ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

Διπλωματική εργασία

«Η θεωρία του Social Engineering: Εργαλεία τεχνικές και τρόποι άμυνας κατά των επιθέσεων Phishing»

Μούρτος Θωμάς ΜΤΕ1728

Επιβλέπων καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2017-2018

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Λαμπρινουδάκη Κωνσταντίνο για την ανάθεση και την καθοδήγηση της παρούσας διπλωματικής εργασίας.

Σύντομη Περιγραφή Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια ολοκλήρωσης των μεταπτυχιακών σπουδών του Τμήματος Ασφάλειας Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά. Έχει ως τίτλο «Η θεωρία του Social Engineering: Εργαλεία τεχνικές και τρόποι άμυνας κατά των επιθέσεων Phishing» εστιάζοντας σε μια - όχι και τόσο σύγχρονη - μορφή απάτης αλλά και στον τρόπο που εξελίχτηκε και αποτελεί μια από τις μεγαλύτερες απειλές του κλάδου της Ασφάλειας Πληροφοριών, τις επιθέσεις Phishing. Οι ψυχολογικοί μηχανισμοί και η ανθρωπινή συμπεριφορά πίσω από τις επιθέσεις Κοινωνικής Μηχανικής (Social Engineering) και η μελέτη του «Ηλεκτρονικού Ψαρέματος» (Phishing) ως κυριότερο φαινόμενο εκδήλωσης επιθέσεων του είδους, η αναφορά σε αυτές τις επιθέσεις και οι τρόποι αντιμετώπισής τους αποτελούν τις κυριότερες πτυχές της εργασίας. Ο βασικός στόχος της εργασίας δεν είναι η επίδειξη επιθέσεων κοινωνικής μηχανικής υπό το πρίσμα των τεχνικών προδιαγραφών που απαιτούνται για τον αποτελεσματικό προγραμματισμό, σχεδιασμό, και υλοποίηση τους. Αντίθετα η εργασία επικεντρώνεται στο να αναδείξει τις ανθρώπινες συμπεριφορές οι οποίες ευνοούν την επιτυχία τέτοιων επιθέσεων και κατ' επέκταση στους τρόπους με τους οποίους μπορούμε να προάγουμε την ευαισθητοποίηση του κοινού απέναντι σε αυτές, ειδικότερα για θέματα Ασφάλειας Πληροφοριών.

Πιο συγκεκριμένα, η διπλωματική εργασία απαρτίζεται από δύο κύρια μέρη. Το πρώτο μέρος αφορά τη θεωρητική προσέγγιση του φαινομένου της Κοινωνικής Μηχανικής και συγκεκριμένα του Phishing και το δεύτερο, την πρακτική εφαρμογή Phishing προσομοιώσεων σε επιλεγμένους στόχους στα πλαίσια διεξαγωγής εκπαιδευτικού προγράμματος Cyber Security Awareness. Το θεωρητικό υπόβαθρο περιλαμβάνει εννέα κεφάλαια. Σε αυτά με την σειρά τους αναλύονται οι έννοιες οι ορισμοί και η ιστορία του Social Engineering καθώς και ο κύκλος ζωής του δηλαδή τα στάδια που το αποτελούν και πως αυτά είναι αλληλεπιδρούν. Στη συνέχεια θα γίνει αναφορά στο κομμάτι της ανθρώπινης ψυχολογίας και στο τι είναι αυτό που μας καθιστά επιρρεπή ως άτομα σε τέτοιας μορφής άπατες.

Στο πέμπτο κεφάλαιο, παρουσιάζονται εκτενώς οι πιο διαδεδομένες μορφές απάτης που αξιοποιούν τεχνικές Κοινωνικής Μηχανικής, μαζί τον τρόπο που αυτές μπορούν

δυνητικά να στραφούν ενάντια σε έναν προσωπικό ή εταιρικό υπολογιστικό σύστημα του χρήστη. Στο έκτο κεφάλαιο, γίνεται μια αναλυτική αναφορά στο φαινόμενο του Phishing και παρουσιάζονται πληροφορίες σχετικά με τους τρόπους που μπορεί να εφαρμοστεί, τα διαφορετικά ήδη επιθέσεων που έχουν κάνει την εμφάνιση τους κατά τα χρόνια και το πως αυτές οι επιθέσεις είναι σχεδιασμένες για να στοχεύουν ένα μεγάλο εύρος διαφορετικών χρηστών.

Οι κοινές πρακτικές και τεχνικές που αξιοποιεί ένας επιτιθέμενος για να οργανώσει και να φέρει εις πέρας μια τέτοια επίθεση αναλύονται στο επόμενο κεφάλαιο της διπλωματικής εργασίας. Σε συνέχεια των πρακτικών και τεχνικών, το όγδοο κεφάλαιο είναι αφιερωμένο στην παρουσίαση των εργαλείων που μπορεί να αξιοποιήσει κάποιος κακόβουλος χρήστης για να υλοποιήσει μια επίθεση αλλά και των εργαλείων τα οποία θεωρούνται λιγότερο «κακόβουλα» και χρησιμοποιούνται για προσομοιώσεις και εκπαιδευτικούς σκοπούς. Τέλος στο ένατο κεφάλαιο παρουσιάζονται τομείς που μπορούμε να επικεντρωθούμε για να οχυρώσουμε το προσωπικό ενός οργανισμού και να συμβάλουμε στην καλύτερη αντιμετώπιση τέτοιων επιθέσεων.

Στο δεύτερο μέρος είναι αφιερωμένο εξ ολοκλήρου στην οργάνωση και διεξαγωγή πραγματικών καμπανιών Phishing στα πλαίσια μιας επιχείρησης, Θα δοκιμαστούν τρία διάφορα διαφορετικά σενάρια βασιζόμενοι στην θεωρία της ανθρώπινης συμπεριφοράς η οποία αναφέρθηκε στο πρώτο μέρος και θα προσπαθήσουμε να εξάγουμε συμπεράσματα για το τι πραγματικά καθιστά μια επίθεση πετυχημένη.

Περιεχόμενα

ΜΕΡΟΣ Ι 9
1. Εισαγωγή 9
2. Κοινωνική Μηχανική (Social Engineering) 11
3. Κύκλος ζωής της κοινωνικής μηχανικής 13
3.1 Footprinting 13
3.2 Establishing Trust 15
3.3 Psychological Manipulation 15
3.4 The Exit 16
4. Ο ρόλος της Ανθρώπινης συμπεριφοράς 17
4.1 Εξουσία 20
4.2 Κοινωνική αποδοχή 21
4.3 Διαπροσωπικές σχέσεις 22
4.4 Υποχρέωση 23
5. Τεχνικές Social Engineering 25
5.1 Shoulder Surfing 26
5.2 Dumpster Diving 26
5.3 Εξαπάτηση και Role Playing 27
5.4 Κακόβουλο λογισμικό – Trojan Horses 28
5.5 Μηχανές Αναζήτησης 28
5.6 Αντίστροφη Κοινωνική Μηχανική 28
6. Ηλεκτρονικό «Ψάρεμα» - Phishing 30
6.1 Mass Phishing 31
6.2 Whaling 31
6.3 Clone Phishing 32
6.4 Spear Phishing 33
6.5 Phishing Variations 34
7. Τα «όπλα» των επιτιθέμενων 35
7.1 Παραποίηση Συνδέσμων (Hyperlink Manipulation) 35
7.2 Παράκαμψη φίλτρων 37
7.3 Πλαστογράφηση έγκυρων ιστοσελίδων. 38
7.4 Phishing Mules 39
8. Εργαλεία, Λογισμικό και έτοιμες λύσεις 41
8.1 Εργαλεία για Επίθεση 41
8.1.1 Social Engineering Toolkit (SET) 41
8.1.2 ShellPhish 44
8.1.3 Hiddeneye 45
8.2 Εργαλεία για Εκπαιδευτικούς Σκοπούς 47

8.2.1 Basic Tools 48
8.2.2 Open Source Πλατφόρμες 48
8.2.3 Demo εκδοχές εμπορικών προϊόντων 50
9. Τρόποι και μηχανισμοί άμυνας 54
9.1 Σταθερά Θεμέλια: Πολιτική Ασφάλειας 54
9.2 Ευαισθητοποίηση και Εκπαίδευση 55
9.2.1 Εκπαίδευση ευαισθητοποίησης ασφάλειας για όλους τους χρήστες 55
9.2.2 Επιπλέον ενίσχυση Προσωπικού σε κομβικές θέσεις 57
9.3 Φυσική Ασφάλεια 59
9.4 Background Checks 60
9.5 Ελαχιστοποίηση διαρροής δεδομένων 60
9.6 Διαβάθμιση Ασφάλειας 61
9.7 .Πρόσθετα μέτρα ενίσχυσης 61
Μέρος ΙΙ 64
1. Μελέτη σε πραγματικές συνθήκες. 64
1.1 Η Εταιρία 64
1.2 Συνοπτική περιγραφή πειράματος 65
2. Καμπάνια Phishing 1 - Αρχική Αξιολόγηση 66
2.1 Προγραμματισμός Καμπάνιας 66
2.2 Πίνακας Περιγραφής Σεναρίου 66
3. Καμπάνια Phishing 2 - Διερεύνηση της Έλξης 68
3.1 Προγραμματισμός Καμπάνιας 68
3.2 Πίνακας Περιγραφής Σεναρίου 69
4. Καμπάνια Phishing 3 - Διερεύνηση της Οικειότητας 72
4.1 Προγραμματισμός Καμπάνιας 73
4.2 Πίνακας Περιγραφής Σεναρίου 74
5. Παρουσίαση Αποτελεσμάτων και Συμπεράσματα 77
5.1 Αποτελέσματα – Καμπάνια 1 77
5.2 Αποτελέσματα – Καμπάνια 2 79
5.3 Αποτελέσματα – Καμπάνια 3 81
5.4 Γενικές Παρατηρήσεις Μελέτης 83
6. Συμπεράσματα 84
Βιβλιογραφία 85

Πίνακας Εικόνων

Εικόνα 1 - Ο κύκλος ζωής μιας επίθεσης Social Engineering 13
Εικόνα 2 - Authoritive Figures | Ίσως μας κάνουν να νιώθουμε "μικροί" και αδυνατούμε να σκεφτούμε λογικά..... 20
Εικόνα 3 - Social Acceptance | Που θα φτάναμε για να γίνουμε αποδεκτοί από τους άλλους; 21
Εικόνα 4 - Υποχρέωση | Προσωπικές επιθυμίες ή συμμόρφωση; 24
Εικόνα 5 - Τεχνικές επιθέσεων Social Engineering 25
Εικόνα 6 - Στις επιθέσεις Shoulder Surfing η οθόνη και το πληκτρολόγιο είναι εκτεθειμένα 26
Εικόνα 7 - Ο επιτιθέμενος μπορεί να υποδυθεί πολλούς διαφορετικούς ρόλους..... 27
Εικόνα 8 - Ιεραρχία επιθέσεων Phishing..... 30
Εικόνα 9 - Whaling VS Traditional Phishing..... 32
Εικόνα 10 - Spear Phishing 33
Εικόνα 11 - Παραδείγματα IDN Spoofing | Πανομοιότυπα γράμματα άλλα διαφορετικό αλφάβητο..... 36
Εικόνα 12 - Παράδειγμα επίθεσης Phishing URL 37
Εικόνα 13 - Παράδειγμα επίθεσης Phishing Mule 40
Εικόνα 14 - Εργαλείο SET | Περιβάλλον χρήσης 42
Εικόνα 15 - Εργαλείο SET | Υπόδειγμα επίθεσης..... 43
Εικόνα 16 - Εργαλείο ShellPhish | Μενού επιλογών..... 44
Εικόνα 17 - Εργαλείο ShellPhish | Υπόδειγμα αποτελεσμάτων επίθεσης 45
Εικόνα 18 - Εργαλείο Hiddeneye | Περιβάλλον χρήσης 46
Εικόνα 19 - Εργαλείο Hiddeneye | Περιβάλλον χρήσης (2)..... 46
Εικόνα 20 - Εργαλείο Hiddeneye | Υπόδειγμα επίθεσης..... 47
Εικόνα 21 - Εργαλείο GoPhish | Περιβάλλον χρήσης..... 49
Εικόνα 22 - Εργαλείο Phishing Frenzy| Περιβάλλον χρήσης 50
Εικόνα 23 - Εργαλείο Lucy | Περιβάλλον χρήσης 51
Εικόνα 24 - Εργαλειο Phish Insight | Συλλογη Templates..... 52
Εικόνα 25 - Εργαλείο Phish Insight | Εκπαιδευτικές επιλογές και feedback χρηστών 53

ΜΕΡΟΣ Ι

1. Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο αποτελεί ένα ζήτημα το οποίο καθίσταται όλο και πιο σοβαρό για ολόκληρο τον κόσμο, με εισβολείς που επιτίθενται σε μικρές και μεγάλου μεγέθους εταιρίες και οργανισμούς με το κίνητρο να αποκτήσουν πρόσβαση σε απόρρητες πληροφορίες και απόρρητο περιεχόμενο. Σύμφωνα με έρευνα της CSI για την ηλεκτρονική εγκληματικότητα και την ασφάλεια συστημάτων, ήδη από την περίοδο 2010-2011, σχεδόν οι μισοί από τους συμμετέχοντες ανέφεραν πως έχει υποπέσει στην αντίληψη τους κάποιο περιστατικό ασφάλειας, με το 45,6% να αναφέρει ότι είχαν υπάρξει δέκτες τουλάχιστον μιας στοχευμένης επίθεση.

Με την ανάπτυξη των τεχνολογιών τα τελευταία χρόνια και βλέποντας μια μεγάλη στροφή των ειδικών πληροφορικής σε θέματα Ασφάλειας Πληροφοριών γίνεται εύκολα αντιληπτό πως προσπαθώντας να αποτρέψουμε τις απειλές σε τεχνικό επίπεδο και αγνοώντας το φυσικό-κοινωνικό επίπεδο, δηλαδή τον παράγοντα της ανθρώπινης συμπεριφοράς, δεν μπορεί ποτέ να επιτευχθεί η απόλυτη ασφάλεια.

Δύο ενδεικτικά παραδείγματα του πόσο μπορεί μια επίθεση Κοινωνικής Μηχανικής να απέχει από τεχνικά μέσα είναι:

- Το φαινόμενο κατά το όποιο οι επιτιθέμενοι καταφεύγουν στο να ψάχνουν ακόμα και τους κάδους απορριμμάτων μιας εταιρίας - στόχου (Dumpster Diving) προκειμένου να αποκτήσουν ευαίσθητες πληροφορίες (πχ οικονομικά στοιχεία) από έγγραφα και εκτυπώσεις που έχουν απορριφθεί από τους υπαλλήλους.
- Τη σκηνή από τα παιχνίδια πολέμου όπου ο χαρακτήρας του Matthew Broderick μελέτησε τον στόχο του σε προσωπικό επίπεδο προτού επιχειρήσει να σπάσει τον κωδικό του στρατιωτικού συστήματος πληροφορικής.

Η Κοινωνική Μηχανική είναι μια απειλή που παραβλέπεται στις περισσότερες οργανώσεις, αλλά μπορεί εύκολα να αξιοποιηθεί καθώς εκμεταλλεύεται την ανθρώπινη ψυχολογία και όχι απαραίτητα ευπάθειες ή αδυναμίες στα τεχνικά μέτρα που προστατεύουν τα πληροφοριακά σύστημα.

Παρακάτω παρατίθεται ένα συνηθισμένο παράδειγμα του γεγονότος αυτού:

Ένα άτομο λαμβάνει ένα μήνυμα στην επαγγελματική διεύθυνση ηλεκτρονικού ταχυδρομείου του αναφέροντας ότι ο υπολογιστής του έχει μολυνθεί από ιό. Το μήνυμα περιέχει έναν σύνδεσμο και υποδεικνύει ότι ο παραλήπτες θα πρέπει να κατεβάσει και να εγκαταστήσει το εργαλείο από το σύνδεσμο για να αφαιρέσει τον ιό από τον υπολογιστή του. Το άτομο που βρίσκεται σε κατάσταση σύγχυσης ακολουθεί στον σύνδεσμο για να αφαιρέσει τον ιό, αλλά στην πραγματικότητα, χωρίς φυσικά να το αντιλαμβάνεται, δίνει στον επιτιθέμενο πρόσβαση στον υπολογιστή του και στη συνέχεια μια εύκολη είσοδο στο εταιρικό δίκτυο.

Για να διασφαλιστεί η πλήρης ασφάλεια ενός οργανισμού από κάθε είδους εσωτερικούς και εξωτερικούς παράγοντες, ο Υπεύθυνος Ασφάλειας Πληροφοριών πρέπει να έχει πλήρη γνώση του κύκλου ζωής της Κοινωνικής Μηχανικής, των τεχνικών που μπορεί να χρησιμοποιηθεί από έναν εισβολέα και των διαθέσιμων αντίμετρων για τη μείωση της πιθανότητας επιτυχίας της επίθεσης.

2. Κοινωνική Μηχανική (Social Engineering)

Κατά καιρούς αρκετοί επιστήμονες και μελετητές έχουν αποδώσει την έννοια της Κοινωνικής Μηχανικής με ορισμούς που εξυπηρετούν το εκάστοτε γνωστικό αντικείμενο το οποίο καλούνται να εκπροσωπήσουν. Έτσι, ενδεικτικά, μελετώντας το συγκεκριμένο ζήτημα μπορεί κανείς να συναντήσει τους εξής ορισμούς:

- «Η κοινωνική μηχανική αναφέρεται στις προσπάθειες ενός ατόμου η μιας ομάδας ατόμων να επηρεάσει τις προσωπικές και τις κοινωνικές συμπεριφορές σε μεγάλη κλίμακα, είτε με αξιοποίηση κυβερνητικών δομών, ή μέσων μαζικής ενημέρωσης ή ακόμα και μέσα από θρησκευτικές η ιδιωτικές ομάδες, προκειμένου να προάγουν επιθυμητές συμπεριφορές σε έναν πληθυσμό-στόχο.» (Κοινωνιολογία) (1)
- «Η κοινωνική μηχανική μπορεί να κατανοηθεί φιλοσοφικά ως ένα ντετερμινιστικό φαινόμενο όπου πραγματοποιούνται οι προθέσεις και οι στόχοι των ηγετών-δημιουργών μιας νέας κοινωνικής δομής.» (Φιλοσοφία)
- Ο Roscoe Pound, Νομικός μελετητής και ακαδημαϊκός εκπαιδευτικός, αναφέρει «Ο νόμος είναι μια μορφή κοινωνικής μηχανικής καθώς αποσκοπεί στην ισορροπία μεταξύ των ανταγωνιστικών συμφερόντων στην κοινωνία». Σύμφωνα με αυτό, η εφαρμοσμένη Νομική επιστήμη χρησιμοποιείται για την επίλυση ατομικών και κοινωνικών προβλημάτων υποχρεώνοντας έτσι άτομα η ομάδες ατόμων να προσαρμόσουν την συμπεριφορά τους και να συμμορφωθούν με νόμους. (Νομική) (2)
- «Στον τομέα της ψυχικής υγείας κλάδοι όπως αυτός της κοινωνικής ψυχολογίας αναφέρονται σε τεχνικές κοινωνικής μηχανικής με βάση τις οποίες μπορούν να προξενήσουν αλλαγές στην ζωή των ασθενών, ενισχύοντας θετικές συμπεριφορές, με το να διαμορφώνουν κατάλληλα το κοινωνικό περιβάλλον τους.» (Ψυχολογία) (3)

Ο κοινός παρονομαστής σε όλες τις παραπάνω διαφορετικές ερμηνείες είναι η πρόκληση της αλλαγής συμπεριφοράς, η απόκλιση από έναν γενικευμένο και αναμενόμενο σύνολο αντίδρασης και τέλος η υποκίνηση ενεργειών που ο αποδέκτης πιθανότατα δε θα πραγματοποιούσε χωρίς εξωτερική παρέμβαση. Αυτή ακριβώς η φύση της κοινωνικής μηχανικής είναι ο λόγος που έχει κινήσει το ιδιαίτερα αυξανόμενο ενδιαφέρον της επιστημονικής και ακαδημαϊκής κοινότητάς καθώς για την αποτελεσματική εφαρμογή της απαιτείται η συνύπαρξή και ο συνδυασμός πολλών διαφορετικών συστατικών στοιχείων συχνά προερχομένων από διαφορετικούς γνωστικούς τομείς.

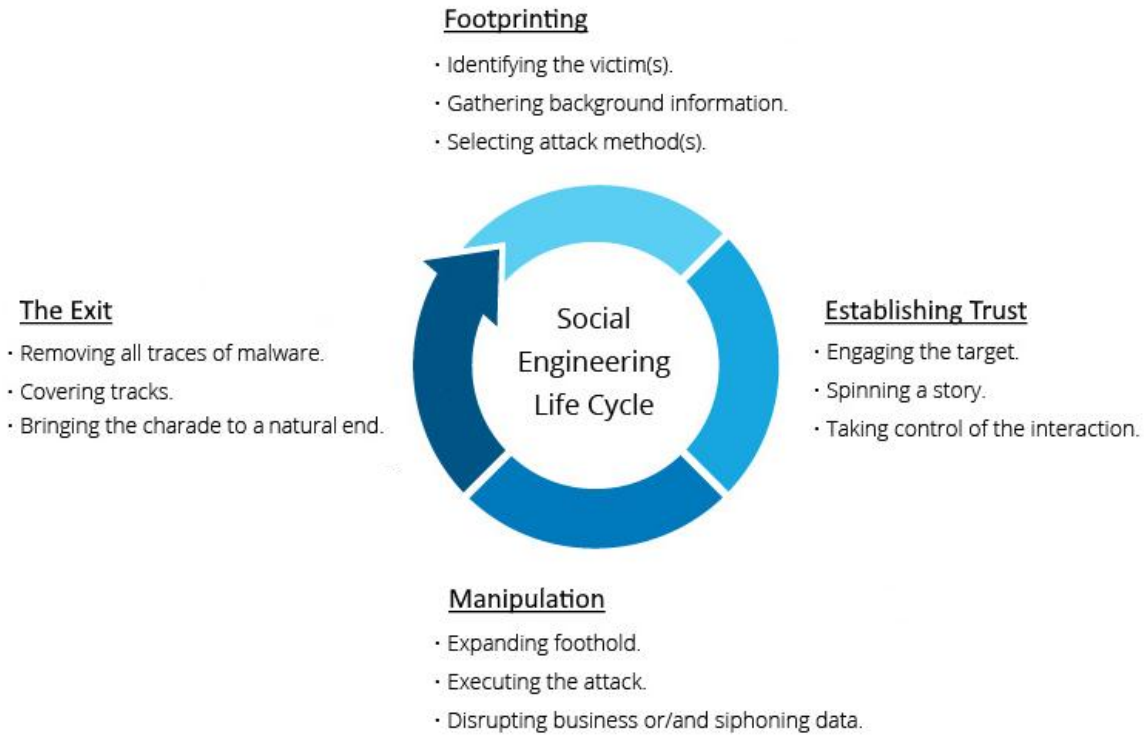
Στην Ασφάλεια Πληροφοριών ως περιστατικό Κοινωνικής Μηχανικής μπορεί να θεωρηθεί οποιαδήποτε πράξη χειραγώγησης ενός ατόμου με σκοπό την άμεση η έμμεση απόσπαση πληροφοριών. Η διαφορά με τις περιπτώσεις απλής απατής έγκειται στο ότι η συγκεκριμένη ορολογία είναι σε μεγάλο βαθμό συνδεδεμένη με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα.

Για την επικράτηση του όρου υπεύθυνος είναι ο Kevin David Mitnick ο οποίος αρχικά από την πλευρά του επιτιθέμενου αξιοποίησε τέτοιες τεχνικές για να αποσπάσει ευαίσθητες πληροφορίες και να αποκτήσει πρόσβαση σε απόρρητα συστήματα. Ο ίδιος διέδωσε τον όρο κοινωνική μηχανική αργότερα στην ζωή του έχοντας πλέον βρεθεί στο αντίθετο στρατόπεδο από αυτό του επιτιθέμενου, εργαζόμενος ως σύμβουλος για θέματα Ασφάλειας Πληροφοριών, υποστηρίζοντας ότι είναι πολύ πιο εύκολο να ξεγελάσεις κάποιο άτομο προκειμένου να αποκαλύψει τον κωδικό πρόσβασής του από το να προσπαθήσεις να τον «σπάσεις» με τεχνικά μέσα. (4)

Σε αυτή την ενότητα θα μελετηθούν επιμέρους παράμετροι όπως ο κύκλο ζωής της Κοινωνικής Μηχανικής, οι διάφορες τεχνικές που χρησιμοποιούνται, οι ψυχολογικές βάσεις πάνω στις οποίες στηρίζονται οι επιθέσεις καθώς και κατηγορίες επιθέσεων για να γίνει αντιληπτό το πως ένας επιτιθέμενος μπορεί να αξιοποιήσει στο μέγιστο τα εργαλεία που υπάρχουν διαθέσιμα έτσι ώστε να πραγματοποιήσει μια επίθεση.

3. Κύκλος ζωής της κοινωνικής μηχανικής

Κάθε επίθεση Κοινωνικής Μηχανικής είναι μοναδική, αλλά εξετάζοντας προσεκτικά τις διαφορετικές αυτές περιπτώσεις (υπαρκτές επιθέσεις και case scenarios) μπορούμε να αρχίσουμε να δομούμε μια απεικόνιση όλων των δραστηριοτήτων που αποτελούν μια τέτοια επίθεση. (5)



Εικόνα 1 - Ο κύκλος ζωής μιας επίθεσης Social Engineering

3.1 Footprinting

Το πρώτο και βασικότερο βήμα στην σχεδίαση μιας επίθεσης Social Engineering είναι η συλλογή πληροφοριών σχετικά με τους στόχους και το περιβάλλον το οποίο τους συναποτελεί. Η αποτύπωση αυτών των πληροφοριών μπορεί να αποκαλύψει τα άτομα που σχετίζονται με τον στόχο, τον τρόπο με τον οποίο αυτά τα άτομα συνδέονται και μοτίβα ή συνήθειες που συνδέονται με την συμπεριφορά τους. Η

αποτελεσματική αξιοποίηση τέτοιων στοιχείων είναι τόσο κρίσιμη που μπορεί από μόνη της να συμβάλει δραματικά στην επιτυχία των στόχων μιας επίθεσης.

Η συλλογή πληροφοριών κατά τη διάρκεια της φάσης Footprinting που σχετίζεται με τα άτομα - στόχους μπορεί να περιλαμβάνει ενδεικτικά:

- Κατάλογος των ονομάτων και των τηλεφωνικών αριθμών των εργαζομένων μιας εταιρίας.
- Εταιρικοί λογαριασμοί email.
- Λογαριασμούς υπαλλήλων της εταιρίας σε Social Media πλατφόρμες
- Οργανόγραμμα της Εταιρίας
- Πληροφορίες για την οργανωτική διάρθρωση μιας εταιρίας
- Πληροφορίες φυσικής τοποθεσίας
- Πληροφορίες εξωτερικής επικοινωνίας, προγραμμάτων και ρουτινών συνεργατών

Επιπλέον το στάδιο αυτό μπορεί να συμπεριλάβει και τα πληροφοριακά συστήματα, λαμβάνοντας πάντα υπ' όψιν τον τελικό στόχο της επίθεσης. Ενδεικτικά σε αυτή την περίπτωση μπορεί να έχουμε:

- Καταγραφή δομής εταιρικού δικτύου.
- Αναγνώριση θυρών δικτύου προσβάσιμες από το διαδίκτυο
- Πληροφορίες σχετικά με εταιρικά λογισμικά(λειτουργικά συστήματα σταθμών εργασίας υπαλλήλων, servers OS κ.α)
- Πληροφορίες σχετικά με λογισμικά ασφάλειας προκειμένου να σχεδιαστεί κάποια στρατηγική για την αποφυγή τους.
- Ρόλους και οντότητες στο domain της εταιρίας καθώς και πληροφορίες για δικαιώματα χρηστών και κοινόχρηστους φακέλους.

Το Footprinting γενικά αποτελεί μία από τις πρώιμες φάσης της επίθεσης, δηλαδή ανήκει στις πιθανές εργασίες που εκτελούνται πριν από την πραγματοποίηση της.

3.2 Establishing Trust

Εξίσου σημαντικό με το προηγούμενο στάδιο αποτελεί και το στάδιο κατά το οποίο ο επιτιθέμενος καλείται να αναπτύξει μια ισχυρή σχέση με τον στόχο – θύμα. Η καθιέρωση σχέσεων εμπιστοσύνης μπορεί να συμβαδίζει με το στάδιο συλλογής πληροφοριών, το οποίο περιγράφηκε προηγουμένως, η ακόμα να αποτελέσει και μέσο για την διείσδυση ενός επιτιθέμενου σε έναν οργανισμό.

