ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ
UNIVERSITY OF THE
AEGEAN

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΠΙΣΚΟΠΗΣΗ ΜΕΘΟΔΩΝ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ελευθέριος Θεοδωρέλλης

Κυριάκος Κρητικός

Σάμος, Μάρτιος 2025

ΕΠΙΣΚΟΠΗΣΗ ΜΕΘΟΔΩΝ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ

Ελευθέριος Θεοδωρέλλης

Επιβλέπων Καθηγητής:

Κυριάκος Κρητικός

Μέλη εξεταστικής επιτροπής:

Κρητικός Κυριάκος, Καρύδα Μαρία, Κωνσταντίνου Ελισάβετ

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Πίνακας Συντομεύσεων

AI	Artificial Intelligence
AR	Augmented Reality
BEC	Business Email Compromise
CAN	Controller Area Network
CNNs	Convolutional Neural Networks
DDoS	Distributed Denial of Service
DLP	Data Leakage Protection
DNS	Domain Name System
DRP	Disaster Recovery Plan
ENISA	European Union Agency for Network and Information Security
IAM systems	Identity and Access Management systems
IDS	Intrusion Detection Systems
IMS	Incident Management Systems
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Protection Systems
ISACs	Information Sharing and Analysis Centers
IT	Information Technology
MAC	Media Access Control
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
ML	Machine Learning
NLP	Natural Language Processing
OSINT	Open-Source Intelligence
OTP	One Time Password
PGP	Pretty Good Privacy
SEPTA	Social Engineering Penetration Testing Approach
SERA	Social Engineering Risk Assessment
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SSID	Service Set Identifier

TTPs	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
USB	Universal Serial Bus
UYCS	Use Your Common Sense
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VR	Virtual Reality
XSS	Cross-Site Scripting

Πίνακας Λεξικού Όρων

Attorney Impersonation	Πλαστοπροσωπία Δικηγόρου
Artificial Intelligence	Τεχνητή Νοημοσύνη
Augmented Reality	Επαυξημένη Πραγματικότητα
Baiting	Δελεασμός
Bogus Invoice Scheme	Σχέδιο Πλαστού Τιμολογίου
Business Email Compromise	Παραβίαση Επιχειρηματικού Ηλεκτρονικού Ταχυδρομείου
CEO Fraud	Απάτη Διευθύνοντος Συμβούλου
Compliance audits	Έλεγχοι Συμμόρφωσης
Convolutional Neural Networks	Συνελικτικά Νευρωνικά Δίκτυα
Cross-Site Scripting	Προγραμματισμός Κατά Μήκος Ιστοτόπων
Cyberbullying	Διαδικτυακός Εκφοβισμός
Data Leakage Protection	Προστασία Δεδομένων από Διαρροές
Disaster Recovery Plan	Σχέδιο Αποκατάστασης Καταστροφών
Distributed Denial of Service	Κατανεμημένη Άρνηση Υπηρεσίας
Diversion Theft	Επίθεση Εκτροπής Κλοπής
Dumpster Diving	Αναζήτηση σε Κάδους Απορριμμάτων
Ensemble learning	Συνδυαστική Μάθηση
European Union Agency for Network and Information Security	Πρακτορείο της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών
Evil Twin	Κακόβουλο Δίδυμο
Four-eyes principle	Αρχή των Τεσσάρων Ματιών
Grooming	Προετοιμασία Θυμάτων
Hacking	Χακάρισμα
Hardware	Υλικό
Honey Trap	Παγίδα Μελιού
Identity and Access Management System	Σύστημα Διαχείρισης Ταυτότητας και Ελέγχου Πρόσβασης
Impersonation	Πλαστοπροσωπία
Incident Management System	Σύστημα Διαχείρισης Περιστατικών

Incident Response Team	Ομάδα Αντιμετώπισης Περιστατικών
Information Sharing and Analysis Centers	Κέντρα Διαμοιρασμού & Ανάλυσης Πληροφοριών Ασφαλείας
Information Technology	Τεχνολογία των Πληροφοριών
Intrusion Detection Systems	Σύστημα Ανίχνευσης Εισβολών
Intrusion Protection Systems	Σύστημα Προστασίας από Εισβολές
Invoice Modification Scheme	Σχέδιο Τροποποίησης Τιμολογίου
Internet of Things	Διαδίκτυο των Πραγμάτων
Link	Σύνδεσμος
Machine Learning	Μηχανική Μάθηση
Malicious website	Κακόβουλος Ιστότοπος
Malware	Κακόβουλο Λογισμικό
Multi-Factor Authentication	Πολυπαραγοντική Αυθεντικοποίηση
Natural Language Processing	Ανάλυση Φυσικής Γλώσσας
One Time Password	Κωδικός Μίας Χρήσης
Open door policy	Πολιτική Ανοιχτής Πόρτας
Open-Source Intelligence	Νοημοσύνη Ανοιχτών Πηγών
Password Cracking	Σπάσιμο Κωδικών Πρόσβασης
Penetration testing	Δοκιμές Διείσδυσης
Phishing	Ηλεκτρονικό Ψάρεμα
Pop-up windows	Αναδυόμενα Παράθυρα
Pretexting	Προσποίηση
Quantum computing	Κβαντική Υπολογιστική
Ransomware	Λυτρισμικό
Reverse Social Engineering	Αντίστροφη Κοινωνική Μηχανική
Sandboxing	Απομόνωση Εκτέλεσης
Scareware	Λογισμικό Εκφοβισμού
Service Set Identifier	Αναγνωριστικό Συνόλου Υπηρεσιών Δικτύου
Shoulder Surfing	Σερφάρισμα Πάνω από τον Ώμο
Smishing / SMS Phishing	Ηλεκτρονικό Ψάρεμα μέσω SMS
Social Engineering	Κοινωνική Μηχανική
Software	Λογισμικό

Spear Phishing	Στοχευμένο Ηλεκτρονικό Ψάρεμα
SQL Injection	Έκχυση Κακόβουλου Κώδικα SQL
Supplier Swindle	Εξαπάτηση Προμηθευτή
Pharming	Παραπλάνηση Μέσω Ανακατεύθυνσης
Quid Pro Quo	Αντίκρισμα
Tactics, Techniques, and Procedures	Τακτικές, Τεχνικές και Διαδικασίες
Tailgating ή Piggybacking	Παραβίαση Ασφαλείας με Ακολούθηση
Threat Detection System	Σύστημα Ανίχνευσης Απειλών
Two-person rule	Κανόνας των "Δύο Ατόμων"
Typosquatting	Τυποκαταλήστευση
URL Hijacking	Πειρατεία Συνδέσμων URL
Universal Serial Bus	Σειριακός Δίαυλος Γενικής Χρήσης
Virtual Reality	Εικονική Πραγματικότητα
Vishing / Voice Phishing	Φωνητική Απάτη ή Φωνητικό Ψάρεμα
Watering Hole Attack	Επίθεση σε Σημείο Συγκέντρωσης
Whaling	Φαλαινοθηρία

Περίληψη

Η παρούσα εργασία παρουσιάζει μια εκτενή επισκόπηση των μεθόδων προστασίας από επιθέσεις κοινωνικής μηχανικής, εστιάζοντας στις τεχνολογικές, εκπαιδευτικές και οργανωτικές στρατηγικές που μπορούν να υιοθετηθούν για την πρόληψη και την αντιμετώπισή των επιθέσεων αυτών. Στο πλαίσιο της έρευνας, προτείνεται μια νέα κατηγοριοποίηση των επιθέσεων κοινωνικής μηχανικής, η οποία συνδυάζει τα αποτελέσματα προηγούμενων ερευνών και εισάγει νέες διαστάσεις για την κατηγοριοποίηση των επιθέσεων, προσφέροντας μια πιο ολοκληρωμένη ανάλυση. Επιπλέον, μέσω μιας συστηματικής ανασκόπησης της σύγχρονης βιβλιογραφίας, αναλύονται διεξοδικά τα κυρίαρχα μοντέλα προστασίας και τα εργαλεία που χρησιμοποιούνται για την αποτροπή των επιθέσεων. Ιδιαίτερη έμφαση δίνεται στον ανθρώπινο παράγοντα και στην εκπαίδευση των χρηστών, καθώς και στη συμβολή της τεχνητής νοημοσύνης στην ανίχνευση και στην αντιμετώπιση των επιθέσεων. Η εργασία εξετάζει επίσης τις αναδυόμενες απειλές, και τις μελλοντικές τάσεις στον τομέα της κοινωνικής μηχανικής, προσφέροντας μια ολοκληρωμένη εικόνα των προκλήσεων που αντιμετωπίζουν οι οργανισμοί και τα άτομα. Τα ευρήματα της έρευνας υποδεικνύουν ότι ο συνδυασμός των τεχνολογικών μέτρων, της τακτικής εκπαίδευσης, της τήρησης των θεσπισμένων οργανωτικών διαδικασιών και της καλλιέργειας μιας κουλτούρας ασφάλειας αποτελεί την πιο αποτελεσματική προσέγγιση για την προστασία έναντι των απειλών της κοινωνικής μηχανικής. Η εργασία καταλήγει με προτάσεις για τη βελτίωση των υφιστάμενων μεθόδων προστασίας και προτείνει κατευθύνσεις για μελλοντική έρευνα στον τομέα.

Λέξεις-κλειδιά: Κοινωνική Μηχανική, Επιθέσεις Κυβερνοασφάλειας, Μέθοδοι Προστασίας, Εκπαίδευση Χρηστών, Τεχνητή Νοημοσύνη, Ασφάλεια Πληροφοριών, Διαχείριση Κινδύνων, Κυβερνοεπίγνωση

Abstract

This thesis presents a comprehensive overview of protection methods against social engineering attacks, focusing on technological, educational, and organizational strategies that can be adopted for their prevention and mitigation. A new categorization of social engineering attacks is proposed in this research, combining the findings from previous studies and introducing new dimensions for classifying attacks, offering a more comprehensive analysis. Further, through a systematic review of contemporary literature, the dominant protection models and tools used to prevent attacks are thoroughly analysed. Special emphasis is placed on the human factor and the user education, as well as the contribution of artificial intelligence in detecting and countering attacks. The study also examines emerging threats, and future trends in the field of social engineering, offering a complete picture of the challenges faced by organizations and individuals. The research findings indicate that the combination of technological measures, regular training, adherence to established organizational procedures, and the cultivation of a security culture constitutes the most effective approach to protection against social engineering threats. The thesis concludes with suggestions for improving existing protection methods and proposes directions for future research in the field.

Keywords: Social Engineering, Cybersecurity Attacks, Protection Methods, User Education, Artificial Intelligence, Information Security, Risk Management, Cyber Awareness

1. ΕΙΣΑΓΩΓΗ

1.1. Σύντομη Επισκόπηση της Κοινωνικής Μηχανικής

Η κοινωνική μηχανική (social engineering) αποτελεί μια πολύπλευρη έννοια που εκτείνεται σε διάφορους τομείς, από την ασφάλεια πληροφοριών μέχρι τις κοινωνικές επιστήμες. Στο πλαίσιο της ασφάλειας των πληροφοριών, ο Hadnagy (2010) αποδίδει τον παρακάτω σύντομο ορισμό:

«Η κοινωνική μηχανική είναι η τέχνη ή η επιστήμη της επιδέξιας χειραγώγησης ανθρώπων ώστε να προβούν σε ενέργειες που μπορεί να είναι ή να μην είναι προς το συμφέρον τους».

Αυτός ο ορισμός υπογραμμίζει τη βασική πτυχή της κοινωνικής μηχανικής, που είναι η εκμετάλλευση της ανθρώπινης ψυχολογίας για την επίτευξη συγκεκριμένων στόχων. Στο πεδίο της κυβερνοασφάλειας, η κοινωνική μηχανική συχνά χρησιμοποιείται για κακόβουλους σκοπούς, όπως η απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα ή η εξαγωγή ευαίσθητων πληροφοριών.

1.2. Υπόβαθρο και Σημασία του Θέματος

Η έννοια της κοινωνικής μηχανικής έχει τις ρίζες της βαθιά στην ανθρώπινη ιστορία. Ιστορικά παραδείγματα που υποδηλώνουν τη χρήση τεχνικών παρόμοιων με την προαναφερθείσα έννοια περιλαμβάνουν (Hasan et al., 2010; Samonas, 2016; Yasin et al., 2020):

- Την ιστορία του Δούρειου Ίππου κατά τον Τρωικό Πόλεμο, όπου οι Έλληνες χρησιμοποίησαν εξαπάτηση για να εισέλθουν στην Τροία.
- Τις στρατηγικές του Κινέζου στρατηγού Σουν Τζου, ο οποίος στο έργο του «Η Τέχνη του Πολέμου» τόνισε τη σημασία της εξαπάτησης και της χειραγώγησης των αντιλήψεων του εχθρού.

Στο πλαίσιο της σύγχρονης ασφάλειας των πληροφοριών, ο Kevin Mitnick έπαιξε καθοριστικό ρόλο στην ανάδειξη της σημασίας της κοινωνικής μηχανικής. Ο Mitnick απέδειξε ότι, παρά την εξέλιξη των τεχνολογικών μέτρων ασφαλείας, ο ανθρώπινος παράγοντας παραμένει ο πιο αδύναμος κρίκος στην αλυσίδα της ασφάλειας (Mitnick & Simon, 2002).

Η κατανόηση και η αντιμετώπιση της κοινωνικής μηχανικής απαιτεί μια διεπιστημονική προσέγγιση, συνδυάζοντας γνώσεις από την ψυχολογία, την κοινωνιολογία, την ασφάλεια πληροφοριών και άλλους σχετικούς τομείς. Η εκπαίδευση και η ευαισθητοποίηση των χρηστών, σε συνδυασμό με την εφαρμογή ισχυρών πολιτικών ασφαλείας, αποτελούν βασικά στοιχεία για την προστασία από επιθέσεις κοινωνικής μηχανικής.

1.3. Σκοπός και Στόχοι της Εργασίας

Η εργασία αυτή εστιάζει στη συστηματική μελέτη και ανάλυση των επιθέσεων κοινωνικής μηχανικής και των μεθόδων προστασίας από αυτές. Ως κεντρική συνεισφορά, προτείνεται μια νέα κατηγοριοποίηση των επιθέσεων κοινωνικής μηχανικής, η οποία συνδυάζει τα αποτελέσματα προηγούμενων ερευνών και προτείνει μια πιο ευέλικτη και επεκτάσιμη προσέγγιση για την καλύτερη κατηγοριοποίηση και κατανόηση των επιθέσεων στον σύγχρονο ψηφιακό κόσμο. Αυτή η νέα κατηγοριοποίηση αποσκοπεί στην αποτελεσματικότερη πρόληψη και αντιμετώπιση των επιθέσεων.

Ο κύριος σκοπός της παρούσας επισκόπησης είναι να διερευνήσει τις μεθόδους και τα εργαλεία προστασίας από επιθέσεις κοινωνικής μηχανικής, παρέχοντας μια ολοκληρωμένη εικόνα των διαθέσιμων τεχνικών και της αποτελεσματικότητάς τους. Η εργασία επικεντρώνεται τόσο στις τεχνολογικές όσο και στις ανθρώπινες παραμέτρους που επηρεάζουν την τρωτότητα των χρηστών, αναδεικνύοντας τις πιο αποδοτικές μεθόδους πρόληψης και αντιμετώπισης. Επιπλέον, προτείνονται βελτιώσεις στις υφιστάμενες πρακτικές και μέτρα ασφαλείας.

Οι επιμέρους στόχοι της εργασίας περιλαμβάνουν την απάντηση στα κύρια ερευνητικά ερωτήματα της μεθοδολογίας ανασκόπησης (Κεφάλαιο 2), όπως η αξιολόγηση των κυρίαρχων τεχνικών και διοικητικών προσεγγίσεων, ο ρόλος της εκπαίδευσης χρηστών στην πρόληψη, η συνεισφορά της τεχνητής νοημοσύνης (AI) και η διερεύνηση των κοινωνικών και ψυχολογικών παραμέτρων που επηρεάζουν τις αδυναμίες των χρηστών. Η ανάλυση αυτή στοχεύει στην κατανόηση των σύγχρονων προκλήσεων και στην ανάδειξη βέλτιστων πρακτικών για την προστασία από επιθέσεις κοινωνικής μηχανικής.

1.4. Περιορισμοί και Οριοθέτηση της Έρευνας

Ένας από τους περιορισμούς αυτής της μελέτης είναι ότι δεν περιλαμβάνονται εμπειρικές μελέτες ή πειραματικά δεδομένα, περιορίζοντας την ικανότητα αξιολόγησης της εφαρμογής των πρακτικών εργαλείων ή τεχνικών σε πραγματικά περιβάλλοντα. Επιπλέον, η ανασκόπηση εστιάζει κυρίως σε διαθέσιμα εργαλεία και τεχνικές που χρησιμοποιούνται ευρέως, χωρίς να καλύπτει σε βάθος τα ιδιόκτητα ή κλειστά συστήματα που ενδέχεται να χρησιμοποιούνται από συγκεκριμένες επιχειρήσεις.

Η οριοθέτηση του πεδίου έρευνας εστιάζει αποκλειστικά στις επιθέσεις κοινωνικής μηχανικής και τις τεχνικές προστασίας που σχετίζονται με αυτές. Άλλες μορφές κυβερνοεπιθέσεων, όπως οι επιθέσεις τύπου κατανεμημένης άρνησης υπηρεσίας (DDoS:

Distributed Denial of Service) ή οι παραβιάσεις φυσικής ασφάλειας, δεν καλύπτονται. Επίσης, η μελέτη εστιάζει στην ασφάλεια πληροφοριών κυρίως για επιχειρηματικούς και τεχνολογικούς οργανισμούς, καθώς αυτοί αποτελούν τους συχνότερους στόχους επιθέσεων κοινωνικής μηχανικής και διαθέτουν την πιο εκτενή τεκμηρίωση περιστατικών και αντιμέτρων. Τα θέματα που αφορούν την ασφάλεια σε προσωπικό ή κρατικό επίπεδο αν και εξίσου σημαντικά, απαιτούν διαφορετική προσέγγιση και μεθοδολογία ανάλυσης, και ως εκ τούτου δεν περιλαμβάνονται στο πεδίο της παρούσας μελέτης.

1.5. Συνεισφορά της Εργασίας

Η συνεισφορά της εργασίας αναμένεται να είναι σημαντική στο πεδίο της ασφάλειας πληροφοριών και συστημάτων, καθώς παρέχει μια συνολική επισκόπηση των πιο σύγχρονων μεθόδων προστασίας από επιθέσεις κοινωνικής μηχανικής. Μέσω της ανάλυσης των υπαρχόντων τεχνικών, εκπαιδευτικών προσεγγίσεων και της τεχνητής νοημοσύνης, η εργασία αυτή μπορεί να αποτελέσει σημείο αναφοράς για μελλοντικές έρευνες και εξελίξεις στον τομέα. Επιπλέον, αναδεικνύει τη σημασία του ανθρώπινου παράγοντα και τις αδυναμίες που αυτός επιδεικνύει, συμβάλλοντας στην κατανόηση των τρόπων βελτίωσης των συστημάτων ασφαλείας.

Σε πρακτικό επίπεδο, τα ευρήματα αυτής της μελέτης μπορούν να βοηθήσουν οργανισμούς και άτομα να βελτιώσουν τις στρατηγικές πρόληψης και αντιμετώπισης των επιθέσεων της κοινωνικής μηχανικής. Οι οργανισμοί μπορούν να αξιοποιήσουν τις προτάσεις για την ενίσχυση της ασφάλειας των πληροφοριών τους, ενώ οι χρήστες θα είναι πιο ευαισθητοποιημένοι σχετικά με τις μορφές των επιθέσεων και τα μέτρα προστασίας που πρέπει να λαμβάνουν. Η μελέτη μπορεί επίσης να καθοδηγήσει εκπαιδευτικά προγράμματα για την ενίσχυση της αντίστασης των χρηστών σε επιθέσεις κοινωνικής μηχανικής.

1.6. Δομή της Εργασίας

Η εργασία αυτή είναι οργανωμένη σε έξι κύρια κεφάλαια. Στο δεύτερο κεφάλαιο περιγράφεται η μεθοδολογία που ακολουθήθηκε για την ανασκόπηση της βιβλιογραφίας, συμπεριλαμβανομένων των ερευνητικών ερωτημάτων, των στρατηγικών αναζήτησης, των κριτηρίων επιλογής, της διαδικασίας εξαγωγής και ανάλυσης δεδομένων, καθώς και των περιορισμών της μεθοδολογίας.

Το τρίτο κεφάλαιο εστιάζει στην κοινωνική μηχανική και τις μεθόδους της, παρέχοντας τον πλήρη ορισμό της, τις βασικές έννοιες και τους παράγοντες επιτυχίας των επιθέσεων. Ακολουθεί λεπτομερής κατηγοριοποίηση και ανάλυση των επιθέσεων σε τέσσερις βασικές

κατηγορίες: επιθέσεις μέσω ψηφιακής επικοινωνίας, επιθέσεις βασισμένες σε φυσική αλληλεπίδραση, επιθέσεις βασισμένες σε ψυχολογική χειραγώγηση και επιθέσεις βασισμένες σε τεχνικές παραπλάνησης.

Το τέταρτο κεφάλαιο επικεντρώνεται στην εμπεριστατωμένη ανάλυση των μεθόδων προστασίας από επιθέσεις κοινωνικής μηχανικής, καλύπτοντας τεχνικά μέτρα προστασίας, εκπαίδευση και ευαισθητοποίηση χρηστών, οργανωτικές πολιτικές και διαδικασίες, εταιρική κουλτούρα ασφάλειας, αξιολόγηση και διαχείριση κινδύνων, δοκιμές ασφαλείας και αντιμετώπιση περιστατικών.

Τέλος, το έκτο κεφάλαιο συνοψίζει τα ευρήματα της μελέτης, παρουσιάζει προτάσεις για τη βελτίωση της προστασίας και προτείνει κατευθύνσεις για μελλοντική έρευνα.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΑΝΑΣΚΟΠΗΣΗΣ

Η παρούσα εργασία επιχειρεί μια συστηματική βιβλιογραφική ανασκόπηση του φαινομένου της κοινωνικής μηχανικής στον κυβερνοχώρο, με έμφαση στις σύγχρονες προσεγγίσεις αντιμετώπισης και πρόληψης των επιθέσεων κοινωνικής μηχανικής. Η μεθοδολογία που ακολουθήθηκε βασίζεται στις αρχές της συστηματικής ανασκόπησης (Kitchenham & Charters, 2007), προσαρμοσμένη στις ιδιαιτερότητες του πεδίου της κυβερνοασφάλειας.

2.1. Ερευνητικά Ερωτήματα

Η παρούσα εργασία διερευνά τις επιθέσεις κοινωνικής μηχανικής, εστιάζοντας στις μεθόδους και τεχνικές που χρησιμοποιούν οι επιτιθέμενοι, στα σύγχρονα εργαλεία προστασίας (από επιθέσεις κοινωνικής μηχανικής) και στην εκπαίδευση των χρηστών (για την αντιμετώπισή τους). Τα παρακάτω ερευνητικά ερωτήματα καθοδήγησαν την ανασκόπηση και την ανάλυση, παρέχοντας ένα πλαίσιο για την κατανόηση της απειλής (της κοινωνικής μηχανικής) και των διαθέσιμων στρατηγικών πρόληψης και αντιμετώπισης:

- ***Ποιες είναι οι πιο γνωστές και ευρέως καταγεγραμμένες επιθέσεις κοινωνικής μηχανικής;*** Στόχος είναι η καταγραφή των σημαντικότερων περιστατικών κοινωνικής μηχανικής, συμπεριλαμβανομένων των τεχνικών και στρατηγικών που χρησιμοποιούν οι επιτιθέμενοι, ώστε η εργασία να λειτουργήσει ως οδηγός κατανόησης των τακτικών και των αδυναμιών που γίνονται εκμεταλλεύσιμες. Η ανάλυση στοχεύει στην εξαγωγή χρήσιμων συμπερασμάτων για τη βελτίωση των τρεχόντων πρακτικών ασφαλείας και την πρόληψη μελλοντικών επιθέσεων. (Βλ. Κεφάλαιο 3).
- ***Πώς επηρεάζουν τα κοινωνικά και ψυχολογικά χαρακτηριστικά των χρηστών την τρωτότητά τους σε επιθέσεις κοινωνικής μηχανικής;*** Η ανάλυση αυτή μελετά κοινωνικούς και ψυχολογικούς παράγοντες που καθιστούν ορισμένους χρήστες περισσότερο ευάλωτους, εντοπίζοντας χαρακτηριστικά και συμπεριφορές που αυξάνουν τον κίνδυνο στοχοποίησης. Η γνώση αυτή υποστηρίζει τον σχεδιασμό πιο αποτελεσματικών πολιτικών προστασίας. (Βλ. Ενότητα 4.5).
- ***Ποια είναι τα σύγχρονα εργαλεία πρόληψης, ανίχνευσης και αντιμετώπισης επιθέσεων κοινωνικής μηχανικής;*** Η ερώτηση αυτή εξετάζει το πλήρες φάσμα των τεχνολογικών και διοικητικών λύσεων που εφαρμόζονται σε όλα τα στάδια μιας επίθεσης, περιλαμβάνοντας προσεγγίσεις για την πρόληψη, ανίχνευση και αντιμετώπιση επιθέσεων. Αναλύονται οι τεχνικές και μέθοδοι που διασφαλίζουν τις

οργανωτικές και ατομικές δομές από επιθέσεις κοινωνικής μηχανικής. (Βλ. Κεφάλαιο 5).

- ***Πώς συμβάλλει η εκπαίδευση των χρηστών στην αντιμετώπιση επιθέσεων κοινωνικής μηχανικής και πώς μπορεί να βελτιστοποιηθεί;*** Η ερώτηση διερευνά τη σημασία του ανθρώπινου παράγοντα, επικεντρώνοντας στην εκπαίδευση και ευαισθητοποίηση των χρηστών σχετικά με τις τακτικές κοινωνικής μηχανικής. Αναλύονται βέλτιστες πρακτικές εκπαίδευσης που βοηθούν τους χρήστες να αναγνωρίζουν και να αντιστέκονται σε επιθέσεις. (Βλ. Ενότητα 5.2).
- ***Ποιες είναι οι κύριες προκλήσεις και οι κατευθύνσεις για μελλοντική έρευνα στην αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής;*** Η ερώτηση αυτή επικεντρώνεται στις υπάρχουσες προκλήσεις και τις μελλοντικές ερευνητικές ανάγκες για την αποτελεσματική αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής. Η διερεύνηση νέων κατευθύνσεων αποσκοπεί στην ανάπτυξη βελτιωμένων στρατηγικών ασφαλείας και στην ενίσχυση της προστασίας απέναντι σε αυτές τις απειλές. (Βλ. Ενότητα 5.3).

2.2. Στρατηγική Αναζήτησης

2.2.1 Πηγές δεδομένων

Η αναζήτηση πραγματοποιήθηκε κυρίως μέσω διαφόρων ευρέων γνωστών και χρησιμοποιούμενων βάσεων δεδομένων (ερευνητικών δημοσιεύσεων): IEEE Xplore, ACM Digital Library, ScienceDirect, Tech Science Press, MDPI, ResearchGate, ACADEMIA, οι οποίες περιλαμβάνουν και εξειδικευμένες δημοσιεύσεις στον τομέα της πληροφορικής και της κυβερνοασφάλειας. Επιπροσθέτως, χρησιμοποιήθηκε η μηχανή αναζήτησης Google Scholar, λόγω της ευρείας κάλυψης ακαδημαϊκών δημοσιεύσεων που αυτή υποστηρίζει και της δυνατότητας που προσφέρει για εύκολη πρόσβαση σε πλήρη κείμενα (των δημοσιεύσεων).

2.2.2 Όροι Αναζήτησης

Οι όροι αναζήτησης περιελάμβαναν συνδυασμούς των ακόλουθων λέξεων-κλειδιών:

("social engineering" AND (Phishing OR "Business Email Compromise" OR "CEO Fraud" OR "Dumpster Diving" OR Impersonation OR Baiting OR "Evil Twin" OR Grooming OR Hacking OR "Honey Trap" OR "Malicious website" OR Malware OR "Pop-up windows" OR Pretexting OR Scareware OR "Shoulder Surfing" OR "Smishing" OR "SMS Phishing" OR "Spear Phishing" OR Pharming OR "Quid Pro Quo" OR "Tailgating" OR "Piggybacking" OR

"Typosquatting" OR "URL Hijacking" OR "Vishing" OR "Voice Phishing" OR "Watering Hole Attack" OR Whaling)) AND (cybersecurity OR "cyber security" OR prevention OR detection OR "user awareness" OR "vulnerability factors" OR "research directions" OR "future challenges" OR "emerging issues").

2.3. Κριτήρια Επιλογής

Για τη διασφάλιση της εγκυρότητας, αξιοπιστίας και της ποιότητας της παρούσας ανασκόπησης, εφαρμόστηκαν συγκεκριμένα κριτήρια επιλογής για το φιλτράρισμα των άρθρων μετά την αναζήτηση και συλλογή τους. Τα κριτήρια αυτά σχεδιάστηκαν για να διασφαλίσουν ότι τα άρθρα που χρησιμοποιούνται στην εργασία σχετίζονται άμεσα με το θέμα της κοινωνικής μηχανικής στον κυβερνοχώρο, ενώ πληρούν υψηλά πρότυπα επιστημονικής ποιότητας. Τα κριτήρια επιμερίζονται σε τρεις κατηγορίες: κριτήρια αποδοχής, κριτήρια αποκλεισμού και κριτήρια ποιότητας, τα οποία συνδυαστικά διασφαλίζουν την αξιοπιστία των ευρημάτων και την πληρότητα της ανάλυσης.

2.3.1 Κριτήρια Αποδοχής

- Άρθρα δημοσιευμένα σε επιστημονικά περιοδικά ή πρακτικά συνεδρίων με σύστημα αξιολόγησης από ομότιμους κριτές καθώς και άλλες αξιόπιστες πηγές που πληρούν αυστηρά επιστημονικά πρότυπα (βιβλία, διατριβές, τεχνικές αναφορές από τον ακαδημαϊκό και ερευνητικό χώρο, κ.λπ.).
- Άμεση σχέση με το θέμα της κοινωνικής μηχανικής στον κυβερνοχώρο.

2.3.2 Κριτήρια Αποκλεισμού

- Άρθρα σε γλώσσα εκτός της αγγλικής και της ελληνικής.
- Δημοσιεύσεις πριν το 2010, με εξαίρεση το βιβλίο "The Art of Deception: Controlling the Human Element of Security" των Mitnick & Simon (2002), το οποίο αποτελεί θεμελιώδες έργο αναφοράς στον τομέα της κοινωνικής μηχανικής.
- Μη επιστημονικές πηγές (π.χ. ιστολόγια, εμπορικές ιστοσελίδες, άρθρα εφημερίδων).
- Διπλότυπες δημοσιεύσεις ή με επικαλυπτόμενο περιεχόμενο (αναφορά σε δημοσιεύσεις από τους ίδιους συγγραφείς που περιλαμβάνουν παρόμοιο περιεχόμενο).

2.3.3 Κριτήρια Ποιότητας

- Σαφήνεια και πληρότητα της μεθοδολογίας.
- Εγκυρότητα και αξιοπιστία των ευρημάτων.
- Σημαντικότητα της συνεισφοράς στο πεδίο.

- Πληρότητα της παρουσίασης των αποτελεσμάτων.
- Παρουσίαση πρωτότυπης έρευνας.
- Βαθμός κατανόησης του κειμένου[1].

2.4. Διαδικασία Επιλογής

Η διαδικασία επιλογής των άρθρων πραγματοποιήθηκε σε τρία στάδια:

- **Αρχική αναζήτηση**: Εφαρμόστηκαν οι όροι αναζήτησης στις προαναφερόμενες επιλεγμένες βάσεις δεδομένων, καταλήγοντας σε ένα αρχικό σύνολο **176** άρθρων.
- **Προκαταρκτική επιλογή**: Από τα **176** άρθρα, **112** πέρασαν στην επόμενη φάση μετά την εφαρμογή των κριτηρίων αποδοχής και αποκλεισμού.
- **Τελική επιλογή**: Από τα **112** άρθρα, **73** άρθρα πληρούσαν τα κριτήρια ποιότητας, έπειτα από ενδελεχή μελέτη τους, και επιλέχθηκαν για την ανάλυση.

2.5. Εξαγωγή Δεδομένων

Για κάθε επιλεγμένο άρθρο, εξήχθησαν τα ακόλουθα δεδομένα:

- Βιβλιογραφικές πληροφορίες (συγγραφείς, έτος, τίτλος, πηγή δημοσίευσης) καθώς και ο τρόπος αξιολόγησης της κάθε συνεισφοράς (θεωρητική σύγκριση με άλλες εργασίες, πειραματική αξιολόγηση κ.λπ.).
- Τύπος μελέτης (π.χ. εμπειρική έρευνα, θεωρητική ανάλυση, ανασκόπηση).
- Κύρια ευρήματα και συμπεράσματα.
- Μεθοδολογία και εργαλεία που χρησιμοποιήθηκαν (π.χ. αναλύσεις δεδομένων, εργαλεία λογισμικού).
- Περιορισμοί της έρευνας.
- Προτάσεις για μελλοντική έρευνα.

2.6. Ανάλυση και Σύνθεση Δεδομένων

Η ανάλυση των δεδομένων πραγματοποιήθηκε με τη μέθοδο της θεματικής ανάλυσης (Braun & Clarke, 2006). Τα βήματα που ακολουθήθηκαν είναι:

1. **Εξοικείωση με τα δεδομένα**: Σε αυτό το στάδιο, μελετήθηκαν τα δεδομένα για να κατανοηθεί το περιεχόμενο και η δομή τους.

[1] Το κείμενο πρέπει να είναι γραμμένο σε κατανοητή γλώσσα, χωρίς σημαντικά συντακτικά και εκφραστικά λάθη. Κείμενα που είναι κακώς διατυπωμένα δυσχεραίνουν την κατανόηση του περιεχομένου και μειώνουν τη συνεισφορά τους στο πεδίο.

