2026-02

þÿ — ± ¾ ¹ ¿ À ¿ ¯ · Ã · Ä É ½ º ¿ ¹ ½ É ½ ¹ º Î

þÿ ´ ¹ º Ä Í É ½ Ã Ä ¿ S o c i a l E n g i n e e r i

þÿ ¨ Å Ç ¿ » ¿ ³ ¹ º - Â Ä µ Ç ½ ¹ º - Â , º ¯ ½ ´ Å

þÿ Ã Ä Á ± Ä · ³ ¹ º - Â ± ½ Ä ¹ ¼ µ Ä Î À ¹ Ã · Â

þÿ ¤ Ã ¹ ¬ ¼ ¿ Å Á ¿ Å , œ ± Á ¯ ±

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ ¨ · Æ ¹ ± º ® š ± ¹ ½ ¿ Ä ¿ ¼ ¯ ± ,
þÿ º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â ¬ Æ ¿ Å

Πανεπιστήμιο Νεάπολις Πάφος

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ, ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

“Η αξιοποίηση των κοινωνικών δικτύων στο Social Engineering: Ψυχολογικές τεχνικές, κίνδυνοι και στρατηγικές αντιμετώπισης”

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΜΑΡΙΑ ΤΣΙΑΜΟΥΡΟΥ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΕΠΙΒΛΕΠΟΝΤΑ: ΣΠΥΡΟΣ ΛΑΒΔΑΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2026

Πανεπιστήμιο Νεάπολις Πάφος

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ, ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

“Η αξιοποίηση των κοινωνικών δικτύων στο Social Engineering: Ψυχολογικές τεχνικές, κίνδυνοι και στρατηγικές αντιμετώπισης”

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση του Μεταπτυχιακού Προγράμματος ‘Πληροφοριακά Συστήματα και Ψηφιακή Καινοτομία’ στο Πανεπιστήμιο Νεάπολις Πάφος

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΜΑΡΙΑ ΤΣΙΑΜΟΥΡΟΥ

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

ΦΕΒΡΟΥΑΡΙΟΣ 2026

Πνευματικά δικαιώματα

Η έγκριση της Διπλωματικής Εργασίας από το Πανεπιστημίου Νεάπολις δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Πανεπιστημίου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σελίδα Εγκυρότητας

Ονοματεπώνυμο Φοιτήτριας: Μαρία Τσιάμουρου

Τίτλος Διπλωματικής Εργασίας: Η αξιοποίηση των κοινωνικών δικτύων στο Social Engineering: Ψυχολογικές τεχνικές, κίνδυνοι και στρατηγικές αντιμετώπισης.

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …… από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη προς τον επιβλέποντα καθηγητή μου, κ. Σπύρο Λαβδα, για τη σταθερή καθοδήγηση, τον πολύτιμο χρόνο που διέθεσε και τις ουσιαστικές συμβουλές που μου παρείχε καθ' όλη τη διάρκεια της εκπόνησης της μεταπτυχιακής μου εργασίας. Η συμβολή του υπήρξε καθοριστική για την ολοκλήρωση της παρούσας μελέτης. Ευχαριστώ επίσης την οικογένειά μου και τους φίλους μου για την συνεχή ενθάρρυνση και υποστήριξή τους σε όλη τη διάρκεια των σπουδών μου.

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τον τρόπο με τον οποίο τα κοινωνικά δίκτυα αξιοποιούνται στο πλαίσιο της κοινωνικής μηχανικής, με έμφαση στους ψυχολογικούς μηχανισμούς που καθιστούν τους χρήστες ευάλωτους σε κακόβουλες πρακτικές. Κύριος στόχος της μελέτης είναι η κατανόηση του τρόπου με τον οποίο οι τεχνικές πειθούς και η ανθρώπινη συμπεριφορά αλληλεπιδρούν, διαμορφώνοντας ένα περιβάλλον υψηλού κινδύνου για εξαπάτηση και παραβίαση προσωπικών δεδομένων.

Η έρευνα εφαρμόζει συνδυαστική μεθοδολογική προσέγγιση, η οποία περιλαμβάνει συστηματική βιβλιογραφική ανασκόπηση και ποσοτική εμπειρική έρευνα μέσω δομημένου ερωτηματολογίου. Η ενσωμάτωση των δύο μεθόδων επιτρέπει τόσο τη θεωρητική κατανόηση του φαινομένου της κοινωνικής μηχανικής όσο και την αποτύπωση πραγματικών συμπεριφορών, αντιλήψεων και στάσεων των χρηστών κοινωνικών δικτύων.

Τα ευρήματα καταδεικνύουν ότι η αυξημένη χρήση κοινωνικών δικτύων συνδέεται με μεγαλύτερη έκθεση σε ύποπτες ή παραπλανητικές προσπάθειες επικοινωνίας. Παράλληλα, οι συμμετέχοντες που δήλωσαν υψηλό επίπεδο ψηφιακών δεξιοτήτων δεν παρουσίασαν απόλυτη προστασία, καθώς παράγοντες όπως το επείγον, ο φόβος και η περιέργεια εξακολουθούν να επηρεάζουν τη λήψη αποφάσεων. Επιπλέον, η εκπαίδευση στην κυβερνοασφάλεια διαπιστώθηκε ότι μειώνει την ευαλωτότητα, αν και πολλοί χρήστες εξακολουθούν να εκδηλώνουν υπερβολική εμπιστοσύνη στις ίδιες τις πλατφόρμες κοινωνικών δικτύων.

Συνολικά, τα ευρήματα υπογραμμίζουν ότι η κοινωνική μηχανική αποτελεί μια πολυδιάστατη απειλή που συνδυάζει τεχνικές, ψυχολογικές και κοινωνικές παραμέτρους. Η ενίσχυση της κριτικής σκέψης, η συνεχής ενημέρωση και η ανάπτυξη συνειδητότητας των χρηστών προκύπτουν ως απαραίτητες προϋποθέσεις για την αποτελεσματική προστασία από τους κινδύνους του ψηφιακού περιβάλλοντος.

Λέξεις κλειδιά: Κοινωνική μηχανική, κοινωνικά δίκτυα, ψυχολογική χειραγώγηση, ευαλωτότητα, κυβερνοασφάλεια, επιθέσεις phishing.

Abstract

This thesis examines how social networks are utilized in the context of social engineering, with an emphasis on the psychological mechanisms that make users vulnerable to malicious practices. The main objective of the study is to understand how persuasion techniques and human behavior interact, creating a high-risk environment for deception and personal data breaches.

The research employs a combined methodological approach, which includes a systematic literature review and quantitative empirical research through a structured questionnaire. The integration of the two methods allows both a theoretical understanding of the phenomenon of social engineering and the recording of real behaviors, perceptions, and attitudes of social network users.

The findings demonstrate that increased use of social networks is associated with greater exposure to suspicious or misleading communication attempts. At the same time, participants who reported a high level of digital skills did not show absolute protection, as factors such as urgency, fear, and curiosity continue to influence decision-making. In addition, cybersecurity education was found to reduce vulnerability, although many users still exhibit excessive trust in the social network platforms themselves.

Overall, the findings highlight that social engineering is a multifaceted threat that combines technical, psychological, and social parameters. Strengthening critical thinking, continuous updating, and developing user awareness emerge as necessary prerequisites for effective protection against the risks of the digital environment.

Keywords: Social engineering, social networks, psychological manipulation, vulnerability, cybersecurity, phishing attacks.

1. Εισαγωγή

Η ταχεία εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών, έχει οδηγήσει σε μια σημαντική μεταμόρφωση του τρόπου με τον οποίο τα άτομα επικοινωνούν, εργάζονται και συμμετέχουν σε κοινωνικές αλληλεπιδράσεις. Οι πλατφόρμες κοινωνικής δικτύωσης - όπως το Facebook, το Instagram, το LinkedIn και το X– αποτελούν πλέον αναπόσπαστο τμήμα της καθημερινότητας εκατομμυρίων χρηστών παγκοσμίως, εξασφαλίζοντας ευκαιρίες για κοινωνική δικτύωση, επαγγελματική προβολή και ανταλλαγή πληροφοριών (Boyd & Ellison, 2007; Silic & Back, 2016). Ωστόσο, η ευρεία διάδοση αυτών των πλατφορμών έχει δημιουργήσει νέες μορφές ευπάθειας, καθιστώντας τους χρήστες και τους οργανισμούς εκτεθειμένους σε κινδύνους Κοινωνικής Μηχανικής (social engineering).

Η κοινωνική μηχανική συνιστά μια σύνθετη μορφή ψυχολογικής εκμετάλλευσης, κατά την οποία ο επιτιθέμενος χειραγωγεί τα θύματα ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ενέργειες που εξυπηρετούν κακόβουλους σκοπούς (Mitnick & Simon, 2002). Σε αντίθεση με τις παραδοσιακές κυβερνοεπιθέσεις που στοχεύουν σε τεχνικά τρωτά σημεία, η κοινωνική μηχανική εστιάζει στον ανθρώπινο παράγοντα, αξιοποιώντας τεχνικές πειθούς, κοινωνικής πίεσης και συναισθηματικής επιρροής (Hadnagy, 2018; Workman, 2008). Οι τεχνικές αυτές περιλαμβάνουν επιθέσεις όπως το phishing, το pretexting ή το baiting, και βασίζονται στην εκμεταλλευση της εμπιστοσύνης, της περιέργειας ή του φόβου των χρηστών (Baki & Verma, 2023; Alkhalil et al., 2021).

Τα κοινωνικά δίκτυα έχουν μετατραπεί σε ένα από τα σημαντικότερα εργαλεία των επιτιθέμενων, καθώς επιτρέπουν την ευκολία πρόσβασης σε προσωπικές πληροφορίες που μπορούν να χρησιμοποιηθούν για τη δημιουργία πειστικών και εξατομικευμένων σεναρίων εξαπάτησης. Σύμφωνα με την μελέτη των Jagatic et al. (2007) αυτή ανέδειξε ότι η «ενσωμάτωση κοινωνικών σχέσεων στα μηνύματα phishing (social phishing) αυξάνει δραματικά την πιθανότητα επιτυχίας των επιθέσεων, καθώς η ψυχολογική επίδραση της εμπιστοσύνης μειώνει την άμυνα του χρήστη». Παρόμοια ευρήματα παρουσιάζουν και οι Albladi & Weir (2020), υπογραμμίζοντας ότι τα κοινωνικά δίκτυα προσφέρουν στους επιτιθέμενους ένα περιβάλλον, όπου η διαχείριση ταυτότητας και η ανθρώπινη συμπεριφορά συνδυάζονται για να αυξήσουν την τρωτότητα.

Προσωπικά δεδομένα όπως ημερομηνίες γενεθλίων, τοποθεσίες, ενδιαφέροντα και επαγγελματικές δραστηριότητες, μπορούν να λειτουργήσουν ως «ψηφιακά ίχνη» που διευκολύνουν την στοχοποίηση (Parsons et al., 2019; Albladi & Weir, 2018). Παράλληλα η οικειότητα που προσφέρουν τα κοινωνικά δίκτυα, οδηγούν τους χρήστες σε υποτίμηση των κινδύνων και σε μειωμένη κριτική στάση απέναντι σε ύποπτες επικοινωνίες και μηνύματα (Halevi et al., 2013; Alshammari et al., 2025). Σύγχρονες εμπειρικές έρευνες επιβεβαιώνουν ότι η ανθρώπινη συμπεριφορά και τα ψυχολογικά χαρακτηριστικά -όπως ευπιστία, αυτοπεποίθηση και άλλα- αποτελούν κρίσιμους δείκτες ευπάθειας απέναντι σε τέτοιες επιθέσεις (Rathod et al., 2025; Zhuo et al., 2024).

Η επιλογή του συγκεκριμένου θέματος προκύπτει από την αυξανόμενη ανάγκη κατανόησης του τρόπου με τον οποίο η διάχυση της κοινωνικής πληροφορίας, ενισχύει τις δυνατότητες της κοινωνικής μηχανικής, αλλά και της ανάγκης ανάπτυξης αποτελεσματικών στρατηγικών πρόληψης και αντιμετώπισης. Η διερεύνηση του φαινομένου είναι ιδιαίτερα κρίσιμη για την επιστήμη της κυβερνοασφάλειας, την ψυχολογία της πειθούς και την κοινωνιοτεχνική αλληλεπίδραση, καθώς συμβάλλει στην κατανόηση της σχέσης ανθρώπου–τεχνολογίας και του τρόπου με τον οποίο οι ψυχολογικές διαδικασίες μπορούν να αξιοποιηθούν για κακόβουλους σκοπούς (Cialdini, 2009; Albladi & Weir, 2018; Halevi et al., 2013).

Η παρούσα εργασία εστιάζει αποκλειστικά στο πεδίο της αξιοποίησης των κοινωνικών δικτύων στο πλαίσιο του social engineering. Δεν εξετάζει άλλες μορφές επιθέσεων κοινωνικής μηχανικής που λαμβάνουν χώρα εκτός ψηφιακού περιβάλλοντος, ούτε τεχνικές επιθέσεις που σχετίζονται με κακόβουλο λογισμικό. Αντιθέτως επικεντρώνεται στην ανθρώπινη διάσταση της ασφάλειας πληροφοριών, καθώς και στις ψυχολογικές τεχνικές πειθούς, στα μοτίβα συμπεριφοράς των θυμάτων και στις στρατηγικές πρόληψης και αντιμετώπισης (Parsons et al., 2014; Workman, 2008; Silic & Back, 2016).

Η διεθνής βιβλιογραφία έχει αναδείξει τη σημασία της κοινωνικής μηχανικής ως κρίσιμου παράγοντα κινδύνου για τους οργανισμούς και τα άτομα (Parsons et al., 2019; Albladi & Weir, 2020), ενώ πρόσφατες μελέτες εξετάζουν τις ψυχολογικές και κοινωνικές διαστάσεις της ευπάθειας των χρηστών και πως αυτές επηρεάζουν την πιθανότητα θυματοποίησης (Rathod et al., 2025; Alshammari et al., 2025; Zhuo et

al., 2024). Παρ ’όλα αυτά, η εστίαση στην επίδραση των κοινωνικών δικτύων ως εργαλείου ενίσχυσης των τεχνικών κοινωνικής μηχανικής παραμένει σχετικά περιορισμένη. Η παρούσα εργασία επιδιώκει να καλύψει αυτό το ερευνητικό κενό μέσω μιας διεπιστημονικής προσέγγισης η οποία συνδυάζει στοιχεία από την ψυχολογία, την επικοινωνία και την ασφάλεια πληροφοριών.

Στόχος της μελέτης είναι να αναλυθούν:
(α) οι κυριότερες τεχνικές κοινωνικής μηχανικής που αξιοποιούν δεδομένα από κοινωνικά δίκτυα. Θα εξεταστούν οι διάφορες μορφές επιθέσεων καθώς και ο τρόπος με τον οποίον τα δημόσια διαθέσιμα δεδομένα ενισχύουν την αξιοπιστία των επιτιθέμενων.
(β) οι ψυχολογικοί μηχανισμοί που ενισχύουν την αποτελεσματικότητα αυτών των τεχνικών. Ο συγκεκριμένος στόχος εστιάζει στην κατανόηση των ψυχολογικών παραγόντων που καθιστούν τους χρήστες ευάλωτους σε πρακτικές κοινωνικής μηχανικής.
(γ) οι στρατηγικές πρόληψης και αντιμετώπισης που μπορούν να εφαρμοστούν τόσο σε ατομικό όσο και σε οργανωτικό επίπεδο. Θα εξεταστούν εκπαιδευτικά προγράμματα ευαισθητοποίησης, τεχνικά μέτρα και οργανωτικές πολιτικές ασφάλειας που προτείνονται από φορείς όπως η ENISA και το NIST.

Η εργασία δομείται ως εξής: Στο Κεφάλαιο 2 παρουσιάζεται η βιβλιογραφική ανασκόπηση, στο πλαίσιο της οποίας εξετάζονται οι βασικές έννοιες του social engineering, η σχέση τους με τα κοινωνικά δίκτυα, οι ψυχολογικές τεχνικές πειθούς που αξιοποιούνται, καθώς και οι κίνδυνοι, οι επιπτώσεις και οι στρατηγικές αντιμετώπισης του φαινομένου. Στο Κεφάλαιο 3 παρουσιάζεται αναλυτικά η ερευνητική μεθοδολογία που ακολουθήθηκε για την εκπόνηση της διπλωματικής εργασίας ενώ το Κεφάλαιο 4 επικεντρώνεται στην παρουσίαση των ερευνητικών αποτελεσμάτων και στην ερμηνευτική τους ανάλυση. Τέλος το Κεφάλαιο 5 συνοψίζει τα βασικά συμπεράσματα της εργασίας και τις προτάσεις για μελλοντική διερεύνηση.

2. Βιβλιογραφική Ανασκόπηση

2.1 Εισαγωγή στη βιβλιογραφία

Η μελέτη της κοινωνικής μηχανικής συνιστά ένα πολυδιάστατο και διεπιστημονικό πεδίο έρευνας, το οποίο συνδυάζει στοιχεία από την ψυχολογία, την κοινωνιολογία, την επιστήμη της πληροφορίας και την Κυβερνοασφάλεια. Ήδη από τις αρχικές προσεγγίσεις, η κοινωνική μηχανική αναγνωρίστηκε ως μια πρακτική που εστιάζει κατά κύριο λόγο στον ανθρώπινο παράγοντα και στην χειραγώγηση των γνωστικών και κοινωνικών του ευπαθειών, και όχι στις τεχνικές αδυναμίες των πληροφοριακών συστημάτων (Workman, 2008). Ο Hadnagy (2018) ενισχύει την προαναφερθείσα θέση, υπογραμμίζοντας ότι η κοινωνική μηχανική βασίζεται στη χειραγώγηση ανθρώπινων συμπεριφορών και στην εκμετάλλευση της ανθρώπινης εμπιστοσύνης, καθιστώντας τους τελικούς χρήστες τον πιο αδύναμο κρίκο στην αλυσίδα της ασφάλειας, ανεξαρτήτως της πολυπλοκότητας ή της προηγμένης φύσης των τεχνολογικών υποδομών.

Η εξέλιξη των κοινωνικών δικτύων (social networking sites) έχει αναδιαμορφώσει ριζικά το τοπίο του social engineering, καθώς πλατφόρμες όπως το Facebook, το Instagram και το LinkedIn λειτουργούν πλέον ως ιδανικά ψηφιακά οικοσυστήματα, για τη συλλογή προσωπικών πληροφοριών και την εξατομικευμένη στόχευση πιθανών θυμάτων. Ήδη από τις πρώτες αναλύσεις, οι Boyd και Ellison (2007) ανέδειξαν τον κοινωνικό και διαμοιραστικό χαρακτήρα αυτών των πλατφορμών, τονίζοντας ότι ο τρόπος με τον οποίο οι χρήστες κατασκευάζουν και παρουσιάζουν την ψηφιακή τους ταυτότητα, επιτρέπει τόσο κοινωνικές συνδέσεις όσο και πιθανές μορφές εκμετάλλευσης. Πιο πρόσφατα, οι Albladi και Weir (2020) υποστήριξαν ότι ο συνδυασμός μεταξύ των δημόσια διαθέσιμων δεδομένων και των γνωστικών αδυναμιών των χρηστών, δημιουργεί ένα περιβάλλον εξαιρετικά ευνοϊκό για τους επιτιθέμενους. Αυτός ο συνδυασμός επιτρέπει τον σχεδιασμό εξατομικευμένων και ιδιαίτερα πειστικών επιθέσεων, αυξάνοντας δραματικά το ποσοστό επιτυχίας τους.

Η βιβλιογραφία δίνει ιδιαίτερη έμφαση στο γεγονός ότι η επιτυχία της κοινωνικής μηχανικής στηρίζεται τόσο στη μηχανική της εξαπάτησης όσο και στη γνωστική ευπάθειας των χρηστών. Ο Cialdini (2009) προσφέρει το θεωρητικό πλαίσιο, περιγράφοντας τους βασικούς μηχανισμούς πειθούς που χρησιμοποιούνται συχνά από τους επιτιθέμενους, ώστε να επηρεάσουν την ανθρώπινη συμπεριφορά. Οι μηχανισμοί αυτοί περιλαμβάνουν την κοινωνική απόδειξη, την αυθεντία και την

αμοιβαιότητα. Η εφαρμογή αυτών των αρχών, καθιστά δυνατό για τους επιτιθέμενους να παρακάμψουν την κριτική σκέψη και να παρακινήσουν άτομα σε συμπεριφορές που υπονομεύουν ή παραβιάζουν τα καθιερωμένα πρωτόκολλα ασφαλείας.

Παράλληλα, οι Parsons et al. (2019) τονίζουν ότι οι προκαταλήψεις (cognitive biases) και οι διανοητικές ευκολίες (heuristics) καθιστούν τους χρήστες περισσότερο ευάλωτους, ιδιαίτερα όταν λειτουργούν υπό γνωστικό φόρτο, πίεση χρόνου, συναισθηματικό φορτίο ή υπερφόρτωση πληροφοριών. Αυτές οι συνθήκες μειώνουν την ικανότητα ορθολογικής κρίσης και καθιστούν ευκολότερη τη χειραγώγηση μέσω πειστικών τεχνικών.

Συνοψίζοντας, η υπάρχουσα βιβλιογραφία καταδεικνύει αδιαμφισβήτητα ότι το social engineering δεν αποτελεί απλώς τεχνικό ζήτημα. Αντιθέτως συνιστά ένα πολύπλευρο και δυναμικό φαινόμενο που αναπτύσσεται στην κριτική διασταύρωση της ανθρώπινης ψυχολογίας και των σύγχρονων ψηφιακών περιβαλλόντων, όπως τα μέσα κοινωνικής δικτύωσης. Ως εκ τούτου, η πλήρης κατανόηση του προβλήματος απαιτεί μια συνδυαστική και ολιστική προσέγγιση, η οποία περιλαμβάνει την εμπεριστατωμένη ανάλυση όχι μόνο των τεχνικών πρακτικών, αλλά και των κοινωνικο-γνωστικών παραμέτρων που εμπλέκονται στη διαδικασία χειραγώγησης.

2.2 Θεωρητικό υπόβαθρο

Η κοινωνική μηχανική αναγνωρίζεται ως μια από τις πιο διαδεδομένες και αποτελεσματικές μορφές κυβερνοεπίθεσης. Η εγγενής της επιτυχία βασίζεται στη στοχευμένη χειραγώγηση της ανθρώπινης συμπεριφοράς με απώτερο σκοπό την πρόσβαση σε ευαίσθητες πληροφορίες, συστήματα ή κρίσιμες υπηρεσίες. Σύμφωνα με τους Mitnick & Simon (2002), η κοινωνική μηχανική ορίζεται ως ένα σύνολο τεχνικών εξαπάτησης που αξιοποιούν στρατηγικά την ανθρώπινη εμπιστοσύνη, την άγνοια ή την αμέλεια, έτσι ώστε ο επιτιθέμενος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε κρίσιμα δεδομένα.

Οι μορφές που μπορεί να λάβει η κοινωνική μηχανική παρουσιάζουν μεγάλη ποικιλία και συνεχή εξέλιξη. Στις κλασικές τεχνικές περιλαμβάνονται τα πιο κάτω:

- phishing: οι επιτιθέμενοι χρησιμοποιούν πλαστά e-mails ή sms για να πείσουν τους χρήστες να αποκαλύψουν ευαίσθητα προσωπικά δεδομένα (όπως κωδικούς πρόσβασης, στοιχεία ταυτότητας κλπ).
- pretexting: οι επιτιθέμενοι δημιουργούν μια ψεύτικη ταυτότητα (πχ.υπάλληλος τράπεζας) για να αποσπάσουν πληροφορίες από τους χρήστες (όπως κωδικούς πρόσβασης, οικονομικά στοιχεία κλπ).
- baiting: ο χρήστης παρασύρεται να αποδεχτεί το δόλωμα σε μορφή δώρου (όπως δωρεάν αρχείο ή USB) αλλά στην πραγματικότητα ενεργοποιεί ένα κακόβουλο λογισμικό (malware) που μολύνει το σύστημα του.
- quid pro quo: είναι η τακτική όπου ο επιτιθέμενος προσφέρει μια ψεύτικη υπηρεσία ή βοήθεια, με αντάλλαγμα την πρόσβαση ή τις πληροφορίες από τον χρήστη.
- tailgating: είναι η παράνομη είσοδος ενός επιτιθέμενου, χωρίς ταυτότητα ή άδεια, σε περιορισμένο χώρο ακολουθώντας έναν εξουσιοδοτημένο εργαζόμενο.

Τα τελευταία χρόνια έχουν προστεθεί πιο εξελιγμένες μέθοδοι, οι οποίες αξιοποιούν τις ψηφιακές τεχνολογίες. Ενδεικτικά παραδείγματα αποτελούν το deepfake-based impersonation και το spear-phishing με αξιοποίηση της Τεχνητής Νοημοσύνης (AI). Η πολυμορφία και η προσαρμογή αυτών των τεχνικών αποδεικνύει ότι το social engineering είναι δυναμικό φαινόμενο, το οποίο εξελίσσεται παράλληλα με την τεχνολογία, τις ψηφιακές υποδομές και τις πρακτικές χρήσης του διαδικτύου.

Βασική παράμετρος για την εις βάθος κατανόηση της κοινωνικής μηχανικής είναι ο ανθρώπινος παράγοντας, ο οποίος αναγνωρίζεται διεθνώς ως ο πιο αδύναμος κρίκος στην αλυσίδα της Κυβερνοασφάλειας. Ο Schneier (2015) υποστηρίζει ότι ανεξάρτητα από τον βαθμό εξέλιξης των τεχνολογικών υποδομών και των μέτρων ασφαλείας, η συνολική τους ακεραιότητα υπονομεύεται συχνά από ανθρώπινες αδυναμίες και γνωστικά σφάλματα. Αυτές οι αδυναμίες αφορούν την υπερβολική εμπιστοσύνη, την απροσεξία, την κόπωση και την επιθυμία για γρήγορη εκτέλεση εργασιών.