Η ισχυρή αυτή σχέση και κατ' επέκταση η εμπιστοσύνη που κερδίζει ο επιτιθέμενος θα χρησιμοποιηθούν αργότερα για την αποκάλυψη εμπιστευτικών πληροφοριών που θα μπορούσαν να προκαλέσουν διαρροή ευαίσθητων δεδομένων ή και ακόμα να συντελέσουν στην απόκτηση πρόσβασης σε απόρρητα συστήματα.

3.3 Psychological Manipulation

Σε αυτό το βήμα, ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη που έχει κερδίσει στην προηγούμενη φάση έτσι ώστε να εξαγάγει όσες περισσότερες εμπιστευτικές πληροφορίες ή και να αποκτήσει πρόσβαση σε λειτουργίες που σχετίζονται με το σύστημα που στοχοποιείται και τις οποίες υπό κανονικές συνθήκες εκτελεί ο ίδιος ο υπάλληλος έτσι ώστε να εισχωρήσει στο σύστημα με μεγάλη ευκολία. Συχνά εδώ μπορούν να εφαρμοστούν ψυχολογικά «τρικ» όπως για παράδειγμα απόσπαση προσοχής η φόβος τα οποία είναι σαφώς πιο αποτελεσματικά εάν έχει προϋπάρξει η δόμηση μιας σχέσης μεταξά εμπιστοσύνης μεταξύ επιτιθεμένου και θύματος.

Αφού συλλεχθούν όλες οι απαιτούμενες ευαίσθητες πληροφορίες, είναι αρκετά συχνό το φαινόμενο κατά το οποίο ο επιτιθέμενος χρησιμοποιεί την γνώση που αποκόμισε για να προχωρήσει στον επόμενο στόχο μέχρι να βρει άμεσα τις πληροφορίες η να αποκτήσει την πρόσβαση ου επιθυμεί. ή να κινηθεί προς εκμετάλλευση του υπό εξέταση συστήματος. Σε αντίθετη περίπτωση ο επιτιθέμενος μπορεί να προσχωρήσει στην εκμετάλλευση του συστήματος που στοχοποίησε.

3.4 The Exit

Τώρα, αφού έχουν εξαχθεί όλες οι επιθυμητές πληροφορίες ή αφού έχει εξασφαλιστεί η απόκτηση πρόσβασης στα στοχοποιημένα συστήματα, ο επιτιθέμενος πρέπει να πραγματοποιήσει μια απρόσκοπτη έξοδο από το σενάριο της επίθεσης. Πιο συγκεκριμένα ο επιτιθέμενος, ιδανικά, επιθυμεί το τέλος της επίθεσης να μην μπορεί να συσχετιστεί σε καμία περίπτωση με οποιαδήποτε κακόβουλη ενέργεια και στοχεύει συνήθως στο να εκτρέψει κάθε είδους υποψία προς το άτομό του.

Εξασφαλίζει ότι δεν αφήνει κανένα είδος απόδειξης της επίσκεψής του, εάν πρόκειται για κάποιο σενάριο επίθεσης που απαιτεί φυσική παρουσία, η οποία θα μπορούσε να οδηγήσει σε αποκάλυψη της πραγματικής του ταυτότητας.

Σε διαφορετική περίπτωση, όταν δηλαδή απαιτείται η μη εξουσιοδοτημένη πρόσβαση σε κάποιο σύστημα, ο επιτιθέμενος ιδανικά επιθυμεί να μην υπάρξει καμία αναφορά η αποδεικτικό που να σχετίζεται με την μη εξουσιοδοτημένη πρόσβαση η οποιαδήποτε κακόβουλη ενέργεια πραγματοποιήθηκε στο εκτεθειμένο πλέον σύστημα στο μέλλον. Η ίδια βασική αρχή ακολουθείται και στις περιπτώσεις επιθέσεων που δεν είναι απαραίτητη η φυσική παρουσία του κακόβουλου χρήστη.

4. Ο ρόλος της Ανθρώπινης συμπεριφοράς

Σύμφωνα με τον Rusch (1999), υπάρχουν δύο βασικές κατηγορίες τρόπων με τους οποίους μπορούμε να επηρεάσουμε – χειραγωγήσουμε ένα άτομο:

- Μια άμεση προσέγγιση που στηρίζεται στην ορθή και αναλυτική συλλογιστική των δεδομένων τα οποία έχει στην διάθεση του το ατόμου και τα οποία προκύπτουν από γεγονότα. Ουσιαστικά πρόκειται για οτιδήποτε ένα άτομο μπορεί να δει, να ακούσει η να γνωρίζει και συνεπώς να σχηματίσει συσχετισμούς οι οποίοι θα οδηγήσουν σε αξιόπιστα, στιβαρά συμπεράσματα.
  Για παράδειγμα το να γνωρίζει κανείς τους κανόνες που θα πρέπει να ακολουθήσει κατά την είσοδο ενός επισκέπτη σε μία εταιρία (γνώση) ή το να είναι σε θέση να αναγνωρίσει αποτελεσματικά τον συνομιλητή του (υπαρκτή και καταχωρημένη πληροφορία).

- Μια πλάγια προσέγγιση που βασίζεται στην αποδοχή εμμέσων και γενικευμένων μηνυμάτων από τον αποδέκτη χωρίς την βαθιά ανάλυση και κατανόηση των γεγονότων, ενεργοποιώντας νοητικές παρακάμψεις (shortcuts) στην συλλογιστική πορεία του ατόμου προκαλώντας συναισθήματα.
  Πρόκειται για τις περιπτώσεις που το άτομο δεν μπορεί να είναι σίγουρο για την ορθότητα των πράξεων του και συνοδεύεται από αίσθημα αβεβαιότητας, υποχρέωσης κτλ.
  Για παράδειγμα τον τρόπο που ενεργεί κανείς υπό πίεση (αβεβαιότητα) η υπό τον φόβο επιβολής κυρώσεων (υποχρέωση).

Φυσικά, στην περίπτωση που κάποιος κακόβουλος χρήστης επιλέξει να αξιοποιήσει κάποια τεχνική Social Engineering για να οργανώσει μια επίθεση η άμεση προσέγγιση δεν αποτελεί εύκολη επιλογή. Αντίθετα θα επιδιώξει να αξιοποιήσει πλάγια μέσα για να εξαπατήσει το θύμα του και να εξάγει πληροφορίες η να προκαλέσει σύγχυση και να παραπλανήσει το θύμα στην ολοκλήρωση μη αναμενόμενων ενεργειών. (6)

Ο Gragg (2003) ανέλυσε τη βιβλιογραφία για την πειθώ, την επιρροή και την κοινωνική μηχανική και πρότεινε επτά ψυχολογικούς παράγοντες που αναφέρονται ρητά ως εφαρμοστέοι σε αντίστοιχες περιπτώσεις. (7)

Ο Scheeres (2008) έχει συμπεράνει πως οι επτά αυτοί παράγοντες του Gragg είναι σύμφωνοι με τις αρχές του Robert Cialdini (2009). Αυτό σημαίνει ότι το αποτέλεσμα των ερευνών του Cialdini για την ψυχολογία ισχύουν και για την Κοινωνική Μηχανική ενισχύοντας την παραδοχή πως οι δυο αυτές «επιστήμες» είναι αλληλένδετες. Επιπλέον, είναι γενικά αποδεκτό ότι οι ίδιες ψυχολογικές τεχνικές εφαρμόζονται στην Κοινωνική Μηχανική όπως στις παραδοσιακές μορφές απάτης (Rusch, 1999). Ως εκ τούτου, οι Stajano και Wilson (2011) εντόπισαν επτά ψυχολογικές αρχές χειραγωγησης που πραγματικά εφαρμόζονται και στην Κοινωνική Μηχανική. (8)

Αυτοί οι ψυχολογικοί μηχανισμοί ή παράγοντες μπορούν να περιγραφούν συνοπτικά στον παρακάτω πίνακα:

Ψυχολογικός Παράγοντας	**Περιγραφή**
Εξουσία	• Προγραμματισμός για υπακοή σε πρόσωπα που επιβάλουν πειθαρχία (authoritive figures). • Φόβος για πιθανές ποινές μη συμμόρφωσης. • Ευφορία, ανακούφιση, περηφάνια και αίσθημα ικανοποίησης προερχόμενο από την υπακοή και την συμμόρφωση.
Κοινωνική Αποδοχή (η επιβεβαίωση της αγέλης)	• Η εμπιστοσύνη στην προφανή συμπεριφορά της πλειοψηφίας και ο καθορισμός της κατάλληλης συμπεριφοράς σε ατομικό επίπεδο με βάση αυτή. • Αλλαγή συμπεριφοράς συμφώνα με την πλειοψηφία ακόμα και αν οδηγήσει σε αρνητικές επιπτώσεις.
Διαπροσωπικές σχέσεις (Συμπάθεια, προτίμηση, ομοιότητα, έλξη)	• Φιλοφρονήσεις και κομπλιμέντα δημιουργούν θετικά συναισθήματα στον δεκτή. • Έλξη – Ελκυστικά πρόσωπα η καταστάσεις είναι σε γενικές γραμμές πιο προσιτά και επιθυμητά.

	• Η ομοιότητα και καθετί γνώριμο ορίζει ασυνείδητα πως το πρόσωπο απέναντι μας θα συμπεριφερθεί όπως εμείς. Αναμένουμε αντίστοιχες συμπεριφορές και πράξεις από άτομα που μας μοιάζουν. • Το φαινόμενου του φωτοστέφανου – Όταν ένα βασικό χαρακτηριστικό ενός ατόμου (εξωτερική εμφάνιση) είναι αρκετό για να θολώσει την κρίση και να επισκιάσει όλα τα υπόλοιπα γνωρίσματα του.
Υποχρέωση (Δέσμευση, ανταπόδοση και συνέπεια)	• Ικανοποίηση των προσδοκιών. Αίσθημα ανικανότητας, απογοήτευσης ή ντροπής αν δεν σταθούμε αντάξιοι των περιστάσεων. • Θετικά συναισθήματα στις περιπτώσεις που ανταποκριθούμε σε μια υπόσχεση η δέσμευση.
Αποδιοργάνωση και αντιπερισπασμός	• Μειωμένη προσοχή δίνεται συχνά σε σημαντικές διεργασίες και πράξεις όταν αυτές είναι επαναλαμβανόμενες η δεν συνάδουν με τα προσωπικά μας ενδιαφέροντα. • Απόσπαση προσοχής με χρήση τεχνασμάτων όπως ο αντιπερισπασμός. Το άτομο θα ενδιαφερθεί άμεσα για κάτι παράξενο, παράδοξο, η εκτός της καθημερινής του ρουτίνας η για κάτι που συμβαδίζει με τα προσωπικά του γούστα.

4.1 Εξουσία

Σύμφωνα με τον Robert Cialdini η κοινωνία εκπαιδεύει τους ανθρώπους στο να μην αμφισβητούν την εξουσία προγραμματίζοντας τους έτσι ώστε να ανταποκρίνονται σε αυτήν χωρίς να την αμφισβητούν. Πράγματι, ιστορικά, η συμμόρφωση μας με τις επιθυμίες και τις διαταγές ατόμων που εκπροσωπούν την επιβολή εξουσίας έχει αποδειχθεί ωφέλιμη. Αρχικά ως φιγούρες εξουσίας για όλους μας μπορούν να θεωρηθούν, σε πιο πρώιμα στάδια της ζωής μας, οι γονείς, οι δάσκαλοι και οι καθηγητές μας. Αργότερα τον ρόλο αυτό μπορούν να αναλάβουν συνεργάτες και προϊστάμενοι μας και άτομα που σχετίζονται με την επιβολή του νόμου.

Εικόνα 2 - Authoritive Figures | Ίσως μας κάνουν να νιώθουμε "μικροί" και αδυνατούμε να σκεφτούμε λογικά

Κάθε άτομο σε έναν βαθμό έστω και ασυνείδητα θεωρεί πως τα άτομα που κατέχουν αυτούς τους ρόλους χαρακτηρίζονται ως «αυθεντίες» στον εκάστοτε τομέα δραστηριοποίησης. Επιπλέον δεν πρέπει να παραβλέψουμε το γεγονός πως σε κάθε σχεδόν μορφή ανεπτυγμένης κοινωνίας αυτά τα πρόσωπα σχετίζονται άμεσα με τις έννοιες της ανταμοιβής και της τιμωρίας. Αυτό το μοτίβο συνεχίζει να μας ακολουθεί και στη ενήλικη ζωή του ατόμου ανεξάρτητα με τον τρόπο που η έννοια της εξουσίας μπορεί να εκφραστεί.

Από την πλειοψηφία των ατόμων θεωρείτε πρέπον να συμμορφωθούν στα αιτήματα και τις προσταγές κάποιου ανώτερου στην ιεραρχία και στον οποίο η εναντίωση θα μπορούσε να επιφέρει κυρώσεις. Επεκτείνοντας αυτές τις ιδέες, οι Stajano και Wilson

υποστήριξαν πως σε ανάλογες περιπτώσεις όχι μόνο δεν είναι εύκολο να εναντιωθεί κανείς σε μια φιγούρα εξουσίας, αλλά αντίθετα θα δράσει με αυθορμητισμό και αψηφώντας νοητικούς φραγμούς θεωρώντας πως πρόκειται για κάτι που του επιβάλλεται και νιώθοντας πως φέρει λιγότεροί μερίδιο ευθύνης.

4.2 Κοινωνική αποδοχή

Υπάρχουν πολλαπλές μελέτες που στηρίζουν πως οι άνθρωποι βασίζονται σε άλλους για να καθορίσουν τι είναι κατάλληλο και αποδεκτό σε οποιαδήποτε δεδομένη κατάσταση. Σύμφωνα με τον Cialdini (2009), η εμπειρία μας λέει να ενεργούμε σύμφωνα με τα κοινωνικά πρότυπα δηλαδή με βάση το τι θα ήταν κοινωνικά αποδεκτό και όχι το αντίθετο. Ειδικά όταν η αβεβαιότητα μιας κατάστασης καθιστά αδύνατο το να αντιδράσει κανείς, η συμπεριφορά της μάζας ή αλλιώς της αγέλης είναι ένα σημείο αναφοράς από το οποίο θα αντλήσει κανείς πληροφορίες και θα μιμηθεί.

Εικόνα 3 - Social Acceptance | Που θα φτάναμε για να γίνουμε αποδεκτοί από τους άλλους;

Όπως επεσήμανε ο Stajano και ο Wilson (2011) και ο Gragg (2003), η συμπεριφορά ανθρώπων όμοιων με εμάς δημιουργεί πιο ισχυρή την πεποίθηση ότι κάτι θεωρείται αποδεκτό. Πρόκειται ουσιαστικά για παρότρυνση σε μια συμπεριφορά ή ενέργεια συνυφασμένη με ένα αίσθημα εμπιστοσύνης και ασφάλειας για τη διεξαγωγή μιας κατά τα αλλά αμφισβητήσιμης ή αντίθετης με το προσωπικό συμφέρον δράσης.

"Οι άνθρωποι τείνουν να χαλαρώνουν τις άμυνες τους και την καχυποψία τους όταν όλοι οι άλλοι φαίνεται να μοιράζονται τις ίδιες σκέψεις και συμπεριφορές. Με αυτόν τον τρόπο οι άνθρωποι έστω και ασυνείδητα θεωρούν ότι δεν θα είναι αποκλειστικά υπεύθυνοι για τις πράξεις τους" (Cialdini, 2009).

4.3 Διαπροσωπικές σχέσεις

Οι άνθρωποι έχουν την τάση να υπομένουν συμπεριφορές, να συμμορφώνονται και γενικότερα να αντιδρούν θετικά όταν βρίσκονται απέναντι σε άτομα με τα οποία προϋπάρχει ή αναπτύσσεται μια, έστω και βασικής μορφής, διαπροσωπική σχέση. Παρόμοιες σχέσεις μπορούν να εκδηλωθούν και να ενισχυθούν μέσα από ένα μεγάλο εύρος μηχανισμών , σύμφωνα με τον Cialdini, όπως:

- **Έλξη**: Η φυσική ελκυστικότητα είναι ένα χαρακτηριστικό που συχνά συνδέεται από πολλούς, και τις περισσότερες φορές ασυνείδητα, με ένα "φωτοστέφανο". Ως εκ τούτου, οι άνθρωποι τείνουν να αποδίδουν ευνοϊκά γνωρίσματα όπως ευγένεια, ειλικρίνεια και αξιοπιστία σε ελκυστικά πρόσωπα και επομένως αντιμετωπίζουν αυτά τα άτομα ευνοϊκότερα.

- **Οικειότητα**: Η ύπαρξη ίδιων ή παρόμοιων χαρακτηριστικών με ένα άτομο ενθαρρύνει τους άλλους να ευνοούν αυτό το άτομο. Αυτή η ομοιότητα μπορεί να εκφραστεί με ένα ευρύ φάσμα χαρακτηριστικών, όπως όμοιες απόψεις, χαρακτηριστικά γνωρίσματα, προσωπικά συμφέροντα, υπόβαθρο, εμφάνιση κ.λπ. Είναι μια διαπίστωση εύκολα παρατηρίσιμη και στην καθημερινή μας ζωή, αρκεί να εξετάσουμε την ίδια μας την συμπεριφορά και το πώς φερόμαστε σε ανθρώπους με τους οποίους έχουμε αρκετά κοινά.

- **Επιβράβευση**: Οι άνθρωποι τείνουν να αντιδρούν θετικά σε εκδηλώσεις επιβράβευσης όπως επαίνους, επιδοκιμασίες ή γενικά φιλοφρονήσεις και μάλιστα επιζητούν παρόμοιες συμπεριφορές σε βαθμό τέτοιο ώστε να συμμορφώνονται στις επιθυμίες των άλλων πολλές φορές ακόμα και εις βάρος των προσωπικών τους επιθυμιών ή αξιών.

- **Επικοινωνία και Συνεργασία**: Η στάση και η συμπεριφορά μας, ιδιαίτερα οι ευνοϊκές, προς ένα άτομο επηρεάζεται από την έκθεση μας σε αυτό. Ως εκ τούτου, η εξοικείωση που προκαλείται από την διαπροσωπική επαφή συνήθως οδηγεί σε ένα πιο ευνοϊκό κλίμα επικοινωνίας. Αυτό μπορεί να αυξηθεί ακόμη και μέσω της αμοιβαίας συνεργασίας, κάτι που παρατηρείται συχνά μεταξύ συναδέλφων ή μαθητών μιας τάξης, ή της προσπάθειας δημιουργίας ενός αισθήματος ομαδικότητας ("εμείς" ή "εμάς" όπως επισημαίνει ο Gragg (2003)).

- **Προδιάθεση και Συσχέτιση**: Η απλή συσχέτιση με θετικά η αρνητικά γεγονότα επηρεάζει τον τρόπο που οι άνθρωποι αισθάνονται για κάποιον άλλον. Αρκεί λοιπόν οι ανάμιξη ενός τρίτου με θετικές η αρνητικές καταστάσεις για να προκαλέσει τα επιθυμητά αποτελέσματα (συμπάθεια η αντιπάθεια) (Lott and Lott, 1965).

4.4 Υποχρέωση

Το αίσθημα του να είναι κάποιος υποχρεωμένος αποτελεί έναν εξαιρετικά ισχυρό κινητήριο παράγοντα αφού μπορεί να επιφέρει στο άτομο το χρέος της δέσμευσης, συναισθήματα αμοιβαιότητας και ανάγκη για συνέπεια. Οι άνθρωποι αισθάνονται ότι είναι επιτακτικό να είναι συνεπείς όταν έχουν δεσμευτεί σε μια συγκεκριμένη πράξη. Ο Cialdini επιπλέον διατύπωσε την άποψη πως αυτή η τάση της ανθρώπινης συμπεριφοράς δεν μετριάζεται ακόμα και στις περιπτώσεις που η δέσμευση αφορά πράξεις που θέτουν σε κίνδυνο τα συμφέροντα του ίδιου του ατόμου. Η άποψη αυτή βρίσκει σύμφωνους και τους Stajano και Wilson (2011) και Gragg (2003), οι οποίοι επέκτειναν αυτή την διαπίστωση συμπληρώνοντας πως η «δέσμευση» μας για κάτι

μπορεί να είναι τοσο ισχυρή ώστε να οδηγήσει σε αψήφιση κανονισμών η ακόμα και παραβατικές πράξεις. (9)

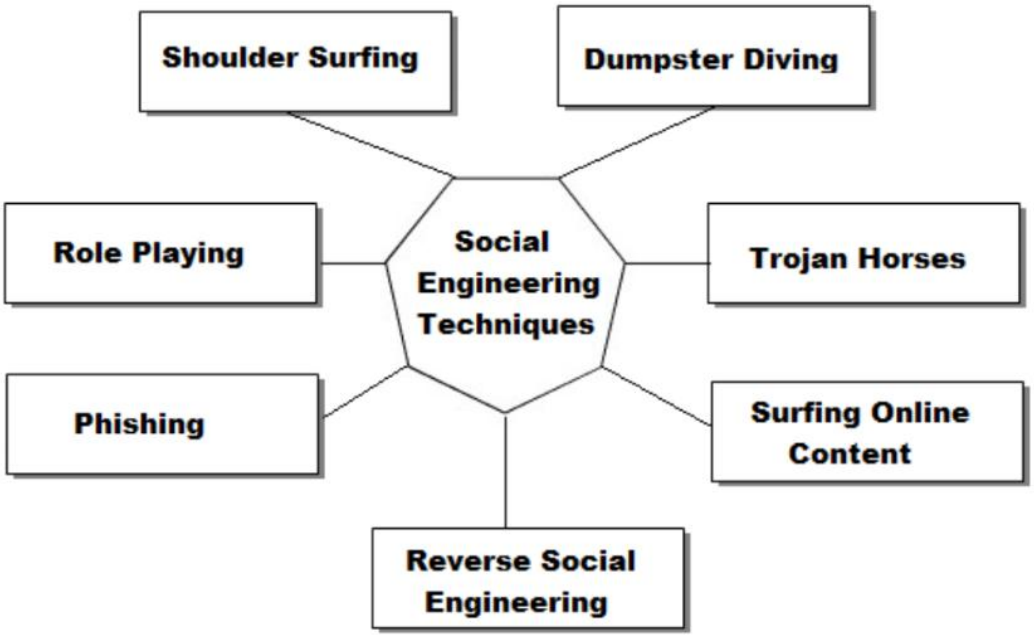
Σύμφωνα με τον Cialdini (2009), οι άνθρωποι αντιμετωπίζουν κοινωνικές και διαπροσωπικές πιέσεις για να παραμείνουν συνεπείς με μια προηγούμενη δέσμευση, αναγκάζοντάς τους να ενεργούν ανάλογα με την προηγούμενη δέσμευσή τους. Οι άνθρωποι τείνουν να υποβάλλονται σε δυσάρεστες καταστάσεις για να παραμείνουν συνεπείς (Rusch, 1999). Η διατήρηση της συνέπειάς θεωρείται στην πραγματικότητα ως βασικό χαρακτηριστικό της συμπεριφοράς του ανθρώπου, καθώς ανταμείβεται ιδιαίτερα στον πολιτισμό μας. Συνδέεται με ακεραιότητα, προσωπική και πνευματική δύναμη, ενώ αντίθετα, το χαρακτηριστικό της ασυνέπειας θεωρείται ως αναξιόπιστο και ως εκ τούτου ως ανεπιθύμητο γνώρισμα ενός ατόμου. Η συνέπεια παρέχει ευνοϊκό προσανατολισμό στη ζωή μας.

Όπως και με άλλες ανθρώπινες συμπεριφορές, οι οποίες ενισχύονται σημαντικά από κοινωνικά στερεότυπα, έτσι και στην περίπτωση της υποχρέωσης και της δέσμευσης επικρατεί μια προκατάληψη για άτομα τα οποία παίρνουν και δεν επιστρέφουν τίποτα καθιστώντας τα πιο επιρρεπή στο να κριθούν αρνητικά από τον κοινωνικό τους περίγυρο. Είναι λοιπόν εγγενής επιθυμία του ανθρώπου να προσπαθεί να το αποφύγει.

Εικόνα 4 - Υποχρέωση | Προσωπικές επιθυμίες ή συμμόρφωση;

5. Τεχνικές Social Engineering

Όλοι αυτοί οι παράγοντες που αναλύθηκαν παραπάνω μπορεί να βασίζονται σε πολλαπλούς ψυχολογικούς μηχανισμούς και ένστικτα άρρηκτα συνυφασμένα με την ανθρώπινη φύση, αυτό ωστόσο δεν σημαίνει πως απαιτείται ιδιαίτερη εξειδίκευση για να τα εκμεταλλευτεί κάποιος στην καθημερινότητα. Οι παραδοσιακές επιθέσεις οι οποίες στόχευαν στις πληροφοριακές υποδομές ενός οργανισμού τείνουν να αντικαθίστανται με νέες προσεκτικά σχεδιασμένες επιθέσεις που στο στόχαστρο τους έχουν τα άτομα που πλαισιώνουν αυτόν τον οργανισμό. Επιθέσεις που βασίζονταν στο να «σπάσουν» κωδικούς πρόσβασης δοκιμάζοντας όλους τους πιθανούς συνδυασμούς πλέον έχουν στραφεί στο πώς θα «μαντέψουν» ή ακόμα στο πως θα αποσπάσουν οι επιτιθέμενοι τον κωδικό πρόσβασης από έναν έγκυρο χρήστη / υπάλληλο. Αντίστοιχα οι επιθέσεις που αποσκοπούσαν στο να ανακαλύψουν ευπάθειες σε ένα δίκτυο μέσω Port Scanning έχουν σταδιακά αρχίσει να αντικαθίστανται από σαφώς πιο αποδοτικές ως προς τον λόγο οικονομικής δαπάνης / επιθυμητό αποτέλεσμα. (10)



Εικόνα 5 - Τεχνικές επιθέσεων Social Engineering

5.1 Shoulder Surfing

Όσο απλή και αναποτελεσματική ίσως να μοιάζει αυτή η μέθοδος, πρόκειται για ένα υπαρκτό φαινόμενο κατά το οποίο ο επιτιθέμενος στηριζόμενος στην παρατηρητικότητα του συλλέγει πληροφορίες για κάποια ενέργεια που πραγματοποιεί κάποιος άλλος χρήστης και απαιτεί την χρήση ευαίσθητων πληροφοριών (π.χ. χρήση κωδικού πρόσβασης). Τέτοιου είδους επιθέσεις ονομάστηκαν έτσι διότι η πιο απλή και διαδεδομένη μέθοδος υλοποίησης προϋποθέτει την φυσική παρουσία του επιτιθέμενου αρκετά κοντά στο θύμα χρήστη έτσι ώστε ο πρώτος να έχει οπτική επαφή και να μπορεί να δει την οθόνη και το πληκτρολόγιο του δεύτερου. Φυσικά όπως και οι περισσότερες επιθέσεις, το Shoulder Surfing πλέον έχει εξελιχθεί και επεκταθεί στην χρήση οπτικών και ακουστικών βοηθημάτων όπως κάμερες υψηλής ανάλυσης, αλγορίθμους ανάλυσης κίνησης, κιαλιών και μικροφώνων. (11)

Εικόνα 6 - Στις επιθέσεις Shoulder Surfing η οθόνη και το πληκτρολόγιο είναι εκτεθειμένα

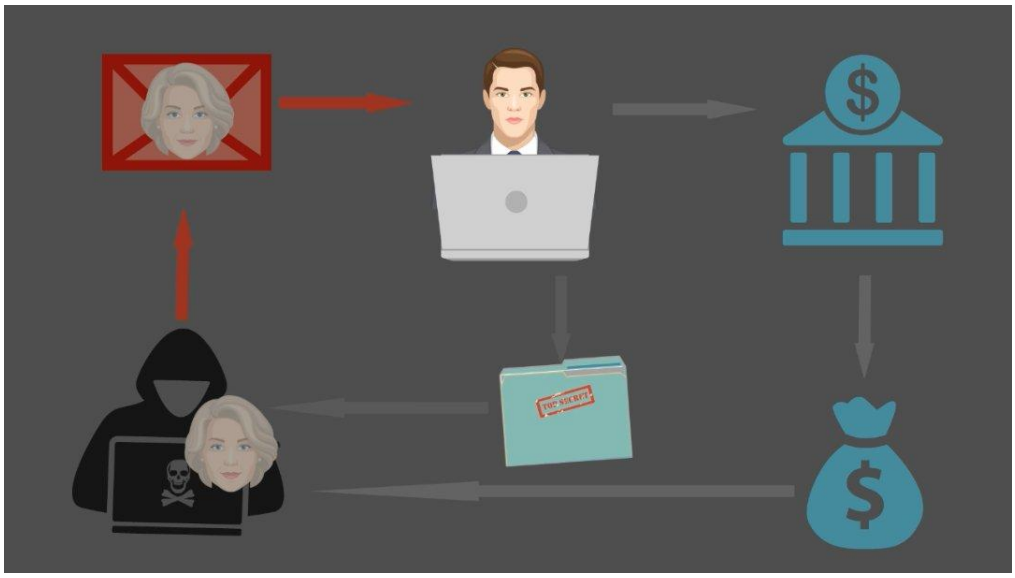
5.2 Dumpster Diving

Πολύ συχνά σημαντικά αρχεία και ψηφιακές φορητές συσκευές εταιριών και οργανισμών καταλήγουν σε κοινούς κάδους απορριμμάτων. Τέτοια αρχεία και μέσα μπορεί να αναφέρονται σε τηλεφωνικούς καταλόγους, σε εγχειρίδια χρήσης συστημάτων ή συσκευών, σε οργανογράμματα και βαρδιολόγια, σε εκτυπώσεις που ενδεχομένως να περιέχουν ευαίσθητα δεδομένα, σε σκληρούς δίσκους, κινητά τηλέφωνα και USB drives κτλ, και συχνά καταλήγουν στα απορρίμματα από αμέλεια ή και άγνοια για την σημαντικότητα τους. Οι επιτιθέμενοι μπορούν να αξιοποιήσουν με πολλούς τρόπους τα συγκεκριμένα δεδομένα και να αντλήσουν πληροφορίες για