2. **Αρχική κωδικοποίηση**: Τα δεδομένα διασπάστηκαν σε μικρότερα κομμάτια και κωδικοποιήθηκαν για να αναγνωριστούν βασικές έννοιες και ιδέες.
3. **Αναζήτηση θεμάτων**: Σε αυτή τη φάση, αναζητήθηκαν σημαντικά θέματα που αναδεικνύουν βασικά μοτίβα και απαντήσεις στις ερευνητικές ερωτήσεις. Αυτά τα θέματα συνοψίζουν τα κύρια σημεία και τις τάσεις που προκύπτουν από τα δεδομένα.
4. **Επανεξέταση θεμάτων**: Τα προτεινόμενα θέματα αξιολογούνται και, αν χρειαστεί, αναθεωρούνται για να διασφαλιστεί η συνοχή τους.
5. **Ορισμός και ονομασία θεμάτων**: Τα θέματα ορίζονται με σαφήνεια και ονομάζονται ώστε να αντικατοπτρίζουν τη σημασία τους για την έρευνα.
6. **Παραγωγή της τελικής αναφοράς**: Συντάσσεται η τελική αναφορά που ενσωματώνει τα ευρήματα και τις αναλύσεις

Η σύνθεση των δεδομένων έγινε με τη μέθοδο της αφηγηματικής σύνθεσης, αναδεικνύοντας τις διαφορές και τις ομοιότητες που προκύπτουν από τις διάφορες μελέτες στον τομέα της κοινωνικής μηχανικής.

2.7. Κατανομή Επιλεγμένων Άρθρων

α) Κατανομή ανά Έτος Δημοσίευσης

Η κατανομή των 74 επιλεγμένων άρθρων ανά έτος δημοσίευσης είναι η εξής:

2024:15 άρθρα
2023:14 άρθρα
2022:10 άρθρα
2021:6 άρθρα
2020:5 άρθρα
2019:3 άρθρα
2018:3 άρθρα
2017:5 άρθρα
2016:2 άρθρα
2015:1 άρθρο
2014:6 άρθρα
2011:2 άρθρα
2010:1 άρθρο
2002:1 άρθρο

Και η απεικόνισή τους με μορφή ραβδογράμματος:

Σχήμα 1: Κατανομή του αριθμού των άρθρων που δημοσιεύθηκαν κάθε έτος

Αυτή η κατανομή αντικατοπτρίζει την αυξανόμενη προσοχή που δίνεται στο θέμα τα τελευταία χρόνια, με ιδιαίτερη έμφαση κατά την περίοδο της πανδημίας COVID-19.

β) Κατανομή ανά Είδος Άρθρου

Παρακάτω παρατίθεται η κατανομή των επιλεγμένων άρθρων ανά είδος:

Περιοδικά (Journals): 46%

Συνέδρια (Conference Proceedings): 17%

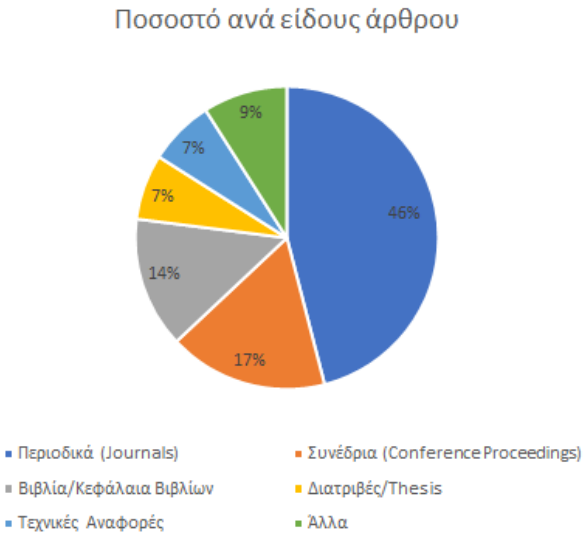
Βιβλία/Κεφάλαια Βιβλίων: 14%

Διατριβές/Thesis: 7%

Τεχνικές Αναφορές: 7%

Άλλα: 9%

Και η απεικόνισή τους με μορφή πίτας:



Σχήμα 2: Κατανομή του ποσοστού των άρθρων ανά είδος

γ) Κατανομή ανά Εκδότη

Στην παρακάτω λίστα παρατίθεται (με στρογγυλοποίηση) η κατανομή των επιλεγμένων άρθρων ανά εκδότη:

IEEE: 31%

Elsevier: 17%

Springer: 5%

Wiley: 8%

ACM: 4%

MDPI: 7%

USENIX: 2%

Taylor & Francis: 3%

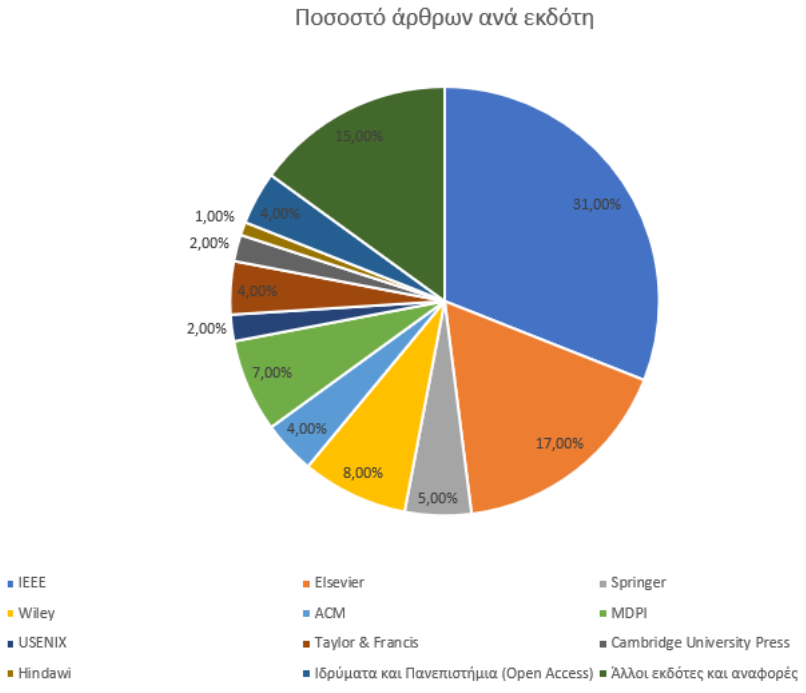
Cambridge University Press: 2%

Hindawi: 1%

Ιδρύματα και Πανεπιστήμια (Open Access): 4%

Άλλοι εκδότες και αναφορές: 15%

Και η απεικόνισή της με μορφή πίτας:



Σχήμα 3: Κατανομή του ποσοστού των άρθρων ανά εκδότη

2.8. Περιορισμοί της Μεθοδολογίας

Παρά την προσπάθεια για μια συστηματική και αμερόληπτη προσέγγιση, η παρούσα μεθοδολογία υπόκειται σε ορισμένους περιορισμούς:

- Η χρήση μόνο αγγλόφωνων δημοσιεύσεων ενδέχεται να έχει αποκλείσει σημαντικές έρευνες σε άλλες γλώσσες.
- Η εστίαση σε δημοσιεύσεις μετά το 2016 μπορεί να έχει παραβλέψει σημαντικές παλαιότερες μελέτες.
- Την ενδεχόμενη υποκειμενικότητα στην εφαρμογή των κριτηρίων ποιότητας, παρά την σημαντική προσπάθεια για αντικειμενικότητα.
- Η ραγδαία εξέλιξη του πεδίου της κυβερνοασφάλειας σημαίνει ότι ορισμένα ευρήματα μπορεί να έχουν ξεπεραστεί κατά τη διάρκεια της ανασκόπησης.

3. ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ: ΜΕΘΟΔΟΙ ΚΑΙ ΤΕΧΝΙΚΕΣ

3.1. Ορισμός και Βασικές Έννοιες της Κοινωνικής Μηχανικής

3.1.1 Εκτενής Ορισμός, Τακτικές και Στόχοι των Επιτιθέμενων

Η κοινωνική μηχανική αποτελεί μια πολύπλευρη προσέγγιση που συνδυάζει ψυχολογικές τεχνικές και τεχνολογικές μεθόδους με στόχο την χειραγώγηση ατόμων ή ομάδων. Ο Kevin Mitnick, πρωτοπόρος στον τομέα της κοινωνικής μηχανικής, την όρισε ως «μια μορφή ψυχολογικής χειραγώγησης και εξαπάτησης, όπου οι επιτιθέμενοι εκμεταλλεύονται την ανθρώπινη συμπεριφορά για να ανακτήσουν ευαίσθητες πληροφορίες, να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή εγκαταστάσεις, ή να χειραγωγήσουν άτομα ώστε να εκτελέσουν ενέργειες που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια ή να παραβιάσουν τις οργανωτικές πολιτικές» (Mitnick & Simon, 2002).

Σε αντίθεση με τις παραδοσιακές τεχνικές χακαρίσματος (hacking) που επικεντρώνονται στην εκμετάλλευση των τεχνικών ευπαθειών, οι επιθέσεις κοινωνικής μηχανικής στοχεύουν στον ανθρώπινο παράγοντα μέσω παραπλανητικών τακτικών. Οι πιο συνηθισμένες μέθοδοι περιλαμβάνουν την προσποίηση (pretexting), την πλαστοπροσωπία (impersonation), το ηλεκτρονικό ψάρεμα (phishing) και το δόλωμα (baiting), με σκοπό την εκμετάλλευση των ανθρώπινων αδυναμιών και την επίτευξη εμπιστοσύνης.

Η προσποίηση είναι μια εξελιγμένη τεχνική όπου ο επιτιθέμενος δημιουργεί ένα προσεκτικά κατασκευασμένο σενάριο για να αποσπάσει πληροφορίες από το θύμα. Σύμφωνα με την έκθεση Data Breach Investigations Report της Verizon για το 2023, οι περισσότερες από τις παραβιάσεων δεδομένων εμπεριείχε τον ανθρώπινο παράγοντα, με το pretexting να αποτελεί μία από τις κύριες μεθόδους εκμετάλλευσης. Οι επιτιθέμενοι συχνά χρησιμοποιούν λεπτομερή έρευνα για το θύμα και τον οργανισμό του, δημιουργώντας αληθοφανή σενάρια που βασίζονται σε πραγματικές επαγγελματικές καταστάσεις (Kalajžić, 2019; Verizon, 2023).

Η πλαστοπροσωπία αποτελεί μια θεμελιώδη μέθοδο που διατρέχει τις περισσότερες τεχνικές κοινωνικής μηχανικής. Σύμφωνα με την έκθεση Ransomware Insights του 2023 από την Barracuda, το 69% των επιθέσεων ransomware (λυτρισμικού) ξεκίνησαν με emails πλαστοπροσωπίας, όπου οι επιτιθέμενοι μιμούνται νόμιμους οργανισμούς ή άτομα εξουσίας για να πείσουν τα θύματα να προβούν σε συγκεκριμένες ενέργειες, όπως το άνοιγμα μολυσμένων συνημμένων ή τη μεταφορά χρημάτων (Doncevic, 2023). Η αποτελεσματικότητα αυτής της μεθόδου ενισχύεται με την επίκληση στην εξουσία, τη δημιουργία αίσθησης επείγοντος, τον χειρισμό συναισθημάτων και την εκμετάλλευση τρεχόντων γεγονότων.

Το ηλεκτρονικό ψάρεμα (phishing) αποτελεί μια από τις πιο διαδεδομένες μεθόδους κοινωνικής μηχανικής, με την ENISA να αναφέρει ότι το 2023 αντιπροσώπευε το 41% όλων των περιστατικών κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Η επιτυχία του phishing βασίζεται στον συνδυασμό τεχνολογικής εξαπάτησης και ψυχολογικής χειραγώγησης, εκμεταλλευόμενο την τάση των ανθρώπων να εμπιστεύονται φαινομενικά επίσημα μηνύματα (Bridgers et al., 2023; ENISA, 2023).

Το δόλωμα διαφοροποιείται από τις άλλες μεθόδους καθώς εκμεταλλεύεται την περιέργεια και την απληστία των θυμάτων, προσφέροντας κάτι δελεαστικό σε αντάλλαγμα για πληροφορίες ή πρόσβαση. Η τεχνική αυτή είναι ιδιαίτερα αποτελεσματική καθώς εκμεταλλεύεται βασικά ανθρώπινα ένστικτα και συμπεριφορές (Hobel et al., 2014).

Οι επιτιθέμενοι μπορεί να υποδυθούν αρχές, συναδέλφους, τεχνικούς υποστήριξης ή άλλα άτομα εμπιστοσύνης για να αποκτήσουν πρόσβαση σε συστήματα ή ευαίσθητες πληροφορίες (Salahdine & Kaabouch, 2019). Οι επιθέσεις μπορεί να πραγματοποιηθούν μέσω διαφόρων καναλιών επικοινωνίας, όπως τηλέφωνο, email, μέσα κοινωνικής δικτύωσης ή ακόμα και δια ζώσης (Edwards et al., 2024). Σε ορισμένες περιπτώσεις, οι επιτιθέμενοι μπορεί να δημιουργήσουν πλαστές ταυτότητες ή διαπιστευτήρια για να ενισχύσουν την αξιοπιστία τους (Mugala, 2014).

Οι τεχνολογικές εξελίξεις, όπως τα deepfakes, έχουν αυξήσει την πολυπλοκότητα και την αποτελεσματικότητα των τεχνικών τους. Για παράδειγμα, έχουν αναφερθεί περιπτώσεις όπου πολιτικοί έλαβαν πλαστές βιντεοκλήσεις από άτομα που προσποιούνταν άλλους αξιωματούχους (Noval, 2023).

Οι δράστες έχουν αναπτύξει αυτές τις μεθόδους με σκοπό την παράκαμψη των τεχνικών μέτρων ασφαλείας που έχουν σχεδιαστεί για την αποτροπή εισβολών στα διάφορα συστήματα. Η κοινωνική μηχανική εφαρμόζει ψυχολογικά στρατηγήματα με απώτερο στόχο τόσο την απόσπαση ευαίσθητων δεδομένων όσο και την πρόκληση συμπεριφορών που μπορούν να παραβιάσουν την ασφάλεια του συστήματος (Krombholz et al., 2015).

Οι στόχοι των επιθέσεων μπορεί να περιλαμβάνουν (Zaoui et al., 2024):

- Απόκτηση ευαίσθητων πληροφοριών (π.χ. ονόματα χρηστών, κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών).
- Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα ή εγκαταστάσεις.
- Χειραγώγηση ατόμων για την εκτέλεση συγκεκριμένων ενεργειών (ακόμη και εις βάρους τους).
- Οικονομική απάτη, όπως μεταφορά χρημάτων σε λογαριασμούς των επιτιθέμενων.
- Παραβίαση οργανωτικών πολιτικών και διαδικασιών ασφαλείας.

- Εγκατάσταση κακόβουλου λογισμικού σε συστήματα-στόχους.

Υπό το πρίσμα αυτό, και δεδομένου ότι κανένα ψηφιακό σύστημα δεν είναι πλήρως ανεξάρτητο από τον ανθρώπινο παράγοντα, η κοινωνική μηχανική αποτελεί ένα θέμα μείζονος σημασίας τόσο στη σύγχρονη κοινωνία όσο και στην ασφάλεια των (πληροφοριακών) συστημάτων. Πάντοτε θα υπάρχουν άνθρωποι σε θέσεις-κλειδιά για τη διαχείριση πληροφοριών και τη συντήρηση των συστημάτων, γεγονός που καθιστά την ανθρώπινη παρέμβαση αναπόφευκτη και, συνεπώς, ευάλωτη σε τεχνικές κοινωνικής μηχανικής (Hasan et al., 2024; Syafitri et al., 2022; Vrhovec et al., 2022).

3.1.2 Παράγοντες Επιτυχίας των Επιθέσεων

Η ευπάθεια των ατόμων σε επιθέσεις κοινωνικής μηχανικής έχει αποτελέσει αντικείμενο εκτενούς έρευνας. Ποικίλοι παράγοντες συμβάλλουν στη θυματοποίηση ενός ατόμου, συμπεριλαμβανομένων της απληστίας, του εγωκεντρισμού, του φόβου, των ενοχών, της ευπιστίας και της άγνοιας. Οι επιτυχημένοι δράστες κοινωνικής μηχανικής επιδεικνύουν αυτοπεποίθηση και ικανότητα ελέγχου της συνομιλίας με το θύμα τους. Για παράδειγμα, μπορεί να προσποιηθούν ότι είναι μέλη του συστήματος ασφαλείας στο οποίο επιδιώκουν πρόσβαση, παρά την έλλειψη νόμιμης εξουσιοδότησης. Η αυτοπεποίθησή τους συχνά επαρκεί για να υπερκεράσει τις αμφιβολίες των υπευθύνων διαχείρισης του συστήματος.

Οι τεχνικές που χρησιμοποιούν οι δράστες στοχεύουν ακριβώς σε αυτούς τους παράγοντες ευπάθειας. Για παράδειγμα, η χρήση κολακείας εκμεταλλεύεται τον εγωκεντρισμό του θύματος, ενώ η προσφορά μικρών δώρων μπορεί να ενεργοποιήσει το αίσθημα της απληστίας ή να δημιουργήσει αισθήματα ενοχής και υποχρέωσης. Επιπλέον, η χρήση χιούμορ αποσκοπεί στην εκμετάλλευση της ευπιστίας του θύματος, καθώς δημιουργεί μια ψευδή αίσθηση οικειότητας και εμπιστοσύνης. Όλες αυτές οι ενέργειες συνδυάζονται για να δημιουργήσουν μια σχέση εμπιστοσύνης και σύνδεσης, η οποία μπορεί να υπονομεύσει τις αμφιβολίες των ατόμων που είναι υπεύθυνα για τη διαφύλαξη των ευαίσθητων δεδομένων.

Η συμπάθεια και η συνεργασία μεταξύ των ανθρώπων είναι ζωτικής σημασίας όχι μόνο για τη γενική κοινωνική λειτουργία, αλλά και για την πρόοδο στις επιστήμες και σε άλλους τομείς. Ωστόσο, αυτή η τάση για συνεργασία μπορεί να καταστήσει τα άτομα ευάλωτα σε κακόβουλη εκμετάλλευση. Συγκεκριμένα άτομα, λόγω ελλιπούς εμπειρίας, προσωπικών αναγκών ή συγκεκριμένου ψυχολογικού προφίλ, μπορεί να είναι ιδιαίτερα επιρρεπή στο να εμπιστεύονται αγνώστους. Αυτό το γεγονός καθιστά τον ανθρώπινο παράγοντα ιδιαίτερα ευάλωτο σε επιθέσεις κοινωνικής μηχανικής.

Ένα χαρακτηριστικό παράδειγμα τεχνικής κοινωνικής μηχανικής είναι η προσφορά μπόνους ή άλλου δείγματος εύνοιας, το οποίο συχνά δημιουργεί μια αίσθηση υποχρέωσης για αμοιβαιότητα στον αποδέκτη. Αυτή η αίσθηση υποχρέωσης μπορεί να οδηγήσει στην ανταλλαγή πληροφοριών. Ωστόσο, η αξία αυτών των χειρονομιών τείνει να μειώνεται με την πάροδο του χρόνου. Συνεπώς, ένας ικανός δράστης κοινωνικής μηχανικής θα υπενθυμίζει συχνά στα άτομα-στόχους τις προηγούμενες ευεργεσίες του, διατηρώντας έτσι την αίσθηση υποχρέωσης.

Η περιέργεια και η έλλειψη ενημέρωσης αποτελούν επίσης σημαντικούς παράγοντες που καθιστούν τα άτομα ευάλωτα σε στρατηγικές κοινωνικής μηχανικής. Στο πλαίσιο των επιθέσεων σε συστήματα υπολογιστών, οι δράστες συχνά χρησιμοποιούν ελκυστικά σχεδιασμένα στοιχεία διεπαφής, όπως μεγάλα κουμπιά ή παράθυρα που υπόσχονται ενδιαφέρουσες εμπειρίες. Αυτά τα στοιχεία προσελκύουν τους χρήστες να κάνουν κλικ σε συνδέσμους ή να επισκεφθούν ιστότοπους χωρίς να αξιολογήσουν επαρκώς τους πιθανούς κινδύνους.

Τα μηνύματα που χρησιμοποιούνται σε τέτοιες επιθέσεις συχνά δημιουργούν μια αίσθηση κατεπείγοντος ή αναγκαιότητας, ωθώντας τους χρήστες να ενεργήσουν παρορμητικά, χωρίς να λάβουν υπόψη τις πιθανές αρνητικές συνέπειες των ενεργειών τους. Αυτή η τακτική εκμεταλλεύεται την τάση των ανθρώπων να αντιδρούν γρήγορα σε καταστάσεις που αντιλαμβάνονται ως επείγουσες, παρακάμπτοντας έτσι τη λογική σκέψη και την προσεκτική αξιολόγηση.

Η καλοσύνη και η αλληλεγγύη προς όσους φαίνεται να έχουν ανάγκη αποτελούν επίσης χαρακτηριστικά που συχνά εκμεταλλεύονται οι δράστες. Για παράδειγμα, ένας εισβολέας μπορεί να προσποιηθεί ότι μεταφέρει μια μεγάλη στοίβα εγγράφων, προκαλώντας το προσωπικό ασφαλείας να παραβλέψει τους τυπικούς (φυσικούς) ελέγχους ταυτότητας προκειμένου να τον βοηθήσουν. Αυτή η τεχνική εκμεταλλεύεται την ανθρώπινη τάση για αλτρουισμό και βοήθεια προς τους άλλους.

Η απληστία αποτελεί έναν ακόμη σημαντικό παράγοντα που καθιστά τα άτομα ευάλωτα σε τέτοιου είδους τεχνικές. Το προσωπικό σε χαμηλόμισθες θέσεις, όπως φύλακες, καθαριστές ή κλητήρες, μπορεί να είναι ιδιαίτερα ευάλωτο σε προσπάθειες δωροδοκίας ή εξαπάτησης. Η δυσαρέσκεια με τις αποδοχές τους μπορεί να τους κάνει πιο πρόθυμους να παρέχουν πρόσβαση ή πληροφορίες με αντάλλαγμα το οικονομικό όφελος. Αντίθετα, οι εργαζόμενοι με υψηλότερες αποδοχές τείνουν να είναι λιγότερο ευάλωτοι σε τέτοιες προσεγγίσεις.

Η διακριτικότητα είναι ένα ακόμη χαρακτηριστικό που οι δράστες κοινωνικής μηχανικής μπορούν να εκμεταλλευτούν. Οι άνθρωποι συχνά διστάζουν να ζητήσουν ταυτοποίηση από αγνώστους ή να παρακολουθήσουν στενά την εισαγωγή κωδικών πρόσβασης. Ένα παράδειγμα επίθεσης που εκμεταλλεύεται αυτή την τάση θα μπορούσε να περιλαμβάνει έναν δράστη που προσποιείται τον νέο υπάλληλο που «ξέχασε» την κάρτα πρόσβασής του, βασιζόμενος στη διστακτικότητα των άλλων να αμφισβητήσουν ή να ελέγξουν την ταυτότητά του.

Η έλλειψη προσοχής και η προχειρότητα στις ενέργειες αποτελούν επίσης αδυναμίες που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Για παράδειγμα, ένας δράστης θα μπορούσε να στείλει ένα email που μοιάζει με νόμιμη εταιρική επικοινωνία, αλλά περιέχει έναν κακόβουλο σύνδεσμο. Οι εργαζόμενοι που δεν είναι προσεκτικοί ή βιάζονται μπορεί να κάνουν κλικ στο σύνδεσμο χωρίς να ελέγξουν προσεκτικά την πηγή του.

Η απάθεια των εργαζομένων αποτελεί άλλο ένα σημαντικό ζήτημα που μπορεί να υπονομεύσει την ασφάλεια ενός συστήματος. Αυτό το πρόβλημα σχετίζεται άμεσα με τις πρακτικές διαχείρισης ανθρώπινου δυναμικού του οργανισμού, συμπεριλαμβανομένων των διαδικασιών επιλογής προσωπικού. Εργαζόμενοι που αισθάνονται αποξενωμένοι από το εργασιακό τους περιβάλλον μπορεί να επιδείξουν μειωμένα αντανακλαστικά και απροθυμία, καθιστώντας τους παθητικούς παρατηρητές σε περιστατικά που θα μπορούσαν να απειλήσουν την ασφάλεια του συστήματος. Για παράδειγμα, ένας απαθής υπάλληλος μπορεί να παρατηρήσει κάποιον άγνωστο να περιφέρεται σε έναν περιορισμένο χώρο χωρίς να αναλάβει δράση ή να αναφέρει το περιστατικό, θέτοντας έτσι σε κίνδυνο την ασφάλεια του οργανισμού.

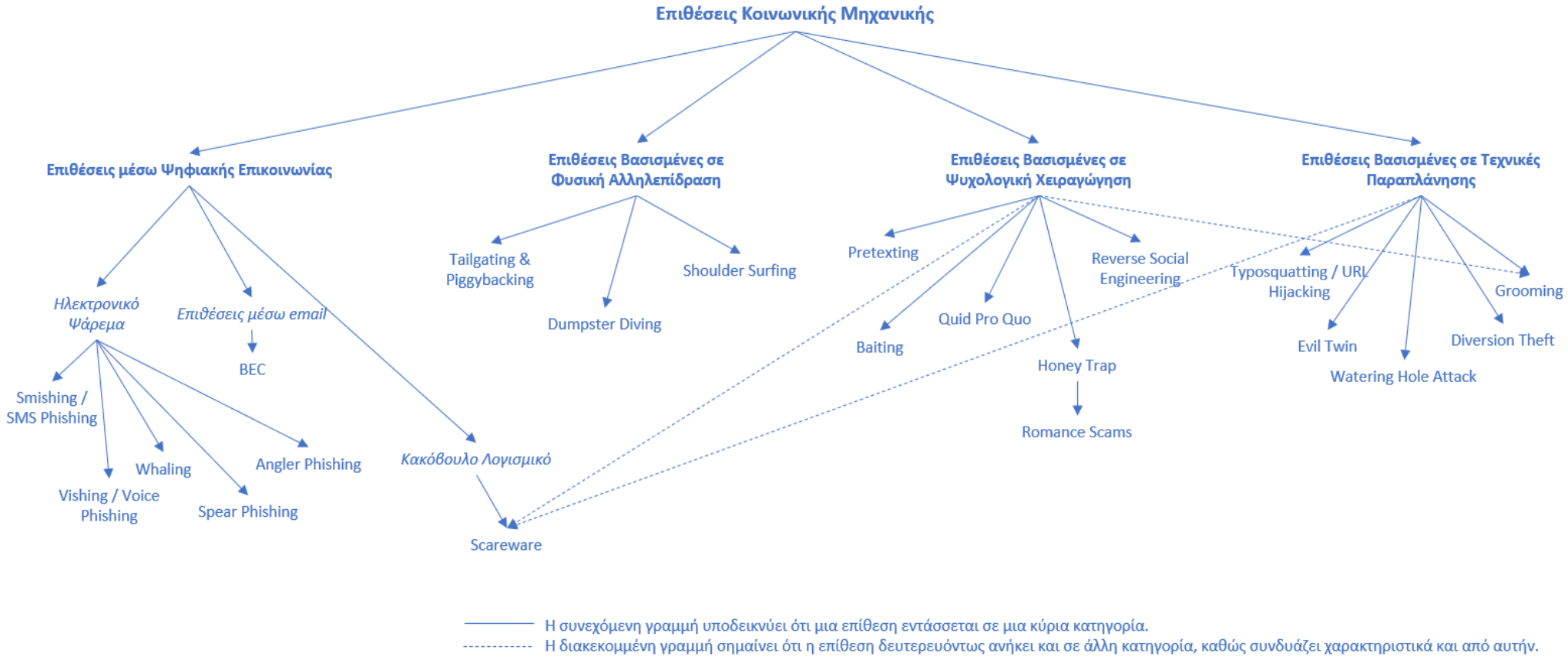
Η πλήξη των εργαζομένων αποτελεί έναν ακόμη παράγοντα κινδύνου, ιδιαίτερα σε επαναλαμβανόμενες εργασίες όπου οι κανόνες ασφαλείας μπορεί να παραβλέπονται. Αυτό μπορεί να οδηγήσει τους εργαζομένους να ακολουθούν συντομότερες διαδρομές για την επίτευξη των στόχων τους, θυσιάζοντας την ασφάλεια για χάρη της ευκολίας. Για παράδειγμα, ένας εργαζόμενος που εκτελεί καθημερινά την ίδια διαδικασία εισόδου σε ένα σύστημα μπορεί να κουραστεί από την επαναλαμβανόμενη ανάκληση του κωδικού πρόσβασης, στη μνήμου του και να αναζητήσει έναν πιο εύκολο και άμεσο τρόπο αποθήκευσης του κωδικού, όπως το να τον γράψει σε ένα σημειωματάριο ή σε ένα αυτοκόλλητο χαρτάκι στην οθόνη του υπολογιστή του, δημιουργώντας έτσι μια σοβαρή ευπάθεια ασφαλείας. Οι δράστες κοινωνικής μηχανικής συχνά στοχεύουν τέτοιους εργαζομένους, γνωρίζοντας ότι είναι πιο πιθανό να λάβουν τις απαιτούμενες πληροφορίες ή να αποκτήσουν την πολυπόθητη πρόσβαση με τη λιγότερη (δυνατή) αντίσταση.

Ο φόβος της εξουσίας αποτελεί έναν ακόμη σημαντικό παράγοντα που εκμεταλλεύονται οι δράστες κοινωνικής μηχανικής. Πολλοί άνθρωποι τείνουν να υπακούουν σε εντολές που φαίνεται να προέρχονται από ανώτερα στελέχη ή αρχές, ακόμη και αν δεν είναι απόλυτα σίγουροι για την ταυτότητα του ατόμου που δίνει την εντολή. Αυτό μπορεί να οδηγήσει σε καταστάσεις όπου οι εργαζόμενοι εκτελούν ενέργειες που παραβιάζουν τις πολιτικές ασφαλείας, φοβούμενοι τις συνέπειες της μη συμμόρφωσης. Για παράδειγμα, ένας επιτιθέμενος μπορεί να προσποιηθεί ότι είναι ανώτερο στέλεχος της εταιρείας και να ζητήσει επείγουσα πρόσβαση σε ευαίσθητα δεδομένα ή να απαιτήσει την εκτέλεση μιας μεταφοράς χρημάτων. Ο φόβος της ανυπακοής σε έναν υποτιθέμενο ανώτερο μπορεί να οδηγήσει τους εργαζόμενους να παρακάμψουν τις καθιερωμένες διαδικασίες ασφαλείας (Greavu-Şerban & Şerban, 2014).

Σε αντίθεση με τα τεχνικά στοιχεία ενός συστήματος ασφαλείας, τα οποία μπορούν να αναβαθμιστούν ή να αντικατασταθούν σχετικά εύκολα, ο ανθρώπινος τρόπος λήψης αποφάσεων είναι πολύ πιο περίπλοκος και δύσκολο να τροποποιηθεί ή να βελτιωθεί. Ωστόσο, είναι σημαντικό να σημειωθεί ότι τα άτομα μπορούν να βελτιώσουν την ικανότητά τους να αναγνωρίζουν και να αποκρούουν τέτοιου είδους επιθέσεις μέσω κατάλληλης εκπαίδευσης και αυξημένης επαγρύπνησης, είτε έχουν πέσει θύματα επίθεσης κοινωνικής μηχανικής, είτε όχι. Η εκπαίδευση και η ευαισθητοποίηση των εργαζομένων αποτελούν κρίσιμα στοιχεία στην αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής.

3.2. Κατηγοριοποίηση & Ανάλυση Επιθέσεων Κοινωνικής Μηχανικής

Στο παρακάτω διάγραμμα (Εικόνα 1) απεικονίζεται η ιεραρχική κατηγοριοποίηση των επιθέσεων κοινωνικής μηχανικής με τέσσερις βασικές διαστάσεις, οι οποίες διακρίνονται με βάση το κύριο μέσο και τη μέθοδο που χρησιμοποιείται για την εξαπάτηση.



Εικόνα 1: Κατηγοριοποίηση Επιθέσεων Κοινωνικής Μηχανικής

Πιο αναλυτικά, οι γενικές κατηγορίες που παρουσιάζονται είναι οι κάτωθι:

1. **Επιθέσεις μέσω Ψηφιακής Επικοινωνίας**: Περιλαμβάνει επιθέσεις που εκμεταλλεύονται τα ψηφιακά κανάλια επικοινωνίας. Αναλύονται στην υποενότητα 3.2.1 και περιλαμβάνουν το ηλεκτρονικό ψάρεμα με τις παραλλαγές του, τις επιθέσεις μέσω email και το κακόβουλο λογισμικό.
2. **Επιθέσεις Βασισμένες σε Φυσική Αλληλεπίδραση**: Αφορά επιθέσεις που απαιτούν φυσική παρουσία ή εγγύτητα με το στόχο. Αναλύονται στην υποενότητα 3.2.2 και περιλαμβάνουν τεχνικές, όπως tailgating (παραβίαση ασφαλείας με ακολούθηση), dumpster diving (αναζήτηση σε κάδους απορριμμάτων) και shoulder surfing (σερφάρισμα πάνω από τον ώμο).
3. **Επιθέσεις Βασισμένες σε Ψυχολογική Χειραγώγηση:** Επικεντρώνονται στην εκμετάλλευση ανθρώπινων συναισθημάτων και συμπεριφορών. Αναλύονται στην υποενότητα 3.2.3 και περιλαμβάνουν τεχνικές, όπως pretexting (προσποίηση), baiting, quid pro quo (αντίκρισμα), honey trap (παγίδα μελιού) και reverse social engineering (επίθεση αντίστροφης κοινωνικής μηχανικής).
4. **Επιθέσεις Βασισμένες σε Τεχνικές Παραπλάνησης**: Εστιάζουν στη δημιουργία παραπλανητικών καταστάσεων ή περιβαλλόντων. Αναλύονται στην υποενότητα 3.2.4 και περιλαμβάνουν τεχνικές, όπως typosquatting (τυποκαταλήστευση), evil twin (κακόβουλο δίδυμο), watering hole attacks (επίθεση στο σημείο συγκέντρωσης), diversion theft (επίθεση εκτροπής κλοπής) και grooming (προετοιμασία θυμάτων).

Αξίζει να σημειωθεί ότι η κατηγοριοποίηση αυτή δεν είναι αυστηρά διαχωρισμένη, καθώς πολλές επιθέσεις συνδυάζουν χαρακτηριστικά από διαφορετικές κατηγορίες. Για παράδειγμα:

- Το Scareware, που εμφανίζεται ως κακόβουλο λογισμικό, χρησιμοποιεί τόσο ψυχολογική χειραγώγηση όσο και τεχνικές παραπλάνησης.
- Το Grooming, αν και κατηγοριοποιείται στις τεχνικές παραπλάνησης, βασίζεται έντονα στην ψυχολογική χειραγώγηση.