Παράλληλα, οι Jansson & von Solms (2013) επισημαίνουν ότι η αποτελεσματικότητα πολλών οργανωτικών πολιτικών ασφάλειας, εξαρτάται άμεσα

από την συνεπή τήρηση τους από τους εργαζομένους, γεγονός που καθιστά την ανθρώπινη συμπεριφορά κρίσιμο παράγοντα για την επίτευξη της συνολικής προστασίας των πληροφοριακών συστημάτων. Μέσα από αυτό το πρίσμα, η κοινωνική μηχανική δεν είναι απλώς ένα τεχνικό ζήτημα, αντιθέτως αποτελεί μια εκδήλωση των αλληλεπιδράσεων μεταξύ ανθρώπων, τεχνολογίας και του ευρύτερου κοινωνικού πλαισίου.

Η κοινωνική χειραγώγηση αποτελεί τον θεμελιώδη πυρήνα της κοινωνικής μηχανικής και συνδέεται στενά με τα θεωρητικά μοντέλα επιρροής και πειθούς. Ο Cialdini (2009) περιγράφει έξι βασικές αρχές οι οποίες αξιοποιούνται συστηματικά από τους επιτιθέμενους για να επηρεάσουν τις αποφάσεις των θυμάτων, όπου αυτές είναι:

- κοινωνική απόδειξη
- αμοιβαιότητα
- δέσμευση και συνέπεια
- αυθεντία
- έλλειψη και
- συμπάθεια

Στα περιβάλλοντα ψηφιακής επικοινωνίας, αυτές οι αρχές μπορούν να λειτουργήσουν εντονότερα και αποτελεσματικότερα, λόγω της έλλειψης φυσικής παρουσίας και της αδυναμίας του χρήστη να ελέγξει τα μη-λεκτικά στοιχεία της επικοινωνίας ή την αυθεντικότητα της πηγής.

Τέλος, η έννοια της ευπάθειας και της εμπιστοσύνης στο διαδίκτυο συνδέεται άμεσα με την επιτυχία τεχνικών κοινωνικής μηχανικής. Οι Williams, Beardmore & Joinson (2017) υποστηρίζουν ότι οι χρήστες τείνουν να διαμορφώνουν υψηλά επίπεδα εμπιστοσύνης απέναντι στις διαδικτυακές πλατφόρμες, συχνά παραλείποντας να αξιολογούν κριτικά την αυθεντικότητα των πληροφοριών ή των αλληλεπιδράσεων. Αυτή η μη-κριτική στάση δημιουργεί ένα γνωστικό κενό το οποίο αξιοποιείται εύκολα από τους κακόβουλους φορείς.

Η αυξημένη διαδικτυακή εμπιστοσύνη σε συνδυασμό με τις γνωστικές προκαταλήψεις, οδηγεί σε αυξημένη ευαλωτότητα σε επιθέσεις της κοινωνικής

μηχανικής. Ιδιαίτερα αποτελεσματικές είναι οι επιθέσεις που αντικατοπτρίζουν κοινωνική εγγύτητα (πχ. φίλος ή συνάδελφος) ή επαγγελματική αξιοπιστία (πχ. επίσημος φορέας).

Συμπερασματικά, το θεωρητικό υπόβαθρο της παρούσας μελέτης αναδεικνύει ότι η κοινωνική μηχανική είναι σύνθετο αποτέλεσμα μιας αλληλεπίδρασης τεχνικών, ψυχολογικών και κοινωνικών παραγόντων. Η ολοκληρωμένη κατανόηση αυτών των τριών διαστάσεων είναι απολύτως απαραίτητη τόσο για την ερμηνεία του φαινομένου social engineering όσο και για την σχεδίαση και ανάπτυξη αποτελεσματικών στρατηγικών πρόληψης και αντιμετώπισης των σχετικών κυβερνοεπιθέσεων.

2.3 Η κοινωνική μηχανική στα κοινωνικά δίκτυα

Η ραγδαία διάδοση των πλατφορμών κοινωνικής δικτύωσης κατά την τελευταία δεκαετία, έχει μετασχηματίσει θεμελιακά την επικοινωνία, την κοινωνική αλληλεπίδραση και τον τρόπο που ανταλλάσσουν πληροφορίες άτομα και οργανισμοί. Πλατφόρμες όπως το Facebook, Instagram, LinkedIn και X/Twitter έχουν μετεξελιχθεί σε πολυδιάστατα οικοσυστήματα που εξυπηρετούν ένα ευρύ φάσμα προσωπικών, επαγγελματικών και επιχειρηματικών δραστηριοτήτων. Η βιβλιογραφία τονίζει ότι αυτή η εξέλιξη οδήγησε στην δημιουργία ενός περιβάλλοντος υψηλής έκθεσης, καθώς ο τεράστιος όγκος ευαίσθητων δεδομένων που είναι διαθέσιμα δημόσια ή ιδιωτικά στις πλατφόρμες, τις καθιστά ιδιαίτερα ελκυστικούς στόχους για επιτιθέμενους που χρησιμοποιούν τεχνικές κοινωνικής μηχανικής (Albladi & Weir, 2018; Chetioui et al., 2022).

Το Facebook παραμένει η μεγαλύτερη πλατφόρμα παγκοσμίως και η ιδιότητα του ως χώρος ανταλλαγής και διακίνησης προσωπικών δεδομένων (τοποθεσία, φωτογραφίες, προτιμήσεις) το καθιστά ιδανικό έδαφος για στοχευμένες επιθέσεις εξαπάτησης. Από τις διάφορες δημοσιεύσεις των χρηστών, δημιουργείται ένας πλούσιος όγκος δεδομένων τον οποίον οι επιτιθέμενοι αξιοποιούν εύκολα για profiling και δημιουργία πειστικών σεναρίων εξαπάτησης (ENISA, 2022).

Το Instagram, έχοντας ως κύρια στοιχεία του την οπτική επικοινωνία και το Lifestyle, έχει εξελιχθεί σε μια πλατφόρμα όπου οι επιθέσεις βασίζονται στην συστηματική δημιουργία πλαστών λογαριασμών που αναπαριστούν επαγγελματίες ή μοντέλα,

στην ανάπτυξη δόλιων προσφορών (giveaway scams), στην υποκλοπή ταυτότητας αναγνωρισμένων δημόσιων προσώπων και στην χειραγώγηση μέσω άμεσων μηνυμάτων (direct messages) (Williams et al., 2017; Parsons et al., 2019).

Το LinkedIn λόγω του επαγγελματικού χαρακτήρα του, αποτελεί την κορυφαία πλατφόρμα για στοχευμένες επιθέσεις σε στελέχη επιχειρήσεων. Οι λεπτομέρειες που μοιράζονται οι χρήστες σχετικά με την εργασία τους, τα έργα και τις εταιρείες που δραστηριοποιούνται, επιτρέπει στους επιτιθέμενουw να αναπτύξουν spear-phishing μηνύματα (Albladi & Weir, 2018).

Το X/Twitter ως πλατφόρμα ταχείας διάχυσης πληροφοριών αποτελεί ιδανικό έδαφος για επιθέσεις που εκμεταλλεύονται την τρέχουσα επικαιρότητα και τις τάσεις συζήτησης. Η έλλειψη ελέγχου στην γρήγορη αναπαραγωγή πληροφοριών, σε συνδυασμό με την ευκολία ανώνυμης δημιουργίας λογαριασμών, αυξάνει δραματικά τον κίνδυνο των επιθέσεων πλαστοπροσωπίας (impersonation) (Chetioui et al., 2022; ENISA, 2022).

Σύμφωνα με την ENISA (2022), οι επιθέσεις social engineering αποτελούν πλέον τον συχνότερο τρόπο για την αρχική παραβίαση των συστημάτων στην Ευρώπη, με το ποσοστό να αυξάνεται σταθερά κάθε χρόνο. Καθώς οι επιτιθέμενοι εκμεταλλεύονται τον τεράστιο αριθμό ενεργών χρηστών και το χαμηλό επίπεδο επίγνωσης κινδύνου, το phishing και το spear-phishing μέσω κοινωνικών δικτύων, παρουσιάζουν σημαντική αύξηση. Σύμφωνα με τις οδηγίες ασφάλειας του NIST(2020) υπάρχει μια αυξανόμενη τάση των επιτιθέμενων να χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης για τη συλλογή πληροφοριών, καθώς οι χρήστες τείνουν να δημοσιεύουν εκεί δεδομένα και πληροφορίες που δεν θα αποκάλυπταν σε διαφορετικό περιβάλλον.

Αναφορές δείχνουν ότι οι οργανισμοί δέχονται συχνά συστηματικές επιθέσεις οι οποίες έχουν ως αφετηρία τις πλατφόρμες κοινωνικής δικτύωσης. Ζητήματα επικαιρότητας όπως η πανδημία, η τηλεργασία και η αυξημένη ψηφιακή δραστηριότητα, επιτάχυναν ακόμη περισσότερο αυτή την τάση, αφήνοντας τους χρήστες εκτεθειμένους σε επιθέσεις που εκμεταλλεύονται τα εν λόγω θέματα (ENISA, 2022).

Η βιβλιογραφία καθορίζει πολλούς παράγοντες ευαλωτότητας των χρηστών απέναντι σε επιθέσεις κοινωνικής μηχανικής. Οι Williams et al. (2017) επισημαίνουν ότι οι χρήστες τείνουν να μην δίνουν τη δέουσα σημασία στους κινδύνους των ψηφιακών περιβαλλόντων, και να υπερεκτιμούν την ικανότητα τους να αναγνωρίζουν απειλές. Αυτό έχει ως αποτέλεσμα συμπεριφορές όπως η αποδοχή αιτημάτων φιλίας από άγνωστα άτομα, το κλικ σε ύποπτους συνδέσμους και η δημοσιοποίηση προσωπικών πληροφοριών.

Παράλληλα, ο Parsons et al. (2019) υποστηρίζουν ότι η έλλειψη κατάλληλης εκπαίδευσης, η συναισθηματική χειραγώγηση σε συνδυασμό με την ευκολία πρόσβασης σε πληροφορίες στα κοινωνικά δίκτυα και η μειωμένη προσοχή, ενισχύουν την πιθανότητα επιτυχίας των επιτιθέμενων. Επιπλέον τα κοινωνικά δίκτυα προωθούν την άμεση ανταπόκριση και τη συνεχή αλληλεπίδραση, γεγονός που συμβάλλει στη λήψη παρορμητικών αποφάσεων.

Τέλος, οι Tullet-Prado et al. (2023) αναδεικνύουν ότι η ευαλωτότητα των χρηστών έχει και ψυχολογική διάσταση, καθώς συχνά επηρεάζονται από την ανάγκη κοινωνικής αποδοχής, την εμπιστοσύνη που δείχνουν σε φίλους ή επαγγελματίες γνωστούς, καθώς και από την τάση τους για άμεση ανταπόκριση σε αιτήματα που μοιάζουν ως επείγοντα ή υψηλής σημασίας.

Η αξία της μελέτης πραγματικών επιθέσεων είναι καθοριστικής σημασίας για την πρακτική κατανόηση του τρόπου λειτουργίας της κοινωνικής μηχανικής.

Πρώτη μελέτη, η περίπτωση LinkedIn Breach το 2021. Όπως αναφέρετε στη σελίδα του LinkedIn “το 2021, πληροφορίες από περίπου 700 εκατομμύρια χρήστες του LinkedIn συλλέχθηκαν και πωλήθηκαν σε φόρουμ του dark web. Αν και η διαρροή προήλθε από scraping τεχνικές και όχι από παραβίαση των συστημάτων της εταιρείας, το περιστατικό ανέδειξε τη μεγάλη έκταση των διαθέσιμων δημόσιων πληροφοριών στην πλατφόρμα. Οι επιτιθέμενοι αξιοποίησαν αυτά τα δεδομένα για τη δημιουργία ρεαλιστικών spear-phishing εκστρατειών, στοχεύοντας στελέχη επιχειρήσεων και επαγγελματίες υψηλής αξίας”.

Δεύτερη περίπτωση το Facebook Data Leaks & Regulatory Investigations, την περίοδο 2022-2023. Η Αρχή Ανταγωνισμού και Αγορών του Ηνωμένου Βασιλείου

(CMA) εξέτασε εκείνη την περίοδο ζητήματα διαχείρισης δεδομένων και διαφάνειας, τονίζοντας ότι οι διαρροές μπορούν να αξιοποιηθούν σε μεγάλης κλίμακας εξαπατήσεις. Οι επιτιθέμενοι χρησιμοποίησαν δημοσιοποιημένα στοιχεία για να πραγματοποιήσουν επιθέσεις impersonation, εκμεταλλευόμενοι τόσο την εμπιστοσύνη μεταξύ φίλων, όσο και την ευκολία αποστολής άμεσων μηνυμάτων (UK CMA, 2023).

2.4 Ψυχολογικές τεχνικές πειθούς

Η κοινωνική μηχανική θεμελιώνεται στην εκμετάλλευση της ανθρώπινης ψυχολογίας, με αποτέλεσμα ο άνθρωπος να καθίσταται ο πιο ευάλωτος και προβλέψιμος κρίκος στην αλυσίδα της κυβερνοασφάλειας. Σύμφωνα με τους Mitnick & Simon (2002), οι επιτιθέμενοι δεν ‘χακάρουν’ συστήματα αλλά ανθρώπους, αξιοποιώντας τις παγιωμένες συμπεριφορές, τα συναισθήματα και τις γνωστικές προκαταλήψεις. Η βιβλιογραφία των Hadnagy (2018) και Siddiqi et al. (2022) επιβεβαιώνει ότι οι ψυχολογικές τεχνικές πειθούς και χειραγώγησης βρίσκονται στο επίκεντρο των περισσότερων επιθέσεων social engineering, ιδιαίτερα στα περιβάλλοντα κοινωνικής δικτύωσης.

Στον πυρήνα της κοινωνικής μηχανικής περιλαμβάνονται τεχνικές όπως το pretexting, το phishing, το baiting, το quid pro quo και το impersonation. Οι Mitnick & Simon (2002) εξηγούν ότι αυτές οι τεχνικές δομούνται με τη δημιουργία πειστικών αφηγημάτων που ωθούν τα θύματα σε ενέργειες προς όφελος του επιτιθέμενου. Ο Hadnagy (2018) καταγράφει “έξι βασικές τακτικές χειραγώγησης: οικοδόμηση εμπιστοσύνης, εκμετάλλευση φόβου, επίκληση εξουσίας, επίκληση κοινωνικής απόδειξης, δημιουργία σχέσης οικειότητας και ενεργοποίηση παρορμητικής συμπεριφοράς μέσω επείγοντος”.

Το έργο των Siddiqi et al. (2022) επικαιροποιεί τα προαναφερθέντα ευρήματα, διαπιστώνοντας ότι οι σχετικές τεχνικές έχουν εξελιχθεί, προκειμένου να ευθυγραμμιστούν με τα μοντέρνα χαρακτηριστικά των κοινωνικών δικτύων. Οι επιτιθέμενοι τείνουν να στοχοθετούν ευάλωτες στιγμές των χρηστών, όπως περιόδους χαμηλής προσοχής, στιγμές συναισθηματικής φόρτισης ή έντονης επικαιρότητας, ενισχύοντας έτσι την πιθανότητα επιτυχούς εξαπάτησης.

Όπως αναφέρθηκε και στο προηγούμενο υποκεφάλαιο, ο Cialdini (2009) αναλύει έξι θεμελιώδεις αρχές πειθούς, κοινωνική απόδειξη, αμοιβαιότητα, δέσμευση και συνέπεια, αυθεντία, έλλειψη και συμπάθεια, οι οποίες έχουν άμεση εφαρμογή στην κοινωνική μηχανική. Οι επιτιθέμενοι ενσωματώνουν αυτές τις αρχές στα κοινωνικά δίκτυα, ούτως ώστε να μπορούν να αυξήσουν την αξιοπιστία τους και να ελέγξουν την συμπεριφορά των χρηστών.

Για παράδειγμα, η αρχή της συμπάθειας αξιοποιείται από τους επιτιθέμενους μέσω ελκυστικών ή φιλικών προφίλ, με σκοπό να προκαλέσουν θετική συναισθηματική αντίδραση και να μειώσουν την κριτική σκέψη του χρήστη. Η κοινωνική απόδειξη χρησιμοποιείται μέσω πλαστών προφίλ που εμφανίζουν χιλιάδες «ακόλουθους» ή «κοινές επαφές» κάνοντας έτσι το προφίλ πιο αξιόπιστο. Η αυθεντία από την άλλη, εμφανίζεται με τη δημιουργία πλαστών λογαριασμών που μιμούνται εταιρικούς επίσημους ή κρατικούς φορείς ή στελέχη, ενισχύοντας έτσι την υπακοή και αποτρέποντας την αμφισβήτηση.

Η εφαρμογή ψυχολογικών τεχνικών στα κοινωνικά δίκτυα αποδεικνύεται ιδιαίτερα αποτελεσματική, όπως τεκμηριώνουν οι Hadnagy (2018) και Fadhil (2023). Οι επιτιθέμενοι εκμεταλλεύονται:

- το εύρος και την υψηλή ταχύτητα διάδοσης πληροφοριών,
- τη δημόσια προβολή προσωπικών δεδομένων και στοιχείων ταυτότητας,
- τον αυθόρμητο χαρακτήρα και την αμεσότητα των αλληλεπιδράσεων,
- την κοινωνική πίεση για άμεση ανταπόκριση,
- καθώς και τις προκαθορισμένες συναισθηματικές αντιδράσεις των χρηστών.

Σε πλατφόρμες όπως το Facebook και το Instagram, τα προφίλ-απάτες αξιοποιούν οπτικό υλικό, δημοσιεύσεις και δημόσιες σχέσεις για την δημιουργία εξατομικευμένων σεναρίων. Αντιθέτως σε επαγγελματικά δίκτυα όπως το LinkedIn, η απειλή εντείνεται, καθώς τα προφίλ εμφανίζονται ως στελέχη εταιρειών ή recruiters, μεγιστοποιώντας έτσι την επίδραση της εξουσίας και της αξιοπιστίας στην προσπάθεια εξαπάτησης.

Είναι κρίσιμο να σημειωθεί ότι, οι πολυάριθμες μορφές ψηφιακής εξαπάτησης (scams) ενισχύονται από τις γνωστικές προκαταλήψεις των χρηστών. Η προκατάληψη υπερβολικής αυτοπεποίθησης (overconfidence bias), οδηγεί τους

χρήστες σε υπερεκτίμηση της ικανότητάς τους για αναγνώριση απάτης, με αποτέλεσμα την υποτίμηση των κινδύνων. Η προκατάληψη επιβεβαίωσης (confirmation bias), ωθεί τους χρήστες στην αποδοχή πληροφοριών που επιβεβαιώνουν προϋπάρχουσες προσδοκίες ή επιθυμίες, παραμερίζοντας έτσι κρίσιμες ενδείξεις κινδύνου (Ferreira et al., 2015; Jansen & van Schaik, 2022).

Οι προαναφερθείσες προκαταλήψεις συνδυάζονται με τη χαλαρή στάση που υιοθετείται συχνά κατά τη διάρκεια της καθημερινής χρήσης των κοινωνικών δικτύων. Σε αυτό το περιβάλλον, οι χρήστες βιώνουν το αίσθημα οικειότητας και ασφάλειας, το οποίο μειώνει την κριτική εγρήγορση, με αποτέλεσμα οι επιτιθέμενοι να το εκμεταλλεύονται.

Πέραν των ενδογενών γνωστικών προκαταλήψεων, η επιτυχία του social engineering ενισχύεται περαιτέρω από την εκμετάλλευση του συναισθηματικού παράγοντα. Οι Parsons et al. (2019) και Halevi et al. (2013) αποδεικνύουν ότι ορισμένα συναισθήματα, όπως φόβος, περιέργεια, ενθουσιασμός, βιασύνη και απληστία λειτουργούν ως ισχυροί μοχλοί. Αυτοί οι μοχλοί έχουν ως αποτέλεσμα την αναστολή της ικανότητας λογικής σκέψης (rational decision-making) και κατ' επέκταση την αύξηση της ευαλωτότητας του χρήστη.

Ο φόβος χρησιμοποιείται σε μηνύματα που προειδοποιούν για δήθεν παραβιάσεις λογαριασμών ή επικείμενες κυρώσεις, οδηγώντας τους χρήστες σε άμεση ενέργεια. Η περιέργεια ενεργοποιείται μέσω ‘εντυπωσιακών’ συνδέσμων, viral περιεχομένου ή υποτιθέμενων αποκαλύψεων. Η βιασύνη ενισχύεται με τη χρήση επειγόντων αιτημάτων, όπως προειδοποιήσεις για λήξη χρόνου ή προσφορές περιορισμένης διάρκειας, κάτι που συνδέεται άμεσα με την αρχή της σπανιότητας του Cialdini (2009).

2.5 Κίνδυνοι και επιπτώσεις της κοινωνικής μηχανικής

Η κοινωνική μηχανική αποτελεί πλέον έναν από τους πιο διαδεδομένους και αποτελεσματικούς τύπους κυβερνοαπειλών, αφού δεν στοχεύει σε τεχνικά συστήματα αλλά στον ανθρώπινο παράγοντα που είναι το ‘ασθενέστερο σημείο της αλυσίδας ασφάλειας’ (Jansson & von Solms, 2013). Οι κίνδυνοι και οι επιπτώσεις της κοινωνικής μηχανικής επιφέρουν δυσμενείς επιπτώσεις σε πολλαπλά επίπεδα –ατομικό, οργανωτικό και επιχειρησιακό- υπονομεύοντας την ακεραιότητα των

δεδομένων, τη λειτουργική συνέχεια, την εταιρική φήμη και την οικονομική σταθερότητα των εμπλεκόμενων φορέων (Hadnagy, 2018).

Σε επίπεδο χρήστη, οι απειλές περιλαμβάνουν κλοπή προσωπικών δεδομένων, κατάχρηση ψηφιακής ταυτότητας, οικονομική απάτη, καθώς και πρόσβαση σε ευαίσθητες πληροφορίες οι οποίες επιτρέπουν την πραγματοποίηση πιο στοχευμένων επιθέσεων. Σύμφωνα με την ENISA (2022), η αύξηση των ψηφιακών υπηρεσιών και η εξάρτηση των πολιτών από πλατφόρμες κοινωνικής δικτύωσης, έχει οδηγήσει σε εντονότερη χρήση του social engineering, ιδιαίτερα μέσω εξατομικευμένων επιθέσεων που εκμεταλλεύονται τα προσωπικά δεδομένα των χρηστών.

Σε οργανωσιακό επίπεδο, οι συνέπειες της κοινωνικής μηχανικής κλιμακώνονται σοβαρά, καθώς η τακτική αυτή αξιοποιείται ως ‘αρχικό σημείο παραβίασης’ (initial attack vector) για την πρόσβαση σε κρίσιμες υποδομές. Επιθέσεις όπως το phishing, το vishing και το pretexting, οδηγούν σε μια αλυσίδα ζημίας: υποκλοπή διαπιστευτηρίων, παραβίαση λογαριασμών και εγκατάσταση malware, με τελικό αποτέλεσμα την πλήρη παραβίαση συστημάτων ή τη διαρροή εμπιστευτικών εταιρικών δεδομένων (Hadnagy, 2018). Οι οικονομικές συνέπειες είναι πολλαπλές: άμεσες απώλειες από δόλιες συναλλαγές, υψηλό κόστος αποκατάστασης συστημάτων, πιθανές νομικές κυρώσεις και απώλεια εσόδων λόγω διακοπής λειτουργίας. Παράλληλα, οι επιθέσεις κοινωνικής μηχανικής πλήττουν σοβαρά τη φήμη του οργανισμού και την εμπιστοσύνη πελατών και συνεργατών.

Η ENISA (2022) επισημαίνει ότι η πλειονότητα των επιτυχημένων κυβερνοεπιθέσεων ξεκινούν μέσω της ανθρώπινης αλληλεπίδρασης, αναδεικνύοντας έτσι τη στρατηγική σημασία της εκπαίδευσης του προσωπικού και της εφαρμογής πολυεπίπεδων πολιτικών ασφαλείας. Συγκεκριμένα οι οργανισμοί που παρουσιάζουν ελλείψεις σε μηχανισμούς ανίχνευσης phishing, σε σαφείς πολιτικές διαχείρισης δικαιωμάτων πρόσβασης (Access Control Management) ή σε διαδικασίες επαλήθευσης αιτημάτων, είναι ιδιαίτερα ευάλωτοι σε επιθέσεις.

Σύμφωνα με διεθνή δεδομένα, το social engineering αποτελεί κυρίαρχη τάση στον χώρο των κυβερνοεπιθέσεων. Το Verizon Data Breach Investigations Report (DBIR) έχει καταγράψει διαχρονικά ότι πάνω από το 80% των παραβιάσεων

αποδίδονται σε παράγοντες όπως το ανθρώπινο λάθος, η κοινωνική μηχανική ή η κατάχρηση διαπιστευτηρίων. Μεγάλο ποσοστό των περιστατικών οφείλεται σε phishing emails, τα οποία παραμένουν η μέθοδος με την μεγαλύτερη απόδοση για την παράκαμψη εφαρμοζόμενων τεχνικών μέτρων ασφαλείας. Ταυτόχρονα, τα ENISA Threat Landscape Reports αναδεικνύουν “συνεχή αύξηση των social engineering τεχνικών, με ιδιαίτερη έμφαση σε επιθέσεις που πραγματοποιούνται μέσω messaging apps και κοινωνικών δικτύων, καθώς και στη χρήση τεχνικών αυτοματοποίησης μέσω εργαλείων AI” (ENISA, 2023).

Οι τελευταίες τάσεις στον τομέα της κοινωνικής μηχανικής, καταδεικνύουν αυξημένη πολυπλοκότητα και αξιοποίηση των νέων τεχνολογιών, όπου το phishing παραμένει η πιο διαδεδομένη και θεμελιώδης μορφή επίθεσης social engineering. Παράλληλα, η ευρεία χρήση των smartphones έχει οδηγήσει σε αύξηση του smishing, δηλαδή στην αποστολή δόλιων μηνυμάτων SMS που ωθούν τον χρήστη να πατήσει σε κακόβουλο σύνδεσμο ή να επικοινωνήσει με μια πλαστή υπηρεσία υποστήριξης.