την οργανωτική δομή ενός οργανισμού η και ακόμα για την πληροφοριακή και δικτυακή υποδομή του. Αυτές οι πληροφορίες μπορούν να φανούν χρήσιμες για την οργάνωση μιας δεύτερης επίθεσης κοινωνικής μηχανικής καθώς μερικές προσωπικές πληροφορίες ενός υπαρκτού πελάτη (πχ ονοματεπώνυμο , τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου) μπορούν να συμβάλουν στην πετυχημένη διεξαγωγή μιας επερχόμενης επίθεσης Phishing. (12)

5.3 Εξαπάτηση και Role Playing

Αποτελεί ένα από τα πιο δυνατά διαθέσιμα όπλα για την οργάνωση επιθέσεων κοινωνικής μηχανικής. Αυτή η μέθοδος στηρίζεται στην συλλογή πληροφοριών μέσω της εξαπάτησης του θύματος αφού ο επιτιθέμενος για να πραγματοποιήσει τον στόχο του υιοθέτει τον ρόλο μιας αξιόπιστης οντότητας. Ο επιτιθέμενος προσπαθεί να αποσπάσει τις επιθυμητές πληροφορίες πείθοντας το άλλο πρόσωπο πως είναι κάποιος άλλος και αυτό μπορεί να γίνει απομακρυσμένα μέσω Phishing emails η γενικότερα με τη χρήση κάθε μέσου που μπορεί να χρησιμοποίει το θύμα για επικοινωνία. Τα πιο διαδομένα σενάρια βρίσκουν συνήθως τον επιτιθέμενο να υποδύεται τον ρόλο του τεχνικού υποστήριξης, του τηλεφωνητή / receptionist, και του πελάτη. (13)



Εικόνα 7 - Ο επιτιθέμενος μπορεί να υποδυθεί πολλούς διαφορετικούς ρόλους

5.4 Κακόβουλο λογισμικό – Trojan Horses

Πρόκειται για μια από τις πιο βασικές μεθόδους που χρησιμοποιούνται σήμερα από τους hackers και συχνά σε συνδυασμό με άλλες επιθέσεις κοινωνικής μηχανικής. Το πιο διαδεδομένο σενάριο αφορά την εξαπάτηση των θυμάτων μέσω ενός Phishing email προκειμένου ο παραλήπτης να κατεβάσει ένα κακόβουλο αρχείο στο σύστημα του, το οποίο κατά την εκτέλεση του θα δημιουργήσει ένα back-door το οποίο στην συνεχεία θα μπορέσει αν χρησιμοποιηθεί από τον εισβολέα. Αυτό επιτρέπει την πλήρη πρόσβαση στο σύστημα του θύματος σε μελλοντικό χρόνο και οποιαδήποτε στιγμή το επιθυμεί ο επιτιθέμενος. (13)

5.5 Μηχανές Αναζήτησης

Τεράστιος όγκος πληροφοριών για επιχειρήσεις και οργανισμούς μπορεί να βρεθεί κάνοντας μια απλή αναζήτηση στο διαδίκτυο. Εταιρικά emails, πληροφορίες για την οργανωτική δομή, τηλεφωνικοί αριθμοί βρίσκονται δημόσια στις επίσημες ιστοσελίδες των εταιριών. Επιπλέον με μια σύντομη ερευνά σε λογαριασμούς Social Media των εταιριών μπορεί κανείς να ανακαλύψει πληροφορίες για το προσωπικό τους πελάτες, τους συνεργάτες ακόμα και για τα συστήματα και τις τεχνολογικές λύσεις που χρησιμοποιούνται. Φυσικά όλα αυτά τα δεδομένα μπορούν όπως αναφέρθηκε και προηγουμένως να παίξουν καταλυτικό ρόλο για την οργάνωση την διεξαγωγή και την τελική έκβαση μιας μελλοντικής επίθεσης.

5.6 Αντίστροφη Κοινωνική Μηχανική

Πρόκειται για μια ολόκληρη κατηγορία εξαπάτησης η όποια ακολουθεί μια αντιστροφή μέθοδο από τις συνηθισμένες. Σε αυτές τις περιπτώσεις ο επιτιθέμενος προσπαθεί να πείσει το θύμα του ότι βρίσκεται σε κίνδυνο ή ότι υπάρχει κάποιο πρόβλημα το οποίο και προσφέρεται να επιλύσει. Με αυτό τον τρόπο ο επιτιθέμενος κατασκευάζει τις ιδανικές συνθήκες για να χτίσει την επικοινωνία με το θύμα το οποίο όχι μόνο δεν υποπτεύεται κάτι αλλά αντιθέτως νιώθει ευγνωμοσύνη. Αυτές οι επιθέσεις αποτελούνται από τρία μέρη: (14)

1. **Δολιοφθορά:** Σε αυτό το στάδιο ο επιτιθέμενος προκαλεί μια βλάβη στο σύστημα του θύματος ή τον πείθει πως πρόκειται για μια βλάβη ή ότι

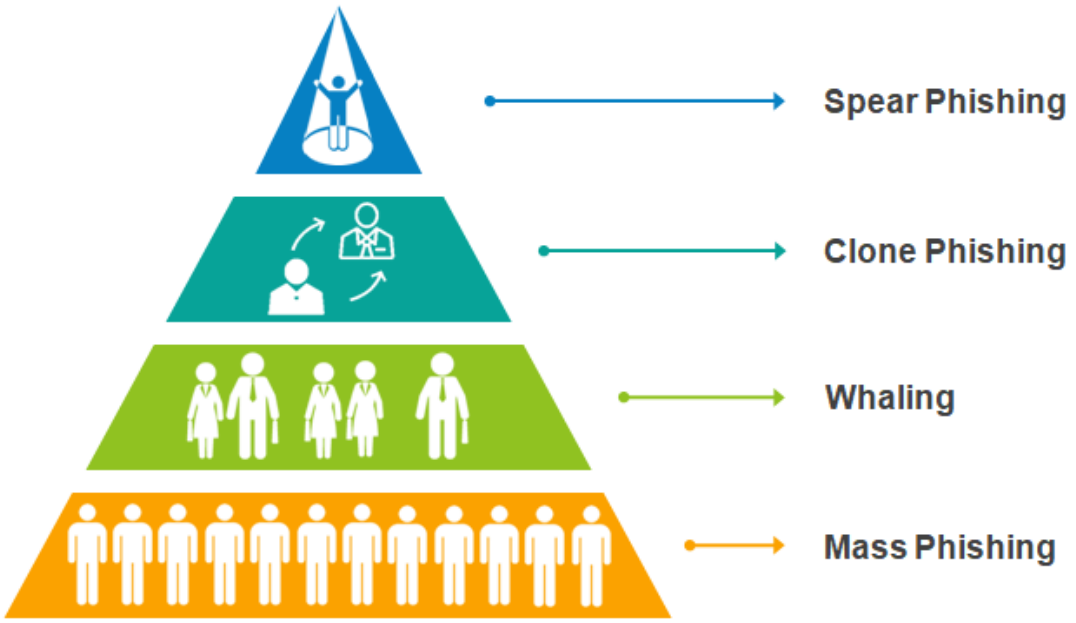
αντιμετωπίζει κάποιο πρόβλημα. Κάτι τέτοιο μπορεί να επιτευχτεί με μια επίθεση DoS σε κάποιο σύστημα του θύματος με πιο συχνό στόχο να αποτελεί κάποια ιστοσελίδα ή web υπηρεσία.

2. **Αυτοπροβολή:** Σε αυτό το στάδιο ο επιτιθέμενος παρουσιάζεται ως «από μηχανής θεός» την κατάλληλη στιγμή και καθησυχάζει το θύμα πως έχει την σωστή λύση για το πρόβλημα του.
3. **Υποστήριξη:** Στο τελευταίο στάδιο η επίθεση ολοκληρώνεται. Ο επιτιθέμενος έχει αποκτήσει την εμπιστοσύνη του χρήστη – θύματος και μπορεί να προχωρήσει στην «επίλυση» του επίπλαστου προβλήματος. Φυσικά ο χρήστης θα αποκαλύψει πληροφορίες και θα δώσει πρόσβαση σε ότι σύστημα ζητηθεί προκειμένου να φτάσει στην επίλυση.

6. Ηλεκτρονικό «Ψάρεμα» - Phishing

Δεν είναι τυχαίο το γεγονός ότι σκεπτόμενοι τον όρο «Κοινωνική Μηχανική» το πρώτο πράγμα που μας έρχεται στο μυαλό είναι οι επιθέσεις ηλεκτρονικού ψαρέματος. Αυτή η σύνδεση έχει επικρατήσει τα τελευταία χρόνια διότι κάθε επίθεση η οποία στηρίζεται σε τεχνικές κοινωνικής μηχανικής το πιθανότερο είναι να συνοδεύεται από μια επίθεση Phishing τουλάχιστον. Συνοπτικά, οι επιθέσεις Phishing συνδυάζουν πολλές φορές όλα τα προηγούμενα εργαλεία και πάντα έχουν ως στόχο την εξαπάτηση με χρήση παραπλανητικών, μη αυθεντικών emails, ιστοσελίδων και εφαρμογών. Η διαφορά με άλλες μορφές εξαπάτησης ουσιαστικά εντοπίζεται στο ότι στις επιθέσεις αυτές πάντα εμπλέκεται κάποια μορφή ψηφιακής επικοινωνίας και σχεδόν πάντα η επίθεση πραγματοποιείται απομακρυσμένα αντίθετα με τις περιπτώσει του Role Playing κατά τις οποίες ο επιτιθέμενος θα πρέπει να έρθει σε επαφή, έστω και τηλεφωνικά, με το θύμα. (15)

Οι επιθέσεις αυτές ωστόσο μπορούν να κατηγοριοποιηθούν στις παρακάτω κατηγορίες αναλόγως με το εύρος και το είδος των αποδεκτών.



Εικόνα 8 - Ιεραρχία επιθέσεων Phishing

6.1 Mass Phishing

Αποτελεί την πιο εύκολη να οργανωθεί επίθεση καθώς απευθύνεται σε τεράστια μερίδα παραληπτών. Εδώ ο επιτιθέμενος δεν έχει κάποιον συγκεκριμένο στόχο και αποσκοπεί στο να στείλει τα εν λόγω παραπλανητικά μηνύματα προκειμένου να έχει περισσότερες πιθανότητες να «Ψαρέψει» κάποια θύματα. Τα μηνύματα αυτής της επίθεσης είναι γενικά με περιεχόμενο το οποίο θα μπορούσε να απευθύνεται στον οποιοδήποτε. Τις περισσότερες φορές το μήνυμα αυτό δεν συνοδευτεί από κάποια επισύναψη ούτε εμπλέκεται κάποιο πιο περίπλοκο μέσο (πχ παραπλανητική Phishing webpage). Ο επιτιθέμενος θα αρκεστεί στο να αποσπάσει τραπεζικές πληροφορίες από τα εκάστοτε θύματα του ή θα προσπαθήσει να τα πείσει να καταθέσουν κάποιο χρηματικό ποσό η να πραγματοποιήσουν κάποια συναλλαγή με μη υπαρκτή οντότητα. (16)

6.2 Whaling

Αναφέρεται σε έναν συγκεκριμένο τύπο επίθεση Spear Phishing που στοχεύει σε υψηλού κύρους υπαλλήλους, όπως ο Διευθύνων Σύμβουλος ή ο CFO, προκειμένου να υποκλαπούν ευαίσθητες πληροφορίες, όπως αυτές που κατέχουν οι υψηλότερες θέσεις στην εταιρεία και οι οποίες έχουν συνήθως πλήρη πρόσβαση σε ευαίσθητα δεδομένα. Ο όρος Whaling (φαλαινοθηρία) προέρχεται από το μέγεθος των επιθέσεων και οι «φάλαινες» αναφέρονται επιπλέον στους στόχους που επιλέγονται με βάση την εξουσία τους μέσα στην εταιρεία. Σε πολλές επιθέσεις Whaling ο στόχος μπορεί να είναι και καθαρά οικονομικός, με τον επιτιθέμενο να χειραγωγεί το θύμα στην εξουσιοδότηση μεταφοράς υψηλών χρηματικών από εταιρικούς τραπεζικούς λογαριασμούς. Αυτές οι επιθέσεις μπορούν να ξεγελάσουν τα θύματα επειδή οι επιτιθέμενοι είναι πρόθυμοι να αφιερώσουν περισσότερο χρόνο, προσπάθεια και οικονομικούς πόρους για την οργάνωση τέτοιων επιθέσεων εξαιτίας των δυνητικά υψηλών κερδών στα οποία αποσκοπούν. Οι επιτιθέμενοι θα χρησιμοποιούν συχνά τα κοινωνικά μέσα, όπως το Facebook, το Twitter και το LinkedIn, για να συλλέξουν προσωπικές πληροφορίες σχετικά με το θύμα τους για να καταστήσουν πιο πειστική την επίθεση. (16)

Εικόνα 9 - Whaling VS Traditional Phishing

6.3 Clone Phishing

Πρόκειται για έναν ακόμα τύπος επίθεσης ηλεκτρονικού "ψαρέματος" (Phishing), κατά τον οποίο ένα έγκυρο, υπαρκτό και προηγουμένως παραδοθέν μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει ένα συνημμένο ή ένα σύνδεσμο έχει υποκλαπεί και χρησιμοποιείται για τη δημιουργία σχεδόν πανομοιότυπου ή η ακόμα και εξολοκλήρου κοινοποιημένου μηνύματος ηλεκτρονικού ταχυδρομείου. Το συνημμένο ή ο σύνδεσμος στο ηλεκτρονικό ταχυδρομείο αντικαθίσταται με μια κακόβουλη έκδοση και στη συνέχεια αποστέλλεται από μια διεύθυνση ηλεκτρονικού ταχυδρομείου που είναι πλαστογραφημένη και φαίνεται να προέρχεται από τον αρχικό αποστολέα. Το συνηθέστερο σε αυτές τις περιπτώσεις είναι ο ισχυρισμός πρόκειται για μια επαναληπτική αποστολή της αρχικής ή μιας ενημερωμένης έκδοσης του πρωτότυπου μηνύματος. Συνήθως, αυτό απαιτεί προεργασία αφού για να αποκτήσει κάποιος κακόβουλος τρίτος ένα τέτοιο emailθα πρέπει προηγουμένως να έχει αποκτήσει πρόσβαση με κάποιον τρόπο στον λογαριασμό του αρχικού αποστολέα η του τελικού παραλήπτη.

6.4 Spear Phishing

Αντίθετα με την περίπτωση του mass Phishing,όπου οι επιτιθέμενοι κατευθύνονται σε μεγάλο αριθμό στόχων σχετικά χαμηλής απόδοσης, το Spear Phishing επικεντρώνεται σε συγκεκριμένους στόχους χρησιμοποιώντας ειδικά σχεδιασμένα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται στο υποτιθέμενο θύμα τους. Η εξοικείωση λοιπόν είναι αυτό που καθιστά πιο επιτυχημένες τις επιθέσεις αυτές. Οι επιτιθέμενοι συλλέγουν πληροφορίες από κοινωνικά μέσα ενημέρωσης σχετικά με πιθανούς στόχους, συμπεριλαμβανομένων των προσωπικών και επαγγελματικών σχέσεών τους και άλλων προσωπικών στοιχείων. Ο εισβολέας χρησιμοποιεί αυτές τις πληροφορίες για να δημιουργήσει ένα εξατομικευμένο μήνυμα που φαίνεται και ακούγεται αυθεντικό για να πείσει τον στόχο να ανταποκριθεί στο αίτημα του αποστολέα. Ο αποστολέας μπορεί να ζητήσει από τον χρήστη να απαντήσει απευθείας στο μήνυμα ηλεκτρονικού ταχυδρομείου ή το μήνυμα μπορεί να περιλαμβάνει έναν κακόβουλο σύνδεσμο ή συνημμένο που εγκαθιστά κακόβουλο λογισμικό στη συσκευή του προορισμού ή κατευθύνει τον στόχο σε έναν κακόβουλο ιστότοπο ο οποίος έχει ρυθμιστεί για να τον εξαπατήσει να δίνει ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης, πληροφορίες λογαριασμού ή πληροφορίες πιστωτικής κάρτας.

Εικόνα 10 - Spear Phishing

6.5 Phishing Variations

Δεν πρόκειται για μια «πραγματική» αν προσπαθήσει κάνεις να την κατατάξει με βάση τον στόχο αφού οι προηγούμενες κατηγορίες καλύπτουν όλη την γκάμα των πιθανών επιθέσεων. Αξίζουν ωστόσο μια αναφορά δεδομένου ότι πρόκειται για μια κατηγορία που φιλοξένει επιθέσεις οι οποίες συνηθίζεται να γίνονται με συγκεκριμένα μέσα επικοινωνίας έτσι έχουν επικρατήσει και οι παρακάτω ορισμοί:

- **Vishing (voice Phishing):** Αναφέρεται σε περιπτώσεις που η επίθεση γίνεται εξ ολοκλήρου τηλεφωνικά η μια τηλεφωνική συσκευή η επικοινωνία μέσω αυτής συμβάλει στην επιτυχία της επίθεσης. Λογά της φύσης της τηλεφωνικής επικοινωνίας αυτή η μέθοδος δεν μπορεί να χρησιμοποιηθεί για Mass Phishing. Ωστόσο είναι αρκετά αποτελεσματική μέθοδος αφού στηρίζεται στις ίδιες βασικές αρχές με το Spear Phishing και πολλές φορές η αμεσότητα της προφορικής επικοινωνίας ίσως συμβάλει αποτελεσματικά στην απόσπαση πληροφοριών.

  Ακόμα έχουν εμφανιστεί περιπτώσεις κατά τις οποίες πλαστά τηλεφωνικά νούμερα κοινοποιούνται μέσω παραπλανητικών emails και τα όποια προτρέπουν τον παραλήπτη να τα καλέσει, δήθεν ως τμήμα κάποιας τραπεζικής διαδικασίας. Τα τηλεφωνά αυτά ανήκουν σε VoIP γραμμή online υπηρεσιών και είναι δύσκολο να εντοπιστεί ο δράστης. Όταν το θύμα τα καλέσει οι επιτιθέμενοι στα πλαίσια κάποιας επιβεβαίωσης στοιχείων θα τους ζητήσουν να πληκτρολογήσουν τον κωδικό της κάρτας τους και άλλα προσωπικά στοιχειά τα όποια μέσω παλμικής αναγνώρισης μπορούν να αποσπάσουν σε μορφή κειμένου. (17)
- **Smishing:** Πρόκειται για απάτες που στηρίζονται σε αποστολή και λήψη μηνυμάτων sms. Μπορεί να αφορούν κομμάτι μιας άλλης επίθεσης καθώς μπορούν να αποσκοπούν στην απλή συλλογή πληροφοριών η ακόμα μπορεί να χρησιμοποιηθούν για παραβίαση two factor authentication με την αλλοίωση one time pass κωδικών.

7. Τα «όπλα» των επιτιθέμενων

Για να πραγματοποιηθούν όλες οι περιπτώσεις επιθέσεων που έχουν προαναφερθεί υπάρχουν διαθέσιμα πολλά διαφορετικά μέσα. Όπως γίνεται εύκολα αντιληπτό, τα εργαλεία, τεχνικά και μη, που θα χρησιμοποιηθούν εξαρτώνται από τον χρόνο και του πόρους που επιθυμεί να αφιερώσει ο επιτιθέμενος αλλά και από την προσωπική του εξοικείωση με την τεχνολογία. Σε περιπτώσεις όπου το ζητούμενο είναι η απόκτηση ευαίσθητων πληροφοριών η χρήση ενός απλού τηλεφώνου για την προσποίηση και εξαπάτηση του θύματος είναι αρκετή. Στο ίδιο σκεπτικό μπορεί να βασιστεί και μια επίθεση Dumpster Diving ή Shoulder Surfing δεδομένου του γεγονότος ότι ο επιτιθέμενος χρειάζεται μόνο φυσική πρόσβαση κοντά η στο εσωτερικό μιας εταιρίας.

Ωστόσο οι πιο αποδοτικές επιθέσεις απαιτούν την χρήση πιο εξεζητημένων μεθόδων για την αποτελεσματική διεξαγωγή τους. Ο επιτιθέμενος θα πρέπει να ανακαλύψει πληροφορίες, να τις συνδυάσει και να τις παρουσιάσει με τρόπο πειστικό συχνά τόσο πειστικό που ακόμα και άτομα εξοικειωμένα με ζητήματα Ασφάλειας Πληροφοριών θα δυσκολευτούν να εντοπίσουν την απάτη. Για τέτοιους σκοπούς υπάρχει μια πληθώρα τεχνικών τις οποίες ο καθένας θα μπορούσε με την κατάλληλη γνώση να ενσωματώσει στην επίθεση του. Επιπλέον υπάρχουν διαθέσιμες έτοιμες σουίτες και πακέτα λογισμικών οι οποίες μπορούν να αυτοματοποιήσουν σε μεγάλο βαθμό αυτές τις τεχνικές.

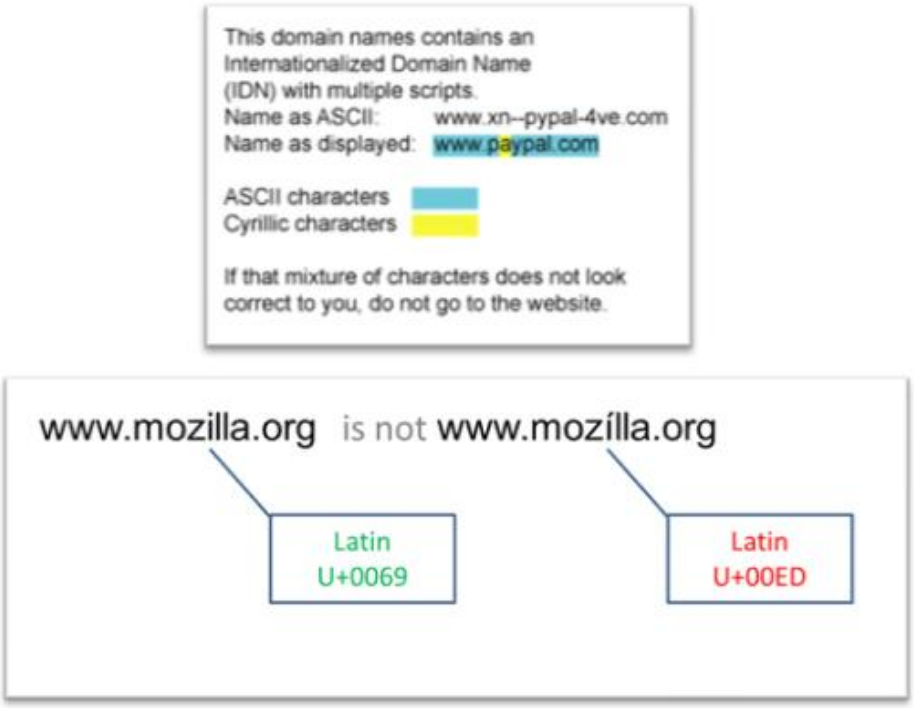
7.1 Παραποίηση Συνδέσμων (Hyperlink Manipulation)

Στις επιθέσεις Phishing συγκεκριμένα υπάρχει πολύ συχνά η ανάγκη για την εξαπάτηση του παραλήπτη με χρήση και παραπομπή του σε διάφορα κακόβουλα URLs. Τα URLs αυτά πρέπει να δείχνουν έγκυρα και ότι ανήκουν στον πραγματικό αποστολέα. Έτσι λοιπόν οι επιτιθέμενοι συχνά χρησιμοποιούν τεχνικά και μη τεχνικά μέσα όπως: (18)

- Τα εσκεμμένα τυπογραφικά κατά την κατοχύρωση ενός domain. Για παράδειγμα εάν κάποιος ήθελε να δημιουργήσει έναν παραπλανητικό κλώνο της γνωστής ιστοσελίδας www.google.com θα μπορούσε κατά την κατοχύρωση του ονόματος Domain να πληκτρολογήσει τα «go0gle» ή

«goog1e». Με αυτόν τον απλό τρόπο ο κακόβουλος χρήστης μπορεί να αυξήσει σημαντικά τα την πιθανότητα επιτυχίας μιας επίθεσης αφού εξασφαλίζει την εξοικείωση.

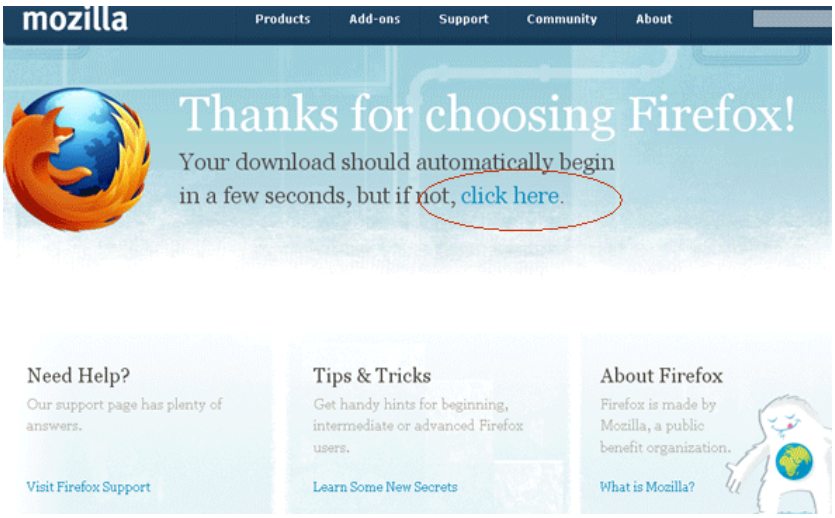
- Την μέθοδο IDN. Το ακρωνύμιο IDN προέρχεται από τον όρο Internationalized domain names και αναφέρεται σε domain names τα οποία χρησιμοποιούν χαρακτήρες ου δεν ανήκουν στο λατινικό αλφάβητο. Αυτό επιτρέπει σε χρήστες να δημιουργούν και να μπορούν αντίστοιχα να επισκέπτονται ιστοσελίδες χρησιμοποιώντας το δικό τους αλφάβητο. Ενας κακόβουλο χρήστης θα μπορούσε να εκμεταλλευτεί αυτή την δυνατότητα για να δημιουργήσει ένα domain name οπτικά πανομοιότυπο με το πραγματικό στο οποίο ωστόσο θα έχει αντικατασταθεί ένας η παραπάνω χαρακτήρες με ίδιους χαρακτήρες διαφορετικού αλφάβητου.



Εικόνα 11 - Παραδείγματα IDN Spoofing | Πανομοιότυπα γράμματα άλλα διαφορετικό αλφάβητο

- Την επεξεργασία των hyperlink tags. Κάθε URL εμφανίζεται ως ένα ενεργό οπτικά διαφοροποιημένο στοιχειό του user interface της εκάστοτε εφαρμογής. Από τις αρχές του διαδικτύου και ειδικότερα σήμερα έχει επικρατήσει η

τακτική να διαμορφώνονται τα hyperlinks έτσι ώστε να είναι περιγραφικά και καλαίσθητα χωρίς απαραίτητα να φανερώνουν την πλήρη διεύθυνση της ιστοσελίδας στην όποια οδηγούν. Αυτή την δυνατότητα εκμεταλλεύονται οι επιτιθέμενοι πολύ συχνά, και ιδιαίτερα όταν δεν έχουν την δυνατότητα να παραμετροποιήσεων δικό τους domain name, οι οποίοι πολύ εύκολα μπορούν να «καλύψουν» τον πραγματικό προορισμό ενός URL. Συχνά ο παραλήπτης θα δει κάποιον ενεργό σύνδεσμο με κάποια σήμανση όπως «Πατήστε εδώ», «Εγγραφή», «Login» κτλ. χωρίς να μπορεί να δει άμεσα την πραγματική διεύθυνση.



