Σελίδα τίτλου

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΤΑΤΙΣΤΙΚΗ ΜΕΛΕΤΗ ΓΙΑ ΤΗΝ ΑΠΟΔΟΧΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΜΕΛΕΤΩΝ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

Παπαευαγγέλου Βασιλική

Επιβλέπων: Λιάγκου Βασιλική

Επίκουρος Καθηγητής, ΔΕΠ

Άρτα, Ιούλιος, 2025

STATISTICAL STUDY ON THE ACCEPTANCE OF CRYPTOGRAPHICS IN MODERN ELECTRONIC SERVICES

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Άρτα, 2025

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

   Βασιλική Λιάγκου,

2. Μέλος επιτροπής

   Όνομα Επίθετο,

3. Μέλος επιτροπής

   Όνομα Επίθετο,

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Παπαευαγγέλου, Βασιλική

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Είναι σημαντική η αναγνώριση της βοήθειας που έλαβε ο φοιτητής/ η φοιτήτρια κατά τη διάρκεια της προπαρασκευής της εργασίας του. Η βοήθεια μπορεί να είναι ακαδημαϊκή, τεχνική, γραμματειακή, διοικητική και προσωπική (π.χ. οικογένεια). Δεν υπερβαίνει τη μία παράγραφο.

[Διαγράψτε αυτή τη σελίδα αν δεν τη χρειάζεστε.]

ΠΕΡΙΛΗΨΗ

Η ασφάλεια ενός χρήστη, όσον αφορά την πρόσβαση σε ένα σύστημα, βασίζεται σε ισχυρούς κωδικούς πρόσβασης. Όσο πιο τυχαίοι είναι αυτοί οι κωδικοί τόσο πιο ασφαλή καθιστούν την αυθεντικοποίηση του χρήστη. Η βιομετρία προσφέρει ένα σαφές πλεονέκτημα για τη δημιουργία τέτοιων κωδικών. Ωστόσο, η μετάδοση και η αποθήκευσή τους αποτελούν σημαντικά ζητήματα καθώς τα βιομετρικά δεδομένα είναι στενά συνδεδεμένα με την ταυτότητα του χρήστη και γι' αυτό θα πρέπει να διασφαλιστεί το απόρρητο της πληροφορίας που φέρουν.

Η ανάπτυξη της πληροφορικής έχει οδηγήσει σε διάφορες καινοτομίες σε διάφορους τομείς. Αυτές οι καινοτομίες έχουν φέρει σημαντικές αλλαγές στον τρόπο ζωής, εργασίας και επικοινωνίας. Δεν είναι περίεργο που αυτές οι αλλαγές έχουν οδηγήσει σε έναν ψηφιακό τρόπο ζωής. Όμως όλες αυτές οι αλλαγές απαιτούν και μέτρα προστασίας στις ηλεκτρονικές υπηρεσίες με κρυπτογραφικά και μη συστήματα για την καλύτερη εξυπηρέτηση των πολιτών.

Στόχος της παρούσας εργασίας είναι να αναπτύξουμε ένα ερωτηματολόγιο που μετρά τις γνώσεις, τη στάση και τη συμπεριφορά για το απόρρητο και την ασφάλεια σε ένα ευρύ επίπεδο με ένα ευρύ φάσμα θεμάτων όπως έλεγχος ταυτότητας, παρακολούθηση ιστού, λειτουργικά συστήματα, κινητές συσκευές, ανταλλαγή άμεσων μηνυμάτων και μέσα κοινωνικής δικτύωσης, θα μπορούσαν να είναι κάποια βασικά σημεία της έρευνας μας.

Αρχικά θα αξιολογήσουμε ορισμένες μεθόδους που χρησιμοποιήθηκαν σε παρόμοιες μελέτες για την κρυπτογραφία σε ψηφιακά πορτοφόλια και γενικά ψηφιακά εργαλεία σε τράπεζες καθώς επίσης και για ένα κακόβουλο λογισμικό και πως αντιμετωπίστηκε. Επίσης θα αναλύσουμε και ορισμένες βασικές της έννοιες, τεχνικούς όρους καθώς και διάφορους αλγόριθμους (συμμετρικούς και ασύμμετρους) που έχουν αναπτυχθεί ιστορικά, κατά το πέρασμα των χρόνων.

Λέξεις-κλειδιά: Κρυπτογραφία, υπηρεσίες, δεδομένα, ασφάλεια

ABSTRACT

A user's security in accessing a system relies on strong passwords. The more random these codes are, the more secure they make user authentication. Biometrics offer a clear advantage for creating such codes. However, their transmission and storage are important issues as biometric data is closely linked to the user's identity and therefore the privacy of the information they carry should be ensured.

The development of IT has led to various innovations in various fields. These innovations have brought significant changes in the way we live, work and communicate. It is no wonder that these changes have led to a digital lifestyle. But all these changes also require protection measures in electronic services with cryptographic and non-cryptographic systems to better serve citizens.

The aim of this paper is to develop a questionnaire that measures privacy and security knowledge, attitude and behavior at a broad level with a wide range of topics such as authentication, web tracking, operating systems, mobile devices, instant messaging and social media, could be some key points of our research.

First we will evaluate some methods used in similar studies for cryptography in digital wallets and general digital tools in banks as well as for a malware and how it was treated. We will also analyze some of its basic concepts, technical terms as well as various algorithms (symmetric and asymmetric) that have been developed historically, over the years.

Keywords: Cryptography, services, data, security

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΓΡΑΦΗΜΑΤΩΝ - ΠΙΝΑΚΩΝ

1 ΕΙΣΑΓΩΓΗ

1.1 Σκοπός και Σημασία της Μελέτης

Στην εποχή της ψηφιακής δικτύωσης, της συνεχούς συνδεσιμότητας και της μαζικής χρήσης διαδικτυακών υπηρεσιών, η προστασία των προσωπικών δεδομένων και η ασφάλεια στον κυβερνοχώρο αποτελούν κρίσιμες παραμέτρους της καθημερινότητας. Παρά την εντυπωσιακή πρόοδο στην ανάπτυξη τεχνολογικών λύσεων ασφαλείας — όπως η κρυπτογράφηση, οι διαχειριστές κωδικών πρόσβασης (password managers), τα εικονικά ιδιωτικά δίκτυα (VPN), και οι πολιτικές ελέγχου ταυτότητας — παρατηρείται ένα σημαντικό χάσμα μεταξύ της διαθεσιμότητας αυτών των εργαλείων και της πραγματικής υιοθέτησής τους από το ευρύ κοινό.

Το πρόβλημα αυτό δεν είναι αποκλειστικά τεχνικό, αλλά σε μεγάλο βαθμό ανθρωποκεντρικό. Η απλή ύπαρξη τεχνολογικά εξελιγμένων εργαλείων δεν εγγυάται την εφαρμογή ή την αποδοχή τους από τον τελικό χρήστη. Τέσσερα βασικά εμπόδια συμβάλλουν καθοριστικά στη δημιουργία αυτού του χάσματος:

(1) το γνωσιακό εμπόδιο, που σχετίζεται με την πολυπλοκότητα της τεχνολογικής ορολογίας και την ελλιπή κατανόηση των κινδύνων,

(2) το εμπόδιο χρηστικότητας, που απορρέει από τον σχεδιασμό εργαλείων που απαιτούν τεχνικές γνώσεις και αυξημένο γνωστικό φορτίο,

(3) το ψυχολογικό εμπόδιο, το οποίο περιλαμβάνει τη στρεβλή αντίληψη κινδύνου και την "κούραση από αποφάσεις" (decision fatigue),

και (4) το οικονομικό ή προσβατικό εμπόδιο, όπου το κόστος ορισμένων λύσεων λειτουργεί αποτρεπτικά για μεγάλο μέρος του πληθυσμού.

Η παρούσα πτυχιακή εργασία διερευνά το εν λόγω χάσμα μέσα από την προσέγγιση των ανθρωποκεντρικών παραγόντων που επηρεάζουν τη στάση των χρηστών απέναντι στην ψηφιακή ασφάλεια. Στόχος είναι να κατανοηθεί γιατί οι χρήστες δεν υιοθετούν ευρέως διαθέσιμες και τεχνικά αξιόπιστες λύσεις, και να προταθούν αρχές σχεδιασμού εργαλείων και παρεμβάσεων που γεφυρώνουν αυτό το χάσμα, δίνοντας έμφαση στην εμπειρία χρήστη (UX), στην εκλαΐκευση της ασφάλειας και στη μείωση των ψυχολογικών και πρακτικών φραγμών.

Ενδεικτικά, οι υπηρεσίες να αποφασίσουν αν θα πρέπει να πραγματοποιούν συναλλαγές μόνο με αυτόν τον τρόπο πληρωμών καθώς και αν οι συμβαλλόμενοι μπορούν να ανταποκριθούν. Ο σύγχρονος τρόπος ζωής με τη ραγδαία ανάπτυξη της τεχνολογίας και των ηλεκτρονικών πληρωμών, οι οποίες ενισχύθηκαν περαιτέρω λόγω του παγκόσμιου προβλήματος που προκάλεσε η πανδημία του κορωνοιού και η ανάγκη για απομακρυσμένες συναλλαγές δίχως φυσική παρουσία, καθιστούν την έρευνα απολύτως επίκαιρη.

Η μελέτη στοχεύει:

- Στον εντοπισμό του επιπέδου ενημέρωσης των χρηστών σχετικά με τις μεθόδους κρυπτογράφησης που χρησιμοποιούνται για την ασφάλεια των δεδομένων τους.
- Στην αξιολόγηση της εμπιστοσύνης των χρηστών απέναντι στις τεχνολογίες αυτές.
- Στην καταγραφή τυχόν ανησυχιών ή επιφυλάξεων ως προς την αποτελεσματικότητα ή τη διαφάνεια των μηχανισμών κρυπτογράφησης.
- Στην εξέταση πιθανών δημογραφικών ή κοινωνικών παραγόντων που επηρεάζουν την αποδοχή ή την απόρριψη των εν λόγω τεχνολογιών.

Η μελέτη χρησιμοποιεί στατιστικές μεθόδους για την επεξεργασία των δεδομένων, με στόχο την εξαγωγή χρήσιμων συμπερασμάτων για φορείς που αναπτύσσουν, εφαρμόζουν ή επιβλέπουν ψηφιακές υπηρεσίες.

Σημασία της Μελέτης

Παρά την ύπαρξη αξιόπιστων εργαλείων και μεθόδων για την ψηφιακή ασφάλεια και την προστασία της ιδιωτικότητας, η αποτελεσματικότητά τους μειώνεται από τη σημαντική ανθρώπινη παράμετρο: την έλλειψη κατανόησης και την αδυναμία συνεπούς εφαρμογής τους από τον μέσο χρήστη.