Η παρούσα κατηγοριοποίηση των επιθέσεων κοινωνικής μηχανικής που εντάχθηκε στην εργασία, βασίζεται σε συνδυασμό των ερευνητικών εργασιών των Salahdine & Kaabouch (2019), Odeh et al. (2021), Kushwaha et al. (2024) και Zaoui et al. (2024), οι οποίοι πρότειναν παρόμοιες ταξινομήσεις. Αυτή η συνδυασμένη προσέγγιση αξιοποιεί τα βασικά ευρήματα από τις παραπάνω εργασίες και ενσωματώνει νέα στοιχεία που προκύπτουν από την ανάλυση που πραγματοποιήθηκε στα πλαίσια της μελέτης, δημιουργώντας μια πιο πλήρη και ευέλικτη κατηγοριοποίηση.

Στις επόμενες ενότητες, παρουσιάζεται ο βασικός ορισμός της κάθε επίθεσης, ενώ ταυτόχρονα αναλύονται λεπτομερώς οι επιθέσεις ανά κατηγορία και υποκατηγορία, συνοδευόμενες από παραδείγματα και προτάσεις προστασίας.

3.2.1. Επιθέσεις μέσω Ψηφιακής Επικοινωνίας

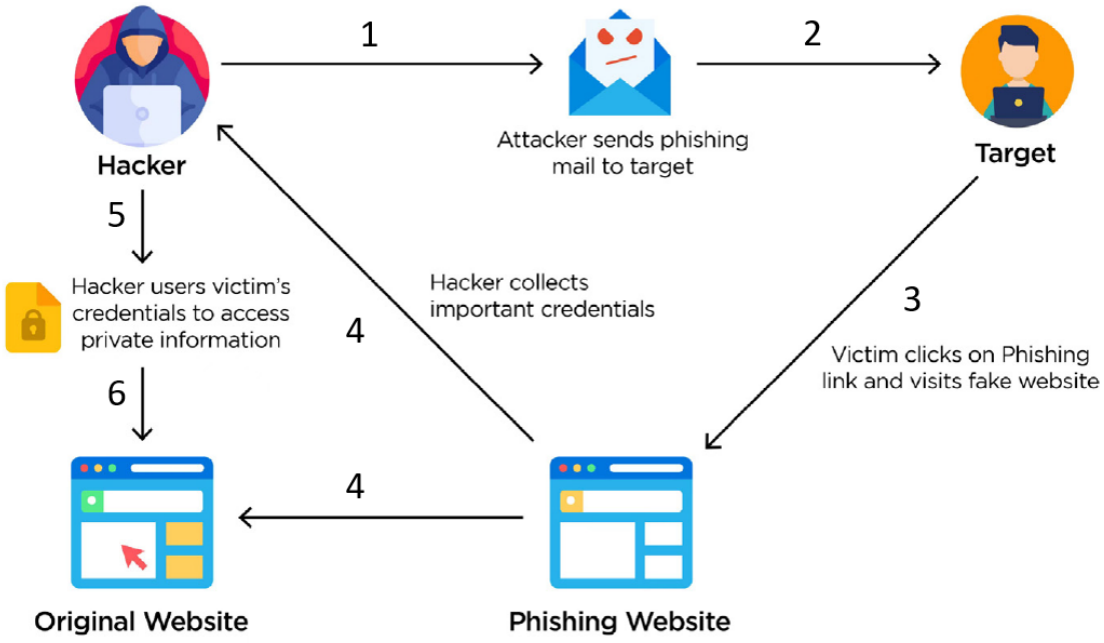
Οι επιθέσεις που βασίζονται στην ψηφιακή επικοινωνία αποτελούν ίσως την πιο διαδεδομένη μορφή κοινωνικής μηχανικής στη σύγχρονη ψηφιακή εποχή. Αυτές οι επιθέσεις εκμεταλλεύονται την εξάρτηση του σύγχρονου ανθρώπου και εργαζόμενου από τα ηλεκτρονικά μέσα επικοινωνίας, όπως το email και τα μηνύματα κειμένου, για να παραπλανήσουν τα θύματα και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και περιλαμβάνουν ποικιλία μεθόδων που εκμεταλλεύονται την ψηφιακή αλληλεπίδραση, για την αποκόμιση ευαίσθητων πληροφοριών μεταξύ άλλων σκοπών ή στόχων. Στις επιθέσεις αυτές περιλαμβάνονται υποκατηγορίες του ηλεκτρονικού ψαρέματος, όπως το spear phishing, το whaling, το vishing, το smishing και το angler phishing. Επιπλέον, το Business Email Compromise (BEC) είναι μια άλλη μορφή επίθεσης που εκμεταλλεύεται τους ηλεκτρονικούς λογαριασμούς για να εξαπατήσει τους χρήστες, ενώ το scareware αποτελεί κακόβουλο λογισμικό που χρησιμοποιεί το φόβο για να πείσει τα θύματα να εγκαταστήσουν ή να αγοράσουν κακόβουλα προϊόντα.

3.2.1.1. Ηλεκτρονικό Ψάρεμα

Το ηλεκτρονικό ψάρεμα (phishing) αποτελεί μια από τις πλέον διαδεδομένες και εξελισσόμενες μορφές κυβερνοεπιθέσεων στον σύγχρονο ψηφιακό κόσμο, με ιδιαίτερη απήχηση στο εταιρικό περιβάλλον. Σύμφωνα με την αναφορά της Cisco (2021), περίπου το 86% των οργανισμών ανέφερε ότι τουλάχιστον ένα άτομο μέσα στον οργανισμό έπεσε θύμα phishing, κάνοντας κλικ σε κακόβουλο σύνδεσμο, γεγονός που συχνά οδηγεί σε σοβαρά περιστατικά ασφαλείας. Η πανδημία του COVID-19 επιδείνωσε την κατάσταση, συμβάλλοντας σε μια δραματική αύξηση του αριθμού των επιθέσεων ηλεκτρονικού ψαρέματος. Συγκεκριμένα, το τρίτο τρίμηνο του 2021 καταγράφηκε η δημιουργία άνω των 400.000 μοναδικών phishing ιστοσελίδων, με μια συνεχιζόμενη αύξηση της τάσης αυτής και στο τέταρτο τρίμηνο (Johnson, 2021).

Πιο αναλυτικά, το ηλεκτρονικό ψάρεμα είναι μια μορφή κοινωνικής μηχανικής όπου ο επιτιθέμενος προσπαθεί να αποσπάσει ευαίσθητες πληροφορίες ή να εγκαταστήσει κακόβουλο λογισμικό χρησιμοποιώντας τεχνικές παραπλάνησης. Όπως απεικονίζεται στην παρακάτω εικόνα, μια τυπική επίθεση phishing ξεκινά με την αποστολή ενός δόλιου ψηφιακού μηνύματος

που μιμείται αξιόπιστες πηγές (π.χ. τράπεζες, γνωστές εταιρείες, κυβερνητικούς οργανισμούς). Το θύμα συνήθως οδηγείται σε μια πλαστή ιστοσελίδα όπου του ζητείται να καταχωρήσει προσωπικά στοιχεία, τραπεζικά δεδομένα ή διαπιστευτήρια πρόσβασης, τα οποία στη συνέχεια ο επιτιθέμενος χρησιμοποιεί για κακόβουλους σκοπούς. Εναλλακτικά, μπορεί να κληθεί να ανοίξει συνημμένα αρχεία ή να επισκεφθεί κακόβουλους ιστοτόπους, μέσω των οποίων εγκαθίσταται κακόβουλο λογισμικό στον υπολογιστή του (Adu-Manu et al., 2023; NIST, 2024a; Shombot et al., 2024; Yasin et al., 2024).



Εικόνα 2: Διαδικασία μιας επίθεσης ηλεκτρονικού ψαρέματος

Πηγή: (Yasin et al., 2024)

Οι κυβερνοεγκληματίες αξιοποιούν ποικίλες τεχνικές για να προσδώσουν αξιοπιστία στα μηνύματα ηλεκτρονικού ψαρέματος, που έχουν ως απώτερο στόχο να παραπλανήσουν τα θύματά τους. Αυτές οι τεχνικές περιλαμβάνουν τη χρήση επίσημων λογοτύπων στους τίτλους και στο σώμα των emails, την παραποίηση του τομέα (domain) του αποστολέα μέσω της τεχνικής του domain spoofing (πλαστοπροσωπία τομέα), καθώς και την αντιγραφή του στυλ γραφής και της δομής των επίσημων επικοινωνιών. Ένας από τους μηχανισμούς που χρησιμοποιούνται συχνά για την αποφυγή ανίχνευσης από τα φίλτρα anti-spam είναι η εισαγωγή μεγάλων ποσοτήτων κρυφού κειμένου μέσω HTML/CSS τεχνικών διαφυγής (Gallo et al., 2024).

Οι επιθέσεις phishing εκμεταλλεύονται τον ανθρώπινο παράγοντα, ο οποίος συχνά θεωρείται ο πιο ευάλωτος κρίκος στην αλυσίδα της κυβερνοασφάλειας. Εμπειρικές μελέτες έχουν επισημάνει ότι τα χαρακτηριστικά προσωπικότητας που εντάσσονται στο πλαίσιο Big Five (ανοιχτότητα, ευσυνειδησία, εξωστρέφεια, προσήνεια, νευρωτισμός) συχνά συνδέονται με την ευαισθησία του ατόμου σε αυτού του τύπου τις επιθέσεις.

Πρωτοποριακή έρευνα των Dhamija et al. (2006) κατέδειξε ότι οι περισσότεροι χρήστες αποτυγχάνουν να αναγνωρίσουν τη διαφορά ανάμεσα σε δόλια και νόμιμα URLs (Uniform Resource Locators). Τα αποτελέσματα αυτής της μελέτης έδειξαν ότι παράγοντες, όπως η ηλικία, το φύλο, το επίπεδο εκπαίδευσης και η συχνότητα χρήσης υπολογιστών, δεν αποτελούν αξιόπιστους δείκτες της ικανότητας των χρηστών να εντοπίζουν επιθέσεις ηλεκτρονικού ψαρέματος. Ωστόσο, η αυξημένη γνώση σε τομείς, όπως η επιστήμη των υπολογιστών, τα πιστοποιητικά HTTPS και η κατανόηση των μηχανισμών κρυπτογράφησης και αυθεντικότητας, έχουν βρεθεί να ενισχύουν σημαντικά την ικανότητα των χρηστών να ξεχωρίζουν νόμιμα από κακόβουλα μηνύματα (Gallo et al., 2024).

Οι επιτιθέμενοι χρησιμοποιούν τεχνικές που βασίζονται στις αρχές πειθούς, εκμεταλλευόμενοι γνωστικές ευπάθειες των θυμάτων. Οι αρχές αυτές, όπως περιγράφηκαν από τον Cialdini (1984), περιλαμβάνουν την εξουσία, τη συμπάθεια, τη σπανιότητα, τη συνέπεια, την κοινωνική απόδειξη και την αμοιβαιότητα. Στις επιθέσεις ηλεκτρονικού ψαρέματος, οι επιτιθέμενοι εφαρμόζουν αυτές τις αρχές για να αυξήσουν την πιθανότητα επιτυχίας της απάτης, επιδιώκοντας μια πιο πειστική προσέγγιση. Ειδικότερα, η έννοια των γνωστικών τεχνικών αναφέρεται στην εισαγωγή στοιχείων ή μηνυμάτων που ενεργοποιούν τις συγκεκριμένες αρχές πειθούς στον παραλήπτη. Έρευνα των Wang et al. (2021) εξέτασε την επίδραση που έχουν οι γνωστικοί παράγοντες και οι δείκτες εξαπάτησης στις αποφάσεις των θυμάτων κατά τη διάρκεια αυτών των επιθέσεων, δείχνοντας ότι η χρήση γνωστικών τεχνικών αυξάνει σημαντικά την πιθανότητα ανταπόκρισης του θύματος, ενώ αντίθετα οι δείκτες εξαπάτησης, όπως γραμματικά λάθη και ψευδή τομείς email, μειώνουν την αποτελεσματικότητα της επίθεσης (Gallo et al., 2024).

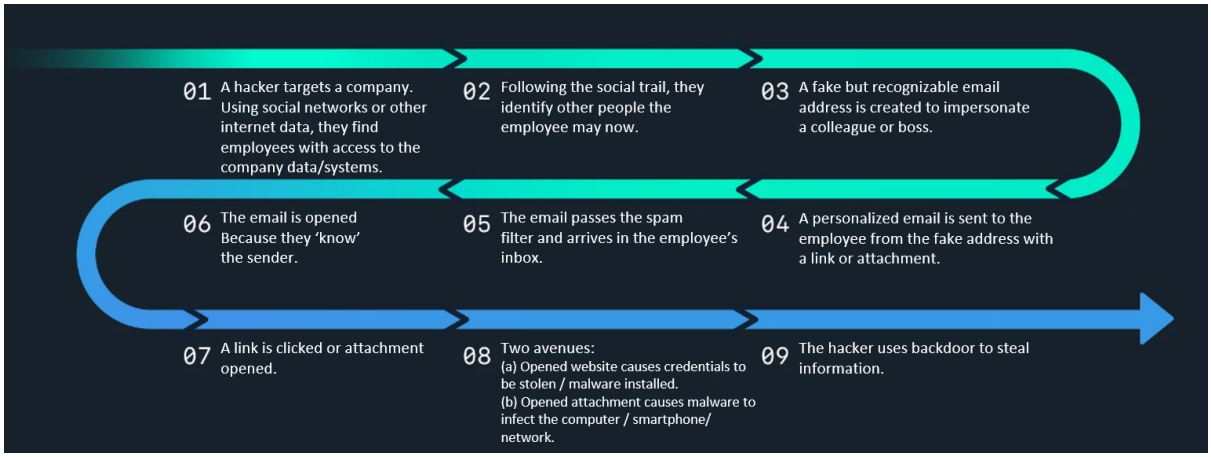
Η ανίχνευση επιθέσεων phishing είναι σχετικά εύκολη χάρη στα σύγχρονα φίλτρα spam και τα συστήματα ασφάλειας email, τα οποία εντοπίζουν την πλειονότητα αυτών των επιθέσεων.

3.2.1.1.1. Spear Phishing

Το spear phishing (στοχευμένο ηλεκτρονικό ψάρεμα) είναι μια εξειδικευμένη μορφή ηλεκτρονικού ψαρέματος που στοχεύει συγκεκριμένα άτομα ή ομάδες μέσα σε έναν

οργανισμό, χρησιμοποιώντας πληροφορίες σχετικές με το θύμα για να αυξήσει την πιθανότητα επιτυχίας. Η διαδικασία ξεκινά με τη συγκέντρωση πληροφοριών για το θύμα-στόχο μέσω κοινωνικών δικτύων και άλλων διαδικτυακών πηγών. Στη συνέχεια, ο επιτιθέμενος χαρτογραφεί το κοινωνικό δίκτυο του στόχου, δημιουργεί πειστικές απομιμήσεις διευθύνσεων ηλεκτρονικού ταχυδρομείου γνωστών επαφών, και αποστέλλει προσωποποιημένα μηνύματα που συχνά περιέχουν κακόβουλους συνδέσμους ή συνημμένα.

Η επίθεση ολοκληρώνεται όταν ο παραλήπτης, πιστεύοντας ότι το μήνυμα προέρχεται από αξιόπιστη πηγή, ανοίγει το συνημμένο ή ακολουθεί το σύνδεσμο, επιτρέποντας στον επιτιθέμενο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα συστήματα του οργανισμού (βλ. Εικόνα 3). Αυτός ο τύπος επίθεσης, αν και ευρύτερα διαδεδομένος, διαφοροποιείται από τις επιθέσεις **BEC** ή **whaling**, καθώς μπορεί να στοχεύσει οποιοδήποτε στέλεχος ανεξαρτήτως ιεραρχίας και συχνά δεν απαιτεί προηγούμενη παραβίαση ή μίμηση ενός συγκεκριμένου λογαριασμού email. (Adu-Manu et al., 2023; NIST, 2024a; Yasin et al., 2024).



Εικόνα 3: Ανατομία ενός στοχευμένου ηλεκτρονικού ψαρέματος

Πηγή: (Effect, 2024)

Μελετητές, όπως οι Burda και συν. (2020) διεξήγαγαν πειράματα σε υπαλλήλους πανεπιστημίων και συμβουλευτικών εταιρειών, αναλύοντας τον τρόπο με τον οποίο αντιδρούν στα στοχευμένα phishing emails. Τα αποτελέσματα της μελέτης έδειξαν ότι οι νεότεροι εργαζόμενοι, ειδικά στο ακαδημαϊκό περιβάλλον, ήταν πιο ευάλωτοι από τους παλαιότερους, τους ανώτερους και τους υπαλλήλους υποστήριξης. Παρόλα αυτά, οι επιθέσεις που εξαπολύθηκαν στους υπαλλήλους εταιρειών συνολικά παρουσίασαν υψηλότερα ποσοστά επιτυχίας από ό,τι στους πανεπιστημιακούς υπαλλήλους, κάτι που αναδεικνύει τους περιορισμούς των υφιστάμενων εκπαιδευτικών πρακτικών στις επιχειρήσεις. Η διαδικασία σχεδιασμού στοχευμένων επιθέσεων ηλεκτρονικού ψαρέματος περιελάμβανε τη χρήση

OSINT (Open-Source Intelligence[2]) (Νοημοσύνη Ανοιχτών Πηγών) για τη συλλογή πληροφοριών, τη δημιουργία προφίλ στόχων και την κλωνοποίηση ιστοσελίδων, καθώς και την κατασκευή εξειδικευμένων email templates που στοχεύουν σε συγκεκριμένες αδυναμίες ή ανάγκες των θυμάτων (Gallo et al., 2024).

Οι επιθέσεις spear-phishing, λόγω του εξατομικευμένου και στοχευμένου χαρακτήρα τους, παρουσιάζουν μεγαλύτερη πρόκληση για τα συστήματα ανίχνευσης, καθώς συχνά παρακάμπτουν τους αυτοματοποιημένους ελέγχους.

3.2.1.1.2. Whaling

Ο όρος whaling (φαλαινοθηρία) αναφέρεται σε έναν εξειδικευμένο τύπο ηλεκτρονικού ψαρέματος που στοχεύει αποκλειστικά σε υψηλόβαθμα στελέχη ή σημαντικά πρόσωπα εντός μιας οργανωτικής δομής, όπως διευθυντές ή ανώτατα διοικητικά στελέχη, όπως απεικονίζεται στην Εικόνα 4. Αν και μοιράζεται κάποια κοινά χαρακτηριστικά με το **spear phishing**, η βασική του διαφορά έγκειται στην αποκλειστική στόχευση ατόμων που έχουν πρόσβαση σε κρίσιμες πληροφορίες και εξουσία να εγκρίνουν οικονομικές ή διοικητικές αποφάσεις μεγάλης σημασίας.

Εικόνα 4: Φαλαινοθηρική επίθεση

Πηγή: (Tarada, 2022)

[2] Ο όρος OSINT μπορεί να αποδοθεί στα ελληνικά ως "Πληροφοριακή Συλλογή από Ανοιχτές Πηγές" ή απλούστερα "Πληροφόρηση Ανοιχτών Πηγών".
Πρόκειται για μια μεθοδολογία συλλογής, ανάλυσης και αξιοποίησης πληροφοριών που προέρχονται από δημόσια διαθέσιμες πηγές, όπως:

1. Μέσα κοινωνικής δικτύωσης
2. Εταιρικές ιστοσελίδες
3. Δημόσια έγγραφα
4. Ειδησεογραφικούς ιστότοπους
5. Επαγγελματικά δίκτυα (π.χ. LinkedIn)
6. Δημόσιες βάσεις δεδομένων
7. Φόρουμ και blogs

Οι επιτιθέμενοι δημιουργούν εξαιρετικά προσαρμοσμένα και πειστικά μηνύματα που συχνά περιλαμβάνουν αιτήματα για αποκάλυψη ευαίσθητων πληροφοριών, μεταφορά χρημάτων, ή παροχή πρόσβασης σε σημαντικά συστήματα. Οι επιθέσεις **whaling** διαφοροποιούνται από την **BEC**, καθώς δεν απαιτούν απαραίτητα παραβίαση ή μίμηση ενός λογαριασμού email. Ωστόσο, η στόχευση συγκεκριμένων ατόμων με σημαντικά προνόμια καθιστά αυτές τις επιθέσεις εξαιρετικά επικίνδυνες και δυνητικά καταστροφικές για έναν οργανισμό. (Greavu-Șerban & Șerban, 2014; Adu-Manu et al., 2023; NIST, 2024c; Syafitri et al., 2022).

Οι επιθέσεις whaling, που επικεντρώνονται σε υψηλόβαθμα στελέχη και χρησιμοποιούν προσωπικές ή ευαίσθητες μορφές επικοινωνίας, είναι πολύ δύσκολο να εντοπιστούν λόγω της μοναδικότητας των μηνυμάτων τους.

3.2.1.1.3. Smishing / SMS Phishing

Το Smishing / SMS Phishing (ηλεκτρονικό ψάρεμα μέσω SMS -Short Message Service-) είναι μια μορφή ηλεκτρονικής απάτης, η οποία πραγματοποιείται μέσω σύντομων μηνυμάτων κειμένου που αποστέλλονται στο κινητό τηλέφωνο του θύματος (Udochukwu & Bode-Asa, 2023; Khan, 2023; Timko & Rahman, 2024).

Μια επίθεση smishing (δείτε Εικόνα 5) διαδραματίζεται ως εξής (iefimerida, 2022):

- Το θύμα λαμβάνει ένα SMS στο κινητό του, το οποίο φαίνεται να προέρχεται από μια αξιόπιστη οντότητα, οργανισμό ή άτομο.
- Το μήνυμα είναι σύντομο και περιέχει έναν σύνδεσμο (link).
- Όταν ο ανυποψίαστος χρήστης κάνει κλικ στον σύνδεσμο, είτε εγκαθιστά κακόβουλο λογισμικό (malware) στη συσκευή του, είτε ανακατευθύνεται σε έναν κακόβουλο ιστότοπο (malicious website) όπου του ζητείται να εισάγει διάφορα προσωπικά δεδομένα, όπως ευαίσθητες πληροφορίες, κωδικούς πρόσβασης, στοιχεία ταυτότητας ή διαβατηρίου, δεδομένα τραπεζικών λογαριασμών και στοιχεία τραπεζικής κάρτας.

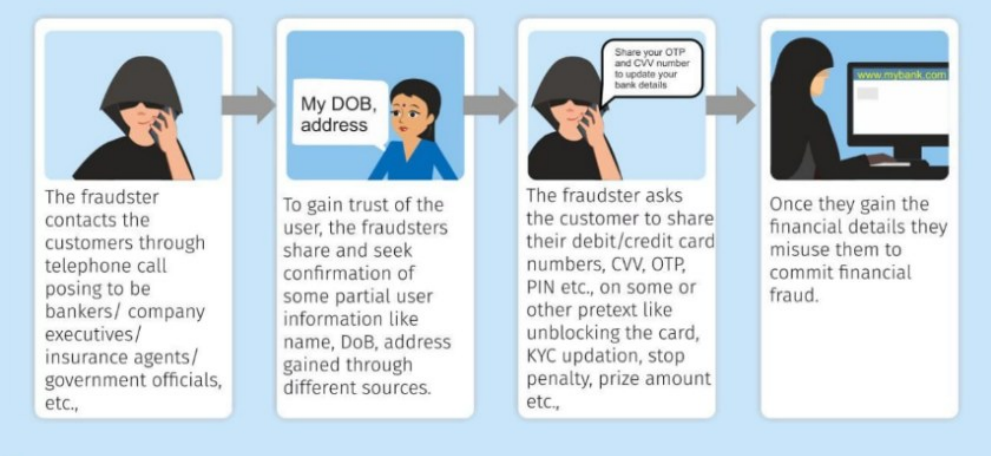
Εικόνα 5: Απεικόνιση μιας επίθεση ηλεκτρονικού ψαρέματος μέσω SMS

Πηγή: (Knezevic, 2024)

Οι επιθέσεις smishing και αλλά και vishing (phishing μέσω φωνητικών κλήσεων) που εξετάζονται στην επόμενη υποενότητα καθίστανται δυσκολότερα ανιχνεύσιμες, καθώς παρακάμπτουν τα παραδοσιακά φίλτρα ασφαλείας που βασίζονται σε email.

3.2.1.1.4. Vishing / Voice Phishing

Το Vishing / Voice Phishing (φωνητική απάτη ή φωνητικό ψάρεμα) αποτελεί μια μορφή κοινωνικής μηχανικής που αξιοποιεί τις φωνητικές κλήσεις, συχνά μέσω τεχνολογιών VoIP (Voice over Internet Protocol), για να παραπλανήσει τα θύματα να αποκαλύψουν ευαίσθητες πληροφορίες ή να εκτελέσουν ενέργειες που απειλούν την ασφάλειά τους. Οι επιτήδειοι, όπως απεικονίζεται στην Εικόνα 6, προσποιούνται ότι είναι αξιόπιστοι φορείς, όπως τράπεζες ή κυβερνητικές υπηρεσίες, και χρησιμοποιούν διάφορες ψυχολογικές τεχνικές, όπως απειλές ή δημιουργία άγχους, για να παρασύρουν τους χρήστες να παρέχουν προσωπικά δεδομένα, όπως αριθμούς πιστωτικών καρτών ή κωδικούς πρόσβασης (Khan, 2023; Syafitri et al., 2022; Zaoui et al., 2024).



Εικόνα 6: Τρόπος δράσης των επιτιθέμενων φωνητικού ψαρέματος

Πηγή: (Cyber Yodha, 2023)

3.2.1.1.5. Angler Phishing

Το Angler Phishing (ψάρεμα μέσω κοινωνικών δικτύων) αποτελεί μια εξελιγμένη μορφή ηλεκτρονικής απάτης, κατά την οποία οι δράστες δημιουργούν ψεύτικα προφίλ ή κλωνοποιούν τους επίσημους λογαριασμούς εξυπηρέτησης πελατών εταιρειών. Στόχος τους είναι να εξαπατήσουν τους πελάτες εκμεταλλευόμενοι τις δημόσιες αναρτήσεις τους. Συνήθως, οι επιτιθέμενοι εντοπίζουν άτομα που εκφράζουν δυσαρέσκεια, προσεγγίζοντάς τα με ψεύτικες προτάσεις επίλυσης ζητημάτων, όπως απεικονίζεται στην παρακάτω εικόνα. Προσποιούμενοι ότι είναι εκπρόσωποι της εταιρείας, ζητούν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή προσωπικά δεδομένα.

Εικόνα 7: Ψάρεμα μέσω κοινωνικών δικτύων

Πηγή: (Irwin; 2019)

Ωστόσο, ακόμη και οι πελάτες που εκφράζουν ικανοποίηση ή ενθουσιασμό από τις υπηρεσίες μπορεί να πέσουν θύματα αυτής της μορφής ψαρέματος. Σε αυτές τις περιπτώσεις, οι επιτιθέμενοι ενδέχεται να εκμεταλλευτούν την αυξημένη εμπιστοσύνη και θετική διάθεσή

τους, προσφέροντας ψεύτικες προσφορές ή δώρα, τα οποία απαιτούν την παροχή προσωπικών στοιχείων για την υποτιθέμενη ενεργοποίηση. Ο ενθουσιασμός των πελατών μπορεί να μειώσει την επιφυλακτικότητά τους, καθιστώντας τους εν τέλει ευάλωτους σε τέτοιες απάτες (Irwin; 2019; Syafitri et al., 2022).

3.2.1.2. Επιθέσεις μέσω Email

Η ανιχνευσιμότητα των επιθέσεων μέσω email κυμαίνεται από μέτρια έως υψηλή, ανάλογα με τον τύπο της επίθεσης και τα μέτρα προστασίας που έχουν υιοθετηθεί από τους οργανισμούς. Τα συστήματα προστασίας από κακόβουλο λογισμικό και τα φίλτρα email είναι σε θέση να εντοπίσουν ύποπτα συνημμένα αρχεία ή συνδέσμους, ωστόσο οι επιθέσεις που χρησιμοποιούν τεχνικές κοινωνικής μηχανικής ή επιθέσεις εκμετάλλευσης που εκμεταλλεύονται ευπάθειες λογισμικού που δεν έχουν ακόμη ανακαλυφθεί (zero-day exploits) είναι εξαιρετικά δύσκολο να ανιχνευθούν. Οι επιθέσεις αυτές εκμεταλλεύονται αδυναμίες που δεν είναι ακόμα γνωστές στο κοινό και, ως εκ τούτου, η άμυνα απέναντί τους απαιτεί συνεχιζόμενη ενημέρωση και δυναμική ανίχνευση νέων απειλών.

3.2.1.2.1. BEC

Η παραβίαση επιχειρηματικού ηλεκτρονικού ταχυδρομείου (BEC: Business Email Compromise) (δείτε Εικόνα 8) είναι μια εξειδικευμένη και στοχευμένη μορφή κοινωνικής μηχανικής που επικεντρώνεται σε επιχειρηματικές συναλλαγές και εσωτερικές διαδικασίες. Σε αντίθεση με τις επιθέσεις phishing, όπου οι δράστες στοχεύουν στη μαζική συλλογή προσωπικών δεδομένων, το BEC συνήθως περιλαμβάνει είτε την παραβίαση ενός εταιρικού λογαριασμού email είτε τη χρήση λογαριασμών που μιμούνται έναν νόμιμο (π.χ., μέσω domain spoofing ή look-alike domains).

Η επίθεση BEC διαφέρει επίσης από το spear-phishing και το whaling, αν και μοιράζεται με αυτά κοινά χαρακτηριστικά, όπως η εξατομίκευση. Ειδικότερα:

- **Whaling:** Εστιάζει σε ανώτερα στελέχη (C-level executives) και στοχεύει στην υποκλοπή δεδομένων ή κεφαλαίων, με πιο στρατηγική στόχευση.
- **Spear-phishing:** Περιλαμβάνει την αποστολή κακόβουλων emails με τη μορφή στοχευμένων επιθέσεων, αλλά δεν απαιτεί απαραίτητα παραβίαση ή μίμηση ενός εταιρικού λογαριασμού email.
- **BEC:** Εστιάζει κυρίως στη χειραγώγηση κρίσιμων εταιρικών ρόλων (π.χ., οικονομικούς διευθυντές, λογιστήρια) με στόχο την πραγματοποίηση μη εξουσιοδοτημένων οικονομικών συναλλαγών. Αυτό επιτυγχάνεται μέσω της

παραβίασης εταιρικών emails ή της εξαπάτησης μέσω ψεύτικων emails που μοιάζουν πολύ με πραγματικά.

Οι επιτιθέμενοι στο BEC χρησιμοποιούν εξαιρετικά ακριβείς πληροφορίες για να δημιουργήσουν πειστικά σενάρια, όπως επείγουσες αιτήσεις μεταφοράς χρημάτων, παρακάμπτοντας τις τυπικές διαδικασίες ελέγχου. Οι στοχευμένες αυτές επιθέσεις συχνά οδηγούν σε σημαντικές οικονομικές απώλειες για τις επιχειρήσεις (Naz et al., 2024; Salahdine & Kaabouch, 2019; Tawalbeh & Muheidat, 2023; Tsinganos et al., 2024).

Εικόνα 8: Παραβίαση επιχειρηματικού ηλεκτρονικού ταχυδρομείου

Πηγή: (Gatefy, 2021)

Σύμφωνα με στοιχεία του FBI, τα σενάρια BEC μπορούν να κατηγοριοποιηθούν κυρίως με βάση την οντότητα που πλαστοπροσωπείται. Οι τέσσερις κύριες κατηγορίες είναι οι εξής (Gatefy, 2021):

1. *Πλαστοπροσωπία Διευθύνοντος Συμβούλου (CEO Fraud):*

   Σε αυτή την περίπτωση, ο εγκληματίας προσποιείται ότι είναι υψηλόβαθμο στέλεχος της επιχείρησης, όπως ο Διευθύνων Σύμβουλος (CEO) ή ο Οικονομικός Διευθυντής (CFO). Τα μηνύματα συχνά περιλαμβάνουν αιτήματα για επείγουσες χρηματοοικονομικές συναλλαγές, όπως τραπεζικά εμβάσματα. Αυτός ο τύπος απάτης, γνωστός και ως Πλαστοπροσωπία Στελέχους, μπορεί να οδηγήσει σε διάφορες επιπτώσεις, όπως η κλοπή χρημάτων μέσω τραπεζικών εμβασμάτων ή η διαρροή κρίσιμων πληροφοριών.

2. *Πλαστοπροσωπία Υπαλλήλου Εταιρείας (Employee Account Compromise):*

   Σε αυτό το σενάριο, ο εγκληματίας είτε αποκτά πρόσβαση στον λογαριασμό email ενός υπαλλήλου, είτε χρησιμοποιεί έναν ψεύτικο λογαριασμό που μιμείται τον πραγματικό

(π.χ. μέσω domain spoofing ή look-alike domains). Στην πρώτη περίπτωση, έχοντας πλήρη έλεγχο του λογαριασμού, μπορεί να στέλνει μηνύματα εκ μέρους του υπαλλήλου, εκμεταλλευόμενος την αξιοπιστία που συνδέεται με τον εταιρικό λογαριασμό. Στη δεύτερη περίπτωση, η απάτη βασίζεται στην οπτική ή δομική ομοιότητα του κακόβουλου email με ένα γνήσιο, παραπλανώντας τους παραλήπτες. Και στις δύο περιπτώσεις, οι επιπτώσεις περιλαμβάνουν την κλοπή χρημάτων ή την παραπλάνηση τρίτων (π.χ. πελάτες ή συνεργάτες).

3. *Πλαστοπροσωπία Προμηθευτή (Bogus Invoice Scheme):*

   Σε αυτή την περίπτωση, οι εγκληματίες παριστάνουν τους προμηθευτές της εταιρείας και ζητούν πληρωμές σε έναν νέο, δόλιο τραπεζικό λογαριασμό. Αυτή η απάτη είναι γνωστή και ως Απάτη Προμηθευτή ή Σχέδιο Τροποποίησης Τιμολογίου (Supplier Swindle and Invoice Modification Scheme). Το σενάριο αυτό συχνά περιλαμβάνει αποστολή πλαστών τιμολογίων ή αιτήματα αλλαγής στοιχείων πληρωμής, με αποτέλεσμα την οικονομική ζημία για τον οργανισμό.

4. *Πλαστοπροσωπία Δικηγόρου (Attorney Impersonation):*

   Σε αυτό το είδος απάτης, ο δράστης προσποιείται ότι είναι δικηγόρος και επικοινωνεί με το θύμα, συχνά ισχυριζόμενος ότι εκπροσωπεί έναν πελάτη που απειλεί με νομικές ενέργειες. Το μήνυμα συνήθως απαιτεί επείγουσα δράση, όπως πληρωμή χρημάτων για την αποφυγή μήνυσης ή εξωδικαστικού διακανονισμού. Η πίεση του επείγοντος και η αποφυγή δημοσιότητας καθιστούν τα θύματα ευάλωτα σε αυτό το είδος απάτης.

