλητής «email phishing detection skills».

	p-value
17.1 Μπορώ να αξιολογήσω ένα ιστότοπο με βάση την αυθεντικότητα, αξιοπιστία, εμφάνιση, περιεχόμενο του κτλ.	<0,001
17.2 Μπορώ να αξιολογήσω εάν ένας ιστότοπος είναι ασφαλής & αξιόπιστος ή πλαστός.	<0,001
17.3 Μπορώ να αξιολογήσω εάν ένα email είναι ανεπιθύμητο, διαφημιστικό, phishing ή απάτη.	<0,001

Πίνακας 4: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 17.1 έως 17.3 και της μεταβλητής «Information Evaluation».

	p-value
17.4 Οι άνθρωποι που είναι σημαντικοί για μένα πιστεύουν ότι πρέπει να είμαι προσεκτικός με τις επιθέσεις phishing.	<0,001
17.5 Οι δάσκαλοι ή οι συνεργάτες μου με έχουν βοηθήσει στο να μάθω σχετικά με τις επιθέσεις phishing.	<0,001
17.6 Γενικά, το πανεπιστήμιο μου ή σχολείο μου ή οργανισμός μου κτλ. έχει πολιτικές και μέτρα προστασίας από επιθέσεις phishing.	<0,001

Πίνακας 5: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 17.4 έως 17.6 και της μεταβλητής «Social Influence Phishing Detection».

	p-value
17.7 Ξέρω πώς να ανιχνεύω απόπειρες phishing	<0,001
17.8 Μπορώ να μάθω πώς να εντοπίζω εύκολα απόπειρες phishing	<0,001
17.9 Παρακολουθώ τις εξελίξεις για απόπειρες phishing	<0,001
17.10 Ξέρω πολλές διαφορετικές μεθόδους για να εντοπίζω απόπειρες phishing	<0,001
17.11 Είμαι σίγουρος για τις ικανότητές μου στο να εντοπίζω απόπειρες phishing για τη λήψη πληροφοριών από τον Ιστό	<0,001
17.12 Έχω τις τεχνικές δεξιότητες που χρειάζομαι για να εντοπίζω απόπειρες phishing	<0,001

Πίνακας 6: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 17.7 έως 17.12 και της μεταβλητής «Self-efficacy on Phishing Detection».

Στους πίνακες 4,5,6 απεικονίζονται τα υποερωτήματα της ερώτησης 17 στην οποία ο ερωτώμενος έπρεπε να δηλώσει τον βαθμό στον οποίο συμφωνεί ή διαφωνεί με αυτά. Σύμφωνα με τον πίνακα 4 συμπεραίνουμε ότι υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στη δυνατότητα που έχει ο ερωτώμενος να αναλύσει έναν ιστότοπο και ένα email σχετικά με την αξιοπιστία του και της μεταβλητής «Information Evaluation». Στη συνέχεια ο πίνακας 5 δείχνει ότι υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στη συμβολή που προσφέρει ο κοινωνικός περίγυρος του ερωτώμενου για τη προστασία του από το «phishing» και της μεταβλητής «Social Influence Phishing Detection». Τέλος, από το πίνακα 6 συμπεραίνουμε ότι υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στη γνώση που κατέχει ο κάθε ερωτώμενος για το «phishing» και της μεταβλητής «Self-efficacy on Phishing Detection».

	p-value
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	0,011
11. Θα βάζατε τους κωδικούς σας εδώ;	<0,001
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	<0,001
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "l")	<0,001
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	<0,001
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	<0,001
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	<0,001
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	<0,001

Πίνακας 7: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 9, 11, 12,13 και της μεταβλητής «e-banking phishing detection skills».

	p-value
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	<0,001
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	<0,001
14.3. Άγνωστος αποστολέας μηνύματος email	<0,001
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	<0,001

Πίνακας 8: Έλεγχος συσχέτισης μεταξύ της απάντησης στην ερώτηση 14 και της μεταβλητής «email phishing detection skills».

Ο πίνακας 7 δείχνει πως υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των ερωτήσεων 9 έως 13.5, οι οποίες αναφέρονται στην ικανότητα που έχουν οι χρήστες του διαδικτύου να αναγνωρίσουν μία «phishing» ιστοσελίδα που προέρχεται από τη «τράπεζα» και της μεταβλητής «e-banking phishing detection skills». Η ερώτηση 11 απεικονίζει μία «phishing» ιστοσελίδα τράπεζας ενώ η ερώτηση 12 ένα «phishing email» με σκοπό να εξετάσει αν η γνώση που κατέχει ο ερωτώμενος για το «phishing» εφαρμόζεται και στη πράξη. Στο πίνακα 8 βλέπουμε ότι υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των δεξιοτήτων που κατέχουν οι χρήστες του ιντερνετ για να αναγνωρίσουν αν ένα email που προέρχεται από τη «τράπεζα» είναι γνήσιο ή «phishing» και της μεταβλητής «email phishing detection skills».

	p-value «Information Evaluation»	p-value «Social Influence Phishing Detection»	p-value «Self-efficacy on Phishing Detection»
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	<0,001	0,002	<0,001
11. Θα βάζατε τους κωδικούς σας εδώ;	0,006	**0,114**	**0,325**
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	<0,001	0,001	0,011
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "I")	<0,001	0,001	<0,001
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	<0,001	**0,241**	**0,071**
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	<0,001	0,027	<0,001
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	<0,001	<0,001	0,006
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	<0,001	0,016	<0,001
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	**0,435**	**0,992**	**0,619**
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	0,026	**0,218**	**0,724**
14.3. Άγνωστος αποστολέας μηνύματος email	0,049	**0,414**	**0,706**
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001	**0,409**	**0,476**
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	0,003	**0,231**	**0,363**

Πίνακας 9: Έλεγχος συσχέτισης μεταξύ των μεταβλητών «Information Evaluation», «Social Influence Phishing Detection», «Self-efficacy on Phishing Detection» και των απαντήσεων στις ερωτήσεις 9,11,12,13 και 14.