1.2 Ερευνητικά ερωτήματα

Η παρούσα μελέτη επιδιώκει να διερευνήσει τους λόγους για τους οποίους, παρά τη διαθεσιμότητα εξελιγμένων λύσεων ψηφιακής ασφάλειας, η υιοθέτησή τους από το ευρύ κοινό παραμένει περιορισμένη. Στο πλαίσιο αυτό, διατυπώνονται ορισμένα βασικά ερευνητικά ερωτήματα, τα οποία κρίνονται αναγκαία για την εις βάθος κατανόηση του φαινομένου και θα αποτελέσουν τον θεμέλιο λίθο της εμπειρικής έρευνας.

Τα ερωτήματα αυτά θα εξεταστούν μέσω της δημιουργίας και διανομής ερωτηματολογίου, με στόχο την αποτύπωση των αντιλήψεων, της στάσης και της συμπεριφοράς των χρηστών σε σχέση με την ιδιωτικότητα και τα διαθέσιμα εργαλεία προστασίας της. Συγκεκριμένα, η μελέτη επιδιώκει να απαντήσει στα εξής ερωτήματα:

i. Ποιο είναι το επίπεδο γνώσης των χρηστών σχετικά με τις κρυπτογραφικές μεθόδους που χρησιμοποιούνται στις ηλεκτρονικές υπηρεσίες;
ii. Σε ποιο βαθμό οι χρήστες εμπιστεύονται την αποτελεσματικότητα της κρυπτογράφησης για την προστασία των προσωπικών τους δεδομένων;
iii. Υπάρχει συσχέτιση μεταξύ του επιπέδου εκπαίδευσης των χρηστών και της αποδοχής των κρυπτογραφικών μεθόδων;

iv. Ποιοι είναι οι βασικοί λόγοι που οδηγούν έναν χρήστη να αποδεχτεί ή να απορρίψει τις κρυπτογραφικές τεχνολογίες στις ηλεκτρονικές του συναλλαγές;
v. Επηρεάζει η ηλικία ή το φύλο των χρηστών την εμπιστοσύνη τους απέναντι στην κρυπτογράφηση των δεδομένων;
i. Πόσο ενημερωμένοι αισθάνονται οι χρήστες για την ύπαρξη και τη λειτουργία των μηχανισμών κρυπτογράφησης στις εφαρμογές που χρησιμοποιούν καθημερινά;
ii. Ποια είναι η στάση των χρηστών απέναντι σε ενδεχόμενες απειλές ασφαλείας, ακόμα και όταν εφαρμόζονται κρυπτογραφικές μέθοδοι;
iii. Ποιοι παράγοντες (τεχνολογικοί, κοινωνικοί, ψυχολογικοί) φαίνεται να επηρεάζουν περισσότερο την αποδοχή των κρυπτογραφικών τεχνολογιών;

1.3 Μεθοδολογία

Η παρούσα έρευνα βασίστηκε σε ποιοτική μεθοδολογική προσέγγιση με σκοπό τη συλλογή, ανάλυση και ερμηνεία δεδομένων σχετικά με την αποδοχή των κρυπτογραφικών μεθόδων από τους χρήστες ηλεκτρονικών υπηρεσιών. Μέσω του άρθρου των Parsons et al. (2014) με τίτλο «Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)» που παρουσιάζει την ανάπτυξη και αρχική αξιολόγηση ενός εργαλείου μέτρησης της επίγνωσης των εργαζομένων σε θέματα ασφάλειας πληροφοριών, εμείς θα αναπτύξουμε ένα ερωτηματολόγιο με συνεντεύξεις(ποιοτικά δεδομένα). Μέσω του ερωτηματολογίου δόθηκαν ερωτήσεις που αφορούσαν κάποιους βασικούς άξονες. Το ερωτηματολόγιο όπως θα δούμε αποτελείται από τέσσερις βασικές ενότητες:

- Δημογραφικά στοιχεία: Περιλαμβάνει ερωτήσεις σχετικά με το φύλο, την ηλικία, το επίπεδο εκπαίδευσης και το επάγγελμα.
- Ενημέρωση και κατανόηση κρυπτογράφησης: Περιλαμβάνει ερωτήσεις για το κατά πόσο οι χρήστες γνωρίζουν τι είναι η κρυπτογράφηση, ποια είδη υπάρχουν και αν αναγνωρίζουν τη χρήση της σε καθημερινές υπηρεσίες (π.χ. e-banking, cloud storage, ψηφιακά πορτοφόλια).
- Στάσεις και αντιλήψεις για την ασφάλεια: Ερωτήσεις που εξετάζουν το επίπεδο εμπιστοσύνης των συμμετεχόντων απέναντι στις κρυπτογραφικές τεχνολογίες και αν τις θεωρούν επαρκείς για την προστασία των προσωπικών δεδομένων.

- Αποδοχή και χρήση: Ερωτήσεις σχετικά με την προθυμία υιοθέτησης τεχνολογιών που χρησιμοποιούν κρυπτογράφηση, καθώς και τυχόν επιφυλάξεις, ανησυχίες ή προσδοκίες.

Η πλειονότητα των ερωτήσεων είναι τύπου Likert και υπάρχουν και ερωτήσεις ανοιχτού τύπου όπου πρέπει να αναφέρουν προσδοκίες ή τι τους ανησυχεί.

Δειγματοληψία και Συμμετέχοντες

Η έρευνα πραγματοποιήθηκε με μη πιθανοθετική δειγματοληψία ευκολίας, αξιοποιώντας κυρίως ψηφιακά μέσα (φόρμες Google/Online διανομή/ Μέσα κοινωνικής δικτύωσης). Στο δείγμα συμμετείχαν 60 άτομα (από τα οποία απάντησαν τα 50) και τα οποία χρησιμοποιούν τακτικά ηλεκτρονικές υπηρεσίες όπως ηλεκτρονική τραπεζική, online αγορές, cloud αποθήκευση και ψηφιακά πορτοφόλια.

1.4 Δομή της εργασίας

Η πτυχιακή εργασία δομείται σε επτά κεφάλαια, τα οποία αναπτύσσονται με λογική ακολουθία, ώστε να επιτυγχάνεται η ομαλή μετάβαση από το θεωρητικό υπόβαθρο στην ερευνητική διαδικασία και, τελικά, στα συμπεράσματα της μελέτης.

Στο πρώτο κεφάλαιο παρουσιάζεται το αντικείμενο της μελέτης, αναλύεται ο σκοπός και η σημασία της έρευνας και τίθενται τα ερευνητικά ερωτήματα που καθοδηγούν την εργασία. Επιπλέον, περιγράφεται η μεθοδολογική προσέγγιση που ακολουθήθηκε και παρατίθεται συνοπτικά η διάρθρωση του κειμένου.

Το δεύτερο κεφάλαιο εστιάζει στην ανάλυση του θεωρητικού πλαισίου που υποστηρίζει την έρευνα. Εξετάζονται οι έννοιες της ιδιωτικότητας και της ασφάλειας πληροφοριών, η συμβολή της κρυπτογράφησης στις ηλεκτρονικές υπηρεσίες και η σημασία της επίγνωσης των χρηστών αναφορικά με ζητήματα ιδιωτικότητας και ασφάλειας.

Στο τρίτο κεφάλαιο παρουσιάζονται μελέτες που διερευνούν την επίγνωση της ιδιωτικότητας και της ασφάλειας πληροφοριών, ενώ παράλληλα συγκρίνονται διαφορετικές μεθοδολογικές προσεγγίσεις, όπως το μοντέλο KAB και ο δείκτης Privacy Awareness Index. Η ανάλυση αυτή οδηγεί στη διατύπωση συμπερασμάτων από τη βιβλιογραφική ανασκόπηση.

Το τέταρτο κεφάλαιο περιγράφει τον σχεδιασμό της ερευνητικής διαδικασίας και του ερωτηματολογίου, παρουσιάζει τα δημογραφικά χαρακτηριστικά του δείγματος και αναλύει τα εργαλεία αξιολόγησης που χρησιμοποιήθηκαν (κλίμακες Likert, στατιστικοί δείκτες κ.ά.). Επιπλέον, καθορίζονται οι βασικές μεταβλητές που εξετάστηκαν, όπως η γνώση, η στάση και η συμπεριφορά των χρηστών.

Στο πέμπτο κεφάλαιο παρατίθενται τα αποτελέσματα της έρευνας και πραγματοποιείται η στατιστική τους ανάλυση. Τα ευρήματα εξετάζονται τόσο συνολικά όσο και ανά υποομάδες συμμετεχόντων (π.χ. Pragmatists, Fundamentalists), ενώ διερευνώνται οι συσχετίσεις μεταξύ ιδιωτικότητας και αποδοχής κρυπτογραφικών μεθόδων.

Το έκτο κεφάλαιο επικεντρώνεται στη συζήτηση των αποτελεσμάτων, τα οποία ερμηνεύονται υπό το πρίσμα των ερευνητικών ερωτημάτων και της υπάρχουσας βιβλιογραφίας. Ιδιαίτερη έμφαση δίνεται στην επιβεβαίωση ή μη της αρχικής υπόθεσης.

Και στο τελευταίο κεφάλαιο συνοψίζουμε τα βασικά συμπεράσματα που προέκυψαν από την έρευνα, διατυπώνουμε προτάσεις για την ενίσχυση της αποδοχής και χρήσης κρυπτογραφικών πρακτικών και προτείνουμε κατευθύνσεις για μελλοντική ερευνητική δραστηριότητα στον συγκεκριμένο τομέα.

2 ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

2.1 Η Έννοια της Ιδιωτικότητας και της Ασφάλειας Πληροφοριών

Η έννοια της ιδιωτικότητας (privacy) αποτελεί θεμελιώδες ανθρώπινο δικαίωμα και έχει αποκτήσει αυξημένη σημασία στο πλαίσιο των ψηφιακών τεχνολογιών και του διαδικτύου. Σύμφωνα με τον Bergmann (2009), η ιδιωτικότητα νοείται ως το δικαίωμα του ατόμου στον αυτοκαθορισμό αναφορικά με την κοινολόγηση των προσωπικών του δεδομένων. Ουσιαστικά, ο κάθε χρήστης οφείλει να διατηρεί τον έλεγχο του πόσα, σε ποιον και για ποιο σκοπό θα γνωστοποιεί προσωπικές πληροφορίες.