3.2.1.3. Κακόβουλο Λογισμικό

Η ανιχνευσιμότητα του κακόβουλου λογισμικού (malware) διαφέρει σημαντικά ανάλογα με τον τύπο του. Τα παραδοσιακά κακόβουλα προγράμματα, όπως οι ιοί (viruses), είναι σχετικά εύκολο να ανιχνευθούν με τα σύγχρονα αντιϊικά προγράμματα. Ωστόσο, προηγμένα είδη malware, όπως οι πολυμορφικοί ιοί (polymorphic viruses), που μεταλλάσσονται για να αποφύγουν την ανίχνευση, καθώς και οι επιθέσεις τύπου zero-day, οι οποίες εκμεταλλεύονται ευπάθειες που δεν έχουν ακόμα εντοπιστεί ή αναφερθεί από τους προγραμματιστές, είναι εξαιρετικά δύσκολο να εντοπιστούν. Αυτές οι επιθέσεις συνήθως περνούν απαρατήρητες για μεγάλα χρονικά διαστήματα, καθιστώντας τη συστηματική και διαρκή παρακολούθηση του δικτύου και των συστημάτων ζωτικής σημασίας για την ανακάλυψη τέτοιων απειλών.

3.2.1.3.1. Scareware

Η επίθεση Scareware (λογισμικό εκφοβισμού) αποτελεί μια τεχνική κοινωνικής μηχανικής που χρησιμοποιεί τακτικές εκφοβισμού και παραπλάνησης, με στόχο να πείσει τους χρήστες ότι οι συσκευές τους έχουν μολυνθεί από κακόβουλο λογισμικό ή ότι αντιμετωπίζουν σοβαρά προβλήματα ασφαλείας. Στόχος είναι να ωθήσει τα θύματα είτε να εγκαταστήσουν (ενδεχομένως μετά από αγορά) ψεύτικο λογισμικό ασφαλείας είτε να αποκαλύψουν ευαίσθητες πληροφορίες (Aun et al., 2023; Nanda & De, 2022; Zaoui et al., 2024).

Οι επιθέσεις Scareware εκδηλώνονται κυρίως μέσω ψεύτικων αναδυόμενων παραθύρων (pop-up windows) ή ειδοποιήσεων που εμφανίζονται κατά την περιήγηση στο διαδίκτυο, όπως παρουσιάζεται στην παρακάτω εικόνα. Αυτές οι ειδοποιήσεις προέρχονται από μολυσμένους ή κακόβουλους ιστότοπους, οι οποίοι έχουν σχεδιαστεί για να τρομάξουν τους χρήστες, εμφανίζοντας προειδοποιήσεις για υποτιθέμενες μολύνσεις από ιούς, καταστροφή δίσκων ή άλλα σοβαρά προβλήματα ασφαλείας (Syafitri et al., 2022). Συχνά, οι επιτιθέμενοι εκμεταλλεύονται την αυξημένη ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια, χρησιμοποιώντας τεχνικές που προκαλούν άγχος, φόβο και πανικό (Udochukwu & Bode-Asa, 2023).

Εικόνα 9: Παράδειγμα λογισμικού εκφοβισμού

Πηγή: (Lee, 2024)

Σε πολλές περιπτώσεις, οι χρήστες παροτρύνονται να κατεβάσουν και να εγκαταστήσουν ψεύτικο λογισμικό ασφαλείας, το οποίο υποτίθεται ότι επιλύει τα προβλήματα. Αυτό το λογισμικό μπορεί (Federal Trade Commission, 2008, 2012):

- Να είναι εντελώς άχρηστο, με τους επιτιθέμενους να ζητούν πληρωμή για την εκφόρτωση και εγκατάσταση της "πλήρους έκδοσης" του λογισμικού, αποσπώντας έτσι οικονομικά οφέλη.
- Να είναι κακόβουλο, δίνοντας στον επιτιθέμενο πρόσβαση στη συσκευή του χρήστη για περαιτέρω εκμετάλλευση.

Μέθοδοι Διανομής Scareware

Οι επιθέσεις Scareware βασίζονται σε διάφορους τρόπους διανομής και διάδοσης, οι οποίοι συχνά περιλαμβάνουν:

- *Μολυσμένες διαφημίσεις (malvertising)*: Οι επιτιθέμενοι ενσωματώνουν κακόβουλο κώδικα σε διαδικτυακές διαφημίσεις που προβάλλονται σε δημοφιλείς ιστοτόπους. Αυτές οι διαφημίσεις ενεργοποιούν την εμφάνιση ψεύτικων ειδοποιήσεων όταν ο χρήστης τις δει ή τις πατήσει.
- *Κακόβουλους ιστότοπους ή ιστοσελίδες*: Οι επιτιθέμενοι δημιουργούν ιστότοπους που προσομοιάζουν με αξιόπιστες πηγές (π.χ. εταιρείες λογισμικού ασφαλείας) και εμφανίζουν τρομακτικά μηνύματα.
- *Αποτελέσματα αναζήτησης εικόνων*: Ορισμένοι επιτιθέμενοι εκμεταλλεύονται τις μηχανές αναζήτησης, προσπαθώντας να εμφανίσουν ψεύτικες σελίδες ή μολυσμένες εικόνες στα αποτελέσματα. Όταν ο χρήστης πατήσει πάνω στην εικόνα ή τον σύνδεσμο, μεταφέρεται σε κακόβουλη σελίδα όπου εμφανίζονται scareware ειδοποιήσεις.

Οι επιτιθέμενοι συχνά καταφέρνουν να κάνουν τις ειδοποιήσεις να φαίνονται αυθεντικές, μιμούμενοι την εμφάνιση και το λεκτικό ύφος αξιόπιστων οργανισμών ή εταιρειών κυβερνοασφάλειας (Zaoui et al., 2024).

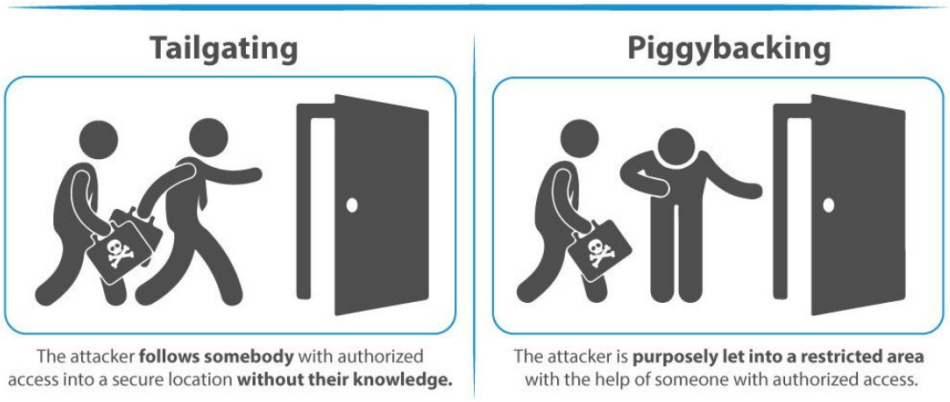
3.2.2. Επιθέσεις Βασισμένες σε Φυσική Αλληλεπίδραση

Οι επιθέσεις που βασίζονται στη φυσική αλληλεπίδραση περιλαμβάνουν χειρισμούς στον φυσικό κόσμο, όπως η εισαγωγή μη εξουσιοδοτημένων ατόμων σε ελεγχόμενους χώρους ή η κλοπή πληροφοριών από φυσικά αντικείμενα.

3.2.2.1. Tailgating & Piggybacking

Οι επιθέσεις Tailgating (παραβίαση ασφαλείας με ακολούθηση) και Piggybacking (συνεργατική είσοδος) είναι δύο παρόμοιες τεχνικές κοινωνικής μηχανικής (δείτε Εικόνα 10) που επιτρέπουν σε έναν επιτιθέμενο να αποκτήσει μη εξουσιοδοτημένη φυσική πρόσβαση σε έναν περιορισμένο χώρο ή σύστημα, ακολουθώντας στενά ένα εξουσιοδοτημένο άτομο και

εκμεταλλευόμενος την ανθρώπινη τάση για ευγένεια και αποφυγή αντιπαράθεσης. Στην πρώτη περίπτωση ο επιτιθέμενος εκμεταλλεύεται το διάστημα κατά το οποίο η πόρτα παραμένει ανοιχτή καθώς διέρχεται ο προπορευόμενός του ενώ στη δεύτερη περίπτωση υπάρχει μια πιο «συνεργατική» διάσταση, όπου ο επιτιθέμενος μπορεί να ζητήσει ή να πάρει την άδεια του ατόμου που προπορεύεται για να εισέλθει και ο ίδιος στον χώρο (Edwards et al., 2024; Kalajžić, 2019; Salahdine & Kaabouch, 2019).



Εικόνα 10: Παραβίαση ασφαλείας με ακολούθηση

Πηγή: (Keepnet, 2024)

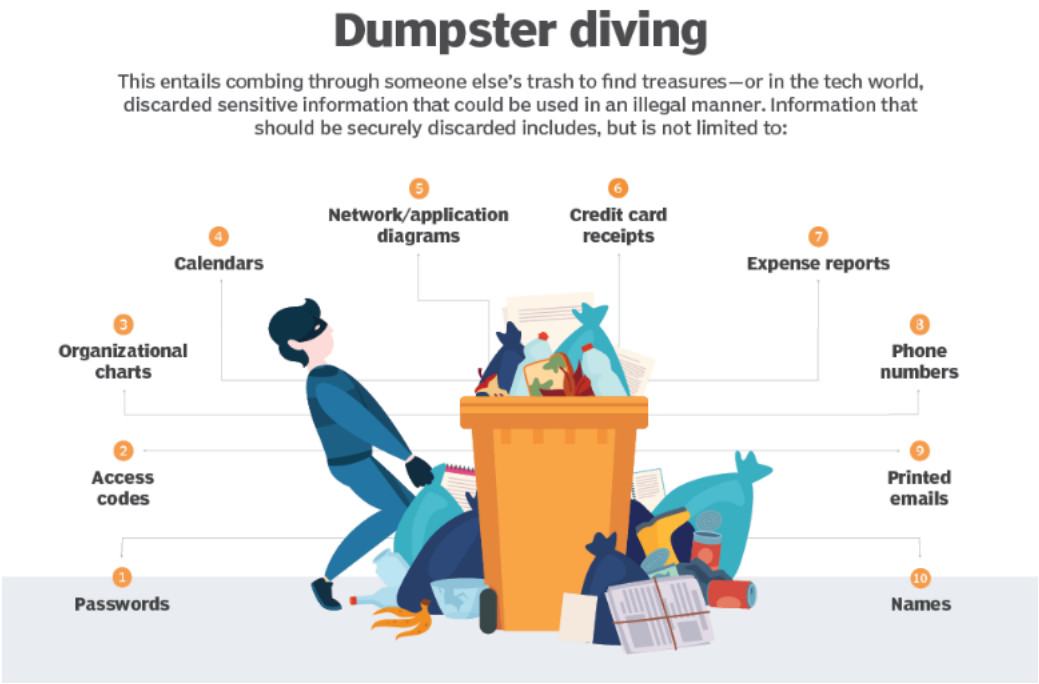
Ο επιτιθέμενος μπορεί επίσης να υποδυθεί κάποιον με νόμιμη πρόσβαση, όπως έναν υπάλληλο παράδοσης (αγαθών) ή τεχνικό (Edwards et al., 2024). Οι επιθέσεις αυτού του τύπου στοχεύουν συνήθως σε περιοχές με περιορισμένη (φυσική) πρόσβαση που απαιτούν κάποια μορφή ελέγχου ταυτότητας, όπως κάρτες αναγνώρισης ή κάρτες RFID (Kalajžić, 2019). Ο απώτερος στόχος είναι η απόκτηση πρόσβασης σε ευαίσθητα δεδομένα, χρήματα ή άλλους πολύτιμους πόρους (Edwards et al., 2024).

Η επιτυχία αυτής της επίθεσης βασίζεται στην εκμετάλλευση των ανθρώπινων τάσεων, όπως η ευγένεια, η αποφυγή αντιπαράθεσης και η απροθυμία αμφισβήτησης κάποιου που φαίνεται να ανήκει στον χώρο. Οι επιτιθέμενοι συχνά χρησιμοποιούν τεχνικές κοινωνικής μηχανικής, όπως η αυτοπεποίθηση, μια καλή ιστορία και μικρή συζήτηση για να πείσουν τα θύματά τους (Chetiouia et al., 2021). Ωστόσο, οι τεχνικές αυτές είναι εύκολα ανιχνεύσιμες αφού ο επιτιθέμενος μπορεί να εντοπιστεί γρήγορα μέσω καμερών ασφαλείας και συστημάτων ελέγχου πρόσβασης.

3.2.2.2. Dumpster Diving

Η αναζήτηση σε κάδους απορριμμάτων (Dumpster Diving) είναι μια τεχνική κοινωνικής μηχανικής κατά την οποία ο επιτιθέμενος αναζητά και συλλέγει ευαίσθητες πληροφορίες από

τα απορρίμματα ή τα απορριφθέντα υλικά ενός ατόμου ή οργανισμού, με σκοπό να τις χρησιμοποιήσει για κακόβουλους σκοπούς. Το dumpster diving αποτελεί μια σημαντική μέθοδο συλλογής πληροφοριών για τους κοινωνικούς μηχανικούς και τους hackers. Μέσω αυτής της τεχνικής, οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα χωρίς να απαιτείται άμεση επαφή με τους εργαζόμενους του στόχου. Τα είδη των πληροφοριών (δείτε Εικόνα 11) που μπορούν να ανακτηθούν περιλαμβάνουν τηλεφωνικούς καταλόγους, οργανογράμματα, υπομνήματα, εγχειρίδια πολιτικής, ημερολόγια συναντήσεων, εκτυπώσεις ευαίσθητων δεδομένων, ονόματα χρηστών και κωδικούς πρόσβασης, πηγαίο κώδικα, δίσκους και ταινίες, επιστολόχαρτα και φόρμες υπομνημάτων της εταιρείας (Greavu-Serban & Serban, 2014).



Εικόνα 11: Αναζήτηση σε κάδους απορριμμάτων

Πηγή: (Wright, 2024)

Η τεχνική του Dumpster Diving περιλαμβάνει την αναζήτηση χρήσιμων πληροφοριών σε απορρίμματα και έχει επεκταθεί από τον φυσικό κόσμο στον ψηφιακό. Στον φυσικό κόσμο, οι επιτιθέμενοι συχνά αναζητούν έγγραφα, αποδείξεις ή άλλα αντικείμενα που απορρίπτονται, αλλά μπορεί να περιέχουν ευαίσθητες πληροφορίες. Στον ψηφιακό κόσμο, η πρακτική αυτή έχει εξελιχθεί σε αναζήτηση πληροφοριών σε ψηφιακούς "κάδους απορριμμάτων", όπως φάκελοι "απορριμμάτων" ή "ανακύκλωσης" σε σκληρούς δίσκους, καθώς και δεδομένα που παραμένουν προσωρινά αποθηκευμένα στη μνήμη μηχανών αναζήτησης (Gehl & Lawson, 2022).

Οι "ψηφιακοί κάδοι απορριμμάτων" συχνά αναφέρονται σε δεδομένα που παραμένουν διαθέσιμα σε:

- *Διαμοιραζόμενα συστήματα*: Όπου χρήστες μπορεί να μοιράζονται προσωρινά ή μόνιμα κοινή πρόσβαση σε αποθηκευτικούς χώρους (π.χ., δημόσια υπολογιστικά νέφη, διαμοιραζόμενοι δίσκοι).
- *Συστήματα που έχουν παραβιαστεί*: Όπου ο επιτιθέμενος έχει ήδη διεισδύσει, αποκτώντας πρόσβαση σε φακέλους "ανακύκλωσης" ή σε άλλες πηγές προσωρινής αποθήκευσης δεδομένων.

Η αποτελεσματικότητα του dumpster diving οφείλεται στο γεγονός ότι οι περισσότεροι άνθρωποι υποθέτουν ότι κανείς δεν θα ψάξει εκούσια στα φυσικά ή ψηφιακά σκουπίδια τους και έτσι τείνουν να πετούν δυνητικά πολύτιμες πληροφορίες (Kalajžić, 2019). Αυτό καθιστά τη μέθοδο ιδιαίτερα επικίνδυνη, καθώς οι επιτιθέμενοι μπορούν να συλλέξουν σημαντικές πληροφορίες για την οργάνωση και τη λειτουργία ενός οργανισμού, τις οποίες μπορούν στη συνέχεια να χρησιμοποιήσουν για πιο στοχευμένες επιθέσεις (Hasan et al., 2010).

Είναι σημαντικό να σημειωθεί ότι η αναζήτηση σε κάδους απορριμμάτων παραμένει μια δημοφιλής τεχνική ακόμη και στη σύγχρονη εποχή. Επαγγελματίες κοινωνικοί μηχανικοί, όπως ο Chris Hadnagy και η Sharon Conheady, έχουν συμπεριλάβει οδηγίες για το dumpster diving στα βιβλία τους ως μέρος των δοκιμών διείσδυσης (penetration testing) (Gehl & Lawson, 2022). Επιπλέον, υπάρχουν πολλοί οδηγοί βίντεο για την πρακτική αυτή στο YouTube, υποδεικνύοντας τη συνεχιζόμενη σημασία και χρήση της.

Η ανιχνευσιμότητα αυτών των επιθέσεων εξαρτάται από την παρουσία του επιτιθέμενου και το περιβάλλον στο οποίο πραγματοποιείται η επίθεση. Σε περιβάλλοντα όπου υπάρχουν κάμερες ασφαλείας ή περιπολίες, η ανίχνευση τέτοιων επιθέσεων είναι συνήθως μέτρια προς υψηλή. Ωστόσο, όταν αυτές οι επιθέσεις πραγματοποιούνται εκτός ωρών λειτουργίας ή σε απομακρυσμένες περιοχές, η ανίχνευση μπορεί να είναι πιο δύσκολη.

3.2.2.3. Shoulder Surfing

Το σερφάρισμα πάνω από τον ώμο (Shoulder Surfing) είναι μια τεχνική κοινωνικής μηχανικής και φυσικής παρατήρησης, κατά την οποία ο επιτιθέμενος παρακολουθεί κρυφά τις ενέργειες του θύματος σε μια ηλεκτρονική συσκευή, με σκοπό την θέαση και επακόλουθη απόκτηση ευαίσθητων πληροφοριών, όπως κωδικοί πρόσβασης, PIN ή άλλα εμπιστευτικά δεδομένα (δείτε Εικόνα 12).

Τονίζεται πως το shoulder surfing δεν απαιτεί απαραίτητα κάποια προηγούμενη σχέση ή οικειότητα μεταξύ του θύτη και του θύματος. Ειδικότερα, ένας επιτιθέμενος μπορεί να

παρατηρεί το θύμα χωρίς να έχει καμία αλληλεπίδραση μαζί του, απλά εκμεταλλευόμενος την κατάσταση ή το περιβάλλον. Για παράδειγμα, σε δημόσιους χώρους, όπως στα μέσα μαζικής μεταφοράς ή σε ουρές, ο θύτης μπορεί να έχει άμεση οπτική πρόσβαση στη συσκευή του θύματος, αποκτώντας έτσι πληροφορίες χωρίς καμία προειδοποίηση (Adu-Manu et al., 2023; Kalajžić, 2019; Krombholz et al., 2015; Zaoui et al., 2024).

Εικόνα 12: Σερφάρισμα πάνω από τον ώμο

Πηγή: (InfosecTrain, 2018)

Το shoulder surfing είναι μια ευρέως διαδεδομένη τεχνική κοινωνικής μηχανικής που βασίζεται στην άμεση φυσική παρατήρηση (Krombholz et al., 2015). Συνήθως πραγματοποιείται σε πολυσύχναστους δημόσιους χώρους, όπως αεροδρόμια, καφετέριες και εμπορικά κέντρα, όπου οι επιτιθέμενοι μπορούν εύκολα να παρακολουθήσουν τις οθόνες ή τα πληκτρολόγια των θυμάτων χωρίς να γίνουν αντιληπτοί (Kalajžić, 2019; Krombholz et al., 2015). Η επίθεση μπορεί να πραγματοποιηθεί με απλή οπτική παρατήρηση ή με τη χρήση εξοπλισμού, όπως κιάλια ή κάμερες, για την καταγραφή ευαίσθητων πληροφοριών.

Η αποτελεσματικότητα του shoulder surfing έχει αυξηθεί σημαντικά με την εξάπλωση των φορητών συσκευών και των οθονών αφής. Έρευνες δείχνουν ότι η επίθεση μπορεί να είναι επιτυχής έως και στο 97,07% των περιπτώσεων σε συσκευές με πληκτρολόγια αφής (Adu-Manu et al., 2023). Οι χρήστες συχνά χρησιμοποιούν τέτοιες συσκευές για πρόσβαση σε

ευαίσθητες πληροφορίες, όπως τραπεζικούς λογαριασμούς ή επαγγελματικά email σε δημόσιους χώρους, αυξάνοντας τον κίνδυνο έκθεσης (Adu-Manu et al., 2023).

Θα πρέπει να σημειωθεί, ωστόσο, ότι το shoulder surfing έχει υψηλή ανιχνευσιμότητα, καθώς η φυσική παρουσία του επιτιθέμενου είναι εύκολο να εντοπιστεί σε ελεγχόμενα περιβάλλοντα.

3.2.3. Επιθέσεις Βασισμένες σε Ψυχολογική Χειραγώγηση

Η ψυχολογική χειραγώγηση αποτελεί τον πυρήνα πολλών επιθέσεων κοινωνικής μηχανικής. Αυτές οι τεχνικές εκμεταλλεύονται ανθρώπινα συναισθήματα και συμπεριφορές, όπως την περιέργεια, τον φόβο, την απληστία ή τη προθυμία για βοήθεια. Στην υποενότητα αυτή, θα εξεταστούν λεπτομερώς σχετικές μέθοδοι, όπως το pretexting, το baiting και το quid pro quo, αναλύοντας πώς οι επιτιθέμενοι χρησιμοποιούν αυτές τις τεχνικές για να παραπλανήσουν τα θύματά τους και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες ή συστήματα.

3.2.3.1. Pretexting

Η επίθεση προσποίησης (Pretexting) (δείτε Εικόνα 14) είναι μια τεχνική κοινωνικής μηχανικής όπου ο επιτιθέμενος δημιουργεί μια πειστική ιστορία (pretext) ή σενάριο με σκοπό να αποκτήσει εμπιστοσύνη και να εξαπατήσει το θύμα ώστε να αποκαλύψει ευαίσθητες πληροφορίες ή να εκτελέσει ενέργειες που θέτουν σε κίνδυνο την ασφάλεια (Salahdine & Kaabouch, 2019; Kalajžić, 2019). Ο επιτιθέμενος συνήθως υποδύεται κάποιο άτομο εξουσίας ή αξιόπιστη οντότητα, όπως έναν συνάδελφο, αστυνομικό, υπάλληλο τράπεζας ή εφορίας (Zaoui et al., 2024; Tsinganos et al., 2024; Syafitri et al., 2022).

Εικόνα 13: Επίθεση προσποίησης

Πηγή: (NBKomputer, 2024)

Σε μια επίθεση προσποίησης προκειμένου αυτό να είναι πειστικό, απαιτείται προσεκτικός σχεδιασμός και έρευνα για το θύμα εκ των προτέρων (Salahdine & Kaabouch, 2019; Conheady, 2014). Ο επιτιθέμενος συγκεντρώνει πληροφορίες από δημόσιες πηγές όπως ιστοσελίδες, μέσα κοινωνικής δικτύωσης και τηλεφωνικούς καταλόγους (Abdulla et al., 2023). Αυτό του επιτρέπει να δημιουργήσει ένα αληθοφανές σενάριο που αφήνει ελάχιστα περιθώρια αμφιβολίας στο θύμα (Chetiouia et al., 2021).

Η επίθεση μπορεί να πραγματοποιηθεί μέσω διαφόρων καναλιών επικοινωνίας, όπως τηλεφωνικές κλήσεις, email ή ακόμα και με φυσική παρουσία (Kalajžić, 2019; Zaoui et al., 2024; Aun et al., 2023). Ο σκοπός είναι ο επιτιθέμενος να αποσπάσει από το θύμα ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, οικονομικά δεδομένα ή προσωπικά στοιχεία (Tsinganos et al., 2024; Syafitri et al., 2022). Σε ορισμένες περιπτώσεις, ο επιτιθέμενος μπορεί να επιδιώκει και φυσική πρόσβαση σε εγκαταστάσεις του οργανισμού-στόχου (Adu-Manu et al., 2023).

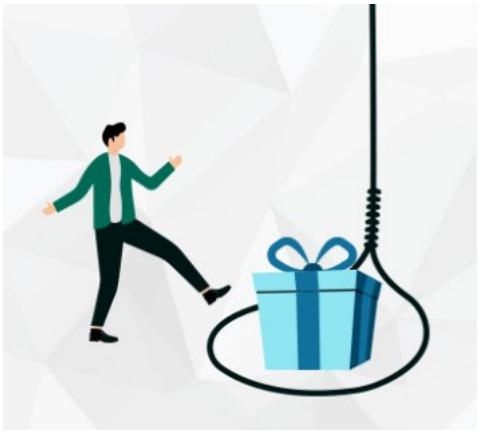
Σε αντίθεση με άλλες τεχνικές κοινωνικής μηχανικής που βασίζονται στο φόβο ή την αίσθηση του επείγοντος, το pretexting εκμεταλλεύεται την ανθρώπινη τάση να εμπιστευόμαστε και να βοηθάμε τους άλλους (Khan, 2023). Ο επιτιθέμενος χτίζει σταδιακά μια σχέση εμπιστοσύνης με το θύμα, κάνοντας δυσκολότερο τον εντοπισμό της απάτης (Nanda & De, 2022).

Αυτού του είδους η επίθεση θεωρείται μια από τις πιο προηγμένες και απαιτητικές τεχνικές κοινωνικής μηχανικής, καθώς συνδυάζει την εκμετάλλευση κοινωνικών δομών και στερεοτύπων με ιδιαίτερες δεξιότητες χειραγώγησης και υποκριτικής από τον επιτιθέμενο (Alsufyani & Alzahrani, 2020). Ένας από τους πιο διάσημους κοινωνικούς μηχανικούς που χρησιμοποίησε εκτενώς αυτή την τεχνική ήταν ο Kevin Mitnick (Salim, 2024). Η επιτυχία του Mitnick βασιζόταν στην ικανότητά του να αναγνωρίζει και να εκμεταλλεύεται ευάλωτα σημεία στις ανθρώπινες αλληλεπιδράσεις και τις κοινωνικές δομές, ενώ παράλληλα χρησιμοποιούσε δεξιότητες που απαιτούν υψηλή ψυχολογική ευφυΐα και προσαρμοστικότητα (Gehl & Lawson, 2022). Η ανιχνευσιμότητα της επίθεσης pretexting κυμαίνεται από χαμηλή προς μέτρια, καθώς εξαρτάται από την ικανότητα του επιτιθέμενου να κατασκευάσει μια αξιόπιστη ιστορία και από την προσοχή των θυμάτων.

3.2.3.2. Baiting

Το baiting (δελεασμός) (δείτε Εικόνα 14) είναι μια τεχνική κοινωνικής μηχανικής όπου ο επιτιθέμενος χρησιμοποιεί ένα δέλεαρ για να παρασύρει το θύμα σε μια παγίδα με σκοπό την κλοπή ευαίσθητων πληροφοριών ή τη μόλυνση των συστημάτων του με κακόβουλο λογισμικό.

Το δέλεαρ σχεδιάζεται ώστε να είναι ελκυστικό και χειριστικό, εκμεταλλευόμενο την περιέργεια ή τις επιθυμίες των ανθρώπων. Για παράδειγμα, ένας επιτιθέμενος μπορεί να δημιουργήσει ψεύτικες εφαρμογές που προσφέρουν δωρεάν λειτουργίες, αλλά στην πραγματικότητα εγκαθιστούν κακόβουλο λογισμικό. Επιπλέον, μπορεί να αφήσει ένα USB (Universal Serial Bus) (Σειριακός Δίαυλος Γενικής Χρήσης) stick σε δημόσιους χώρους, το οποίο φέρει σήματα γνωστών λογότυπων ή επωνυμιών, προσελκύοντας το θύμα να το συνδέσει στον υπολογιστή του ή σε άλλα ψηφιακά μέσα, μολύνοντας με αυτό τον τρόπο τα συστήματά του. Άλλες περιπτώσεις περιλαμβάνουν δωρεάν προσφορές ή διαγωνισμούς που απαιτούν την εισαγωγή προσωπικών στοιχείων, καθώς και ψεύτικες ιστοσελίδες που μιμούνται νόμιμες υπηρεσίες, παρασύροντας τα θύματα να αποκαλύψουν ευαίσθητες πληροφορίες. (Chinta et al, 2016; Edwards et al., 2024).



Εικόνα 14:Δελεασμός

Πηγή: (Terranovasecurity, 2024)

Το baiting μπορεί να πραγματοποιηθεί τόσο σε φυσικό όσο και σε ψηφιακό περιβάλλον. Στο φυσικό περιβάλλον, οι επιτιθέμενοι συχνά χρησιμοποιούν μολυσμένα αποθηκευτικά μέσα, όπως USB sticks ή CD, τα οποία αφήνουν σε δημόσιους χώρους για να βρεθούν από τα θύματα (Salahdine & Kaabouch, 2019). Όταν τα θύματα συνδέουν αυτές τις συσκευές στους υπολογιστές τους, ενεργοποιείται το κακόβουλο λογισμικό χωρίς αυτό να γίνεται αντιληπτό (Hobel et al., 2014).

Στο ψηφιακό περιβάλλον, οι τεχνικές baiting αξιοποιούν ελκυστικές προσφορές, όπως δωρεάν λήψεις μουσικής, ταινιών ή εφαρμογών, για να προσελκύσουν πιθανά θύματα (Chetiouia et al., 2021). Σε ορισμένες περιπτώσεις, οι διαφημίσεις αυτές μπορεί να περιέχουν ή να προωθούν κακόβουλο λογισμικό. Το θύμα πείθεται να κατεβάσει και να εγκαταστήσει το κακόβουλο λογισμικό, επιδιώκοντας να ικανοποιήσει τις ψυχαγωγικές του ανάγκες, χωρίς να γνωρίζει τους κινδύνους που διατρέχει. Συχνά, οι ιστότοποι αυτοί ζητούν προσωπικές

πληροφορίες ή περιέχουν λογισμικό που μολύνει τον υπολογιστή του χρήστη κατά τη λήψη (Nanda & De, 2022).

Οι επιθέσεις baiting εκμεταλλεύονται ανθρώπινες αδυναμίες, όπως η περιέργεια, η απληστία ή η επιθυμία για δωρεάν προϊόντα/υπηρεσίες. Οι επιτιθέμενοι συχνά προσαρμόζουν το δέλεαρ στα ενδιαφέροντα του στόχου για να αυξήσουν την πιθανότητα επιτυχίας (Udochukwu & Bode-Asa, 2023). Για παράδειγμα, μπορεί να χρησιμοποιηθούν USB sticks με εταιρικά λογότυπα ή αρχεία με ονόματα όπως "Μισθοί Υπαλλήλων" για να προσελκύσουν την προσοχή συγκεκριμένων θυμάτων (Khan, 2023). Από την άλλη, η ανιχνευσιμότητα των επιθέσεων τύπου baiting είναι μέτρια, καθώς τα φυσικά μέσα (π.χ. USB sticks) μπορεί να εντοπιστούν μέσω καμερών ασφαλείας ή από την αναφορά προσωπικού, ενώ τα ψηφιακά baiting (όπως κακόβουλοι σύνδεσμοι ή προσφορές) μπορούν να ανιχνευθούν από συστήματα ασφαλείας δικτύου και προστασίας τελικών σημείων.

3.3.2.2.1 Επιθέσεις Baiting Αυξημένης Πολυπλοκότητας

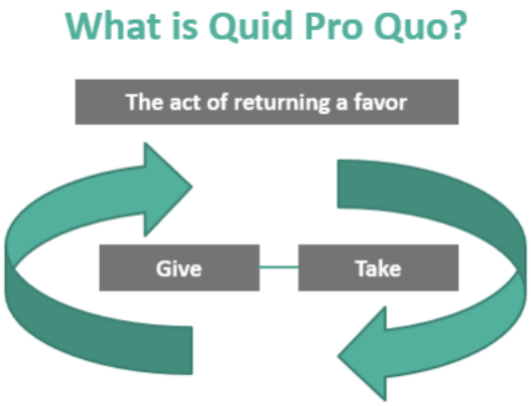
Πέρα από τις συμβατικές τεχνικές baiting, έχουν καταγραφεί περιπτώσεις επιθέσεων baiting αυξημένης πολυπλοκότητας. Χαρακτηριστικό παράδειγμα αποτελεί η επίθεση CANDY (CAN: Controller Area Network), η οποία, σύμφωνα με τους Salahdine και Kaabouch (2019), στοχεύει τα συστήματα infotainment των σύγχρονων οχημάτων.

Η συγκεκριμένη επίθεση εκμεταλλεύεται τη διασύνδεση των συστημάτων infotainment με το Controller Area Network (CAN) του οχήματος, το οποίο διαχειρίζεται την επικοινωνία μεταξύ των ηλεκτρονικών μονάδων του. Η διείσδυση στο σύστημα επιτυγχάνεται μέσω ειδικά διαμορφωμένων USB συσκευών ή κακόβουλων εφαρμογών, επιτρέποντας την εγκατάσταση κακόβουλου λογισμικού. Αυτό παρέχει στον επιτιθέμενο τη δυνατότητα απομακρυσμένου ελέγχου του οχήματος, συλλογής προσωπικών δεδομένων, όπως το ιστορικό πλοήγησης, και χειρισμού διαφόρων λειτουργιών, συμπεριλαμβανομένου του συστήματος κλειδώματος και φωτισμού.

Ένα τυπικό σενάριο εκτέλεσης της επίθεσης περιλαμβάνει την τοποθέτηση ενός μολυσμένου USB stick σε στρατηγικά σημεία, όπως χώροι στάθμευσης ή περιοχές πλησίον του οχήματος-στόχου. Το μέσο συνήθως φέρει ελκυστικές επιγραφές όπως "Αναβάθμιση" ή "Εμπιστευτικό". Η σύνδεση της συσκευής στο σύστημα infotainment από το ανυποψίαστο θύμα πυροδοτεί την αυτόματη εγκατάσταση του κακόβουλου λογισμικού στο δίκτυο CAN, παρέχοντας στον επιτιθέμενο πλήρη απομακρυσμένο έλεγχο του οχήματος.