Εικόνα 12 - Παράδειγμα επίθεσης Phishing URL

7.2 Παράκαμψη φίλτρων

Πλέον οι περισσότεροι Email service providers αλλά και πολλές instant messaging και chatting υπηρεσίες διαθέτουν εγκατεστημένα και ενεργά ως προεπιλογή φίλτρα τα οποία αποσκοπούν στο να μπλοκάρουν περιεχόμενο το οποίο θεωρείται κακόβουλο ή επικίνδυνο. Τέτοιου είδους φίλτρα λειτουργούν με βάση το περιεχόμενο ενός μηνύματος ηλεκτρονικού ταχυδρομείου είτε αναλύοντας επιτόπου και ψάχνοντας για λέξεις ή επισυνάψεις με βάση τον τύπο τους (π.χ. απόρριψη εκτελέσιμων αρχείων με κατάληξη .exe) είτε συγκρίνοντας την διεύθυνση του αποστολέα η τυχόν hyperlinks με το περιεχόμενο λιστών που βρίσκονται online και οι οποίες περιέχουν διευθύνσεις που έχουν ήδη χαρακτηριστεί ως κακόβουλες (spam lists).

Καθώς τα πιο πολλά αντίμετρα στηρίζονται στην επεξεργασία και ανάλυση, του κειμένου ενός email στη συνέχεια επικράτησε το να στέλνονται όλα τα κακόβουλα email σαν εικόνα. Με άλλα λόγια ο επιτιθέμενος μετέτρεπε όλο το μήνυμα ηλεκτρικού ταχυδρομείου σε μια εικόνα μορφής .jpg οποία είναι αναγνώσιμη από άνθρωπο, αλλά δεν μπορεί να αναλυθεί από πρόγραμμα. Ως αντίμετρο σε αυτήν την περίπτωση οι mail servers υιοθέτησαν την πρακτική του να απορρίπτουν αυτομάτως όλα τα emails τα οποία αποτελούνταν από μια μόνο εικόνα

Οι κακόβουλοι χρήστες στην συνέχεια άρχισαν να συνδυάζουν λέξεις και προτάσεις (συνήθως άσχετες με την επίθεση) με εικόνες (οι οποίες περιείχαν το κακόβουλό περιεχόμενο). Αυτό δεν αντιμετωπίστηκε ποτέ επιτυχώς από μόνο του. Κατάλοιπο αυτού είναι, ακόμα και σήμερα, οι πιο πολύ email clients αλλά και webmail (όπως hotmail), να μην δείχνουν εξορισμού ποτέ τις εικόνες σε ένα email αλλά να πρέπει ο χρήστης να επιλέξει να τις εμφανίσει. Αντίστοιχα είναι κοινή πρακτική για τους επιτιθέμενους να κρύβουν κακόβουλα αρχεία σε φαινομενικά έγκυρες επισυνάψεις τροποποιώντας την επέκταση των αρχείων (19)

7.3 Πλαστογράφηση έγκυρων ιστοσελίδων.

Στις περιπτώσεις που απαιτείται η υποκλοπή credentialsείναι πολύ συνηθισμένο και αποδοτικό το να προσπαθήσει ο επιτιθέμενος να πείσει το θύμα να καταχωρίσει οικειοθελώς αυτά τα στοιχεία σε μια κακόβουλη ιστοσελίδα. Οι επιτιθέμενοι σχεδιάζουν πανομοιότυπες ιστοσελίδες τις οποίες θα συμπεριλάβουν σε ένα Phishing email. Ο ανυποψίαστος χρήστης θα ακολουθήσει το link και θα βρεθεί σε ένα γνώριμο περιβάλλον όπου θα του ζητηθεί να κάνει Login όμως στην πραγματικότητα τα στοιχεία του θα σταλούν στον κακόβουλο χρήστη. Από εκεί και πέρα εξαρτάται και πάλι από τον επιτιθέμενο το προδιατεθειμένος είναι να επενδύσει πόρους στο να καταστήσει την επίθεση ακόμα πιο πειστική. Πολλές φορές μετά την εισαγωγή των credentials οι χρηστές θα δουν μια λευκή οθόνη η κάποιο σφάλμα το οποίο θα τους κάνει να υποψιαστούν ενώ σε άλλες περιπτώσεις ο επιτιθέμενος έχει προνοήσει να μεταφέρει το θύμα στο πραγματικό, αξιόπιστο website μετά την ολοκλήρωση της επίθεσης. Ορισμένες απάτες ωστόσο χρησιμοποιούν εντολές JavaScript για να αλλάξουν τη γραμμή διευθύνσεων του ιστότοπου στον οποίο οδηγούν. Αυτό γίνεται

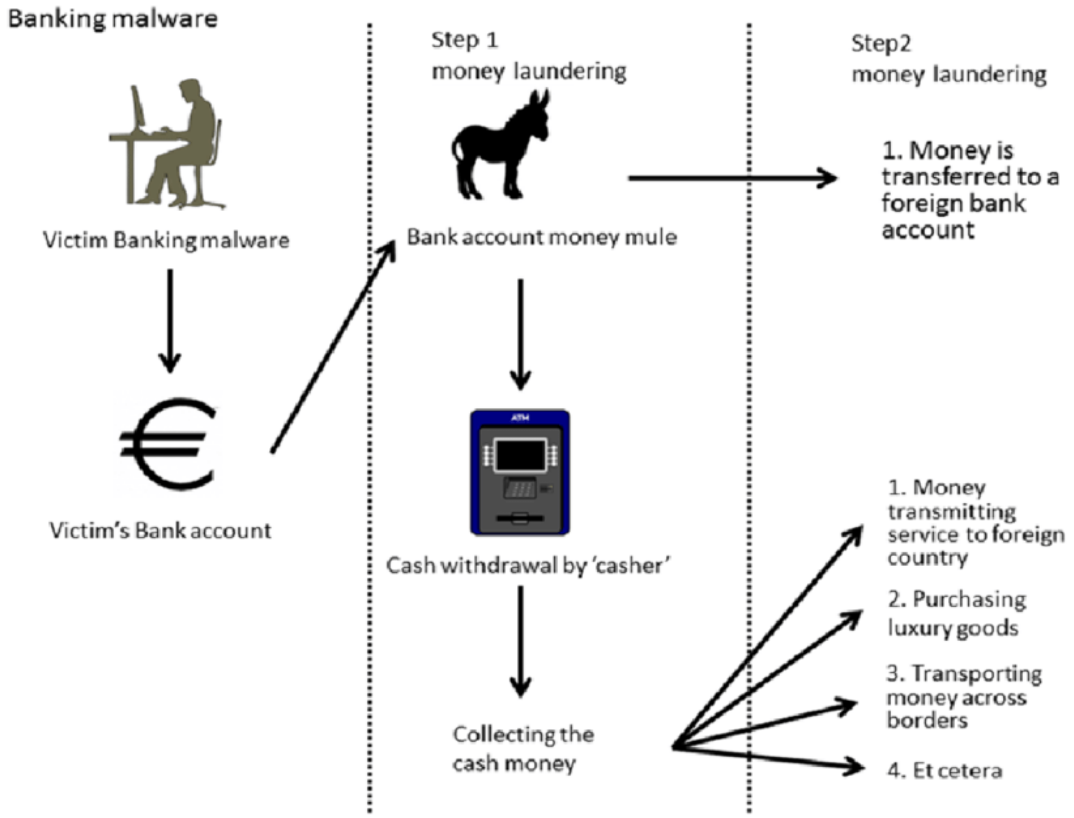
είτε τοποθετώντας μια εικόνα της έγκυρης διεύθυνσης URL στη γραμμή διευθύνσεων είτε κλείνοντας την αρχική γραμμή και ανοίγοντας μια νέα με τη έγκυρη διεύθυνση URL. Και στις δυο αυτές περιπτώσεις ο χρήστης θεώρει πως έχει επισκεφθεί μια έγκυρη σελίδα ενώ ουσιαστικά πλοηγείτε σε ένα υπό-παράθυρο το οποίο έχει σχεδιαστεί επάνω από την πραγματική ιστοσελίδα.

7.4 Phishing Mules

Αξίζει να αναφερθεί και πάλι ότι οι επιθέσεις που στηρίζονται σε τεχνικές Social Engineering είναι πολύπλευρες και συχνά έχουν πολλά διαφορετικά επιμέρους σκέλη. Ένας ακόμα λοιπόν πόρος που εκμεταλλεύονται οι επιτιθέμενοι ως εργαλείο και όχι απαραίτητα ως στόχο είναι οι ίδιοι οι άνθρωποι.

Όταν πρόκειται για οικονομική απάτη συχνά οι επιτιθέμενοι συγκεντρώνουν τα οικονομικά στοιχεία ατόμων μέσω Phishing, και έτσι είναι σε θέση να καταχραστούν τα στοιχεία αυτά και να υποκλέψουν χρήματα από τους εκτεθειμένους λογαριασμούς.

Για να καλύψουν όμως τα ίχνη τους και να κατασταθεί η επίθεση πραγματικά επιτυχημένη, αναθέτουν σε ανυποψίαστα άτομα να παίξουν το ρόλο μεσολαβητών, δημοσιεύοντας διάφορες δελεαστικές αγγελίες εργασίας που υπόσχονται στους ενδιαφερομένους ότι θα κερδίσουν χρήματα γρήγορα, χωρίς ιδιαίτερες απαιτήσεις και με ελάχιστη προσπάθεια. Τα άτομα αυτά είναι γνωστά ως «mules». Οι τραπεζικοί λογαριασμοί των mules χρησιμοποιούνται για την παραλαβή εμβασμάτων από τους παραβιασμένους τραπεζικούς λογαριασμούς των πραγματικών θυμάτων. Το επόμενο στάδιο βρίσκει τους επιτιθέμενος να ζητούν συνήθως ως χάρη ή στα πλαίσια των «εργασιακών» τους καθηκόντων από τους mules να ρευστοποιήσουν τα χρήματα από το λογαριασμό τους και έπειτα να τα αποστείλουν στους ίδιους με κάποιον άλλο τρόπο για μεταφορά χρημάτων ο οποίος μπορεί να τους εξασφαλίσει ανωνυμία (υπηρεσίες διεθνών εμβασμάτων όπως το money gram). Το πιο σύνηθες είναι να υπόσχονται και ένα μέρος του πόσου ως προμήθεια στους mules το οποίο και τους το παραχωρούν καθιστώντας την όλη κατάσταση ελκυστική. χρησιμοποιώντας μια υπηρεσία διεθνών εμβασμάτων. Οι εγκέφαλοι της απάτης διατηρούν έτσι την ανωνυμία τους, αφήνοντας εκτεθειμένους τους Phishing mules, τους οποίους μπορούν να παρακολουθήσουν οι αρχές



Εικόνα 13 - Παράδειγμα επίθεσης Phishing Mule

Εδώ σε αυτή την περίπτωση βλέπουμε μια επίθεση Phishing εμφωλευμένη μέσα σε μια μεγαλύτερη. Ο επιτιθέμενος μετά την απόσπαση των χρημάτων χρησιμοποιεί τα ίδια τεχνάσματα για να παραπλανήσει τους mules, χτίζει σχέση εμπιστοσύνης μαζί τους ζητώντας τους συχνά να φέρουν εις πέρας άπλες εργασίες και το αίτημα της μεταφοράς χρημάτων συνήθως συμβαίνει σε δεύτερο χρόνο καθιστώντας πιο δύσκολο το να υποπτευτεί κανείς ότι πρόκειται για απάτη. Δεν είναι λίγες οι περιπτώσεις που άτομα τα οποία έχουν εμπλακεί ως mules μαθαίνουν για την απάτη από τις αρχές βρισκόμενοι υπόλογοι. (20) (21)

8. Εργαλεία, Λογισμικό και έτοιμες λύσεις

Κατά καιρούς σε διαφορές μελέτες που έχουν γίνει σχετικά με την Ευαισθητοποίηση του κοινού για θέματα κοινωνικής μηχανικής έχει διατυπωθεί η ευρύτερη γνώμη ότι οι επιθέσεις Phishing στην πλειοψηφία τους είναι αρκετά γενικές και στοχεύουν την μάζα. Επιπλέον αρκετές είναι οι περιπτώσεις που στελέχη επιχειρήσεων δεν επενδύουν σε μετρά κατά του Phishing διότι ακριβώς θεωρούν πως αναφέρεται σε commercial χρήστες και δεν απασχολεί τόσο τον enterprise τομέα. Αυτό σαφώς πηγάζει από την λανθασμένη ιδέα ότι το Phishing είναι μόνο οι γνωστές generic απάτες με τα κακογραμμένα emails τα οποία χαρακτηρίζονται από συντακτικά, λεκτικά και ορθογραφικά σφάλματα που αποστέλλεται κατά καιρούς μαζικά σε χρήστες και κατ' επέκταση από την εντύπωση πως ένας επιτιθέμενος θα πρέπει να διαθέτει υπερβολικές και εξεζητημένες γνώσεις για να μπορέσει να διεξάγει μια πραγματικά πειστική επίθεση. (22)

8.1 Εργαλεία για Επίθεση

Στην πραγματικότητα ένας κακόβουλος χρήστης φυσικά θα μπορούσε να αξιοποιήσει περίπλοκες γνώσεις προγραμματισμού και πρωτοκόλλων επικοινωνίας και να οργανώσει μια επίθεση αλλά κάτι τέτοιο απαιτεί χρόνο και αφοσίωση. Υπάρχουν όμως διαθέσιμα αρκετά εργαλεία τα οποία μπορούν να αυτοματοποιήσουν και να διευκολύνουν τον σχεδιασμό μιας επίθεσης καθώς διαθέτουν έτοιμα templates, έτοιμους mail servers εργαλεία crawling και αναζήτησης προσωπικών στοιχείων κα τα οποία καθιστούν το Social Engineering εύκολη υπόθεση ακόμα και για κάποιον λιγότερο εξοικειωμένο χρήστη. Ενδεικτικά παρουσιάζονται κάποια τέτοια εργαλεία παρακάτω:

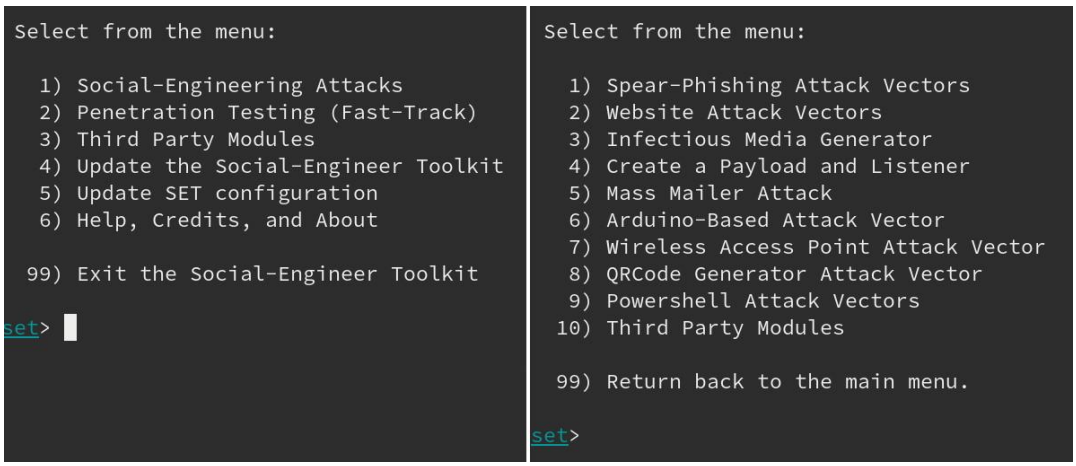
8.1.1 Social Engineering Toolkit (SET)

Η συγκεκριμένη σουίτα εργαλείων, η οποία είναι γνωστή και ως SET βρίσκεται προεγκατεστημένη στο Kali Linux distro και είναι ιδιαίτερα διαδεδομένη αφού πλέον καταμετρά πάνω από 2 εκατομμύρια λήψεις. Έχει αναπτυχτεί σε Python από τον Dave Kennedy μέλος της TrustedSec, και διατίθεται ως εργαλείο ανοιχτού κώδικα, ελεύθερο που χρησιμοποιείται από ερευνητές ασφαλείας, penetration testers αλλά αρκετά συχνά και από κακόβουλους χρήστες. Ο λόγος που είναι τόσο διαδεδομένο, περά από την ελεύθερη διάθεση του είναι και το ότι προσφέρει πολλές «έξυπνες»

λειτουργίες, συμπεριλαμβανομένης της απομίμησης τηλεφωνικών αριθμών, της αποστολής μηνυμάτων SMS ή την δημιουργία παραπλανητικών σελίδων ηλεκτρονικού "ψαρέματος" με την άμεση κλωνοποίηση της πρωτότυπης. (23)

Πιο αναλυτικά, μερικές από τις πιο σημαντικές δυνατότητες που παρέχει είναι:

- Multi-platform Μπορεί να εγκατασταθεί και να τρέξει σε Unix, Linux και Windows
- Αυξημένη και εξελισσόμενη λειτουργικότητα αφού επιτρέπει την χρήση πρόσθετων λειτουργιών από third-parties
- Επιτρέπει την πλήρη παραμετροποίηση όλων των επιμέρους λειτουργιών του παρέχοντας την μέγιστο customizability
- Μπορεί να χρησιμοποιηθεί για μια μεγάλη γκάμα επιθέσεων όπως επιθέσεις Spear-Phishing, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based επιθέσεις, QRCode επιθέσεις, επιθέσεις Powershell κ.α.



Εικόνα 14 - Εργαλείο SET | Περιβάλλον χρήσης

Web Attack: Αυτή η κατηγορία συνδυάζει διάφορες επιθέσεις για να στοχευσει ο επιτηθέμενος το υποψήφιο θύμα. Περιλαμβάνει τεχνικές επίθεσης όπως Java Applet Attack και Metasploit Browser Exploit για την αποστολή Payloads. Επίσης, χρησιμη μπορεί να φανεί η μέθοδος Credential Harvester, η οποία επιτρέπει την πιστή αντιγραφή ενός ιστοτοπου και την συλλογή των στοιχείων σύνδεσης από πεδία για login, καθώς και τεχνικές TabNabbing, HTA Attack, Web-Jacking και Multi-Attack, οι οποίες αποσκοπούν όλες στο να υποκλαπούν τα στοιχεία σύνδεσης των χρηστών.

Infectious Media Generator: Αυτή η λειτουργία επιτρέπει την δημιουργία μιας «μολυσμένης» συσκευής πολυμέσων (USB / CD / DVD) με ένα αρχείο autorun.inf, το οποίο μπορεί να εισαχθεί αργότερα σε οποιοδήποτε μηχάνημα και να εκτελέσει αυτόματα ένα Metasploit Payload εάν είναι ενεργοποιημένο το autorun στον υπολογιστή του θύματος.

Payload and Listener: Αυτή η λειτουργία επιτρέπει την δημιουργία κακόβουλων payloads για τα Windows, συμπεριλαμβανομένων των Shell Reverse_TCP, Reverse_TCP Meterpreter, Shell Reverse_TCP X64 και Meterpreter Reverse HTTPS.

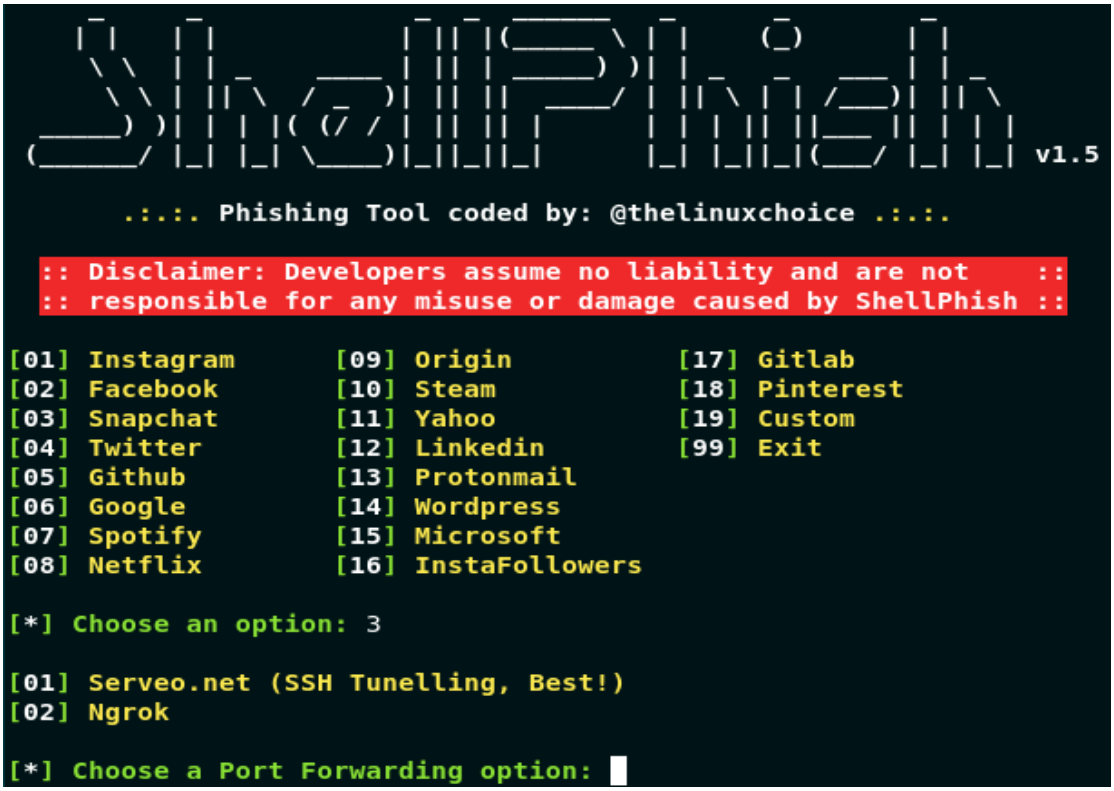
Mass Attack Mailer: Αυτός ο τύπος επίθεσης μπορεί να στραφεί εναντίον ενός ή πολλών ατόμων, επιτρέποντάς την εισαγωγη λιστας χρηστών για την αποστολή κακόβουλων emails. Δίνεται η δυναντότητα χρήσης gmail account για την διεξαγωγή της επίθεσης κάτι το όποιο είναι ιδιαίτερα χρήσιμο για εκπαιδευτικούς σκοπούς η την δοκιμή templates και φυσικά επιτρέπει την χρήση custom domains και την χρήση Relays για αποστολή μαζικών μηνυμάτων.

```
set:mailer>1
set:phishing> Send email to:nn@securitytrails.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):cservice@paypal.io
set:phishing> The FROM NAME the user will see:PP Customer SERVICE
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Your account has been limited untiI we hear from you
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Dear client,
Next line of the body: Recently, your account was reviewed and flagged because of a potential
. To avoid an eventual restriction to your account, please verify your informations by logging
Next line of the body: Check My Account [link]
Next line of the body: END
[*] SET has finished sending the emails
```

Εικόνα 15 - Εργαλείο SET | Υπόδειγμα επίθεσης

8.1.2 ShellPhish

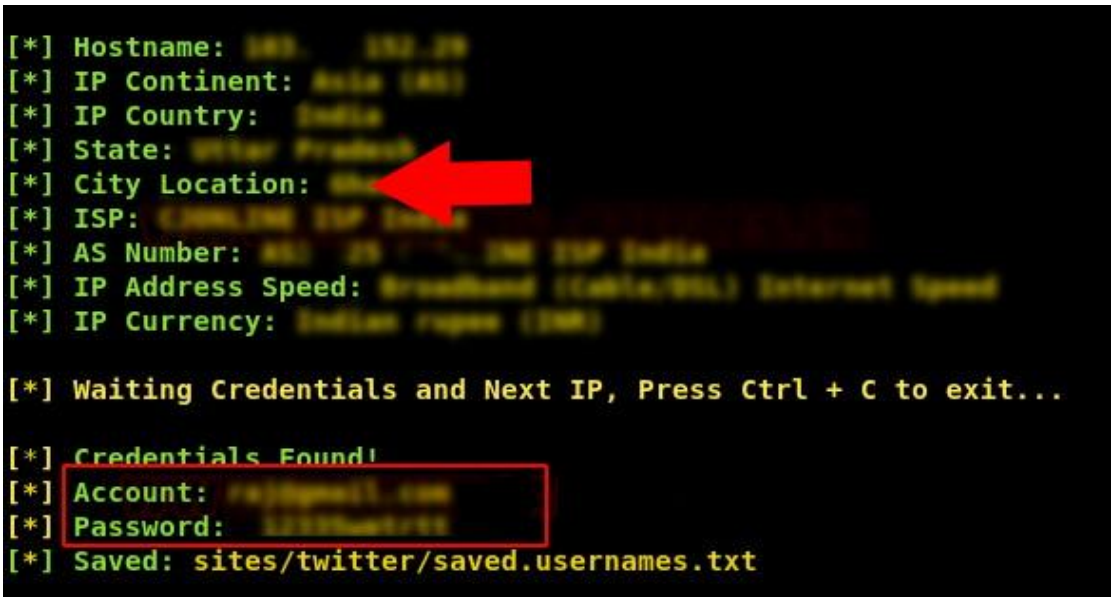
Το Shellphish είναι ένα ενδιαφέρον εργαλείο αποδεικνύει το πόσο έχουν εξελιχτεί τα εργαλεία Phishing σε εύκολα και αποτελεσματικά σήμερα. Το εργαλείο αξιοποιεί ορισμένα από τα πρότυπα που δημιουργούνται από ένα άλλο εργαλείο που ονομάζεται SocialFish. Το εργαλείο προσφέρει πρότυπα ηλεκτρονικού "ψαρέματος" για 18 δημοφιλείς ιστότοπους, η πλειοψηφία των οποίων επικεντρώνεται στα Social Media και τους παρόχους ηλεκτρονικού ταχυδρομείου μεταξύ των οποίων και τα Instagram, Facebook, Snapchat, Github, Twitter, Yahoo, Spotify, Netflix, Linkedin, WordPress, Steam, Microsoft, Gitlab, Pinterest κ.α. Υπάρχει επίσης μια επιλογή χρήσης ενός προσαρμοσμένου προτύπου, εάν το επιθυμείτε.



Εικόνα 16 - Εργαλείο ShellPhish | Μενού επιλογών

Το εργαλείο όχι μόνο μπορεί να δημιουργήσει πανομοιότυπες σελίδες σύνδεσης αλλά χρησιμοποιώντας την υπηρεσία Ngrok μπορεί να κάνει host το σύνδεσμο Phishing. Αυτό μας δίνει το HTTPS στις σελίδες ηλεκτρονικού "ψαρέματος" και τις καθιστά ακόμα πιο πειστικές. Ακριβώς επιλέγοντας αυτή την επιλογή, το εργαλείο ξεκινά έναν διακομιστή php και Ngrok και εμφανίζει το σύνδεσμο ηλεκτρονικού ψαρέματος.