Η ραγδαία εξάπλωση των διαδικτυακών υπηρεσιών και των τεχνολογιών παρακολούθησης έχει οδηγήσει σε επανεξέταση του τρόπου με τον οποίο προστατεύονται τα δεδομένα των χρηστών, τόσο σε επίπεδο νομοθεσίας όσο και σε επίπεδο τεχνικών λύσεων. Στην ευρωπαϊκή νομοθεσία, το δικαίωμα στην ιδιωτικότητα έχει κεντρική θέση, όπως κατοχυρώνεται στη Οδηγία 95/46/EC περί προστασίας δεδομένων, η οποία αντικαταστάθηκε από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

Στενά συνυφασμένη με την έννοια της ιδιωτικότητας είναι η έννοια της informational self-determination (πληροφοριακή αυτοδιάθεση). Όπως ορίζεται στο ίδιο άρθρο, πρόκειται για το δικαίωμα του ατόμου να καθορίζει ελεύθερα ποια προσωπικά του δεδομένα θα συλλεχθούν, πώς θα χρησιμοποιηθούν και ποιοι τρίτοι θα έχουν πρόσβαση σε αυτά.

Η πληροφοριακή αυτοδιάθεση αποτελεί τη βάση πάνω στην οποία χτίζεται κάθε σύγχρονη προσέγγιση προστασίας προσωπικών δεδομένων, ενισχύοντας την ιδέα ότι η συναίνεση του χρήστη πρέπει να είναι ενεργή, ρητή και βασισμένη σε πλήρη κατανόηση των όρων της κοινολόγησης.

Επιπλέον, σύμφωνα με τη θεωρητική προσέγγιση του Bergmann (2009) μία από τις βασικές αρχές της επεξεργασίας προσωπικών δεδομένων είναι και η δέσμευση σκοπού (purpose binding). Η αρχή αυτή ορίζει ότι τα προσωπικά δεδομένα που συλλέγονται πρέπει να χρησιμοποιούνται αποκλειστικά για τον σαφώς καθορισμένο σκοπό για τον οποίο παρασχέθηκαν και όχι για άλλους, μη συναφείς σκοπούς.[27]

Η ύπαρξη σαφούς δήλωσης σκοπού ενισχύει τη διαφάνεια και επιτρέπει στον χρήστη να αντιληφθεί τη χρήση των δεδομένων του, μειώνοντας την αβεβαιότητα και τον φόβο κατάχρησης. Για παράδειγμα, εάν μία διεύθυνση email συλλέγεται για αποστολή επιβεβαιωτικών μηνυμάτων, δεν επιτρέπεται η χρήση της για εμπορική προώθηση χωρίς πρόσθετη συναίνεση.

Τέλος, σύμφωνα πάλι με τον Bergmann (2009) η ενημερωμένη συγκατάθεση (informed consent) αποτελεί και αυτή απαραίτητη προϋπόθεση για κάθε νόμιμη και ηθική επεξεργασία προσωπικών δεδομένων. Δεν αρκεί ο χρήστης να αποδέχεται παθητικά όρους· η συναίνεση πρέπει να βασίζεται σε πλήρη, σαφή και κατανοητή πληροφόρηση για ποια δεδομένα συλλέγονται, για ποιον λόγο, για πόσο διάστημα αποθηκεύονται, εάν διαμοιράζονται με τρίτους και ποιες είναι οι συνέπειες της άρνησης ή ανάκλησης της συγκατάθεσης.[27]

Η ανάγκη για ουσιαστική και όχι τυπική συγκατάθεση αναδεικνύεται έντονα στην εργασία του, όπου τονίζεται ότι οι χρήστες συχνά αγνοούν τις πολιτικές απορρήτου ή δεν τις κατανοούν, με αποτέλεσμα η συγκατάθεσή τους να είναι ουσιαστικά ανενημέρωτη και άκυρη ως προς τη νομική και ηθική της ισχύ.

Οπότε, το θεωρητικό πλαίσιο της παρούσας εργασίας βασίζεται σε αυτές τις θεμελιώδεις έννοιες της ιδιωτικότητας, της πληροφοριακής αυτοδιάθεσης, της δέσμευσης σκοπού και της ενημερωμένης συγκατάθεσης, όπως παρουσιάζονται στην ερευνητική προσέγγιση του Bergmann (2009). Η κατανόηση αυτών των εννοιών είναι καθοριστική για την ανάλυση και αξιολόγηση πρακτικών επεξεργασίας προσωπικών δεδομένων στο σύγχρονο ψηφιακό περιβάλλον, καθώς και για τη σχεδίαση φιλικών προς τον χρήστη και νομικά συμβατών συστημάτων.

Στη συνέχεια θα δούμε πως η ασφάλεια πληροφοριών (Information Security) αποτελεί τον κεντρικό άξονα προστασίας των πληροφοριακών πόρων σε κάθε ψηφιακό περιβάλλον. Στοχεύει στην αποτροπή της μη εξουσιοδοτημένης πρόσβασης, χρήσης, αποκάλυψης, αλλοίωσης ή καταστροφής των δεδομένων. Η προστασία αυτή βασίζεται σε δύο βασικά θεωρητικά πλαίσια: το Τρίπτυχο CIA και τη διαστρωματωμένη προσέγγιση ασφαλείας.

- Το Τρίπτυχο CIA (CIA Triad)

Σύμφωνα με τον Andress (2011), η έννοια της ασφάλειας πληροφοριών διαρθρώνεται γύρω από τρεις θεμελιώδεις αρχές:

- Εμπιστευτικότητα (Confidentiality):

Αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Η εμπιστευτικότητα διασφαλίζει ότι τα δεδομένα είναι διαθέσιμα μόνο σε εξουσιοδοτημένα άτομα ή συστήματα, διατηρώντας έτσι την ιδιωτικότητα των πληροφοριών.

- Ακεραιότητα (Integrity):

Αναφέρεται στην ακρίβεια και την πληρότητα των πληροφοριών. Η ακεραιότητα εγγυάται ότι τα δεδομένα δεν θα τροποποιηθούν ή καταστραφούν κατά τρόπο μη εξουσιοδοτημένο ή τυχαίο, εξασφαλίζοντας τη γνησιότητα και αξιοπιστία τους.

- Διαθεσιμότητα (Availability):

Υποδηλώνει ότι τα δεδομένα και τα πληροφοριακά συστήματα είναι προσβάσιμα στους εξουσιοδοτημένους χρήστες όποτε τα χρειάζονται. Η διαθεσιμότητα προστατεύει από επιθέσεις τύπου Denial-of-Service (DoS), τεχνικές δυσλειτουργίες και άλλες απειλές που περιορίζουν την πρόσβαση.

Το τρίπτυχο CIA αποτελεί το θεωρητικό θεμέλιο πάνω στο οποίο στηρίζεται η σχεδίαση και υλοποίηση κάθε πολιτικής και τεχνικής μέτρου ασφάλειας.

Η αποτελεσματική προστασία των πληροφοριών δεν μπορεί να στηρίζεται σε ένα μόνο μέτρο ή τεχνολογία. Όπως υπογραμμίζουν οι Whitman και Mattord (2012), η ασφάλεια πρέπει να υλοποιείται σε πολλαπλά επίπεδα που καλύπτουν τόσο τις τεχνικές όσο και τις οργανωτικές παραμέτρους:

- Φυσική Ασφάλεια (Physical Security):

Προστασία φυσικών πόρων (όπως εξοπλισμός, κτίρια, servers) από παράνομη πρόσβαση, καταστροφή ή κλοπή.

- Ασφάλεια Προσωπικού (Personnel Security):

Εξασφάλιση ότι τα άτομα με πρόσβαση σε κρίσιμα δεδομένα ή συστήματα είναι αξιόπιστα και εκπαιδευμένα, μέσω ελέγχων πρόσληψης, πολιτικών πρόσβασης και εκπαίδευσης.

- Ασφάλεια Λειτουργιών (Operations Security):

Προστασία των διαδικασιών και δραστηριοτήτων ενός οργανισμού, ώστε να αποφεύγεται η διαρροή ευαίσθητων πληροφοριών μέσω καθημερινών λειτουργιών.

- Ασφάλεια Επικοινωνιών (Communication Security):

Αφορά την προστασία της μετάδοσης πληροφοριών από παρακολούθηση, υποκλοπή ή αλλοίωση.

- Ασφάλεια Δικτύου (Network Security):

Εστιάζει στην προστασία των υποδομών δικτύου (δρομολογητές, firewalls, servers) από επιθέσεις ή εισβολές.

- Ασφάλεια Πληροφορίας (Information Security):

Ενσωματώνει τις αρχές της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας σε όλα τα επίπεδα διαχείρισης της πληροφορίας, μέσω πολιτικών, εκπαίδευσης και τεχνολογικών λύσεων.

- <u>Διαστρωματωμένη προσέγγιση ασφάλειας</u>

Η διαστρωματωμένη ασφάλεια λειτουργεί ως σύστημα αλληλεπικαλυπτόμενων μέτρων, που ενισχύει τη συνολική ανθεκτικότητα των πληροφοριακών υποδομών απέναντι σε απειλές εσωτερικές και εξωτερικές.

Ένα ερωτηματολόγιο που βασίζεται σε αυτές τις έννοιες που αναφέραμε προσφέρει μια ολοκληρωμένη μέθοδο καταγραφής και αξιολόγησης της επίγνωσης και των στάσεων των χρηστών απέναντι στην προστασία των προσωπικών τους δεδομένων. Αποτελεί δηλαδή ένα ισχυρό εργαλείο για την ερευνητική διερεύνηση αλλά και για την αποτύπωση των αναγκών που πρέπει να καλύπτονται από τις ψηφιακές πολιτικές απορρήτου.

2.2 Κρυπτογράφηση και Ηλεκτρονικές Υπηρεσίες

Η κρυπτογράφηση (encryption) αποτελεί βασική τεχνολογία για την προστασία των δεδομένων κατά την αποθήκευση και τη μετάδοση, και είναι αναπόσπαστο μέρος της ασφάλειας πληροφοριών. Στο πλαίσιο των ηλεκτρονικών υπηρεσιών –ιδίως των ψηφιακών πορτοφολιών (digital wallets) και εφαρμογών ηλεκτρονικών πληρωμών (e-payment apps)– η κρυπτογράφηση λειτουργεί ως θεμέλιο για τη διασφάλιση της εμπιστευτικότητας (confidentiality) και την ενίσχυση της εμπιστοσύνης των χρηστών.

Η κρυπτογράφηση είναι ένας μηχανισμός που μετατρέπει αναγνώσιμα δεδομένα σε μη αναγνώσιμη μορφή, ώστε να αποτραπεί η πρόσβαση από μη εξουσιοδοτημένα πρόσωπα. Εφαρμόζεται τόσο κατά τη μετάδοση των δεδομένων (π.χ. HTTPS, TLS), όσο και κατά την αποθήκευσή τους (π.χ. κρυπτογράφηση βάσεων δεδομένων, αρχείων). Στην τριάδα CIA, η κρυπτογράφηση σχετίζεται κυρίως με την εμπιστευτικότητα (Confidentiality), ενώ ενισχύει έμμεσα και την ακεραιότητα (Integrity) μέσω ψηφιακών υπογραφών και ελέγχου μεταβολών.