3.2.3.3. Quid Pro Quo

Η επίθεση quid pro quo (αντίκρισμα) (δείτε Εικόνα 15) είναι μια τεχνική κοινωνικής μηχανικής όπου ο επιτιθέμενος προσφέρει μια υπηρεσία ή όφελος με αντάλλαγμα ευαίσθητες πληροφορίες ή παροχή πρόσβασης από το θύμα. Ο όρος προέρχεται από τη λατινική φράση που σημαίνει "κάτι για κάτι" ή "αυτό για εκείνο" (Zaoui et al., 2024). Συνήθως ο επιτιθέμενος προσποιείται έναν ειδικό πληροφορικής ή εκπρόσωπο τεχνικής υποστήριξης, με στόχο την απόκτηση ευαίσθητων δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού.



Εικόνα 15: Αντίκρισμα

Πηγή: (Jayachandran, 2024)

Η επίθεση Quid Pro Quo συνήθως περιλαμβάνει έναν επιτιθέμενο που προσποιείται ότι είναι ένας ειδικός πληροφορικής ή εκπρόσωπος τεχνικής υποστήριξης, προσφέροντας βοήθεια σε ένα θύμα που αντιμετωπίζει τεχνικά προβλήματα (Salahdine & Kaabouch, 2019). Ο στόχος του επιτιθέμενου είναι να εγκαταστήσει κακόβουλο λογισμικό στο σύστημα του χρήστη ή να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης (Breda et al., 2020; Alsufyani & Alzahrani, 2020).

Αυτός ο τύπος επίθεσης εκμεταλλεύεται την επιθυμία των ατόμων για βοήθεια ή ευκολία, ιδιαίτερα όταν αντιμετωπίζουν τεχνικά προβλήματα (Jamuna, 2024). Οι επιθέσεις αυτές συχνά στοχεύουν άτομα με περιορισμένες τεχνολογικές γνώσεις, εκμεταλλευόμενοι ανθρώπινους παράγοντες, όπως η περιέργεια και το άγχος (Aun et al., 2023). Για παράδειγμα, οι τελικοί χρήστες είναι πιο πιθανό να συμμορφωθούν με αιτήματα υποστήριξης πληροφορικής όταν αντιμετωπίζουν τεχνικά ζητήματα και να παραδώσουν διαπιστευτήρια ελεύθερα για γρήγορες λύσεις (Aun et al., 2023). Η αύξηση της απομακρυσμένης εργασίας έχει δημιουργήσει νέες ευκαιρίες για αυτόν τον τύπο επίθεσης, καθώς οι εργαζόμενοι μπορεί να είναι πιο ευάλωτοι σε αιτήματα απομακρυσμένης πρόσβασης ή τεχνικής υποστήριξης (Aun et al., 2023). Η ανιχνευσιμότητα της επίθεσης κυμαίνεται από μέτρια προς χαμηλή, καθώς

συχνά περιλαμβάνει αθώα και καθημερινά αιτήματα, που φαίνονται φυσιολογικά, κάνοντάς την δύσκολη να εντοπιστεί.

3.2.3.4. Honey Trap

Η επίθεση Honey Trap (παγίδα μελιού) είναι μια τεχνική κοινωνικής μηχανικής που χρησιμοποιούν οι κακόβουλοι χρήστες για να παραπλανήσουν και να εκμεταλλευτούν τα θύματά τους, συνήθως μέσω της δημιουργίας ψεύτικων διαδικτυακών ταυτοτήτων ή προφίλ με σκοπό την απόσπαση ευαίσθητων πληροφοριών ή την εγκατάσταση κακόβουλου λογισμικού. Η επίθεση αυτή βασίζεται στην εκμετάλλευση της ανθρώπινης ψυχολογίας και της ανάγκης για κοινωνική σύνδεση και εμπιστοσύνη. Οι επιτιθέμενοι δημιουργούν πειστικές ψεύτικες περσόνες, χρησιμοποιώντας πληροφορίες από τα μέσα κοινωνικής δικτύωσης ή άλλες πηγές, για να προσεγγίσουν συγκεκριμένους στόχους. Αφού κερδίσουν την εμπιστοσύνη του θύματος, προχωρούν στην εξαγωγή ευαίσθητων πληροφοριών ή πείθουν το θύμα να κατεβάσει κακόβουλο λογισμικό (NIELIT Patna, 2024).

Η ειδοποιός διαφορά ανάμεσα σε αυτή τη μέθοδο και το pretexting έγκειται στη φύση της προσέγγισης. Συγκεκριμένα, το pretexting βασίζεται σε μια ψεύτικη επαγγελματική ή επίσημη ταυτότητα, ενώ η παγίδα μελιού εστιάζει κυρίως, αλλά όχι αποκλειστικά, σε μια προσωπική και συναισθηματική προσέγγιση. Στο Pretexting, η εξαπάτηση επιτυγχάνεται μέσω επαγγελματικής εμπιστοσύνης, ενώ στο Honey Trap κυρίως μέσω συναισθηματικού δεσίματος (Fortinet, 2024c).

Οι επιθέσεις honey trap εμφανίζονται σε διάφορες μορφές:

1. *Ψεύτικα προφίλ σε μέσα κοινωνικής δικτύωσης*: Οι επιτιθέμενοι δημιουργούν ελκυστικά προφίλ χρησιμοποιώντας κλεμμένες φωτογραφίες και πλαστά στοιχεία. Στοχεύουν στη δημιουργία φιλικών ή ρομαντικών σχέσεων για να αποσπάσουν προσωπικές πληροφορίες ή χρήματα.
2. *Απάτες σε ιστοσελίδες γνωριμιών*: Αποτελούν μια εξειδικευμένη μορφή honey trap, γνωστή ως romance scams (αισθηματικές απάτες). Αυτές οι απάτες εστιάζουν αποκλειστικά στη αισθηματική εξαπάτηση, συνήθως με οικονομικό κίνητρο. Οι δράστες δημιουργούν πειστικά προφίλ και αφιερώνουν σημαντικό χρόνο στην οικοδόμηση εμπιστοσύνης πριν ζητήσουν χρήματα για υποτιθέμενες έκτακτες ανάγκες (ftc.gov, 2022).
3. *Ψεύτικες προσφορές εργασίας*: Οι επιτιθέμενοι δημιουργούν ελκυστικές αγγελίες εργασίας για να συλλέξουν προσωπικά δεδομένα μέσω βιογραφικών ή να

εγκαταστήσουν κακόβουλο λογισμικό μέσω υποτιθέμενων εγγράφων σχετικών με την αίτηση εργασίας (NIELIT Patna, 2024).

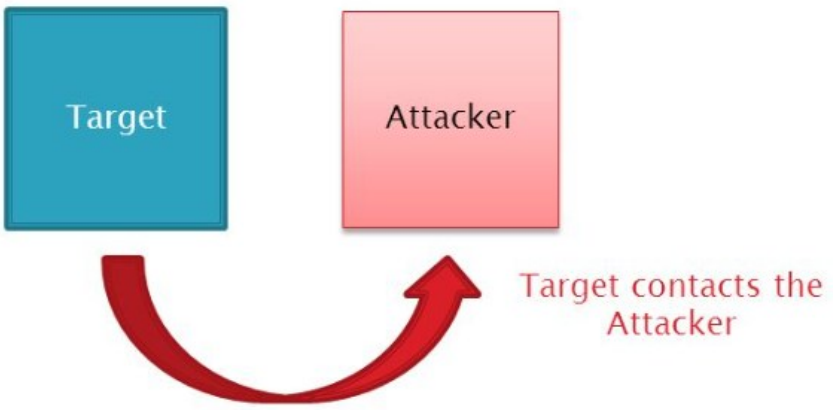
Ιδιαίτερο ενδιαφέρον παρουσιάζει η εξέλιξη των επιθέσεων honey trap στον τομέα της στοχευμένης κατασκοπείας. Παρότι η μέθοδος διατηρεί τον συναισθηματικό της χαρακτήρα - που τη διαφοροποιεί από το pretexting - η εφαρμογή της σε περιπτώσεις κατασκοπείας είναι πιο σύνθετη. Για παράδειγμα, ένας αξιωματούχος άμυνας συνελήφθη αφού έπεσε θύμα τέτοιας επίθεσης από πράκτορες του ISIS με βάση το Πακιστάν στα μέσα κοινωνικής δικτύωσης. Οι επιτιθέμενοι χρησιμοποίησαν συναισθηματική χειραγώγηση και προσωπική προσέγγιση, παρά το επαγγελματικό πλαίσιο του στόχου, οδηγώντας στη διαρροή κρίσιμων στρατιωτικών πληροφοριών (Yawar, 2024b).

Οι συνέπειες των επιθέσεων honey trap μπορεί να είναι σοβαρές τόσο για άτομα όσο και για οργανισμούς, συμπεριλαμβανομένης της κλοπής ταυτότητας, οικονομικής απάτης και παραβίασης εταιρικών δικτύων (Kaspersky, 2024a). Αυτό υπογραμμίζει τη σημασία της εκπαίδευσης σε θέματα κυβερνοασφάλειας, ιδιαίτερα για άτομα σε ευαίσθητες θέσεις.

Η ανιχνευσιμότητα των επιθέσεων αυτού του τύπου είναι ιδιαίτερα χαμηλή, καθώς βασίζονται σε προσωπικές σχέσεις και συναισθηματική χειραγώγηση, κάτι που καθιστά δύσκολη την αναγνώρισή τους εκ των προτέρων.

3.2.3.5. Reverse Social Engineering

Η επίθεση αντίστροφης κοινωνικής μηχανικής (Reverse Social Engineering) είναι μια προηγμένη τεχνική κοινωνικής μηχανικής όπου ο επιτιθέμενος δημιουργεί μια κατάσταση που ωθεί το θύμα να επικοινωνήσει μαζί του, αντί να προσεγγίσει ο ίδιος άμεσα το θύμα (δείτε Εικόνα 16). Ο στόχος είναι να αποκτήσει την εμπιστοσύνη του θύματος και να αποσπάσει ευαίσθητες πληροφορίες ή να αποκτήσει πρόσβαση σε συστήματα (Irani et al., n.d.; Zaoui et al., 2024). Για παράδειγμα, ένας επιτιθέμενος απενεργοποιεί ένα πληροφοριακό σύστημα ενός οργανισμού και στέλνει ένα μαζικό email, προσποιούμενος ότι είναι μέλος του IT helpdesk. Οι υπάλληλοι, πιστεύοντας ότι επικοινωνούν με την υποστήριξη, παρέχουν τα διαπιστευτήρια ή τις πληροφορίες πρόσβασής τους (Yawar, 2024a).



Εικόνα 16: Αντίστροφη κοινωνική μηχανική

Πηγή: (SlidePlayer.com Inc., 2024)

Η επίθεση αντίστροφης κοινωνικής μηχανικής συνήθως περιλαμβάνει τρία βασικά στάδια: δολιοφθορά (sabotage), διαφήμιση (advertising) και βοήθεια (assisting) (Hobel et al., 2014; Salahdine & Kaabouch, 2019). Στο πρώτο στάδιο, ο επιτιθέμενος προκαλεί ένα πρόβλημα στο σύστημα του θύματος, όπως μια δυσλειτουργία του δικτύου. Στη συνέχεια, διαφημίζει ότι μπορεί να επιλύσει το πρόβλημα, συχνά υποδυόμενος έναν ειδικό πληροφορικής ή τεχνικό υποστήριξης. Τέλος, όταν το θύμα ζητήσει βοήθεια, ο επιτιθέμενος "επιλύει" το πρόβλημα ενώ ταυτόχρονα αποσπά ευαίσθητες πληροφορίες ή εγκαθιστά κακόβουλο λογισμικό (Greavu-Serban & Serban, 2014).

Η αποτελεσματικότητα αυτής της τεχνικής βασίζεται στο γεγονός ότι το θύμα είναι αυτό που ξεκινά την επικοινωνία, δημιουργώντας έτσι μια αίσθηση εμπιστοσύνης προς τον επιτιθέμενο (Hasan et al., 2010). Αυτό μειώνει την πιθανότητα να προκληθούν υποψίες και αυξάνει τις πιθανότητες επιτυχίας της επίθεσης. Επιπλέον, η τεχνική αυτή εκμεταλλεύεται την αρχή της αμοιβαιότητας, καθώς το θύμα αισθάνεται υποχρεωμένο προς τον επιτιθέμενο που "έλυσε" το πρόβλημα (Wang et al., 2021).

Παρόλο που η αντίστροφη κοινωνική μηχανική μπορεί να είναι ιδιαίτερα αποτελεσματική, απαιτεί σημαντική προετοιμασία, έρευνα και προγραμματισμό από την πλευρά του επιτιθέμενου (Mugala, 2014.; Soni et al., 2024). Αυτό την καθιστά πιο δύσκολη στην εκτέλεση σε σύγκριση με τις παραδοσιακές μεθόδους κοινωνικής μηχανικής, αλλά ταυτόχρονα πιο επικίνδυνη λόγω του υψηλού επιπέδου εμπιστοσύνης που δημιουργείται.

Στις επιθέσεις reverse social engineering, η ανίχνευση είναι δύσκολη, παρόλο που η τεχνική θεωρείται ότι έχει χαμηλή έως μέτρια ανιχνευσιμότητα. Αυτό συμβαίνει επειδή ο επιτιθέμενος δημιουργεί τις συνθήκες που οδηγούν το θύμα να επικοινωνήσει οικειοθελώς μαζί του, π.χ., μέσω παραπλανητικών μηνυμάτων, ψευδών προβλημάτων ή επείγουσας

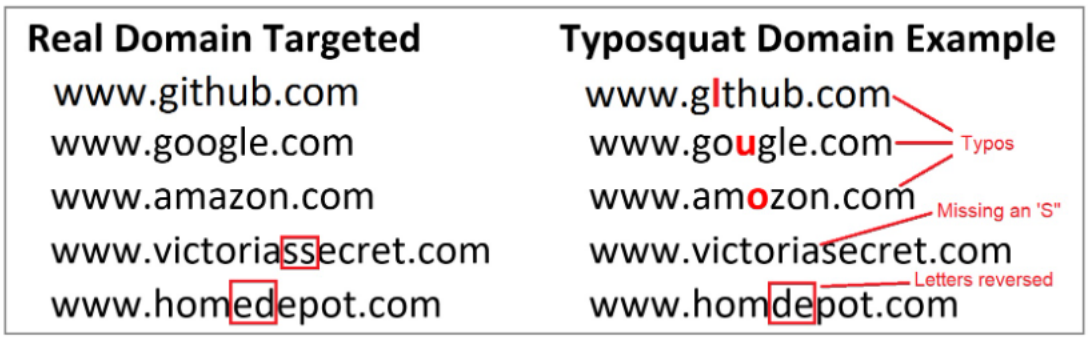
κατάστασης που φαίνεται αξιόπιστη. Ως αποτέλεσμα, τα παραδοσιακά συστήματα ανίχνευσης απειλών δεν ενεργοποιούνται, διότι η επικοινωνία ξεκινά από το θύμα και όχι από τον επιτιθέμενο.

3.2.4. Επιθέσεις Βασισμένες σε Τεχνικές Παραπλάνησης

Οι επιθέσεις που βασίζονται σε τεχνικές παραπλάνησης αποτελούν μια εξελιγμένη μορφή κοινωνικής μηχανικής που επικεντρώνεται στην εξαπάτηση μέσω της παραποίησης ή απομίμησης νόμιμων πηγών και συστημάτων. Σε αντίθεση με τις επιθέσεις πλαστοπροσωπίας που βασίζονται κυρίως στην υιοθέτηση ψεύτικων ταυτοτήτων, αυτές οι μέθοδοι εστιάζουν στη δημιουργία παραπλανητικών περιβαλλόντων και καταστάσεων που μιμούνται γνήσιες υπηρεσίες ή συστήματα. Συνδυάζουν την τεχνολογική εξαπάτηση με την ψυχολογική χειραγώγηση, εκμεταλλευόμενες την τάση των χρηστών να εμπιστεύονται οικείες διεπαφές και δομές. Στην υποενότητα αυτή, θα αναλυθούν τεχνικές όπως το typosquatting, το evil twin και οι watering hole επιθέσεις, εξετάζοντας πώς οι επιτιθέμενοι δημιουργούν απατηλά περιβάλλοντα που παρασύρουν τους χρήστες σε μη ασφαλείς αλληλεπιδράσεις.

3.2.4.1. Typosquatting / URL Hijacking

Η τυποκαταλήστευση ή πειρατεία συνδέσμων URL (Typosquatting ή URL Hijacking) αποτελεί μια μορφή κυβερνοεπίθεσης (δείτε Εικόνα 17) που εκμεταλλεύεται τα τυπογραφικά λάθη των χρηστών κατά την πληκτρολόγηση ονομάτων τομέων (domain names) στο διαδίκτυο (Szurdi et al., 2017). Οι επιτιθέμενοι καταχωρούν ονόματα τομέων που είναι παρόμοια με δημοφιλείς και νόμιμους ιστότοπους, εκμεταλλευόμενοι συχνά λάθη πληκτρολόγησης, όπως παράλειψη τελείας, αντιμετάθεση γραμμάτων, ή λανθασμένη πληκτρολόγηση (Szurdi & Christin, 2017). Όταν ο χρήστης πληκτρολογήσει λανθασμένα το όνομα τομέα, ανακατευθύνεται σε έναν πλαστό ιστότοπο που μιμείται πιστά την εμφάνιση και λειτουργικότητα του νόμιμου ιστότοπου. Τέτοιοι πλαστοί ιστότοποι συνήθως χρησιμοποιούνται είτε για ηλεκτρονικό ψάρεμα (όπου ζητούνται προσωπικά δεδομένα και στοιχεία πληρωμών από τους ανυποψίαστους χρήστες), είτε για τη διανομή κακόβουλου λογισμικού μέσω μολυσμένων αρχείων ή συνδέσμων (Szurdi et al., 2017; Taylor et al., 2020).



Εικόνα 17: Παραδείγματα λανθασμένης πληκτρολόγησης ονομάτων τομέων που διευκολύνουν μια επίθεση τυποκαταλήστευσης

Πηγή: (NASA Federal Credit Union, 2019)

Το φαινόμενο αυτό έχει εξελιχθεί σημαντικά με την πάροδο του χρόνου. Αρχικά, οι επιθέσεις typosquatting επικεντρώνονταν σε πολύ δημοφιλείς ιστότοπους, καθώς προσέφεραν μεγαλύτερο όγκο πιθανών θυμάτων. Ωστόσο, η αυξανόμενη ανταγωνιστικότητα και οι βελτιωμένοι μηχανισμοί προστασίας των μεγάλων ιστοτόπων έχουν οδηγήσει τους επιτιθέμενους να στοχεύουν και σε λιγότερο δημοφιλείς προορισμούς, δημιουργώντας μια "μακριά ουρά" από typosquatting domains (Szurdi et al., 2014). Αυτή η στρατηγική είναι αποτελεσματική λόγω του συνδυασμού χαμηλού κόστους καταχώρησης domain names και της μειωμένης επαγρύπνησης των μικρότερων οργανισμών για τέτοιου είδους απειλές.

Οι typosquatters χρησιμοποιούν διάφορες μεθόδους για να αποκομίσουν κέρδη, συμπεριλαμβανομένης της προβολής διαφημίσεων, της ανακατεύθυνσης σε τρίτους ιστότοπους, του phishing και της διάδοσης κακόβουλου λογισμικού (Szurdi et al., 2014). Η απλή και οικονομική διαδικασία καταχώρησης ονομάτων τομέων επιτρέπει στους επιτιθέμενους να καταχωρούν μαζικά παρόμοια ονόματα, αυξάνοντας τις πιθανότητες επιτυχίας (Taylor et al., 2020).

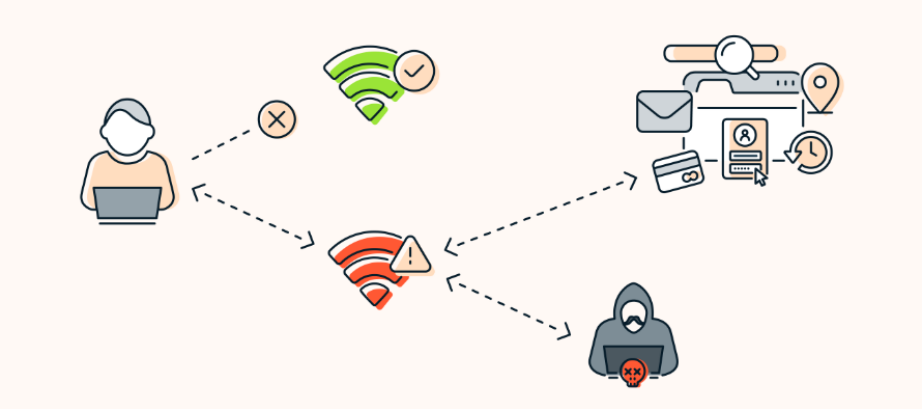
Ο εντοπισμός τέτοιων επιθέσεων είναι ιδιαίτερα δύσκολος λόγω της οπτικής ομοιότητας των ονομάτων τομέων και του μεγάλου αριθμού πιθανών παραλλαγών (Taylor et al., 2020). Οι επιπτώσεις για τους χρήστες μπορεί να κυμαίνονται από απλή απώλεια χρόνου σε άσχετους ιστότοπους μέχρι έκθεση σε κακόβουλο περιεχόμενο ή phishing (Szurdi et al., 2014). Σε νομικό επίπεδο, το typosquatting θεωρείται παράνομο σε πολλές δικαιοδοσίες και μπορεί να οδηγήσει σε νομικές διαμάχες για παραβίαση εμπορικών σημάτων (Szurdi & Christin, 2017).

3.2.4.2. Evil Twin

Η επίθεση Evil Twin (κακόβουλου διδύμου) είναι μια τεχνική κυβερνοεπίθεσης που εξαπολύεται μέσω των ασύρματων δικτύων Wi-Fi, κατά την οποία ένας κακόβουλος χρήστης εγκαθιστά ένα πλαστό σημείο πρόσβασης (access point) που μιμείται ένα νόμιμο (δείτε Εικόνα 18). Υπάγεται στην κατηγορία των κοινωνικών επιθέσεων καθώς εκμεταλλεύεται συγκεκριμένα ψυχολογικά χαρακτηριστικά και συμπεριφορές των χρηστών (Hsu et al., 2022). Συγκεκριμένα, η επίθεση αξιοποιεί:

- Την εξοικείωση των χρηστών με γνώριμα ονόματα δικτύων και την τάση τους να εμπιστεύονται αυτόματα δίκτυα που έχουν χρησιμοποιήσει στο παρελθόν
- Την ανάγκη για γρήγορη και απρόσκοπτη πρόσβαση στο διαδίκτυο, ειδικά σε δημόσιους χώρους
- Την προτίμηση των χρηστών σε ισχυρότερα σήματα Wi-Fi, ακόμα και όταν προέρχονται από αμφίβολες πηγές
- Την περιορισμένη τεχνική γνώση των περισσότερων χρηστών σχετικά με την ασφάλεια των ασύρματων δικτύων

Ο μηχανισμός λειτουργίας της επίθεσης βασίζεται στη δημιουργία ενός πλαστού σημείου πρόσβασης Wi-Fi που μιμείται το αναγνωριστικό του συνόλου των υπηρεσιών δικτύου (SSID: Service Set Identifier) και τη διεύθυνση MAC (Media Access Control) ενός νόμιμου σημείου πρόσβασης (Hsu et al., 2022), όπως παρουσιάζεται στην παρακάτω εικόνα. Εκμεταλλευόμενος την ανθρώπινη τάση για επιλογή του ισχυρότερου σήματος, ο επιτιθέμενος συχνά ρυθμίζει το πλαστό σημείο πρόσβασης να εκπέμπει ισχυρότερο σήμα από το νόμιμο, αυξάνοντας την πιθανότητα οι χρήστες να επιλέξουν τη σύνδεση σε αυτό (Agarwal et al., 2018).



Εικόνα 18: Απεικόνιση μιας επίθεσης κακόβουλου διδύμου

Πηγή: (Ghimiray, 2022)

Οι στόχοι και οι επιπτώσεις της επίθεσης Evil Twin είναι ιδιαίτερα σοβαροί. Εκμεταλλευόμενος την ψευδή αίσθηση ασφάλειας που δημιουργείται από την οικειότητα με το όνομα του δικτύου, ο επιτιθέμενος μπορεί να υποκλέψει ευαίσθητα δεδομένα των χρηστών, όπως κωδικούς, στοιχεία πιστωτικών καρτών και προσωπικές πληροφορίες (Daldoul, 2023). Επιπλέον, μπορεί να εξαπολύσει επιθέσεις man-in-the-middle, να ανακατευθύνει τους χρήστες σε κακόβουλες ιστοσελίδες ή να παρακολουθήσει την κίνηση των δεδομένων τους, εκμεταλλευόμενος την περιορισμένη τεχνική γνώση των θυμάτων σχετικά με την ασφάλεια των ασύρματων δικτύων (Adinkrah-Appiah et al., 2021).

Η ανιχνευσιμότητα αυτής της επίθεσης είναι μέτρια, καθώς μπορεί να εντοπιστεί μέσω συστημάτων παρακολούθησης ασύρματων δικτύων και ανίχνευσης rogue access points (παράνομων σημείων πρόσβασης). Ωστόσο, σε πολυσύχναστους χώρους ή περιβάλλοντα με πολλά διαθέσιμα δίκτυα Wi-Fi, η αναγνώριση της επίθεσης μπορεί να είναι πιο δύσκολη, απαιτώντας συνεχόμενη παρακολούθηση και ανίχνευση παράξενων ή μη εξουσιοδοτημένων συνδέσεων.

3.2.4.3. Watering Hole Attack

Η επίθεση στο σημείο συγκέντρωσης (Watering Hole Attack) (δείτε Εικόνα 19) είναι μια προηγμένη τεχνική κοινωνικής μηχανικής, κατά την οποία ο επιτιθέμενος μολύνει με κακόβουλο λογισμικό μία ή περισσότερες νόμιμες ιστοσελίδες που επισκέπτεται συχνά ο στόχος. Στην κλασική μορφή της επίθεσης, η μόλυνση των συστημάτων του στόχου (μέσω κακόβουλου λογισμικού) πραγματοποιείται μέσω drive-by download επιθέσεων - δηλαδή, με την αυτόματη και σιωπηλή εκμετάλλευση τρωτοτήτων του φυλλομετρητή του χρήστη κατά την επίσκεψή του στη μολυσμένη ιστοσελίδα, χωρίς να απαιτείται καμία ενέργεια από την πλευρά του και χωρίς να γίνει αντιληπτή η εγκατάσταση του κακόβουλου λογισμικού.

Μια ενδιαφέρουσα παραλλαγή της επίθεσης Watering Hole, όπου η παραπλάνηση είναι πιο εμφανής, είναι η χρήση της για τη διάδοση χρήσιμων αλλά μολυσμένων εργαλείων. Σε αυτή την περίπτωση, ο επιτιθέμενος χρησιμοποιεί τον μολυσμένο ιστότοπο για να διαφημίσει και να διανείμει ένα φαινομενικά χρήσιμο εργαλείο, το οποίο όμως περιέχει κρυφό κακόβουλο κώδικα. Η διαφήμιση του εργαλείου στον μολυσμένο ιστότοπο στοχεύει στο να δελεάσει συγκεκριμένους χρήστες να το κατεβάσουν και να το εγκαταστήσουν οικειοθελώς. Αυτή η τακτική εκμεταλλεύεται την αρχή της "προτίμησης" στην κοινωνική μηχανική, στοχεύοντας συγκεκριμένες ομάδες χρηστών με βάση τα ενδιαφέροντά τους (Fortinet, 2024a; Zheng et al., 2019).

Εικόνα 19: Διεξαγωγή της επίθεσης στο σημείο συγκέντρωσης

Πηγή: (Wright & Bacon, 2024)

Τα βασικά σημεία μιας επίθεσης τύπου watering hole είναι τα κάτωθι:

1. *Μηχανισμός λειτουργίας*: Ο επιτιθέμενος αρχικά εντοπίζει και αναλύει τις διαδικτυακές συνήθειες του στόχου, προσδιορίζοντας τις ιστοσελίδες που επισκέπτεται συχνά (Zaoui et al., 2024). Στη συνέχεια, εκμεταλλεύεται ευπάθειες σε μία ή περισσότερες από αυτές τις ιστοσελίδες για να τις μολύνει με κακόβουλο λογισμικό (Breda et al., 2020). Όταν ο στόχος επισκεφθεί την μολυσμένη ιστοσελίδα, το κακόβουλο λογισμικό μεταφορτώνεται και εγκαθίσταται στο σύστημά του, συχνά χωρίς ο χρήστης να το αντιληφθεί (επίθεση drive-by download) (Alsufyani & Alzahrani, 2020).
2. Η επίθεση Watering Hole θεωρείται ιδιαίτερα προηγμένη και απαιτεί σημαντικές τεχνικές γνώσεις από τον επιτιθέμενο (Breda et al., 2020). Συνήθως στοχεύει συγκεκριμένες ομάδες, όπως οργανισμούς, βιομηχανίες ή γεωγραφικές περιοχές (Zheng et al., 2019). Η επίθεση εκμεταλλεύεται την εμπιστοσύνη του στόχου προς τις ιστοσελίδες που επισκέπτεται συχνά, καθιστώντας την ιδιαίτερα αποτελεσματική (Soni et al., 2024). Η ανίχνευση αυτού του τύπου επίθεσης είναι ιδιαίτερα δύσκολη, καθώς το κακόβουλο λογισμικό διανέμεται μέσω νόμιμων και αξιόπιστων ιστοσελίδων, παρακάμπτοντας έτσι πολλούς παραδοσιακούς μηχανισμούς ασφαλείας.
3. *Επιπτώσεις και σκοποί*: Μέσω της επίθεσης Watering Hole, ο επιτιθέμενος μπορεί να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα του στόχου, να υποκλέψει ευαίσθητες πληροφορίες ή να εξαπλώσει την επίθεση σε ολόκληρο το δίκτυο του οργανισμού. Η τεχνική αυτή χρησιμοποιείται συχνά σε επιθέσεις κυβερνοκατασκοπείας εναντίον πολλαπλών στόχων σε διάφορους επιχειρηματικούς τομείς (Udochukwu & Bode-Asa, 2023).

Η ανιχνευσιμότητα αυτής της επίθεσης είναι μέτρια προς υψηλή, καθώς τα σύγχρονα αντιϊικά προγράμματα και τα συστήματα ασφαλείας δικτύου μπορούν να ανιχνεύσουν κακόβουλο περιεχόμενο ή ύποπτες δραστηριότητες σε μια ιστοσελίδα. Παρ' όλα αυτά, για πιο

εξειδικευμένες και στοχευμένες επιθέσεις, η ανίχνευση μπορεί να είναι δύσκολη, ιδιαίτερα αν οι ιστοσελίδες είναι δημοφιλείς και οι επιθέσεις είναι καλά κρυμμένες μέσα στο νόμιμο περιεχόμενο.

3.2.4.4. Diversion Theft

Η επίθεση εκτροπής κλοπής (Diversion Theft) (δείτε Εικόνα 20) είναι μια τεχνική κοινωνικής μηχανικής στην οποία ο επιτιθέμενος παραπλανά το θύμα μέσω πειστικών ψευδών σεναρίων ή/και πλαστοπροσωπίας, ώστε το θύμα να παραδώσει ή να αποστείλει ευαίσθητες πληροφορίες ή αγαθά σε λάθος παραλήπτη ή τοποθεσία, με σκοπό την υποκλοπή ή κλοπή τους, αντίστοιχα. Μια υποθετική περίπτωση diversion theft θα μπορούσε να είναι η εξής: ο επιτιθέμενος προσποιείται ότι είναι υπάλληλος του τμήματος προμηθειών μιας μεγάλης εταιρείας τεχνολογίας και επικοινωνεί με τον προμηθευτή εξοπλισμού πληροφορικής, ισχυριζόμενος ότι το κεντρικό κέντρο δεδομένων (datacenter) (της εταιρείας τεχνολογίας) αντιμετωπίζει προβλήματα και ζητά την παράδοση των εξυπηρετητών (servers) σε μια εναλλακτική τοποθεσία. Η επίθεση εκτροπής κλοπής έχει τις ρίζες της σε παραδοσιακές offline απάτες, όπου οι κακοποιοί παραπλανούσαν τους οδηγούς φορτηγών να παραδώσουν εμπορεύματα σε λάθος τοποθεσία (Wood, 2020).

Εικόνα 20: Επίθεση εκτροπής κλοπής

Πηγή: (Cyber Witcher, 2024)

Στη σύγχρονη εποχή, η τεχνική της επίθεσης εκτροπής έχει εξελιχθεί και προσαρμοστεί στο ψηφιακό περιβάλλον. Σε μια τυπική online επίθεση τέτοιου τύπου, ο κακόβουλος χρήστης εξαπατά το θύμα ώστε να στείλει εμπιστευτικές πληροφορίες σε λάθος παραλήπτη (Lenaerts-Bergmans, 2023). Αυτό συχνά επιτυγχάνεται μέσω τεχνικών πλαστοπροσωπίας (spoofing), όπου ο επιτιθέμενος μεταμφιέζεται ως αξιόπιστη πηγή, για παράδειγμα μιμούμενος τη

διεύθυνση ηλεκτρονικού ταχυδρομείου κάποιου από την εταιρεία του θύματος (Copado Team, 2022).

Μια πιο εξελιγμένη μορφή της επίθεσης περιλαμβάνει τη χρήση εταιρειών ταχυμεταφορών για την εισαγωγή κακόβουλου λογισμικού ή rootkits σε υπολογιστές ή συστήματα που αποστέλλονται και χρησιμοποιούνται από μια εταιρεία. Αυτό μπορεί να επιτευχθεί αν οι επιτιθέμενοι αποκτήσουν φυσική πρόσβαση σε αυτά τα αγαθά πριν από την αποστολή τους, είτε μέσω συνεργών εντός της αλυσίδας εφοδιασμού είτε με παρεμβολή κατά τη διαδικασία μεταφοράς (Syafitri et al., 2022). Η μέθοδος αυτή επιτρέπει στο κακόβουλο λογισμικό να εισέλθει στο εταιρικό δίκτυο, μειώνοντας τις πιθανότητες ανίχνευσής του.

Οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιήσουν τεχνολογία για να παρεμβληθούν και να τροποποιήσουν τα προγράμματα παράδοσης, διευκολύνοντας την εκτροπή αγαθών ή πληροφοριών. Είναι σημαντικό να σημειωθεί ότι η επίθεση εκτροπής συχνά συνδυάζεται με άλλες τεχνικές κοινωνικής μηχανικής, όπως το spear phishing, το whaling, το vishing και οι επιθέσεις προσποίησης (pretexting). Αυτός ο συνδυασμός τεχνικών καθιστά την επίθεση πιο περίπλοκη και δύσκολη στην ανίχνευση, αυξάνοντας την πιθανότητα επιτυχίας για τους κακόβουλους χρήστες (Wood, 2020).