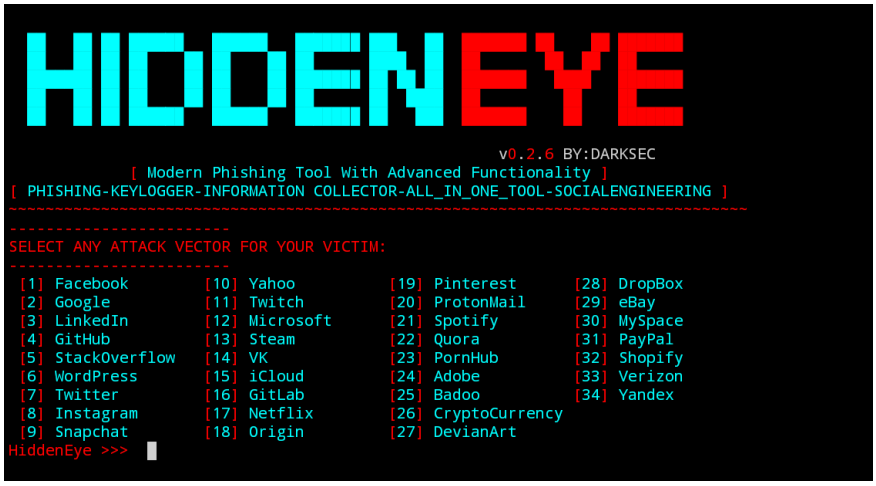
Στη συνεχεία αυτός ο σύνδεσμος θα αποσταλεί στο θύμα με ένα τυπικό mail αναλόγως με το σενάριο και όταν το θύμα ακολουθήσει το link, το εργαλείο ShellPhish αρχίζει να εμφανίζει ενδείξεις δραστηριότητας δίνοντας ορισμένες λεπτομέρειες όπως την IP του θύματος, το πρόγραμμα περιήγησης που χρησιμοποιει, τη χώρα και την πόλη στην οποία βρίσκεται κοκ. Το βασικό όμως στοιχείο , τα credentials του θύματος, θα μεταφερθούν στον επιτιθέμενο σε μορφή απλού κειμένου όπως μπορεί να φάνει και στην εικόνα παρακάτω. (24)



Εικόνα 17 - Εργαλείο ShellPhish | Υπόδειγμα αποτελεσμάτων επίθεσης

8.1.3 Hiddeneye

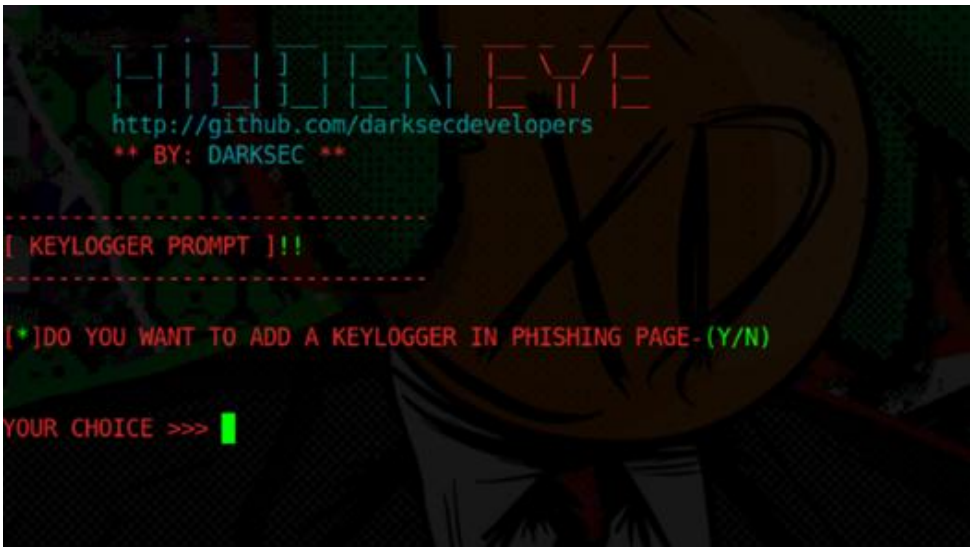
Το HiddenEye είναι ένα από τα πιο σύγχρονα εργαλεία Phishing με προηγμένες λειτουργίες και πλέον υποστηρίζει και το Android. Παρέχει ζωντανή πληροφόρηση σχετικά με τα θύματα, όπως: IP ADDRESS, Geolocation, ISP, Χώρα κ.α.



Εικόνα 18 - Εργαλείο Hiddeneye | Περιβάλλον χρήσης

Ανάλογα με τον επιλεγόμενο τύπο επίθεσης μπορεί να χρησιμοποιηθεί για την παραβίαση λογαριασμών χρηστών όπως το Facebook, το Twitter, το Instagram, το Snapchat και άλλα. Μπορεί να χρησιμοποιηθεί για τη διεξαγωγή επιθέσεων Phishing παρέχοντας έτοιμα και ενημερωμένα templates – κλώνους από 30 και παραπάνω γνωστούς ιστότοπους, κοινωνικά δίκτυα και web εφαρμογές. (25)

- Το εργαλείο μπορεί επίσης να εκτελεστεί σε συσκευές Android μέσω της εφαρμογής UserLand ή της εφαρμογής Termux.
- Μπορεί να εκτελέσει live επιθέσεις (IP, γεωγραφική περιοχή, χώρα κ.λπ.)
- Μπορεί να υποκλέψει credentials, στοιχεία επικοινωνίας, στοιχεία πληρωμών και πιστωτικών καρτών και γενικότερα όλη την γραπτή δραστηριότητα του θύματος. (χρησιμοποιώντας τη λειτουργία keylogger)



Εικόνα 19 - Εργαλείο Hiddeneye | Περιβάλλον χρήσης (2)

- Δυνατότητες Serveo URL επιτρέποντας στον επιτιθέμενο να επιλέγει μεταξύ RANDOM URL και CUSTOM URL και δυνατότητα απαρατήρητης ολοκλήρωσης των επιθέσεων με link redirection.

Εικόνα 20 - Εργαλείο Hiddeneye | Υπόδειγμα επίθεσης

8.2 Εργαλεία για Εκπαιδευτικούς Σκοπούς

Οι επιθέσεις Phishing έχουν αυξηθεί εκθετικά τα τελευταία χρόνια και πλέον θεωρούνται από τους ειδικούς ως η πιο επικίνδυνη μορφή επίθεσης για μια εταιρία ή έναν οργανισμό με 3.4 δισεκατομμύρια κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου να αποστέλλονται καθημερινά . Αυτό έχει καταστήσει αναγκαία σε πρώτο επίπεδο την ενημέρωση των υπάλληλων που πλαισιώνουν μια εταιρία για την ύπαρξη αυτών των επιθέσεων και βασικότερα την προετοιμασία τους ώστε να μπορούν να διαχειριστούν τέτοιες καταστάσεις. Στην προηγούμενη ενότητα παρουσιαστήκαν εργαλεία και λογισμικό που μπορεί να χαρακτηριστεί ύποπτο αφού μπορεί πραγματικά να αξιοποιηθεί για να φέρει εις πέρας μια πραγματική επίθεση Phishing. Για τον σκοπό της ενημέρωσης και της ευαισθητοποίησης των χρηστών λοιπόν έχουν αναπτυχτεί εργαλεία που επιτρέπουν την εκτέλεση προσομοίωσης επιθέσεων Phishing δηλαδή την δημιουργία και αποστολή μηνυμάτων Phishing σε πραγματικούς παραλήπτες χωρίς ωστόσο να τίθεται σε πραγματικό κίνδυνο ο στόχος.

Συνήθως τέτοια εργαλεία επικεντρώνονται στο να αναγνωρίσουν τις ενέργειες που πραγματοποίησε ένας χρήστης χωρίς να συλλέγουν πραγματικά τα στοιχειά του η να έχουν κακόβουλο χαρακτήρα. Αυτά τα εργαλεία εμπίπτουν στις εξής κατηγορίες:

8.2.1 Basic Tools

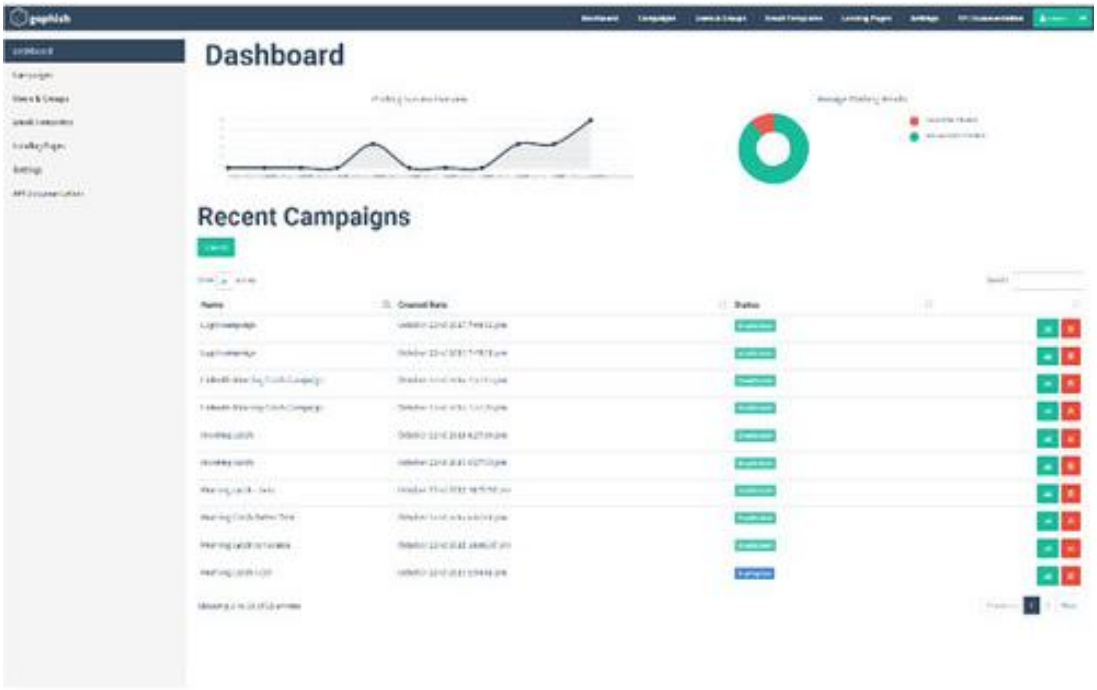
Επιτρέπουν την δημιουργία απλών μηνυμάτων ηλεκτρονικού ταχυδρομείου και την αποστολή σε έναν ή περισσότερους παραλήπτες χρησιμοποιώντας έναν συγκεκριμένο διακομιστή αλληλογραφίας. Συνήθως αποτελούν Plugins ή addons για υπάρχοντα εργαλεία Penetration Testing και διαθέτουν πολύ περιορισμένες δυνατότητες. Χαρακτηριστικά όπως η δημιουργία reports ή η διαχείριση των Campaigns συχνά δεν αποτελούν επιλογή, καθιστώντας τα κατά βάση ως εργαλεία Penetration Testing παρά ως ολοκληρωμένους προσομοιωτές.

8.2.2 Open Source Πλατφόρμες

Είναι μια ενδιαφέρουσα κατηγορία η οποία αποκτά όλο και περισσότερη προσοχή. Τα λογισμικά ανοιχτού κώδικα προσφέρουν όλα τα συνηθισμένα οφέλη, όπως οι δωρεάν εκδόσεις, η υποστήριξη απο online κοινότητες και την δυνατότητα παραμετροποίησης. Ταυτόχρονα όμως υπάρχουν και όλες οι συνηθισμένες αδυναμίες: εργαλεία όπως αυτά απαιτούν συνήθως ορισμένες σημαντικές τεχνικές δεξιότητες για την εγκατάσταση, τη παραμετροποίηση και την εκτέλεση τους. Επιπλέον, τα περισσότερα από αυτά είναι βασισμένα σε περιβάλλον Linux.

Gophish

Όντας μια πλατφόρμα ηλεκτρονικού ψαρέματος ανοιχτού κώδικα, η Gophish έχει καταφέρει να ισορροπήσει την ευκολία χρήσης με την λειτουργικότητα παρέχοντας απλά αλλά ιδιαίτερο ελκυστικά χαρακτηριστικά. Υποστηρίζεται από τα περισσότερα λειτουργικά συστήματα και η εγκατάσταση είναι τόσο απλή όσο η λήψη και η εξαγωγή ενός φακέλου ZIP, η διασύνδεση είναι απλή και διαισθητική και τα χαρακτηριστικά, αν και περιορισμένα, έχουν επιλεχθεί προσεκτικά.



Εικόνα 21 - Εργαλείο GoPhish | Περιβάλλον χρήσης

Οι χρήστες προστίθενται εύκολα, είτε χειροκίνητα είτε μέσω μαζικής εισαγωγής CSV. Τα templates των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι εύκολο να δημιουργηθούν (δεν έχουν συμπεριληφθεί εν τούτοις by default, ωστόσο μπορούν να γίνουν import μέσω repository που υποστηρίζεται από την κοινότητα) και να τροποποιηθούν χρησιμοποιώντας μεταβλητές που επιτρέπουν την εύκολη εξατομίκευση. Η δημιουργία των Campaigns είναι μια απλή διαδικασία και τα reports που παράγονται εμφανίζονται σε ελκυστική μορφή διαγραμμάτων ενώ μπορούν αν γίνουν και export ως raw data σε μορφή CSV με πολλαπλά επίπεδα λεπτομέρειας αναφορικά με τις ενέργειες του παραλήπτη. Παρολαυτα δεν υπάρχουν λειτουργίες εκπαίδευσης για την ευαισθητοποίηση όσον αφορά το Phishing καθώς επίσης και επιλογές για χρονικό προγραμματισμό της καμπάνιας σχετικά με την αυτοματοποιημένη αποστολή των emails.

Phishing Frenzy

Αυτή η εφαρμογή ανοιχτού κώδικα (Ruby on Rails) έχει σχεδιαστεί ως εργαλείο penetration testing, όμως διαθέτει πολλά χαρακτηριστικά που θα μπορούσαν να την καταστήσουν αποτελεσματική λύση για εσωτερικές καμπάνιες Phishing.

Το ποιο αξιόλογο χαρακτηριστικό είναι η δυνατότητα προβολής λεπτομερών στατιστικών στοιχείων καμπάνιας και η εύκολη αποθήκευση των πληροφοριών σε ένα αρχείο PDF ή ένα αρχείο XML. Αυτό ωστόσο που δεν την καθιστά ιδιαίτερα ελκυστική είναι το γεγονός ότι το Phishing Frenzy είναι μια εφαρμογή που υποστηρίζεται μόνο σε Linux, με την εγκατάσταση της να μην είναι εύκολα διαχειρίσιμη από έναν αρχάριο χρήστη.

Εικόνα 22 - Εργαλείο Phishing Frenzy| Περιβάλλον χρήσης

8.2.3 Demo εκδοχές εμπορικών προϊόντων.

Η πλειοψηφία των εμπορικών λογισμικών προσομοίωσης Phishing προσφέρεται ως Software-As-A-Service (SaaS). Με αυτά, συνεπάγονται όλα τα πλεονεκτήματα από τις πλήρης, εμπορικά διαθέσιμες εκδόσεις: ευκολία χρήσης, up to date δυνατότητες και templates, πλούσια χαρακτηριστικά (συμπεριλαμβανομένου του reporting), τεχνική υποστήριξη κλπ. Δεδομένου του όγκου των εργαλείων που παρέχονται και των vendors που πλέον εμπλέκονται είναι πολύ εύκολο κάνεις να αποκτήσει μια τέτοια δοκιμαστική έκδοση και να οργανώσει μια εκπαιδευτική Καμπανιά η ακόμα και να αξιολογήσει το υφιστάμενο προσωπικό.

Lucy

Το LUCY παρέχει δωρεάν λήψη της ελεύθερης (κοινότητας) έκδοσης της πλατφόρμας. Το μόνο που χρειάζεστε είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου και το όνομα του χρήστη και μπορεί να γίνει άμεση λήψη του LUCY ως Virtual Appliance ή ως installation script για την εγκατάσταση σε Debian Distro.

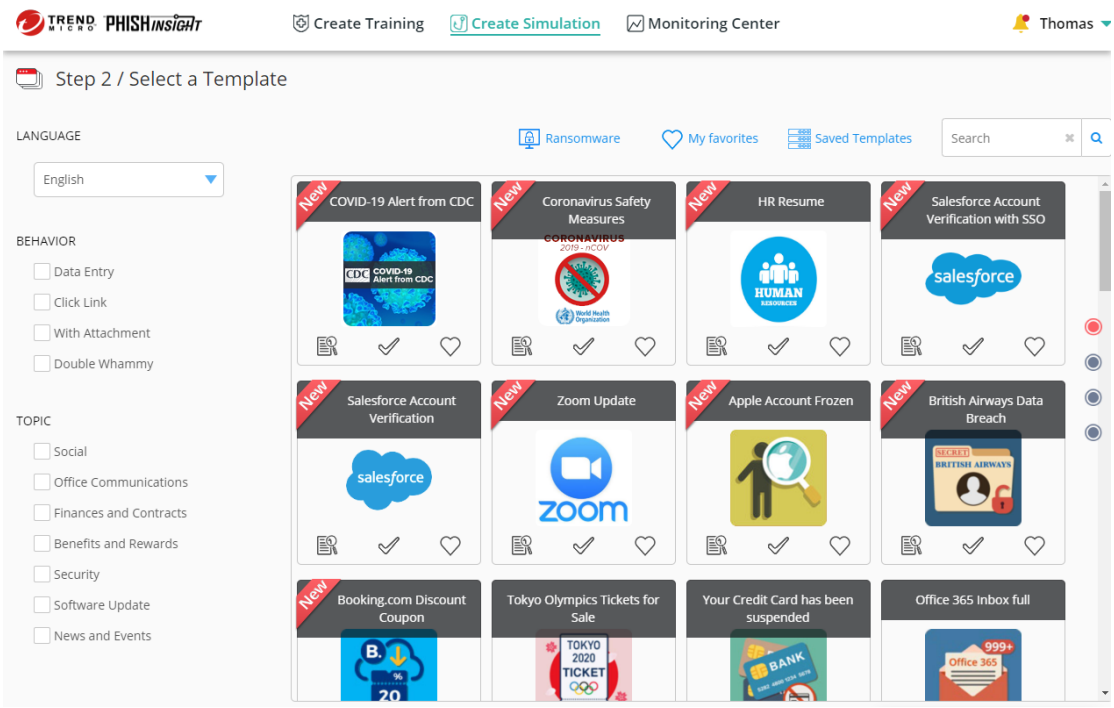
Το γραφικό περιβάλλον το οποίο συναντά ο χρήστης είναι ελκυστικό και υπάρχουν πολλά χαρακτηριστικά αφού το LUCY έχει σχεδιαστεί ως πλατφόρμα προσομοίωσης Κοινωνικής Μηχανικής που ξεπερνά τις επιθέσεις Phishing. Υποστηρίζει πολύ αποτελεσματικά εργαλεία για την ενίσχυση της ευαισθητοποίησης με αλληλεπιδραστικές ενότητες και ερωτηματολόγια αξιολόγησης, δυνατότητες για άμεσο feedback χρηστών κτλ.

Εικόνα 23 - Εργαλείο Lucy | Περιβάλλον χρήσης

Ωστόσο η δωρεάν έκδοση του LUCY έχει πάρα πολλούς περιορισμούς για να χρησιμοποιηθεί αποτελεσματικά σε ένα επιχειρηματικό περιβάλλον. Ορισμένες σημαντικές λειτουργίες δεν είναι διαθέσιμες στην ελεύθερη έκδοση, όπως εξαγωγή στατιστικών στοιχείων καμπάνιας, διεξαγωγή επιθέσεων με στόχο αρχεία (συννημένα) και, κυρίως, την δυνατότητα προγραμματισμού μιας καμπάνιας. Με αυτούς τους περιορισμούς λοιπόν η δωρεάν έκδοση μπορεί να αποτελέσει μια καλή εισαγωγή σε κάποιον ο οποίος θέλει να διερευνήσει το κομμάτι του Social Engineering σε βασικό επίπεδο. (26)

Phish Insight by Trend micro

Πρόκειται για μια πραγματικά σύγχρονη προσπάθεια για την παροχή ολοκληρωμένης εκπαιδευτικής λύσης αναφορικά με τις επιθέσεις Phishing. Η συγκεκριμένη πλατφόρμα διατίθεται και δωρεάν ως δοκιμαστική αλλά χωρίς να βάζει περιορισμούς στην λειτουργικότητα. Και εδώ μπορεί ο κάθε ενδιαφερόμενος να βρει ένα σύνολο λειτουργιών όπως έτοιμα templates για παραπλανητικά mails και landing pages. Αυτό όμως το οποίο το καθιστά πιο αποτελεσματικό είναι η παροχή ετοίμων σεναρίων. Ο χρήστης μπορεί να επιλέξει να ταξινομήσει τα σενάρια ανάλογα με την χρήση η την επίθεση που επιθυμεί να προσομοιώσει (π.χ. επίθεση με χρήση συνημμένου, επίθεση credentials harvesting κτλ.) (27)



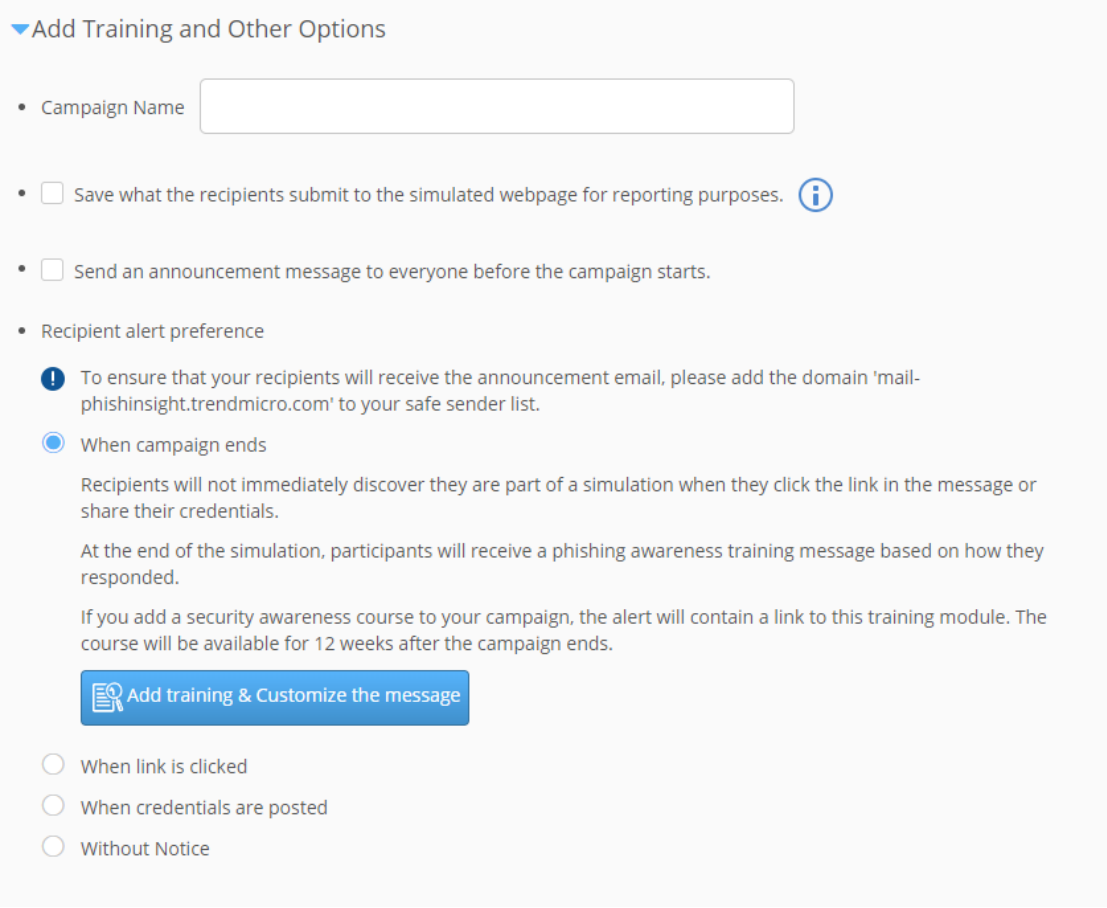
Εικόνα 24 - Εργαλειο Phish Insight | Συλλογη Templates

Επιπλέον δίνεται η δυνατότητα για τον προγραμματισμό των Campaigns και την οργάνωση πολλαπλών ώστε να τρέχουν παράλληλα. Ανάμεσα στις δυνατότητες προγραμματισμού είναι και η εισαγωγή πολλαπλών ομάδων παραληπτών, ο ορισμός του πότε θα αποσταλούν τα παραπλανητικά μηνύματα αλλά και ο ορισμός της χρονικής διαρκείς κατά την όποια θα γίνεται monitor η δραστηριότητα του παραλήπτη σχετικά με το μήνυμα.

Η πλατφόρμα τέλος μπορεί να παράγει αναλυτικά reports για όλες τις ενέργειες του χρηστή όπως το αν άνοιξε το mail αν επισκοπήθηκε το κακόβουλο link και αν τέλος εισήγαγε τα στοιχειά του στην παραπλανητική σελίδα.

Φυσικά εδώ μπορεί κανείς να βρει ενισχυμένες λειτουργίες για ανατροφοδότηση και εκπαίδευση των χρηστών. Υπάρχουν λοιπόν πολλαπλές επιλογές για να «κλείσει» μια επίθεση:

- Ο παραλήπτης δεν δέχεται καμία ενημέρωση η ανατροφοδότηση
- Ο παραλήπτης θα λάβει ενημέρωση πως έπεσε θύμα Phishing Attack
- Ο παραλήπτης θα λάβει μήνυμα πως έπεσε θύμα και μπορεί να συνοδεύετε και με ένα custom μήνυμα σχετικά με τις λεπτομέρειες της επίθεσης και τι θα έπρεπε να είχε προσέξει.
- Ο χρήστης θα μεταφερθεί σε μια εκπαιδευτική παρουσίαση σχετικά με το Social Engineering και τις επιθέσεις Phishing



Εικόνα 25 - Εργαλείο Phish Insight | Εκπαιδευτικές επιλογές και feedback χρηστών

9. Τρόποι και μηχανισμοί άμυνας

Αυτή η ενότητα θα ξεκινήσει με ένα απαισιόδοξο μήνυμα το όποιο όμως έχει αποδεδειχθεί ως πραγματικό γεγονός:

Δεν υπάρχει αποτελεσματικός και καθολικός τρόπος άμυνας εναντία σε επιθέσεις Κοινωνικής Μηχανικής.

Αυτό συμβαίνει διότι ανεξάρτητα του τι μέτρα προστασίας, τεχνικά και οργανωτικά, θα λάβει κανείς, οι επιθέσεις αυτές στηρίζονται στην συνιστώσα του ανθρώπινου παράγοντα η οποία είναι αδύνατο να προβλεφτεί αποτελεσματικά. Αυτό που έχει αποδειχτεί αποτελεσματικό σε ένα βαθμό είναι η προσπάθεια μείωσης της πιθανότητας να ολοκληρωθεί μια επίθεση επιτυχημένα και όχι η εξάλειψη της εμφάνισης της. Παρακάτω αναφέρονται οι τομείς που συστήνεται να επικεντρωθούν οι επιχειρήσεις και οι οργανισμοί. (28)

9.1 Σταθερά Θεμέλια: Πολιτική Ασφάλειας

Κανένα οίκημα δεν θα μπορέσει να σταθεί σταθερό χωρίς γερά θεμέλια. Η πολιτική ασφάλειας για έναν οργανισμό είναι ακριβώς: τα θεμέλια του για όλα τα επιπλέον τεχνικά και οργανωτικά μέτρα. Η πολιτική ασφαλείας καθορίζει τα πρότυπα και το επίπεδο ασφάλειας που θα έχει ένα σύστημα. Δίνει επίσης στο σύστημα αυτό η στο δίκτυο μια γνωστή κατάσταση που μπορεί θεωρείται αποδεκτή, δίνει καθοδήγηση για το τι δεν είναι αναμενόμενο και θεωρείται απόκλιση και δίνει επιπλέον τρόπους προσαρμογής για να παραμένει το σύστημα σταθερό ανάλογα με τις μεταβαλλόμενες ανάγκες και το εξωτερικό περιβάλλον ανάγκες.

Η κοινωνική μηχανική στοχεύει άτομα που πρέπει να γνωρίζουν πώς να ανταποκρίνονται σε αμφισβητήσιμα αιτήματα και παράδοξες καταστάσεις. Μια καθιερωμένη πολιτική λοιπόν που έχει συμπερίλαβε τις πτυχές του Social Engineering βοηθά τους τελικούς χρήστες με το να αισθάνονται σαν να μην έχουν άλλη επιλογή παρά να αντισταθούν στους ισχυρισμούς και τις πιέσεις ενός κακόβουλου τρίτου.

Δεν θα πρέπει να αναμένεται από τους υπάλληλους να κρίνουν και να αποφασίζουν αυθαίρετα για το εάν μπορούν ή όχι να παρασχεθούν ορισμένες πληροφορίες. Κάτι τέτοιο θα πρέπει να οριστεί εκ των προτέρων από ανθρώπους που έχουν σκεφτεί σοβαρά την αξία της κάθε πληροφορίας.

Μια πολιτική ασφάλειας πρέπει να απευθύνεται σε ορισμένους τομείς, προκειμένου να αποτελέσει σωστή βάση για την αντιμετώπιση στην Κοινωνική Μηχανική. Θα πρέπει να καλύπτει τομείς όπως ο έλεγχος πρόσβασης στις πληροφορίες, τη ρύθμιση λογαριασμών, την έγκριση πρόσβασης και τις αλλαγές κωδικού πρόσβασης, την τακτική εκπαίδευση των χρηστών, την φυσική ασφάλεια, και γενικότερα την διαχείριση της πληροφορίας ως αγαθό με αξία.

9.2 Ευαισθητοποίηση και Εκπαίδευση

Η ευαισθητοποίηση σχετικά με την ασφάλεια είναι η απλούστερη λύση και πιο αποτελεσματική λύση για την αποφυγή επιθέσεων κοινωνικής μηχανικής. Κάθε άτομο στα πλαίσια της εργασίας του σε μια εταιρία πρέπει να λαμβάνει βασική εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια τακτικά σε περιοδικά χρονικά διαστήματα. Όμως δεν αρκεί μόνο η ενημέρωση του προσωπικού για την ύπαρξη τέτοιων φαινομένων ούτε η αναφορά στις κατηγορίες αυτών των επιθέσεων.