Ο πίνακας 9 εξετάζει την υπόθεση (Hypothesis Testing) αν οι μεταβλητές «Information Evaluation», «Social Influence Phishing Detection» και «Self-efficacy on Phishing Detection» επηρεάζουν τις ερωτήσεις του ερωτηματολογίου που σχετίζονται με την ικανότητα που έχουν οι χρήστες του διαδικτύου να αναγνωρίσουν ένα «phishing email» και μία «phishing» ιστοσελίδα αναξιόπιστης τράπεζας. Όπως φαίνεται στο πίνακα δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ της μεταβλητής «Information Evaluation» και της ερώτησης 14.1 που αναφέρεται σε ένα από τα στοιχεία που έχουν τα «phishing emails». Επιπλέον, στο πίνακα φαίνεται ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στις μεταβλητές «Social Influence Phishing Detection», «Self-efficacy on Phishing Detection» και στις ερωτήσεις 11, 13.2 που αναφέρονται στα χαρακτηριστικά ενός «phishing» ιστότοπου τράπεζας. Ακόμη, όπως φαίνεται στο πίνακα δεν υπάρχει στατιστικά σημαντική συσχέτιση ούτε ανάμεσα στις μεταβλητές «Social Influence Phishing Detection», «Self-efficacy on Phishing Detection» και στα υποερωτήματα της ερώτησης 14 που σχετίζονται με τα χαρακτηριστικά ενός «phishing email».

	p-value 15.1. Εμπιστοσύνη στον αποστολέα του μηνύματος email (π.χ. όνομα τράπεζας)	**p-value** 15.2. Περιέργεια	**p-value** 15.3. Άγχος	**p-value** 15.4. Βιασύνη	**p-value** 15.5. Ελλιπής γνώση για προστασία από phishing
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	**0,195**	**0,164**	0,002	<0,001	<0,001
11. Θα βάζατε τους κωδικούς σας εδώ;	0,032	0,002	0,001	<0,001	<0,001
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	0,001	<0,001	<0,001	<0,001	<0,001
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "l")	**0,534**	**0,163**	0,049	0,001	0,003
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	**0,439**	**0,160**	**0,200**	**0,105**	**0,271**
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	**0,759**	**0,140**	<0,001	0,005	<0,001
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	**0,095**	**0,150**	0,005	0,011	<0,001
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	**0,410**	**0,210**	0,031	0,005	<0,001
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	<0,001	<0,001	<0,001	**0,083**	0,018
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	<0,001	0,025	<0,001	0,007	0,001
14.3. Άγνωστος αποστολέας μηνύματος email	<0,001	0,018	0,013	0,001	<0,001
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001	0,029	0,012	<0,001	0,004
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	<0,001	0,004	<0,001	<0,001	**0,068**

Πίνακας 10 Έλεγχος συσχέτισης μεταξύ των παραγόντων που ωθούν τους χρήστες του Internet να κάνουν «κλικ» σε ένα «phishing link» που προέρχεται από τη «τράπεζα» και των απαντήσεων στις ερωτήσεις 9,11,12,13 και 14.

Ο πίνακας 10 εξετάζει την υπόθεση (Hypothesis Testing) αν καθεμία απο τις απαντήσεις στις ερωτήσεις 15.1 έως 15.5 που αναφέρονται στους παράγοντες που ωθούν τους χρήστες του διαδικτύου να κάνουν «κλικ» σε ένα «phishing link» που προέρχεται από τη «τράπεζα» επηρεάζει τις ερωτήσεις 9, 11, 12, 13 και 14 που έχουν απαντήσει οι ερωτώμενοι. Όπως φαίνεται στο πίνακα το πόσο καλά γνωρίζουν οι ερωτώμενοι πως να προστατευτούν από απόπειρες «phishing» δεν έχει στατιστικά σημαντική συσχέτιση με την εμπιστοσύνη που δείχνουν στον αποστολέα του μηνύματος email (Ερώτηση 15.1)και τη περιέργεια που πολλές φορές ωθεί τους αναγνώστες ενός email να κάνουν «κλικ» σε κάποιο σύνδεσμο(Ερώτηση 15.2). Στη συνέχεια παρατηρούμε ότι τα υποερωτήματα της ερώτησης 13 που σχετίζονται με την ικανότητα των χρηστών του Internet να αναγνωρίζουν ένα «phishing email» που προέρχεται από τη «τράπεζα» δεν έχουν στατιστικά σημαντική συσχέτιση με τις ερωτήσεις 15.1 και 15.2. Παρατηρούμε επίσης ότι η ερώτηση 13.2 που αναφέρεται στη μη ύπαρξη κλειστού λουκέτου σε μία ιστοσελίδα δεν έχει στατιστικά σημαντική