Η ανιχνευσιμότητα αυτής της επίθεσης είναι μέτρια, καθώς μπορεί να εντοπιστεί μέσω συστημάτων παρακολούθησης και επαλήθευσης των διαδικασιών παράδοσης και παραλαβής. Ωστόσο, αν η παραπλάνηση είναι προσεκτικά σχεδιασμένη, μπορεί να είναι δύσκολο να εντοπιστεί εγκαίρως.

3.2.4.5. Grooming

Το cybergrooming (προετοιμασία θυμάτων) είναι μια μορφή διαδικτυακής κοινωνικής εξαπάτησης και εγκληματικής δραστηριότητας, όπου ο δράστης (ο "groomer") χρησιμοποιεί ψυχολογικές τεχνικές και τεχνολογίες πληροφορικής για να αποκτήσει την εμπιστοσύνη του θύματος (δείτε Εικόνα 21). Αν και συνήθως στοχεύει ανήλικα άτομα, δεν περιορίζεται αποκλειστικά σε αυτά. Οι στόχοι του cybergrooming μπορεί να περιλαμβάνουν τη σεξουαλική εκμετάλλευση, αλλά και άλλες μορφές κακόβουλης δραστηριότητας, όπως οικονομική απάτη, ριζοσπαστικοποίηση, trafficking, διαδικτυακό εκφοβισμό (cyberbullying), κατασκοπεία και άλλες παράνομες ενέργειες (Guo et al., 2023; Syafitri et al., 2022).

Η διαδικασία του cybergrooming εξελίσσεται σταδιακά. Αρχικά, ο δράστης οικοδομεί μια σχέση εμπιστοσύνης με το πιθανό θύμα, συχνά χρησιμοποιώντας ψεύτικες ταυτότητες σε διαδικτυακές πλατφόρμες. Στη συνέχεια, συλλέγει ευαίσθητες προσωπικές πληροφορίες ή χειραγωγεί το θύμα για να το οδηγήσει στην εκπλήρωση των στόχων του. Αυτό μπορεί να

περιλαμβάνει, ανάλογα με την περίπτωση, τη συμμετοχή σε παράνομες δραστηριότητες, τη δημιουργία επικίνδυνων σχέσεων ή ακόμα και φυσική συνάντηση (Guo et al., 2023).

Εικόνα 21: Τεχνική εκμετάλλευσης "grooming"

Πηγή: (CSA, 2024)

Η ανιχνευσιμότητα αυτής της επίθεσης είναι χαμηλή προς μέτρια, καθώς η φύση της είναι συχνά σταδιακή και κρυφή. Αξιοποιεί την εμπιστοσύνη που χτίζεται με το χρόνο, κάνοντάς την δύσκολη να εντοπιστεί άμεσα.

3.2.4.5.1. Η Απειλή του Cybergrooming

Το cybergrooming αποτελεί σοβαρή απειλή για την ασφάλεια στο διαδίκτυο, επηρεάζοντας κυρίως ευάλωτες ομάδες, όπως ανήλικους ηλικίας 12-15 ετών, αλλά και ενήλικες σε περιπτώσεις οικονομικής απάτης, κατασκοπείας ή ριζοσπαστικοποίησης (Guo et al., 2023). Οι επιτιθέμενοι εκμεταλλεύονται την ανωνυμία του διαδικτύου, την έλλειψη γνώσης για τις διαδικτυακές απειλές και τα ψυχολογικά κίνητρα των θυμάτων. Οι επιπτώσεις για τα θύματα μπορεί να είναι σοβαρές και μακροχρόνιες, περιλαμβάνοντας ψυχολογικό τραύμα, οικονομική ζημία ή νομικές συνέπειες (Guo et al., 2023).

3.2.4.5.2. Παράγοντες Ευαλωτότητας και Προληπτική Προστασία

Η ανάλυση των παραγόντων ευαλωτότητας των πιθανών θυμάτων είναι κρίσιμη για την προληπτική προστασία από το cybergrooming. Μελέτες έχουν δείξει ότι χαρακτηριστικά, όπως η ριψοκίνδυνη διαδικτυακή συμπεριφορά και η αναζήτηση θετικών συναισθημάτων, σχετίζονται θετικά με την πιθανότητα θυματοποίησης. Αντίθετα, η υψηλή γνωστική ικανότητα φαίνεται να λειτουργεί προστατευτικά (Guo et al., 2023). Ειδικά για το grooming, η προληπτική προστασία περιλαμβάνει την εκπαίδευση των νέων στη σωστή χρήση του διαδικτύου, την παρακολούθηση των διαδικτυακών δραστηριοτήτων από τους γονείς και την ανάπτυξη εργαλείων ανίχνευσης ύποπτης συμπεριφοράς στις πλατφόρμες κοινωνικής

δικτύωσης. Ωστόσο, τα ευρήματα για τον ρόλο των οικογενειακών σχέσεων και της κοινωνικής υποστήριξης ως παραγόντων ευαλωτότητας παραμένουν αντικρουόμενα (Guo et al., 2023).

4. ΜΕΘΟΔΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ

Στο σύγχρονο ψηφιακό περιβάλλον, η προστασία από επιθέσεις κοινωνικής μηχανικής αποτελεί θεμελιώδη πρόκληση για οργανισμούς και ιδιώτες. Η αποτελεσματική θωράκιση απέναντι σε τέτοιες απειλές απαιτεί μια ολιστική προσέγγιση που συνδυάζει τεχνολογικά μέτρα, εκπαιδευτικές πρωτοβουλίες και οργανωσιακές πολιτικές.

Οι οργανωσιακές πολιτικές διαδραματίζουν καθοριστικό ρόλο στη διαμόρφωση ενός ασφαλούς περιβάλλοντος. Μέσα από την υιοθέτηση σαφών διαδικασιών, όπως η πολιτική ασφαλούς πρόσβασης στα δεδομένα, η διαχείριση των κινδύνων και η έγκαιρη αντιμετώπιση περιστατικών ασφαλείας, εξασφαλίζεται η συνέπεια και η ευθύνη σε όλα τα επίπεδα του οργανισμού. Η συμμόρφωση με διεθνή πρότυπα και κανονισμούς, όπως ο GDPR, ενισχύει περαιτέρω την ανθεκτικότητα απέναντι στις απειλές.

Η καλλιέργεια μιας κουλτούρας ασφάλειας αποτελεί τον ακρογωνιαίο λίθο της προστασίας, όπου κάθε μέλος ενός οργανισμού συμμετέχει ενεργά στην αναγνώριση και αντιμετώπιση πιθανών απειλών. Αυτό επιτυγχάνεται μέσω συστηματικής εκπαίδευσης, προσομοιώσεων επιθέσεων και συνεχούς ενημέρωσης για αναδυόμενους κινδύνους.

Παράλληλα, η τεχνική θωράκιση με εργαλεία, όπως η πολυπαραγοντική αυθεντικοποίηση (MFA: Multi-Factor Authentication) και τα προηγμένα συστήματα φιλτραρίσματος ηλεκτρονικού ταχυδρομείου, σε συνδυασμό με αυστηρά πρωτόκολλα διαχείρισης δεδομένων, δημιουργούν ένα ισχυρό πλαίσιο προστασίας. Η διαρκής επαγρύπνηση και η κριτική σκέψη των χρηστών, μαζί με τη συνεργασία μεταξύ οργανισμών και αρχών επιβολής του νόμου, συμπληρώνουν το οπλοστάσιο άμυνας έναντι των επιθέσεων κοινωνικής μηχανικής (International Telecommunication Union, 2024).

Η Ευρωπαϊκή Ένωση, μέσω του Πρακτορείου για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA: European Union Agency for Network and Information Security), προωθεί μια ολοκληρωμένη προσέγγιση που συνδυάζει τεχνικές και κοινωνικές πτυχές της ασφάλειας πληροφοριών. Τονίζεται ιδιαίτερα η σημασία της συνεργασίας μεταξύ των γονέων και των εκπαιδευτικών, της κοινωνίας των πολιτών, των κρατικών οργανισμών και της Ευρωπαϊκής Επιτροπής για την αντιμετώπιση των αναδυόμενων κινδύνων ασφαλείας στο διαδίκτυο (ENISA, 2011).

4.1. Δομή του Κεφαλαίου

Στις επόμενες ενότητες, θα αναλυθούν οι μέθοδοι προστασίας από επιθέσεις κοινωνικής μηχανικής, οι οποίες καλύπτουν τις εξής πτυχές:

- **Τεχνικά μέτρα προστασίας**: Περιγραφή εργαλείων και τεχνολογιών που συμβάλλουν στη θωράκιση απέναντι σε διαφορετικά είδη επιθέσεων κοινωνικής μηχανικής.
- **Εκπαίδευση και ευαισθητοποίηση χρηστών**: Παρουσίαση στρατηγικών εκπαίδευσης, εξειδικευμένων οδηγιών και καινοτόμων μεθόδων, όπως τα παιχνίδια προσομοίωσης.
- **Οργανωσιακές πολιτικές και διαδικασίες**: Εξέταση των θεσμικών μέτρων που ενισχύουν την ανθεκτικότητα οργανισμών στις επιθέσεις.
- **Κουλτούρα ασφάλειας**: Ανάλυση της σημασίας της διαμόρφωσης ασφαλών συμπεριφορών και συλλογικής ευθύνης.
- **Αξιολόγηση και διαχείριση κινδύνων**: Εντοπισμός και εκτίμηση των κινδύνων που συνδέονται με τις επιθέσεις κοινωνικής μηχανικής.
- **Δοκιμές ασφαλείας και προσομοιώσεις επιθέσεων**: Εξέταση προληπτικών πρακτικών που ενισχύουν την ανίχνευση και τη διαχείριση περιστατικών.
- **Αντιμετώπιση περιστατικών και αποκατάσταση**: Παρουσίαση διαδικασιών για την αποτελεσματική διαχείριση περιστατικών ασφαλείας και την αποκατάσταση των επιπτώσεων.

Η ολιστική προσέγγιση που παρουσιάζεται στις ενότητες αυτές στοχεύει στη δημιουργία ενός πλήρους πλαισίου άμυνας απέναντι στις απειλές της κοινωνικής μηχανικής.

4.2. Οργανωτικές Πολιτικές και Διαδικασίες

Η θέσπιση οργανωτικών μέτρων για την προστασία από επιθέσεις κοινωνικής μηχανικής βασίζεται σε τρεις αλληλένδετους πυλώνες: πολιτικές, διαδικασίες και στρατηγικές εφαρμογής. Οι πολιτικές καθορίζουν το γενικό πλαίσιο προστασίας και τους κανόνες που πρέπει να ακολουθούνται, συμπεριλαμβανομένων των επιπέδων εξουσιοδότησης και των κριτηρίων λήψης αποφάσεων. Οι διαδικασίες περιγράφουν αναλυτικά τα βήματα εφαρμογής αυτών των κανόνων, καθορίζοντας συγκεκριμένες ενέργειες και υπευθυνότητες. Οι στρατηγικές αποτελούν το μακροπρόθεσμο σχέδιο υλοποίησης των πολιτικών μέσω των διαδικασιών, με στόχο τη διαρκή βελτίωση της ανθεκτικότητας του οργανισμού έναντι επιθέσεων κοινωνικής μηχανικής. Περιλαμβάνουν την καθιέρωση προγραμμάτων διαρκούς εκπαίδευσης, την προσαρμογή των πολιτικών ασφαλείας στις εξελισσόμενες απειλές και την

ανάπτυξη μηχανισμών ταχείας ανταπόκρισης σε νέα είδη επιθέσεων. Επιπλέον, ενσωματώνουν τη συνεργασία με εξωτερικούς φορείς, όπως οργανισμούς κυβερνοασφάλειας και ακαδημαϊκά ιδρύματα, ώστε να αξιοποιούνται οι βέλτιστες πρακτικές και οι πιο σύγχρονες μεθοδολογίες προστασίας (Mouton et al., 2020; Washo, 2021).

Σε επίπεδο διαδικασιών για την αντιμετώπιση της κοινωνικής μηχανικής, κάθε οργανισμός οφείλει να καθιερώσει συγκεκριμένα πρωτόκολλα επαλήθευσης ταυτότητας. Αυτά περιλαμβάνουν την επαλήθευση αιτημάτων μέσω προκαθορισμένων καναλιών επικοινωνίας, όπως εγκεκριμένες διευθύνσεις email και τηλεφωνικούς αριθμούς, τη χρήση κωδικών λέξεων για ευαίσθητες συναλλαγές, και την εφαρμογή του κανόνα των «δύο ατόμων» (two-person rule) ή της «αρχής των τεσσάρων ματιών» (four-eyes principle) για κρίσιμες αποφάσεις. Επιπρόσθετα, απαιτείται η καταγραφή και τεκμηρίωση όλων των εξουσιοδοτήσεων και των σχετικών επικοινωνιών (Chapagain et al., 2024; Chinta et al., 2016; Petrič & Roer, 2022).

Ενώ το τμήμα IT (IT: Information Technology) είναι υπεύθυνο για την εγκατάσταση και διαχείριση τεχνικών συστημάτων ασφαλείας, οι οργανωτικές πολιτικές καθορίζουν το πλαίσιο χρήσης τους από όλα τα τμήματα. Για παράδειγμα, το IT εγκαθιστά συστήματα διαχείρισης ταυτότητας και ελέγχου πρόσβασης (IAM: Identity and Access Management systems) και διαχείρισης περιστατικών (IMS: Incident Management Systems), αλλά οι πολιτικές προσδιορίζουν τις διαδικασίες με τις οποίες κάθε τμήμα αναφέρει περιστατικά, επαληθεύει ταυτότητες και διαχειρίζεται προσβάσεις. Οι πολιτικές επομένως, όχι μόνο προσδιορίζουν τις διαδικασίες με τις οποίες κάθε τμήμα αναφέρει περιστατικά, επαληθεύει ταυτότητες και διαχειρίζεται προσβάσεις, αλλά επηρεάζουν και τη διαμόρφωση των τεχνικών συστημάτων ασφάλειας. Αυτή η διάκριση μεταξύ τεχνικής υλοποίησης και οργανωτικής χρήσης είναι κρίσιμη για την αποτελεσματική προστασία από επιθέσεις κοινωνικής μηχανικής (Asante, 2022; Matyokurehwa, 2022; Heartfield & Loukas, 2019).

Οι οργανωτικές πολιτικές περιλαμβάνουν επίσης ειδικές προβλέψεις για την αντιμετώπιση συγκεκριμένων τεχνικών κοινωνικής μηχανικής. Για την προστασία από dumpster diving, καθορίζονται αυστηρές διαδικασίες καταστροφής εγγράφων σύμφωνα με τα πρότυπα NIST SP 800-88, ενώ για την αποτροπή του tailgating εφαρμόζονται πολυεπίπεδα συστήματα ελέγχου φυσικής πρόσβασης. Κάθε εργαζόμενος λαμβάνει σαφείς οδηγίες και εκπαίδευση στην εφαρμογή αυτών των διαδικασιών (Kissel et al., 2014; Odeh, 2021; Hove, 2020).

Για την αποτελεσματική εφαρμογή των πολιτικών, οι οργανισμοί αναπτύσσουν ολοκληρωμένα προγράμματα εκπαίδευσης και ευαισθητοποίησης. Αυτά περιλαμβάνουν προσομοιώσεις επιθέσεων κοινωνικής μηχανικής, εκπαίδευση στην αναγνώριση μεθόδων

χειραγώγησης και ψυχολογικής πίεσης, καθώς και τακτικές ασκήσεις ετοιμότητας με σενάρια βασισμένα σε πραγματικά περιστατικά (Saleem et al., 2017; Syafitri et al., 2022).

Η επιτυχής εφαρμογή των παραπάνω απαιτεί συστηματική αξιολόγηση και επικαιροποίηση, με ιδιαίτερη έμφαση στην προσαρμογή στις εξελισσόμενες μεθόδους κοινωνικής μηχανικής. Κάθε πολιτική και διαδικασία συνοδεύεται από μετρήσιμους δείκτες αποτελεσματικότητας, όπως ο χρόνος αναγνώρισης και αντίδρασης σε περιστατικά, το ποσοστό επιτυχίας στις προσομοιώσεις επιθέσεων, και η συχνότητα αναφοράς ύποπτων ενεργειών. Τα πρωτόκολλα αναθεώρησης προβλέπουν τακτική επανεξέταση και προσαρμογή βάσει των αποτελεσμάτων αυτών των μετρήσεων (Li et al., 2023; Odeh, 2021; Estella, 2024).

Ως απαραίτητο συμπλήρωμα, η τακτική διεξαγωγή ασκήσεων προσομοίωσης περιστατικών και η αξιολόγηση της ετοιμότητας αντιμετώπισης κρίσεων επιτρέπουν στους οργανισμούς να εντοπίζουν κενά στις διαδικασίες τους και να βελτιώνουν συνεχώς την αποτελεσματικότητα των μέτρων προστασίας τους.

4.3. Εταιρική Κουλτούρα Ασφάλειας

Η διαμόρφωση κουλτούρας ασφάλειας αποτελεί το επιστέγασμα των οργανωτικών πολιτικών και διαδικασιών για την προστασία από επιθέσεις κοινωνικής μηχανικής. Η κουλτούρα αυτή αναπτύσσεται σταδιακά μέσω της συστηματικής εφαρμογής εκπαιδευτικών προγραμμάτων, προσομοιώσεων επιθέσεων και συστημάτων επιβράβευσης που ενθαρρύνουν την ενεργή συμμετοχή των εργαζομένων στην αναγνώριση και αναφορά ύποπτων ενεργειών κοινωνικής μηχανικής (Washo, 2021· Chapagain et al., 2024).

Ιδιαίτερη έμφαση δίνεται στην καλλιέργεια κριτικής σκέψης απέναντι σε τεχνικές χειραγώγησης που χρησιμοποιούνται στην κοινωνική μηχανική. Οι εργαζόμενοι εκπαιδεύονται να αναγνωρίζουν τακτικές, όπως το pretexting, baiting και quid pro quo, ενώ παράλληλα ενθαρρύνονται να εφαρμόζουν πρακτικές επαλήθευσης ταυτότητας πριν την αποκάλυψη ευαίσθητων πληροφοριών (Chinta et al., 2016· Asante, 2022· Estella, 2024).

Για την αποτελεσματική αντιμετώπιση επιθέσεων κοινωνικής μηχανικής, είναι κρίσιμη η δημιουργία περιβάλλοντος όπου οι εργαζόμενοι αισθάνονται ασφαλείς να αναφέρουν ύποπτες δραστηριότητες χωρίς φόβο αντιποίνων. Αυτό επιτυγχάνεται μέσω σαφών διαδικασιών αναφοράς περιστατικών και προστασίας (whistleblowers), παράλληλα με την εφαρμογή δίκαιων συστημάτων κυρώσεων για παραβιάσεις των πρωτοκόλλων ασφαλείας (Odeh, 2021· Salahdine & Kaabouch, 2019).

Η ανώτερη διοίκηση διαδραματίζει καθοριστικό ρόλο στη διαμόρφωση της κουλτούρας ασφάλειας μέσω συγκεκριμένων πρακτικών. Για παράδειγμα, τα στελέχη

επιδεικνύουν προσωπικά την τήρηση των πρωτοκόλλων ασφαλείας, όπως τη χρήση πολλαπλών παραγόντων αυθεντικοποίησης και την επαλήθευση αιτημάτων μέσω επίσημων καναλιών επικοινωνίας. Η πολιτική "ανοιχτής πόρτας" (open door policy[3]) διευκολύνει την άμεση αναφορά ύποπτων περιστατικών κοινωνικής μηχανικής, ενώ η συμμετοχή σε δίκτυα ανταλλαγής πληροφοριών για απειλές (threat intelligence sharing networks) ενισχύει την προληπτική αντιμετώπιση νέων μεθόδων επίθεσης (Grassegger & Nedbal, 2021; Hove, 2020· Syafitri et al., 2022).

Η συνεχής ευαισθητοποίηση στις μεθόδους κοινωνικής μηχανικής είναι θεμελιώδης, καθώς οι επιτιθέμενοι συχνά εκμεταλλεύονται ανθρώπινες συμπεριφορές και προκαταλήψεις. Τα προγράμματα εκπαίδευσης εστιάζουν στην αναγνώριση ψυχολογικών τεχνικών χειραγώγησης, όπως η επίκληση στην εξουσία (authority), η δημιουργία αισθήματος επείγοντος (urgency) και η εκμετάλλευση της οικειότητας (familiarity) (Saleem et al., 2017· Li et al., 2023).

Συμπερασματικά, η κουλτούρα ασφάλειας αποτελεί το τελικό αποτέλεσμα της συστηματικής εφαρμογής πολιτικών, εκπαιδευτικών προγραμμάτων και πρακτικών ευαισθητοποίησης. Η επιτυχής αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής προϋποθέτει τη συνεχή ενίσχυση αυτής της κουλτούρας μέσω της ενεργού συμμετοχής όλων των επιπέδων του οργανισμού.

4.4. Εκπαίδευση & Ευαισθητοποίηση Χρηστών

Η εκπαίδευση του προσωπικού αποτελεί βασικό παράγοντα για την πρόληψη επιθέσεων κοινωνικής μηχανικής και πρέπει να είναι διαρκής, συστηματική και ολιστική, καλύπτοντας όλους τους τύπους απειλών με ιδιαίτερη έμφαση στο phishing, μία από τις πιο διαδεδομένες μεθόδους επίθεσης κοινωνικής μηχανικής (Chapagain et al., 2024). Η συνεχής ενημέρωση σχετικά με νέες απειλές και εξελισσόμενες τεχνικές επιθέσεων διασφαλίζει την υψηλή ετοιμότητα των χρηστών και τη δυνατότητα άμεσης προσαρμογής στις αλλαγές του τοπίου απειλών (Asante, 2022; Estella, 2024).

4.4.1 Απαιτήσεις Εκπαίδευσης Χρηστών

Η εκπαίδευση θα πρέπει να στοχεύει στη δημιουργία μιας σταθερής και διαρκούς επίγνωσης των κινδύνων, ώστε οι εργαζόμενοι να παραμένουν συνεχώς προσεκτικοί και σε εγρήγορση

[3] Πρόκειται για μια διοικητική πρακτική που ενθαρρύνει την άμεση και ανοιχτή επικοινωνία μεταξύ εργαζομένων και διοίκησης. Στο πλαίσιο της ασφάλειας, σημαίνει ότι οι εργαζόμενοι μπορούν να απευθυνθούν απευθείας στα ανώτερα στελέχη για να αναφέρουν ανησυχίες ή περιστατικά σχετικά με την ασφάλεια, χωρίς να χρειάζεται να ακολουθήσουν την τυπική ιεραρχική οδό.

απέναντι σε πιθανές απειλές. Είναι ύψιστης σημασίας να αναγνωρίζονται οι περιορισμοί της ευαισθητοποίησης, λόγω της συνεχούς καινοτομίας των επιτιθέμενων. Γι' αυτόν τον λόγο, προτείνεται η τακτική επανάληψη της εκπαίδευσης προκειμένου να διασφαλιστεί ότι οι εργαζόμενοι είναι ενημερωμένοι για τις πιο πρόσφατες απειλές και τις επικαιροποιημένες στρατηγικές προστασίας (Asante, 2022).

Μέσα από διαδραστικά και καινοτόμα προγράμματα, οι υπάλληλοι μπορούν να εκπαιδευτούν στις σύγχρονες τεχνικές πρόληψης και να ενισχυθεί η αντίληψή τους στην έγκαιρη αναγνώριση ύποπτων συμπεριφορών. Ορισμένα μοντέλα προτείνουν την εφαρμογή της τεχνικής UYCS (Use Your Common Sense) για την ανίχνευση ύποπτων emails, με κριτήρια, όπως τα ορθογραφικά λάθη, την ύπαρξη συγκεκριμένων συμβόλων ή την ασυνήθιστη μορφολογία των διευθύνσεων αποστολέων (Chinta et al., 2016; Saleem et al., 2017). Επιπλέον, η εκπαίδευση των χρηστών δεν θα πρέπει να περιορίζεται μόνο σε γενικά προγράμματα ευαισθητοποίησης, αλλά να περιλαμβάνει εξειδικευμένη ενημέρωση για τους κινδύνους που συνδέονται με κάθε είδος κοινωνικής επίθεσης. Με αυτόν τον τρόπο, οι συμμετέχοντες αποκτούν μια πιο ολοκληρωμένη εικόνα των πιθανών απειλών και των τρόπων πρόληψής τους, γεγονός που ενισχύει την ικανότητά τους να αναγνωρίζουν ύποπτες καταστάσεις και να αντιδρούν κατάλληλα, μειώνοντας την πιθανότητα να πέσουν θύματα επιθέσεων (Li et al., 2023; Syafitri et al., 2022).

Βασικό σημείο της εκπαίδευσης των χρηστών για την προστασία τους από διάφορες επιθέσεις είναι η δημιουργία ισχυρών και ασφαλών κωδικών πρόσβασης, καθώς και η εφαρμογή ασφαλών διαδικτυακών πρακτικών. Αυτό περιλαμβάνει την ασφαλή πλοήγηση στο διαδίκτυο, τον προσεκτικό χειρισμό των ηλεκτρονικών μηνυμάτων, και την ορθή χρήση των μέσων κοινωνικής δικτύωσης, όπως την αποφυγή κοινοποίησης προσωπικών πληροφοριών, τη διαχείριση των ρυθμίσεων απορρήτου, και την εφαρμογή δέουσας προσοχής σε αιτήματα φιλίας ή μηνύματα από αγνώστους (Chapagain et al., 2024).

Παράλληλα, στρατηγικές, όπως η τακτική υπενθύμιση και επιβεβαίωση των οδηγιών ασφαλείας, μπορούν να ενισχύσουν την εμπέδωση των καλών πρακτικών. Ωστόσο, είναι σημαντικό να διασφαλιστεί ότι τέτοιες διαδικασίες, όπως η μηνιαία υπογραφή υπομνημάτων, δεν εκτελούνται μηχανικά, χωρίς οι εργαζόμενοι να επεξεργάζονται το περιεχόμενο λόγω έλλειψης χρόνου ή κινήτρων. Για την αποτελεσματική εφαρμογή αυτής της στρατηγικής, απαιτείται η ενίσχυση της σημασίας της διαδικασίας μέσω θετικών κινήτρων ή ακόμα και μέσω σύντομων, στοχευμένων συνεδριών ανασκόπησης (targeted security awareness review sessions) (Saleem et al., 2017; Syafitri et al., 2022).

Η ευαισθητοποίηση γύρω από τις επιθέσεις κοινωνικής μηχανικής πρέπει να είναι ενδελεχής, λαμβάνοντας υπόψη τα δημογραφικά και συναισθηματικά χαρακτηριστικά των εργαζομένων, όπως η ηλικία, το φύλο και το γνωστικό επίπεδο ή η πανεπιστημιακή εκπαίδευση. Αυτές οι παράμετροι ενδέχεται να επηρεάσουν τη διαχείριση των απειλών, καθώς οι διαφορετικές ηλικιακές ομάδες μπορεί να έχουν διαφορετικές αντιλήψεις και αντιδράσεις απέναντι στις επιθέσεις. Για παράδειγμα, οι νεότεροι εργαζόμενοι μπορεί να είναι πιο εξοικειωμένοι με την τεχνολογία, αλλά και πιο επιρρεπείς σε κοινωνικές πιέσεις, ενώ οι μεγαλύτεροι μπορεί να διαθέτουν περισσότερη εμπειρία αλλά λιγότερη εξοικείωση με τις σύγχρονες απειλές. Εξίσου σημαντική είναι η ενσωμάτωση των πολιτισμικών, περιβαλλοντικών και ψυχολογικών παραμέτρων στις εκπαιδευτικές ενότητες, καθώς οι επιτιθέμενοι συχνά εκμεταλλεύονται τους παραπάνω παράγοντες για να εξαπολύσουν τις επιθέσεις τους (Beu et al., 2023; Matyokurehwa, 2022; Odeh, 2021).

Επιπλέον, η εκπαίδευση θα πρέπει να περιλαμβάνει πρακτικές ασκήσεις και σενάρια που να προσομοιώνουν τις πραγματικές συνθήκες επιθέσεων, καθώς αυτό βοηθά τους χρήστες να αποκτήσουν τις απαραίτητες δεξιότητες και την αυτοπεποίθηση για να διαχειριστούν τέτοιες καταστάσεις. Η εφαρμογή αυτών των στρατηγικών μπορεί να συμβάλει στην ενίσχυση της γενικής ασφάλειας της οργανωτικής δομής και στην ανάπτυξη μιας κουλτούρας προληπτικής στάσης απέναντι στις διαδικτυακές απειλές (Syafitri et al., 2022).

Η εφαρμογή πολιτικών ασφαλείας και η επαναλαμβανόμενη εκπαίδευση των εργαζομένων συμβάλλουν καθοριστικά στη δημιουργία ενός περιβάλλοντος εργασίας με υψηλή ασφάλεια, όπου οι χρήστες είναι σε θέση να εντοπίζουν, να απορρίπτουν και να αναφέρουν ύποπτες επικοινωνίες και ενέργειες (Estella, 2024; Hove, 2020; Saleem et al., 2017). Οι στρατηγικές εκπαίδευσης μπορούν να ενσωματώνουν καινοτόμες τεχνικές, όπως διαδραστικά εκπαιδευτικά εργαλεία, για την ευαισθητοποίηση γύρω από τις επιθέσεις, καθιστώντας την εμπειρία εκμάθησης διασκεδαστική και προσβάσιμη (Li et al., 2023).

4.4.2 Εξειδικευμένη Εκπαίδευση Χρηστών ανά Είδος Κοινωνικής Επίθεσης

Η εξειδικευμένη εκπαίδευση για συγκεκριμένες κοινωνικές επιθέσεις είναι αναγκαία ώστε οι χρήστες να είναι πλήρως προετοιμασμένοι για την αντιμετώπιση διαφορετικών τεχνικών κοινωνικής μηχανικής. Πιο αναλυτικά:

- **Phishing:**
    - **Σωστός χειρισμός email:** Οι χρήστες θα πρέπει να εκπαιδεύονται στον εντοπισμό ύποπτων email μέσω χαρακτηριστικών, όπως ορθογραφικά λάθη,

γενικόλογους χαιρετισμούς (π.χ. "Αγαπητέ χρήστη") και ασυνήθιστες διευθύνσεις αποστολέα (Odeh, 2021).

- **Εξάσκηση σε προσομοιώσεις:** Πραγματοποίηση προσομοιώσεων επιθέσεων phishing, όπου οι χρήστες καλούνται να αναγνωρίσουν και να αναφέρουν ύποπτα email (Odeh, 2021).
- **Εκπαίδευση για τη χρήση email clients:** Οδηγίες για τον τρόπο αναφοράς ύποπτων μηνυμάτων, τη χρήση φίλτρων ανεπιθύμητης αλληλογραφίας και τον έλεγχο των συνδέσμων πριν το κλικ (Odeh, 2021).

- **Dumpster Diving**:
  - **Καταστροφή εμπιστευτικών έντυπων πληροφοριών πριν την απόρριψή τους** (Odeh, 2021).
  - **Ασφαλής διαγραφή προσωπικών και εταιρικών δεδομένων** (όπως αρχεία χρηστών, κωδικοί, emails, οικονομικά στοιχεία) από ηλεκτρονικές συσκευές (Odeh, 2021).
- **Shoulder Surfing**:
  - Αποφυγή χρήσης ευαίσθητων στοιχείων σε δημόσιους χώρους, η εφαρμογή φίλτρων προστασίας οθόνης, η απενεργοποίηση του ήχου πληκτρολόγησης κατά την εισαγωγή ευαίσθητων δεδομένων, και η διακριτική πληκτρολόγηση κωδικών είναι πρακτικές προστασίας απέναντι σε τέτοιου είδους επιθέσεις (Zaoui et al., 2024).
- **Baiting**:
  - **Αναγνώριση ύποπτων συνδέσμων**: Οι χρήστες πρέπει να μαθαίνουν να ελέγχουν τις διευθύνσεις URL για ενδείξεις πλαστογράφησης (π.χ. παράξενες επεκτάσεις ή ανορθόγραφες διευθύνσεις) (Odeh, 2021).
  - **Ενημέρωση για ύποπτα αντικείμενα**: Εκπαίδευση για την αποφυγή χρήσης φυσικών αντικειμένων, όπως USB sticks, που βρίσκονται σε δημόσιους χώρους (Odeh, 2021).
- **Scareware**:
  - **Εκπαίδευση για την αναγνώριση ψεύτικων ειδοποιήσεων:** Παροχή παραδειγμάτων με ψεύτικα μηνύματα (π.χ. "Ο υπολογιστής σας έχει μολυνθεί") και οδηγίες για το πώς να αποφεύγουν οι χρήστες να εκφορτώνουν άγνωστα προγράμματα (Odeh, 2021).

- **Πρακτική ανάλυση περιστατικών:** Προσομοιώσεις όπου οι χρήστες καλούνται να αγνοήσουν ύποπτα αναδυόμενα παράθυρα και να ενημερώνουν την ομάδα IT (Odeh, 2021).

- **Phishing/Vishing/Smishing:**
  - **Οδηγίες για κλήσεις και μηνύματα**: Εκπαίδευση για την επαλήθευση της ταυτότητας καλούντων μέσω επιστροφής κλήσεων ή αναζήτησης επίσημων στοιχείων επικοινωνίας (Odeh, 2021).
  - **Ασφάλεια συνημμένων αρχείων:** Οι χρήστες θα πρέπει να μαθαίνουν να χρησιμοποιούν λογισμικό προστασίας από ιούς για τον έλεγχο συνημμένων και να αποφεύγουν το άνοιγμα των αρχείων από άγνωστες πηγές (Odeh, 2021).
- **Honey Trap**:
  - **Συγκεκριμένες οδηγίες:** Οι χρήστες πρέπει να μαθαίνουν να αναγνωρίζουν ύποπτες προσεγγίσεις που εκμεταλλεύονται προσωπικά τους ενδιαφέροντα ή αδυναμίες. Η εκπαίδευση μπορεί να περιλαμβάνει ανάλυση πραγματικών περιπτώσεων και τρόπους αποφυγής επικοινωνίας με άγνωστα άτομα που προσπαθούν να δημιουργήσουν σχέσεις εμπιστοσύνης (NIELIT Patna, 2024; Yawar, 2024b).
- **Cybergrooming**:
  - **Οδηγίες για την προστασία των ανήλικων:** Οι χρήστες θα πρέπει να εκπαιδεύονται να αναγνωρίζουν ύποπτες συνομιλίες και να χρησιμοποιούν εργαλεία αναφοράς ακατάλληλου περιεχομένου σε πλατφόρμες κοινωνικής δικτύωσης (Syafitri et al., 2022; ENISA, 2011).
  - **Προώθηση ενεργής επικοινωνίας:** Εκπαίδευση των γονέων και εκπαιδευτικών για την αναγνώριση αλλαγών στη συμπεριφορά των παιδιών που μπορεί να συνδέονται με τέτοιες επιθέσεις (Guo et al., 2023).