Οι εργαζόμενοι πρέπει να γνωρίζουν ότι ένας επιτιθέμενος θα προσπαθήσει πρώτα να δημιουργήσει μια σχέση εμπιστοσύνης. Θα εκμεταλλευτεί στη συνέχεια την έμπιστη σχέση για να κερδίσει κάθε είδους πολύτιμες πληροφορίες. Πολλές πληροφορίες μπορούν να αποκτηθούν μέσω περιστασιακών συνομιλιών, όπως η εταιρική γλώσσα, τα ονόματα και οι θέσεις σημαντικών ατόμων στην εταιρεία, τα σημαντικά γεγονότα, η γενική οργανωτική δομή και τα συστήματα που χρησιμοποιούνται.

9.2.1 Εκπαίδευση ευαισθητοποίησης ασφάλειας για όλους τους χρήστες

Ο κάθε υπάλληλος θα πρέπει να γνωρίζει τις αρμοδιότητες και τη ευθύνη του απέναντι σε ανάλογα ζητήματα, και σαφώς θα πρέπει να γνωρίζει ότι δεν επιτρέπεται να αποκαλύπτει πληροφορίες χωρίς την κατάλληλη εξουσιοδότηση και να αναφέρει τυχόν ύποπτη συμπεριφορά. Σε γενικές γραμμές ένα πρόγραμμα εκπαίδευσης θα

πρέπει βασικά να ακολουθεί τις πολιτικές ασφάλειας, αλλά υπάρχουν ορισμένα βασικά σημεία που πρέπει να θυμηθούν όλοι οι χρήστες:

- **Τι έχει αξία;** - Οι περισσότεροι άνθρωποι υποτιμούν τα δεδομένα και την πρόσβασή τους μεχρι να ερθει η καταστροφική στιγμή ενός χαλασμένου σκληρού δίσκου. Θα πρέπει να σκεφτούν τι θα έκαναν αν ξαφνικά δεν είχαν πρόσβαση στον υπολογιστή τους. Κάτι τέτοιο ως ερέθισμα και τροφή για σκέψη θα τους βοηθήσει να καταλάβουν ότι αυτό που δουλεύουν για τα τελευταία χρόνια έχει κάποια αξία. Είναι λοιπόν μια καλή αρχή για να κατανοήσει κανείς την πραγματική σημασία της πληροφορίας και την χρησιμότητα της.

- **Οι «φίλοι» δεν είναι πάντα «φίλοι»** - Σχέσεις οι οποίες αναπτύσσονται μέσω τηλεφώνου όπως στην περίπτωση εξωτερικών συνεργατών η τεχνικών ή που για οποιονδήποτε λόγο θέτουν ερωτήσεις σχετικά με ευαισθητες πληροφορίες μπορεί να μην έχουν και τόσο αγνές προθέσεις. Οι επιτιθέμενοι συχνά συνάπτουν φιλικές σχέσεις με τα θύματά τους πολύ καιρό πριν ζητήσουν το οτιδήποτε. Οι χρήστες λοιπον θα πρέπει να κατανοήσουν ότι το γεγονός ότι κάποιος κάποιος φαίνεται να είναι φίλος δεν σημαίνει ότι μπορούν να εμπιστευτούν με εταιρικές πληροροφορίες η ευαίσθητα δεδομένα. Ανάλογα με την αξία των δεδομένων και το επίπεδο ασφάλειας που έχει οριστεί σε ένα σύστημα, οι επιτιθέμενοι μπορούν να περάσουν από πολλαπλά στάδια για να πείσουν έναν στόχο ότι πρόκειται για άτομα άξια εμπιστοσύνης. Αυτό θα μπορούσε ενδεχομένως να πραγματοποιηθεί σε μια χρονική περίοδο, συμπεριλαμβανομένων ημερών, εβδομάδων ή και ετών.

- **Οι κωδικοί πρόσβασης είναι προσωπικοί** - Παρά το γεγονός ότι ορισμένοι επιτιθέμενοι δεν θα ζητήσουν ποτέ κωδικό πρόσβασης, άλλοι θα καταλήξουν σε πολύ πειστικούς λόγους και μέσα για τους οποίους ένας υπάλληλος θα πρέπει να δώσει τον κωδικό του σε έναν άγνωστο. Δυστυχώς, χωρίς την κατάλληλη κουλτούρα, οι άνθρωποι τείνουν να αποκαλύπτουν τους κωδικούς χωρίς ιδιαίτερη σκέψη και φυσικά χωρίς να σκάφτονται τις πιθανές συνέπειες.

- **Οι κωδικοί πρόσβασης μπορούν να υποκλαπουν με πολλους τρόπους.** Οι ιστοσελίδες και τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν υποσχεθουν την διεκδικήση μεγάλα βραβεία με μόναδικο αντίτιμο την εγγραφή του χρήστη. Κάτι τέτοιο μπορεί να μοιάζει ευκαιρία και εντελώς ακίνδυνο αλλά δεν είναι πάντα έτσι.. Τα ονόματα χρηστών και οι κωδικοί πρόσβασης που χρησιμοποιούν πολλοί άνθρωποι σε ιστότοπους για προσωπική χρήση είναι συχνά οι ίδιοι με αυτούς που χρησιμοποιούνται στα εταιρικά profile και λογαριασμούς. Ετσι μια ψεύτικη κακόβουλή σελίδα συχνά άσχετου ενδιαφέροντος μπορεί να αποσπάσει δυνητικά έναν «master» κωδικό του θύματος που αν ο επιτιθέμενος σταθεί τυχερός θα λειτουργήσει για σχεδόν όλους τους λογαριασμούς του.

9.2.2 Επιπλέον ενίσχυση Προσωπικού σε κομβικές θέσεις

Τα βασικά στελέχη μιας επιχείρησης τα οποία αναμένεται να γίνουν οι πρώτοι στόχοι δεδομένης της φύσης εργασίας τους όπως το προσωπικό Help Desk, την Εξυπηρέτηση Πελατών, βοηθούς επιχειρήσεων, γραμματείς και receptionists και διαχειριστές συστημάτων / μηχανικούς θα πρέπει να αποκτούν επιπλέον «όπλα» προκειμένου να είναι σε θέση να αντισταθούν σε έναν επιτιθέμενο πιο άμεσα και αποτελεσματικά. Μια τέτοια εκπαιδευτική δομή μπορεί να περιλαμβάνει τεχνικές όπως:

- **Case Scenarios.** Ακριβώς όπως με έναν ιό όπου η ελεγχόμενη επαφή μαζί του μέσω του εμβολιασμού μπορεί να μας προκαλέσει την παράγωγη αντισωμάτων και να μας προστατέψει, το ίδιο μπορεί να επιτευχτεί και με την έκθεση των συμμετεχόντων σε ένα εκπαιδευτικό πρόγραμμα σε πραγματικά σενάρια κοινωνικής Μηχανικής. Οι εργαζόμενοι θα εκτίθενται στα επιχειρήματα που θα μπορούσε να χρησιμοποιήσει ένας κοινωνικός μηχανικός μαζί με ισχυρά αντεπιχειρήματα «επαναφοράς» που θα μπορούσαν να χρησιμοποιηθούν από τον εργαζόμενο για να διακοπεί η επίθεση. Μελέτες δείχνουν ότι αυτή είναι μια αποτελεσματική και μακροχρόνια τεχνική για την ενίσχυση της αντίστασης σε επιθέσεις τέτοιου τύπου διότι μαθαίνουν στους δέκτες να σκάφτονται με συγκεκριμένο τρόπο και να είναι έτοιμοι να

αντιδράσουν. Το πρόβλημα έγκειται στο ότι προϋποθέτει ότι ο εκπαιδευτής να είναι σε θέση να προβλέψει τα επιχειρήματα ενός επιτιθέμενου με ρεαλιστικό τρόπο

- **Προειδοποίηση.** Αυτή η τεχνική εμπλέκει τον εκπαιδευτή να δίνει μια ενημέρωση - προειδοποίηση στους συμμετέχοντες για το ότι πρόκειται να λάβουν ένα παραπλανητικό μήνυμα η να δεχτούν κάποια επίθεση στα πλαίσια της εκπαίδευσης. Αυτό κάνει τους συμμετέχοντες να είναι σε εγρήγορση και ενισχύει την συσχέτιση των ερεθισμάτων, την συνδυαστική σκέψη και κατ' επέκταση την αφομοίωση της γνώσης. Μελέτες έχουν δείξει ότι αν δοθεί μια ενημέρωση σχετικά με την φύση ενός παραπλανητικού μηνύματος (πχ ότι θα είναι επιτακτικό η πιεστικό) και αντίστοιχα δοθούν πληροφορίες πιο πρακτικές για το ίδιο μήνυμα (πχ ότι λείπει η υπογραφή, ότι θα υπάρχουν συντακτικά λάθη, ότι ίσως η διεύθυνση του αποστολές να διαφέρει), οι πρακτικές λεπτομέρειες της επιθέσεις τείνουν να αποτυπώνονται εντονότερα. Αυτό σημαίνει ότι όσο μεγαλύτερη η έκθεση ενός ατόμου σε παραπλανητικά mails με τα αντίστοιχα βοηθητικά στοιχειά (hints) τόσο πιο ισχυρό το καθιστούν στο να αναγνωρίσει στο μέλλον αλλά παρόμοια patterns.

- **Προσγείωση στην πραγματικότητα** Ένας από τους λόγους για τους οποίους αποτυγχάνει η εκπαίδευση στην ευαισθητοποίηση σχετικά με την ασφάλεια είναι ότι οι άνθρωποι τείνουν να έχουν μια μη ρεαλιστική αισιοδοξία αναφορικά με δυνατότητες τους. Αυτή η αντίληψη οδηγεί σαφώς σε μειωμένη προσοχή και συμμετοχή σε εκπαιδευτικά προγράμματα αφού τα άτομα αυτά τείνουν να τοποθετούνται εκτός της κατάστασης πιστεύοντας πως αν συνέβαινε στους ίδιους θα μπορούσαν να το αντιμετωπίσουν και συνεπώς οδηγεί πολλούς να αγνοήσουν πραγματικούς κινδύνους και να μην λάβουν τα κατάλληλα μέτρα για την αντιστάθμιση τους. Ωστόσο αυτό μπορεί να ανατραπεί εύκολα από τη στιγμή που θα ξεγελαστούν και τους αποδεικνύεται ότι είναι πράγματι ευάλωτοι και ότι η ενημέρωση πάνω σε αυτά τα ζητήματα είναι σημαντική. Υπάρχουν τρία στάδια αντίληψης και ευαισθησίας σε κίνδυνο. Το πρώτο είναι η συνειδητοποίηση – «Μαθαίνω και γνωρίζω ότι υπάρχει ο κίνδυνος» (Στο σημείο αυτό σταματούν οι περισσότερες εκπαιδευτικές δραστηριότητες ευαισθητοποίησης σχετικά με την ασφάλεια).

Το δεύτερο είναι η γενική ευαισθησία, που είναι η πίστη στην πιθανότητα κινδύνου για τους άλλους – «Γνωρίζω για τον κίνδυνο και πιστεύω πως θα μπορούσε να συμβεί σε κάποιον άλλο». Το τρίτο στάδιο είναι η προσωπική ευαισθησία, η οποία επιτυγχάνεται όταν κάποιος αναγνωρίζει την προσωπική του ευπάθεια. Για να αντιμετωπιστεί αυτό και να φτάσει κάνεις στο τρίτο επίπεδος τα πλαίσια ενός εκπαιδευτικού προγράμματος ενδείκνυται η διεξαγωγή καμπανιών με ρεαλιστικές επιθέσεις και άμεσο feedback έτσι ώστε ο εκπαιδευόμενος – θύμα να μπορεί να συσχετίσει άμεσα τα ερεθίσματα που έλαβε. Επιπλέον μπορεί να γίνεται και χρήση πραγματικών επιθέσεων με χρήση ειδικά εκπαιδευμένων ηθοποιών οι όποιο θα κληθούν να ενσαρκώσουν τον ρολό του κακόβουλου χρήστη για να επεκταθεί η όλη προσπαθεία και περα από το Phishing. Με αυτούς τους τρόπους ο εκπαιδευόμενος παύει να είναι ένας παθητικός δεκτής και μπορεί να αντιληφτεί αμέσως το ποσό εύκολο είναι να πέσει ο ίδιος θύμα αυξάνοντας έτσι κατακόρυφα την προσοχή του και την εγρήγορση του.

9.3 Φυσική Ασφάλεια

Θα πρέπει να υπάρχει κατάλληλος μηχανισμός ελέγχου πρόσβασης, ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένοι άνθρωποι έχουν πρόσβαση σε περιορισμένα τμήματα του οργανισμού. Κάθε ρόλος θα πρέπει να έχει σαφή οδηγία για την πρόσβαση που του επιτρέπεται και η διαβάθμιση θα πρέπει να αυξάνεται όσο αυξάνεται η σημαντικότητα του χώρου στα πλαίσια της εταιρίας (πχ computer room, λογιστήριο κτλ). Κάθε διαχωρισμός στους χώρους θα πρέπει να συνδυάζεται με access control τεχνικούς μηχανισμούς όπως για παράδειγμα η χρήση μαγνητικής κάρτας και οι περιοχές ύψιστης σημασίας θα πρέπει να είναι επιπλέον προστατευμένες. Πρέπει να διασφαλίζεται ακόμα ότι όλα τα φυσικά σημεία εισόδου και εξόδου είναι ασφαλισμένα ανά πάσα στιγμή

Ακόμα, πολύ σημαντική είναι και η διαχείριση των επισκεπτών. Είναι αναμενόμενο πως στα πλαίσια λειτουργίας μια επιχείρησης θα πρέπει να αποκτήσουν πρόσβασης τις εγκαταστάσεις άτομα που δεν ανήκουν στο προσωπικό όπως τεχνικοί συντήρησης, πελάτες, συνεργάτες, υποψήφιοι υπάλληλοι, καθαριστές κτλ. Σε αυτές

λοιπόν τις περιπτώσεις πρέπει να υπάρχει μια σαφής πολίτικη, ένα πρωτόκολλο το οποίο θα ορίζει το πώς θα εισέρχονται αυτά τα άτομα στις εγκαταστάσεις και τι ελευθερία κινήσεων θα έχουν. Συστήνεται να υπάρχει πάντα συνοδεία και επιπλέον να εφαρμόζονται μηχανισμοί όπως βιβλίο λίστας επισκεπτών και προσωρινή ταυτότητα επισκέπτη. Μια εταιρία θα πρέπει αν είναι πάντα σε θέση να κάνει trace back έναν επισκέπτη και να διασταυρώσει τα στοιχεία του.

9.4 Background Checks

Όπως αναφέρθηκε είναι συχνό το φαινόμενο κατά το οποίο ένας επιτιθέμενος θα αναλάβει έναν ξένο ρόλο και θα υποδυθεί κάποιο άλλο πρόσωπο. Υπάρχουν πολλές πιθανότητες ο εισβολέας να εισχωρήσει στην εταιρεία ως υπάλληλος, προκειμένου να συγκεντρώσει πληροφορίες εμπιστευτικές για την εταιρεία. Αυτός ο εισβολέας ενδέχεται να ακολούθησε όλες τις τυπικές διαδικασίες για να εμφανιστεί ως έγκυρος υπάλληλος.

Αυτό καθιστά τους ελέγχους των στοιχείων των εργαζομένων κατά την πρόληψη και την τακτική ενημέρωσης τους μια πραγματικά σημαντική προσθήκη στις πολιτικές της εταιρείας για την αντιμετώπιση της επίθεσης κοινωνικής μηχανικής.

Δεν πρέπει να περιορίζεται μόνο στους εσωτερικούς υπαλλήλους, αλλά πρέπει να επεκταθεί και στους πωλητές και στους λοιπούς συμβατικούς εργαζόμενους προτού καταστούν μέρος του οργανισμού ή αποκτήσουν πρόσβαση στο ευρύτερο δίκτυο της.

9.5 Ελαχιστοποίηση διαρροής δεδομένων

Ενδείκνυται να υπάρχει συνεχής παρακολούθηση ως προς το τι πληροφορίες σχετικά με τον οργανισμό βρίσκονται διαθέσιμες στο διαδίκτυο. Θα πρέπει να δίνεται ιδιαίτερη προσοχή σε αναρτήσεις σε εταιρικά Profiles και επίσημα Fan Pages σε τόπους κοινωνικής δικτύωσης αλλά και ενημέρωση του προσωπικού ώστε να αποφεύγονται ακούσιες διαρροές μέσα από τα προσωπικά τους Profiles.

- Οι υπάλληλοι θα πρέπει να αποφεύγουν να κοινοποιούν η να επικοινωνούν ακόμα και προφορικά πληροφορίες για την εργασία τους, όπως στοιχεία πελατών, υπάρχουσες πολιτικές, να κάνουν αναφορές σε συστήματα να δημοσιοποιούν το πρόγραμμα τους κτλ.

- Η χρήση της εταιρικής ταυτότητας των υπαλλήλων σε δημόσιους διαδικτυακούς χώρους όπως, blogs, φόρουμ συζητήσεων κ.λπ. θα πρέπει να περιοριστεί.
- Οι διαχειριστές των επίσημων ιστοσελίδων μιας εταιρείας σας θα πρέπει να είναι ιδιαίτερα προσεκτικοί ώστε να αποφεύγουν να δημοσιεύουν οργανωτικούς πίνακες, καταστάσεις προσωπικού σε αρχεία και φωτογραφίες όπου εμφανίζονται παρόμοια στοιχεία όπου είναι δυνατόν.

Επιπλέον στα πλαίσια της διασφάλισης της διαρροής πληροφοριών θα πρέπει να ληφθέν τα κατάλληλα τεχνικά μετρά ώστε να διασφαλίζεται κάθε φορητό μέσο από απώλεια η κλοπή. Μηχανισμοί όπως κρυπτογράφηση και κεντρικοποιημενη διαχείριση κινητών συσκευών θεωρούνται αποτελεσματικοί.

Τέτοιες τεχνικές θα καταστήσουν τη συγκέντρωση παθητικών πληροφοριών δύσκολη για τον επιτιθέμενο.

9.6 Διαβάθμιση Ασφάλειας

Πρέπει να υπάρχει καταγεγραμμένη και να εφαρμόζεται πολιτική για την κατάλληλη διαβάθμιση των δεδομένων με βάση τα επίπεδα κρισιμότητάς. Με βάση αυτή την ταξινόμηση και τον ρόλο τους μέσα στην εταιρία θα επιτρέπεται η αντίστοιχη πρόσβαση στο προσωπικό.

Η διαβάθμιση των δεδομένων αποδίδει ένα επίπεδο ευαισθησίας στις πληροφορίες που κατέχει η εταιρεία. Κάθε επίπεδο διαβάθμισης δεδομένων περιλαμβάνει διαφορετικούς κανόνες για την προβολή, επεξεργασία και κοινή χρήση τους.

Αυτό συμβάλει στην ισχυροποίηση των εργαζομένων ενάντια σε επιθέσεις κοινωνικής μηχανικής αφού διαθέτουν έναν σαφή μηχανισμό για να κατανοήσουν ποιες πληροφορίες μπορούν να αποκαλυφθούν και τι δεν μπορούν να μοιραστούν χωρίς την κατάλληλη εξουσιοδότηση

9.7 .Πρόσθετα μέτρα ενίσχυσης

- Προτείνεται η εγκατάσταση και η διατήρηση firewalls, λογισμικών antivirus και λογισμικών προστασίας από spyware και φίλτρα Spam στους email clients. Με αυτό τον τρόπο κακόβουλες επισυνάψεις και μηνύματα ενδέχεται να συναντήσουν πρόβλημα και να μην φτάσουν ποτέ εντός της εταιρίας.

- Οι υπάλληλοι θα πρέπει να είναι προσεκτικοί ώστε να μην επιτρέπουν σε άλλους ανθρώπους να χρησιμοποιούν την πρόσβαση τους στην εταιρία. Είναι πολύ κοινό το να προσπαθήσει κάποιος μη εξουσιοδοτημένος χρήστης να «περάσει» στην είσοδο πίσω από έναν έγκυρο εξουσιοδοτημένο χρήστη ακλουθώντας τον εκμεταλλευόμενος την έλλειψη προσωπικού φυσικής ασφάλειας , την αδιαφορία του έγκυρου χρήστη, και το χρονικό περιθώριο το οποίο έχει στην διάθεση του μέχρι να ξανακλείσει η πόρτα.
- Πρέπει να δίνεται προσοχή στη διεύθυνση URL ενός ιστότοπου. Συχνά τα φαινόμενα απατούν και ενδέχεται μια γνώριμη κατά τα αλλά σελίδα να διαφέρει ως προς την διεύθυνση της καθώς το URL μπορεί να χρησιμοποιεί μια παραλλαγή ορθογραφίας ή εξ ολοκλήρου διαφορετικό domain.
- Εταιρικοί λογαριασμοί οι οποίοι περιέχουν σημαντικά δεδομένα δεν όπως για παράδειγμα το ηλεκτρονικό ταχυδρομείο θα πρέπει να προστατεύονται από μη έμπιστα δίκτυα. Αυτό σημαίνει πως δεν θα πρέπει να επιτρέπεται η πρόσβαση σε δημόσιους χώρους, καφέ, και ξενοδοχεία και γενικότερα σε ελεύθερα και δημόσια δίκτυα. όπου δεν μπορεί να υπάρξει εμπιστοσύνη.
- Οι ευαίσθητες πληροφορίες θα πρέπει να αποστέλλονται μέσω του Διαδικτύου μόνο αφού γίνει έλεγχος και διαπιστωθεί η ασφαλής σύνδεση με τον εκαστοτε ιστοτοπο μέσω https.
- Δεν θα πρέπει να αποκαλύπτονται προσωπικά ή οικονομικά στοιχεία στο ηλεκτρονικό ταχυδρομείο και θα πρέπει να γίνει κατανοητό ότι δεν πρέπει να απαντώνται μηνύματα προτροπές που ζητούν αυτές τις πληροφορίες.
- Αντίστοιχα δεν θα πρέπει να αποκαλύπτονται προσωπικά στοιχεία σε άτομα για τα οποία δεν μπορούμε να είμαστε βέβαιοι για την ταυτότητα τους η την θέση τους στην ιεραρχία και το κατά πόσο έχουν εξουσιοδότηση να λάβουν αυτές τις πληροφορίες.
- Για τα φυσικά έγγραφα θα πρέπει να τηρείται κάποια πολιτική καταστροφής η οποία θα ορίζει πως θα καταστρέφονται (shredding) περιοδικά για την σωστή απόρριψη τους. Ομοίως θα πρέπει να υπάρχει μέθοδος καταστροφής και απόρριψης για τα ψηφιακά μέσα όπως φυσική καταστροφή οπτικών μέσων η ψηφιακή διαγραφή σκληρών δίσκων και USB drives πολλαπλών επιπέδων
- Τέλος κανένα από όλα αυτά τα μέτρα δεν μπορεί να διασφαλίσει 100% προστασία. Πρέπει λοιπόν να υπάρχει μια σωστή στρατηγική αντιμετώπισης

περιστατικών για τον οργανισμό για να μετριάσει την ζημιά και να περιορίσει πιθανές επιπλέον επιπτώσεις. Μια οργανωμένη και άμεση αντίδραση μπορεί να φάνει κρίσιμη και να ανακόψει τελικά την επίθεση του κακόβουλου χρήστη παρά την επιτυχημένη έναρξη της.

Μέρος ΙΙ

1. Μελέτη σε πραγματικές συνθήκες.

Στα πλαίσια της εκπόνησης της παρούσας εργασίας επιλέχθηκε μια πειραματική προσέγγιση για να διαπιστωθεί το κατά πόσο οι ψυχολογικοί μηχανισμοί οι οποίοι περιγράφηκαν όντως μπορούν να συμβάλουν σημαντικά στην επιτυχία μιας επίθεσης Phishing. Η μελέτη πραγματοποιήθηκε στο σύνολο των υπαλλήλων πολυεθνικής εταιρίας η οποία δραστηριοποιείται και στην Ελλάδα και διήρκησε συνολικά έξι μήνες, από τον Ιανουάριο του 2019 έως τον Ιούνιο του 2019.

1.1 Η Εταιρία

Πρόκειται για μία εταιρεία η οποία ανήκει στον ευρύτερο κλάδο fintech (finance & technology) και δραστηριοποιείται κυρίως στις αναπτυσσόμενες χώρες στην παροχή υπηρεσιών προστιθέμενης αξίας σε παρόχους τηλεπικοινωνιών όπως μικρό-δάνεια, οι ηλεκτρονικές πληρωμές και μεταφορές. Επιπλέον παρέχει και μια γκάμα υπηρεσιών σε διάφορους τομείς που σχετίζονται με την κινητή τηλεφωνία, όπως λύσεις για e–commerce, content marketing καθώς και υπηρεσίες στον τομέα του mobile advertising.

Στις εγκαταστάσεις της εταιρίας που βρίσκονται στην Αττική απασχολούνται σταθερά 64 εργαζόμενοι και ή οργανωτική δομή της εταιρίας διαμορφώνεται ως εξής:

Τμήμα Big Data & Analytics, Τμήμα IT & Engineering, Τμήμα Commercial & Customer Engagement, τμήμα Finance and Accounting, τμήμα Product Innovation, τμήμα Human Resources και τέλος τμήμα Back office.

Καθένα από αυτά τα τμήματα απαρτίζονται από έναν η παραπάνω διοικητικά στελέχη (Head of Department) και επιπλέον στην εταιρία φυσικά υπάρχει και ο Γενικός Διευθυντής.

Η διοίκηση της εταιρείας αναγνωρίζοντας την σημαντικότητα των δεδομένων που συλλέγουν και επεξεργάζονται αποφάσισαν να επενδύσουν στην Ασφάλεια Πληροφοριών και πιο συγκεκριμένα στο να λάβουν μία πιστοποίηση ISO 27001, και επιπρόσθετος, αποφασίστηκε υλοποίηση δράσεων προκειμένου να διασφαλιστεί η

όσο το δυνατόν μεγαλύτερη συμμόρφωση με το γενικό κανονισμό προστασίας προσωπικών δεδομένων.

Μετά από μία ανάλυση των αναγκών της εταιρείας διαπιστώθηκε πως στην πραγματικότητα δεν έχει δοθεί η πρέπουσα έμφαση στην Ασφάλεια Πληροφοριών. Αν και σε γενικές γραμμές η εταιρία έχει λάβει τεχνικά μέτρα όπως χρήση firewall και access control για συγκεκριμένες περιοχές εντοπίστηκαν ελλείψεις σε βασικές πολιτικές και μηχανισμούς προστασίας όπως για παράδειγμα κεντρικοποιημένα Access Rights πολιτικές καταστροφής εντύπων και πολιτικές φορητών μέσων.

Η μελέτη λοιπόν πραγματοποιήθηκε στα πλαίσια της ευρύτερης προσπάθειας συμμόρφωσης με το πρότυπο ISO 27001.

1.2 Συνοπτική περιγραφή πειράματος

Για το σχεδιασμό και την διεξαγωγή όλων των επιμέρους καμπανιών χρησιμοποιήθηκε το εργαλείο Phish Insight της Trend Micro. Προκειμένου να διερευνηθεί το επίπεδο ευαισθητοποίησης των εργαζομένων σε θέματα που αφορούν την Ασφάλεια Πληροφοριών διεξήχθη αρχικά μία πολύ βασική καμπάνια Phishing. Η καμπάνια αυτή κρίθηκε αρκετά απλή και όχι στοχευμένη έτσι ώστε να διερευνηθεί το πώς θα αντιδρούσε το σύνολο των εργαζομένων σε μία πιθανή επίθεση Mass Phishing.

Στην συνέχεια με την χρήση του εργαλείου Phish Insight τα αποτελέσματα των υπάλληλών αναλύθηκαν και αποτέλεσαν κεντρικό άξονα προκειμένου να διαμορφωθεί η πορεία της παρούσας Μελέτης.