συσχέτιση με καμία από τις απαντήσεις 15.1 έως 15.5. Τέλος, από το πίνακα φαίνεται όχι μόνο ότι το υποερώτημα 14.1 που αναφέρεται στη χρήση επειγουσών λέξεων σε ένα μήνυμα email δεν έχει στατιστικά σημαντική συσχέτιση με τη βιασύνη των χρηστών του διαδικτύου που συμβάλλει στην εξαπάτηση τους από «phishers», αλλά και ότι το υποερώτημα 14.5 που αναφέρεται στα ορθογραφικά και γραμματικά λάθη σε ένα μήνυμα email δεν έχει στατιστικά σημαντική συσχέτιση με την ελλιπή γνώση των χρηστών του ιντερνετ για τη προστασία τους από το «phishing».

	p-value 16.1. Δημιουργία Black list	**p-value** 16.2. Δημιουργία White list	**p-value** 16.3. Εκπαίδευση στο σχολείο, πανεπιστήμιο, εργασία, κτλ.	**p-value** 16.4. Αυτό-εκπαίδευση από εφαρμογές	**p-value** 16.5. Ενεργητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	**0,428**	**0,276**	**0,836**	**0,352**	**0,175**
11. Θα βάζατε τους κωδικούς σας εδώ;	**0,458**	**0,885**	**0,660**	**0,077**	**0,185**
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	<0,001	0,030	0,022	0,016	0,049
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "l")	**0,077**	**0,438**	0,044	0,047	**0,146**
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	**0,349**	**0,322**	**0,263**	**0,827**	**0,579**
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	0,015	0,038	**0,066**	**0,265**	0,029
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	**0,470**	**0,322**	**0,236**	**0,107**	**0,864**
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https:// lnkd.in/ dm8hxDj5, http:// 147.46.236.55/ PayPal / login. html)	0,004	**0,381**	**0,392**	0,011	**0,089**
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	<0,001	0,002	<0,001	<0,001	<0,001
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	<0,001	<0,001	<0,001	<0,001	<0,001
14.3. Άγνωστος αποστολέας μηνύματος email	<0,001	<0,001	<0,001	<0,001	<0,001
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001	<0,001	<0,001	<0,001	<0,001
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	0,004	0,008	<0,001	0,003	<0,001

Πίνακας 11: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 9,11,12,13,14 και στους τρόπους αντιμετώπισης του phishing.

Ο πίνακας 11 εξετάζει την αντίστροφη υπόθεση (Hypothesis Testing) από τον πίνακα 10, δηλαδή πως οι ερωτήσεις 9, 11, 12, 13 και 14 που απάντησαν οι ερωτώμενοι επηρεάζουν τις απαντήσεις στις ερωτήσεις 16.1 έως 16.5. Αρχικά, παρατηρούμε ότι οι ερωτήσεις 9,11,13.2 και 13.4 δεν έχουν στατιστικά σημαντική συσχέτιση με τα πέντε πρώτα υποερωτήματα της ερώτησης 16 που αναφέρονται στα μέτρα που μπορούν να ληφθούν για να προστατέψουν τους χρήστες του διαδικτύου από

απόπειρες “phishing”. Ακόμη, παρατηρούμε ότι η ερώτηση 13.1 που σχετίζεται με την ύπαρξη αναγραμματισμού ή ανεπαίσθητης διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. “ngb” αντί για “nbg”, “l” αντί για “l”) έχει στατιστικά σημαντική συσχέτιση με την ερώτηση 16.3.(Εκπαίδευση στο σχολείο, πανεπιστήμιο, εργασία, κτλ.) και 16.4 (Αυτό-εκπαίδευση από εφαρμογές), ενώ η ερώτηση 13.3 που αναφέρεται στο αν ζητάει ένα μήνυμα email από τον παραλήπτη να κάνει μια ενέργεια επειγόντως δεν έχει στατιστικά σημαντική συσχέτιση με τις ερωτήσεις 16.3 και 16.4. Ακόμη, παρατηρούμε ότι η ερώτηση 13.5 που αναφέρεται στο αν το μονοπάτι/διεύθυνση URL που αναγράφεται στο μήνυμα email είναι συντομευμένο ή «περίεργο» έχει στατιστικά σημαντική συσχέτιση με την ερώτηση 16.1(δημιουργία Black list) και την ερώτηση 16.4(αυτό-εκπαίδευση από εφαρμογές). Τέλος, όπως φαίνεται στο πίνακα 11 όλα τα υποερωτήματα της ερώτησης 14 που περιλαμβάνουν τα κριτήρια που φανερώνουν στους χρήστες του ιντερνετ αν η ιστοσελίδα της τράπεζας είναι γνήσια ή phishing έχουν στατιστικά σημαντική συσχέτιση με τους τρόπος αντιμετώπισης κατά του «phishing» που φαίνονται στο πίνακα.

	p-value 16.6. Παθητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ	p-value 16.7. Φιλτράρισμα μηνυμάτων email από λογισμικό	p-value 16.8. Εγκατάσταση Antivirus λογισμικό στις συσκευές μου	p-value 16.9. Απευθείας σύνδεση στον επίσημο ιστότοπο και όχι μέσω κάποιου συνδέσμου (link)
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	**0,561**	0,005	**0,242**	**0,222**
11. Θα βάζατε τους κωδικούς σας εδώ;	**0,125**	**0,344**	**0,390**	**0,176**
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	**0,415**	**0,219**	**0,617**	**0,976**
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "I")	**0,352**	0,005	**0,059**	**0,171**
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	**0,244**	**0,635**	**0,055**	**0,190**
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	**0,096**	0,007	**0,053**	**0,580**
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	**0,509**	**0,756**	**0,188**	**0,601**
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	**0,366**	**0,282**	**0,534**	**0,275**
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	<0,001	<0,001	<0,001	<0,001
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	<0,001	<0,001	<0,001	<0,001
14.3. Άγνωστος αποστολέας μηνύματος email	<0,001	<0,001	<0,001	<0,001
14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	<0,001	<0,001	<0,001	<0,001
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	<0,001	<0,001	<0,001	<0,001

Πίνακας 12: Έλεγχος συσχέτισης μεταξύ των απαντήσεων στις ερωτήσεις 9,11,12,13,14 και στους τρόπους αντιμετώπισης του phishing.