Μια από τις σημαντικότερες εξελίξεις είναι η αξιοποίηση deepfake τεχνολογιών, οι οποίες επιτρέπουν στους επιτιθέμενους να δημιουργούν ψεύτικες φωνές, βίντεο ή εικόνες υψηλής ποιότητας. Η αυξανόμενη ρεαλιστικότητα των deepfakes καθιστά ολοένα και πιο δύσκολη την ανίχνευση απάτης, δημιουργώντας νέους κινδύνους για impersonation attacks, όπως η αποστολή πλαστών εντολών από ανώτερα στελέχη (CEO fraud) ή εξαπάτηση μέσω video calls (Chesney & Citron, 2019). Παράλληλα, η ταχεία ανάπτυξη των generative AI εργαλείων δίνει τη δυνατότητα δημιουργίας πειστικών κειμένων, emails και μηνυμάτων σε μεγάλη κλίμακα, γεγονός που αυξάνει τόσο την ποιότητα όσο και την κλίμακα των επιθέσεων (Williams et al., 2017).

Επιπλέον, καταγράφεται σημαντική αύξηση σε στοχευμένες επιθέσεις (spear-phishing), όπου οι επιτιθέμενοι συλλέγουν λεπτομερή πληροφοριακά στοιχεία για τα θύματα τους, ώστε να διαμορφώσουν πειστικό και στοχευμένο περιεχόμενο (Parsons et al., 2019). Η πρακτική αυτή συνδέεται στενά με την πληθώρα δεδομένων που διατίθενται δημοσίως στα κοινωνικά δίκτυα, όπου το digital footprint των χρηστών λειτουργεί ως βασικό εργαλείο στα χέρια των δραστών (Hadnagy, 2018· ENISA, 2022). Ως αποτέλεσμα, οι επιτιθέμενοι μπορούν να αποτυπώσουν προσωπικά ενδιαφέροντα, επαγγελματικές σχέσεις ή ευαισθησίες, αυξάνοντας σημαντικά την αποτελεσματικότητα της εξαπάτησης.

2.6 Στρατηγικές αντιμετώπισης

Η αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής απαιτεί μια πολυδιάσταση και ολιστική προσέγγιση, καθώς η απειλή δεν είναι μόνο τεχνολογική αλλά σε σημαντικό βαθμό ψυχολογική και συμπεριφορική. Η διεθνής βιβλιογραφία (Hadnagy, 2018; ENISA, 2023) καταδεικνύει σαφώς ότι κανένα μεμονωμένο μέτρο δεν είναι επαρκές. Αντιθέτως απαιτείται η συνδυαστική εφαρμογή της εκπαίδευσης, τεχνικών μηχανισμών, οργανωτικών πολιτικών και συνεχούς αξιολόγησης του κινδύνου.

Αρχικά, η πρώτη προσέγγιση επικεντρώνεται στην εκπαίδευση και ευαισθητοποίηση χρηστών. Η εκπαίδευση αποτελεί τον πυρήνα της άμυνας απέναντι στο social engineering, καθώς ο ανθρώπινος παράγοντας παραμένει η κύρια είσοδος στις κυβερνοεπιθέσεις (Parsons et al., 2019). Έρευνες δείχνουν ότι η καλλιέργεια της κριτικής σκέψης και η κατανόηση ψυχολογικών τεχνικών πειθούς, καθώς και των γνωστικών προκαταλήψεων και των κοινωνικών μηχανισμών που εκμεταλλεύονται οι επιτιθέμενοι, μειώνουν αποδεδειγμένα την πιθανότητα επιτυχούς εξαπάτησης (Parsons et al., 2019). Για να είναι αποτελεσματικά τα διάφορα προγράμματα κατάρτισης οφείλουν να περιλαμβάνουν προσομοιώσεις phishing, πρακτικά σενάρια και δομημένη ανατροφοδότηση, ενισχύοντας έτσι την ικανότητα των χρηστών να αναγνωρίζουν τα σημάδια χειραγώγησης σε πραγματικό χρόνο.

Η ENISA (2023) προτείνει τη σταδιακή και συνεχή εκπαίδευση ευαισθητοποίησης (continuous awareness training) αφού η διαρκής έκθεση και η ενημέρωση για τις εξελισσόμενες μορφές και τεχνικές κοινωνικής μηχανικής, ενισχύουν την ανθεκτικότητα των χρηστών. Επιπρόσθετα, η εκπαίδευση πρέπει να προσαρμόζεται στο επίπεδο ψηφιακής ωριμότητας και στους ρόλους κάθε ομάδας χρηστών. Για παράδειγμα, τα στελέχη υψηλής ευθύνης πρέπει να χρήζουν εξειδικευμένης κατάρτισης (spear-phishing και CEO fraud), ενώ νεότεροι χρήστες χρειάζονται ενισχυτική πρακτική εκπαίδευση (προστασία προσωπικών δεδομένων και υπεύθυνη χρήση κοινωνικών δικτύων).

Σε συνδυασμό με την εκπαίδευση, η τεχνολογία αποτελεί ένα κρίσιμο συμπλήρωμα στην άμυνα κατά της κοινωνικής μηχανικής. Το NIST (2020) τονίζει την ανάγκη εφαρμογής μηχανισμών ισχυρής ταυτοποίησης, όπως την πολυπαραγοντική

αυθεντικοποίηση (MFA), η οποία θεωρείται θεμελιώδης πρακτική. Η MFA μειώνει δραστικά τις πιθανότητες επιτυχούς παραβίασης των λογαριασμών ακόμη και όταν τα διαπιστευτήρια πρόσβασης του χρήστη έχουν υποκλαπεί.

Πρόσθετα τεχνικά μέτρα περιλαμβάνουν:

- Έξυπνα φίλτρα spam και phishing detection: ενισχυμένα με machine learning (*NIST, SP 800-63B*, 2020)
- Data Loss Prevention (DLP), για τον έλεγχο διαρροής ευαίσθητων πληροφοριών (*NIST, SP 800-53*)
- Τακτική ενημέρωση λογισμικού, patching (*NIST, SP 800-40*)
- Endpoint protection, με behavioral analysis (*NIST, SP 800-83*)

Τέλος, οι σύγχρονες ερευνητικές προσεγγίσεις, αναδεικνύουν ότι τα συστήματα ανίχνευσης απειλών που βασίζονται στην τεχνητή νοημοσύνη (AI) μπορούν να εντοπίσουν μοτίβα χειραγώγησης στα κοινωνικά δίκτυα (Schmitt & Flechais, 2024). Ωστόσο, ακόμη και τα πιο εξελιγμένα τεχνικά εργαλεία δεν μπορούν να υποκαταστήσουν την ανθρώπινη κρίση, γι' αυτό και τονίζεται η ανάγκη συνδυασμού τεχνολογικών και συμπεριφορικών μέτρων.

Οι δυο πιο πάνω στρατηγικές, μπορούν να ενισχυθούν και από τα πρότυπα και τις κατευθυντήριες οδηγίες Διεθνών Οργανισμών Κυβερνοασφάλειας. Οι συγκεκριμένοι διεθνείς οργανισμοί παρέχουν δομημένα πλαίσια και εξειδικευμένες οδηγίες που βοηθούν τους οργανισμούς και τις επιχειρήσεις να δομήσουν ολοκληρωμένα προγράμματα προστασίας.

- Η ENISA προτείνει συγκεκριμένες βέλτιστες πρακτικές για την ασφαλή χρήση των κοινωνικών δικτύων, όπως την ελαχιστοποίηση του ψηφιακού αποτυπώματος (digital footprint), την αυστηρή διαχείριση δικαιωμάτων πρόσβασης και τη συνεπή χρήση μηχανισμών επαλήθευσης.
- Το NIST (2020) προσφέρει πρότυπα για το πλαίσιο διαχείρισης κινδύνου (Risk Management Framework), το οποίο περιλαμβάνει την τυποποίηση διαδικασιών για τον εντοπισμό απειλών social engineering, την αξιολόγηση της τρωτότητας και την υλοποίηση διαδικασιών απόκρισης.
- Ο οργανισμός CERT συμβάλλει ενεργά παρέχοντας πρακτικούς οδηγούς για την αναγνώριση της παραπλάνησης και την τυποποίηση της διαδικασίας

αναφοράς περιστατικών ασφαλείας, εξασφαλίζοντας έτσι την γρήγορη και αποτελεσματική αντιμετώπιση.

- Η ενσωμάτωση διεθνών προτύπων, όπως το ISO 27001 και το ISO 27002, ενισχύουν τη συστηματική προστασία, καθώς θέτουν σαφείς απαιτήσεις για πολιτικές πρόσβασης, προστασία των δεδομένων και διαχείριση των συμβάντων ασφαλείας, όλα σημεία άμεσα σχετιζόμενα με την κοινωνική μηχανική.

Η βιβλιογραφία συμφωνεί ότι η αντιμετώπιση του social engineering απαιτεί μια πολυεπίπεδη στρατηγική, η οποία συνδυάζει συμπεριφορικά, τεχνικά και οργανωτικά μέτρα (Hadnagy, 2018). Στο επίπεδο της ανθρώπινης άμυνας, σημαντικό ρόλο διαδραματίζουν η συνεχής εκπαίδευση χρηστών, οι προσομοιώσεις επιθέσεων και η ενίσχυση κουλτούρας ασφάλειας εντός του οργανισμού. Στο τεχνολογικό επίπεδο, η στρατηγική περιλαμβάνει ανάπτυξη εργαλείων AI-based detection, την εφαρμογή αυτοματοποιημένων συστημάτων ειδοποίησης και την ενίσχυση προστασίας λογαριασμών και endpoints. Παράλληλα, η οργανωτική άμυνα στηρίζεται στην καθιέρωση πολιτικών χρήσεων κοινωνικών δικτύων, στη διαχείριση πρόσβασης (least privilege) και στην υιοθέτηση διαδικασιών αναφοράς περιστατικών.

Σύμφωνα με τους Albladi & Weir (2020), η αποτελεσματικότητα των μέτρων ασφαλείας αυξάνεται όταν αυτά βασίζονται σε μοντέλα που λαμβάνουν υπόψη τόσο τα τεχνικά όσο και τα ψυχολογικά χαρακτηριστικά των χρηστών. Οι Quayyum & Freberg (2023) τεκμηριώνουν περαιτέρω αυτή την ανάγκη, υποστηρίζοντας ότι ‘η ενοποίηση τεχνολογικών εργαλείων με στρατηγικές επικοινωνίας και εκπαίδευσης, ενισχύει σημαντικά την ανθεκτικότητα των οργανισμών απέναντι σε στοχευμένες επιθέσεις που πραγματοποιούνται μέσω πλατφορμών κοινωνικών δικτύων’.

Συμπερασματικά η αντιμετώπιση της κοινωνικής μηχανικής δεν αποτελεί ζήτημα μόνο τεχνολογίας, αλλά είναι μια σύνθετη διαδικασία που απαιτεί συνδυασμό γνώσης, εργαλείων, διαδικασιών και κουλτούρας ασφάλειας. Η διεθνής βιβλιογραφία υπογραμμίζει ότι οι οργανισμοί που εφαρμόζουν πολυεπίπεδες στρατηγικές, συνδυάζοντας εκπαίδευση, τεχνικά μέτρα και διεθνή πρότυπα ασφάλειας, εμφανίζουν σημαντικά χαμηλότερο κίνδυνο επιτυχημένων επιθέσεων κοινωνικής μηχανικής.

2.7 Συμπεράσματα και προσανατολισμός της παρούσας έρευνας

Με βάση την παραπάνω βιβλιογραφική ανασκόπηση, αναδεικνύεται με σαφήνεια ότι η κοινωνική μηχανική συνιστά ένα πολυσύνθετο φαινόμενο, το οποίο εδράζεται κυρίως στον ανθρώπινο παράγοντα και ενισχύεται από τα σύγχρονα ψηφιακά περιβάλλοντα, και ιδιαίτερα από τα κοινωνικά δίκτυα. Η υφιστάμενη βιβλιογραφία αναδεικνύει ότι οι επιτιθέμενοι αξιοποιούν συστηματικά ψυχολογικές τεχνικές πειθούς, γνωστικές προκαταλήψεις, συναισθηματικά ερεθίσματα καθώς και στοιχεία της ψηφιακής ταυτότητας των χρηστών, με σκοπό την αύξηση της αποτελεσματικότητας των επιθέσεων social engineering.

Παράλληλα, τονίζεται ότι, παρά την ύπαρξη τεχνικών μέτρων προστασίας, παραγοντες όπως έλλειψη επαρκούς εκπαίδευσης, μη-κριτική χρήση των κοινωνικών δικτύων κ.ά., αυξάνουν σημαντικά την ευαλωτότητα των χρηστών. Ωστόσο, η βιβλιογραφία επικεντρώνεται κυρίως σε θεωρητικά μοντέλα, μελέτες περίπτωσης ή οργανωσιακά περιβάλλοντα, αφήνοντας περιορισμένο πεδίο για την εμπειρική διερεύνηση των αντιλήψεων, στάσεων και συμπεριφορών των ίδιων των χρηστών, στο πλαίσιο της καθημερινής χρήσης των κοινωνικών δικτύων.

Στο πλαίσιο αυτό, η παρούσα έρευνα αποσκοπεί να γεφυρώσει ένα θεωρητικό - εμπειρικό χάσμα, διερευνώντας τον τρόπο με τον οποίο οι χρήστες αντιλαμβάνονται τους κινδύνους του social engineering, τον ρόλο των ψυχολογικών παραγόντων στη λήψη διαδικτυακων αποφάσεων καθώς και την αποτελεσματικότητα των υφιστάμενων στρατηγικών αντιμετώπισης. Κεντρικός στόχος της έρευνας, είναι να εξεταστεί η σχέση μεταξύ χρήσης των κοινωνικών δικτύων, των ψυχολογικών ερεθισμάτων, του επιπέδου εκπαίδευσης και των ψηφιακών δεξιοτήτων με την ευαλωτότητα τους απέναντι σε επιθέσεις κοινωνικής μηχανικής. Ειδικότερα, η έρευνα εστιάζει στη διερεύνηση του βαθμού επίδρασης των συναισθηματικών παραγόντων, της εκπαίδευσης στην κυβερνοασφάλεια και των ατομικών χαρακτηριστικών στη διαμόρφωση της διαδικτυακής συμπεριφοράς των χρηστών στα κοινωνικά δίκτυα.

3. Μεθοδολογία Έρευνας

Στο παρόν κεφάλαιο περιγράφετε αναλυτικά η μεθοδολογική προσέγγιση που ακολουθήθηκε για την υλοποίηση της διπλωματικής εργασίας. Η έρευνα εφαρμόζει συνδυαστική μεθοδολογική προσέγγιση, η οποία περιλαμβάνει συστηματική βιβλιογραφική ανασκόπηση, και ποσοτική εμπειρική έρευνα μέσω ερωτηματολογίου, με στόχο την ολοκληρωμένη διερεύνηση του φαινομένου της κοινωνικής μηχανικής στα κοινωνικά δίκτυα. Η βιβλιογραφική ανασκόπηση καλύπτει το θεωρητικό επίπεδο της ανάλυσης, ενώ η ποσοστική έρευνα εστιάζει στην εμπειρική διερεύνηση των στάσεων, αντιλήψεων και επιπέδων ευαλωτότητας των χρηστών, σύμφωνα με τις κατευθύνσεις της σχετικής επιστημονικής βιβλιογραφίας (Parsons et al., 2019; Albladi & Weir, 2020; Tullet-Prado et al., 2023).

3.1 Σχεδιασμός της έρευνας

Η παρούσα έρευνα ακολουθεί περιγραφικό και διερευνητικό σχεδιασμό. Το εμπειρικό μέρος της μελέτης βασίζεται σε ποσοτική προσέγγιση μέσω δομημένου ερωτηματολογίου, το οποίο επιτρέπει τη διερεύνηση σχέσεων μεταξύ μεταβλητών και τον εντοπισμό προτύπων συμπεριφοράς.

Η ποσοτική έρευνα αποσκοπεί στη διερεύνηση της σχέσης μεταξύ ανεξάρτητων μεταβλητών και εξαρτημένων μεταβλητών. Οι ανεξάρτητες μεταβλητές περιλαμβάνουν:

- δημογραφικά χαρακτηριστικά (φύλο, ηλικία, επίπεδο εκπαίδευσης),
- το επίπεδο χρήσης των κοινωνικών δικτύων (διάρκεια χρήσης),
- τον τύπο πλατφορμών κοινωνικής δικτύωσης που χρησιμοποιούνται (π.χ. Facebook, Instagram, LinkedIn),
- το επίπεδο γνώσης και επίγνωσης κινδύνων κυβερνοασφάλειας,

Ως εξαρτημένες μεταβλητές ορίζονται:

- η αντιλαμβανόμενη ευαλωτότητα σε επιθέσεις κοινωνικής μηχανικής,
- η αυτοαναφερόμενη ικανότητα αναγνώρισης επιθέσεων phishing και impersonation,
- η στάση των χρηστών απέναντι σε ύποπτα μηνύματα και αιτήματα στα κοινωνικά δίκτυα.

Η επιλογή αυτών των εξαρτημένων μεταβλητών προέκυψε άμεσα από τα ερευνητικά κενά που εντοπίστηκαν κατά τη συστηματική βιβλιογραφική

ανασκόπηση και τη θεματική ομαδοποίηση της υφιστάμενης γνώσης. Στη συνέχεια δικαιολογείται η επιλογή των εξαρτημένων μεταβλητών.

Πρώτον, η αντιλαμβανόμενη ευαλωτότητα επιλέχθηκε για να καλύψει το κενό που αφορά τη διαφοροποίηση μεταξύ αντικειμενικού και υποκειμενικού κινδύνου. Η βιβλιογραφία υποδεικνύει ότι πολλοί χρήστες υποτιμούν την έκθεσή τους σε επιθέσεις κοινωνικής μηχανικής, ωστόσο σπανίως εξετάζεται συστηματικά πώς οι ίδιοι αντιλαμβάνονται τον προσωπικό τους κίνδυνο στο περιβάλλον των κοινωνικών δικτύων. Η μεταβλητή αυτή επιτρέπει τη διερεύνηση της γνωστικής διάστασης της ευαλωτότητας, η οποία παραμένει ανεπαρκώς χαρτογραφημένη.

Δεύτερον, η αυτοαναφερόμενη ικανότητα αναγνώρισης και αντιμετώπισης επιθέσεων ανταποκρίνεται σε ένα επιπλέον ερευνητικό κενό που αφορά στην αποτελεσματικότητα της εκπαίδευσης και της δεξιότητας χρήσης ψηφιακών τεχνολογιών. Αν και πολλές μελέτες υποστηρίζουν ότι η εκπαίδευση βελτιώνει την ασφάλεια, λίγες εξετάζουν εμπειρικά κατά πόσο οι χρήστες αισθάνονται ικανοί να εφαρμόσουν αυτή τη γνώση σε πραγματικές συνθήκες κοινωνικής μηχανικής. Η μεταβλητή αυτή γεφυρώνει το χάσμα μεταξύ θεωρητικής κατάρτισης και αντιλαμβανόμενης λειτουργικής ικανότητας.

Τρίτον, η στάση των χρηστών απέναντι στα κοινωνικά δίκτυα και στις πρακτικές κυβερνοασφάλειας επιλέχθηκε για να καλύψει το κενό που αφορά τις κοινωνικές και ψυχολογικές διαστάσεις της ασφάλειας πληροφοριών. Η βιβλιογραφία τείνει να αντιμετωπίζει τους χρήστες ως παθητικούς αποδέκτες κινδύνων, παραβλέποντας τον ρόλο των στάσεων, των πεποιθήσεων και των προθέσεων στη διαμόρφωση συμπεριφορών που είτε ενισχύουν είτε περιορίζουν την ευαλωτότητα.

Συνεπώς, οι τρεις εξαρτημένες μεταβλητές συγκροτούν ένα ενιαίο αναλυτικό πλαίσιο που ανταποκρίνεται στα κενά της υφιστάμενης βιβλιογραφίας, επιτρέποντας μια πολυδιάστατη προσέγγιση της ανθρώπινης ευαλωτότητας σε επιθέσεις κοινωνικής μηχανικής στο περιβάλλον των κοινωνικών δικτύων.

3.2 Πληθυσμός της έρευνας και δειγματοληψία

Ο πληθυσμός της έρευνας αποτελείται απο ενήλικους χρήστες κοινωνικών δικτύων, οι οποίοι χρησιμοποιούν τουλάχιστον μία πλατφόρμα κοινωνικής δικτύωσης σε

καθημερινή βάση και εκτίθενται συστηματικά σε ψηφιακές αλληλεπιδράσεις και ως εκ τούτου, βρίσκονται αντιμέτωποι με αυξημένο κίνδυνο επιθέσεων κοινωνικής μηχανικής (Albladi & Weir, 2020).

Το δείγμα επιλέχθηκε με τη μέθοδο της δειγματοληψίας ευκολίας, η οποία κρίνεται κατάλληλη για διερευνητικές μελέτες, λαμβάνοντας υπόψη τους χρονικούς και πρακτικούς περιορισμούς της παρούσας έρευνας. Το τελικό μέγεθος του δείγματος ανήλθε σε 105 συμμετέχοντες.

Τα βασικά δημογραφικά χαρακτηριστικά που καταγράφηκαν περιλαμβάνουν: το φύλο, ηλικιακή ομάδα, επίπεδο εκπαίδευσης και επαγγελματική κατάσταση.

3.3 Μέσα συλλογής δεδομένων

Για τη συλλογή των πρωτογενών δεδομένων χρησιμοποιήθηκε δομημένο ερωτηματολόγιο, το οποίο σχεδιάστηκε ειδικά για τις ανάγκες της παρούσας μελέτης, βασιζόμενο σε υφιστάμενα θεωρητικά μοντέλα και προηγούμενες σχετικές έρευνες στον τομέα της κοινωνικής μηχανικής. Η αξιοποίηση ερωτηματολογίων αποτελεί μία από τις βασικές μεθοδολογικές προσεγγίσεις για τη διερεύνηση του ανθρώπινου παράγοντα στην κυβερνοασφάλεια και ειδικότερα για τη μελέτη της ευαλωτότητας των χρηστών σε επιθέσεις κοινωνικής μηχανικής.

Παρά τη μεθοδολογική αξία των ερωτηματολογίων, η διεθνής βιβλιογραφία περιλαμβάνει σχετικά περιορισμένο αριθμό εμπειρικών μελετών που εξετάζουν άμεσα την ευαλωτότητα σε επιθέσεις phishing σε περιβάλλοντα κοινωνικής δικτύωσης μέσω αυτοαναφερόμενων δεδομένων. Δύο από τις πλέον αντιπροσωπευτικές και συχνά αναφερόμενες μελέτες στο συγκεκριμένο πεδίο είναι το “*Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model”* και το “*Phishing, Personality Traits and Facebook”*.

Η μελέτη “*Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model”* των Frauenstein & Flowerday (2020), αξιοποιεί ερωτηματολόγια βασισμένα στο μοντέλο των Πέντε Μεγάλων Διαστάσεων Προσωπικότητας (Big Five), όπως εξωστρέφεια, ευσυνειδησία, προνοητικότητα, νευρωτισμός και δεκτικότητα, σε συνδυασμό με κλίμακες που μετρούν heuristic και systematic processing (επιφανειακή και ελεγχόμενη επεξεργασία). Τα

αποτελέσματα έδειξαν ότι ο επιφανειακός τρόπος αξιολόγησης μηνυμάτων σχετίζεται με αυξημένη ευαλωτότητα σε phishing επιθέσεις σε πλατφόρμες κοινωνικής δικτύωσης, ενώ χαρακτηριστικά όπως η ευσυνειδησία λειτουργούν προστατευτικά. Επίσης η ευαλωτότητα σε phishing δεν είναι θέμα μόνο τεχνικής ή γνώσης, αλλά συμπεριφορικών και γνωστικών χαρακτηριστικών που επηρεάζουν τον τρόπο σκέψης. Η συγκεκριμένη προσέγγιση αναδεικνύει τη δυνατότητα των ερωτηματολογίων να λειτουργήσουν ως εργαλείο πρόβλεψης συμπεριφοράς χρηστών σε περιβάλλοντα social networking.

Αντίστοιχα, η μελέτη "*Phishing, Personality Traits and Facebook",* των Halevi, Lewis & Memon (2013), εξετάζει τη σχέση μεταξύ χαρακτηριστικών προσωπικότητας, συμπεριφοράς χρήσης του Facebook και ανταπόκρισης σε phishing επιθέσεις. Μέσω ερωτηματολογίων, που μετρούν τόσο τα χαρακτηριστικά προσωπικότητας όσο και τη συμπεριφορά κοινοποίησης προσωπικών δεδομένων, οι συγγραφείς καταδεικνύουν ότι ορισμένα χαρακτηριστικά προσωπικότητας σχετίζονται με αυξημένη έκθεση προσωπικών πληροφοριών και λιγότερο αυστηρές ρυθμίσεις ιδιωτικότητας. Παρότι η άμεση σύνδεση μεταξύ προσωπικότητας της επιτυχίας phishing επιθέσεων δεν είναι πάντα ισχυρή, τα ευρήματα υποδεικνύουν τη σημασία της συμπεριφοράς στα κοινωνικά δίκτυα ως παράγοντα κινδύνου.

Με βάση τις θεωρητικές και εμπειρικές προσεγγίσεις που παρουσιάστηκαν ανωτέρω, το ερωτηματολόγιο που ετοιμάστηκε αποτελείται από πέντε ενότητες. Κάθε ενότητα του ερωτηματολογίου σχεδιάστηκε ώστε να αντιστοιχεί σε συγκεκριμένες μεταβλητές και ερευνητικούς στόχους της μελέτης. Οι ερωτήσεις της πρώτης ενότητας (ερωτήσεις 1–5) αφορούν στα δημογραφικά και επαγγελματικά χαρακτηριστικά των συμμετεχόντων και χρησιμοποιούνται ως ανεξάρτητες μεταβλητές, προκειμένου να διερευνηθούν πιθανές διαφοροποιήσεις των χρηστών απέναντι σε επιθέσεις κοινωνικής μηχανικής.

Οι ερωτήσεις της δεύτερης ενότητας (ερωτήσεις 6–10) εστιάζουν στις συνήθειες χρήσης των κοινωνικών δικτύων, στο επίπεδο ψηφιακών δεξιοτήτων και στην προηγούμενη εμπειρία των χρηστών με περιστατικά phishing ή κοινωνικής μηχανικής. Η ενότητα αυτή αποσκοπεί στη διερεύνηση της σχέσης μεταξύ της έκθεσης των χρηστών στα κοινωνικά δίκτυα και της πιθανότητας εμπλοκής τους σε περιστατικά κοινωνικής μηχανικής.