4.4.3 Μέθοδοι Εκπαίδευσης για την Αντιμετώπιση των Επιθέσεων

Η εκπαίδευση για την αντιμετώπιση επιθέσεων κοινωνικής μηχανικής αποτελεί θεμελιώδες στοιχείο της στρατηγικής κυβερνοασφάλειας κάθε οργανισμού. Η αποτελεσματική προστασία απαιτεί μια πολύπλευρη προσέγγιση που συνδυάζει διαφορετικές εκπαιδευτικές μεθόδους, καθώς καμία μεμονωμένη προσέγγιση δεν μπορεί να καλύψει όλες τις πτυχές της απειλής. Οι σύγχρονες μέθοδοι εκπαίδευσης για την αντιμετώπιση αυτών των επιθέσεων εξελίσσονται διαρκώς, προσαρμοζόμενες στις νέες απειλές και τεχνικές που αναπτύσσουν οι κακόβουλοι

χρήστες. Η επιτυχημένη εκπαίδευση συνδυάζει παραδοσιακές, διαδραστικές και ψηφιακές μεθόδους, δημιουργώντας ένα ολοκληρωμένο πλαίσιο μάθησης και ευαισθητοποίησης.

4.4.3.1 Παραδοσιακές Μέθοδοι Εκπαίδευσης

Οι παραδοσιακές μέθοδοι εκπαίδευσης αποτελούν το θεμέλιο κάθε εκπαιδευτικού προγράμματος κυβερνοασφάλειας. Περιλαμβάνουν δομημένες διαλέξεις, σεμινάρια, παρουσιάσεις και έντυπο εκπαιδευτικό υλικό, που παρέχουν το θεωρητικό υπόβαθρο και τις βασικές γνώσεις για την κατανόηση των επιθέσεων τέτοιου τύπου. Οι εκπαιδευτές παρουσιάζουν αναλυτικά τις διάφορες τεχνικές επίθεσης, τα χαρακτηριστικά τους και τις μεθόδους αναγνώρισης και αντιμετώπισής τους.

Η πρακτική εξάσκηση με μελέτες περιπτώσεων αποτελεί αναπόσπαστο κομμάτι της παραδοσιακής εκπαίδευσης. Οι εκπαιδευόμενοι αναλύουν πραγματικά περιστατικά επιθέσεων, κατανοώντας τις τεχνικές που χρησιμοποιήθηκαν, τα σημεία αστοχίας στην άμυνα και τις βέλτιστες πρακτικές αντιμετώπισης. Αυτή η προσέγγιση βοηθά στην ανάπτυξη κριτικής σκέψης και αναλυτικών ικανοτήτων (Hove, 2020; Odeh et al., 2021).

4.4.3.2 Διαδραστικές Μέθοδοι

Οι εργαστηριακές ασκήσεις προσφέρουν hands-on εμπειρία στην αναγνώριση και αντιμετώπιση επιθέσεων κοινωνικής μηχανικής. Σε ειδικά διαμορφωμένα εργαστήρια, οι εκπαιδευόμενοι εξασκούνται στη χρήση εργαλείων και τεχνικών ασφαλείας, αναλύουν ύποπτα μηνύματα και εφαρμόζουν πρωτόκολλα ασφαλείας σε πραγματικό χρόνο.

Τα role-playing scenarios αποτελούν μια ιδιαίτερα αποτελεσματική μέθοδο εκπαίδευσης, όπου οι συμμετέχοντες υποδύονται διαφορετικούς ρόλους σε σενάρια επιθέσεων κοινωνικής μηχανικής. Αυτή η προσέγγιση βοηθά στην κατανόηση τόσο της οπτικής του επιτιθέμενου όσο και του θύματος, ενώ παράλληλα αναπτύσσει τις επικοινωνιακές δεξιότητες και την ετοιμότητα αντίδρασης των εκπαιδευομένων.

Οι ομαδικές συζητήσεις και η ανάλυση περιστατικών προωθούν την ανταλλαγή εμπειριών και γνώσεων μεταξύ των συμμετεχόντων. Μέσω της συλλογικής ανάλυσης πραγματικών περιστατικών, οι εκπαιδευόμενοι μαθαίνουν από τα λάθη και τις επιτυχίες άλλων, ενώ αναπτύσσουν κριτική σκέψη και ικανότητες επίλυσης προβλημάτων (Baki et al., 2017; Sam, 2024; Wang et al.,2021).

Οι προσομοιώσεις πραγματικών σεναρίων επίθεσης επιτρέπουν στους εκπαιδευόμενους να εξασκηθούν σε ένα ελεγχόμενο εικονικό περιβάλλον. Μέσω προσεκτικά σχεδιασμένων σεναρίων, οι συμμετέχοντες καλούνται να αναγνωρίσουν και να

αντιμετωπίσουν τυπικές επιθέσεις κοινωνικής μηχανικής, αποκτώντας πρακτική εμπειρία χωρίς τους κινδύνους μιας πραγματικής επίθεσης (Hove, 2020; Odeh et al., 2021). Για παράδειγμα, η αποστολή εικονικών phishing emails επιτρέπει στους εργαζομένους να εξοικειώνονται με πραγματικά σενάρια και να αναγνωρίζουν τις ενδείξεις κακόβουλων πρακτικών. Τα δεδομένα που συλλέγονται, όπως το ποσοστό κλικαρίσματος και ο χρόνος αντίδρασης, μπορούν να χρησιμοποιηθούν για τη βελτίωση των εκπαιδευτικών προγραμμάτων (Matyokurehwa, 2022; Syafitri et al., 2022).

4.4.3.3 Ψηφιακές Μέθοδοι Εκπαίδευσης

Οι ψηφιακές μέθοδοι εκπαίδευσης αξιοποιούν σύγχρονες τεχνολογίες για την παροχή διαδραστικής και εξατομικευμένης μάθησης. Πλατφόρμες ηλεκτρονικής μάθησης, προσομοιώσεις επιθέσεων και εικονικά περιβάλλοντα εκπαίδευσης επιτρέπουν στους εκπαιδευόμενους να εξασκούνται με το δικό τους ρυθμό και να λαμβάνουν άμεση ανατροφοδότηση.

Η παιχνιδοποίηση (gamification) αποτελεί μια καινοτόμο προσέγγιση στην ψηφιακή εκπαίδευση, όπως φαίνεται από την περίπτωση του "PhishI" και άλλων παρόμοιων εφαρμογών. Αυτές οι πλατφόρμες συνδυάζουν στοιχεία παιχνιδιού με εκπαιδευτικό περιεχόμενο, καθιστώντας τη μάθηση πιο ελκυστική και αποτελεσματική (Yasin et al., 2020).

Μεταξύ των σύγχρονων ψηφιακών μεθόδων εκπαίδευσης, ξεχωρίζει η έρευνα των Yasin και συν. (2024) που παρουσιάζει μία καινοτόμο προσέγγιση μέσω παιχνιδοποίησης (gamification). Συγκεκριμένα, ανέπτυξαν το "PhishI", ένα ψηφιακό παιχνίδι που αξιοποιεί την ταξινόμηση Bloom ως ένα από τα παιδαγωγικά του εργαλεία. Το παιχνίδι λειτουργεί ως διαδικτυακή εφαρμογή και ενσωματώνει σύγχρονα τεχνολογικά στοιχεία, όπως QR codes, παράλληλα με άλλες εκπαιδευτικές τεχνικές.

Η μεθοδολογία του παιχνιδιού περιλαμβάνει διάφορα εκπαιδευτικά εργαλεία, συμπεριλαμβανομένου ενός συστήματος καρτών (Attack, Rules, Psychology), το οποίο λειτουργεί συμπληρωματικά με άλλες μεθόδους πρακτικής εξάσκησης. Η προσέγγιση αυτή συνδυάζεται με παραδοσιακές μεθόδους εκπαίδευσης και διαδραστικές τεχνικές για μέγιστη αποτελεσματικότητα.

Η συνεχής εξέλιξη των ψηφιακών τεχνολογιών επιτρέπει την ανάπτυξη όλο και πιο εξελιγμένων εκπαιδευτικών εργαλείων, συμπεριλαμβανομένων συστημάτων προσομοίωσης βασισμένων σε τεχνητή νοημοσύνη και εικονική πραγματικότητα. Αυτές οι τεχνολογίες προσφέρουν ρεαλιστικές εμπειρίες εκπαίδευσης και δυνατότητες προσαρμογής στις ατομικές ανάγκες κάθε εκπαιδευόμενου.

4.5. Τεχνικά Μέτρα Προστασίας

Η προστασία από επιθέσεις κοινωνικής μηχανικής απαιτεί συνδυασμό γενικών μέτρων ασφάλειας, εξειδικευμένων τεχνικών και πολιτικών ευαισθητοποίησης των χρηστών. Στην παρούσα ενότητα παρουσιάζονται τόσο γενικά όσο και εξειδικευμένα μέτρα για την πρόληψη και ανίχνευση τέτοιων επιθέσεων, εμπλουτισμένα με πρόσθετες πληροφορίες και πηγές από την έρευνα.

4.5.1 Γενικά Μέτρα Προστασίας

Τα παρακάτω μέτρα αποτελούν θεμέλια για την ασφάλεια πληροφοριών και, παρότι δεν στοχεύουν αποκλειστικά την κοινωνική μηχανική, συνεισφέρουν στη συνολική προστασία:

- **Ισχυροί κωδικοί πρόσβασης**: Οι χρήστες πρέπει να υιοθετούν κωδικούς μεγάλης πολυπλοκότητας που περιλαμβάνουν γράμματα, αριθμούς και σύμβολα, με τακτική ανανέωση τους. Οι οργανισμοί μπορούν να επιβάλουν τέτοιες πρακτικές μέσω πολιτικών ασφαλείας (Chinta et al., 2016).
- **Πολυπαραγοντική ταυτοποίηση (MFA):** Ο συνδυασμός μεθόδων ταυτοποίησης, όπως κάρτες πρόσβασης, κωδικοί μίας χρήσης (OTP: One Time Password) και βιομετρικά δεδομένα (π.χ. δακτυλικό αποτύπωμα), μειώνει δραστικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης (Estella, 2024).
- **Ενημερώσεις λογισμικού και εφαρμογή επιθεμάτων (patches):** Η τακτική ενημέρωση λογισμικού διασφαλίζει ότι κενά ασφαλείας, που μπορεί να εκμεταλλευτούν οι επιτιθέμενοι, αντιμετωπίζονται εγκαίρως (Syafitri et al., 2022).
- **Κρυπτογράφηση δεδομένων:** Η χρήση τεχνολογιών, όπως VPNs (Virtual Private Networks), PGP (Pretty Good Privacy) και S/MIME (Secure Multipurpose Internet Mail Extensions) προστατεύει την ιδιωτικότητα της επικοινωνίας, ιδιαίτερα σε απομακρυσμένες συνδέσεις (Chapagain et al., 2024).
- **Firewalls και συστήματα ανίχνευσης και προστασίας εισβολών (IDS/IPS):** Τα τείχη προστασίας καθώς και τα εργαλεία IDS (Intrusion Detection Systems) και IPS (Intrusion Protection Systems) εντοπίζουν και αποτρέπουν ύποπτη δραστηριότητα στο δίκτυο, ενισχύοντας την ασφάλεια (Washo, 2021).
- **Διαχωρισμός δικτύου (network segmentation):** Η οργάνωση των δικτύων σε επιμέρους τμήματα και η περιορισμένη πρόσβαση σε εξουσιοδοτημένα άτομα μειώνει τον κίνδυνο εκτεταμένων παραβιάσεων (Chinta et al., 2016).

4.5.2 Εξειδικευμένα Μέτρα Προστασίας ανά Είδος Επίθεσης

Παρακάτω παρουσιάζονται ειδικά μέτρα για την πρόληψη των κυριότερων ειδών των επιθέσεων κοινωνικής μηχανικής:

- **Προστασία από επιθέσεις phishing**
    - **SPF, DKIM και DMARC:** Τα πρωτόκολλα αυτά επαληθεύουν την ταυτότητα του αποστολέα, περιορίζοντας τις πιθανότητες επιτυχίας πλαστών emails (Asante, 2022).
    - **Ανάλυση λογοτύπων και διευθύνσεων URL**: Οι χρήστες θα πρέπει να αναγνωρίζουν ύποπτα emails, όπως μηνύματα με ορθογραφικά λάθη ή παραπλανητικούς συνδέσμους. Προς διευκόλυνσή τους, η αυτόματη ανάλυση λογοτύπων και διευθύνσεων URL μπορεί να αυξήσει την αποτελεσματικότητα ανίχνευσης κατά 97%-98% (Minocha & Singh, 2022). Για την επίτευξη αυτού του στόχου, μπορούν να χρησιμοποιηθούν τεχνικές μηχανικής μάθησης, όπως η αναγνώριση προτύπων εικόνας και η χρήση συνελικτικών νευρωνικών δικτύων (CNNs: Convolutional Neural Networks) για την ταξινόμηση λογοτύπων και τον εντοπισμό πλαστών ιστότοπων (Kulkarni, 2023).
    - **Ανάλυση περιεχομένου emails**: Εξειδικευμένα εργαλεία εντοπίζουν κακόβουλα URL ή συνημμένα αρχεία (Saleem et al., 2017), χρησιμοποιώντας τεχνικές όπως η ανάλυση φυσικής γλώσσας (NLP: Natural Language Processing) για την αναγνώριση ύποπτων λέξεων-κλειδιών και η μηχανική μάθηση (ML: Machine Learning) για την ταξινόμηση ύποπτων μηνυμάτων (Buber et al., 2008).
- **Προστασία από baiting**
    - **Πολιτική περιορισμένης πρόσβασης**: Οι εξωτερικές συσκευές (π.χ. USB drives) θα πρέπει να σαρώνονται αυτόματα για κακόβουλο λογισμικό πριν χρησιμοποιηθούν.
    - **Απομόνωση συστημάτων**: Η χρήση sandboxing (απομόνωσης εκτέλεσης) για την εκτέλεση ύποπτων αρχείων αποτρέπει τη διάδοση κακόβουλου λογισμικού (Salahdine & Kaabouch, 2019). Αυτό μπορεί να γίνει σε συνδυασμό με το διαχωρισμό δικτύου και την αποτροπή διάδοσης της μόλυνσης σε ένα τμήματα του δικτύου/συστήματος.
- **Προστασία από scareware**
    - **Αυτόματη ανίχνευση απειλών:** Τεχνολογίες, όπως το CryptoDrop, ειδοποιούν για ύποπτες ενέργειες και αποτρέπουν την εγκατάσταση κακόβουλου

λογισμικού (Saleem et al., 2017). Το CryptoDrop μπορεί να χαρακτηριστεί ως σύστημα ανίχνευσης απειλών (Threat Detection System) που χρησιμοποιεί μηχανική μάθηση για την αναγνώριση και παρεμπόδιση ransomware επιθέσεων, λειτουργώντας συμπληρωματικά με τα παραδοσιακά συστήματα IDS/IPS (Maigida et al., 2019).

- **Sandboxing και αντικά προγράμματα**: Η απομόνωση ύποπτων προγραμμάτων μέσω sandboxing και η χρήση αντικών προγραμμάτων περιορίζει τη διάδοσή τους (Salahdine & Kaabouch, 2019).

- **Προστασία από tailgating**
  - **Φυσικός έλεγχος πρόσβασης:** Οι εγκαταστάσεις πρέπει να χρησιμοποιούν κάρτες πρόσβασης, τουρνικέ ή βιομετρικά συστήματα (Li et al., 2023).
  - **Άμεση Ανάλυση Βίντεο (Live video analytics):** Τεχνολογίες ανίχνευσης εικόνας/βίντεο μπορούν να εντοπίζουν άμεσα μη εξουσιοδοτημένη είσοδο.
- **Προστασία από watering hole attacks**
  - **Web filtering:** Το φιλτράρισμα ιστοσελίδων αποτρέπει την πρόσβαση σε ύποπτους ιστότοπους.
  - **Ανάλυση συμπεριφοράς χρηστών:** Εργαλεία ανίχνευσης εντοπίζουν μη φυσιολογική δραστηριότητα, όπως παρεκκλίσεις στη συμπεριφορά περιήγησης των χρηστών ή αλλαγές στο περιεχόμενο των ιστοτόπων, που μπορεί να υποδηλώνουν επίθεση τύπου watering hole (Amato et al., 2021).

4.5.3 Χρήση Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης

Η τεχνητή νοημοσύνη (AI: Artificial Intelligence) και η μηχανική μάθηση παίζουν καθοριστικό ρόλο στην ανίχνευση επιθέσεων κοινωνικής μηχανικής:

- **Ανάλυση μη φυσιολογικής συμπεριφοράς:** Τα μοντέλα ML εντοπίζουν ύποπτη δραστηριότητα χρηστών ή συσκευών (Mao et al., 2018). Παράλληλα, μπορούν να χρησιμοποιηθούν και για την ανάλυση του περιεχομένου των ιστοτόπων, την ανίχνευση phishing emails, πλαστών διευθύνσεων ιστοτόπων, την ανάλυση λογοτύπων και κακόβουλου λογισμικού.
- **Υβριδικές λύσεις:** Ο συνδυασμός ML και παραδοσιακών τεχνικών (π.χ. κανόνες βάσει υπογραφών) αυξάνει την ακρίβεια (Alani & Tawfik, 2022). Το ίδιο ισχύει και με το συνδυασμό διαφορετικών τεχνικών ML (πχ. εποπτευόμενη ταξινόμηση/κατάταξη & νευρωνικά δίκτυα)

- **Εξατομικευμένη ανίχνευση:** Η AI προσαρμόζεται στα πρότυπα συμπεριφοράς ενός οργανισμού, εντοπίζοντας αποκλίσεις (Al-Sarem et al., 2021).

Τα μέτρα προστασίας από επιθέσεις κοινωνικής μηχανικής πρέπει να περιλαμβάνουν τόσο τεχνολογικές λύσεις όσο και εκπαίδευση των χρηστών. Η συνδυαστική προσέγγιση ενισχύει την άμυνα ενός οργανισμού απέναντι σε αυτές τις απειλές, ενώ η χρήση σύγχρονων τεχνολογιών, όπως η AI και το sandboxing, αποτελεί απαραίτητο εργαλείο προστασίας έναντι κακόβουλων ενεργειών.

4.6. Αξιολόγηση και Διαχείριση Κινδύνων

Η αξιολόγηση και διαχείριση των κινδύνων που σχετίζονται με τις επιθέσεις κοινωνικής μηχανικής αποτελεί ζωτικής σημασίας διαδικασία για την ενίσχυση της ανθεκτικότητας των οργανισμών. Οι απειλές αυτού του είδους στοχεύουν όχι μόνο τεχνικές αδυναμίες, αλλά κυρίως το ανθρώπινο στοιχείο, αξιοποιώντας ψυχολογικές τεχνικές χειραγώγησης. Ολοκληρωμένα πλαίσια και εργαλεία, όπως οι δοκιμές συμμόρφωσης, οι δοκιμές διείσδυσης, η ανάλυση μέσω γραφημάτων και οι προσομοιώσεις επιθέσεων, συνδυάζονται για την κατανόηση των ευπαθειών και την ανάπτυξη αποτελεσματικών στρατηγικών αντιμετώπισης.

Παράλληλα, η δημιουργία κουλτούρας ασφάλειας και η συστηματική εκπαίδευση του προσωπικού συμβάλλουν καθοριστικά στη μείωση του ρίσκου. Η αποτελεσματική αξιολόγηση κινδύνων απαιτεί τη διαρκή αναθεώρηση των διαδικασιών, την προσαρμογή στις εξελισσόμενες απειλές και τη διασφάλιση της συνέχειας λειτουργίας μέσω ολοκληρωμένων σχεδίων αποκατάστασης.

4.6.1 Ανίχνευση & Αναγνώριση Ρίσκου

Η ανίχνευση και αναγνώριση κινδύνων αποτελεί το πρώτο και κρίσιμο βήμα για την πρόληψη επιθέσεων κοινωνικής μηχανικής. Οι οργανισμοί πρέπει να αξιοποιούν εξειδικευμένα εργαλεία και δομημένες μεθοδολογίες, όπως (Edwards et al., 2017; Heartfield et al., 2022):

- **Δοκιμές συμμόρφωσης (compliance audits**): Εντοπίζουν τεχνικές και διαδικαστικές αδυναμίες που μπορούν να αξιοποιηθούν από επιτιθέμενους.
- **Δοκιμές διείσδυσης (penetration testing):** Όταν προσαρμόζονται σε σενάρια κοινωνικής μηχανικής, περιλαμβάνουν προσομοιώσεις επιθέσεων phishing, pretexting και baiting. Αυτές βοηθούν στην αποκάλυψη ευπαθειών τόσο στα τεχνικά συστήματα όσο και στις διαδικασίες και στην εκπαίδευση του ανθρώπινου δυναμικού.

Το πλαίσιο SERA (Social Engineering Risk Assessment) προσφέρει μια δομημένη μεθοδολογία που εστιάζει στην κατανόηση των ψυχολογικών τεχνικών χειραγώγησης και στην

αξιολόγηση της αποτελεσματικότητας των αντιμέτρων (Salahdine & Kaabouch, 2019). Παράλληλα, η μεθοδολογία SEPTA (Social Engineering Penetration Testing Approach) παρέχει ένα σαφές μοντέλο για την προσομοίωση επιθέσεων και την αξιολόγηση της ανθεκτικότητας των οργανισμών (Li et al., 2022).

Ένα από τα πιο ευρέως χρησιμοποιούμενα εργαλεία είναι το πλαίσιο MITRE ATT&CK, το οποίο χαρτογραφεί τακτικές, τεχνικές και διαδικασίες (TTPs: Tactics, Techniques, and Procedures) που χρησιμοποιούνται σε επιθέσεις κοινωνικής μηχανικής. Το MITRE ATT&CK παρέχει στους οργανισμούς τη δυνατότητα να εντοπίζουν αδυναμίες στις υφιστάμενες δομές ασφαλείας και να αναπτύσσουν στοχευμένες στρατηγικές προστασίας, ενώ ενημερώνεται συνεχώς με νέες απειλές και τεχνικές (MITRE Corporation, 2024).

4.6.2 Ανάλυση Ρίσκου

Η ανάλυση κινδύνων περιλαμβάνει τη λεπτομερή διερεύνηση των πιθανών διαδρομών επίθεσης, την κατανόηση των παραγόντων που επηρεάζουν την επιτυχία των επιθέσεων και την ποσοτικοποίηση των κινδύνων. Οι οργανισμοί καλούνται να συνδυάσουν την ανάλυση τεχνικών ευπαθειών με την εξέταση της ανθρώπινης συμπεριφοράς και της ψυχολογίας, χρησιμοποιώντας προηγμένα μοντέλα και μεθόδους, όπως:

- **Μοντέλα ανάλυσης επιθέσεων μέσω γραφημάτων:** Το μοντέλο των Beckers et al. (2022) ενσωματώνει τεχνικές, κοινωνικές και οργανωτικές παραμέτρους, παρέχοντας μια πιο ολοκληρωμένη εικόνα της δυναμικής των επιθέσεων.
- **Προβλεπτικές μέθοδοι:** Η χρήση Bayesian ανάλυσης επιτρέπει την πρόβλεψη συμπεριφορών υψηλού κινδύνου και τη βελτίωση της στρατηγικής πρόληψης (Salahdine & Kaabouch, 2019).
- **Δυναμικά μοντέλα προσομοίωσης**: Όπως αυτά που προτείνουν οι Abri et al. (2022), βοηθούν στην κατανόηση της εξέλιξης των επιθέσεων και στη διαμόρφωση στρατηγικών μετριασμού.

Η αξιολόγηση κινδύνων δεν είναι στατική διαδικασία. Οι οργανισμοί πρέπει να χαρτογραφούν τα κρίσιμα περιουσιακά τους στοιχεία και να υπολογίζουν τη δυνητική επίδραση των απειλών. Ειδικότερα, η ανάλυση των τρωτών σημείων πρέπει να εστιάζει στις ανθρώπινες αδυναμίες, καθώς αυτές συχνά αποτελούν τον πιο ευάλωτο κρίκο στην αλυσίδα ασφαλείας (Hove, 2020; Syafitri et al., 2022).

4.6.3 Αντιμετώπιση Ρίσκου / Περιστατικών

Η αποτελεσματική αντιμετώπιση περιστατικών κοινωνικής μηχανικής απαιτεί μια σαφώς δομημένη προσέγγιση που περιλαμβάνει τις παρακάτω φάσεις:

1. **Προετοιμασία**: Η ύπαρξη ενός ολοκληρωμένου σχεδίου αποκατάστασης καταστροφών (DRP: Disaster Recovery Plan) είναι απαραίτητη για τη διασφάλιση της επιχειρησιακής συνέχειας. Το DRP πρέπει να περιλαμβάνει ειδικές οδηγίες για την αντιμετώπιση όλων των τύπων των επιθέσεων της κοινωνικής μηχανικής (Chapagain et al., 2024; Chinta et al., 2016).
2. **Ανίχνευση και Περιορισμός**: Τα σύγχρονα συστήματα ανίχνευσης εισβολών (IDS/IPS) αξιοποιούν μηχανική μάθηση για την ανάλυση ύποπτων προτύπων και την αυτόματη ανταπόκριση στις απειλές (Washo, 2021). Ωστόσο, η αποδοτικότητα αυτών των συστημάτων δεν είναι πάντα αρκετή. Επιπλέον, απαιτούνται και άλλα αντίμετρα, όπως αντιβιοτικά λογισμικά για την αντιμετώπιση κακόβουλου λογισμικού και προγράμματα DLP (Data Leakage Protection) για την αποτροπή διαρροής δεδομένων. Ο οργανισμός θα πρέπει να προτεραιοποιεί τα διαθέσιμα αντίμετρα, εφαρμόζοντας εκείνα που μειώνουν σημαντικά τους κινδύνους και είναι εντός του προβλεπόμενου προϋπολογισμού της εταιρείας/οργανισμού (Herrera Montano et al., 2022).
3. **Αποκατάσταση**: Η γρήγορη ανάκτηση δεδομένων από ασφαλή αντίγραφα και η εφαρμογή διορθωτικών μέτρων, όπως η άμεση αλλαγή κωδικών πρόσβασης, μειώνουν τις επιπτώσεις των επιθέσεων (Li et al., 2023).

Μετά από κάθε περιστατικό, η post-incident analysis (ανάλυση μετά το συμβάν/περιστατικό) περιλαμβάνει εγκληματολογική ανάλυση (forensic analysis), την καταγραφή του χρονοδιαγράμματος της επίθεσης και την αξιολόγηση της αποτελεσματικότητας των μέτρων αντιμετώπισης. Αυτή η διαδικασία ενισχύει τις στρατηγικές άμυνας και προσαρμόζει τα αντίμετρα στις νεότερες απειλές.

Παράλληλα, η εκπαίδευση του προσωπικού είναι κρίσιμη για την αναγνώριση και αναφορά ύποπτων δραστηριοτήτων. Οι οργανισμοί οφείλουν να προάγουν την κουλτούρα ασφάλειας, ενθαρρύνοντας τη συμμετοχή όλων των επιπέδων διοίκησης στη διαχείριση κινδύνων.

Τέλος, η συνεργασία με εξειδικευμένους φορείς και κοινότητες ανταλλαγής πληροφοριών, όπως τα Information Sharing and Analysis Centers (ISACs) (Κέντρα Διαμοιρασμού & Ανάλυσης Πληροφοριών Ασφαλείας), προσφέρει πολύτιμη υποστήριξη για την αντιμετώπιση σύνθετων επιθέσεων. Η συνεχής ενημέρωση των πολιτικών ασφαλείας και

η προσαρμογή τους στις εξελισσόμενες απειλές παραμένουν βασικοί παράγοντες για την ενίσχυση της ανθεκτικότητας (Syafitri et al., 2022; Hove, 2020).

5. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

Η προστασία από επιθέσεις κοινωνικής μηχανικής απαιτεί μια πολυδιάστατη προσέγγιση, συνδυάζοντας τεχνικά μέτρα, εκπαίδευση των χρηστών καθώς και οργανωτικές πολιτικές και διαδικασίες. Η σύγχρονη ψηφιακή εποχή χαρακτηρίζεται από την αυξανόμενη πολυπλοκότητα των κυβερνοεπιθέσεων, με τις επιθέσεις κοινωνικής μηχανικής να αποτελούν μία από τις πιο επικίνδυνες απειλές για την ασφάλεια των οργανισμών. Η ανάγκη για επένδυση των οργανισμών στην εκπαίδευση και ευαισθητοποίηση των χρηστών, την ανάπτυξη πρωτοκόλλων ασφαλείας και τη διατήρηση μιας ισχυρής κουλτούρας ασφάλειας καθίσταται πλέον επιτακτική.

Η ραγδαία εξέλιξη της τεχνολογίας και η αυξανόμενη διασύνδεση των συστημάτων έχουν δημιουργήσει ένα περίπλοκο περιβάλλον όπου οι παραδοσιακές μέθοδοι προστασίας δεν επαρκούν. Οι επιτιθέμενοι αξιοποιούν όλο και πιο εξελιγμένες τεχνικές, συνδυάζοντας ψυχολογικούς χειρισμούς με τεχνολογικά εργαλεία, καθιστώντας τις επιθέσεις κοινωνικής μηχανικής ιδιαίτερα δύσκολες στην ανίχνευση και αντιμετώπιση.

Οι πιο αποτελεσματικές μέθοδοι αντιμετώπισης ενσωματώνουν ένα ολοκληρωμένο συνδυασμό στρατηγικών για την καταπολέμηση των επιθέσεων κοινωνικής μηχανικής. Σύμφωνα με εκτενείς έρευνες, οι συνδυαστικές μέθοδοι που περιλαμβάνουν εκπαιδευτικά προγράμματα και αυστηρές πολιτικές ασφαλείας έχουν αποδειχθεί σημαντικά αποτελεσματικότερες σε σχέση με τα μεμονωμένα τεχνικά μέτρα (Saleem et al., 2017).

Το τελευταίο κεφάλαιο της εργασίας οργανώνεται σε τρεις διακριτές υποενότητες, κάθε μία εκ των οποίων καλύπτει διαφορετική πτυχή της ανάλυσης και των προτάσεων που σχετίζονται με τις επιθέσεις κοινωνικής μηχανικής.

Η πρώτη Ενότητα (5.1. Σύνοψη Ευρημάτων), παρέχει μια συνοπτική παρουσίαση των κεντρικών συμπερασμάτων της έρευνας, εστιάζοντας στις βασικές προκλήσεις και αδυναμίες που εντοπίστηκαν μέσω της ανάλυσης της βιβλιογραφίας και των ερευνητικών δεδομένων. Η έρευνα καταδεικνύει τρεις θεμελιώδεις άξονες που είναι κρίσιμοι για την επιτυχή άμυνα κατά των επιθέσεων κοινωνικής μηχανικής.

Η δεύτερη Ενότητα (5.2. Οδηγίες και Στρατηγικές Βελτίωσης της Προστασίας από Επιθέσεις Κοινωνικής Μηχανικής) περιλαμβάνει συγκεκριμένες, πρακτικές προτάσεις που μπορούν να εφαρμοστούν από οργανισμούς για την ισχυροποίηση της προστασίας απέναντι στις επιθέσεις κοινωνικής μηχανικής. Η έμφαση δίνεται τόσο σε τεχνολογικές όσο και σε εκπαιδευτικές λύσεις, προσαρμοσμένες στις ανάγκες του σύγχρονου περιβάλλοντος απειλών.

Η τρίτη Ενότητα (5.3. Κατευθύνσεις για Μελλοντική Έρευνα) ασχολείται με την προοπτική περαιτέρω ερευνών. Περιγράφονται πιθανές κατευθύνσεις για την ανάπτυξη νέων εργαλείων και στρατηγικών, όπως και η ανάγκη για μελέτη διαφορετικών παραμέτρων που επηρεάζουν την αποτελεσματικότητα των μεθόδων αντιμετώπισης.

5.1. Σύνοψη Ευρημάτων

Η εμπεριστατωμένη ανάλυση της βιβλιογραφίας και των ερευνητικών δεδομένων ανέδειξε τρεις θεμελιώδεις άξονες που είναι κρίσιμοι για την αποτελεσματική αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής.

Πρώτον, οι κίνδυνοι στον τομέα της πληροφορικής παραμένουν μια διαρκής απειλή. Οι επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται πρωτίστως την ανθρώπινη αδυναμία, κάτι που τονίστηκε εκτενώς στην υποενότητα 3.1.2 («Παράγοντες επιτυχίας των επιθέσεων»), στην οποία αναλύθηκε η προδιάθεση των ανθρώπων σε ψυχολογικούς χειρισμούς. Η κατανόηση αυτής της παραμέτρου είναι κρίσιμη για τη διαμόρφωση στρατηγικών προστασίας που εστιάζουν τόσο στην πρόληψη όσο και στη μείωση της επίπτωσης τέτοιων επιθέσεων.

Δεύτερον, η ευαισθητοποίηση και εκπαίδευση του προσωπικού αναδεικνύεται ως ακρογωνιαίος λίθος για την ασφάλεια των οργανισμών. Όπως αναφέρθηκε στις Ενότητες 4.4 («Εκπαίδευση & Ευαισθητοποίηση Χρηστών») και 4.5 («Τεχνικά Μέτρα Προστασίας»), η συνεχής εκπαίδευση των χρηστών, σε συνδυασμό με τη χρήση εξειδικευμένων εργαλείων προστασίας, ενισχύει την προετοιμασία και την ανθεκτικότητα των οργανισμών απέναντι σε κοινωνικούς μηχανισμούς.

Τρίτον, η ανάπτυξη ανθεκτικών οργανωτικών πολιτικών, όπως παρουσιάστηκε στην Ενότητα 4.2 («Οργανωτικές Πολιτικές και Διαδικασίες») και η διαχείριση ρίσκου (βλ. Ενότητα 4.6. Αξιολόγηση και Διαχείριση Κινδύνων) καθίστανται απαραίτητες. Οι οργανισμοί οφείλουν να υιοθετούν ευέλικτες πολιτικές ασφαλείας και να εφαρμόζουν συστηματική και συνεχιζόμενη διαχείριση κινδύνου (Risk Management), που περιλαμβάνει την αναγνώριση, την αξιολόγηση και τη μετρίαση των πιθανών απειλών.