Σε συνέχεια του πίνακα 11 έχουμε τον πίνακα 12 ο οποίος απεικονίζει το πως οι ερωτήσεις 9, 11, 12, 13 και 14 που απάντησαν οι ερωτώμενοι επηρεάζουν τις απαντήσεις στις ερωτήσεις 16.6 έως και 16.9. Αρχικά, παρατηρούμε ότι οι ερωτήσεις 11,12,13.2,13.4 και 13.5 οι οποίες σχετίζονται με την εφαρμογή στη πράξη της γνώσης που έχουν οι ερωτώμενοι για το «phishing» και τα τρία από τα χαρακτηριστικά που έχουν τα «phishing emails» που προέρχεται από τη «τράπεζα» δεν έχουν στατιστικά σημαντική συσχέτιση με τα μέτρα που μπορούν να ληφθούν για να προστατέψουν τους χρήστες του διαδικτύου από απόπειρες «phishing». Αντίθετα, όπως είναι πρόδηλο από τον πίνακα, η ερώτηση 9, 13.1 και 13.3 έχουν στατιστικά σημαντική συσχέτιση με την ερώτηση 16.7 (Φιλτράρισμα μηνυμάτων email από λογισμικό).

	p-value φύλο	**p-value** ηλικία	**p-value** επίπεδο εκπαίδευσης	**p-value** είδος απασχόλησης	**p-value** ώρες στο Ίντερνετ με υπολογιστή	**p-value** ώρες στο Ίντερνετ με κινητό
7. Πόσα μηνύματα email λαμβάνετε κάθε μέρα;	**0,237**	0,002	0,003	0,006	<0,001	0,004
8. Δέχεστε μηνύματα email από τη τράπεζά σας;	**0,884**	0,043	0,031	**0,247**	0,007	**0,414**
9. Πόσο καλά γνωρίζετε πως να προστατευτείτε από απόπειρες phishing;	**0,173**	0,005	0,010	<0,001	0,015	**0,269**
10. Περίπου τι ποσοστό από τα μηνύματα email που λαμβάνετε είναι phishing;	**0,370**	**0,137**	**0,134**	**0,413**	0,049	**0,371**
11. Θα βάζατε τους κωδικούς σας εδώ;	**0,973**	**0,053**	**0,770**	**0,159**	**0,394**	**0,062**
12. Τι θα κάνατε αν λαμβάνατε το παρακάτω μήνυμα email;	**0,771**	0,034	0,028	**0,054**	**0,785**	0,027
13.1. Αν υπάρχει αναγραμματισμός ή ανεπαίσθητη διαφορά στα γράμματα για το μονοπάτι/διεύθυνση URL (π.χ. "ngb" αντί για "nbg", "l" αντί για "I")	0,043	**0,257**	0,025	0,026	<0,001	**0,150**
13.2. Αν δεν υπάρχει κλειστό λουκέτο ή το μονοπάτι/διεύθυνση URL δεν αρχίζει με "https"	0,005	**0,429**	**0,074**	**0,071**	**0,082**	0,006
13.3. Αν ζητάει να κάνετε κάποια ενέργεια επειγόντως	**0,538**	**0,060**	0,002	**0,220**	**0,188**	0,037
13.4. Αν υπάρχουν ορθογραφικά, γραμματικά ή συντακτικά λάθη	**0,933**	<0,001	**0,069**	0,008	**0,055**	**0,283**
13.5. Αν το μονοπάτι/διεύθυνση URL είναι συντομευμένο ή «περίεργο» (π.χ. https://lnkd.in/dm8hxDj5, http://147.46.236.55/PayPal/login.html)	**0,276**	0,023	0,005	**0,064**	0,024	0,015
14.1. Χρήση επειγουσών λέξεων στο μήνυμα email	**0,493**	**0,169**	0,024	**0,155**	**0,117**	**0,372**
14.2. Αίτημα για ευαίσθητες και προσωπικές πληροφορίες (π.χ. κωδικούς)	0,007	**0,141**	**0,216**	**0,761**	**0,249**	**0,207**
14.3. Άγνωστος αποστολέας μηνύματος email	0,015	**0,071**	**0,697**	**0,789**	0,046	**0,112**