Οι ερωτήσεις 11–15 εξετάζουν την αντιλαμβανόμενη αποτελεσματικότητα των υφιστάμενων μέτρων ασφάλειας, τον ρόλο της εκπαίδευσης κυβερνοασφάλειας και τη στάση των χρηστών απέναντι σε νέες τεχνολογικές λύσεις εκπαίδευσης. Μέσω των ερωτήσεων αυτών επιχειρείται η αποτύπωση του βαθμού στον οποίο η εκπαίδευση και τα τεχνικά μέτρα συμβάλλουν στη μείωση της ευαλωτότητας των χρηστών.

Οι ερωτήσεις 16–19 εστιάζουν σε παράγοντες συμπεριφοράς και ψυχολογίας, όπως η επαλήθευση πηγών, η συναισθηματική επιρροή και η ψυχολογική κατάσταση των χρηστών, με στόχο τη διερεύνηση της ανθρώπινης διάστασης, της ασφάλειας πληροφοριών και του τρόπου με τον οποίο οι παράγοντες αυτοί αξιοποιούνται σε επιθέσεις κοινωνικής μηχανικής.

Τέλος, οι ερωτήσεις 20–25 αφορούν σύγχρονες και αναδυόμενες απειλές, όπως περιεχόμενο παραγόμενο από τεχνητή νοημοσύνη, deepfakes, προηγμένες τεχνικές phishing και ζητήματα προστασίας απορρήτου. Η ενότητα αυτή επιδιώκει μια διερευνητική αποτύπωση της ετοιμότητας των χρηστών απέναντι σε εξελισσόμενες μορφές κοινωνικής μηχανικής και της αντιλαμβανόμενης ευθύνης των πλατφορμών κοινωνικής δικτύωσης.

Συνολικά το ερωτηματολόγιο σχεδιάστηκε με διερευνητικό χαρακτήρα, με στόχο την αρχική εμπειρική αποτύπωση της ευαλωτότητας, χωρίς πρόθεση γενίκευσης των αποτελεσμάτων στο σύνολο του πληθυσμού. Το πλήρες ερωτηματολόγιο περιγράφεται και αναλύεται στην ενότητα 3.8 που ακολουθεί, ενώ παρατίθεται πλήρως στο Παράρτημα Β της παρούσας εργασίας.

Πίνακας 1: Ανάλυση ερωτήσεων ερωτηματολογίου: σκοπός και στόχος

Ερωτήσεις	Σκοπός	Στόχος
1–5	Δημογραφικά & επαγγελματικά	Σύγκριση ομάδων
6–7	Διάρκεια & τύπος χρήσης social media	Έκθεση σε κίνδυνο
8–10	Ψηφιακές δεξιότητες & εμπειρία	Προηγούμενη ευαλωτότητα
11	Αντίληψη τεχνικών μέτρων	Αποτελεσματικότητα άμυνας

Ερωτήσεις	Σκοπός	Στόχος
12, 18	Συναισθηματική επιρροή	Ψυχολογικές τεχνικές
13–15	Εκπαίδευση & awareness	Ρόλος εκπαίδευσης
16, 24	Συμπεριφορά επαλήθευσης	Προληπτικές πρακτικές
17, 19	Προσωπικοί & ψυχολογικοί παράγοντες	Ανθρώπινη ευαλωτότητα
20–23	AI, deepfakes, profiling	Αναδυόμενες απειλές
25	Ευθύνη πλατφορμών	Συστημική προστασία

Οι περισσότερες ερωτήσεις είναι κλειστού τύπου και βασίζονται σε πενταβάθμια κλίμακα Likert (1 = Ποτέ έως 5 = Πολύ συχνά), πρακτική που χρησιμοποιείται ευρέως για τη μελέτη των ανθρώπινων παραγόντων στην ασφάλεια πληροφοριών (Parsons et al., 2019).

3.4 Διαδικασία συλλογής δεδομένων

Η συλλογή των δεδομένων πραγματοποιήθηκε μέσω ηλεκτρονικής διανομής του ερωτηματολογίου με τη χρήση πλατφόρμας διαδικτυακών φορμών, Google Forms. Η επιλογή της συγκεκριμένης μεθόδου κρίθηκε κατάλληλη, καθώς διευκόλυνε την πρόσβαση σε μεγαλύτερο αριθμό συμμετεχόντων και διασφάλισε την ανωνυμία και την προστασία των προσωπικών δεδομένων τους. Η διαδικασία περιλάμβανε αρχικά την σύνταξη και τον πιλοτικό έλεγχο του ερωτηματολογίου, ακολούθως τη διάθεση του ερωτηματολογίου στο ερευνητικό δείγμα και τη συλλογή των απαντήσεων, καθώς και τον έλεγχο της πληρότητας και της εγκυρότητας των απαντήσεων. Στο τελικό στάδιο, τα δεδομένα κωδικοποιήθηκαν και προετοιμάστηκαν κατάλληλα για στατιστική ανάλυση. Η χρονική διάρκεια της διαδικασίας συλλογής δεδομένων διήρκεσε περίπου 3 εβδομάδες.

3.5 Στατιστική ανάλυση δεδομένων

Τα αποτελέσματα της ανάλυσης και οι θεματικές συστάδες (clusters) που παρουσιάζονται στη μελέτη, προέκυψαν από το λογισμικό εργαλείο myAutoML (Bakas et al., 2025) και συγκεκριμένα από το Bibliometrics module, το οποίο πραγματοποιεί βιβλιομετρική χαρτογράφηση και ομαδοποίηση της βιβλιογραφίας με βάση τα μεταδεδομένα των δημοσιεύσεων (https://mireng.ai/bibliometrics). Το

εργαλείο δέχεται βιβλιογραφικά αρχεία σε μορφή BibTeX, εξάγει αυτόματα βασικά στοιχεία (π.χ. συγγραφείς, τίτλους, λέξεις-κλειδιά, έτη δημοσίευσης) και στη συνέχεια κατασκευάζει δίκτυα συν-εμφάνισης όρων και συνεργασιών, πάνω στα οποία εφαρμόζει μια dissimilarity-consistent προσέγγιση για τη μέτρηση αποστάσεων/ομοιοτήτων και τον εντοπισμό θεματικών ομάδων. Επιπλέον, ενσωματώνει χρονική ανάλυση ώστε να αποτυπώνει την εξέλιξη των θεμάτων και να υποστηρίζει την ανάδειξη τάσεων, ενώ παρέχει διαδραστικές οπτικοποιήσεις (βιβλιομετρικούς χάρτες και δίκτυα) και αναφορές με στατιστικές συνοψίσεις, διευκολύνοντας μια πιο γρήγορη και τεκμηριωμένη χαρτογράφηση του ερευνητικού πεδίου.

3.6 Βιβλιογραφική ανασκόπηση ως μεθοδολογικό εργαλείο

Η βιβλιογραφική ανασκόπηση αποτέλεσε θεμελιώδες στάδιο της παρούσας έρευνας και λειτούργησε όχι μόνο περιγραφικά, αλλά και αναλυτικά και ερμηνευτικά**,** με στόχο τον εντοπισμό ερευνητικών κενών. Όπως παρουσιάστηκε αναλυτικά στο Κεφάλαιο 2, η ανασκόπηση της διεθνούς βιβλιογραφίας πραγματοποιήθηκε συστηματικά και οργανωμένα, ακολουθώντας μεθοδολογικές πρακτικές που προτείνονται για τη χαρτογράφηση ώριμων και αναδυόμενων ερευνητικών πεδίων (Parsons et al., 2019; Albladi & Weir, 2020).

Στο πλαίσιο αυτό, χρησιμοποιήθηκαν βιβλιομετρικά και αναλυτικά εργαλεία (όπως εργαλεία αναζήτησης και ομαδοποίησης επιστημονικών πηγών σε βάσεις δεδομένων όπως Scopus, Web of Science, IEEE Xplore, Google Scholar, MDPI και άλλα), με σκοπό την ανίχνευση θεματικών μοτίβων, τη συχνότητα εμφάνισης εννοιών και τη μεταξύ τους συνάφεια. Μέσα από τη διαδικασία αυτή προέκυψαν θεματικές συστάδες (clusters) της βιβλιογραφίας, οι οποίες αντιστοιχούν σε βασικούς άξονες έρευνας στον τομέα της κοινωνικής μηχανικής και των κοινωνικών δικτύων.

Για κάθε θεματικό cluster πραγματοποιήθηκε συνοπτική αλλά στοχευμένη ανάλυση της υφιστάμενης γνώσης, γεγονός που επέτρεψε τον εντοπισμό περιοχών με περιορισμένη εμπειρική τεκμηρίωση, ασυνέπειες στα ερευνητικά ευρήματα ή ανεπαρκή διερεύνηση του ρόλου των κοινωνικών δικτύων ως ενισχυτικού μηχανισμού των επιθέσεων κοινωνικής μηχανικής. Τα ερευνητικά αυτά κενά

αξιοποιήθηκαν ως θεωρητικό υπόβαθρο για τη διαμόρφωση των ερευνητικών ερωτημάτων και του ερωτηματολογίου της παρούσας μελέτης.

Συγκεκριμένα οι θεματικές συστάδες που προέκυψαν είναι οι εξής:
Cluster 1: Υπάρχει περιορισμένη γνώση για το πόσο αποτελεσματικά είναι τα υφιστάμενα αντίμετρα απέναντι σε νέες μορφές phishing, ιδιαίτερα σε κινητές συσκευές και κοινωνικά δίκτυα. Επίσης, δεν έχει μελετηθεί επαρκώς η διαχρονική επίδραση της εκπαίδευσης χρηστών, ούτε οι ψυχολογικοί και οργανωτικοί παράγοντες που επηρεάζουν την ευαλωτότητα των χρηστών.

Cluster 2: Η αποτελεσματικότητα των σημερινών προγραμμάτων εκπαίδευσης σε πραγματικές συνθήκες δεν έχει επαρκώς τεκμηριωθεί, ούτε η μακροχρόνια επίδρασή τους σε διαφορετικά οργανωτικά πλαίσια. Παράλληλα, υπάρχει κενό γνώσης σχετικά με το πώς οι ψυχολογικοί παράγοντες επηρεάζουν την ευαλωτότητα στις επιθέσεις κοινωνικής μηχανικής, ενώ η αξιοποίηση αναδυόμενων τεχνολογιών, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση, παραμένουν ανεπαρκώς διερευνημένες για την ανάπτυξη προσαρμοστικών και πιο αποτελεσματικών εκπαιδευτικών λύσεων.

Cluster 3: Ενώ οι επιπτώσεις των επιθέσεων κοινωνικής μηχανικής έχουν μελετηθεί εκτενώς, η αποτελεσματικότητα των στρατηγικών μετριασμού σε πραγματικές συνθήκες και οι ψυχολογικές πτυχές μεταξύ δημογραφικών ομάδων παραμένουν ανεπαρκώς διερευνημένες. Μελλοντικές μελέτες μπορούν να εστιάσουν σε στοχευμένες στρατηγικές παρεμβάσεις και προσαρμοσμένα εκπαιδευτικά μοντέλα, αξιοποιώντας παράλληλα τεχνολογίες, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση για την πρόβλεψη και πρόληψη νέων μορφών απειλών.

Cluster 4: Υπάρχει έλλειψη εμπειρικών δεδομένων για την αποτελεσματικότητα των εκπαιδευτικών προγραμμάτων για τον ψηφιακό γραμματισμό και την ασφάλεια, ενώ οι τεχνολογίες επιρροής και τα deepfakes που βασίζονται στην τεχνητή νοημοσύνη, δημιουργούν νέες ηθικές και πρακτικές προκλήσεις. Η μελλοντική έρευνα πρέπει να εστιάσει σε παρεμβάσεις που ενισχύουν την κριτική σκέψη απέναντι στην παραπληροφόρηση σε διαφορετικές δημογραφικές ομάδες και σε πλαίσια αξιολόγησης των ευρύτερων επιπτώσεων αυτών των τεχνολογιών στην εμπιστοσύνη και στις διαδικτυακές αλληλεπιδράσεις.

Συνεπώς, το ερωτηματολόγιο που χρησιμοποιήθηκε στην εμπειρική φάση της έρευνας, σχεδιάστηκε έτσι ώστε να αντλεί άμεσα από τα εντοπισμένα ερευνητικά κενά, επιδιώκοντας όχι την πλήρη κάλυψή τους — κάτι που δεν είναι εφικτό στο πλαίσιο μίας διπλωματικής εργασίας — αλλά τη διεξαγωγή μιας διερευνητικής αποτύπωσης της συμπεριφοράς των χρηστών. Η προσέγγιση αυτή αποσκοπεί στη διαμόρφωση μιας αρχικής εικόνας σχετικά με το κατά πόσο τα θεωρητικά κενά που καταγράφονται στη βιβλιογραφία, αντανακλώνται και σε εμπειρικό επίπεδο καθώς και στον προσδιορισμό πιθανών κατευθύνσεων για μελλοντική, εκτενέστερη έρευνα.

3.7 Ηθικά ζητήματα

Η έρευνα συμμορφώθηκε πλήρως με τις αρχές της ερευνητικής δεοντολογίας. Η συμμετοχή ήταν εθελοντική και ανώνυμη, ενώ πριν την έναρξη του ερωτηματολογίου παρέχονταν πληροφορίες σχετικά με τον σκοπό της έρευνας και τη χρήση των δεδομένων.

Δεν συλλέχθηκαν προσωπικά δεδομένα που να επιτρέπουν την ταυτοποίηση των συμμετεχόντων. Σύμφωνα με τη φύση της έρευνας και τη χρήση ανώνυμου ερωτηματολογίου, απαιτήθηκε έγκριση από την Επιτροπή Δεοντολογίας και Βιοηθικής του Πανεπιστημίου Νεάπολις Πάφος, η οποία εκδόθηκε και υπάρχει συνημμένη στο Παράρτημα Α.

3.8 Ανάλυση ερωτήσεων ερωτηματολογίου

Ακολουθεί αναλυτική περιγραφή των ερωτήσεων του ερωτηματολογίου, οι οποίες διαμορφώθηκαν με στόχο να προσανατολιστούν στις περιοχές περιορισμένης εμπειρικής τεκμηρίωσης, που αναδείχθηκαν από τη βιβλιογραφική ανάλυση, ώστε να επιτευχθεί στοχευμένη διερεύνηση των λιγότερο φωτισμένων πτυχών της κοινωνικής μηχανικής στο περιβάλλον των κοινωνικών δικτύων.

1. Φύλο

2. Ηλικία

3. Επίπεδο Εκπαίδευσης

4. Επάγγελμα / Απασχόληση

5. Τομέας Εργασίας (αν εργάζεστε)

Οι πέντε πιο πάνω ερωτήσεις αποτελούν τμήμα των ανεξάρτητων μεταβλητών και είναι απαραίτητες, διότι μπορούν να ερμηνεύσουν τις διαφοροποιήσεις στην

ευαλωτότητα μεταξύ των ατόμων, λειτουργώντας ως δημογραφικοί και κοινωνικοί προσδιοριστές του κινδύνου.

6. Χρήση Κοινωνικών Δικτύων (Χρόνος ανά ημέρα)

- Τύπος: Ανεξάρτητη μεταβλητή
- Αποσκοπεί να δείξει αν ο χρόνος που αφιερώνει κάποιος στα social media σχετίζεται με μεγαλύτερη ή μικρότερη ευαλωτότητα σε social engineering ή phishing

7. Πλατφόρμες που χρησιμοποιείτε συχνότερα (Επιλέξτε έως 3)

- Τύπος: Ανεξάρτητη μεταβλητή
- Αποσκοπεί να εξετάσει αν συγκεκριμένες πλατφόρμες (π.χ. TikTok, Facebook) σχετίζονται με διαφορετικά επίπεδα έκθεσης ή κίνδυνου.

8. Επίπεδο Ψηφιακών Δεξιοτήτων (αυτοαξιολόγηση)

- Τύπος: Ανεξάρτητη μεταβλητή
- Αποσκοπεί να διερευνήσει αν οι ψηφιακές δεξιότητες επηρεάζουν την ικανότητα αναγνώρισης απειλών και την αντίσταση σε social engineering.

9. Έχετε παρακολουθήσει ποτέ εκπαίδευση/σεμινάριο κυβερνοασφάλειας;

- Τύπος: Ανεξάρτητη μεταβλητή
- Αποσκοπεί να μετρήσει αν η εκπαίδευση σχετίζεται με καλύτερη επίγνωση και μικρότερη ευαλωτότητα.

10. Έχετε πέσει θύμα διαδικτυακής απάτης / phishing / social engineering;

- Τύπος: Ανεξάρτητη μεταβλητή
- Αποσκοπεί να αξιολογήσει αν η προηγούμενη εμπειρία επηρεάζει τη μελλοντική συμπεριφορά ή την επαγρύπνηση του χρήστη.

11. Πόσο αποτελεσματικά θεωρείτε ότι είναι τα τρέχοντα μέτρα ασφαλείας (όπως φίλτρα spam, προειδοποιήσεις browser, ειδοποιήσεις εφαρμογών κινητού) στην προστασία σας από νέες ή άγνωστες απόπειρες phishing;

- Τύπος: Εξαρτημένη μεταβλητή
- Σχετίζεται με την αντίληψη αποτελεσματικότητας των στρατηγικών αντιμετώπισης του phishing.

12. Πόσο συχνά βασίζεστε στη διαίσθηση ή σε συναισθηματικά ερεθίσματα (π.χ. αίσθηση επείγοντος, φόβος, περιέργεια) όταν αποφασίζετε αν θα εμπιστευτείτε ένα μήνυμα ή έναν σύνδεσμο στο διαδίκτυο;

- Τύπος: Εξαρτημένη μεταβλητή

- Μετρά πόσο οι συναισθηματικές αντιδράσεις επηρεάζουν την έκθεση σε απάτες στο διαδίκτυο όπως phishing ή επιθέσεις social engineering.

13. Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αντιμετωπίζετε αποτελεσματικά πραγματικές ή απρόσμενες απόπειρες κοινωνικής μηχανικής;

- Τύπος: Εξαρτημένη μεταβλητή
- Σχετίζεται με το ερευνητικό κενό για την έλλειψη αξιολόγησης της πραγματικής αποτελεσματικότητας των εκπαιδεύσεων

14. Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αναπτύξετε την ικανότητα αναγνώρισης και εντοπισμού ψευδών ή παραπλανητικών πληροφοριών στα κοινωνικά δίκτυα;

- Τύπος: Εξαρτημένη μεταβλητή
- Δείχνει την έλλειψη μελέτης της αποτελεσματικότητας εκπαιδευτικών προγραμμάτων ψηφιακού γραμματισμού.

15. Πόσο θετικά θα βλέπατε τη χρήση "έξυπνων" εργαλείων εκπαίδευσης (π.χ. προσαρμοστικών εκπαιδευτικών modules με τεχνητή νοημοσύνη) που προσαρμόζονται στο προφίλ και τις ανάγκες του χρήστη για την ενίσχυση της προστασίας από επιθέσεις κοινωνικής μηχανικής;

- Τύπος: Εξαρτημένη μεταβλητή
- Συνδέεται με το κενό που αφορά την ανάγκη για ενσωμάτωση τεχνητής νοημοσύνης σε adaptive training.

16. Πόσο συχνά ελέγχετε αν ένας σύνδεσμος ή μια προσφορά που εμφανίζεται στο κοινωνικό δίκτυο που χρησιμοποιείτε προέρχεται από αξιόπιστη πηγή πριν κάνετε κλικ;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στη συμπεριφορική επαγρύπνηση του χρήστη στα κοινωνικά δίκτυα απέναντι σε τεχνικές social engineering.

17. Σε ποιο βαθμό πιστεύετε ότι προσωπικά χαρακτηριστικά όπως ηλικία ή εμπειρία στο διαδίκτυο επηρεάζουν την πιθανότητά σας να πέσετε θύμα κοινωνικής μηχανικής στα κοινωνικά δίκτυα;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στην αντίληψη του χρήστη για το πώς οι ψυχολογικοί και δημογραφικοί παράγοντες επηρεάζουν την ευαλωτότητά τους σε social engineering.

18. Πόσο συχνά νιώθετε ότι μηνύματα ή αναρτήσεις στα κοινωνικά δίκτυα προσπαθούν να επηρεάσουν τα συναισθήματά σας (π.χ. φόβο, επείγον, συμπόνια) για να σας πείσουν να κάνετε κάποια ενέργεια;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στην αντίληψη του χρήστη για τη συναισθηματική χειραγώγηση για να τον οδηγήσουν σε επικίνδυνη συμπεριφορά.

19.Σε ποιο βαθμό θεωρείτε ότι η δική σας ψυχολογική κατάσταση (π.χ. κόπωση, άγχος, διάσπαση προσοχής, βιασύνη) μειώνει την προσοχή σας και αυξάνει την πιθανότητα να παραβλέψετε σημάδια κινδύνου σε μια πιθανή επίθεση phishing ή κοινωνικής μηχανικής;

- Τύπος: Εξαρτημένη μεταβλητή
- Ευθυγραμμίζεται με το κενό για την περιορισμένη μελέτη της αλληλεπίδρασης ψυχολογικών παραγόντων και ευαλωτότητας σε social engineering.

20. Πόσο προετοιμασμένοι αισθάνεστε να εντοπίσετε περιεχόμενο που μπορεί να έχει δημιουργηθεί ή τροποποιηθεί από τεχνητή νοημοσύνη (π.χ. AI-generated posts, bots, προπαγάνδα) με σκοπό την παραπλάνηση;

- Τύπος: Εξαρτημένη μεταβλητή
- Δείχνει την εμπιστοσύνη και την επίγνωση του χρήστη απέναντι σε AI-ενισχυμένες επιρροές.

21. Όταν βλέπετε βίντεο ή εικόνες στα κοινωνικά δίκτυα, πόσο συχνά εξετάζετε την πιθανότητα να είναι αλλοιωμένα ή deepfakes πριν τα θεωρήσετε αξιόπιστα;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στην ικανότητα κριτικής σκέψης απέναντι σε Deepfakes και σε οπτικές παραποιήσεις.

22. Πόσο συχνά αντιμετωπίζετε ή αναγνωρίζετε μηνύματα/email που φαίνεται να είναι phishing, αλλά χρησιμοποιούν μεθόδους πέρα από την παραπλάνηση μέσω URL (π.χ. παραπλανητικά μηνύματα, συνημμένα αρχεία, fake ανακοινώσεις);

- Τύπος: Εξαρτημένη μεταβλητή
- Συνδέεται με το κενό για την ανάγκη εξέτασης πολλαπλών τεχνικών phishing πέρα από το URL mimicking (παραπλάνηση URL).

23. Πόσο συχνά θεωρείται ότι επιτιθέμενοι κοινωνικής μηχανικής αξιοποιούν στοιχεία του προσωπικού σας προφίλ (π.χ. ενδιαφέροντα, δημόσιες

αναρτήσεις, λίστα φίλων) στα κοινωνικά δίκτυα για να δημιουργήσουν πειστικά μηνύματα;

- Τύπος: Εξαρτημένη μεταβλητή
- Μετρά αν οι χρήστες κατανοούν ότι τα κοινωνικά δίκτυα δεν είναι απλώς πλατφόρμες επικοινωνίας, αλλά και “δεξαμενές πληροφοριών” για επιθέσεις.

24. Πόσο συχνά ελέγχετε τις ρυθμίσεις απορρήτου στα κοινωνικά σας δίκτυα;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στην προληπτική συμπεριφορά ασφάλειας του χρήστη στα social media και τη μείωση της έκθεσης σε social engineering.

25. Θεωρείτε ότι τα κοινωνικά δίκτυα κάνουν αρκετά για να προστατεύσουν τους χρήστες από phishing και social engineering;

- Τύπος: Εξαρτημένη μεταβλητή
- Αφορά στην αντίληψη των χρηστών για την ευθύνη και την αποτελεσματικότητα των ίδιων των πλατφορμών κοινωνικής δικτύωσης στην κυβερνοασφάλεια.

4. Αποτελέσματα και Ερμηνευτική Ανάλυση

4.1 Εισαγωγικός σχολιασμός – Σκοπός και ερευνητικές υποθέσεις

Σκοπός της παρούσας εμπειρικής έρευνας είναι η διερεύνηση της ευαλωτότητας των χρηστών των κοινωνικών δικτύων απέναντι σε επιθέσεις κοινωνικής μηχανικής, με έμφαση στη σχέση μεταξύ δημογραφικών χαρακτηριστικών, προτύπων χρήσης των social media, επιπέδου ψηφιακών δεξιοτήτων, ψυχολογικών παραγόντων και προληπτικής συμπεριφοράς ασφάλειας. Στο πλαίσιο αυτό, η μελέτη εξετάζει κατά πόσο οι παραπάνω παράγοντες συνδέονται με την αυξημένη ή μειωμένη έκθεση σε πρακτικές phishing και social engineering, αλλά και με τον τρόπο που οι χρήστες αντιλαμβάνονται την αποτελεσματικότητα των ίδιων των πλατφορμών στην προστασία τους.

Με βάση τη βιβλιογραφία και τα θεωρητικά μοντέλα που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, διατυπώθηκαν συγκεκριμένα ερευνητικά ερωτήματα και υποθέσεις που αφορούν:

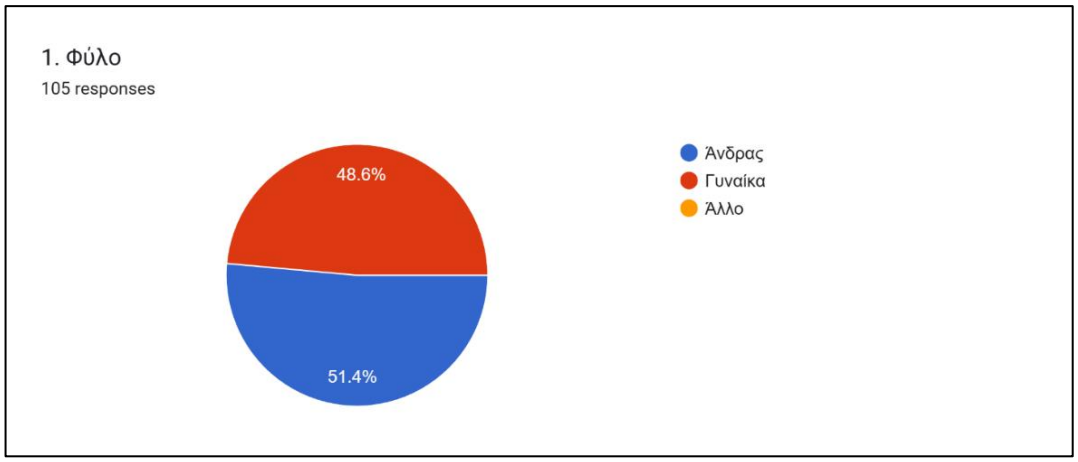
(α) τη σχέση δημογραφικών μεταβλητών και επιπέδου εκπαίδευσης με την ευαλωτότητα σε επιθέσεις κοινωνικής μηχανικής,

(β) την επίδραση των ψηφιακών δεξιοτήτων και της εκπαίδευσης στην κυβερνοασφάλεια στην προληπτική συμπεριφορά των χρηστών και

(γ) τη σημασία των συναισθηματικών και ψυχολογικών ερεθισμάτων στη λήψη διαδικτυακών αποφάσεων.