Η υπόλοιπη μελέτη επικεντρώθηκε αρχικά στην διαπίστωση του κατά πόσο στέλνοντας διαφορετικά ερεθίσματα στους παραλήπτες μπορούμε να τραβήξουμε το ενδιαφέρον τους η να τους απωθήσουμε και συνεπώς να επηρεάσουμε την τελική έκβαση των αποτελεσμάτων. Στη συνέχεια το ενδιαφέρον στράφηκε στην αποτελεσματική οργάνωση μιας εκπαιδευτικής καμπάνιας Phishing και πιο συγκεκριμένα στο να εντοπιστεί το εάν υπάρχουν τρόποι ώστε μια ανάλογη εκπαιδευτική ενέργεια μπορεί να δώσει αντιπροσωπευτικά – πραγματικά αποτελέσματα και να θα διαρθρωθεί ως εξής:

1. Γενική Διερεύνηση – Αρχική Αξιολόγηση
2. Διερεύνηση της Έλξης
3. Διερεύνηση της Οικειότητας

2. Καμπάνια Phishing 1 - Αρχική Αξιολόγηση

Οι υπάλληλοι δεν είναι ενημερωμένοι και δεν έχουν καμία γνώση για το ότι πρόκειται να λάβουν τα αντίστοιχα παραπλανητικά emails. Συνεπώς τα αποτελέσματα αυτής της πρώτης καμπάνιας είναι καθαρά ενδεικτικά. Όλοι οι υπάλληλοι έλαβαν ταυτόχρονα ένα πολύ γενικό μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο αναφερόταν σε μια αποτυχημένη συναλλαγή που δεν έγινε δεκτή. Όπως φαίνεται από την εικόνα παρακάτω πρόκειται για μια εξαιρετικά απλή προσπάθεια. Ο παραλήπτης συναντά έναν πολύ γενικευμένο χαιρετισμό, μια πολύ απλή μορφοποίηση, ενω δεν αναφέρεται πουθενά η τράπεζα η οποία χρησιμοποιήθηκε και ως υπογραφή υπάρχει απλά το domain name από την ηλεκτρονική διεύθυνση του αποστολέα.

Ομοίως αν κάποιος ακολούθησε τον σύνδεσμο θα συναντήσει μια εξαιρετικά απλή οθόνη σύνδεσης χωρίς κανένα λογότυπο η κάποιο άλλο γραφικό στοιχειό.

2.1 Προγραμματισμός Καμπάνιας

Η εν λόγο καμπανιά πραγματοποιήθηκε χωρίς ιδιαίτερο προγραμματισμό από πλευράς παράδοσης των μηνυμάτων. Στόχος ήταν να προσομοιαστεί μια Mass Phishing επίθεση. Όλα τα μηνύματα λοιπόν στάλθηκαν την τελευταία εβδομάδα του Ιανουαρίου του 2019, συγκεκριμένα στις 29/01/2019

2.2 Πίνακας Περιγραφής Σεναρίου

Αποστολέας	**notification@paymoney.com**
Θέμα	**Your transaction was rejected**
Παραλήπτης	Σύνολο του προσωπικού (**65 υπάλληλοι**)
Σενάριο	**Ενημερωτικό email σχετικά με χρέωση η όποια δεν έγινε δεκτή**
Email Template	

Dear Sir/Madam

The transaction, recently initiated from your bank account, was rejected.

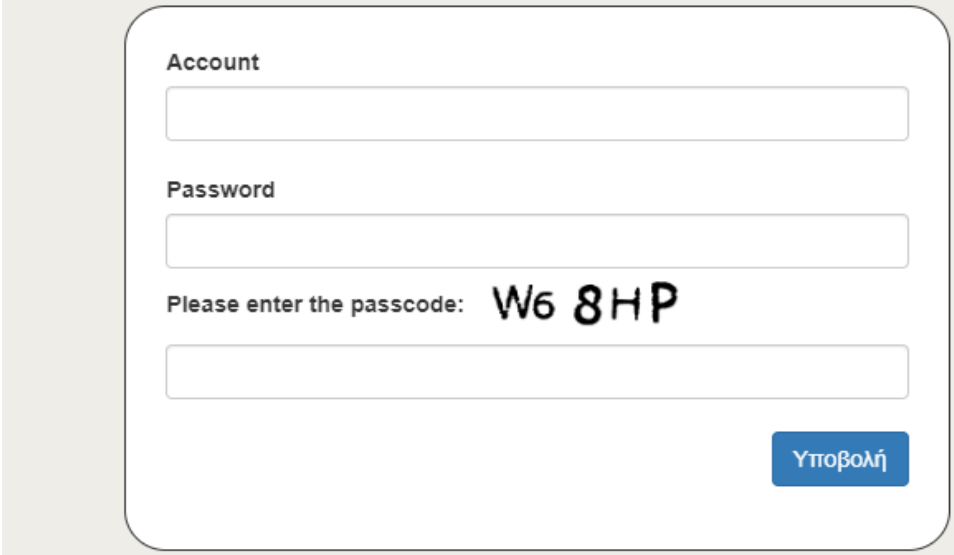
Aborted transaction	
Processing Case ID	AGLW19J
Amount	$3264.99 USD
Order Date	{{campaign_start_date}}
Reason for rejection	Open details

Please hit the link given above to have more details about your order.

Your bank account may be compromised

PayMoney.com 2019

Landing Webpage



3. Καμπάνια Phishing 2 - Διερεύνηση της Έλξης

Για να διερευνηθεί η παραδοχή ότι ως άτομα είμαστε πιο επιρρεπείς στο να επηρεαστούμε από άτομα τα οποία μας ελκύουν διεξήχθη μια καμπανιά η οποία βασίστηκε στο σενάριο Linkedin connection request. Όλοι οι συμμετέχοντες θα λάβουν ένα μήνυμα ηλεκτρονικού ταχυδρομείου το όποιο θα προέρχεται από ένα άγνωστο πρόσωπο το οποίο θα τους ζητά να συνδεθούν στο κοινωνικό αυτό δίκτυο.

Προκειμένου όμως να διαπιστωθεί το αν η εμφάνιση του προσώπου αυτού θα παίξει κάποιο ρόλο στο αποτέλεσμα της επίθεσης, οι συμμετέχοντες χωρίστηκαν σε 2 διαφορετικές ομάδες με την παρακάτω διάρθρωση. Σε αυτή την καμπάνια επιλέχτηκε τυχαία να μην συμμετάσχει ένας υπάλληλος για λόγους ομοιομορφίας των ομάδων.

Το προφίλ των εικονιζόμενων όπως και οι ίδιοι δεν είναι πραγματικά. Τα πρόσωπα είναι αποτέλεσμα μελέτης του 2002 σχετικά με την ελκυστικότητα και τα χαρακτηριστικά που καθιστούν ένα πρόσωπο πιο αρεστό. (29)

1. Για την $1^{η}$ ομάδα επιλέχθηκαν πρόσωπα τα οποία χαρακτηρίστηκαν ως ελκυστικά
2. Για την $2^{η}$ ομάδα επιλέχτηκαν πρόσωπα χαρακτηρισμένα ως μη ελκυστικά. Η επιλογή του ψεύδους προσώπου για τον κάθε υπάλληλο έγινε τυχαία

Όπως φαίνεται και στους πίνακες περιγραφής παρακάτω, το μήνυμα που έλαβαν οι χρηστές αποτελεί μια πιστή αντιγραφή του πραγματικού και ο μόνος τρόπος να διαπιστωθεί ότι πρόκειται για απάτη ήταν μόνο αν παρατηρήσει κανείς την διεύθυνση του αποστολέα με domain name «linkeIn» και όχι «LinkedIn».

3.1 Προγραμματισμός Καμπάνιας

Για να διεξήχθη η συγκεκριμένη Καμπάνια έτσι ώστε να μην κινήσει την υποψία των συμμετεχόντων, επιλέχθηκε τα μηνύματα να στέλνονται σταδιακά. Τα μηνύματα σταλθήκαν στην διάρκεια των 2,5 μηνών από τον Φεβρουάριο του 2019 έως και Απρίλιο του ιδίου έτους. Σταλθήκαν 6 μηνύματα ανά εβδομάδα και τα μηνύματα αποστέλλονταν κάθε δεύτερη ημέρα. Κάθε δεύτερη ημέρα λοιπόν στέλνονταν ένα ζευγάρι από τα εικονικά μας LinkedIn Profiles.

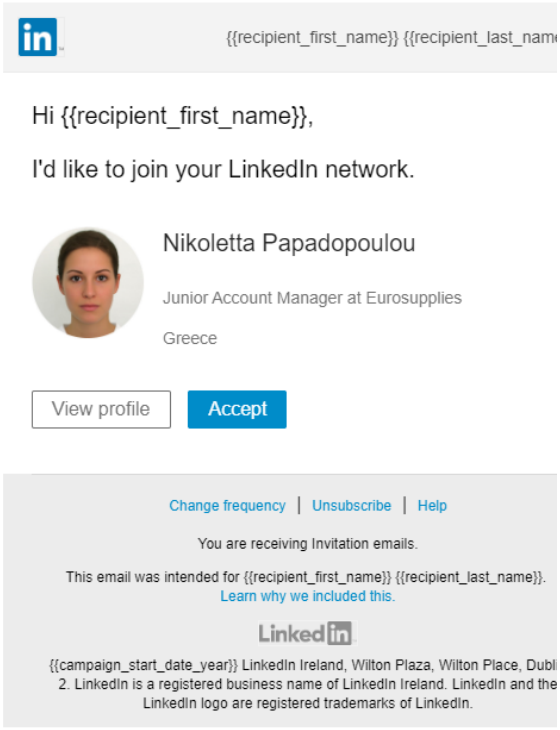
Αφού οι συμμετέχοντας χωρίστηκαν σε δυο ομάδες τους έγινε assign ένα τυχαίο Profile αναλόγως με την ομάδα στην όποια άνηκαν. Αφού αυτή η διαδικασία ολοκληρώθηκε και υπήρχε ένα διαθέσιμο ζευγάρι «Υπάλληλος – Linkedin Profile» για όλους έγινε ο χρονοπρογραμματισμός και κατά συνέπεια το πρόγραμμα αποστολής των εν λόγω μηνυμάτων διαμορφώθηκε ως εξής:

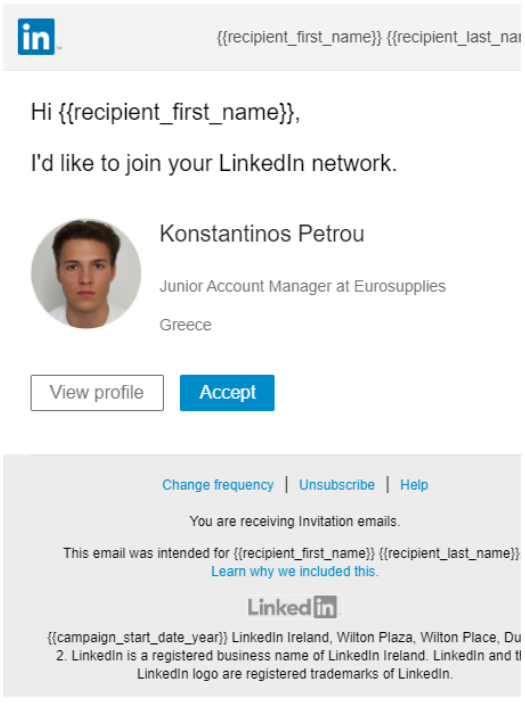
	Week 1			Week 2			Week 3			Week 4		
	Mon	Wed	Fri	Mon	Wed	Fri	Mon	Wed	Fri	Mon	Wed	Fri
Feb.	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√
										√√	√√	√√
Mar.	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√	√√
Apr.	√√	√√	√√	√√	√√	√√	√√	√√				

√ = Male Profile
√ = Female Profile

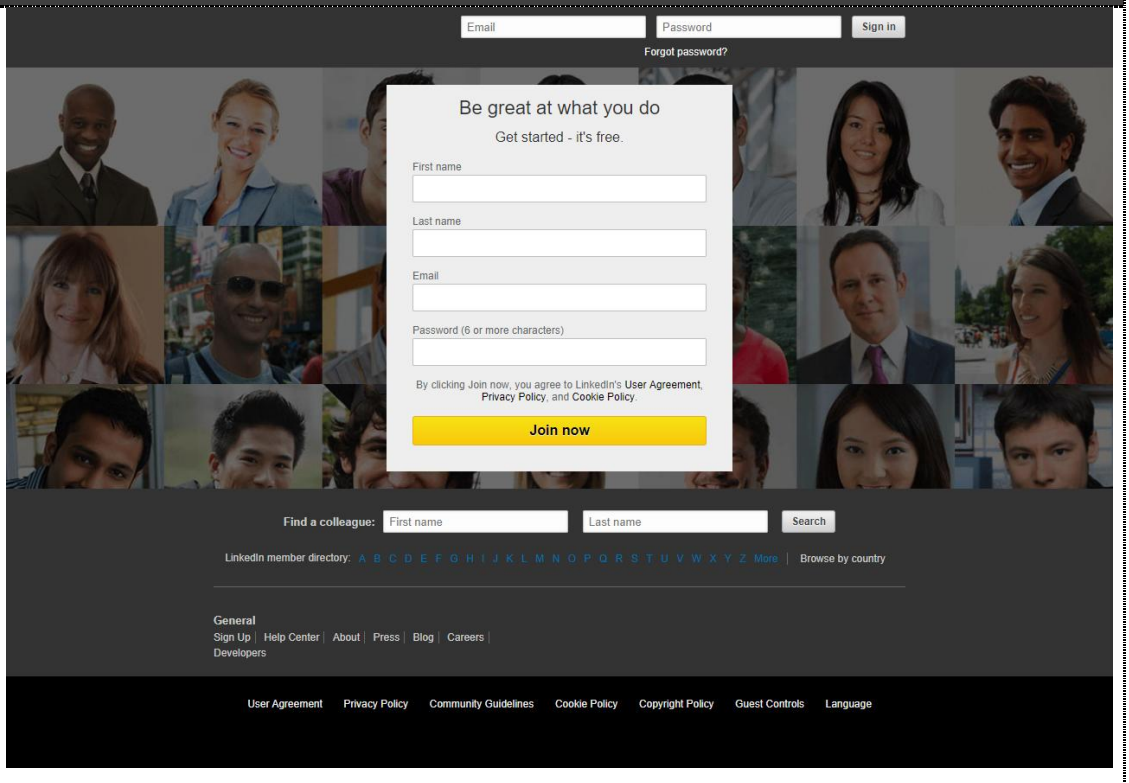
3.2 Πίνακας Περιγραφής Σεναρίου

Αποστολέας	**invitations@linkeIn.com**
Θέμα	**{{recipient_first_name}}, please add me to your Linkedln network**
Παραλήπτης	**Ομάδα 1 (32 υπάλληλοι)**
Σενάριο	**Αίτημα σύνδεσης σε λογαριασμό LinkedIn**
Email Template	





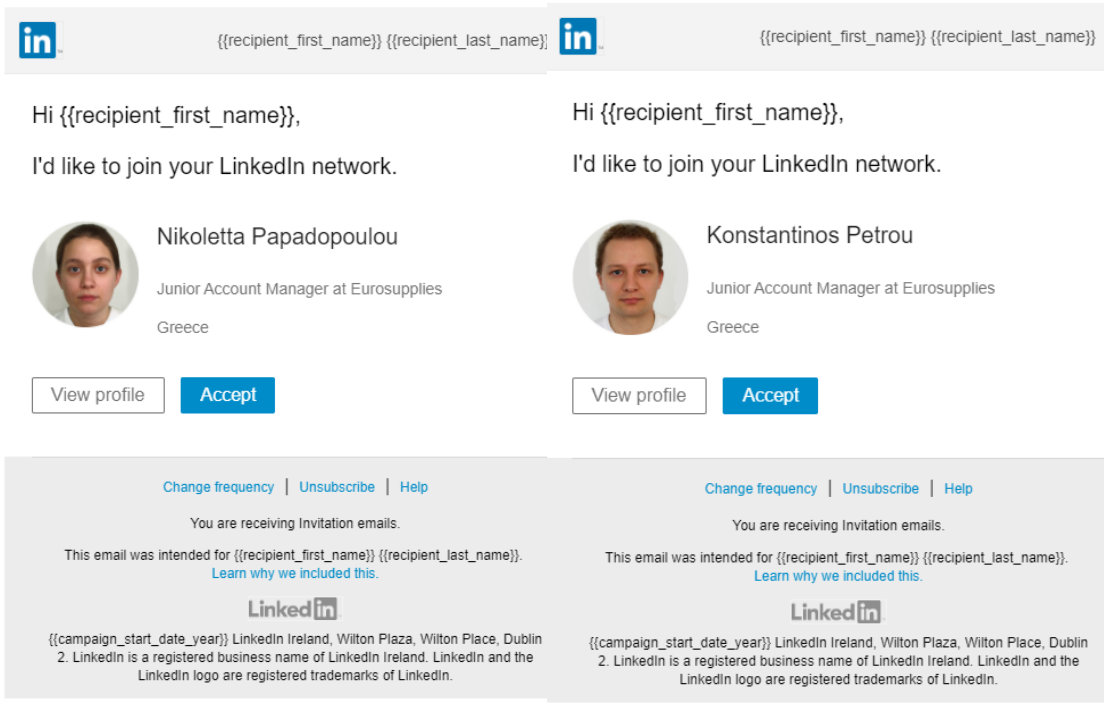
Landing Webpage



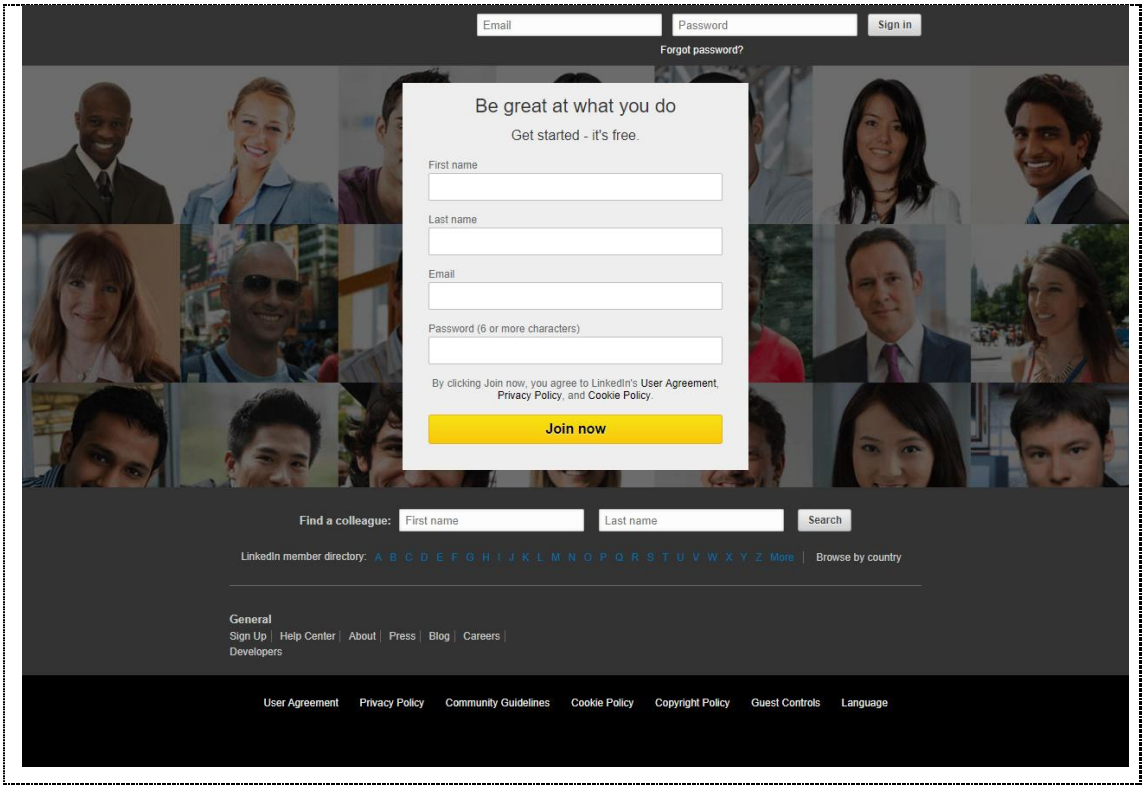
Αποστολέας	invitations@linkeIn.com

Θέμα	{{recipient_first_name}}, please add me to your Linkedln network
Παραλήπτης	Ομάδα 2 (32 υπάλληλοι)
Σενάριο	Αίτημα σύνδεσης σε λογαριασμό LinkedIn

Email Template



Landing Webpage



4. Καμπάνια Phishing 3 - Διερεύνηση της Οικειότητας

Για να διερευνηθεί η παραδοχή ότι οι άνθρωποι είναι πιο δεκτικοί σε οικεία πρόσωπα και καταστάσεις διεξήχθη μια καμπανιά η οποία στηρίχτηκε στην υπηρεσία Microsoft 365. Πιο αναλυτικά, όλοι οι υπάλληλοι της εταιρίας κάνουν χρήση έναν λογαριασμό 365 στον οποίο και στηρίζεται και η ηλεκτρονική αλληλογραφία τους. Επιπλέον κάνουν χρήση επιπρόσθετων υπηρεσιών όπως one drive, office 365 και teams. Συνεπώς θεωρείται πως το προσωπικό είναι ιδιαίτερα εξοικειωμένο με το brand της Microsoft αφού έχει κληθεί πολλαπλές φορές να συνδεθεί στις υπηρεσίες της. Σε αυτή την καμπάνια οι συμμετέχοντες έλαβαν ένα ενημερωτικό μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο τους ενημέρωνε πως θα πρέπει να συνδεθούν με το Microsoft account τους προκειμένου να διαβάσουν και να αποδεχτούν την ανανεωμένη πολίτικη απόρρητου της εταιρίας.

Γι να εξετάσουμε το πώς θα επηρεάσει την κρίση των παραληπτών μια τόσο γνώριμη σελίδα, χωρίσαμε το προσωπικό σε 2 ομάδες:

1. Η πρώτη ομάδα έλαβε ένα μήνυμα είχε σχεδιαστεί έτσι ώστε να θυμίζει το brand. Χρησιμοποιήθηκε κατάλληλη γραμματοσειρά και εικόνες και το τελικό αποτέλεσμα ήταν σαφώς πιο πειστικό. Ωστόσο χρησιμοποιήθηκε μια απλή λεύκη landing page η οποία προέτρεπε τον χρηστή να κάνει login.

2. Η Δεύτερη ομάδα έλαβε το προσαρμοσμένο οπτικά μήνυμα και οδηγήθηκε σε ένα πιστό αντίγραφο της οθόνης σύνδεσης (login) της Microsoft.

4.1 Προγραμματισμός Καμπάνιας

Για την συγκεκριμένη καμπάνια επιλέχτηκε και πάλι για τους ίδιους λόγους (να παραμείνουν οι υπάλληλοι ανυποψίαστοι) να παραδοθούν τα emails κυλιόμενα και όχι ταυτόχρονα σε όλους . Τα μηνύματα σταλθήκαν στην διάρκεια των 1 περίπου μήνα (Μάιο και Ιούνιο 2019).

Αφού οι συμμετέχοντας χωρίστηκαν σε δυο ομάδες τους έγινε assign ένα τυχαίο Landing Page (πειστικό ή μη πειστικό) αναλόγως με την ομάδα στην όποια άνηκαν. Αφού αυτή η διαδικασία ολοκληρώθηκε και υπήρχε ένα διαθέσιμο ζευγάρι «Υπάλληλος – Landing Page» για όλους έγινε ο χρονοπρογραμματισμός.

Θα στέλνονταν τυχαία 3 μηνύματα ανά ημέρα όπως φαίνεται παρακάτω ξεκινώντας στις 14 Μαΐου και ολοκληρώνοντας τις αποστολές στις 12 Ιουνίου

Αναλυτικότερα το πρόγραμμα αποστολής των εν λόγω μηνυμάτων διαμορφώθηκε ως εξής:

	Week 1					**Week 2**					**Week 3**					**Week 4**				
	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F	M	T	W	T	F
May							√	√	√	√	√	√	√	√	√	√	√	√	√	√
June	√	√	√	√	√	√	√	√												

√ = x3 emails
√ = x2 emails

4.2 Πίνακας Περιγραφής Σεναρίου

Αποστολέας	ITsupport@{{user_email_domain}}.com
Θέμα	O365 Privacy Policy Update Notice
Παραλήπτης	Ομάδα 1 (32 υπάλληλοι)
Σενάριο	Ενημερωτικό μήνυμα από Microsoft για ανανεωμένη πολιτική απορρήτου την όποια αν ο χρήστης δεν αποδεχτεί δεν θα μπορεί να κάνει χρήση των υπηρεσιών της. Το email μοιάζει πειστικό αλλά το hyperlink που εμπεριέχεται θα οδηγήσει σε μια φανερά διαφορετική σελίδα.

Email Template

Landing Webpage

Αποστολέας	ITsupport@{{user_email_domain}}.com
Θέμα	O365 Privacy Policy Update Notice
Παραλήπτης	Ομάδα 2 (32 υπάλληλοι)
Σενάριο	Ενημερωτικό μήνυμα από Microsoft για ανανεωμένη πολιτική απορρήτου την όποια αν ο χρήστης δεν αποδεχτεί δεν θα μπορεί να κάνει χρήση των υπηρεσιών της. Το email μοιάζει πειστικό αλλά το hyperlink που εμπεριέχεται θα οδηγήσει σε μια πανομοιότυπη σελίδα με την αυθεντική
Email Template	

Office 365

Hi {{recipient_first_name}}

At Microsoft we respects the privacy of our users. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our website and use our services, including any other media form, media channel, mobile website, or mobile application related or connected thereto. Please read this privacy policy carefully.

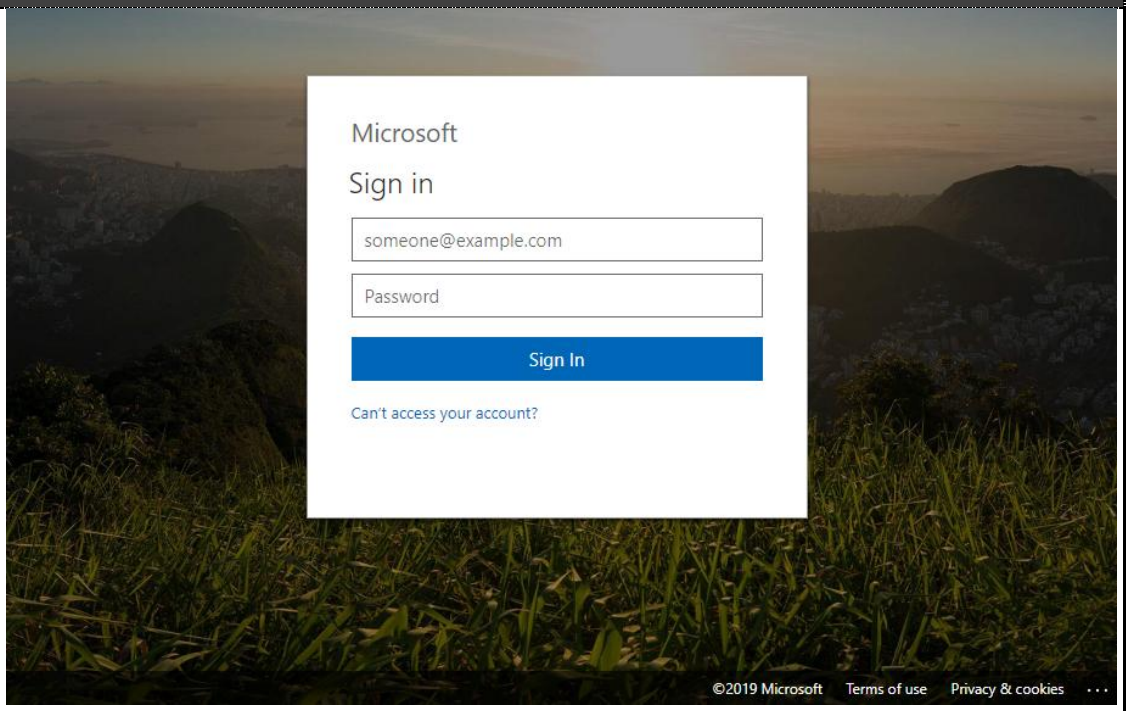
If you do not agree with the terms of this privacy policy, **you will not be able to access this site and its services.**

Please read our updated Privacy Policy.