14.4. Ύποπτος σύνδεσμος (π.χ. http://147.46.236.55/PayPal/login.html) στο μήνυμα email	**0,068**	0,004	**0,079**	**0,451**	**0,109**	0,034
14.5. Ορθογραφικά και γραμματικά λάθη στο μήνυμα email	**0,106**	0,010	**0,211**	**0,071**	**0,062**	**0,617**
15.1. Εμπιστοσύνη στον αποστολέα του μηνύματος email (π.χ. όνομα τράπεζας)	**0,233**	**0,105**	**0,842**	**0,654**	**0,144**	**0,716**
15.2. Περιέργεια	0,014	0,033	**0,591**	**0,782**	**0,242**	0,006
15.3. Άγχος	**0,388**	**0,294**	**0,492**	**0,534**	**0,664**	<0,001
15.4. Βιασύνη	**0,068**	**0,188**	**0,555**	**0,869**	**0,404**	<0,001
15.5. Ελλιπής γνώση για προστασία από phishing	**0,289**	0,002	**0,211**	0,014	**0,705**	0,003
16.1. Δημιουργία Back list (με ύποπτες διευθύνσεις IP-URL, λέξεις-κλειδιά που χρησιμοποιούν οι phishers)	**0,282**	**0,089**	**0,706**	**0,321**	**0,538**	**0,318**
16.2. Δημιουργία White list (με νόμιμες-επίσημες διευθύνσεις URL τραπεζών κτλ.)	**0,200**	**0,225**	**0,392**	**0,329**	**0,942**	**0,204**
16.3. Εκπαίδευση στο σχολείο, πανεπιστήμιο, εργασία, κτλ.	**0,908**	**0,060**	**0,793**	**0,513**	**0,174**	**0,941**
16.4. Αυτό-εκπαίδευση από εφαρμογές (π.χ. εξειδικευμένα παιχνίδια)	0,033	0,012	**0,309**	**0,309**	**0,205**	**0,196**
16.5. Ενεργητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ (π.χ. αποκλεισμός δραστηριότητας χωρίς να επιτρέπει στο χρήστη να συνεχίσει)	**0,123**	**0,194**	**0,481**	**0,426**	**0,618**	**0,189**
16.6. Παθητικές προειδοποιήσεις από τα προγράμματα που χρησιμοποιώ (π.χ. προειδοποιητικό μήνυμα προς τον χρήστη και μετέπειτα πράξη με δική του ευθύνη)	0,020	0,022	**0,609**	**0,138**	**0,932**	**0,137**
16.7. Φιλτράρισμα μηνυμάτων email από λογισμικά	**0,148**	0,033	**0,609**	**0,223**	**0,878**	**0,187**
16.8. Εγκατάσταση Antivirus λογισμικό στις συσκευές μου	**0,931**	0,048	**0,436**	**0,460**	**0,663**	**0,291**
16.9. Απευθείας σύνδεση στον επίσημο ιστότοπο και όχι μέσω κάποιου συνδέσμου (link)	**0,099**	**0,198**	**0,648**	**0,374**	**0,983**	**0,081**
17.1. Μπορώ να αξιολογήσω ένα ιστότοπο με βάση την αυθεντικότητα, αξιοπιστία, εμφάνιση, περιεχόμενο του κτλ.	0,047	0,006	**0,650**	<0,001	0,033	**0,603**
17.2. Μπορώ να αξιολογήσω εάν ένας ιστότοπος είναι ασφαλής & αξιόπιστος ή πλαστός.	**0,200**	<0,001	**0,362**	<0,001	0,027	**0,886**
17.3. Μπορώ να αξιολογήσω εάν ένα email είναι ανεπιθύμητο, διαφημιστικό, phishing ή απάτη.	**0,385**	<0,001	0,045	0,004	0,030	**0,326**
17.4. Οι άνθρωποι που είναι σημαντικοί για μένα πιστεύουν ότι πρέπει να είμαι προσεκτικός με τις επιθέσεις phishing.	**0,999**	**0,704**	**0,341**	**0,433**	**0,947**	**0,378**
17.5. Οι δάσκαλοι ή οι συνεργάτες μου με έχουν βοηθήσει στο να μάθω σχετικά με τις επιθέσεις phishing.	**0,490**	**0,544**	**0,846**	**0,297**	**0,525**	0,002

17.6. Γενικά, το πανεπιστήμιο μου ή σχολείο μου ή οργανισμός μου κτλ. έχει πολιτικές και μέτρα προστασίας από επιθέσεις phishing.	**0,517**	**0,278**	**0,335**	**0,131**	**0,231**	**0,091**
17.7. Ξέρω πώς να ανιχνεύω απόπειρες phishing	**0,051**	0,013	0,006	<0,001	0,012	**0,370**
17.8. Μπορώ να μάθω πώς να εντοπίζω εύκολα απόπειρες phishing	**0,103**	0,003	**0,058**	**0,139**	**0,209**	**0,290**
17.9. Παρακολουθώ τις εξελίξεις για απόπειρες phishing	**0,851**	**0,143**	**0,135**	0,027	**0,506**	**0,218**
17.10. Ξέρω πολλές διαφορετικές μεθόδους για να εντοπίζω απόπειρες phishing	0,019	**0,317**	**0,140**	0,007	**0,097**	**0,699**
17.11. Είμαι σίγουρος για τις ικανότητές μου στο να εντοπίζω απόπειρες phishing για τη λήψη πληροφοριών από τον Ιστό	0,012	0,020	0,042	<0,001	**0,225**	**0,443**
17.12. Έχω τις τεχνικές δεξιότητες που χρειάζομαι για να εντοπίζω απόπειρες phishing	0,020	**0,129**	**0,148**	<0,001	**0,134**	**0,521**
18. Ποια πιστεύετε ότι είναι η κατάλληλη ηλικία για να εκπαιδευτεί κάποιος για το phishing;	**0,140**	**0,076**	**0,967**	**0,911**	**0,495**	0,005

Πίνακας 13: Έλεγχος Kruskal–Wallis non-parametric tests ανάμεσα στις 18 ερωτήσεις του ερωτηματολογίου και των μεταβλητών φύλο,ηλικία,επίπεδο εκπαίδευσης,είδος απασχόλησης,ώρες στο ίντερνετ μέσω υπολογιστή και ώρες στο ίντερνετ μέσω κινητού.