Οι ψηφιακές χρηματοοικονομικές υπηρεσίες, όπως τα e-wallets, βρίσκονται στο επίκεντρο της σύγχρονης ψηφιακής καθημερινότητας. Σύμφωνα με την έρευνα των Fadhilah et al. (2021), το 82.7% των ερωτηθέντων ανέφεραν ότι χρησιμοποιούν τα ψηφιακά πορτοφόλια, με το 81.6% να βασίζει την επιλογή του στην εμπιστοσύνη προς το προϊόν. Ωστόσο, η αυξημένη χρήση συνοδεύεται και από ψηφιακές απειλές, όπως:

- Phishing και Malware
- Man-in-the-Middle (MiTM) Attacks
- SIM Swapping
- Απάτες μέσω πλαστών εφαρμογών και ψεύτικων OTP αιτήσεων

Σε αυτό το πλαίσιο, η χρήση ασφαλών καναλιών επικοινωνίας (π.χ. HTTPS) και η κρυπτογράφηση των προσωπικών δεδομένων και των κωδικών θεωρούνται ουσιώδεις για την αποτροπή παραβιάσεων.

Παρά την ύπαρξη των τεχνολογικών μέτρων, η ανθρώπινη συμπεριφορά εξακολουθεί να αποτελεί τον πιο ευάλωτο κρίκο. Η μελέτη των Fadhilah et al. κατέγραψε ότι πολλοί χρήστες:

- Χρησιμοποιούν δωρεάν VPN, αγνοώντας τους κινδύνους απορρήτου.
- Αποθηκεύουν ευαίσθητα δεδομένα (όπως PIN και αριθμούς λογαριασμών) χωρίς προστασία.
- Εισάγουν προσωπικά δεδομένα σε πλαστά site με υποσχέσεις για ανταμοιβές.

Αυτό δείχνει ότι η ύπαρξη κρυπτογράφησης δεν αρκεί αν ο χρήστης δεν είναι ενήμερος ή ευαισθητοποιημένος απέναντι στην ιδιωτικότητα και τις απειλές.

Η εμπιστοσύνη (trust) αποτελεί κρίσιμο παράγοντα για την αποδοχή των ηλεκτρονικών υπηρεσιών. Η γνώση ότι μια υπηρεσία χρησιμοποιεί ισχυρούς μηχανισμούς κρυπτογράφησης, διασφαλίζει:

- την αποδοχή όρων χρήσης,
- τη συχνότητα χρήσης της υπηρεσίας, και
- τη διάθεση των χρηστών να καταχωρήσουν προσωπικά τους στοιχεία.

Οι πολιτικές απορρήτου που αναφέρουν ρητά την κρυπτογράφηση των δεδομένων, δημιουργούν αίσθημα ασφάλειας και ενισχύουν τη θετική στάση του χρήστη απέναντι στην υπηρεσία.

Η κρυπτογράφηση αποτελεί ουσιώδες στοιχείο των πολιτικών ασφάλειας και απορρήτου σε κάθε ψηφιακή υπηρεσία. Ωστόσο, η αποτελεσματικότητα της εξαρτάται από το επίπεδο ενημέρωσης, κατανόησης και συμπεριφοράς του ίδιου του χρήστη. Συνεπώς, η σύνδεση μεταξύ τεχνολογικών μέτρων (όπως η κρυπτογράφηση) και επίγνωσης ασφάλειας πληροφοριών (information security awareness) είναι θεμελιώδης για την επιτυχία κάθε συστήματος προστασίας.

2.3 Ενημέρωση και Επίγνωση των Χρηστών (Privacy & Security Awareness)

Η ενημέρωση και επίγνωση των χρηστών (privacy & security awareness) αποτελούν κρίσιμες παραμέτρους για την προστασία της ιδιωτικότητας και την πρόληψη απειλών στον ψηφιακό χώρο. Σύμφωνα με τη μελέτη των Fadhilah et al. (2021), η οποία εστιάζει στην επίγνωση ασφάλειας χρηστών ψηφιακών πορτοφολιών στην Ινδονησία, η ανθρώπινη συμπεριφορά εξακολουθεί να αποτελεί έναν από τους σημαντικότερους παράγοντες παραβίασης δεδομένων και επιτυχημένων επιθέσεων.

Η μέτρηση της επίγνωσης βασίστηκε στο μοντέλο Knowledge-Attitude-Behavior (KAB), το οποίο προτείνει ότι η ύπαρξη γνώσης (knowledge) και θετικής στάσης (attitude) απέναντι στην ασφάλεια συντελεί στην ανάπτυξη ορθής συμπεριφοράς (behavior) κατά την αλληλεπίδραση με ψηφιακά συστήματα ενώ για τον καθορισμό των σχετικών βαρών κάθε διάστασης εφαρμόστηκε η μέθοδος Analytic Hierarchy Process (AHP). Το KAB μοντέλο αξιολογήθηκε σε συνδυασμό με επτά επιμέρους θεματικές ενότητες του εργαλείου HAIS-Q (Human Aspects of Information Security Questionnaire), που περιλαμβάνουν: διαχείριση κωδικών, χρήση email, χρήση διαδικτύου, κοινωνικά δίκτυα, κινητές συσκευές, χειρισμό πληροφοριών και αναφορά περιστατικών ασφαλείας.

Η μέθοδος AHP επιλέχθηκε καθώς επιτρέπει την ιεραρχική ανάλυση πολύπλοκων προβλημάτων λήψης αποφάσεων και τη στάθμιση κριτηρίων βάσει συγκριτικών

προτιμήσεων. Στο πλαίσιο της συγκεκριμένης μελέτης, οι ερευνητές διαμόρφωσαν μια ιεραρχική δομή τριών επιπέδων:

- Στο ανώτερο επίπεδο τοποθετήθηκε ο γενικός στόχος, δηλαδή η εκτίμηση του επιπέδου επίγνωσης ασφάλειας πληροφοριών.
- Στο μεσαίο επίπεδο περιλαμβάνονταν οι τρεις κύριες διαστάσεις του μοντέλου KAB (Knowledge, Attitude, Behaviour), οι οποίες λειτούργησαν ως κριτήρια αξιολόγησης.
- Στο κατώτερο επίπεδο τοποθετήθηκαν οι επτά επιμέρους θεματικές περιοχές (password management, email usage, use of internet, use of social media, mobile device, information handling, incident reporting), οι οποίες αποτελούσαν τις εναλλακτικές μεταβλητές προς στάθμιση.

Για τον υπολογισμό των βαρών των τριών διαστάσεων, οι συγγραφείς βασίστηκαν στα βάρη που είχαν προτείνει οι Kruger και Kearney (2006), καθώς το αρχικό τους μοντέλο αποτελεί σημείο αναφοράς στη μέτρηση επίγνωσης ασφάλειας πληροφοριών. Συγκεκριμένα, ορίστηκαν τα εξής βάρη:

- Knowledge: 30%
- Attitude: 20%
- Behaviour: 50%

Ακολούθως, τα δεδομένα που συλλέχθηκαν μέσω ερωτηματολογίων αναλύθηκαν με χρήση της μεθόδου AHP, ώστε να υπολογιστούν τα σταθμισμένα σκορ κάθε θεματικής περιοχής, λαμβάνοντας υπόψη τη συνεισφορά κάθε διάστασης KAB. Το τελικό επίπεδο επίγνωσης προέκυψε από το σταθμισμένο άθροισμα των αποτελεσμάτων, σύμφωνα με τον τύπο που προτείνουν οι Kruger και Kearney.

Η χρήση της AHP εξασφάλισε ότι τα αποτελέσματα αντανακλούν με συστηματικό τρόπο τη σχετική σημασία των τριών διαστάσεων στη διαμόρφωση της συνολικής επίγνωσης ασφάλειας πληροφοριών, προσδίδοντας στη μέτρηση υψηλότερη εγκυρότητα και αντικειμενικότητα.

Η συγκεκριμένη μελέτη των Fadhilah et al. (2021) κατέδειξε ότι το γενικό επίπεδο επίγνωσης των 156 ερωτηθέντων χρηστών ψηφιακών πορτοφολιών στην Ινδονησία ήταν ικανοποιητικό (80.78%), γεγονός που υποδηλώνει μια σχετικά καλή κατανόηση των ζητημάτων ασφάλειας πληροφοριών. Παρ' όλα αυτά, εντοπίστηκαν αδυναμίες σε επιμέρους τομείς, οι οποίες υποδεικνύουν ανάγκη για περαιτέρω εκπαίδευση και ενημέρωση:

- Χρήση κοινωνικών δικτύων (73.35%)

Οι χρήστες παρουσίασαν χαμηλό επίπεδο επίγνωσης σχετικά με τους κινδύνους δημοσιοποίησης προσωπικών δεδομένων. Πολλοί θεωρούν ότι η εμφάνιση πληροφοριών,

όπως ο αριθμός τηλεφώνου, δεν εγκυμονεί κινδύνους, γεγονός που αυξάνει τις πιθανότητες ηλεκτρονικής απάτης.

- Χρήση διαδικτύου και διαχείριση πληροφοριών

Καταγράφηκε χαμηλή επίδοση λόγω έλλειψης γνώσης για τους κινδύνους που προκύπτουν από τη χρήση ανεπίσημων ή δωρεάν VPN και από την αποθήκευση ευαίσθητων δεδομένων, όπως PIN, σε μη ασφαλείς τοποθεσίες (π.χ. στο κινητό τηλέφωνο χωρίς κωδικό πρόσβασης).

- Χρήση ηλεκτρονικού ταχυδρομείου (email)

Εντοπίστηκαν σημαντικά κενά στην αναγνώριση κακόβουλων μηνυμάτων, καθώς αρκετοί χρήστες εξακολουθούν να ανταποκρίνονται σε πλαστές ειδοποιήσεις ή προσφορές που μιμούνται επίσημους παρόχους υπηρεσιών.

Τα παραπάνω ευρήματα επιβεβαιώνουν ότι, αν και το γενικό επίπεδο επίγνωσης είναι θετικό, η στοχευμένη καλλιέργεια γνώσεων και στάσεων γύρω από την ασφάλεια πληροφοριών παραμένει αναγκαία. Οι ελλείψεις αυτές σχετίζονται με τη συμπεριφορά των χρηστών, όπως αποτυπώνεται στο μοντέλο Knowledge–Attitude–Behavior (KAB), όπου η ελλιπής γνώση οδηγεί σε ανεπαρκείς στάσεις και ανασφαλείς πρακτικές.