Note: This message was sent from an un-monitored mailbox, please do not respond

Microsoft

Landing Webpage



5. Παρουσίαση Αποτελεσμάτων και Συμπεράσματα

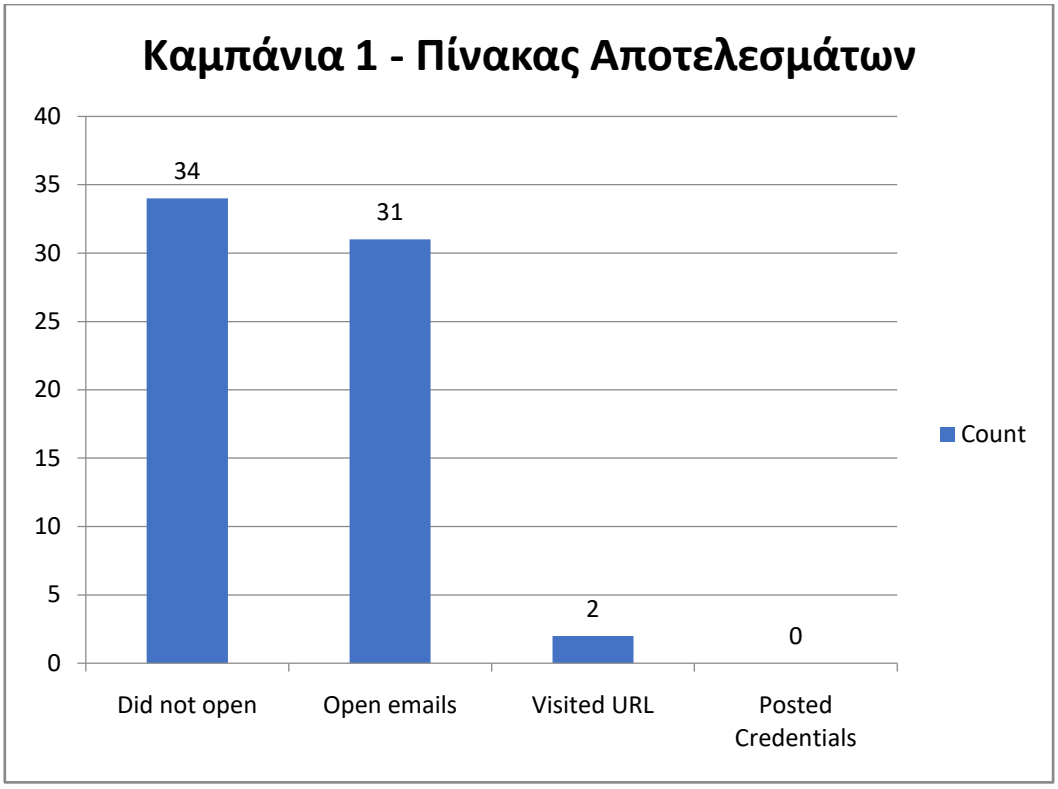
Σε αυτό το σημείο θα παρουσιαστούν τα αποτελέσματα των Campaigns που οργανώθηκαν και επιπλέον θα κοινοποιηθούν τυχόν συμπεράσματα που μπορέσαμε να εξάγουμε από αυτή την σύντομη μελέτη.

5.1 Αποτελέσματα – Καμπάνια 1

Συνοψίζοντας τα αποτελέσματα της καμπάνιας και λαμβάνοντας υπόψη ότι συνολικά 65 υπάλληλοι έλαβαν το μήνυμα ηλεκτρονικού ταχυδρομείου, οι ενέργειες των παραληπτών εμφανίζονται ως εξής

- Ένα σύνολο 34 υπαλλήλων δεν άνοιξε το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
- Συνολικά 31 εργαζόμενοι άνοιξαν το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
- Από όσους το άνοιξαν, μόνο 2 προχώρησαν στο να ακολουθήσουν τον σύνδεσμο που περιείχε το παραπλανητικό μήνυμα.
- Κανένας από τους 2 αυτούς υπάλληλους δεν προχώρησε στην εισαγωγή των διαπιστευτηρίων του.

Πέντε άτομα ανέφεραν το περιστατικό. Από αυτούς ο ένας υπάλληλος ανέφερε πως άνοιξε το μήνυμα από φόβο για πιθανή χρηματική απάτη. Οι υπόλοιποι τρεις ανέφεραν πως το άνοιξαν από περιέργεια και οι δυο από αυτούς υποστήριξαν πως για τον ίδιο λόγο προχώρησαν στο να επισκευθούν την σελίδα δεδομένου ότι η όλη προσπάθεια φάνηκε ερασιτεχνική και ακίνδυνη.



Αυτή η πρώτη καμπανιά μας δείχνει αποτελέσματα σχετικά αναμενόμενα για το background της εταιρίας.

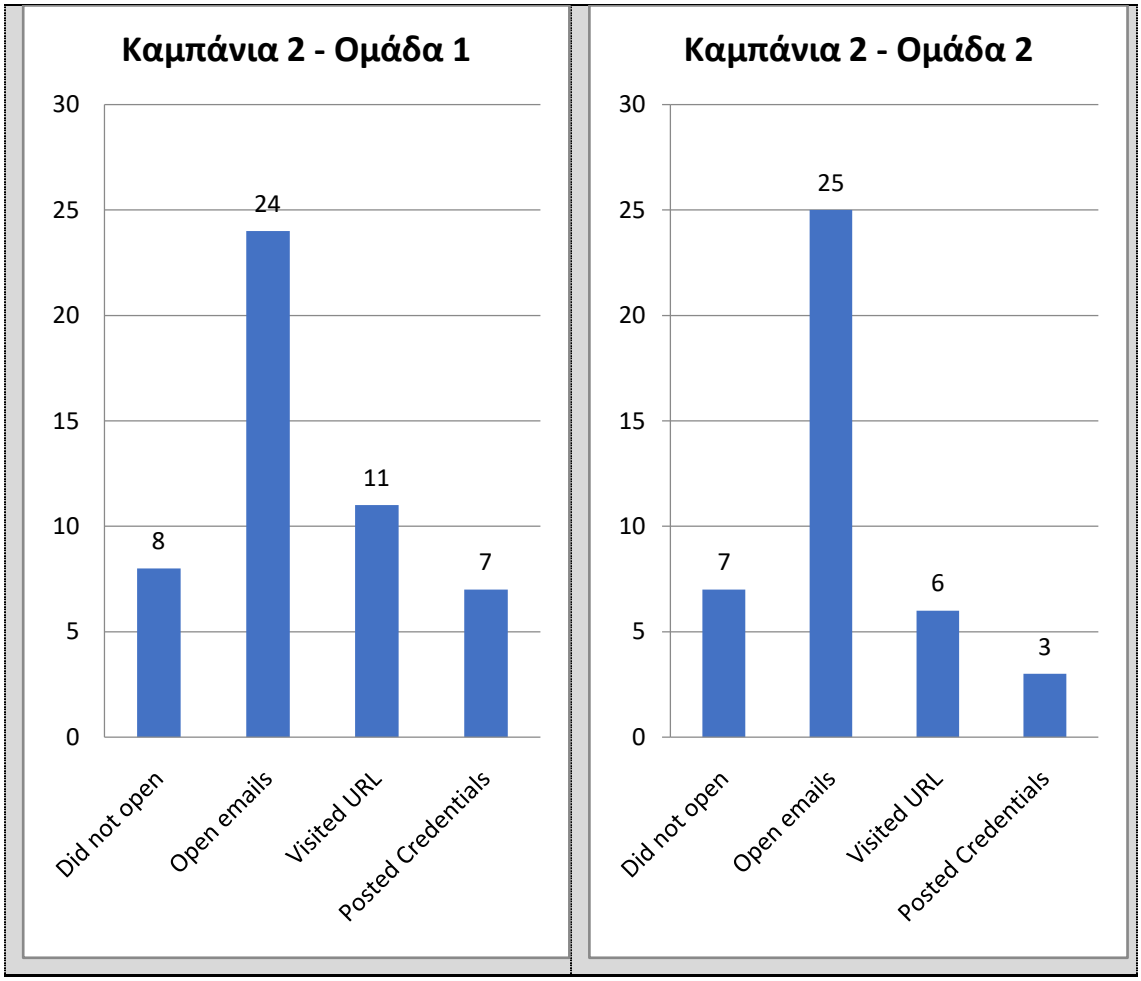
Οι περισσότεροι χρηστές είναι ιδιαίτερα εξοικειωμένοι με την χρήση του διαδικτύου και χρησιμοποιούν καθημερινά τον εταιρικό τους λογαριασμό για να λαμβάνουν και να αποστέλλουν emails. Παρατηρούμε ότι σχεδόν οι μισοί παραλήπτες προχώρησαν στο άνοιγμα του κακόβουλου email. Αυτό φαινομενικά ίσως να θεωρείται αποδεκτό αλλά πρέπει κανείς να αναλογιστεί πως οι παραλήπτες έλαβαν ένα μήνυμα το οποίο αναφερόταν σε αποτυχημένη πληρωμή. Ένα τέτοιο μήνυμα υπό κανονικές συνθήκες δεν θα έπρεπε να φτάσει σε έναν εταιρικό λογαριασμό δεδομένου ότι οι υπάλληλοι τηρούν τις πρακτικές ορθής χρήσης και δεν χρησιμοποιούν τον εταιρικό τους λογαριασμό για προσωπική χρήση. Είναι λοιπόν λογικό να θεωρήσουμε πως τα άτομα τα οποία προχώρησαν και άνοιξαν αυτό το μήνυμα οδηγηθήκαν από δυο συναισθήματα: την περιέργεια και τον φόβο. Περιέργεια ως προς το για ποιο λόγο έχει φτάσει κάτι τέτοιο στον λογαριασμό τους και φόβο για το κατά πόσο κάτι τέτοιο έχει πραγματική υπόσταση και άρα επιπτώσεις στον λογαριασμό τους.

5.2 Αποτελέσματα – Καμπάνια 2

Συνοψίζοντας τα αποτελέσματα της δεύτερης καμπάνιας και λαμβάνοντας υπόψη ότι συνολικά 64 υπάλληλοι έλαβαν το μήνυμα ηλεκτρονικού ταχυδρομείου, οι ενέργειες των παραληπτών εμφανίζονται στον παρακάτω συγκριτικό πίνακα και για τις 2 ομάδες.

Σε αυτό το σημείο θα πρέπει να αναφερθεί πως δεν υπήρξε καμία αφορά από καποιον υπάλληλο σχετικά με το παρόν παραπλανητικό email.

Ομάδα 1 – Ελκυστικό Πρόσωπο	**Ομάδα 2 – Μη Ελκυστικό Πρόσωπο**
Ένα σύνολο 8 υπαλλήλων δεν άνοιξε το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.	Ένα σύνολο 7 υπαλλήλων δεν άνοιξε το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
Συνολικά 24 εργαζόμενοι άνοιξαν το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.	Συνολικά 25 εργαζόμενοι άνοιξαν το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
Από όσους το ανοιξαν, οι 11 προχώρησαν στο να επισκευθούν τον σύνδεσμο που περιείχε το παραπλανητικό μήνυμα	Από όσους το ανοιξαν, οι 6 προχώρησαν στο να επισκευθούν τον σύνδεσμο που περιείχε το παραπλανητικό μήνυμα
Από του υπάλληλους που ακολουθησαν τον σύνδεσμο, 7 άτομα προχωρησαν στην εισαγωγή των διαπιστευτηρίων τους.	Από του υπάλληλους που ακολουθησαν τον σύνδεσμο, 3 άτομα προχώρησαν στην εισαγωγή των διαπιστευτηρίων τους.



Εδώ χωρίς να έχουμε κάποιο feedback από τους παραλήπτες μπορούμε να δούμε πως τα αποτελέσματα αναφορικά με το άνοιγμα η μη του μηνύματος είναι παρεμφερή. Αρχικά θα πρέπει να ανέρθει πως μετά από μια σύντομη αναζήτηση διαπιστώθηκε ότι 5 υπάλληλοι δεν διέθεταν λογαριασμό LinkedIn η τουλάχιστον δεν μπορούσε κανείς να τους εντοπίσει με μια απλή αναζήτηση. Για τον λόγο αυτό τυχαία επιλέχτηκε ένα άτομο από αυτά να μην συμμετάσχει για να έχουμε όσες ομάδες των 32 ατόμων.

Τα άτομα που δεν άνοιξαν το μήνυμα έχουν μια ελάχιστη απόκλιση. Μπορούμε να υποθέσουμε πως στα άτομα που δεν άνοιξαν το μήνυμα συμπεριλαμβάνονται οι χρηστές χωρίς λογαριασμό και επιπλέον κάποιοι χρηστές που ίσως εντόπισαν το περιστατικό είτε λογά της διεύθυνσης του αποστολέα είτε διότι συσχέτισαν το γεγονός και κατάλαβαν πως ένα τέτοιο μήνυμα θα έφτανε στον προσωπικό και όχι στον εταιρικό λογαριασμό τους.

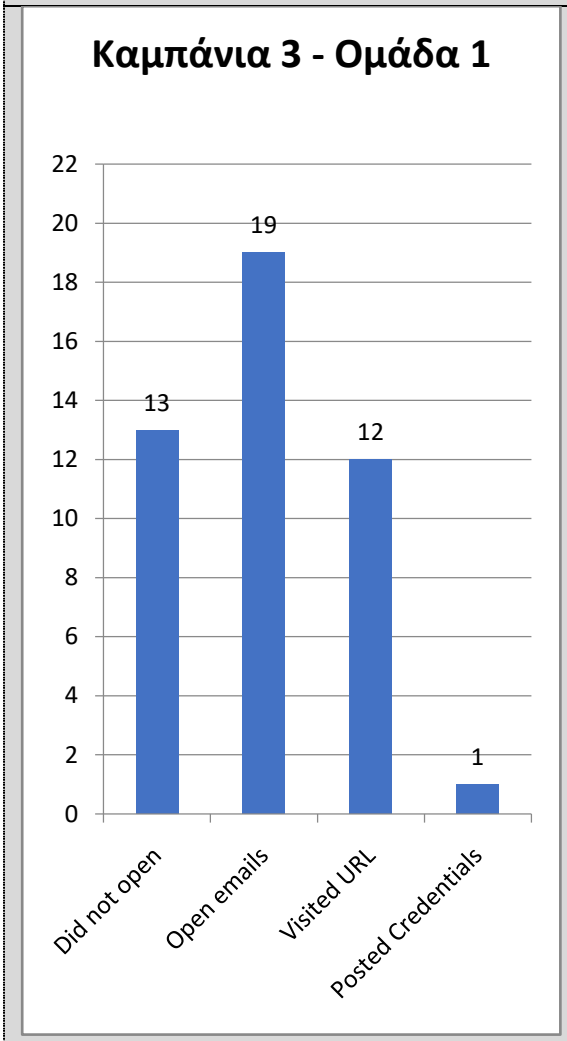
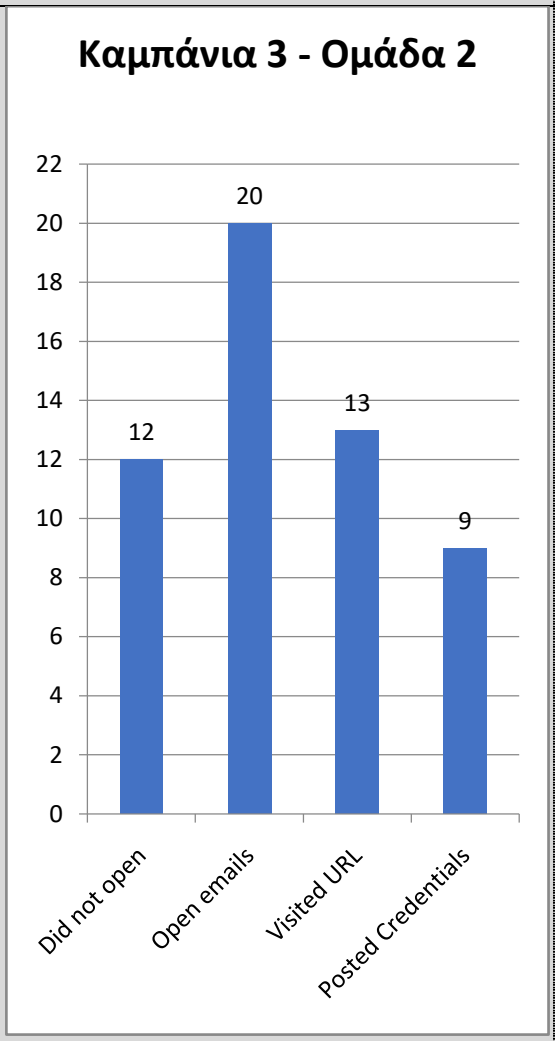
Από εκεί και πέρα τα αποτελέσματα αρχίζουν να εμφανίζουν μια τάση αφού σχεδόν τα διπλασία άτομα από την ομάδα που έλαβε το μήνυμα με την ελκυστική

φωτογραφία Profile ακλούθησαν τον σύνδεσμο και αντίστοιχα τα διπλασία άτομα προχώρησαν στο να συνδεθούν. Φυσικά αναγνωρίζεται πως το δείγμα είναι αρκετά μικρό για να εξάγει κανείς σημαντικά συμπεράσματα αλλά ωστόσο το αποτέλεσμα μας δείχνει να συνάδει με την θεωρία της έλξης. Οι συμμετέχοντες ήταν πιο πρόθυμοι να δεχτούν το αίτημα από το ελκυστικό άτομο και ίσως αυτό έπαιξε ρολό στο να μην εντοπίσουν τα σημάδια της απάτης.

5.3 Αποτελέσματα – Καμπάνια 3

Εδώ υπήρξε σημαντική συμμέτοχη από τους παραλήπτες. Από τους συνολικά 36 χρήστες που άνοιξαν το μήνυμα οι 7 ανέφεραν το περιστατικό με τους 3 από αυτούς να εντοπίζουν την μη αυθεντικότητα στο μήνυμα λόγω του ότι «θύμιζε παλιό». Αυτό σημαίνει πως πιο προσεκτικοί και παρατηρητικοί χρηστές ίσως μπήκαν στην διαδικασία να συγκρίνουν νοητά παρόμοιο μήνυμα και να καταλάβουν πως πρόκειται για παλαιότερο Template. Από αυτά τα 7 άτομα τα 6 προχώρησαν στο να επισκεφθούν τον σύνδεσμο και εκεί τα 2 από αυτά συνάντησαν την σελίδα κλώνο την οποία και δεν εμπιστευτήκαν επηρεασμένοι από το σχεδιασμό του μηνύματος παρόλο που η σελίδα τους φάνηκε έγκυρη. Τα υπόλοιπα 4 άτομα ανέφεραν πως οδηγηθήκαν ε μια φανερά κακόβουλη σελίδα καθώς δεν θύμιζε σε τίποτα το Login interface της Microsoft.

Ομάδα 1 – Generic Landing Page	**Ομάδα 2 – Custom Landing Page**
Ένα σύνολο 13 υπαλλήλων δεν άνοιξε το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.	Ένα σύνολο 12 υπαλλήλων δεν άνοιξε το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
Συνολικά 19 εργαζόμενοι άνοιξαν το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.	Συνολικά 20 εργαζόμενοι άνοιξαν το παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου.
Από όσους το ανοιξαν, οι 12 προχώρησαν στο να επισκευθούν τον σύνδεσμο που περιείχε το παραπλανητικό μήνυμα	Από όσους το ανοιξαν, οι 13 προχώρησαν στο να επισκευθούν τον σύνδεσμο που περιείχε το παραπλανητικό μήνυμα

Από του υπάλληλους που ακολουθησαν τον σύνδεσμο, 1 άτομο προχώρησε στην εισαγωγή των διαπιστευτηρίων του.	Από του υπάλληλους που ακολουθησαν τον σύνδεσμο, 9 άτομα προχώρησαν στην εισαγωγή των διαπιστευτηρίων τους.
	

Εδώ τα αποτελέσματα ήταν τα αναμενόμενα. Οι χρηστές ασχολήθηκαν με το συγκεκριμένο μήνυμα δεδομένου ότι υπήρχε η εξοικείωση με την αναγραφόμενη υπηρεσία. Ωστόσο οι 2 παρατηρητικοί χρηστές οι όποιοι διαπίστωσαν πως κάτι δε πάει καλά με το μήνυμα που έλαβαν καθώς τους ξένισε. Επηρεάστηκαν λοιπόν τόσο που ακόμα και όταν επισκέφτηκαν μια φαινομενικά εύρη σελίδα δεν προχώρησαν στο να συνεχίσουν με την σύνδεση. Αντίθετα όπως είναι αναμενόμενο μόνο 1 χρήστης πείστηκε να προχωρήσει σε αντίθεση με την ομάδα που συνάντησε την πειστική σελίδα με 9 «θύματα». Εδώ μπορούμε να δούμε εύκολα πως η ομοιότητα και κάτι το γνώριμο έπαιξε σημαντικό ρόλο στα αποτελέσματα της επίθεσης.

5.4 Γενικές Παρατηρήσεις Μελέτης

Συνοπτικά λοιπόν κρίνοντας από το σύνολο και ανάμεσα στα σενάρια που χρησιμοποιήθηκαν μπορούμε να καταλήξουμε στα εξής:

- Οι μικρές διαφορές κάνουν την διάφορα. Μια επίθεση μπορεί να κριθεί από την γραμματοσειρά που χρησιμοποίησε ο επιτιθέμενος και από τον τρόπο γραφής.
- Τα σενάρια που εμπλέκεται κάποιο πρόσωπο τείνουν να είναι πιο αποτελεσματικά στο να κινήσουν το ενδιαφέρον των θυμάτων. Όσο πιο γενικευμένο και απρόσωπο το σενάριο της επίθεσης τόσο λιγότερο πιθανό είναι να προσελκύσει το ενδιαφέρον. Η θεωρία της έλξης λοιπόν δείχνει να λειτούργει. Οι άνθρωποι τείνουν να είναι πιο δεκτικοί σε ελκυστικά πρόσωπα, περιβάλλοντα, εικόνες και γραφικά στοιχειά.
- Κάθε υπάλληλος είναι πιο επιρρεπής στο να παραπλανηθεί από ένα πιστό αντίγραφο μιας σελίδας και ενός μηνύματος που λαμβάνει συχνά. Συνεπώς και η αρχή της οικειότητας δείχνει αποτελεσματική. Για αυτό φυσικά και οι επιθέσεις Spear Phishing ως στοχευμένες αποδίδουν καλύτερα.
- Η θέση εργασίας δεν σχετίζεται με την Επαγρύπνηση και την παρατηρητικότητα. Στην μελέτη αυτή διαπιστώθηκε πως μέλη του τμήματος IT προχώρησαν στο να επισκευθούν την κακόβουλη σελίδα μας παρόλο που θεωρητικά θα έπρεπε να είναι πιο εξοικειωμένοι με τέτοια περιστατικά.
- Το αίσθημα του φόβου και η προξένησε άγχους αποδίδει. Στην περίπτωση μας οι παραλήπτες άνοιξαν το μήνυμα σχετικά με την ακυρωμένη συναλλαγή από φόβο και ανησυχία για τον λογαριασμό τραπέζης τους.

6. Συμπεράσματα

Η κοινωνική μηχανική είναι μια πολύ πραγματική απειλή και συγκεκριμένα οι επιθέσεις τέτοιου τύπου υπό την μορφή Phishing σήμερα αποτελούν πραγματικά μια από τις μεγαλύτερες απειλές στον τομέα της Ασφάλειας Πληροφοριών.

Αυτό ωστόσο δεν είναι κάτι που δεν μπορεί να ανατραπεί. Μόλις οι επιχειρήσεις αρχίσουν να παίρνουν στα σοβαρά την Κοινωνική Μηχανική και να εφαρμόζουν τις κατάλληλες τεχνικές για να προστατευτούν από αυτή την απειλή με μια πολυεπίπεδη άμυνα η οποία θα έχει ως βασικό όπλο τα ιδία τα τίμα που τις πλαισιώνουν, οι επιθέσεις αυτής της μορφής θα καταστούν ιδιαιτέρως δύσκολες για του επιτιθέμενους αλλά όχι αδύνατες. Αυτό φυσικά θα έχει αντίκτυπο στην επιλογή των στόχων διότι ένας οργανισμός με όλα τα κατάλληλα τεχνικά και οργανωτικά μετρά θα αποτελεί «πονοκέφαλο» για τους δράστες οι όποιο θα πρέπει να χρησιμοποιήσουν πολλαπλούς πόρους για να οργανώσουν και να ολοκληρώσουν με επιτυχία μια επίθεση.

Αυτό που πρέπει να αφομοιωθεί στις εταιρικές κουλτούρες και βέλτιστες πρακτικές είναι το ότι ο ανθρωπινός παράγοντα είναι, όπως έχει διατυπωθεί από πολλούς ειδικούς του χώρου, ο πιο αδύναμος κρίκος στην «αλυσίδα» της ασφάλειας. Δεν πρέπει να ξεχνάμε πως στο τέλος της ημέρας όλες οι επιθέσεις που στοχεύουν τα πληροφοριακά συστήματα έχουν σχεδιαστεί από ανθρώπους για να στοχεύσουν δημιουργήματα άλλων ανθρώπων. Για τον λόγο αυτό και η «μάχη» μεταξύ επιτιθέμενων και ατόμων που αναλαμβάνουν να αμυνθούν είναι συνεχώς εξελισσόμενη και μοιάζει πως θα συνεχίζεται για πάντα.

Είναι λοιπόν φανερό πως θα πρέπει οι επιχειρήσεις να επενδύσουν στην οχύρωση του ιδίου του προσωπικού ξεπερνώντας τα παραδοσιακά τεχνικά μέσα, μέσω της εκπαίδευσης και της προξένησης ευαισθητοποίησης για ζητήματα Ασφάλειας Πληροφοριών.

Βιβλιογραφία

1. Κοινωνική έρευνα και κρατική πολιτική .

https://ejournals.epublishing.ekt.gr/index.php/sas/article/viewFile/10321/10428.pdf.

2. Social Engineering - Political Science.

https://en.wikipedia.org/wiki/Social_engineering_(political_science).

3. What Is Social Engineering: The Tactics Used to Manipulate You.

https://heimdalsecurity.com/blog/what-is-social-engineering-tactics/.

4. Kevin Mitnick - The Art Of Deception.

https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf.

5. The Social Engineering Framework.

https://www.social-engineer.org/framework/attack-vectors/attack-cycle/.

6. Encyclopedia of Cyber Behavior.

https://books.google.gr/books?id=gLqYYFoVoR8C&lpg=PA935&ots=R2kYxgsIDu&dq=Rusch%2C%201999&hl=el&pg=PA930#v=onepage&q=Rusch,%201999&f=false.

7. Cyber Warfare and Cyber Terrorism.

https://books.google.gr/books?id=XWK9AQAAQBAJ&pg=PT224&lpg=PT224&dq=Gragg+(2003)&source=bl&ots=28YGC7xlmm&sig=ACfU3U2Qgli73BK67D3n76ITYS2iTw4tNQ&hl=el&sa=X&ved=2ahUKEwj49d7RneXoAhXhtYsKHS1eAMIQ6AEwC3oECAYQOg#v=onepage&q=Gragg%20(2003)&f=false.

8. The 6 Principles of Persuasion by Dr. Robert Cialdini.

https://www.influenceatwork.com/principles-of-persuasion/.

9. Understanding Scam Victims: Seven Principles for Systems Security.

https://www.cl.cam.ac.uk/~fms27/papers/2011-StajanoWil-scam.pdf.

10. Social Engineering - An Overview.

http://mytricksmania.blogspot.com/2013/06/social-engineering-overview.html.

11. Shoulder Surfing (computer security).

https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security).

12. The Social Engineering Framework - Dumpster Diving.

https://www.social-engineer.org/framework/information-gathering/dumpster-diving/.

13. Social Engineering - Security.

https://en.wikipedia.org/wiki/Social_engineering_(security).

14. What is a reverse social engineering attack?

https://www.social-engineer.org/wiki/archives/HowToGatherInfo/HowToGatherInfo-ReverseSE.html.

15. Phishing.

https://en.wikipedia.org/wiki/Phishing.

16. The 5 most common types of phishing attack.

https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack.

17. Phone Scams and Voice Phishing (Vishing).

https://safecomputing.umich.edu/be-aware/phone-scams.

18. The definitive guide to manipulative links.

http://www.spamflag.com/link-identification-guide/.

19. Anatomy of a Spam Email and New Techniques Being Used to Evade Detection.

https://www.slickrockweb.com/spam-and-new-evasion-techniques.php.

20. Money Mule.

https://en.wikipedia.org/wiki/Money_mule.

21. Phishing and money mules.

https://ieeexplore.ieee.org/abstract/document/5711465.

22. TOP FIVE PHISHING MYTHS DEBUNKED.

https://www.lookingglasscyber.com/blog/threat-reports/phishing/top-five-phishing-myths-debunked/.

23. Phishing Attack – Step By Step Demo Using Kali Linux Free Tool.

https://www.cybervie.com/blog/phishing-attack-using-kali-linux/.

24. Shellphish: A Phishing Tool.

https://www.hackingarticles.in/shellphish-a-phishing-tool/.

25. Hidden Eye: Modern Phishing Tool with Advanced Functionality.

https://www.cyberpunk.rs/hidden-eye-modern-phishing-tool.

26. Top 9 Phishing Simulators.

https://resources.infosecinstitute.com/top-9-free-phishing-simulators/#gref.

27. TrendMicro - Phishinsight.

https://phishinsight.trendmicro.com/en/.

28. A Multi-Level Defense Against Social Engineering.

https://www.sans.org/reading-room/whitepapers/engineering/paper/920.

29. beautycheck.

https://www.uni-regensburg.de/Fakultaeten/phil_Fak_II/Psychologie/Psy_II/beautycheck/english/sozialewahrnehmung/sozialewahrnehmung.htm.