4.2 Περιγραφικά ευρήματα

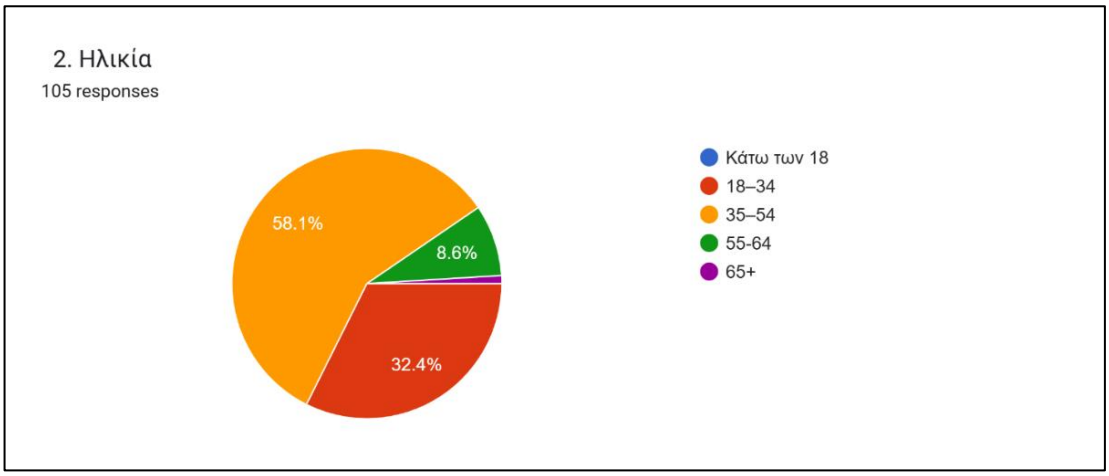
Το τελικό δείγμα της έρευνας αποτελείται από 105 συμμετέχοντες, εκ των οποίων 51 ήταν γυναίκες και 54 άνδρες, γεγονός που υποδηλώνει μια σχετικά ισορροπημένη κατανομή ως προς το φύλο (Διάγραμμα 1). Η σύνθεση αυτή επιτρέπει την αξιόπιστη αποτύπωση τάσεων χωρίς έντονη μεροληψία υπέρ συγκεκριμένης δημογραφικής ομάδας.



Διάγραμμα 1: Φύλο

Πηγή: google forms

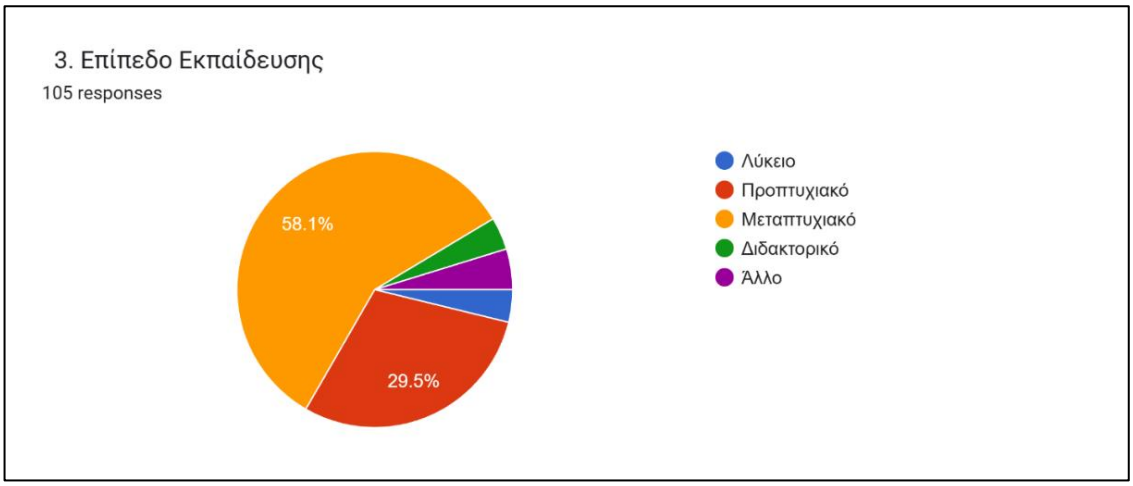
Αναφορικά με τα υπόλοιπα δημογραφικά χαρακτηριστικά, το δείγμα εμφανίζει ουσιαστική ποικιλία, η οποία δεν λειτουργεί μόνο περιγραφικά αλλά και ερμηνευτικά για την κατανόηση της διαδικτυακής συμπεριφοράς και της έκθεσης σε επιθέσεις κοινωνικής μηχανικής. Η ηλικιακή κατανομή (Διάγραμμα 2), με κυρίαρχη την ομάδα 35–54 (58,1%), υποδηλώνει ότι μεγάλο μέρος των συμμετεχόντων βρίσκεται σε φάση ζωής με αυξημένη λειτουργική χρήση του διαδικτύου (εργασιακές επικοινωνίες, υπηρεσίες, συναλλαγές, διαχείριση πολλαπλών υποχρεώσεων). Αυτό έχει σημασία διότι η κοινωνική μηχανική αξιοποιεί συχνά ακριβώς τέτοια περιβάλλοντα “πίεσης χρόνου” και πολλαπλών ρόλων, όπου οι αποφάσεις λαμβάνονται γρηγορότερα και η προσοχή κατακερματίζεται.



Διάγραμμα 2: Ηλικία

Πηγή: google forms

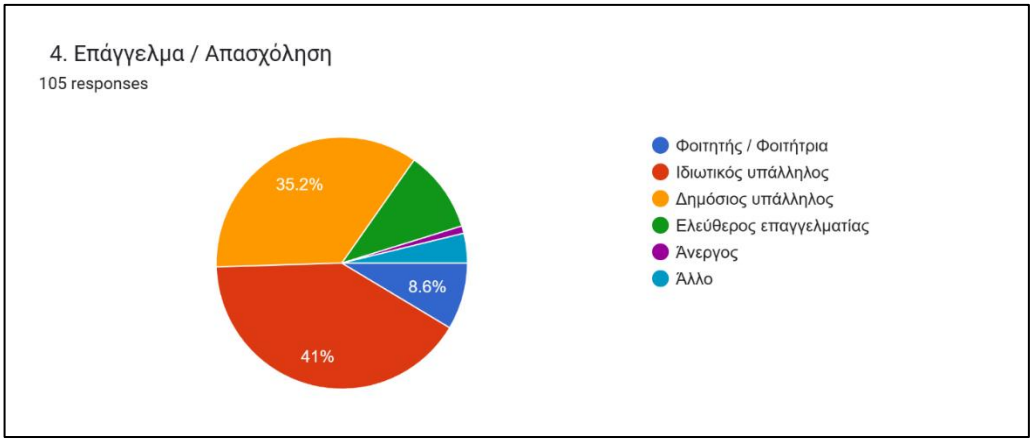
Παράλληλα, το επίπεδο εκπαίδευσης (Διάγραμμα 3) παρουσιάζει διασπορά, με σημαντική παρουσία τριτοβάθμιας/μεταπτυχιακής εκπαίδευσης. Το εύρημα αυτό επιτρέπει μια πιο λεπτή ανάγνωση: από τη μία πλευρά, υψηλότερο μορφωτικό υπόβαθρο μπορεί επιφανειακά να συνδέεται με μεγαλύτερη ικανότητα κατανόησης πληροφοριών και κανόνων ασφάλειας· από την άλλη, δεν εγγυάται αυτόματα ασφαλέστερη συμπεριφορά, καθώς οι επιθέσεις κοινωνικής μηχανικής στηρίζονται περισσότερο σε ψυχολογικούς μηχανισμούς (εμπιστοσύνη, αυθεντία, φόβος, επείγον) παρά σε καθαρά τεχνική γνώση. Επομένως, η ύπαρξη διαφορετικών επιπέδων εκπαίδευσης στο δείγμα βοηθά να διερευνηθεί εάν η “γνώση” λειτουργεί προστατευτικά ή αν υπερισχύουν συμπεριφορικοί παράγοντες.



Διάγραμμα 3: Επίπεδο Εκπαίδευσης

Πηγή: google forms

Η επαγγελματική κατάσταση (Διάγραμμα 4) και ειδικότερα η παρουσία εργαζομένων, φοιτητών και ανέργων δίνει επιπλέον ερμηνευτική ισχύ, επειδή κάθε κατηγορία βιώνει διαφορετικά κίνητρα, ρουτίνες και βαθμό έκθεσης σε ψηφιακές αλληλεπιδράσεις. Για παράδειγμα, οι εργαζόμενοι είναι πιθανότερο να έρχονται συχνά αντιμέτωποι με emails, εταιρικές πλατφόρμες και "τυπικές" ροές επικοινωνίας που μπορούν να μιμηθούν πειστικά οι επιτιθέμενοι (business email compromise, ψευδή τιμολόγια, δήθεν HR/IT ειδοποιήσεις). Αντίστοιχα, οι φοιτητές ενδέχεται να είναι πιο εκτεθειμένοι σε σενάρια που αξιοποιούν εκπαιδευτικές υπηρεσίες ή κοινωνικά δίκτυα, ενώ οι άνεργοι μπορεί να είναι πιο ευάλωτοι σε θεματικές απάτες γύρω από αγγελίες/προσφορές εργασίας ή "ευκαιρίες" που αξιοποιούν την ανάγκη και την προσδοκία.

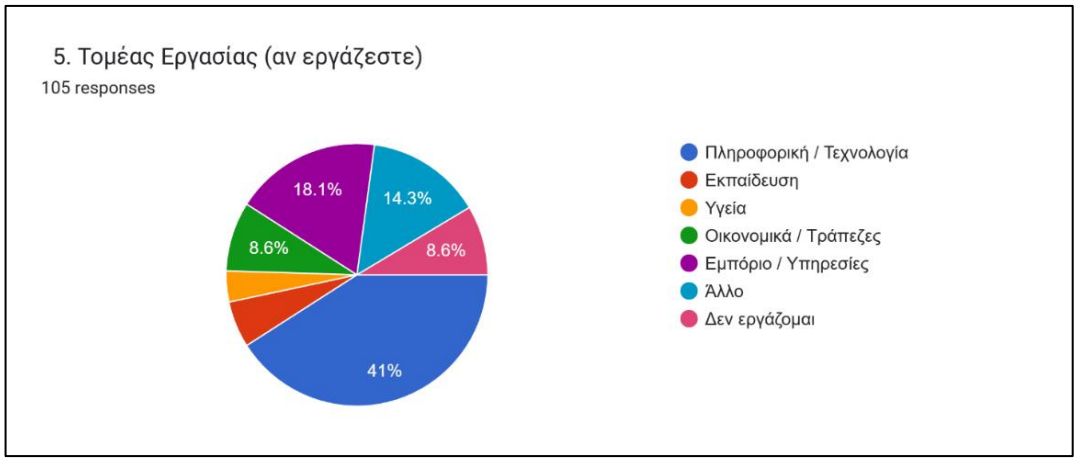


Διάγραμμα 4: Επάγγελμα / Απασχόληση

Πηγή: google forms

Τέλος, ο τομέας εργασίας (Διάγραμμα 5) προσθέτει ένα ιδιαίτερα κρίσιμο επίπεδο ερμηνείας: η έντονη παρουσία ατόμων από την Πληροφορική/Τεχνολογία, αλλά και η συμμετοχή κλάδων όπως Εκπαίδευση, Υγεία, Οικονομικά/Τράπεζες, Εμπόριο κ.ά., επιτρέπει να εξεταστεί εάν η επαγγελματική κουλτούρα και οι καθημερινές πρακτικές ενός κλάδου διαμορφώνουν διαφορετικές "ρουτίνες εμπιστοσύνης". Σε ορισμένους τομείς οι διαδικασίες είναι πιο τυποποιημένες (π.χ. οικονομικές εγκρίσεις), άρα οι επιθέσεις στοχεύουν σε μίμηση διαδικασίας· σε άλλους, η επικοινωνία βασίζεται περισσότερο στη διαπροσωπική εμπιστοσύνη και στην εξυπηρέτηση (π.χ. εκπαίδευση/υγεία), άρα οι επιτιθέμενοι μπορεί να εκμεταλλευτούν την προθυμία ανταπόκρισης. Έτσι, η ποικιλομορφία του Δείγματος δεν ενισχύει μόνο την αντιπροσωπευτικότητα, αλλά επιτρέπει να "διαβαστούν" τα ευρήματα μέσα από διαφορετικά κοινωνικά και εργασιακά πλαίσια — δηλαδή να

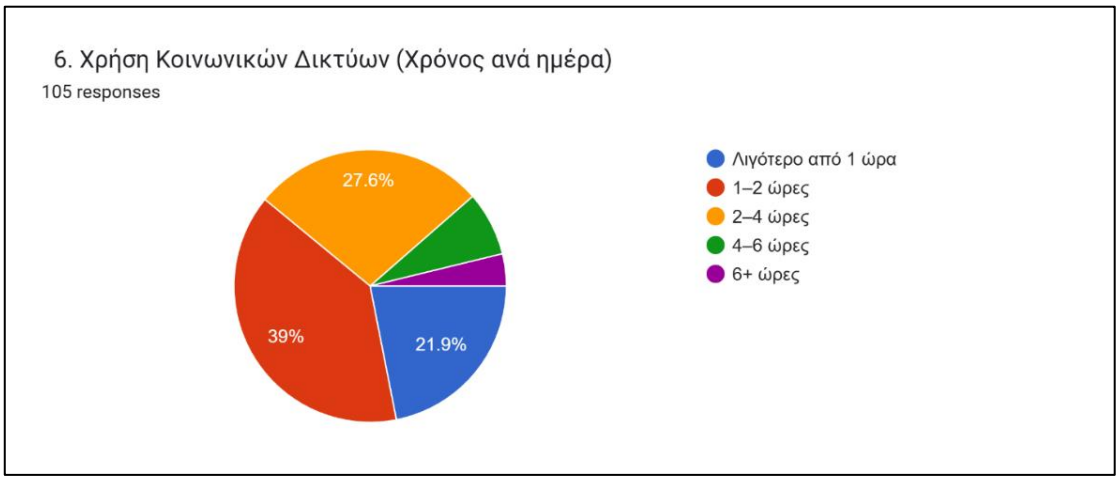
διερευνηθεί όχι μόνο ποιοι είναι ευάλωτοι, αλλά και μέσα σε ποια περιβάλλοντα και με ποιους μηχανισμούς.



Διάγραμμα 5: Τομέας Εργασίας (αν εργάζεστε)

Πηγή: google forms

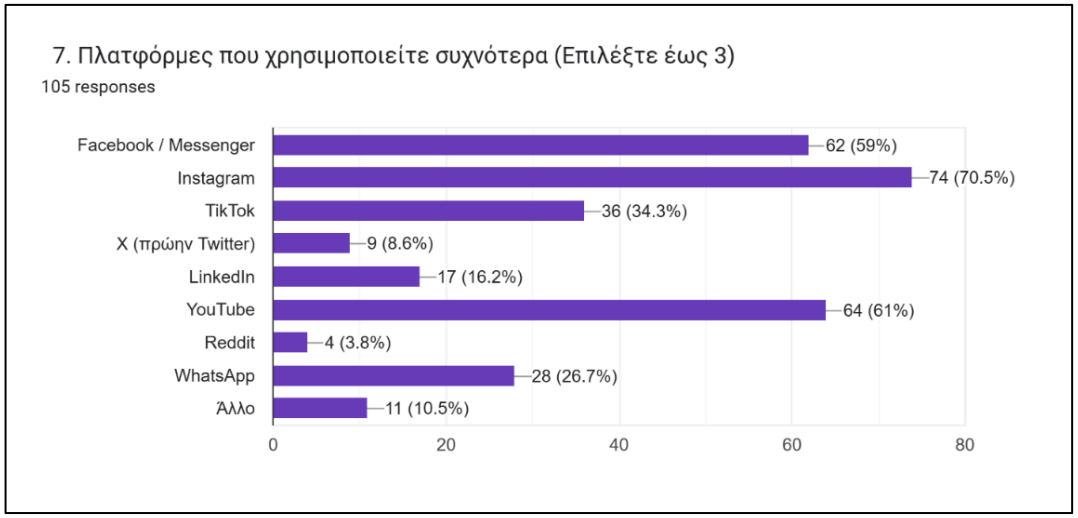
Ως προς τη χρήση των κοινωνικών δικτύων (Διάγραμμα 6), τα αποτελέσματα δείχνουν ότι η πλειονότητα των συμμετεχόντων αφιερώνει σημαντικό χρόνο σε καθημερινή βάση, με κυρίαρχες τις κατηγορίες 1–2 ώρες και 2–4 ώρες ημερησίως. Η συχνή και συστηματική αυτή ενασχόληση υποδηλώνει υψηλό βαθμό έκθεσης σε ψηφιακά ερεθίσματα, ειδοποιήσεις και μηνύματα, συνθήκες που ευνοούν τη μείωση της προσοχής και την εξοικείωση με αυτοματοποιημένες αντιδράσεις. Σε τέτοια περιβάλλοντα, οι επιθέσεις κοινωνικής μηχανικής μπορούν να ενσωματωθούν ομαλά στη “φυσιολογική” ροή περιεχομένου, καθιστώντας δυσκολότερη τη διάκριση μεταξύ νόμιμης και κακόβουλης επικοινωνίας.



Διάγραμμα 6: Χρήση Κοινωνικών Δικτύων (χρόνος ανά ημέρα)

Πηγή: google forms

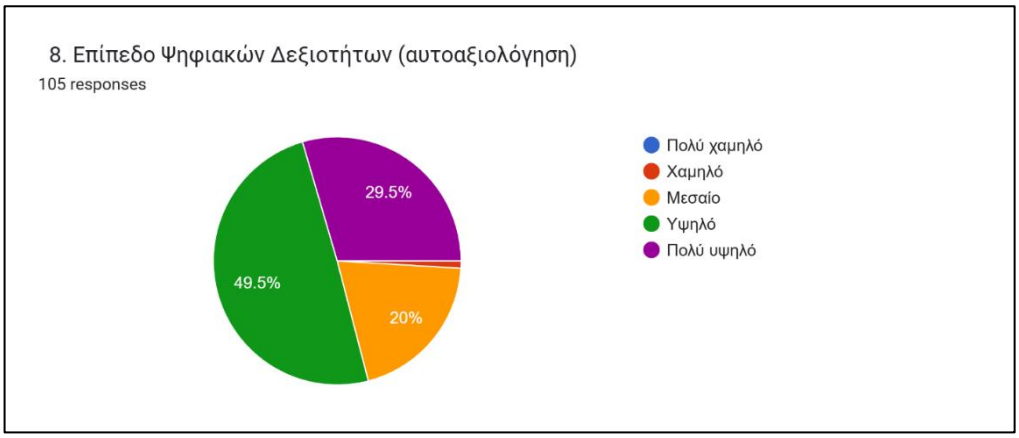
Η ανάλυση των πλατφορμών που χρησιμοποιούνται συχνότερα (Διάγραμμα 7) ενισχύει περαιτέρω αυτή την παρατήρηση. Η κυριαρχία πλατφορμών όπως το Instagram, το YouTube και το Facebook, οι οποίες βασίζονται σε συνεχή αλληλεπίδραση, οπτικό περιεχόμενο και κοινωνική επιβεβαίωση, δημιουργεί περιβάλλοντα αυξημένης εμπιστοσύνης και συναισθηματικής εμπλοκής. Σύμφωνα με τη διεθνή βιβλιογραφία, τέτοιου τύπου πλατφόρμες προσφέρονται ιδιαίτερα για τεχνικές κοινωνικής μηχανικής που αξιοποιούν τη μίμηση οικείων προτύπων επικοινωνίας (π.χ. μηνύματα από “γνωστούς”, ψευδή προφίλ, παραπλανητικά links), γεγονός που καθιστά τη χρήση τους κρίσιμο παράγοντα ερμηνείας της έκθεσης σε κινδύνους.



Διάγραμμα 7: Πλατφόρμες που χρησιμοποιείτε συχνότερα

Πηγή: google forms

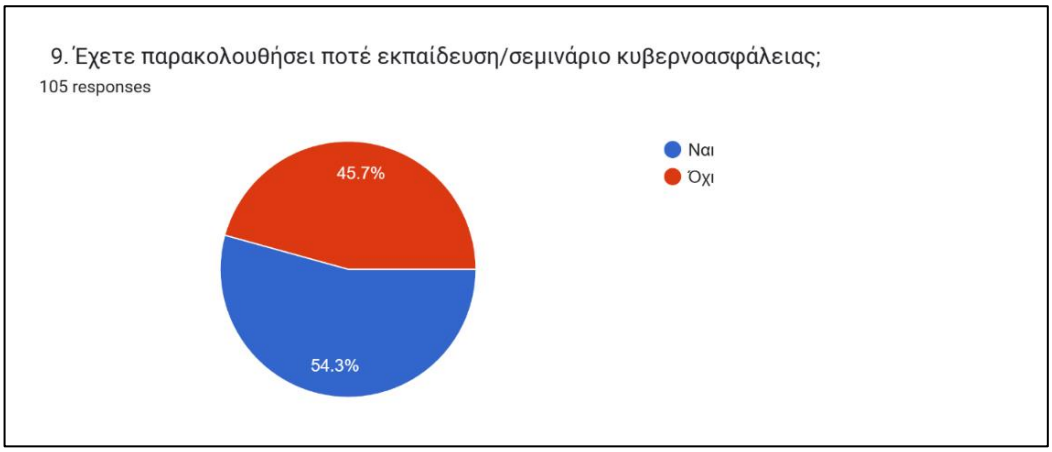
Σε επίπεδο αυτοαξιολόγησης ψηφιακών δεξιοτήτων (Διάγραμμα 8), η πλειονότητα των συμμετεχόντων τοποθετεί τον εαυτό της στις κατηγορίες «μεσαίο», «υψηλό» και «πολύ υψηλό». Το εύρημα αυτό είναι ερμηνευτικά σημαντικό, καθώς η υψηλή αυτοαντίληψη ικανότητας δεν συνεπάγεται απαραίτητα αντίστοιχο επίπεδο ασφαλούς συμπεριφοράς. Αντιθέτως, η βιβλιογραφία έχει δείξει ότι η υπερεκτίμηση των δεξιοτήτων μπορεί να οδηγήσει σε μειωμένη εγρήγορση, χαμηλότερη συμμόρφωση σε βασικές πρακτικές ασφάλειας και αυξημένη εμπιστοσύνη σε φαινομενικά “αθώες” ψηφιακές αλληλεπιδράσεις — παράγοντες που ενισχύουν τη γνωστική ευαλωτότητα.



Διάγραμμα 8: Επίπεδο Ψηφιακών Δεξιοτήτων (αυτοαξιολόγηση)

Πηγή: google forms

Όσον αφορά την εκπαίδευση σε θέματα κυβερνοασφάλειας (Διάγραμμα 9), τα αποτελέσματα καταδεικνύουν μια σχεδόν ισορροπημένη εικόνα, με λίγο πάνω από τους μισούς συμμετέχοντες να έχουν παρακολουθήσει κάποια μορφή σχετικής εκπαίδευσης και ένα ιδιαίτερα υψηλό ποσοστό να μην έχει λάβει καμία. Η ανομοιογενής αυτή κατανομή υποδηλώνει ότι η γνώση και η ευαισθητοποίηση γύρω από τις ψηφιακές απειλές δεν είναι καθολική, γεγονός που περιορίζει την ύπαρξη κοινών “γνωστικών φίλτρων” απέναντι σε επιθέσεις κοινωνικής μηχανικής και καθιστά το δείγμα κατάλληλο για τη μελέτη διαφοροποιήσεων στην αντίληψη κινδύνου.

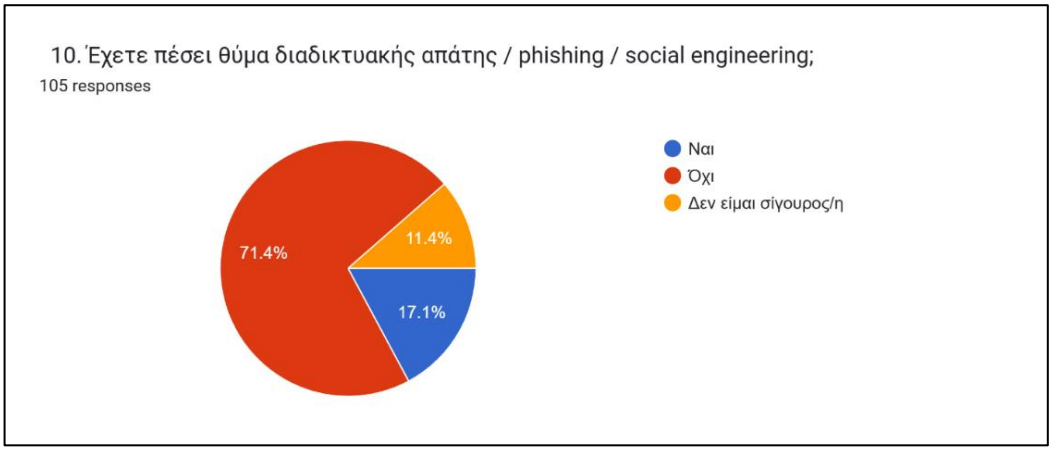


Διάγραμμα 9: Έχετε παρακολουθήσει ποτέ εκπαίδευση/σεμινάριο κυβερνοασφάλειας

Πηγή: google forms

Τέλος, αναφορικά με την εμπειρία των συμμετεχόντων ως προς το αν έχουν πέσει θύμα διαδικτυακής απάτης ή phishing (Διάγραμμα 10), το υψηλό ποσοστό αρνητικών απαντήσεων (71,4%) δεν μπορεί να ερμηνευθεί μονοδιάστατα ως απουσία περιστατικών. Η ύπαρξη σημαντικού ποσοστού αβεβαιότητας (11,4%)

είναι ιδιαίτερα ενδεικτική, καθώς υποδηλώνει ότι ένα μέρος των χρηστών δεν είναι βέβαιο αν έχει στοχοποιηθεί ή αν έχει ήδη εξαπατηθεί. Το εύρημα αυτό ευθυγραμμίζεται με τη βιβλιογραφία, η οποία επισημαίνει ότι πολλά περιστατικά κοινωνικής μηχανικής παραμένουν μη αναγνωρισμένα, ειδικά όταν δεν συνοδεύονται από άμεσες ή εμφανείς συνέπειες. Η αβεβαιότητα αυτή αναδεικνύει τη γνωστική διάσταση της ευαλωτότητας και υπογραμμίζει ότι ο κίνδυνος δεν περιορίζεται μόνο στα επιβεβαιωμένα περιστατικά, αλλά και στην αδυναμία έγκαιρης αναγνώρισής τους.