Οι συγγραφείς προτείνουν στοχευμένες εκπαιδευτικές δράσεις, ενημερωτικές εκστρατείες και πολιτικές που να αποτρέπουν την πρόσβαση μέσω επισφαλών τεχνικών (π.χ. χρήση δωρεάν VPN). Η συνεχής ευαισθητοποίηση των χρηστών αναγνωρίζεται ως ουσιώδης παράγοντας για την ενίσχυση της ψηφιακής ασφάλειας και την προάσπιση της ιδιωτικότητας, ιδιαίτερα σε περιβάλλοντα αυξημένης τεχνολογικής εξάρτησης, όπως οι εφαρμογές ψηφιακών συναλλαγών.

Το άρθρο δείχνει καθαρά ότι η ενημέρωση και επίγνωση των χρηστών είναι κρίσιμος παράγοντας για την προστασία της ιδιωτικότητας και της ασφάλειας στις ψηφιακές συναλλαγές. Ενώ η γενική εικόνα είναι θετική, οι συγκεκριμένες αδυναμίες απαιτούν στοχευμένη παρέμβαση, κυρίως με εκπαίδευση και πολιτικές προστασίας.[22]

2.4 Η αναγκαιότητα για κατανόηση των χρηστών γύρω από αυτές τις τεχνολογίες

Η ευρεία υιοθέτηση των τεχνολογιών ψηφιακών πορτοφολιών (digital wallets) έχει μετασχηματίσει σημαντικά τον τρόπο με τον οποίο οι χρήστες πραγματοποιούν ηλεκτρονικές συναλλαγές. Παρά τα σημαντικά πλεονεκτήματα που προσφέρουν σε επίπεδο ταχύτητας και ευκολίας, η αυξημένη χρήση τους έχει ταυτόχρονα επιφέρει και νέους κινδύνους ασφάλειας. Όπως επισημαίνεται από τους Fadhilah et al. (2021), η ανθρώπινη συμπεριφορά αποτελεί καθοριστικό παράγοντα για την ασφάλεια ή την ευαλωτότητα των

χρηστών, καθώς πολλοί από τους κινδύνους δεν σχετίζονται άμεσα με τεχνικά προβλήματα, αλλά με έλλειψη κατανόησης και επίγνωσης.

Για την ποσοτική αποτίμηση αυτής της επίγνωσης, οι Fadhilah και συνεργάτες χρησιμοποίησαν τη μέθοδο Analytic Hierarchy Process (AHP), η οποία επιτρέπει τον υπολογισμό βαρών μεταξύ των επιμέρους διαστάσεων και πεδίων ασφάλειας με βάση συγκρίσεις προτεραιοτήτων. Μέσω της ιεραρχικής αυτής προσέγγισης, κάθε διάσταση (γνώση, στάση, συμπεριφορά) και κάθε θεματική περιοχή (όπως διαχείριση κωδικών, χρήση διαδικτύου, κοινωνικά δίκτυα, χειρισμός πληροφοριών) αξιολογείται και σταθμίζεται, ώστε να προσδιοριστεί η συνολική στάθμη ενημερότητας των χρηστών. Η Γνώση (Knowledge) η αφορά τις πληροφορίες και δεξιότητες που έχει ο χρήστης σχετικά με την ασφάλεια, όπως η προστασία κωδικών πρόσβασης, η αναγνώριση phishing ή ransomware και η προστασία προσωπικών δεδομένων. Η Στάση (Attitude) εξετάζει τις πεποιθήσεις και την προδιάθεση του χρήστη απέναντι στην ασφάλεια, για παράδειγμα την αντίληψη του σχετικά με τη σημασία της αλλαγής κωδικών ή της προσοχής σε ύποπτα μηνύματα. Τέλος, η Συμπεριφορά (Behavior) αξιολογεί τις πραγματικές ενέργειες του χρήστη, όπως τη χρήση διαφορετικών κωδικών για κάθε εφαρμογή, την αποφυγή ύποπτων συνδέσμων και την ενημέρωση λογισμικού. Ο συνδυασμός αυτών των τριών παραμέτρων επιτρέπει την εκτίμηση του συνολικού επιπέδου επίγνωσης: παράδειγμα χρήστες με υψηλή γνώση, θετική στάση και ασφαλή συμπεριφορά θεωρούνται ότι έχουν υψηλή επίγνωση ασφάλειας πληροφοριών, ενώ χαμηλή γνώση ή αρνητική στάση μειώνουν αντίστοιχα το επίπεδο αυτό, ακόμη και αν η συμπεριφορά είναι εν μέρει σωστή.

Η αξιοποίηση του AHP επιτρέπει την ανάδειξη κρίσιμων πεδίων που απαιτούν εκπαίδευση ή παρέμβαση, ενισχύοντας έτσι την ικανότητα των χρηστών να αντιλαμβάνονται τους κινδύνους και να υιοθετούν ασφαλέστερες πρακτικές. Κατά συνέπεια, η ενσωμάτωση εργαλείων αξιολόγησης όπως το AHP σε έρευνες ευαισθητοποίησης συμβάλλει ουσιαστικά στη διαμόρφωση στοχευμένων στρατηγικών για την ενίσχυση της ασφάλειας και της εμπιστοσύνης στις ψηφιακές υπηρεσίες.

Ενδεικτικά, πολλοί χρήστες δεν αναγνωρίζουν τη σημασία της απόκρυψης προσωπικών δεδομένων, όπως ο αριθμός κινητού τηλεφώνου στα κοινωνικά δίκτυα, ή αγνοούν τους κινδύνους της χρήσης μη ασφαλών καναλιών σύνδεσης, όπως τα δωρεάν VPN. Επιπλέον, αρκετοί χρήστες τείνουν να αποθηκεύουν PIN και άλλα ευαίσθητα δεδομένα στο κινητό τους χωρίς κατάλληλη προστασία, γεγονός που αυξάνει την πιθανότητα παραβίασης της ιδιωτικότητάς τους σε περίπτωση απώλειας ή κακόβουλης πρόσβασης στη συσκευή.

Η κατανόηση των τεχνολογιών και των σχετικών απειλών από τους ίδιους τους χρήστες είναι συνεπώς προϋπόθεση για την αποτελεσματική προστασία των προσωπικών δεδομένων. Οι συγγραφείς προτείνουν ως μέτρα:

- Την ενίσχυση της εκπαίδευσης των χρηστών σχετικά με απειλές και καλές πρακτικές ασφαλείας,
- Τη θέσπιση πολιτικών απαγόρευσης επισφαλών τεχνικών (όπως η χρήση δωρεάν VPN),

- Την τακτική ευαισθητοποίηση μέσω ενημερωτικών εκστρατειών από παρόχους ψηφιακών πορτοφολιών.

Συνολικά, η μελέτη τεκμηριώνει ότι η τεχνολογική ασφάλεια δεν μπορεί να αποδώσει πλήρως χωρίς την παράλληλη ανάπτυξη της ανθρώπινης επίγνωσης, η οποία επιτυγχάνεται μέσα από τη γνώση, τη στάση και τη συνεπή συμπεριφορά των χρηστών.

3 ΕΠΙΓΝΩΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ

3.1 Μελέτες για την επίγνωση Ιδιωτικότητας

Στον σύγχρονο ψηφιακό κόσμο, όπου οι διαδικτυακές συναλλαγές και οι υπηρεσίες βασίζονται ολοένα και περισσότερο στη διακίνηση προσωπικών δεδομένων, η κρυπτογραφία αποτελεί θεμελιώδες εργαλείο για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών. Παρ' όλα αυτά, η αποδοχή των κρυπτογραφικών μεθόδων από τους τελικούς χρήστες δεν είναι αυτονόητη. Η αντίληψη περί ασφάλειας, η κατανόηση των τεχνικών διαδικασιών και η εμπιστοσύνη προς τον πάροχο της υπηρεσίας αποτελούν καθοριστικούς παράγοντες που επηρεάζουν τη στάση του κοινού απέναντι στη χρήση τέτοιων τεχνολογιών.

Η επίγνωση ιδιωτικότητας (privacy awareness), όπως αναδεικνύεται και στη μελέτη του Bergmann (2009), διαδραματίζει καθοριστικό ρόλο στην αποδοχή των τεχνολογικών μέτρων προστασίας. Οι χρήστες που κατανοούν τις αρχές της ενημερωμένης συναίνεσης και της δέσμευσης σκοπού είναι πιθανότερο να εκτιμήσουν και να αποδεχθούν μηχανισμούς κρυπτογράφησης ως μέσα ενίσχυσης της ασφάλειας και προστασίας των δεδομένων τους. Αντίθετα, η έλλειψη ενημέρωσης ή κατανόησης οδηγεί σε διστακτικότητα ή αδιαφορία απέναντι σε λύσεις που, αν και τεχνικά αποτελεσματικές, παραμένουν «αόρατες» για τον μέσο χρήστη.

Συνεπώς, η μελέτη της σχέσης μεταξύ επίγνωσης ιδιωτικότητας και αποδοχής κρυπτογραφικών μεθόδων αποκτά ιδιαίτερη σημασία στο πλαίσιο των ηλεκτρονικών υπηρεσιών. Η ανάλυση αυτής της σχέσης συμβάλλει όχι μόνο στην κατανόηση των ψυχοκοινωνικών παραγόντων που επηρεάζουν τη συμπεριφορά των χρηστών, αλλά και στη βελτίωση του σχεδιασμού συστημάτων που επιδιώκουν να συνδυάσουν την ασφάλεια με τη χρηστικότητα και την εμπιστοσύνη.

Ας δούμε αναλυτικότερα ποια μέθοδο ακολουθεί για την έρευνα του:

Η έρευνα σχεδιάστηκε ως ένα διαδικτυακό πείραμα, όπου οι συμμετέχοντες καλούνταν να εγγραφούν σε μια υποτιθέμενη υπηρεσία αξιολόγησης εστιατορίων με το όνομα ("Foodie"). Οι συμμετέχοντες χωρίστηκαν τυχαία σε δύο ομάδες:

- Πειραματική ομάδα (GPet): Χρησιμοποίησε διεπαφή με ενισχυμένα στοιχεία πολιτικής απορρήτου δίπλα σε κάθε πεδίο εισόδου.

- Ομάδα ελέγχου (GNoPet): Χρησιμοποίησε συμβατική διεπαφή με σύνδεσμο προς τη γενική πολιτική απορρήτου.