Παρατηρώντας τον πίνακα 13 άγεται το συμπέρασμα πως για όσες ερωτήσεις του ερωτηματολογίου το p-value, που προκύπτει από τον έλεγχο Kruskal–Wallis non-parametric tests, είναι μικρότερο από το επίπεδο αποδοχής (συνήθως 0,05) έχουν στατιστικά σημαντικό αποτέλεσμα και επηρεάζονται από το φύλο, την ηλικία, το επίπεδο εκπαίδευσης, το είδος απασχόλησης και τις ώρες που αφιερώνουν οι συμμετέχοντες του ερωτηματολογίου στο ίντερνετ μέσω του υπολογιστή και του κινητού τους. Σε κάθε άλλη περίπτωση, οι 18 ερωτήσεις από τις οποίες απαρτίζεται το ερωτηματολόγιο δεν έχουν στατιστικά σημαντικό αποτέλεσμα και δεν επηρεάζονται από το φύλο, την ηλικία, το επίπεδο εκπαίδευσης, το είδος απασχόλησης και τις ώρες που αφιερώνουν οι συμμετέχοντες του ερωτηματολογίου στο ίντερνετ μέσω του υπολογιστή και του κινητού τους.

ΣΥΖΗΤΗΣΗ

Παρακάτω, θα ελέγξουμε, αν η ικανότητα των χρηστών του διαδικτύου να αναγνωρίσουν ένα «phishing email» ή ένα «phishing» ιστότοπο, που προέρχεται από τη «τράπεζα», επηρεάζεται από τα μέσα που υπάρχουν για να τους προστατέψουν από το «phishing» και ποιοι παράγοντες ωθούν τους χρήστες του διαδικτύου να κάνουν «κλικ» σε «phishing links».

Όπως φαίνεται στην έρευνα των Linfeng Li et al., (Linfeng Li, 2014) η δημιουργία «black list» και «white list» δεν είναι επαρκώς αξιόπιστες για την πρόληψη από απάτες «phishing». Σύμφωνα με την εργασία μου φαίνεται ότι η ικανότητα των χρηστών του διαδικτύου να προστατευθούν από ένα «phishing email» ή μια «phishing» ιστοσελίδα δεν έχουν στατιστικά σημαντική συσχέτιση με τη δημιουργία «black list» και «white list». Οπότε, η δημιουργία λιστών με «phishing» ή νόμιμα URL δεν βοηθούν τους χρήστες του διαδικτύου να αναγνωρίσουν μια «phishing» απάτη.

Στη συνέχεια, όπως έχει συζητηθεί στο βιβλιογραφικό κομμάτι της εργασίας η δημιουργία παιχνιδιών και εφαρμογών εκπαίδευσης για το «phishing» θα βοηθήσουν τους χρήστες του διαδικτύου να αναγνωρίζουν απειλές του «phishing» όπως για παράδειγμα είναι τα «phishing emails» και οι «phishing» ιστοσελίδες που προέρχονται από τη τράπεζα. Στο πίνακα 11, φαίνεται πως η ικανότητα των χρηστών του διαδικτύου να αναγνωρίζουν ένα «phishing» ιστότοπο δεν επηρεάζεται από την εκπαίδευσή τους από εφαρμογές, ενώ η αναγνώριση ενός «phishing email» επηρεάζεται. Η μελέτη του Alghamdi, H. (2017) επέδειξε ότι η εκπαίδευση των χρηστών σχετικά με το «phishing» κάνει τους χρήστες καχύποπτους, χωρίς να ενισχύει την ικανότητα τους να αναγνωρίζουν, αν η ιστοσελίδα και το email που προέρχονται από τη τράπεζα είναι νόμιμη ή «phishing». Σε κάθε περίπτωση όμως, δεν μπορεί να λεχθεί πως η εκπαίδευση για το «phishing» δεν είναι χρήσιμη.

Σύμφωνα με την έρευνα των Egelman S et al., (Egelman S, 2008) οι χρήστες του διαδικτύου υπακούν πολύ περισσότερο στις ενεργητικές προειδοποιήσεις παρά στις παθητικές. Σύμφωνα με τους Wu et al., (Wu, 2006) οι χρήστες του διαδικτύου δεν κοιτούν τη διεύθυνση URL και το κλειστό λουκέτο SSL οπότε αν λείπουν οι ενεργητικές προειδοποιήσεις, όπως είναι και το antivirus, οι χρήστες θα πέσουν εύκολα θύματα. Στη δική μου εργασία παρατηρείται μη στατιστικά σημαντική συσχέτιση μεταξύ της συμπεριφοράς των χρηστών του διαδικτύου όταν συνδέονται σε ένα «phishing» ιστότοπο και των ενεργητικών, παθητικών ενδείξεων. Ωστόσο, η συμπεριφορά των χρηστών του διαδικτύου όταν λαμβάνουν ένα «phishing email» έχει στατιστικά σημαντική συσχέτιση με τις ενεργητικές ενδείξεις και όχι με τις παθητικές.

Σε αντίθεση με τη δική μου εργασία στην οποία υπάρχουν στατιστικά σημαντική συσχέτιση ανάμεσα στην ικανότητα των χρηστών του κυβερνοχώρου να προστατεύονται από απάτες «phishing» και της μεθόδου «φιλτράρισμα μηνυμάτων» ως μέσο προστασίας από «phishing emails», η έρευνα του Almomani A et al., (Almomani A, 2013) υποστηρίζει ότι το φιλτράρισμα των emails έχει αδύναμα σημεία

με αποτέλεσμα ο μηχανισμός φιλτραρίσματος να μη λειτουργεί ορθά και οι χρήστες του διαδικτύου να δέχονται «phishing emails».