Διάγραμμα 10: Έχετε πέσει θύμα διαδικτυακής απάτης/phishing/social engineering

Πηγή: google forms

4.3 Αποτελέσματα επαγωγικών αναλύσεων

Οι επαγωγικές αναλύσεις της παρούσας ενότητας βασίστηκαν σε σύνθετες μεταβλητές που προέκυψαν από ομάδες ερωτήσεων του ερωτηματολογίου και όχι από μεμονωμένες ερωτήσεις.

Η επαγωγική στατιστική ανάλυση επικεντρώθηκε στη διερεύνηση των σχέσεων μεταξύ των ανεξάρτητων μεταβλητών και των δεικτών ευαλωτότητας και προληπτικής συμπεριφοράς, με στόχο όχι μόνο την καταγραφή στατιστικά σημαντικών συσχετίσεων, αλλά και την ερμηνεία τους υπό το πρίσμα των θεωρητικών προσεγγίσεων της κοινωνικής μηχανικής. Τα αποτελέσματα δείχνουν ότι ορισμένοι παράγοντες συνδέονται στατιστικά σημαντικά με αυξημένη έκθεση σε επιθέσεις κοινωνικής μηχανικής, επιβεβαιώνοντας σε μεγάλο βαθμό τις αρχικές ερευνητικές υποθέσεις.

Ειδικότερα, διαπιστώνεται ότι ο αυξημένος χρόνος χρήσης των κοινωνικών δικτύων συνδέεται με υψηλότερα επίπεδα έκθεσης σε ύποπτα μηνύματα και απόπειρες εξαπάτησης, στοιχείο που υποστηρίζει την υπόθεση ότι η εντατική παρουσία στα social media αυξάνει την πιθανότητα στοχοποίησης. Παράλληλα, οι ψηφιακές δεξιότητες όταν συνοδεύονται από προηγούμενη εκπαίδευση στην κυβερνοασφάλεια φαίνεται να λειτουργούν προστατευτικά: οι συμμετέχοντες που δηλώνουν υψηλότερη επάρκεια και έχουν εκπαιδευτεί εμφανίζουν ενισχυμένη προληπτική συμπεριφορά και μειωμένη τάση ανταπόκρισης σε ύποπτα αιτήματα.

Ιδιαίτερη σημασία παρουσιάζουν τα ευρήματα που αφορούν τους ψυχολογικούς και συναισθηματικούς παράγοντες. Τα αποτελέσματα καταδεικνύουν ότι τα μηνύματα που αξιοποιούν στοιχεία επείγοντος, αυθεντίας ή συναισθηματικής φόρτισης επηρεάζουν σημαντικά τη λήψη αποφάσεων των χρηστών, ακόμη και όταν αυτοί δηλώνουν αυξημένη επίγνωση των κινδύνων. Το εύρημα αυτό ενισχύει την υπόθεση ότι η γνώση από μόνη της δεν επαρκεί για την αποτροπή της εξαπάτησης, επιβεβαιώνοντας τα συμπεράσματα της σχετικής βιβλιογραφίας και αναδεικνύοντας τον καθοριστικό ρόλο των συναισθηματικών και γνωστικών μηχανισμών στη λήψη διαδικτυακών αποφάσεων.

Αναφορικά με τα δημογραφικά χαρακτηριστικά, οι στατιστικές αναλύσεις δεν ανέδειξαν ισχυρές και καθολικές διαφοροποιήσεις ως προς το φύλο, ωστόσο εντοπίζονται τάσεις διαφοροποίησης σε σχέση με την ηλικία και το επίπεδο εκπαίδευσης. Οι νεότεροι χρήστες και όσοι διαθέτουν χαμηλότερο επίπεδο εκπαίδευσης εμφανίζονται, σε ορισμένες περιπτώσεις, πιο επιρρεπείς σε πρακτικές κοινωνικής μηχανικής, στοιχείο που υποστηρίζει μερικώς τις αντίστοιχες ερευνητικές υποθέσεις.

4.4 Δευτερεύοντα και μη αναμενόμενα ευρήματα και συνολική απότιμηση

Πέραν των κύριων υποθέσεων, η ανάλυση ανέδειξε και ορισμένα δευτερεύοντα ευρήματα που δεν είχαν προβλεφθεί εξ’ αρχής. Ενδεικτικά, διαπιστώνεται ότι η αυξημένη εμπιστοσύνη στις ίδιες τις πλατφόρμες κοινωνικής δικτύωσης μπορεί να λειτουργεί ως παράγοντας χαλάρωσης της ατομικής επαγρύπνησης, οδηγώντας σε μειωμένη προληπτική συμπεριφορά. Το εύρημα αυτό υποδηλώνει ότι η αντίληψη περί “ασφάλειας εκ των άνω” ενδέχεται να μεταθέτει την ευθύνη από τον χρήστη προς την πλατφόρμα.

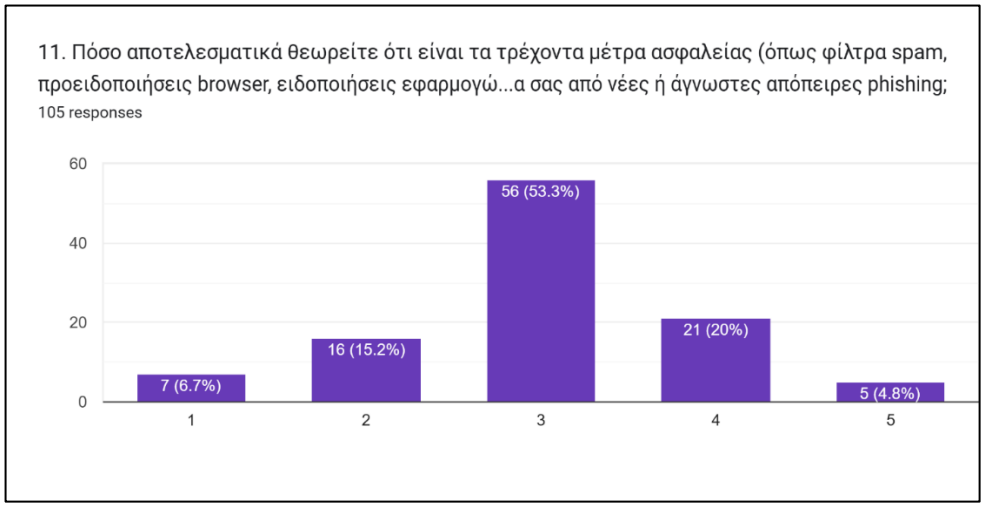
Επιπλέον, παρατηρείται ότι ορισμένοι χρήστες με σχετικά υψηλό επίπεδο ψηφιακών δεξιοτήτων εξακολουθούν να επηρεάζονται από στοχευμένες επιθέσεις που αξιοποιούν κοινωνική εγγύτητα ή επαγγελματική αξιοπιστία, γεγονός που αναδεικνύει τη σημασία της κοινωνικής διάστασης της εξαπάτησης.

Συνοψίζοντας, τα αποτελέσματα του παρόντος κεφαλαίου δείχνουν ότι οι περισσότερες από τις αρχικές ερευνητικές υποθέσεις υποστηρίζονται πλήρως ή μερικώς από τα εμπειρικά δεδομένα. Η υπόθεση που αφορά τη συσχέτιση εντατικής χρήσης των κοινωνικών δικτύων με αυξημένη έκθεση σε social engineering επιβεβαιώνεται, ενώ η υπόθεση σχετικά με τον προστατευτικό ρόλο των ψηφιακών δεξιοτήτων και της εκπαίδευσης στην κυβερνοασφάλεια υποστηρίζεται σε μεγάλο βαθμό. Αντιθέτως, οι υποθέσεις που αφορούν οριζόντιες διαφοροποιήσεις με βάση το φύλο δεν επιβεβαιώνονται πλήρως, γεγονός που υποδηλώνει ότι η ευαλωτότητα δεν καθορίζεται μονοδιάστατα από δημογραφικούς παράγοντες. Η ευαλωτότητα απέναντι στην κοινωνική μηχανική αναδεικνύεται ως αποτέλεσμα αλληλεπίδρασης τεχνικών, γνωστικών και συναισθηματικών παραγόντων, στοιχείο που δικαιολογεί την ανάγκη για πολυεπίπεδες στρατηγικές πρόληψης και εκπαίδευσης, οι οποίες θα συζητηθούν εκτενέστερα στο επόμενο κεφάλαιο.

4.5 Σχολιασμός αποτελεσμάτων ερωτήσεων 11–25

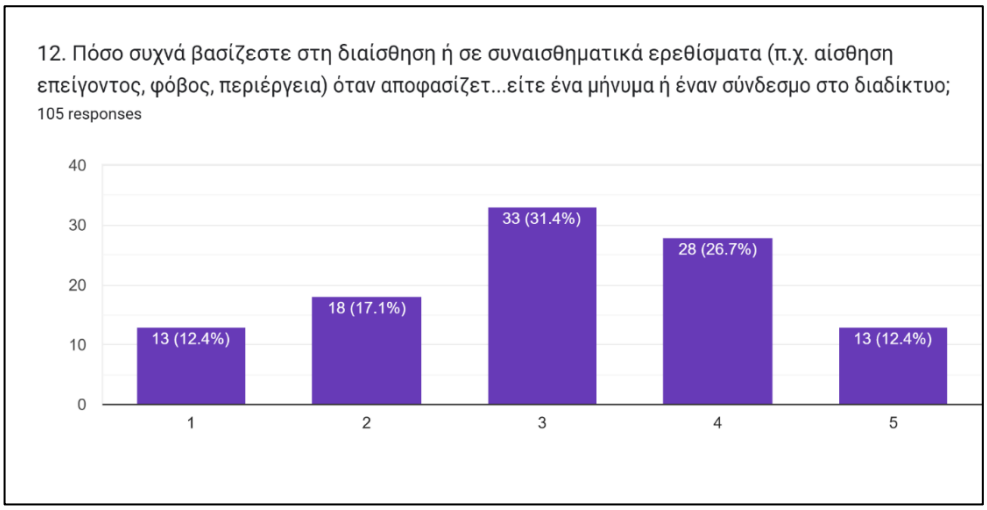
Οι ερωτήσεις 11 έως 25 του ερωτηματολογίου εστιάζουν σε κρίσιμες διαστάσεις της ευαλωτότητας των χρηστών απέναντι στο social engineering, καλύπτοντας στάσεις, αντιλήψεις, συναισθηματικές αντιδράσεις και πρακτικές συμπεριφορές ασφάλειας στα κοινωνικά δίκτυα. Ο συνολικός σχολιασμός των αποτελεσμάτων αυτών των ερωτήσεων αναδεικνύει ότι, παρά το γεγονός πως οι συμμετέχοντες εμφανίζονται σε γενικές γραμμές ενήμεροι για την ύπαρξη κινδύνων, η επίγνωση αυτή δεν μεταφράζεται πάντα σε συνεπή και αποτελεσματική προληπτική συμπεριφορά.

Σχετικά με τα τρέχοντα μέτρα ασφάλειας που αφορούν στην προστασία από νέες ή άγνωστες απόπειρες phishing (Διάγραμμα 11), οι περισσότεροι χρήστες (με ποσοστό 53.3%) θεωρούν ότι τα μέτρα αυτά λειτουργούν σε ικανοποιητικό αλλά όχι πλήρως αξιόπιστο επίπεδο, με ξεκάθαρη ανάγκη για περαιτέρω ενίσχυση και ενημέρωση.



Διάγραμμα 11: Πόσο αποτελεσματικά θεωρείτε ότι είναι τα τρέχοντα μέτρα ασφαλείας (όπως φίλτρα spam, προειδοποιήσεις browser, ειδοποιήσεις εφαρμογών κινητού) στην προστασία σας από νέες ή άγνωστες απόπειρες phishing;
Πηγή: google forms

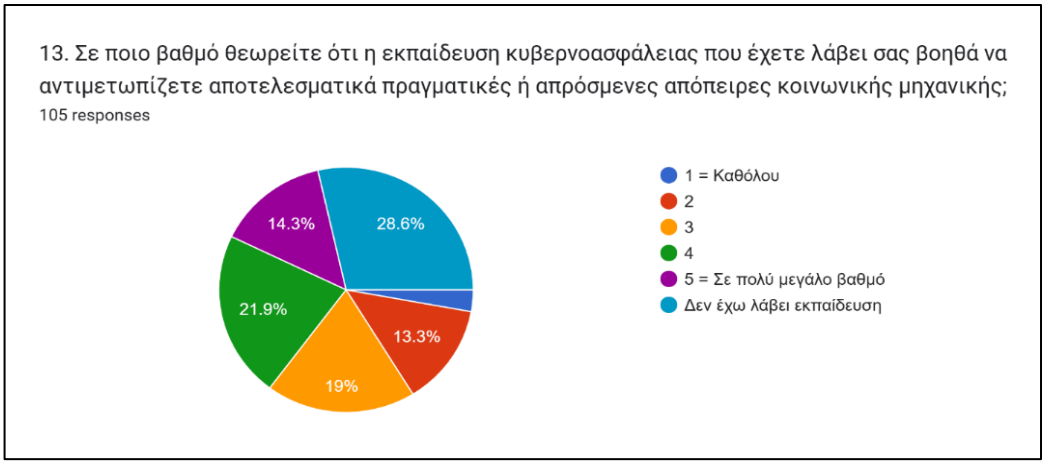
Τα ευρήματα που σχετίζονται με την διαίσθηση ή με συναισθηματικά ερεθίσματα για αποφάσεις εμπιστοσύνης κάποιου συνδέσμου στο διαδίκτυο (Διάγραμμα 12) δείχνουν ότι ένα μεγάλο ποσοστό (58.1%, στα επίπεδα 3 και 4) είναι ευάλωτοι σε χειρισμό μέσω συναισθηματικών triggers, τακτική που είναι κοινή στα phishing μηνύματα. Τα άτομα που απάντησαν 5 (12.4%) αποτελούν μια ιδιαίτερα ευάλωτη ομάδα, καθώς παραδέχονται συχνή ή πολύ συχνή επιρροή από συναισθήματα, ενώ το υπόλοιπο ποσοστό (29.5% συνολικά) έχει πιο ορθολογική και ψύχραιμη προσέγγιση.



Διάγραμμα 12: Πόσο συχνά βασίζεστε στη διαίσθηση ή σε συναισθηματικά ερεθίσματα (π.χ. αίσθηση επείγοντος, φόβος, περιέργεια) όταν αποφασίζετε αν θα εμπιστευτείτε ένα μήνυμα ή έναν σύνδεσμο στο διαδίκτυο;

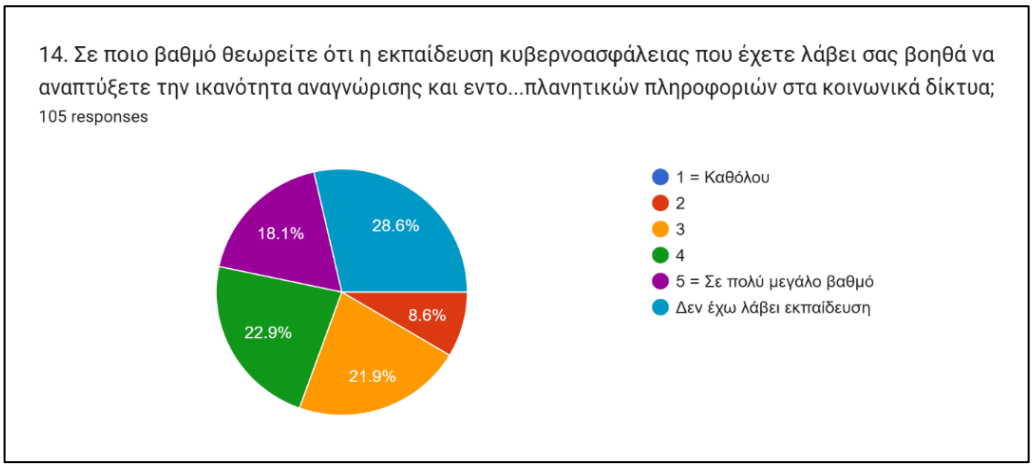
Πηγή: google forms

Ως προς την εκπαίδευση κυβερνοασφάλειας, δεν αξιολογείται ιδιαίτερα υψηλά γενικά (Διάγραμμα 13) αλλά παρουσιάζει ελαφρώς καλύτερη αποτελεσματικότητα όταν αφορά πιο συγκεκριμένες δεξιότητες, όπως η αναγνώριση παραπλανητικού περιεχομένου στα κοινωνικά δίκτυα (Διάγραμμα 14). Παράλληλα, το υψηλό και ίδιο ποσοστό απουσίας εκπαίδευσης (28.6%) και στα δύο διαγράμματα, αποτελεί το μεγαλύτερο εμπόδιο στη συνολική ικανότητα των χρηστών να αναγνωρίζουν και να αντιμετωπίζουν κυβερνοαπειλες.



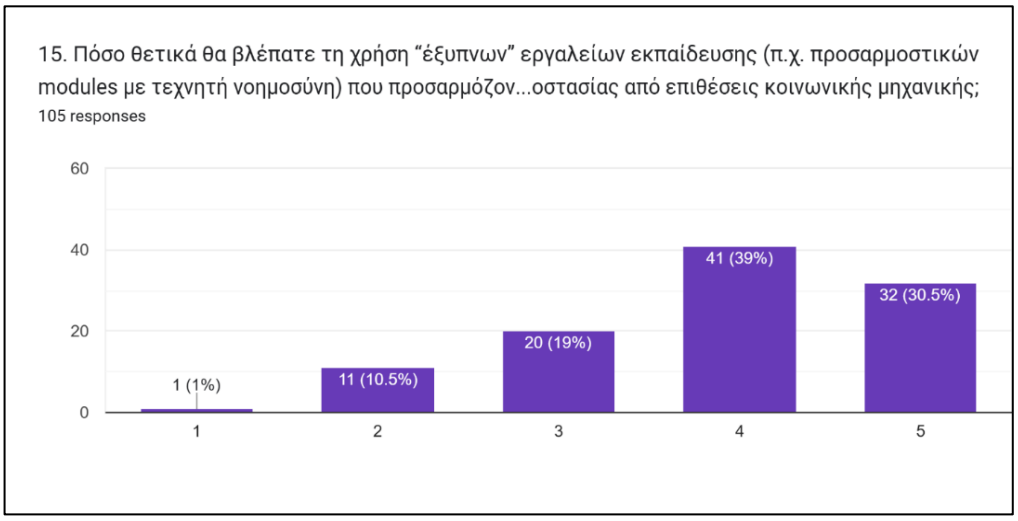
Διάγραμμα 13: Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αντιμετωπίζετε αποτελεσματικά πραγματικές ή απρόσμενες απόπειρες κοινωνικής μηχανικής;

Πηγή: google forms



Διάγραμμα 14: Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αναπτύξετε την ικανότητα αναγνώρισης και εντοπισμού ψευδών ή παραπλανητικών πληροφοριών στα κοινωνικά δίκτυα;
Πηγή: google forms

Επιπλέον οι χρήστες δείχνουν πολύ υψηλή αποδοχή της ιδέας για “έξυπνα”, εξατομικευμένα εργαλεία εκπαίδευσης, θεωρώντας ότι μπορούν να ενισχύσουν σημαντικά την προστασία τους από επιθέσεις κοινωνικής μηχανικής (Διάγραμμα 15).



Διάγραμμα 15: Πόσο θετικά θα βλέπατε τη χρήση “έξυπνων” εργαλείων εκπαίδευσης (π.χ. προσαρμοστικών modules με τεχνητή νοημοσύνη) που προσαρμόζονται στο προφίλ και τις ανάγκες σας για την ενίσχυση της προστασίας από επιθέσεις κοινωνικής μηχανικής;
Πηγή: google forms

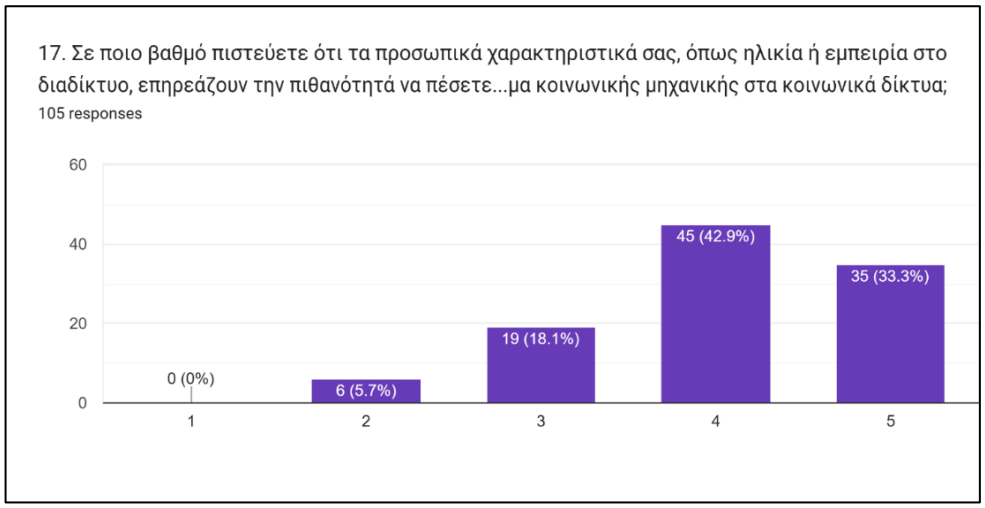
Σε ότι αφορά τον έλεγχο της αξιοπιστίας ενός συνδέσμου από τους χρήστες πριν να κάνουν κλικ (Διάγραμμα 16), τα αποτελέσματα δείχνουν ότι οι περισσότεροι χρήστες, 69 συνολικά στα επίπεδα 4 και 5, έχουν υψηλό επίπεδο επίγνωσης

κινδύνου και υιοθετούν ασφαλείς πρακτικές πριν αλληλεπιδράσουν με περιεχόμενο στα κοινωνικά δίκτυα.

Διάγραμμα 16: Πόσο συχνά ελέγχετε αν ένας σύνδεσμος ή μια προσφορά που εμφανίζεται στο κοινωνικό δίκτυο που χρησιμοποιείτε προέρχεται από αξιόπιστη πηγή πριν κάνετε κλικ; Πηγή: google forms

Με βάση τα ευρήματα των ερωτήσεων 11-16, προκύπτει μια πιο σύνθετη εικόνα σχετικά με το πώς οι χρήστες αξιολογούν τα σενάρια εξαπάτησης. Αρχικά, τα δεδομένα που αφορούν την αναγνώριση ύποπτων μηνυμάτων και πρακτικών phishing δείχνουν ότι οι περισσότεροι χρήστες δηλώνουν πως μπορούν να εντοπίσουν προφανείς ενδείξεις εξαπάτησης. Ωστόσο, η εικόνα αυτή διαφοροποιείται όταν τα σενάρια γίνονται πιο πολύπλοκα και αξιοποιούν στοιχεία κοινωνικής εγγύτητας, επαγγελματικής ιδιότητας ή συναισθηματικής πίεσης. Το εύρημα αυτό υποδηλώνει ότι οι χρήστες βασίζονται συχνά σε επιφανειακά κριτήρια αξιολόγησης, γεγονός που αυξάνει την ευαλωτότητα τους σε στοχευμένες επιθέσεις κοινωνικής μηχανικής.

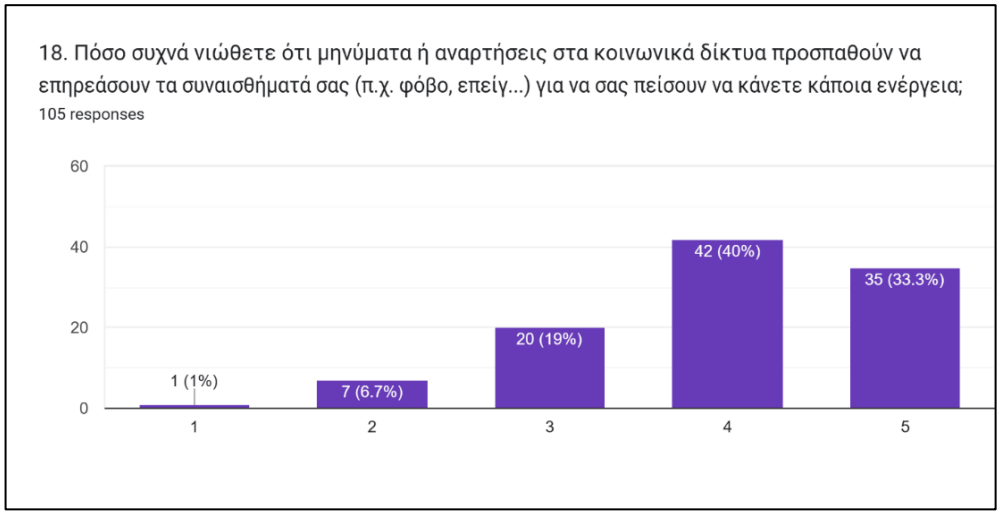
Το διάγραμμα 17 δείχνει ότι υπάρχει πολύ μεγάλη αναγνώριση του ρόλου των προσωπικών χαρακτηριστικών (επίπεδα 4 και 5), γεγονός που δείχνει ότι αυτή η μεγάλη πλειοψηφία (76.2%) έχει καλή αυτογνωσία και αντιλαμβάνεται ότι η ευαλωτότητα δεν εξαρτάται μόνο από τα τεχνικά μέτρα ασφαλείας αλλά και από ποιος είσαι ως χρήστης.