Μετά την ολοκλήρωση της αλληλεπίδρασης, οι χρήστες απάντησαν σε ερωτηματολόγιο ανάκλησης για να μετρηθεί ο δείκτης επίγνωσης ιδιωτικότητας (Privacy Awareness Index - ax).

Στη συνέχεια λάβαμε κάποια αποτελέσματα: Η μελέτη κατέδειξε σαφώς ότι η ενισχυμένη διεπαφή οδήγησε σε σημαντικά υψηλότερα επίπεδα επίγνωσης πολιτικής ιδιωτικότητας, ανεξαρτήτως του βαθμού προκαταρκτικής ανησυχίας του χρήστη για την ιδιωτικότητα (Privacy Concern Index - px). Ειδικότερα:

- Οι "πραγματιστές" (pragmatists) επωφελήθηκαν περισσότερο από την παρουσία στοχευμένων πληροφοριών.
- Ακόμα και οι "θεμελιωτιστές" (fundamentalists), αν και θεωρούνται ευαισθητοποιημένοι, δεν είχαν πάντα αυξημένη ανάκληση των όρων ιδιωτικότητας.
- Ο γενικός δείκτης ax στην πειραματική ομάδα ήταν σημαντικά υψηλότερος από την ομάδα ελέγχου.

Συμπερασματικά, η έρευνα αποδεικνύει ότι η ενσωμάτωση σαφών, κοντινών και σχετικών πληροφοριών πολιτικής απορρήτου εντός των φορμών συλλογής δεδομένων μπορεί να βελτιώσει ουσιαστικά την επίγνωση ιδιωτικότητας του χρήστη. Επιπλέον, τεκμηριώνει τη διαφορά μεταξύ θεωρητικής ανησυχίας και πραγματικής συμπεριφοράς. Οι χρήστες συχνά δηλώνουν ενδιαφέρον για την προστασία προσωπικών δεδομένων, αλλά σπανίως διαβάζουν ή κατανοούν τις πολιτικές απορρήτου.[27]

3.2 Μελέτες για την επίγνωση Ασφάλειας Πληροφοριών

Η έννοια της Επίγνωσης Ασφάλειας Πληροφοριών (Information Security Awareness – ISA) αποτελεί θεμελιώδη παράγοντα για τη διασφάλιση της προστασίας δεδομένων και την αποτροπή απειλών που προέρχονται όχι μόνο από τεχνολογικούς, αλλά κυρίως από ανθρώπινους παράγοντες. Πολλές μελέτες έχουν εξετάσει τη σημασία της ανθρώπινης συμπεριφοράς στην ασφάλεια πληροφοριών και έχουν αναπτύξει μοντέλα μέτρησης για την αξιολόγηση του επιπέδου επίγνωσης. Στην παρούσα ενότητα, παρουσιάζονται οι κυριότερες μελέτες που αναφέρονται στο άρθρο των Fadhilah et al. (2021), το οποίο εφαρμόζει μια εμπειρική μέτρηση επίγνωσης σε χρήστες ψηφιακών πορτοφολιών στην Ινδονησία.

Ας δούμε το Μοντέλο KAB (Knowledge-Attitude-Behavior), πρόκειται για το πιο διαδεδομένο μοντέλο μέτρησης της επίγνωσης ασφάλειας πληροφοριών είναι το KAB των Kruger και Kearney (2006). Το μοντέλο αυτό βασίζεται σε τρεις βασικές διαστάσεις:

- Γνώση (Knowledge): το τι γνωρίζει ο χρήστης για την ασφάλεια πληροφοριών,
- Στάση (Attitude): το πώς αντιλαμβάνεται και αξιολογεί τους κινδύνους,

- Συμπεριφορά (Behavior): το τι κάνει στην πράξη για να προστατεύσει την πληροφορία.

Το KAB μοντέλο αξιοποιείται ως βασικό εργαλείο αξιολόγησης σε πολλές μελέτες, συμπεριλαμβανομένης της παρούσας από τον Fadhilah et al. (2021), με τη χρήση σταθμισμένων ποσοστών ανά διάσταση (30% για γνώση, 20% για στάση, 50% για συμπεριφορά).

Το συγκεκριμένο μοντέλο χρησιμοποιεί το εργαλείο HAIS-Q (Human Aspects of Information Security Questionnaire), το οποίο αναπτύχθηκε από τους Parsons et al. (2014) και χρησιμοποιείται ευρέως για την αποτίμηση της ανθρώπινης διάστασης της ασφάλειας. Αυτό το εργαλείο περιλαμβάνει επτά (7) περιοχές εστίασης:

- Διαχείριση Κωδικών (Password Management),
- Χρήση Email,
- Χρήση Διαδικτύου,
- Χρήση Κοινωνικών Δικτύων,
- Κινητές Συσκευές,
- Διαχείριση Πληροφοριών,
- Αναφορά Περιστατικών (Incident Reporting).

Το εργαλείο αυτό χρησιμοποιήθηκε από την ερευνητική ομάδα της Fadhilah για την κατασκευή του ερωτηματολογίου που μοιράστηκε σε 156 χρήστες ψηφιακών πορτοφολιών.

Αντίστοιχα η μελέτη των Ögütçü et al. (2016) υπογραμμίζει ότι η ασφάλεια δεν είναι αποκλειστικά τεχνολογικό ζήτημα, αλλά επηρεάζεται άμεσα από τις στάσεις και τη συμπεριφορά των χρηστών. Αυτή η οπτική ενισχύει τη σημασία των προγραμμάτων ενημέρωσης και ευαισθητοποίησης για την αλλαγή της συμπεριφοράς.

Τέλος οι Bauer et al. (2017) αναφέρουν ότι η πρόληψη μέσω κατάλληλης εκπαίδευσης και καμπανιών ευαισθητοποίησης είναι πιο αποτελεσματική από την αντιμετώπιση παραβιάσεων μετά την εμφάνισή τους.

Συμπερασματικά, η μελέτη της Fadhilah καταλήγει στο συμπέρασμα ότι η συνολική επίγνωση των χρηστών ψηφιακών πορτοφολιών είναι ικανοποιητική (80.78%), αλλά υπάρχουν επιμέρους περιοχές (όπως η χρήση κοινωνικών δικτύων και το χειρισμό πληροφοριών) όπου απαιτείται ενίσχυση της ενημέρωσης και αλλαγή συμπεριφοράς. Προτείνονται συγκεκριμένες ενέργειες από παρόχους υπηρεσιών, όπως:

- εκπαίδευση σχετικά με την προστασία αριθμών τηλεφώνου και κωδικών,
- αποτροπή χρήσης ανασφαλών VPN,
- ενίσχυση της εμπιστοσύνης στους επίσημους διαύλους επικοινωνίας.[23][24][25][26]

3.3 Σύγκριση μεθοδολογιών

Η μελέτη της επίγνωσης ασφάλειας πληροφοριών και ιδιωτικότητας αποτελεί κρίσιμο πεδίο τόσο στην επιστημονική έρευνα όσο και στη διαμόρφωση πολιτικών προστασίας των χρηστών. Στην παρούσα ενότητα παρουσιάζεται συγκριτική ανάλυση δύο χαρακτηριστικών ερευνών που επικεντρώνονται στη μέτρηση της επίγνωσης σε διαφορετικά περιβάλλοντα: (α) τη μελέτη των Fadhilah et al. (2021) σχετικά με την επίγνωση ασφάλειας πληροφοριών (Information Security Awareness – ISA) σε χρήστες ψηφιακών πορτοφολιών και (β) τη μελέτη του Bergmann (2009) για την επίγνωση ιδιωτικότητας (Privacy Awareness) στο πλαίσιο χρήσης διαδικτυακών υπηρεσιών.

- Ερευνητικά Πλαίσια

Η μελέτη των Fadhilah et al. στοχεύει στη μέτρηση του επιπέδου επίγνωσης ασφάλειας πληροφοριών σε πραγματικούς χρήστες ψηφιακών πορτοφολιών στην Ινδονησία. Αντίθετα, ο Bergmann διερευνά πειραματικά την αντίληψη των χρηστών γύρω από τις πολιτικές απορρήτου, αξιολογώντας την ικανότητα ανάκλησης βασικών πληροφοριών, στο πλαίσιο ενός προσομοιωμένου περιβάλλοντος («Foodie»).

- Μεθοδολογικά μοντέλα

Οι δύο μελέτες βασίζονται σε διαφορετικές θεωρητικές προσεγγίσεις:

- ❖ Fadhilah et al. εφαρμόζουν το μοντέλο KAB (Knowledge – Attitude – Behavior), που εισήγαγαν οι Kruger & Kearney, σε συνδυασμό με το εργαλείο HAIS-Q (Human Aspects of Information Security Questionnaire).
- ❖ Bergmann υιοθετεί ταξινόμηση τύπου Westin (Fundamentalists, Pragmatists, Unconcerned) και κατασκευάζει δείκτες επίγνωσης (Privacy Awareness Index – ax και Privacy Concerns Index – px) με βάση τις απαντήσεις σε pre/post ερωτηματολόγια.

- Μέθοδος Συλλογής Δεδομένων

Στη μελέτη Fadhilah, χρησιμοποιήθηκε ερωτηματολόγιο 55 ερωτήσεων, δομημένο με κλίμακα Likert, και εφαρμόστηκε η μέθοδος AHP (Analytic Hierarchy Process) για την εκτίμηση των βαρών των διαστάσεων. Αντίθετα στη μελέτη Bergmann, χρησιμοποιήθηκε ένα πειραματικό περιβάλλον με 156 συμμετέχοντες που χωρίστηκαν τυχαία σε ομάδα ελέγχου (GNoPet) και πειραματική ομάδα (GPet). Οι συμμετέχοντες αλληλεπίδρασαν με διαφορετικές διεπαφές και στη συνέχεια απάντησαν σε ερωτήσεις κατανόησης των πολιτικών απορρήτου.

- Ανάλυση και Δείκτες

Η μελέτη Fadhilah υπολογίζει ποσοστά επίγνωσης ανά διάσταση και τομέα, με τελική συνολική βαθμολογία 80.78%, που χαρακτηρίζεται ως «καλή». Οι ελλείψεις εντοπίζονται στην ασφαλή χρήση κοινωνικών δικτύων και στη διαχείριση πληροφοριών. Από την άλλη ο Bergmann μετρά την ικανότητα των χρηστών να ανακαλούν σημαντικά σημεία της πολιτικής απορρήτου. Τα αποτελέσματα δείχνουν ότι η πειραματική διεπαφή αυξάνει σημαντικά τον δείκτη επίγνωσης (ax), ιδίως για τους «pragmatists» και «unconcerned» χρήστες.