Στη συνέχεια σύμφωνα με την έρευνα των Martin S. R. Et al., (Martin S. R., 2021) οι χρήστες του διαδικτύου πέφτουν θύματα «phishing» από μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από γνωστές πηγές όπως είναι η τράπεζα ή οι φίλοι του θύματος. Η έρευνα αυτή είναι σύμφωνη με την εργασία μου, καθώς υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στην εμπιστοσύνη που δείχνει το θύμα στον αποστολέα ενός μηνύματος email και της συμπεριφοράς του όταν δέχεται ένα email που προέρχεται από τη «τράπεζα».

Τέλος, σύμφωνα με την εργασία μου, η χρήση επειγουσών λέξεων στο μήνυμα email που δέχεται ο χρήστης του διαδικτύου έχει στατιστικά σημαντική συσχέτιση με τη περιέργεια και το άγχος που τους προκαλούν τα «phishing emails». Όπως επιβεβαιώνεται από την έρευνα των Wang J et al., (Wang J., 2012) οι έντονες συναισθηματικές αντιδράσεις που προκαλούν τα «phishing emails» λόγω της χρήσης επειγουσών λέξεων αποτελούν παράγοντα για να πέσουν θύματα απάτης οι χρήστες του κυβερνοχώρου. Επιπλέον, σύμφωνα με τον πίνακα 10, υπάρχει στατιστικά σημαντική συσχέτιση ανάμεσα στη συμπεριφορά των χρηστών του διαδικτύου όταν δέχονται ένα «phishing email» και της ελλιπούς γνώσης για τη προστασία τους από το «phishing». Σύμφωνα με την ίδια έρευνα των Wang J et al., (Wang J., 2012), αφενός η γνώση που κατέχουν οι χρήστες του διαδικτύου για το «phishing» μπορεί να συμβάλλει στη προστασία τους από την απάτη, αφετέρου, όμως, ο παράγοντας της γνώσης ως μοναδικό μέσο αναγνώρισης μιας «phishing» απάτης δεν αρκεί, γιατί μπορεί να μην είναι επαρκής και για αυτό θα πρέπει να συμβουλεύονται τους ειδικούς για να ταυτοποιήσουν τη ταυτότητα του αποστολέα ενός email, όπως για παράδειγμα είναι το προσωπικό της τράπεζας πριν αξιολογήσουν ένα email που προέρχεται από αυτήν.

Συμπεράσματα

1. Η δημιουργία μαύρης λίστας (black list) και λευκής λίστας (white list) δεν προσφέρουν επαρκή προστασία κατά του «phishing».
2. Εκπαίδευση των χρηστών του διαδικτύου με εφαρμογές και παιχνίδια είναι σημαντική, καθώς ενισχύει την καχυποψία τους για το «phishing», αλλά δεν ενισχύει την ικανότητά τους να αξιολογούν ένα «email» ή έναν ιστότοπο σε νόμιμο ή «phishing».
3. Οι ενεργητικές προειδοποιήσεις είναι αποτελεσματικότερες από τις παθητικές, καθώς οι χρήστες του διαδικτύου υπακούν περισσότερο σε αυτές.
4. Το φιλτράρισμα των emails ως μέσο προστασίας από «phishing email» έχει αδύναμα σημεία με αποτέλεσμα ο μηχανισμός φιλτραρίσματος να μη λειτουργεί ορθά και οι χρήστες του διαδικτύου να δέχονται «phishing emails».

5. Η εμπιστοσύνη στον αποστολέα του αποτελεί παράγοντα που ωθεί τους χρήστες του διαδικτύου να πέσουν θύματα «phishing».
6. Η περιέργεια και το άγχος που προκαλούν τα «phishing emails» στους χρήστες του διαδικτύου αποτελούν παράγοντα για να πέσουν θύματα απάτης «phishing».
7. Η ελλιπής γνώση που κατέχουν οι χρήστες του διαδικτύου για τις απάτες «phishing» αποτελεί παράγοντα, που ωθεί τους χρήστες του διαδικτύου να πέσουν θύματα «phishing», για αυτό πριν πράξουν μια ενέργεια που τους προτρέπει ένα «email» θα πρέπει να ταυτοποιούν τη ταυτότητα του αποστολέα.

Περιορισμοί της έρευνας και συστάσεις για μελλοντική έρευνα

Η διπλωματική εργασία είχε τους εξής περιορισμούς. Αφενός, ένα μεγαλύτερο δείγμα θα έδινε πιο αξιόπιστα αποτελέσματα και αφετέρου μία έρευνα που θα είχε λάβει χώρα σε ολόκληρη την ελληνική περιφέρεια θα παρείχε πιο σαφή αποτελέσματα για τη συμπεριφορά των χρηστών διαδικτύου σε επιθέσεις «phishing». Εξίσου σημαντικός περιορισμός ήταν η πλειοψηφία της ηλικιακής ομάδας που απάντησε, κάτω από 25 έτη καθώς οι νέοι έχουν διαφορετικές ικανότητες και αντιλήψεις από ότι οι μεσήλικες και οι ηλικιωμένοι. Πέραν τούτου, η έρευνα που διεξήχθη για τη σύνταξη της διπλωματικής εργασία ήταν ποιοτική. Μελλοντικά, οι ερευνητές θα μπορούσαν να πραγματοποιήσουν μία ποσοτική έρευνα που θα προσφέρει μια πιο αντικειμενική αξιολόγηση των δεδομένων με πιο αξιόπιστα αποτελέσματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Akdemir, N., & Yenal, S. (2021). How phishers exploit the coronavirus pandemic: A content analysis of COVID-19 themed phishing emails. *Sage Open*, *11*(3), 21582440211031879.