Η εμπειρία από την εφαρμογή των διαφόρων μέτρων προστασίας καταδεικνύει ότι η επιτυχής αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής προϋποθέτει μια ολιστική προσέγγιση που εκτείνεται πέρα από τα στενά όρια της τεχνολογίας. Η ανθρώπινη συμπεριφορά και η οργανωσιακή κουλτούρα διαδραματίζουν εξίσου σημαντικό ρόλο με τα τεχνικά μέτρα προστασίας. Αυτά τα συμπεράσματα επιβεβαιώνουν την ανάγκη για πολυδιάστατες στρατηγικές που συνδυάζουν την τεχνολογία, την ανθρώπινη εκπαίδευση και

την οργανωσιακή προσαρμογή, ώστε να επιτευχθεί μια ισχυρή και ανθεκτική ασπίδα απέναντι στις σύγχρονες απειλές.

5.2. Οδηγίες και Στρατηγικές Βελτίωσης της Προστασίας από Επιθέσεις Κοινωνικής Μηχανικής

Με βάση τα ευρήματα της έρευνας, προτείνεται ένα ολοκληρωμένο πλαίσιο εφαρμογής της προστασίας έναντι των επιθέσεων κοινωνικής μηχανικής, το οποίο συνδυάζει τεχνολογικά εργαλεία, εκπαιδευτικές πρωτοβουλίες και οργανωσιακές πολιτικές.

Εκπαίδευση και πολιτική ασφάλειας

Η εκπαίδευση και οι πολιτικές ασφάλειας πρέπει να αποτελούν αναπόσπαστο μέρος της εταιρικής κουλτούρας. Είναι απαραίτητο να θεσπιστούν υποχρεωτικά προγράμματα τακτικής εκπαίδευσης και ενημέρωσης για όλους τους εργαζομένους. Αυτά τα προγράμματα πρέπει να εστιάζουν στην αναγνώριση και την αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής, καθώς και στην προώθηση ασφαλών πρακτικών εργασίας (Saleem et al., 2017).

Προσομοιώσεις και αξιολόγηση κινδύνου

Η τακτική διεξαγωγή ασκήσεων προσομοίωσης επιθέσεων, σε συνδυασμό με τη συστηματική αξιολόγηση των κινδύνων ασφαλείας, συμβάλλει στην ενίσχυση της επιχειρησιακής ετοιμότητας και στην ανάπτυξη ενός αποτελεσματικού πλαισίου διαχείρισης περιστατικών (Hove, 2020).

Πολυεπίπεδη προσέγγιση για την ασφάλεια

Η εμπειρία δείχνει ότι η αποτελεσματική προστασία απαιτεί την υιοθέτηση μιας προσέγγισης πολλαπλών επιπέδων, η οποία περιλαμβάνει:

1. **Ανάπτυξη προσαρμοστικών συστημάτων ασφαλείας**
    - Εφαρμογή δυναμικών πολιτικών ασφαλείας που προσαρμόζονται στις μεταβαλλόμενες απειλές και το περιβάλλον.
    - Ενσωμάτωση προηγμένων συστημάτων παρακολούθησης και ανάλυσης συμπεριφοράς βασιζόμενα στην Μηχανική Μάθηση και την Τεχνητή Νοημοσύνη.
2. **Ενίσχυση της ανθρωποκεντρικής ασφάλειας**
    - Καλλιέργεια κουλτούρας συνειδητής ασφάλειας μεταξύ των εργαζομένων, με στόχο την αύξηση της ευαισθητοποίησης σχετικά με τους κινδύνους και τις απειλές.
    - Ανάπτυξη προγραμμάτων mentoring, με στόχο τη μεταφορά γνώσεων και εμπειριών που σχετίζονται με την ασφάλεια πληροφοριών, όπως τεχνικές ανίχνευσης των επιθέσεων της κοινωνικής μηχανικής, τρόποι διαχείρισης

ευαίσθητων δεδομένων και τακτικές αποφυγής παραπλανητικών πρακτικών. Αποδέκτες αυτών των προγραμμάτων πρέπει να είναι τόσο οι νέοι εργαζόμενοι όσο και το προσωπικό που αναλαμβάνει κρίσιμες αρμοδιότητες στον τομέα της ασφάλειας.

- Θέσπιση συστήματος κινήτρων, όπως η απονομή βραβείων ή η παροχή οικονομικών επιβραβεύσεων, για την προώθηση ασφαλών πρακτικών. Παραδείγματα περιλαμβάνουν την επιβράβευση εργαζομένων που εντοπίζουν και αναφέρουν επιτυχώς τέτοια περιστατικά ή την παροχή εκπαιδευτικών πιστοποιήσεων σε όσους ολοκληρώνουν προγράμματα ασφαλείας με υψηλές επιδόσεις.

3. **Βελτιστοποίηση διαδικασιών αντιμετώπισης περιστατικών**
    - Δημιουργία ευέλικτων ομάδων αντιμετώπισης περιστατικών, οι οποίες θα ενεργοποιούνται άμεσα σε περιπτώσεις κρίσεων ασφαλείας.
    - Ανάπτυξη αυτοματοποιημένων διαδικασιών απόκρισης, που θα μειώνουν τον χρόνο αντίδρασης σε περιστατικά και θα ελαχιστοποιούν τις επιπτώσεις.
    - Καθιέρωση τακτικών αξιολογήσεων και αναθεωρήσεων των διαδικασιών, με στόχο τη συνεχή βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των πολιτικών ασφαλείας.

Ενίσχυση συνεργασιών και ανταλλαγής πληροφοριών

Η συνεργασία μεταξύ οργανισμών αναδεικνύεται σε ζωτικό παράγοντα για τη βελτίωση της προστασίας. Η ανταλλαγή πληροφοριών για αναδυόμενες απειλές, βέλτιστες πρακτικές και νέα εργαλεία ασφάλειας μπορεί να συμβάλει στη συλλογική θωράκιση απέναντι στις εξελιγμένες μορφές κοινωνικής μηχανικής (Syafitri, 2022).

5.3. Κατευθύνσεις για Μελλοντική Έρευνα

Η συνεχής εξέλιξη των απειλών κοινωνικής μηχανικής απαιτεί στοχευμένη έρευνα σε διάφορους τομείς, ώστε να αναπτυχθούν πιο αποτελεσματικές στρατηγικές προστασίας. Η μελλοντική έρευνα μπορεί να επικεντρωθεί στους εξής βασικούς άξονες:

1. **Αξιοποίηση της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης**
    - *Ανάπτυξη προηγμένων αλγορίθμων για την έγκαιρη ανίχνευση ύποπτων συμπεριφορών*: Στο πλαίσιο των επιθέσεων της κοινωνικής μηχανικής, αυτό περιλαμβάνει την εστίαση σε μοτίβα κοινωνικής αλληλεπίδρασης που μπορεί να υποδεικνύουν κακόβουλες προθέσεις, όπως οι αλλαγές στις συνήθεις επικοινωνιακές πρακτικές.

- *Δημιουργία προσαρμοστικών συστημάτων που μαθαίνουν από προηγούμενες επιθέσεις*: Η πρόκληση είναι η ανάπτυξη μηχανισμών που μπορούν να προσαρμόζονται σε διαφορετικά κοινωνικο-τεχνολογικά πλαίσια, με έμφαση στη μείωση ψευδώς θετικών και αρνητικών ανιχνεύσεων.
- *Σχεδιασμός έξυπνων συστημάτων πρόβλεψης και πρόληψης επιθέσεων*: Ο συνδυασμός τεχνικών κοινωνικής ανάλυσης και αλγορίθμων πρόβλεψης μπορεί να επιτρέψει την πρόληψη επιθέσεων πριν αυτές υλοποιηθούν, ιδίως σε περιβάλλοντα που συνδυάζουν φυσική και ψηφιακή αλληλεπίδραση.

2. **Ψυχολογική Διάσταση των Επιθέσεων**
   - *Μελέτη των ψυχολογικών μηχανισμών που καθιστούν τους χρήστες ευάλωτους*: Η κατανόηση αυτών των μηχανισμών μπορεί να οδηγήσει στη δημιουργία εκπαιδευτικών προγραμμάτων ευαισθητοποίησης και τεχνικών μέτρων που προσαρμόζονται στις ανθρώπινες αδυναμίες. Για παράδειγμα, η ανάλυση της προθυμίας των χρηστών να "κλικάρουν" σε κακόβουλους συνδέσμους υπό συνθήκες πίεσης μπορεί να καθοδηγήσει τη κατάλληλη σχεδίαση αντίμετρων.
   - *Ανάλυση της συμπεριφοράς των επιτιθέμενων και των κινήτρων τους*: Αν και η ανάλυση αυτή αποτελεί ήδη γνωστό πεδίο, η περαιτέρω εστίαση στη σύνδεση των κινήτρων με τη στρατηγική των επιθέσεων μπορεί να προσφέρει νέες κατευθύνσεις για στοχευμένη πρόληψη. Π.χ., η διερεύνηση νέων προτύπων επιθέσεων από οργανωμένα δίκτυα ή μεμονωμένους επιτιθέμενους μπορεί να οδηγήσει σε καλύτερη ταξινόμηση των απειλών.
   - *Εξέταση του ρόλου παραγόντων, όπως το εργασιακό στρες και η πίεση χρόνου*: Η έρευνα πρέπει να επεκταθεί στη διερεύνηση όλων των παραγόντων που επηρεάζουν τη λήψη σωστών ή λανθασμένων αποφάσεων ασφαλείας, π.χ., η επίδραση κουλτούρας ευθύνης στον περιορισμό ανθρώπινων λαθών.
3. **Καινοτόμες Μέθοδοι Εκπαίδευσης**
   - *Αξιοποίηση τεχνολογιών εικονικής (VR: Virtual Reality) και επαυξημένης πραγματικότητας (AR: Augmented Reality)*: Αυτές οι τεχνολογίες, μέσω της δημιουργίας ρεαλιστικών σεναρίων, μπορούν να επιτύχουν υψηλότερα επίπεδα αφομοίωσης γνώσεων και εμπειρίας. Είναι νεωτεριστικές, διότι επιτρέπουν την άμεση ανατροφοδότηση στον χρήστη, ενώ μειώνουν το κόστος εκπαίδευσης σε πραγματικά περιβάλλοντα.

- *Ανάπτυξη εξατομικευμένων προγραμμάτων εκπαίδευσης*: Ειδικά προγράμματα που λαμβάνουν υπόψη το προφίλ κινδύνου κάθε χρήστη μπορούν να αυξήσουν την αποτελεσματικότητα της εκπαίδευσης.
- *Σχεδιασμός διαδραστικών σεναρίων προσομοίωσης επιθέσεων*: Παρότι υπάρχουν ήδη, η έρευνα πρέπει να επικεντρωθεί στην κάλυψη κενών, όπως η έλλειψη σενάριων που συνδυάζουν σύνθετες επιθέσεις (π.χ., phishing σε συνδυασμό με επιθέσεις ransomware).

4. **Μετρήσεις και Δείκτες Αποτελεσματικότητας**
   - *Ανάπτυξη νέων μεθοδολογιών αξιολόγησης μέτρων προστασίας*: Η ανάγκη για νέες μεθοδολογίες προκύπτει από το γεγονός ότι οι επιθέσεις κοινωνικής μηχανικής δεν έχουν μελετηθεί επαρκώς με τρόπο που να αξιολογεί συγκεκριμένα την αποτελεσματικότητα των μέτρων προστασίας.
   - *Δημιουργία δεικτών ανθεκτικότητας*: Οι δείκτες πρέπει να επικεντρώνονται στην ανθεκτικότητα οργανισμών, λαμβάνοντας υπόψη την πολυπλοκότητα και το κοινωνικό στοιχείο των επιθέσεων.
   - *Σχεδιασμός πλαισίου αξιολόγησης ωριμότητας*: Αν και υπάρχουν πλαίσια, η περαιτέρω ανάλυση της ωριμότητας στο πλαίσιο των επιθέσεων είναι απαραίτητη για τον προσδιορισμό των οργανωσιακών κενών και των αδυναμιών.

Ειδικά όσον αφορά στις αναδυόμενες τεχνολογίες και στα ρυθμιστικά πλαίσια, η έρευνα πρέπει να εστιάσει:

- Στις ευπάθειες που δημιουργούν οι τεχνολογίες, όπως το διαδίκτυο των πραγμάτων (IoT: Internet of Things), που παρότι ωριμάζει, παραμένει στο στάδιο ενσωμάτωσης σε πολλές υποδομές. Η σύνδεση του IoT με επιθέσεις κοινωνικής μηχανικής είναι ένα ακόμη ανεκμετάλλευτο πεδίο έρευνας.
- Στις επιπτώσεις τεχνολογιών, όπως η κβαντική υπολογιστική, που θα μπορούσαν να αλλάξουν τα δεδομένα στην ανίχνευση ή και στην εκτέλεση εξελιγμένων επιθέσεων.
- Στην αξιολόγηση των υφιστάμενων ρυθμιστικών πλαισίων και προτύπων ασφαλείας, με στόχο τη διαμόρφωση πιο στοχευμένων και αποτελεσματικών πολιτικών.

Συνολικά, η αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής απαιτεί μια συνεχώς εξελισσόμενη και πολυδιάστατη προσέγγιση, που να συνδυάζει την τεχνολογία με την ανθρώπινη διάσταση της ασφάλειας. Οι προτάσεις για βελτίωση της προστασίας και οι κατευθύνσεις για μελλοντική έρευνα αναδεικνύουν την ανάγκη για διαρκή προσαρμογή στις νέες απειλές και για την ενσωμάτωση καινοτόμων μεθόδων σε κάθε επίπεδο του οργανισμού. Με την ενίσχυση της συνεργασίας, της εκπαίδευσης και της συνεχούς αξιολόγησης, η

ασφάλεια απέναντι στις επιθέσεις κοινωνικής μηχανικής μπορεί να γίνει πιο ανθεκτική και αποδοτική, αντανακλώντας την πραγματικότητα των σύγχρονων τεχνολογικών και κοινωνικών συνθηκών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία και Άρθρα

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). *Analysis of Social Engineering Awareness Among Students and Lecturers*. IEEE Access, 11, 45678-45690.

Abri, F., Zheng, J., Namin, A. S., & Jones, K. S. (2022). *Markov decision process for modeling social engineering attacks and finding optimal attack strategies*. IEEE Access, 10, 118473-118484. https://doi.org/10.1109/ACCESS.2022.3213711

Adinkrah-Appiah, K., Miracle, A. A., & Armah, E. D. (2021). *DPETAS: DETECTION AND PREVENTION OF EVIL TWIN ATTACKS ON WI-FI NETWORKS*. International Journal of Multidisciplinary Studies and Innovative Research, 6, 388-391.

Adu-Manu, K. S., Ahiable, R. K., Appati, J. K., & Mensah, E. E. (2023). *Phishing attacks in social engineering: A review*. Journal of Cyber Security, 2023. https://doi.org/10.32604/jcs.2023.041095

Agarwal, M., Biswas, S., & Nandi, S. (2018*). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks*. International Journal of Wireless Information Networks, 25(2), 130-145. https://doi.org/10.1007/s10776-018-0396-1

Alsufyani, A. A., & Alzahrani, S. (2020). *Social Engineering Attack*. International Journal of Advanced Research in Engineering and Technology, 11(11), 965-975.

Aun, Y., Gan, M.-L., Abdul Wahab, N. H. B., & Guan, G. H. (2023*). Social Engineering Attack Classifications on Social Media Using Deep Learning. Computers, Materials & Continua*. https://doi.org/10.32604/cmc.2023.032373

Baki, S., Verma, R., Mukherjee, A., & Gnawali, O. (2017). *Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation*. Proceedings of ASIA CCS '17, Abu Dhabi, United Arab Emirates. ACM. https://doi.org/10.1145/3052973.3053037

Beckers, K., Krautsevich, L., Yautsiukhin, A. (2022*). Analysis of Social Engineering Threats with Attack Graphs*. International Journal of Information Security, 1(1), 1-10. https://doi.org/10.1007/s10207-022-00677-7

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2023). *Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation*. Computers & Security, 131, 103313.

Breda, F., Barbosa, H., & Morais, T. (2020). *Social engineering and cyber security*. Universidade Lusófona do Porto. INTED2020 Proceedings, 1, 5756-5763.

Bridgers, G., Hausman, C., Tomeo, A., & Umapathy, G. V. (2023). *Phishing for dummies*: Cisco special edition. John Wiley & Sons.

Buber, E., Diri, B., & Sahingoz, Ö. K. (2018). *NLP based phishing attack detection from URLs*. In A. Abraham, et al. (Eds.), ISDA 2017, AISC 736 (pp. 608–618). Springer International Publishing. https://doi.org/10.1007/978-3-319-76348-4_59

Burns, A., Wu, L., Du, X., & Zhu, L. (2017). *A Novel Traceroute-based Detection Scheme for Wi-Fi Evil Twin Attacks*. 2017 IEEE Global Communications Conference (GLOBECOM), 1-6. https://doi.org/10.1109/GLOCOM.2017.8253957

Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). *Deception techniques in social engineering attacks: An analysis of emerging trends and countermeasures*. SEAtech. https://doi.org/10.48550/arXiv.2408.02092

Chetiouia, K., Baha, B., Alami, A. O., & Bahnasse, A. (2021). *Overview of Social Engineering Attacks on Social Networks*. Procedia Computer Science, 198, 656-661. https://doi.org/10.1016/j.procs.2021.12.302

Chinta, M., Alaparthi, J., & Kodali, E. (2016). *A study on social engineering attacks and defence mechanisms*. International Journal of Computer Science and Information Security (IJCSIS), 14(Special Issue).

Conheady, S. (2014). *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw-Hill Education.

Daldoul, Y. (2023). *A Robust Certificate Management System to Prevent Evil Twin Attacks in IEEE 802.11 Networks*. Faculty of Sciences of Monastir, University of Monastir. DOI:10.48550/arXiv.2302.00338

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). *Panning for gold: Automatically analysing online social engineering attack surfaces*. *Computers & Security*, *69*, 18–34.

Edwards, L., Iqbal, M. Z., & Hassan, M. (2024*). A multi-layered security model to counter social engineering attacks: a learning-based approach*. International Cybersecurity Law Review, 5, 313-336. https://doi.org/10.1365/s43439-024-00119-z

ENISA. (2011). *Cyber-Bullying and online Grooming: helping to protect against the risks*. European Network and Information Security Agency.

ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity.

Estella, L. (2024). *Social engineering: Techniques and defenses against manipulative attacks*.

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). *The human factor in phishing: Collecting and analyzing user behavior when reading emails*. Computers & Security, 139, 103671. https://doi.org/10.1016/j.cose.2023.103671

Gehl, R. W., & Lawson, S. T. (2022). *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication.* The MIT Press.

Grassegger, T., & Nedbal, D. (2021). *The role of employees' information security awareness on the intention to resist social engineering*. Procedia Computer Science, 181, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Greavu-Șerban, V., & Șerban, O. (2014). *Social engineering: A general approach*. Informatica Economică, 18(2), 5–12. https://doi.org/10.12948/issn14531305/18.2.2014.01

Guo, Z., Wang, P., Cho, J. H., & Huang, L. (2023). *Text Mining-based Social-Psychological Vulnerability Analysis of Potential Victims to Cybergrooming: Insights and Lessons Learned*. In WWW '23 Companion, April 30–May 04, 2023, Austin, TX, USA. ACM. https://doi.org/10.1145/3543873.3587636

Hadnagy, C. (2018). *Social engineering: The science of human hacking (2nd ed.)*. Wiley.

Hasan, M., Prajapati, N., & Vohara, S. (2010). *Case study on social engineering techniques for persuasion*. International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks (GRAPH-HOC), 2(2), 17-29. https://doi.org/10.5121/jgraphoc.2010.2202

Hasan, M., Rozony, F.Z., Kamruzzaman, M., & Uddin, M. K. S. (2024). Common cybersecurity vulnerabilities: Software bugs, weak passwords, misconfigurations, social engineering. Global Mainstream Journal of Innovation, Engineering & Emerging Technology, 3(4), 42-57.

Herrera Montano, I., García Aranda, J. J., Ramos Diaz, J., Molina Cardín, S., de la Torre Díez, I., & Rodrigues, J. J. P. C. (2022). *Survey of techniques on data leakage protection and methods to address the insider threat*. Cluster Computing, 25(6), 4289–4302. https://doi.org/10.1007/s10586-022-03668-2

Hobel, H., Sánchez, S., Weippl, E., & Kieseberg, P. (2014). *Advanced social engineering attacks*. Journal of Information Security and Applications, 22, 113-122.

Hove, L. T. (2020). *Strategies used to mitigate social engineering attacks (Doctoral dissertation, Walden University)*. ScholarWorks. https://scholarworks.waldenu.edu/dissertations/

Hsu, F.-H., Wu, M.-H., Hwang, Y.-L., Lee, C.-H., Wang, C.-S., & Chang, T.-C. (2022). *WPFD: Active User-Side Detection of Evil Twins*. Applied Sciences, 12(16), 8088. https://doi.org/10.3390/app12168088

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). *Reverse social engineering attacks in online social networks*. Georgia Institute of Technology. DOI: 10.1007/978-3-642-22424-9_4

Jamuna, K. M. (2024). *Social engineering and human factors in penetration testing*. Research.

Kalajžić, I. (2019). *Cybersecurity - the threat of social engineering* [Master's thesis, University of Zagreb]. https://urn.nsk.hr/urn:nbn:hr:148:402256

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for media sanitization (NIST Special Publication 800-88 Rev. 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-88r1

Khan, S. A. (2023). *Social engineering*. In Computer and networks security - Final's Presentation. ST.FX University, Antigonish, NS.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E.R. (2015). *Advanced social engineering attacks*. J. Inf. Secur. Appl., 22, 113-122.

Kulkarni, A. D. (2023). *Convolution neural networks for phishing detection*. International Journal of Advanced Computer Science and Applications, 14(4), 15.

Kushwaha, A., Singh, A. K. P., & Waoo, A. A. (2024). *Review on social engineering attacks and defense mechanisms*. ShodhKosh: Journal of Visual and Performing Arts, 5(5), 362–368. https://doi.org/10.29121/shodhkosh.v5.i5.2024.1887

Li, T., Song, C., & Pang, Q. (2023). *Defending against social engineering attacks: A security pattern-based analysis framework. IET Information Security*. Advance online publication. https://doi.org/10.1049/ise2.12125

Li, Y., Wang, Y., Xiong, X., Zhang, J., & Yao, Q. (2022). *An intelligent penetration test simulation environment construction method incorporating social engineering factors*. Applied Sciences, *12*(12), 6186. https://doi.org/10.3390/app12126186

Maigida, A. M., Abdulhamid, S. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). *Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms*. Journal of Reliable Intelligent Environments, 5(1), 67–89. https://doi.org/10.1007/s40860-019-00080-3

Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., & Liang, Z. (2018). *Detecting phishing websites via aggregation analysis of page layouts*. Procedia Computer Science, 129, 224–230. https://doi.org/10.1016/j.procs.2018.03.053

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Chipfumbu-Kangara, C. T. (2022*). Enhanced social engineering framework mitigating against social engineering attacks in higher education*. Security and Privacy, 5(3). https://doi.org/10.1002/spy2.237

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Mugala, M. (2014). *Social engineering. Masters in Network Administration and Security* [Master's thesis].

Nanda, I., & De, R. (2022). *Social Engineering: An Introduction. Information Management and Computer Science*. 5(2), 36-37. https://doi.org/10.26480/imcs.02.2022.36.37

Noval, S. M. R. (2023). *Indonesia readiness to face social engineering attacks with deepfake technology*. Journal of Law and Sustainable Development, 11(12), 1-17.

Odeh, N., Eleyan, D., & Eleyan, A. (2021). *A survey of social engineering attacks: Detection and prevention tools*. Journal of Theoretical and Applied Information Technology, 99(18), 30 September 2021.

Petrič, G., & Roer, K. (2022). *The impact of formal and informal organizational norms on susceptibility to phishing*: Combining survey and field experiment data. Telematics and Informatics, 67, 101766. https://doi.org/10.1016/j.tele.2021.101766

Sa, A., Nishant, P. R., Baitha, S., & Kumar, K. D. (2024). *An ensemble classification model for phishing mail detection*. Procedia Computer Science, 233, 970–978. https://doi.org/10.1016/j.procs.2024.03.286

Salahdine, F., & Kaabouch, N. (2019). *Social Engineering Attacks*: A Survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

Salim, W. M. (2024). *Prompt Engineering: Unleashing the Power of Large Language Models to Defend Against Social Engineering Attacks*. Iraqi Journal for Computer Science and Mathematics, 5(3), 24-36.

Saleem, J., & Hammoudeh, M. (2017*). Defense methods against social engineering attacks*. In Computer and network security essentials (pp. 35-?). https://doi.org/10.1007/978-3-319-58424-9_35

Sam, J. (2024, May). *Social engineering (to investigate the Scarlet Widow attack)*. Retrieved from https://www.researchgate.net/publication/383606728

Samonas, S. (2016). *Building a theory of socio-technical fraud*. In Proceedings of the Twenty-second Americas Conference on Information Systems (pp. 1-5). AMCIS.

Shombot, E. S., Dusserre, G., Bestak, R., & Ahmed, N. B. (2024). *An application for predicting phishing attacks: A case of implementing a support vector machine learning model*. Cyber Security and Applications, 2, 100036. https://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Soni, S. K., Waoo, A. A., & Chhabra, P. (2024). *Advanced Social Engineering Tactics in Contemporary Cyber Threats*. ResearchGate. https://www.researchgate.net/publication/382488918

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). *Social engineering attacks prevention*: A systematic literature review. IEEE Access, 10, 1-20. https://doi.org/10.1109/ACCESS.2022.3162594

Szurdi, J., & Christin, N. (2017). *Email typosquatting*. In Proceedings of the 2017 Internet Measurement Conference (pp. 419-431).

Szurdi, J., Kocso, B., Cseh, G., Spring, J., Felegyhazi, M., & Kanich, C. (2014). *The long "taile" of typosquatting domain names*. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (pp. 191-206).

Tawalbeh, L. A., & Muheidat, F. (2023). *Factors that Motivate Defense Against Social Engineering Attacks Across Organizations*. Procedia Computer Science, 224, 75-82.

Taylor, M., Vaidya, R., Davidson, D., De Carli, L., & Rastogi, V. (2020). *Defending against package typosquatting*. In International Conference on Financial Cryptography and Data Security (pp. 89-108). Springer, Cham.

Tsinganos, N., Fouliras, P., Mavridis, I., & Gritzalis, D. (2024). *CSE-ARS: Deep Learning-Based Late Fusion of Multimodal Information for Chat-Based Social Engineering Attack Recognition*. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3359030

Udochukwu, D., & Bode-Asa, A. (2023). *An Overview of Social Engineering: The Role of Cognitive Biases Towards Social Engineering-Based Cyber-Attacks, Impacts and Countermeasures*. https://doi.org/10.13140/RG.2.2.12421.12003

Verizon. (2023). *Data breach investigations report (DBIR) 2023.*

Vrhovec, S., Bernik, I., & Markelj, B. (2022). *Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign*. Journal of Cybersecurity Studies, 10(4), 45-60. https://doi.org/10.1016/j.jcyber.2022.11.003

Wang, Z., Zhu, H., & Sun, L. (2021*). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods*. IEEE Access, 9, 11895-11910.

Washo, A. H. (2021). *An interdisciplinary view of social engineering: A call to action for research. Computers in Human Behavior* Reports, 4, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., & Raza, S. (2024). *Can serious gaming tactics bolster spear-phishing and phishing resilience? Securing the human hacking in Information Security*. Information and Software Technology, 170, 107426. https://doi.org/10.1016/j.infsof.2024.107426

Yasin, A., Fatima, R., Liu, L., Wang, J., & Ali, R. (2020). *Understanding social engineers' strategies from the perspective of Sun-Tzu philosophy*. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 254-263). IEEE. https://doi.org/10.1109/COMPSAC48688.2020.00045

Zaoui, M., Yousra, B., Sadqi, Y., Maleh, Y., & Ouazzane, K. (2024). *A comprehensive taxonomy of social engineering attacks and defense mechanisms*: Toward effective mitigation strategies. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3403197

Zheng, K., Wu, T., Wang, X., Wu, B., & Wu, C. (2019). *A Session and Dialogue-Based Social Engineering Framework*. IEEE Access, 7, 184113-184125. https://doi.org/10.1109/ACCESS.2019.2919150

Ιστοσελίδες

Copado Team. (2022). *12 Types of Social Engineering Attacks to Look Out For*. Copado. https://www.copado.com/resources/blog/12-types-of-social-engineering-attacks-to-look-out-for

Cyber Security Authority (CSA). (2024). *COP Advisories. CYBER GROOMING*. https://www.csa.gov.gh/cyber_grooming.php

Cyber Witcher. (2024, May 9). *What is diversionary theft? Attack and defense strategies*. HackYourMom. https://hackyourmom.com/en/kibervijna/shho-take-dyversijna-kradizhka-strategiyi-napadu-ta-zahystu/

Cyber Yodha. (2023). *What is a Vishing Attack?* https://www.cyberyodha.org/2023/03/what-is-vishing-attack.html

Effect, B. (2024). *Social engineering: Attacks, techniques, and defences*. Cybersecurity education. https://fieldeffect.com/blog/social-engineering-attacks

Federal Trade Commission. (2008). *Court Halts Bogus Computer Scans*. https://www.ftc.gov/news-events/news/press-releases/2008/12/court-halts-bogus-computer-scans

Federal Trade Commission. (2012). *FTC Case Results in $163 Million Judgment Against "Scareware" Marketer*. https://www.ftc.gov/news-events/news/press-releases/2012/10/ftc-case-results-163-million-judgment-against-scareware-marketer

Fortinet. (2024a). *Watering Hole Attack. Learn about watering hole attacks, how they work, how to prevent them, and statistics about them*. https://www.fortinet.com/resources/cyberglossary/watering-hole-attack

Fortinet. (2024b). *What Is Eavesdropping? Definition, methods used, how it affects your business, and prevention*. https://www.fortinet.com/resources/cyberglossary/eavesdropping

Fortinet. (2024c). *What Is Social Engineering in Cybersecurity? Learn what social engineering is, its techniques, examples and how to protect against it*. https://www.fortinet.com/resources/cyberglossary/social-engineering

ftc.gov (2022). *What to Know About Romance Scams*. https://consumer.ftc.gov/articles/what-know-about-romance-scams

Gatefy. (2021). *What is BEC (Business Email Compromise) or CEO fraud?* https://gatefy.com/blog/what-bec-business-email-compromise-or-ceo-fraud/

Ghimiray, D. (2022). *What is an evil twin attack and how does it work?* Avast. https://www.avast.com/c-evil-twin-attack

Jayachandran, A. (2024). *Quid pro quo*. Wallstreetmojo. https://www.wallstreetmojo.com/quid-pro-quo/

iefimerida (2022). *Τι είναι το smishing (SMS phishing), πώς εμφανίζεται -Πέντε συμβουλές για να μην πέσουμε θύματα*. https://www.iefimerida.gr/tehnologia/smishing-sms-phishing-ti-prepei-na-prosehete#:~:text=To%20Smishing%20(γνωστό%20και%20ως,(SMS)%20μέσω%20κινητού%20τηλεφώνου.

InfosecTrain. (2018). *Social engineering and its use cases*. https://www.infosectrain.com/blog/social-engineering-and-its-use-cases/

International Telecommunication Union. (2024). *Understanding social engineering: The art of human hacking*. ITU Online. https://www.ituonline.com/blogs/understanding-social-engineering/

Irwin, L. (2019). *What Is Angler Phishing? Definition, Examples & Prevention*. https://www.itgovernance.co.uk/blog/beware-of-angler-phishing

Kaspersky. (2024a.). What is a honeypot? Retrieved from https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

Kaspersky. (2024b). *What Is Pharming and How to Protect Yourself*. https://www.kaspersky.com/resource-center/definitions/pharming

Lee, I. (2024). *What is scareware malware? Removal and protection*. Wallarm. https://www.wallarm.com/what/what-is-scareware-malware-removal-and-protection

Lenaerts-Bergmans, B. (2023). *10 Types of Social Engineering Attacks and how to prevent them*. CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-attacks/#Diversion%20Theft

MITRE Corporation. (2024). *ATT&CK Matrix for Enterprise*. https://attack.mitre.org/

NASA Federal Credit Union. (2019, July 10*). Typosquatting is quickly rising, how to protect yourself.* https://www.nasafcu.com/blog/detail/typosquatting-quickly-rising-protect

National Institute of Standards and Technology (NIST). (2024a). *Glossary - Phishing.* Computer Security Resource Center. https://csrc.nist.gov/glossary/term/phishing

National Institute of Standards and Technology (NIST). (2024b). *Glossary - Spear Phishing.* Computer Security Resource Center. https://csrc.nist.gov/glossary/term/spear_phishing

National Institute of Standards and Technology (NIST). (2024c). *Glossary - Whaling*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/whaling

NBKomputer. (2024). *What is pretexting? How to protect yourself from pretexting*. https://jethrojeff.com/

NIELIT Patna. (2024, January*). Honey Trapping in Cybersecurity*. FutureSkills Prime. Retrieved from https://futureskillsprime.in/knowledge-center/thought-leadership/honey-trapping-cybersecurity

SlidePlayer.com Inc. (2024). *Chapter 4: Can technology alone provide the best security for your organization?* SlidePlayer. https://slideplayer.com/slide/6891548/

Tarada, Y. (2022). *What is a Whaling Attack?* PowerDMARC. https://powerdmarc.com/what-is-whaling-attack/

Terranovasecurity. (2024). *What is baiting in cyber security?* https://www.terranovasecurity.com/blog/what-is-baiting

Yawar, S. (2024a). *Reverse Social Engineering: Explaining a Potent Threat*. https://www.pureversity.com/blog/reverse-social-engineering

Yawar, S. (2024b). *What is a honey trap in cyber security?* Pureversity. https://www.pureversity.com/blog/honey-trap-in-cyber-security

Wright, G. (2024). *What is dumpster diving*? TechTarget. https://www.techtarget.com/searchsecurity/definition/dumpster-diving

Wright, G., & Bacon, M. (2024). *What is a watering hole attack?* TechTarget. https://www.techtarget.com/searchsecurity/definition/watering-hole-attack

Wood, T. (2020). *What is diversion theft? Network Midlands*. https://www.network-midlands.co.uk/what-is-diversion-theft/