Ολοκληρώνοντας διαπιστώνουμε ότι η μελέτη των Fadhilah προσφέρει μια στατιστικά τεκμηριωμένη εικόνα για την επίγνωση ασφάλειας χρηστών, ενώ η μελέτη του Bergmann αναδεικνύει την επίδραση του σχεδιασμού διεπαφών στην ενεργή κατανόηση της ιδιωτικότητας. Η συνδυαστική αξιοποίηση των δύο προσεγγίσεων μπορεί να προσφέρει πιο ολοκληρωμένα εργαλεία μέτρησης για τη σύγχρονη ψηφιακή ασφάλεια.[27][28][29][30]

3.4 Συμπεράσματα από τη Βιβλιογραφική Ανασκόπηση

Η βιβλιογραφική ανασκόπηση αναδεικνύει ότι η επίγνωση ασφάλειας πληροφοριών και ιδιωτικότητας αποτελεί πολυδιάστατη έννοια, η οποία εξελίχθηκε από θεωρητικό πλαίσιο σε πεδίο εμπειρικής και τεχνολογικής εφαρμογής. Η πορεία αυτή αντανακλά τη μετατόπιση του ενδιαφέροντος από το «δικαίωμα στην ιδιωτικότητα» ως νομική αρχή, προς την ενεργητική συμμετοχή του χρήστη στη διαχείριση των προσωπικών του δεδομένων (Westin, 1967, 2003).

Η θεμελιώδης συμβολή του Alan Westin υπήρξε καθοριστική, καθώς προσδιόρισε την ιδιωτικότητα ως μορφή πληροφοριακού ελέγχου και εισήγαγε την ταξινόμηση των χρηστών σε fundamentalists, pragmatists και unconcerned (Westin, 1967). Το έργο του αποτέλεσε τη βάση για τη διαμόρφωση των πρώτων θεωρητικών μοντέλων μέτρησης της privacy concern και επηρέασε μεταγενέστερες εμπειρικές μελέτες, όπως του Bergmann (2009), όπου η επίγνωση ιδιωτικότητας αντιμετωπίζεται ως μετρήσιμο γνωστικό και συμπεριφορικό φαινόμενο.

Κατά τη δεκαετία του 1990 και 2000, η Lorrie Faith Cranor προώθησε την έννοια της χρηστικής ιδιωτικότητας (usable privacy), υποστηρίζοντας ότι η πληροφόρηση δεν επαρκεί και ότι οι χρήστες χρειάζονται οπτικά και διαδραστικά εργαλεία για να κατανοούν τις συνέπειες των επιλογών τους (Cranor, 2005, 2006). Η ίδια ηγήθηκε του έργου P3P (Platform for Privacy Preferences Project), το οποίο επέτρεπε την αυτόματη ανάγνωση πολιτικών απορρήτου από φυλλομετρητές (Cranor & Reagle, 2002), και δημιούργησε το εργαλείο Privacy Birds, που χρησιμοποιούσε γραφικά σύμβολα για να υποδείξει εάν ένας ιστότοπος ήταν συμβατός με τις προτιμήσεις ιδιωτικότητας του χρήστη (Reagle & Cranor, 2002).

Στην Ευρώπη, το ερευνητικό πρόγραμμα PRIME (Privacy and Identity Management for Europe) (Fischer-Hübner et al., 2011) ανέπτυξε την έννοια της χρήστη-κεντρικής διαχείρισης ταυτότητας και εισήγαγε privacy dashboards και contextual indicators, προτείνοντας μια πρακτική προσέγγιση για τη διαφάνεια στη συλλογή δεδομένων. Το

PRIME συνέβαλε στην εξέλιξη του πεδίου Privacy and Identity Management (PIM) και αποτέλεσε πρόδρομο για τις σύγχρονες πολιτικές του GDPR (Hildebrandt & Gutwirth, 2008).

Κατά τη δεκαετία του 2010, η έρευνα στράφηκε προς την ανάπτυξη visual privacy indicators και privacy nudges, οι οποίοι προσφέρουν στους χρήστες οπτική ανατροφοδότηση σχετικά με την πρόσβαση σε δεδομένα, συμβάλλοντας στην ενεργή και στιγμιαία επίγνωση των κινδύνων (Cranor, 2008; Kelley et al., 2010; Anderson & Egelman, 2016). Οι δείκτες αυτοί, όπως τα εικονίδια ειδοποίησης σε εφαρμογές ή τα «privacy nutrition labels», ενσωματώνουν τη διάσταση της συμπεριφορικής ιδιωτικότητας και συνδέουν τη γνώση με την πραγματική δράση του χρήστη.

Παράλληλα, οι μελέτες των Fadhilah et al. (2021) και Bergmann (2009) προσέφεραν διαφορετικά μεθοδολογικά μοντέλα για τη μέτρηση της επίγνωσης. Η ανάλυση των δύο μελετών που εξετάζουν την επίγνωση σε θέματα ιδιωτικότητας και ασφάλειας πληροφοριών καταδεικνύει τον κρίσιμο ρόλο της ενημέρωσης, της διεπαφής χρήστη και της ανθρώπινης συμπεριφοράς στη διαμόρφωση της αντίληψης και της στάσης απέναντι στην προστασία προσωπικών δεδομένων.

Η μελέτη του Bergmann (2009) επικεντρώνεται στην επίγνωση ιδιωτικότητας (privacy awareness) κατά τη χρήση διαδικτυακών υπηρεσιών και αποκαλύπτει ότι η παραδοσιακή μορφή παρουσίασης των πολιτικών απορρήτου είναι ανεπαρκής, καθώς οι περισσότεροι χρήστες τις αγνοούν ή δεν τις κατανοούν. Μέσω ενός ελεγχόμενου πειράματος, διαπιστώνεται ότι η ενσωμάτωση βασικών πληροφοριών απορρήτου δίπλα στα πεδία εισαγωγής δεδομένων βελτιώνει σημαντικά την κατανόηση και την ανάκληση βασικών όρων από τους χρήστες, ιδιαίτερα στους «πραγματιστές» και «αδιάφορους», σύμφωνα με την ταξινόμηση Westin. Το βασικό συμπέρασμα είναι ότι η σαφής, στοχευμένη και εντοπισμένη παρουσίαση των πολιτικών απορρήτου ενισχύει την επίγνωση των χρηστών και προωθεί την έννοια της ενημερωμένης συγκατάθεσης.

Αντίστοιχα, η μελέτη των Fadhilah et al. (2021) αξιολογεί την επίγνωση ασφάλειας πληροφοριών (information security awareness) στους χρήστες ψηφιακών πορτοφολιών στην Ινδονησία, με βάση το μοντέλο Knowledge-Attitude-Behavior (KAB) και μεθοδολογία Analytic Hierarchy Process (AHP). Τα αποτελέσματα δείχνουν ότι η συνολική επίγνωση βρίσκεται σε ικανοποιητικό επίπεδο (80.78%), ωστόσο εντοπίζονται αδυναμίες σε κρίσιμες περιοχές, όπως η χρήση κοινωνικών δικτύων, η χρήση του Διαδικτύου και η διαχείριση πληροφοριών. Παρατηρείται ελλιπής κατανόηση απειλών όπως οι ψεύτικες εφαρμογές, τα παραπλανητικά email και η αποθήκευση κωδικών ή PIN χωρίς προστασία. Η μελέτη προτείνει στοχευμένες εκπαιδευτικές παρεμβάσεις από τους παρόχους, ώστε να ενισχυθεί η προστασία των χρηστών από ηλεκτρονικές απάτες και παραβιάσεις.

Συνολικά, η βιβλιογραφία δείχνει ότι η επίγνωση ιδιωτικότητας και ασφάλειας πληροφοριών πρέπει να αντιμετωπίζεται ολιστικά – ως συνδυασμός γνώσης, στάσης και συμπεριφοράς (όπως προτείνει το KAB), αλλά και ως εμπειρία αλληλεπίδρασης που διαμορφώνεται από τον σχεδιασμό των συστημάτων. Η ενσωμάτωση εργαλείων οπτικής ανατροφοδότησης, εκπαίδευσης χρηστών και προσαρμοσμένων διεπαφών αποτελεί βασικό μοχλό ενίσχυσης της πραγματικής επίγνωσης και υπεύθυνης ψηφιακής συμπεριφοράς. [27][28]

4 ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

4.1 Σχεδιασμός Πειράματος Ερωτηματολογίου

Η ταχύτατη ανάπτυξη των ηλεκτρονικών υπηρεσιών έχει αυξήσει την ανάγκη για ασφαλείς και αξιόπιστες λύσεις προστασίας δεδομένων. Οι κρυπτογραφικές μέθοδοι, ως βασικό εργαλείο για την ασφάλεια των συστημάτων, διαδραματίζουν κεντρικό ρόλο. Παρόλο που η τεχνολογία αυτή θεωρείται κρίσιμη, η αποδοχή της από τους χρήστες μπορεί να επηρεαστεί από παράγοντες όπως η εμπιστοσύνη, η κατανόηση και η εμπειρία.

Σκοπός της Μελέτης:

Σύμφωνα με το επιστημονικό άρθρο «Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)» (Parsons et al., 2014), όπου η μελέτη στόχευε στο: να παρουσιάσει την ανάπτυξη και επικύρωση του Human Aspects of Information Security Questionnaire (HAIS-Q) καθώς επίσης και να διερευνήσει τη σχέση ανάμεσα στη γνώση, τη στάση και τη συμπεριφορά των εργαζομένων σχετικά με την ασφάλεια πληροφοριών (Knowledge–Attitude–Behaviour model – KAB), στη δική μας έρευνα σκοπός είναι να διερευνηθεί η αποδοχή των κρυπτογραφικών μεθόδων από τους χρήστες σύγχρονων ηλεκτρονικών υπηρεσιών, με έμφαση σε παραμέτρους όπως η εμπιστοσύνη, η αντιληπτή ασφάλεια και η ευχρηστία. Πέραν του ερευνητικού δείγματος της έρευνας, ακολουθεί ανάλυση των ερωτήσεων του ερωτηματολογίου της έρευνας, καθώς και η μεθοδολογία της στατιστικής ανάλυσης των δεδομένων.

Ερωτήματα Έρευνας:

- Ποιο είναι το επίπεδο κατανόησης των κρυπτογραφικών μεθόδων από τους χρήστες;
- Ποιοι παράγοντες επηρεάζουν την αποδοχή αυτών των τεχνολογιών;

- Πώς η εμπειρία με ηλεκτρονικές υπηρεσίες σχετίζεται με την εμπιστοσύνη στις κρυπτογραφικές λύσεις;

Μεθοδολογία

Στο πλαίσιο της παρούσας μελέτης, η Αναλυτική Ιεραρχική Μέθοδος (AHP) χρησιμοποιήθηκε για τη στάθμιση των παραγόντων που επηρεάζουν την αποδοχή και εμπιστοσύνη των χρηστών στις κρυπτογραφικές μεθόδους που εφαρμόζονται στις σύγχρονες ηλεκτρονικές υπηρεσίες.