Διάγραμμα 17: Σε ποιο βαθμό πιστεύετε ότι τα προσωπικά χαρακτηριστικά σας, όπως ηλικία ή εμπειρία στο διαδίκτυο, επηρεάζουν την πιθανότητά να πέσετε θύμα κοινωνικής μηχανικής στα κοινωνικά δίκτυα;

Πηγή: google forms

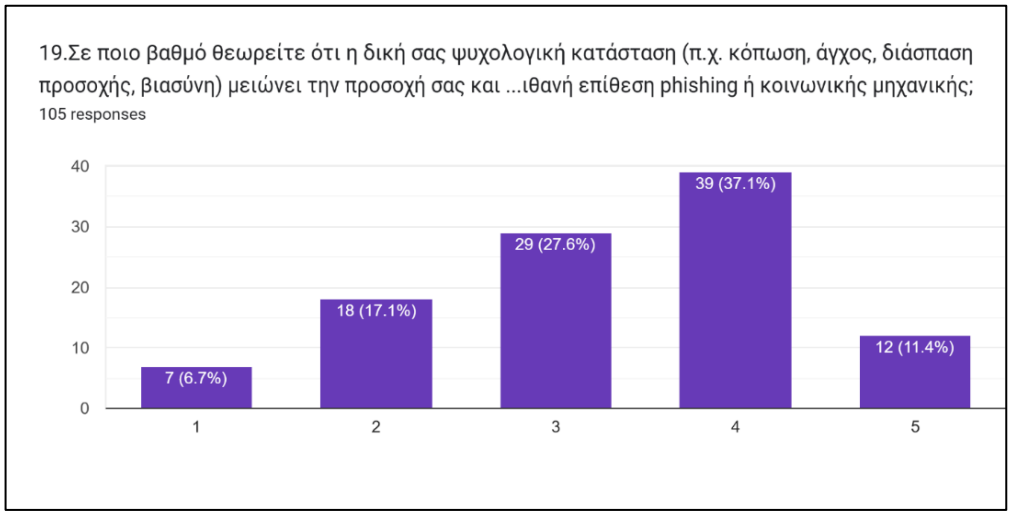
Οι χρήστες σε πολύ μεγάλο ποσοστό αντιλαμβάνονται ότι τα κοινωνικά δίκτυα χρησιμοποιούν συναισθηματικά ερεθίσματα για να επηρεάσουν τη συμπεριφορά τους. Αυτό φαίνεται από το Διάγραμμα 18, όπου η συντριπτική πλειοψηφία, 77 άτομα συνολικά στα επίπεδα 4 και 5, αντιλαμβάνεται συχνά συναισθηματική χειραγώγηση. Αυτό δείχνει υψηλή ωριμότητα απέναντι στις τεχνικές κοινωνικής μηχανικής, ενισχυμένη ικανότητας αναγνώρισης χειριστικών μοτίβων και καλλιεργημένη κριτική σκέψη.



Διάγραμμα 18: Πόσο συχνά νιώθετε ότι μηνύματα ή αναρτήσεις στα κοινωνικά δίκτυα προσπαθούν να επηρεάσουν τα συναισθήματά σας (π.χ. φόβο, επείγον, συμπόνια) για να σας πείσουν να κάνετε κάποια ενέργεια;

Πηγή: google forms

Η αναγνώριση της εξωτερικής χειραγώγησης συνδέεται άμεσα και με την κατανόηση ότι και η εσωτερική ψυχολογική κατάσταση, όπως κόπωση, άγχος, διάσπαση προσοχής και βιασύνη, επηρεάζει την ευαλωτότητα, όπως καταγράφεται στην επόμενη ερώτηση (Διάγραμμα 19).

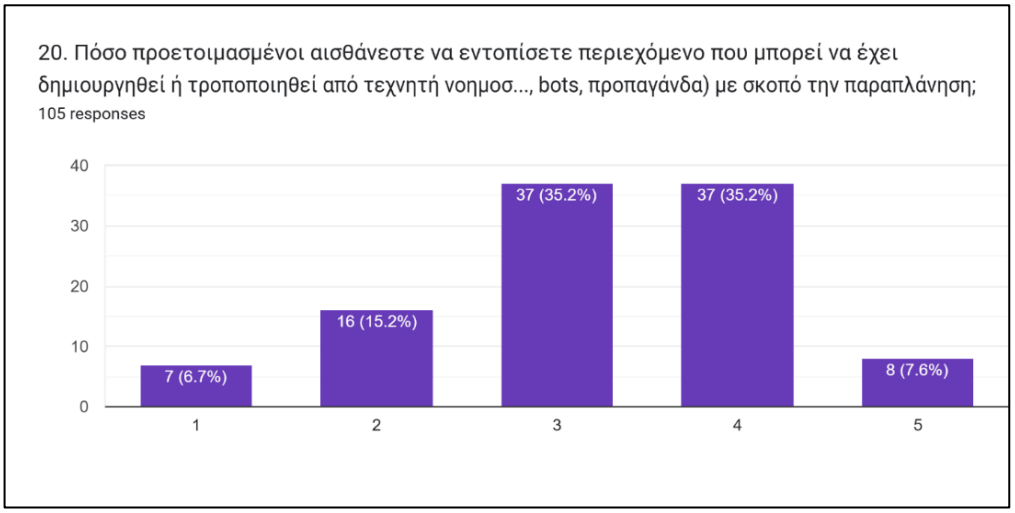


Διάγραμμα 19: Σε ποιο βαθμό θεωρείτε ότι η δική σας ψυχολογική κατάσταση (π.χ. κόπωση, άγχος, διάσπαση προσοχής, βιασύνη) μειώνει την προσοχή σας και αυξάνει την πιθανότητα να παραβλέψετε σημάδια κινδύνου σε μια πιθανή επίθεση phishing ή κοινωνικής μηχανικής;
Πηγή: google forms

Από τη συνολική αποτίμηση των απαντήσεων των ερωτήσεων 17-19, προκύπτει ότι τα συναισθήματα αποτελούν καθοριστικό παράγοντα στη λήψη αποφάσεων. Ακόμη και χρήστες που δηλώνουν αυξημένο επίπεδο ψηφιακών δεξιοτήτων φαίνεται να επηρεάζονται από μηνύματα που προκαλούν άγχος, φόβο απώλειας ή αίσθηση υποχρέωσης για άμεση ανταπόκριση. Το εύρημα αυτό ενισχύει τη θέση ότι το social engineering αξιοποιεί πρωτίστως ψυχολογικούς μηχανισμούς και όχι τεχνικά κενά.

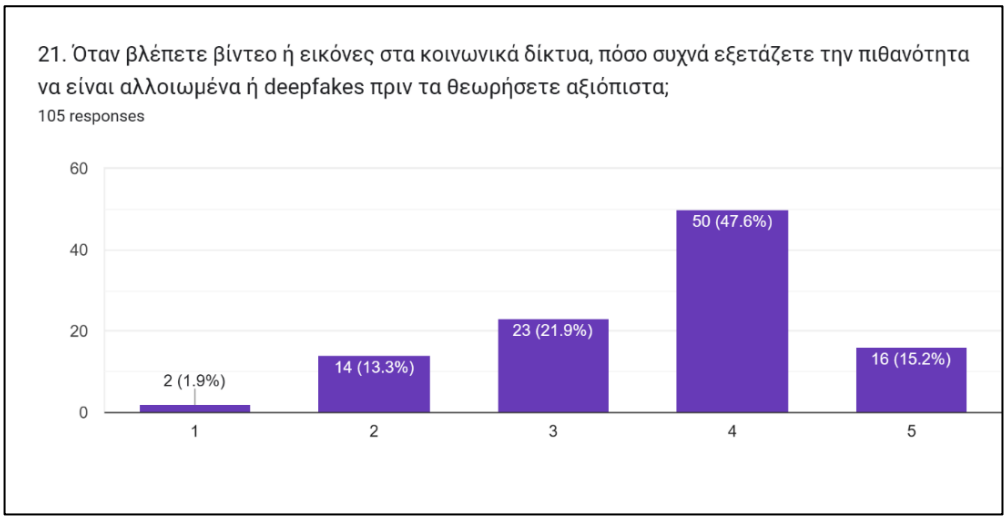
Τα αποτελέσματα που αφορούν τον βαθμό στον οποίο οι χρήστες αισθάνονται προετοιμασμένοι να εντοπίζουν παραπλανητικό περιεχόμενο που έχει δημιουργηθεί ή τροποποιηθεί από τεχνητή νοημοσύνη, bots ή προπαγάνδα (Διάγραμμα 20), καταδεικνύουν ότι η πλειονότητα των συμμετεχόντων αισθάνονται μέτρια έως αρκετά προετοιμασμένοι (35.2% και 35.2% αντίστοιχα), χωρίς ωστόσο να εμφανίζει υψηλό βαθμό ετοιμότητας. Μόνο ένα μικρό ποσοστό των χρηστών (7.6%) δηλώνει ότι αισθάνεται πολύ προετοιμασμένο, ενώ ένα αξιοσημείωτο τμήμα του δείγματος (21,9%), το οποίο εντάσσεται στα χαμηλότερα επίπεδα

προετοιμασίας (επίπεδα 1 και 2), εμφανίζεται ιδιαίτερα ευάλωτο σε σύγχρονες μορφές παραπλάνησης που βασίζονται σε τεχνολογίες τεχνητής νοημοσύνης.

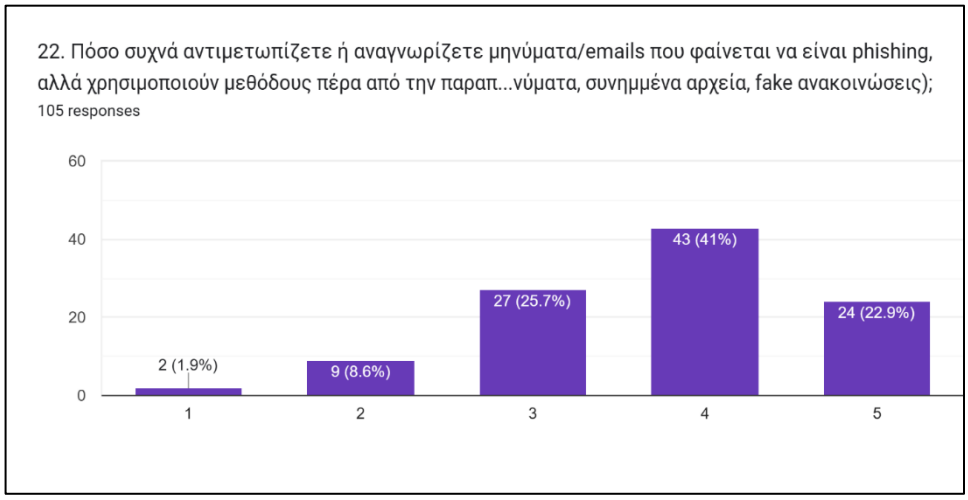


Διάγραμμα 20: Πόσο προετοιμασμένοι αισθάνεστε να εντοπίσετε περιεχόμενο που μπορεί να έχει δημιουργηθεί ή τροποποιηθεί από τεχνητή νοημοσύνη
(π.χ. AI-generated posts, bots, προπαγάνδα) με σκοπό την παραπλάνηση
Πηγή: google forms

Οι χρήστες εμφανίζονται ιδιαίτερα προσεκτικοί απέναντι σε παραπλανητικό περιεχόμενο, είτε αυτό αφορά αλλοιωμένα βίντεο και εικόνες (deepfakes) είτε πιο εξελιγμένες μορφές phishing μηνυμάτων. Όπως προκύπτει από τα Διαγράμματα 21 και 22, η πλειοψηφία κινείται στα υψηλά επίπεδα εγρήγορσης, με πάνω από 60% να δηλώνουν ότι εξετάζουν συστηματικά την αξιοπιστία του περιεχομένου πριν το εμπιστευτούν. Αυτό δείχνει ότι έχουν αναπτύξει έναν σταθερό μηχανισμό εντοπισμού παραπλάνησης, ανεξάρτητα από το αν αυτή εμφανίζεται οπτικά ή μέσω μηνυμάτων. Η ομοιότητα των αποτελεσμάτων επιβεβαιώνει πως η γενική επίγνωση κινδύνων είναι υψηλή και διατηρείται σταθερή σε διαφορετικά είδη ψηφιακής απειλής.

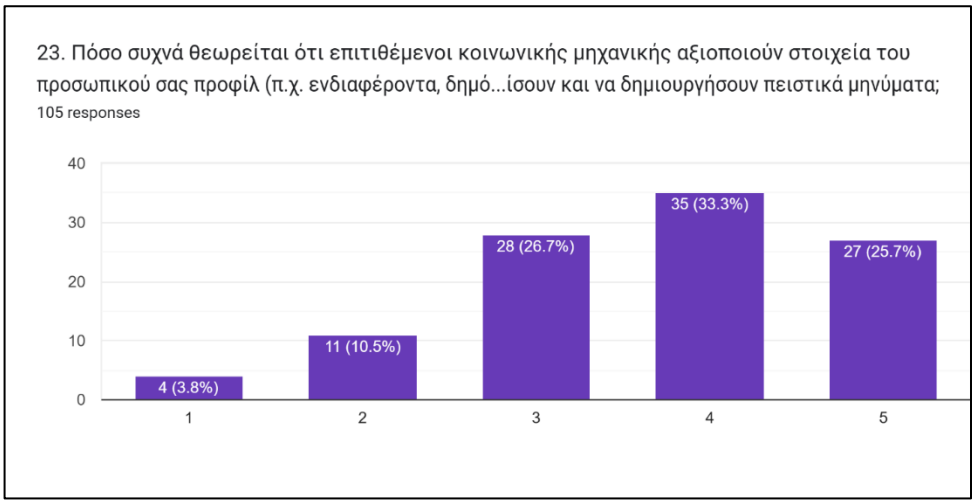


Διάγραμμα 21: Όταν βλέπετε βίντεο ή εικόνες στα κοινωνικά δίκτυα, πόσο συχνά εξετάζετε την πιθανότητα να είναι αλλοιωμένα ή deepfakes πριν τα θεωρήσετε αξιόπιστα;
Πηγή: google forms



Διάγραμμα 22: Πόσο συχνά αντιμετωπίζετε ή αναγνωρίζετε μηνύματα/emails που φαίνεται να είναι phishing, αλλά χρησιμοποιούν μεθόδους πέρα από την παραπλάνηση μέσω ψευτικων URL (π.χ. παραπλανητικά μηνύματα, συνημμένα αρχεία, fake ανακοινώσεις);
Πηγή: google forms

Συμπληρωματικά προς τα παραπάνω, τα αποτελέσματα του Διαγράμματος 23 δείχνουν μια ξεκάθαρη αναγνώριση κινδύνου, αφού οι περισσότεροι χρήστες αντιλαμβάνονται ότι οι επιτιθέμενοι κοινωνικής μηχανικής εκμεταλλεύονται ενεργά πληροφορίες από τα προσωπικά προφίλ τους για να διαμορφώσουν μηνύματα που φαίνονται πιο πραγματικά και προσαρμοσμένα.



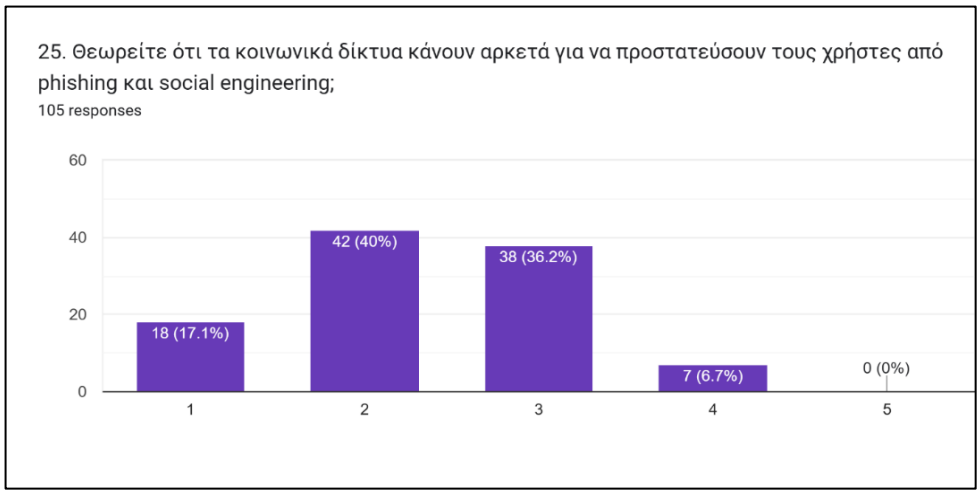
Διάγραμμα 23: Πόσο συχνά θεωρείται ότι επιτιθέμενοι κοινωνικής μηχανικής αξιοποιούν στοιχεία του προσωπικού σας προφίλ (π.χ. ενδιαφέροντα, δημόσιες αναρτήσεις, λίστα φίλων) στα κοινωνικά δίκτυα, για να σας προσεγγίσουν και να δημιουργήσουν πειστικά μηνύματα;
Πηγή: google forms

Σε συνέχεια των προηγούμενων ευρημάτων, τα δεδομένα δείχνουν ότι οι χρήστες δεν ελέγχουν συστηματικά τις ρυθμίσεις απορρήτου στα κοινωνικά δίκτυα (Διάγραμμα 24). Το μεγαλύτερο ποσοστό, 38.1%, βρίσκεται στο επίπεδο 3, δηλώνοντας ότι ελέγχει τις ρυθμίσεις μόνο περιστασιακά, ενώ ένα επιπλέον 29.5% τις ελέγχει σπάνια (επίπεδο 2). Η εικόνα αυτή δείχνει μια ασυνέπεια μεταξύ της αντίληψης κινδύνου και της πραγματικής προληπτικής συμπεριφοράς, επιβεβαιώνοντας ότι η συνειδητοποίηση δεν μεταφράζεται πάντα σε πρακτική δράση.

Διάγραμμα 24: Πόσο συχνά ελέγχετε τις ρυθμίσεις απορρήτου (π.χ.ποιος βλέπει το προφιλ σας, δημοσιεύσεις και φωτογραφίες σας) στα κοινωνικά σας δίκτυα;
Πηγή: google forms

Συνοψίζοντας τα παραπάνω ευρήματα των ερωτήσεων 20-24, προκύπτει ότι παρότι οι συμμετέχοντες αναγνωρίζουν τη σημασία μέτρων όπως ο έλεγχος αποστολέα, η αποφυγή κλικ σε ύποπτους συνδέσμους και η προστασία προσωπικών δεδομένων, δεν εφαρμόζουν πάντα συστηματικά τις πρακτικές αυτές στην καθημερινή χρήση των κοινωνικών δικτύων. Αυτό υποδηλώνει χάσμα μεταξύ πρόθεσης και συμπεριφοράς, το οποίο μπορεί να οφείλεται τόσο σε υπερεκτίμηση ικανοτήτων όσο και σε περιορισμένη επίγνωση των εξελιγμένων τεχνικών εξαπάτησης.

Τέλος, σχετικά με το κατά πόσο τα κοινωνικά δίκτυα θεωρείται ότι προστατεύουν επαρκώς τους χρήστες από phishing και social engineering (Διάγραμμα 25), τα δεδομένα δείχνουν μια ξεκάθαρα χαμηλή εμπιστοσύνη. Το 40% τοποθετείται στο επίπεδο 2 και άλλο ένα 36.2% στο επίπεδο 3, δείχνοντας ότι οι περισσότεροι χρήστες αξιολογούν τα μέτρα προστασίας μέτρια έως ανεπαρκή. Μόνο το 6.7% εκφράζει πιο θετική άποψη, ενώ το 17.1% πιστεύει ότι οι πλατφόρμες κάνουν ελάχιστα. Η συνολική εικόνα καταλήγει στο συμπέρασμα ότι οι χρήστες νιώθουν πως τα κοινωνικά δίκτυα δεν παρέχουν ικανοποιητική θωράκιση απέναντι σε σύγχρονες απειλές και χρειάζονται σημαντικές βελτιώσεις.



Διάγραμμα 25: Θεωρείτε ότι τα κοινωνικά δίκτυα κάνουν αρκετά για να προστατεύσουν τους χρήστες από phishing και social engineering;
Πηγή: google forms

Συνολικά, τα ευρήματα επιβεβαιώνουν τις περισσότερες ερευνητικές υποθέσεις: η εντατική χρήση των social media αυξάνει την ευαλωτότητα, οι ψηφιακές δεξιότητες λειτουργούν προστατευτικά, και η ψυχολογική επίδραση αποτελεί κρίσιμο παράγοντα στη λήψη αποφάσεων. Η ευαλωτότητα δεν εξαρτάται μονοδιάστατα από

δημογραφικούς παράγοντες, αλλά αποτελεί αποτέλεσμα αλληλεπίδρασης τεχνικών, γνωστικών και συναισθηματικών παραμέτρων.

4.6 Συνολική ανακεφαλαίωση ευρημάτων

Η ανάλυση των περιγραφικών και επαγωγικών ευρημάτων της έρευνας αναδεικνύει μια πολυδιάστατη εικόνα σχετικά με την ευαλωτότητα των χρηστών των κοινωνικών δικτύων απέναντι στο social engineering. Τα αποτελέσματα δείχνουν ότι η έκθεση σε τεχνικές εξαπάτησης δεν προκύπτει από έναν μεμονωμένο παράγοντα, αλλά από την αλληλεπίδραση δημογραφικών, συμπεριφορικών, γνωστικών και ψυχολογικών μεταβλητών.

Πρώτον, η εντατική χρήση των κοινωνικών δικτύων επιβεβαιώνεται ως παράγοντας που αυξάνει την πιθανότητα στοχοποίησης. Οι χρήστες που αφιερώνουν περισσότερο χρόνο στις πλατφόρμες εκτίθενται συχνότερα σε ύποπτα μηνύματα, γεγονός που ευθυγραμμίζεται με τη διεθνή βιβλιογραφία που συνδέει τη συχνότητα ψηφιακής αλληλεπίδρασης με αυξημένο κίνδυνο (Parsons et al., 2019; Albladi & Weir, 2018).

Δεύτερον, οι ψηφιακές δεξιότητες και η προηγούμενη εκπαίδευση στην κυβερνοασφάλεια λειτουργούν προστατευτικά, συμβάλλοντας σε μεγαλύτερη προληπτική εγρήγορση και μειωμένη πιθανότητα ανταπόκρισης σε ύποπτες ενέργειες. Ωστόσο, το εύρημα αυτό συνοδεύεται από μία σημαντική αντιφατική διάσταση: ορισμένοι χρήστες με υψηλή αυτοαξιολόγηση δεξιοτήτων εξακολουθούν να επηρεάζονται από μηνύματα που αξιοποιούν ψυχολογικές τεχνικές, όπως το αίσθημα επείγοντος ή αυθεντίας. Το στοιχείο αυτό υπογραμμίζει ότι η ψηφιακή ικανότητα από μόνη της δεν επαρκεί για την αποτροπή της εξαπάτησης, εφόσον οι επιθέσεις στοχεύουν πρωτίστως τη συναισθηματική και γνωστική λειτουργία του ατόμου.

Τρίτον, αν και οι δημογραφικές μεταβλητές δεν παρουσιάζουν έντονες διαφοροποιήσεις στο σύνολο, εντοπίζονται ενδείξεις ότι ηλικιακοί και εκπαιδευτικοί παράγοντες μπορεί να επηρεάσουν τον τρόπο ανταπόκρισης σε τεχνικές social engineering. Αυτό υποδεικνύει την ανάγκη για πιο στοχευμένες παρεμβάσεις σε συγκεκριμένες ομάδες χρηστών.

Τέλος, ένα από τα πιο ενδιαφέροντα δευτερεύοντα ευρήματα αφορά την υπερβολική εμπιστοσύνη στις ίδιες τις πλατφόρμες κοινωνικής δικτύωσης. Οι χρήστες που θεωρούν ότι οι πλατφόρμες παρέχουν υψηλό επίπεδο προστασίας εμφανίζουν χαμηλότερη προσωπική επαγρύπνηση, γεγονός που αυξάνει την πιθανότητα λάθους. Αυτό καταδεικνύει ότι η αίσθηση «ασφάλειας από τρίτους» μπορεί να λειτουργήσει αντιστρόφως ανάλογα με την προληπτική συμπεριφορά.

Τα παραπάνω αποτελέσματα συνοψίζονται συγκριτικά στον ακόλουθο πίνακα, όπου αποτυπώνεται η αντιστοίχιση των βασικών βιβλιογραφικών θέσεων με τα εμπειρικά ευρήματα της παρούσας έρευνας.

Πίνακας 2: Αντιστοίχιση ευρημάτων από βιβλιογραφική ανασκόπηση και εμπειρικών ευρημάτων

Ευρήματα από την βιβλιογραφική ανασκόπηση	**Επαληθεύτηκε**	**Ποια συμπληρωματικά ευρήματα προκύπτουν**
Η εντατική χρήση κοινωνικών δικτύων αυξάνει την έκθεση σε επιθέσεις social engineering- Boyd & Ellison (2007); Albladi & Weir (2018); ENISA (2022)	Ναι	Η αυξημένη έκθεση δεν οδηγεί πάντα σε εξαπάτηση, αλλά αυξάνει την πιθανότητα λήψης ύποπτων μηνυμάτων
Οι ψηφιακές δεξιότητες και η εκπαίδευση στην κυβερνοασφάλεια λειτουργούν προστατευτικά- Parsons et al. (2019); ENISA (2023); NIST (2020)	Ναι (μερικώς)	Η τεχνική γνώση δεν αρκεί όταν τα μηνύματα αξιοποιούν ψυχολογικές τεχνικές (επείγον, αυθεντία, συναισθηματική πίεση)
Η ευαλωτότητα στο social engineering είναι πολυπαραγοντική (συνδυασμός τεχνικών, ψυχολογικών και κοινωνικών παραμέτρων) - Workman (2008); Hadnagy (2018); Schneier (2015)	Ναι	Αναδεικνύεται η ανάγκη για πολυεπίπεδες στρατηγικές πρόληψης που υπερβαίνουν την

		αποκλειστικά τεχνική εκπαίδευση
Οι δημογραφικοί παράγοντες (π.χ. φύλο) καθορίζουν σε μεγάλο βαθμό την ευαλωτότητα - Williams et al.(2017); Parsons et al.(2019)	Όχι	Η ευαλωτότητα προκύπτει από συνδυασμό συμπεριφορικών, γνωστικών και συναισθηματικών παραγόντων
Οι χρήστες που γνωρίζουν τους κινδύνους υιοθετούν συστηματικά ασφαλείς πρακτικές - Ferreira et al.(2015); Jansen & van Schaik (2022); Williams et al.(2017)	Όχι	Παρατηρείται χάσμα μεταξύ αντίληψης κινδύνου και πραγματικής συμπεριφοράς

Η συνολική αξιολόγηση των αποτελεσμάτων ολοκληρώνεται στο επόμενο κεφάλαιο, όπου διατυπώνονται τα τελικά συμπεράσματα, αναδεικνύεται η συμβολή της παρούσας έρευνας και προτείνονται κατευθύνσεις για μελλοντικές επιστημονικές αναζητήσεις.