Alghamdi, H. (2017). Can phishing education enable users to recognize phishing attacks?.

Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T., & Ramachandran, V. (2021). Enterprise Credential Spear-phishing attack detection. *Computers & Electrical Engineering*, *94*, 107363.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Alwanain, M. I. (2020). Phishing awareness and elderly users in social media. *Int J Comput Sci Netw Secur*, *20*(9), 114-19.

Amrutkar, C., Kim, Y. S., & Traynor, P. (2016). Detecting mobile malicious webpages in real time. *IEEE Transactions on Mobile Computing*, *16*(8), 2184-2197.

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*, 139-154.

Catalin, B. O. J. A., & Oiu, A. V. (2007). Optimization of Antivirus Software. *Informatica*, *11*(2007), 99-102.

Bošnjak, L., Sreš, J., & Brumen, B. (2018, May). Brute-force and dictionary attack on hashed real-world passwords. In *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro)* (pp. 1161-1166). IEEE.

Brody, R. G., Mulig, E., & Kimball, V. (2007). PHISHING, PHARMING AND IDENTITY THEFT. *Academy of Accounting & Financial Studies Journal*, *11*(3).

Bu, S. J., & Cho, S. B. (2021, June). Integrating deep learning with first-order logic programmed constraints for zero-day phishing attack detection. In *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 2685-2689). IEEE.

Conrad , E., & Feldman, J. (2017). *Secure sockets layer*. Secure Sockets Layer - an overview | ScienceDirect Topics.

Dada, E. G., Bassi, J. S., Chiroma, H., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, *5*(6).

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35.

Dhamija, R., Tygar, J. D., & Hearst, M. Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems. In *CHI* (Vol. 6, p. 581).

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1065-1074).

Ferreira, A., & Lenzini, G. (2015, July). An analysis of social engineering principles in effective phishing. In *2015 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 9-16). IEEE.

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies*, *125*, 19-31.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3* (pp. 36-47). Springer International Publishing.

Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web* (pp. 649-656).

Freier, A., Karlton, P., & Kocher, P. (2011). *The secure sockets layer (SSL) protocol version 3.0* (No. rfc6101).

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53*, 5019-5081.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *computers & security*, *73*, 519-544.

Jakobsson, M. (Ed.). (2016). *Understanding social engineering based scams* (Vol. 233). New York: Springer.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-31.

Lau, H., Khosrawipour, V., Kocbach, P., Mikolajczyk, A., Schubert, J., Bania, J., & Khosrawipour, T. (2020). The positive impact of lockdown in Wuhan on containing the COVID-19 outbreak in China. *Journal of travel medicine*, *27*(3), taaa037.

Wu, L., Du, X., & Wu, J. (2014, August). MobiFish: A lightweight anti-phishing scheme for mobile phones. In *2014 23rd international conference on computer communication and networks (icccn)* (pp. 1-8). IEEE.

Wu, L., Du, X., & Wu, J. (2015). Effective defense schemes for phishing attacks on mobile computing platforms. *IEEE Transactions on Vehicular Technology*, *65*(8), 6678-6691.

Moore, T., & Clayton, R. (2007, October). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 1-13).

Moore, T., & Clayton, R. (2007, October). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 1-13).

Nguyen, L. A. T., To, B. L., Nguyen, H. K., & Nguyen, M. H. (2014, April). A novel approach for phishing detection using URL-based heuristic. In *2014 international conference on computing, management and telecommunications (ComManTel)* (pp. 298-303). IEEE.

Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P. (2020, September). Investigating teenagers' ability to detect phishing messages. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 140-149). IEEE.

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of information technology*, *35*(3), 214-231.

Sanz, E. P., Hidalgo, J. M. G., & Pérez, J. C. C. (2008). Email spam filtering. *Advances in computers*, *74*, 45-114.

Gastellier-Prevost, S., Granadillo, G. G., & Laurent, M. (2011, February). A dual approach to detect pharming attacks at the client-side. In *2011 4th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1-5). IEEE.

Shankar, A., Shetty, R., & Nath, B. (2019). A review on phishing attacks. *International Journal of Applied Engineering Research*, *14*(9), 5.

Sharevski, F., & Jachim, P. (2022). "Alexa, What'sa Phishing Email?": Training users to spot phishing emails using a voice assistant. *EURASIP Journal on Information Security*, *2022*(1), 7.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).

Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2013). The underground economy of fake antivirus software. In *Economics of information security and privacy III* (pp. 55-78). Springer New York.

Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, *10*, 39325-39343.

Tally, G., Thomas, R., & Van Vleck, T. (2004). Anti-phishing: Best practices for institutions and consumers. *McAfee Research, Mar*.

Shahriar, H., & Zulkernine, M. (2012). Trustworthiness testing of phishing websites: A behavior model-based approach. *Future Generation Computer Systems*, *28*(8), 1258-1271.

Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages.

Yash, T., Kumar, S., & Sharma, K. (2022, May). Ethical Hacking: A Technique to Enhance Information Security. In *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)* (Vol. 1, pp. 780-784). IEEE.Ye, Z., Smith, S., & Anthony, D. (2005). Trusted paths for browsers. *ACM Transactions on Information and System Security (TISSEC)*, *8*(2), 153-186.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.