5. Συμπεράσματα

Το παρόν κεφάλαιο αποτελεί το τελικό μέρος της μελέτης και στοχεύει στη συνολική αξιολόγηση των ευρημάτων, στη συσχέτισή τους με το θεωρητικό πλαίσιο της βιβλιογραφίας, καθώς και στον εντοπισμό περιορισμών, ερευνητικών κενών και δυνατοτήτων για μελλοντική έρευνα και πρακτική αξιοποίηση. Παράλληλα, εξετάζονται οι αρχικοί στόχοι της μελέτης και αξιολογείται ο βαθμός στον οποίο επιτεύχθηκαν.

5.1 Σύνοψη της μελέτης και βασικά συμπεράσματα

Η παρούσα εργασία επικεντρώθηκε στη διερεύνηση της αξιοποίησης των κοινωνικών δικτύων στο social engineering, με έμφαση στις ψυχολογικές τεχνικές που χρησιμοποιούνται, στους παράγοντες ευαλωτότητας των χρηστών και στις δυνατότητες πρόληψης και αντιμετώπισης του φαινομένου. Μέσα από τη συνδυαστική ανάλυση της διεθνούς βιβλιογραφίας και των εμπειρικών δεδομένων που προέκυψαν από το ερωτηματολόγιο, αναδείχθηκε ο πολυπαραγοντικός και δυναμικός χαρακτήρας της ευαλωτότητας απέναντι στις επιθέσεις κοινωνικής μηχανικής.

Ένα από τα κεντρικά συμπεράσματα της μελέτης είναι ότι η εντατική χρήση των κοινωνικών δικτύων αυξάνει την πιθανότητα έκθεσης σε ύποπτα ή κακόβουλα μηνύματα. Το εύρημα αυτό επιβεβαιώνει τις θέσεις της διεθνούς βιβλιογραφίας, σύμφωνα με τις οποίες η αυξημένη ψηφιακή αλληλεπίδραση και η συνεχής παρουσία στα κοινωνικά δίκτυα δημιουργούν περισσότερα σημεία επαφής με επιτιθέμενους (Parsons et al., 2019; Albladi & Weir, 2018).

Παράλληλα, διαπιστώθηκε ότι οι ψηφιακές δεξιότητες και η προηγούμενη εκπαίδευση στην κυβερνοασφάλεια λειτουργούν σε σημαντικό βαθμό προστατευτικά. Ωστόσο, τα αποτελέσματα ανέδειξαν και μία κρίσιμη αντιφατική διάσταση: ακόμη και χρήστες με υψηλή αυτοαξιολόγηση δεξιοτήτων παραμένουν ευάλωτοι σε επιθέσεις που αξιοποιούν έντονες ψυχολογικές τεχνικές, όπως το αίσθημα επείγοντος, η αυθεντία και η κοινωνική εγγύτητα. Το στοιχείο αυτό υπογραμμίζει ότι το social engineering στοχεύει πρωτίστως στη συναισθηματική και γνωστική λειτουργία του ατόμου και όχι αποκλειστικά στην τεχνική του επάρκεια, επιβεβαιώνοντας τις θεωρητικές προσεγγίσεις των Cialdini (2009) και Schneier (2015).

Επιπλέον, αν και οι δημογραφικές μεταβλητές δεν παρουσίασαν έντονες διαφοροποιήσεις στο σύνολο των αποτελεσμάτων, εντοπίστηκαν ενδείξεις ότι η ηλικία και το εκπαιδευτικό επίπεδο ενδέχεται να επηρεάζουν τον τρόπο αντίληψης και ανταπόκρισης στις τεχνικές κοινωνικής μηχανικής. Το εύρημα αυτό συνάδει με προηγούμενες μελέτες που υποστηρίζουν ότι η εμπειρία, η εξοικείωση με την τεχνολογία και το γνωστικό υπόβαθρο διαμορφώνουν διαφορετικά πρότυπα συμπεριφοράς στο ψηφιακό περιβάλλον.

Τέλος, ιδιαίτερη σημασία παρουσιάζει το εύρημα που αφορά την υπερβολική εμπιστοσύνη στις ίδιες τις πλατφόρμες κοινωνικής δικτύωσης. Οι χρήστες που θεωρούν ότι οι πλατφόρμες παρέχουν υψηλό επίπεδο προστασίας εμφανίζουν μειωμένη προσωπική επαγρύπνηση, γεγονός που αυξάνει την πιθανότητα λανθασμένων αποφάσεων. Το συμπέρασμα αυτό επιβεβαιώνει τις παρατηρήσεις των Williams et al. (2017), σύμφωνα με τις οποίες η αίσθηση ασφάλειας που αποδίδεται σε τρίτους, μπορεί να λειτουργήσει αποτρεπτικά ως προς την ανάπτυξη κριτικής στάσης.

5.2 Σύγκριση με τη διεθνή βιβλιογραφία

Συνολικά, τα αποτελέσματα της παρούσας μελέτης επιβεβαιώνουν σε μεγάλο βαθμό τις διαπιστώσεις της διεθνούς βιβλιογραφίας σχετικά με τον ρόλο των κοινωνικών δικτύων ως ευνοϊκών περιβαλλόντων για επιθέσεις social engineering. Η σημασία του ανθρώπινου παράγοντα, των γνωστικών προκαταλήψεων και της συναισθηματικής χειραγώγησης αναδεικνύεται τόσο σε θεωρητικό όσο και σε εμπειρικό επίπεδο.

Ταυτόχρονα, η μελέτη επεκτείνει την υπάρχουσα γνώση, αναδεικνύοντας ότι η ψηφιακή επάρκεια και η εκπαίδευση, αν και αναγκαίες, δεν επαρκούν από μόνες τους για την πλήρη αποτροπή της εξαπάτησης. Η διαπίστωση αυτή ενισχύει την άποψη ότι οι στρατηγικές πρόληψης οφείλουν να ενσωματώνουν όχι μόνο τεχνικά μέτρα, αλλά και παρεμβάσεις που στοχεύουν στη γνωστική και συναισθηματική διάσταση της ανθρώπινης συμπεριφοράς.

5.3 Περιορισμοί της μελέτης

Παρά τη συμβολή της, η παρούσα μελέτη παρουσιάζει ορισμένους περιορισμούς. Αρχικά, η χρήση ερωτηματολογίου βασίστηκε σε αυτοαναφερόμενα δεδομένα, τα οποία ενδέχεται να επηρεάζονται από υποκειμενικές εκτιμήσεις ή κοινωνικά επιθυμητές απαντήσεις. Επιπλέον, το δείγμα της έρευνας ενδέχεται να μην είναι πλήρως αντιπροσωπευτικό του γενικού πληθυσμού, γεγονός που περιορίζει τη δυνατότητα γενίκευσης των αποτελεσμάτων.

Ένας ακόμη περιορισμός αφορά τη δυναμική φύση του social engineering. Οι τεχνικές και οι πρακτικές των επιτιθέμενων εξελίσσονται διαρκώς, γεγονός που σημαίνει ότι ορισμένα ευρήματα ενδέχεται να διαφοροποιηθούν μελλοντικά. Παρ' όλα αυτά, καταβλήθηκε προσπάθεια ώστε τα ερωτήματα και η ανάλυση να εστιάζουν σε θεμελιώδεις ψυχολογικούς και συμπεριφορικούς μηχανισμούς, οι οποίοι διατηρούν τη σημασία τους διαχρονικά.

5.4 Προτάσεις για μελλοντική έρευνα και πρακτική εφαρμογή

Με βάση τα παραπάνω, αναδεικνύεται η ανάγκη για περαιτέρω έρευνα σε πολλαπλά επίπεδα. Μελλοντικές μελέτες θα μπορούσαν να αξιοποιήσουν ποιοτικές μεθόδους, όπως συνεντεύξεις ή μελέτες περίπτωσης, προκειμένου να διερευνηθούν σε μεγαλύτερο βάθος τα κίνητρα και οι γνωστικές διεργασίες των χρηστών κατά την έκθεσή τους σε επιθέσεις social engineering. Επιπλέον, θα ήταν χρήσιμη η διεξαγωγή συγκριτικών ερευνών μεταξύ διαφορετικών ηλικιακών ή επαγγελματικών ομάδων.

Σε πρακτικό επίπεδο, τα συμπεράσματα της μελέτης υποστηρίζουν την ανάγκη για πολυεπίπεδες στρατηγικές πρόληψης. Τέτοιες στρατηγικές θα πρέπει να συνδυάζουν την ενίσχυση των ψηφιακών δεξιοτήτων με εκπαίδευση που εστιάζει στη συναισθηματική και γνωστική διάσταση της εξαπάτησης, καθώς και με ρεαλιστική ενημέρωση των χρηστών σχετικά με τα πραγματικά όρια προστασίας των κοινωνικών δικτύων. Παράλληλα, οι οργανισμοί και οι πάροχοι πλατφορμών μπορούν να διαδραματίσουν καθοριστικό ρόλο, υιοθετώντας σχεδιαστικές και ενημερωτικές πρακτικές που ενισχύουν την κριτική σκέψη και τη συνειδητή χρήση των ψηφιακών υπηρεσιών.

5.5 Επίλογος

Συμπερασματικά, η παρούσα μελέτη επιβεβαιώνει ότι το social engineering στα κοινωνικά δίκτυα αποτελεί ένα σύνθετο φαινόμενο, το οποίο δεν μπορεί να αντιμετωπιστεί αποκλειστικά με τεχνικές λύσεις. Αντιθέτως, απαιτεί μια ολιστική προσέγγιση που λαμβάνει υπόψη τον άνθρωπο, την τεχνολογία και το κοινωνικό πλαίσιο μέσα στο οποίο αναπτύσσεται η ψηφιακή αλληλεπίδραση. Με αυτή την προσέγγιση, η έρευνα συμβάλλει τόσο στην επιβεβαίωση υφιστάμενων θεωρητικών διαπιστώσεων όσο και στην ανάδειξη νέων προβληματισμών, ανοίγοντας τον δρόμο για περαιτέρω επιστημονική διερεύνηση και πρακτική βελτίωση.

6. Βιβλιογραφία

Albladi, S. M., & Weir, G. R. S. (2018). Vulnerability to social engineering in social networks: A proposed measurement approach. *Information & Computer Security, 26*(1), 1–19.

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Applied Computing and Informatics, 16*(2), 168–179.

Aleroud, A., & Zhou, L. (2017). *Phishing environments, techniques, and countermeasures: A survey*. *Computers & Security*, 68, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Alkhalil, Z., et al. (2021). Phishing attacks: A recent comprehensive study and future research directions. *Frontiers in Computer Science*. https://doi.org/10.3389/fcomp.2021.563060

Alshammari, S. S., Soh, B., & Li, A. (2025). Understanding social engineering victimisation on social networking sites: A comprehensive review of factors influencing user susceptibility. *Information, 16*(2), 153. https://doi.org/10.3390/info16020153

Bakas, N., Lavdas, S., Vavousis, K., Christodoulou, C., Langousis, A. (2025). Automated Machine Learning in a Multi-agent Environment. Information Systems. EMCIS 2024. Lecture Notes in Business Information Processing, vol 535. Springer, Cham. https://doi.org/10.1007/978-3-031-81322-1_4

Baki, S., & Verma, R. M. (2023). Sixteen years of phishing user studies: What have we learned? *IEEE Transactions on Dependable and Secure Computing, 20*(2), 1200–1212.

Bouchillon, B. C. (2020). Social Networking for Interpersonal Life: A Competence-Based Approach to the Rich Get Richer Hypothesis. *Social Science Computer Review*, *40*(2), 309-327. https://doi.org/10.1177/0894439320909506

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210–230.

Chetioui, K., Bah, B., Ouali Alami, A., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science, 198*, 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Pearson Education.

Correa, T., Hinsley, A. W., & de Zúñiga, H. G. (2010). Who interacts on the web? The intersection of users' personality and social media use. *Computers in Human Behavior*, 26(2), 247–253. https://doi.org/10.1016/j.chb.2009.09.00

ENISA. (2022). *ENISA threat landscape report 2022*. European Union Agency for Cybersecurity.

ENISA. (2023). *Cybersecurity threat landscape 2023: Social engineering trends*. European Union Agency for Cybersecurity.

Fadhil, H. S. (2023). Social engineering attacks techniques. *Short Communication, 11*(1). American Journal of Computer Science and Engineering Survey.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Lecture Notes in Computer Science* (Vol. 9190, pp. 36–47). doi: 10.1007/978-3-319-20376-8_4

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security, 94*, 101862. https://doi.org/10.1016/j.cose.2020.101862

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon,* 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

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

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *Computers in Human Behavior, 30*, 182–191. https://doi.org/10.48550/arXiv.1301.764

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Jansen, J., & van Schaik, P. (2022). The role of cognitive biases in susceptibility to phishing attacks. *Computers & Security, 121*, 102837. https://doi.org/10.1016/j.cose.2022.102837

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584–593.

LinkedIn. (2025). *Post by CySeck – Centre of Excellence Cybersecurity Karnataka*. https://www.linkedin.com/posts/cyseck-centre-of-excellence-cybersecurity-karnataka_cyseck-cybersecuritykarnataka-cyseckindia-activity-7351481908263845888-IoCR

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

Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers: Improving internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior, 69*, 421–436. https://doi.org/10.1016/j.chb.2016.12.044

myAutoML, Bibliometrics. (2025) https://mireng.ai/bibliometrics

NIST. (2020). *NIST Special Publication 800-63B: Digital identity guidelines*. National Institute of Standards and Technology.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2019). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 88*, 101611.

Quayyum, F., & Freberg, G. (2024). Designing cybersecurity awareness solutions for young people in rural developing countries. In *Proceedings* (pp. 1–18). https://doi.org/10.1007/978-3-031-60881-0_1

Rathod, T., et al. (2025). A comprehensive survey on social engineering-based attacks. *Information Processing & Management, 62*(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

Sarno, D. M., & Neider, M. B. (2021). So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *64*(8), 1379-1403. https://doi.org/10.1177/0018720821999174

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, Article 324. https://doi.org/10.1007/s10462-024-10973-2

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences, 12*(12), 6042.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior, 60*, 35–43. https://doi.org/10.1016/j.chb.2016.02.050

Tullett-Prado, D., Stavropoulos, V., Gomez, R., & Doley, J. (2023). Social media use and abuse: Different profiles of users and their associations with addictive behaviours. *Addictive Behavior Reports, 17*, 100479. https://doi.org/10.1016/j.abrep.2023.100479

UK Competition and Markets Authority. (2023). *CMA annual plan 2023–2024*.https://www.gov.uk/government/publications/cma-annual-plan-2023-to-2024/cma-annual-plan-2023-to-2024

Verizon. (2022) "*Data breach investigations report 2022*", Verizon

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

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*, 412–421.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674.

Zhuo, S., et al. (2024). The impact of workload on phishing susceptibility: An experiment. In *Proceedings of the Symposium on Usable Security and Privacy (USEC 2024)*. https://doi.org/10.14722/usec.2024.23024

Παράρτημα Α - Γνωμοδότηση Διεξαγωγής Έρευνας

Neapolis University Pafos

Επιτροπή Δεοντολογίας-Βιοηθικής του Πανεπιστημίου Νεάπολις Πάφος
Πανεπιστήμιο Νεάπολις Πάφος,
Λεωφόρος Δανάης 2,
Πάφος
8042 Κύπρος
T +357 26843608
Web: www.nup.ac.cy
Email: m.argyrides.1@nup.ac.cy

Προς: Όποιον Ενδιαφέρει

Ημερ. 4/12/2025

Αρ. Πρωτοκόλλου: 72/2025

Θέμα: Γνωμοδότηση Διεξαγωγής Έρευνας

Κυρία Τσιάμουρου,

Σας ενημερώνω ότι το ερευνητικό πρωτόκολλο με τίτλο «Η αξιοποίηση των κοινωνικών δικτύων στο Social Engineering: Ψυχολογικές τεχνικές, κίνδυνοι και στρατηγικές αντιμετώπισης» έχει ελεγχθεί από την Επιτροπή Δεοντολογίας-Βιοηθικής του Πανεπιστημίου Νεάπολις Πάφος η οποία γνωμοδοτεί υπέρ της διεξαγωγής της έρευνας. Σας παρακαλώ λάβετε υπόψη ότι η συγκεκριμένη έρευνα έχει εγκριθεί για ένα έτος και ισχύει για συλλογή δεδομένων που **δεν** θα γίνουν στην Κυπριακή Δημοκρατία. Παρακαλώ όπως βεβαιωθείτε ότι η κυκλοφορία του ηλεκτρονικού συνδέσμου δεν θα συμπεριλάβει κάτοικους της Κυπριακής Δημοκρατίας. Αρμόδιο όργανο το οποίο είναι υπεύθυνο για έγκριση για συλλογή δεδομένων στην Κυπριακή Δημοκρατία είναι η Εθνική Επιτροπή Βιοηθικής Κύπρου. Σας παρακαλώ όπως ελέγξετε επίσης τους κανονισμούς και τις οποιεσδήποτε δεοντολογικές επιτροπές χρειάζεστε από τη χώρα που θα συλλέξετε τα δεδομένα σας.

Με εκτίμηση,

Δρ Μάριος Αργυρίδης
Καθηγητής Συμβουλευτικής Ψυχολογίας
Πρόεδρος Επιτροπής

Παράρτημα Β – Ερωτηματολόγιο

‘Η αξιοποίηση των κοινωνικών δικτύων στο Social Engineering: Ψυχολογικές τεχνικές, κίνδυνοι και στρατηγικές αντιμετώπισης’

1. Φύλο

- Άνδρας
- Γυναίκα
- Άλλο

2. Ηλικία

- Κάτω των 18
- 18–34
- 35–54
- 55–64
- 65+

3. Επίπεδο Εκπαίδευσης

- Λύκειο
- Προπτυχιακό
- Μεταπτυχιακό
- Διδακτορικό
- Άλλο

4. Επάγγελμα / Απασχόληση

- Φοιτητής / Φοιτήτρια
- Ιδιωτικός υπάλληλος
- Δημόσιος υπάλληλος
- Ελεύθερος επαγγελματίας
- Άνεργος
- Συνταξιούχος
- Άλλο

5. Τομέας Εργασίας (αν εργάζεστε)

- Πληροφορική / Τεχνολογία
- Εκπαίδευση

- Υγεία
- Οικονομικά / Τράπεζες
- Δημόσια διοίκηση
- Εμπόριο / Υπηρεσίες
- Άλλο
- Δεν εργάζομαι

6. Χρήση Κοινωνικών Δικτύων (Χρόνος ανά ημέρα)

- Λιγότερο από 1 ώρα
- 1–2 ώρες
- 2–4 ώρες
- 4–6 ώρες
- 6+ ώρες

7. Πλατφόρμες που χρησιμοποιείτε συχνότερα (Επιλέξτε έως 3)

- Facebook/messenger
- Instagram
- TikTok
- X (πρώην Twitter)
- LinkedIn
- YouTube
- Reddit
- WhatApp
- Άλλο

8. Επίπεδο Ψηφιακών Δεξιοτήτων (αυτοαξιολόγηση)

- Πολύ χαμηλό
- Χαμηλό
- Μεσαίο
- Υψηλό
- Πολύ υψηλό

9. Έχετε παρακολουθήσει ποτέ εκπαίδευση/σεμινάριο κυβερνοασφάλειας;

- Ναι
- Όχι

10. Έχετε πέσει θύμα διαδικτυακής απάτης / phishing / social engineering;

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

11. Πόσο αποτελεσματικά θεωρείτε ότι είναι τα τρέχοντα μέτρα ασφαλείας (όπως φίλτρα spam, προειδοποιήσεις browser, ειδοποιήσεις εφαρμογών κινητού) στην προστασία σας από νέες ή άγνωστες απόπειρες phishing;

Κλίμακα πρότασης: 1 = Καθόλου αποτελεσματικά, 5 = Πολύ αποτελεσματικά

12. Πόσο συχνά βασίζεστε στη διαίσθηση ή σε συναισθηματικά ερεθίσματα (π.χ. αίσθηση επείγοντος, φόβος, περιέργεια) όταν αποφασίζετε αν θα εμπιστευτείτε ένα μήνυμα ή έναν σύνδεσμο στο διαδίκτυο;

Κλίμακα πρότασης: 1 = Ποτέ, 5 = Πάντα

13. Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αντιμετωπίζετε αποτελεσματικά πραγματικές ή απρόσμενες απόπειρες κοινωνικής μηχανικής;
Κλίμακα: 1 = Καθόλου, 5 = Σε πολύ μεγάλο βαθμό

- Δεν έχω λάβει εκπαίδευση στην κυβερνοασφάλεια

14. Σε ποιο βαθμό θεωρείτε ότι η εκπαίδευση κυβερνοασφάλειας που έχετε λάβει σας βοηθά να αναπτύξετε την ικανότητα αναγνώρισης και εντοπισμού ψευδών ή παραπλανητικών πληροφοριών στα κοινωνικά δίκτυα;

Κλίμακα: 1 = Καθόλου, 5 = Σε πολύ μεγάλο βαθμό

- Δεν έχω λάβει εκπαίδευση στην κυβερνοασφάλεια

15. Πόσο θετικά θα βλέπατε τη χρήση "έξυπνων" εργαλείων εκπαίδευσης (π.χ. προσαρμοστικών εκπαιδευτικών modules με τεχνητή νοημοσύνη) που προσαρμόζονται στο προφίλ και τις ανάγκες του χρήστη για την ενίσχυση της προστασίας από επιθέσεις κοινωνικής μηχανικής;
Κλίμακα: 1 = Καθόλου θετικά, 5 = Πολύ θετικά

16. Πόσο συχνά ελέγχετε αν ένας σύνδεσμος ή μια προσφορά που εμφανίζεται στο κοινωνικό δίκτυο που χρησιμοποιείτε προέρχεται από αξιόπιστη πηγή πριν κάνετε κλικ;
Κλίμακα: 1 = Ποτέ, 5 = Πάντα

17. Σε ποιο βαθμό πιστεύετε ότι προσωπικά χαρακτηριστικά όπως ηλικία ή εμπειρία στο διαδίκτυο επηρεάζουν την πιθανότητά σας να πέσετε θύμα κοινωνικής μηχανικής στα κοινωνικά δίκτυα;
Κλίμακα: 1 = Καθόλου, 5 = Σε πολύ μεγάλο βαθμό

18. Πόσο συχνά νιώθετε ότι μηνύματα ή αναρτήσεις στα κοινωνικά δίκτυα προσπαθούν να επηρεάσουν τα συναισθήματά σας (π.χ. φόβο, επείγον, συμπόνια) για να σας πείσουν να κάνετε κάποια ενέργεια;
Κλίμακα: 1 = Ποτέ, 5 = Πολύ συχνά

19.Σε ποιο βαθμό θεωρείτε ότι η δική σας ψυχολογική κατάσταση (π.χ. κόπωση, άγχος, διάσπαση προσοχής, βιασύνη) μειώνει την προσοχή σας και αυξάνει την πιθανότητα να παραβλέψετε σημάδια κινδύνου σε μια πιθανή επίθεση phishing ή κοινωνικής μηχανικής;

Κλίμακα: 1 = Καθόλου, 5 = Σε πολύ μεγάλο βαθμό

20. Πόσο προετοιμασμένοι αισθάνεστε να εντοπίσετε περιεχόμενο που μπορεί να έχει δημιουργηθεί ή τροποποιηθεί από τεχνητή νοημοσύνη (π.χ. AI-generated posts, bots, προπαγάνδα) με σκοπό την παραπλάνηση;

Κλίμακα: 1 = Καθόλου προετοιμασμένος/η, 5 = Πολύ προετοιμασμένος/η

21. Όταν βλέπετε βίντεο ή εικόνες στα κοινωνικά δίκτυα, πόσο συχνά εξετάζετε την πιθανότητα να είναι αλλοιωμένα ή deepfakes πριν τα θεωρήσετε αξιόπιστα;
Κλίμακα: 1 = Ποτέ, 5 = Πάντα

22. Πόσο συχνά αντιμετωπίζετε ή αναγνωρίζετε μηνύματα/email που φαίνεται να είναι phishing, αλλά χρησιμοποιούν μεθόδους πέρα από την παραπλάνηση μέσω URL (π.χ. παραπλανητικά μηνύματα, συνημμένα αρχεία, fake ανακοινώσεις);
Κλίμακα: 1 = Ποτέ, 5 = Πολύ συχνά

23. Πόσο συχνά θεωρείται ότι επιτιθέμενοι κοινωνικής μηχανικής αξιοποιούν στοιχεία του προσωπικού σας προφίλ (π.χ. ενδιαφέροντα, δημόσιες αναρτήσεις, λίστα φίλων) στα κοινωνικά δίκτυα για να δημιουργήσουν πειστικά μηνύματα;
Κλίμακα: 1 = Ποτέ, 5 = Πολύ συχνά

24. Πόσο συχνά ελέγχετε τις ρυθμίσεις απορρήτου στα κοινωνικά σας δίκτυα;

Κλίμακα: 1 = Ποτέ, 5 = Πολύ συχνά

25. Θεωρείτε ότι τα κοινωνικά δίκτυα κάνουν αρκετά για να προστατεύσουν τους χρήστες από phishing και social engineering;

Κλίμακα: 1 = Καθόλου, 5 = Σε πολύ μεγάλο βαθμό