Ως κύρια κριτήρια (ανώτερο επίπεδο της ιεραρχίας) υιοθετήθηκαν τρεις βασικές διαστάσεις, εμπνευσμένες από το μοντέλο KAB (Knowledge–Attitude–Behaviour):

- Γνώση (Knowledge): το επίπεδο ενημέρωσης και κατανόησης του χρήστη σχετικά με τις αρχές και λειτουργίες της κρυπτογράφησης,
- Στάση (Attitude): η αντίληψη, η εμπιστοσύνη και η πρόθεση του χρήστη να χρησιμοποιεί υπηρεσίες που εφαρμόζουν κρυπτογραφικές μεθόδους,
- Συμπεριφορά (Behaviour): ο βαθμός στον οποίο ο χρήστης εφαρμόζει στην πράξη ασφαλείς πρακτικές, όπως χρήση ισχυρών κωδικών ή ενεργοποίηση πιστοποίησης δύο παραγόντων.

Ως υποκριτήρια (focus areas) καθορίστηκαν επιμέρους πτυχές που σχετίζονται με την ασφάλεια και τη χρήση ηλεκτρονικών υπηρεσιών, όπως:

- Διαχείριση κωδικών πρόσβασης,
- Χρήση πρωτοκόλλων ασφαλούς επικοινωνίας (SSL/TLS),
- Διαχείριση προσωπικών δεδομένων,
- Αντίληψη για την ασφάλεια ηλεκτρονικών συναλλαγών,
- Εμπιστοσύνη σε παρόχους ηλεκτρονικών υπηρεσιών,
- Εφαρμογή πρακτικών προστασίας ιδιωτικότητας,
- Ανταπόκριση σε περιστατικά παραβίασης ή υποκλοπής.

Για τον καθορισμό των βαρών των κύριων κριτηρίων, εφαρμόστηκε η μέθοδος ζευγαρωτών συγκρίσεων (pairwise comparisons) της AHP, ενώ οι αρχικές αναλογίες βασίστηκαν στη λογική του μοντέλου KAB, δηλαδή:

- Γνώση (Knowledge): 30%,
- Στάση (Attitude): 20%,
- Συμπεριφορά (Behaviour): 50%.

Τα βάρη των υποκριτηρίων προσδιορίστηκαν μέσω αξιολόγησης από ειδικούς στον τομέα της κυβερνοασφάλειας και της κρυπτογραφίας, ώστε να αντικατοπτρίζουν τη σχετική σημασία κάθε παράγοντα στην αποδοχή και χρήση ασφαλών κρυπτογραφικών μεθόδων. Τα τελικά βάρη ενσωματώθηκαν στο μοντέλο υπολογισμού του σταθμισμένου δείκτη αποδοχής, εξασφαλίζοντας αντικειμενικότητα και μεθοδολογική συνέπεια. Σε αυτή τη μελέτη συλλέχθηκαν δεδομένα από 50 χρήστες μέσω ερωτηματολογίου και προσπάθησα να

καλύψω κάποιες διαστάσεις και θεματικούς τομείς. Τα αποτελέσματα έδειξαν ότι το επίπεδο επίγνωσης είναι σχετικά καλό, με περιθώρια βελτίωσης σε τομείς όπως τα κοινωνικά δίκτυα, το email και τον χειρισμό πληροφοριών. Προτάθηκαν κάποια μέτρα προστασίας για περαιτέρω εμπιστοσύνη για την ενίσχυση ψηφιακής προστασίας των χρηστών.

Η Αναλυτική Ιεραρχική Μέθοδο (AHP) όπως αναφέραμε που χρησιμοποιήθηκε και στη μελέτη του Fadhilah, έχει μια ιεραρχική δομή που ήταν ένα από τα στάδια σε αυτή τη μέθοδο. Η κορυφαία ιεραρχική δομή είναι ο σκοπός των αποφάσεων που λαμβάνονται, μετά το επόμενο επίπεδο είναι τα κριτήρια και το χαμηλότερο επίπεδο είναι η εναλλακτική.

Επίσης η ποιότητα των δεδομένων από τους ερωτηθέντες έχει προτεραιότητα έναντι των ποσοτικών δεδομένων κατά την εφαρμογή της μεθόδου AHP. Το μέγεθος του δείγματος στη μέθοδο AHP δεν έχει συγκεκριμένο τύπο ή πρότυπο, υπάρχει γενική συναίνεση ότι το AHP δεν απαιτεί πολύ μεγάλο δείγμα.

Το πρώτο πράγμα που έγινε ήταν να προσδιοριστεί το πρόβλημα που ερευνήθηκε και στη συνέχεια να γίνει μελέτη αυτού, να δημιουργηθεί το ερωτηματολόγιο, να αξιολογηθεί και να διανεμηθεί ώστε να αντληθούν τα αποτελέσματα.

4.2 Δημογραφικά Χαρακτηριστικά Δείγματος

Στην παρούσα ενότητα περιγράφονται τα βασικά δημογραφικά χαρακτηριστικά του δείγματος που συμμετείχε στην έρευνα της πτυχιακής εργασίας με τίτλο «Στατιστική μελέτη για την αποδοχή κρυπτογραφικών μεθόδων στις σύγχρονες ηλεκτρονικές υπηρεσίες». Σκοπός είναι να δοθεί σαφής εικόνα της σύνθεσης του δείγματος ώστε να αξιολογηθεί η εξωτερική εγκυρότητα και να διευκολυνθούν οι συγκρίσεις μεταξύ υποομάδων.

Το δείγμα συγκεντρώθηκε μέσω ηλεκτρονικού ερωτηματολογίου. Στις οδηγίες προς τους συμμετέχοντες αναφερόταν ότι η συμμετοχή είναι ανώνυμη και προαιρετική και ότι τα δεδομένα θα χρησιμοποιηθούν αποκλειστικά για ερευνητικούς σκοπούς. Το τελικό μέγεθος του δείγματος ήταν n = [50 άτομα] (έγκυρα/πλήρη συμπληρωμένα ερωτηματολόγια).

Κάποια από τα δημογραφικά πεδία που περιλαμβάνονται στην μελέτη είναι:

- Ηλικία (κατηγοριοποιημένη σε: 18–24, 25–44, 45+)
- Φύλο (Άνδρας / Γυναίκα / Άλλο / Προτιμώ να μην απαντήσω)
- Επίπεδο εκπαίδευσης (Δευτεροβάθμια / Μεταδευτεροβάθμια / Πτυχίο / Μεταπτυχιακό ή Διδακτορικό)
- Επάγγελμα / Τομέας απασχόλησης (π.χ. Ιδιωτικός, Δημόσιος, Εκπαίδευση, Πληροφορική, Οικονομία/Τραπεζικός)
- Χρήση συγκεκριμένων ηλεκτρονικών υπηρεσιών

4.3 Εργαλεία Ανάλυσης

Στη προκειμένη φάση θα γίνει ανάλυση των εργαλείων που θα χρησιμοποιηθούν στην έρευνα μας αλλά πρώτα θα δούμε κάποια θεωρητικά στοιχεία. Όπως έχουμε αναφέρει και γνωρίζουμε οι απειλές ασφαλείας προέρχονται κυρίως από ανθρώπινες συμπεριφορές (π.χ. λάθη, απροσεξία, αδιαφορία). Προ υπάρχουσες έρευνες εστίαζαν κυρίως σε τεχνικές λύσεις ή μεμονωμένες πτυχές (π.χ. χρήση κωδικών, phishing).

Σκοπός του ερωτηματολογίου είναι η αξιολόγηση του επιπέδου ενημερότητας ασφάλειας πληροφοριών των εργαζομένων, μέσα από τρεις διαστάσεις:

- τη Γνώση των πολιτικών ασφάλειας,
- τη Στάση απέναντι σε αυτές,
- και τη Συμπεριφορά τους κατά τη χρήση υπολογιστή.

Δηλαδή, η αύξηση γνώσης πολιτικών ασφαλείας οδηγεί σε θετικότερη στάση και, τελικά, σε ασφαλέστερη συμπεριφορά. Η διανομή του ερωτηματολογίου πραγματοποιήθηκε ηλεκτρονικά μέσω email και κοινωνικών δικτύων, εξασφαλίζοντας ανωνυμία, και το οποίο θεωρείται σημαντικό για μεγαλύτερη αξιοπιστία στα αποτελέσματα.

Το HAIS-Q αποτελείται από 31 προτάσεις, κατανεμημένες σε 7 θεματικούς τομείς καθώς και κάποιες αρχικές δημογραφικές ερωτήσεις, άρα συνολικά 35. Κάθε τομέας περιλαμβάνει δηλώσεις που αξιολογούν γνώση, στάση και συμπεριφορά μέσω πενταβάθμιας κλίμακας Likert (1 = Διαφωνώ απόλυτα, 5 = Συμφωνώ απόλυτα).

Στη συνέχεια παρουσιάζουμε το ερωτηματολόγιο.

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Μέρος Α: Δημογραφικά Στοιχεία

1. **Φύλο:**
   - Άνδρας
   - Γυναίκα
   - Άλλο / Δε θέλω να απαντήσω
2. **Ηλικία: _____ ετών**
3. **Εκπαιδευτικό επίπεδο:**
   - Δευτεροβάθμια
   - Ανώτερη
   - Ανώτατη
   - Μεταπτυχιακή / Διδακτορική
4. **Επαγγελματικός τομέας:**
   - Δημόσιος
   - Ιδιωτικός
   - Εκπαίδευση

- Πληροφορική
- Οικονομία / Τραπεζικός
- Άλλος

Μέρος Β: Αντίληψη και Συμπεριφορά σχετικά με την Κρυπτογράφηση

Για κάθε δήλωση, επιλέξτε τον βαθμό συμφωνίας σας (1–5): 1 = Διαφωνώ απόλυτα | 2 = Διαφωνώ | 3 = Ούτε συμφωνώ / Ούτε διαφωνώ | 4 = Συμφωνώ | 5 = Συμφωνώ απόλυτα

1. Γνωρίζω τι σημαίνει ο όρος “κρυπτογράφηση δεδομένων”.
2. Γνωρίζω ότι η κρυπτογράφηση προστατεύει τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση.
3. Αν μια εφαρμογή δεν χρησιμοποιεί κρυπτογράφηση, τα δεδομένα μου μπορούν να υποκλαπούν.
4. Πιστεύω ότι η κρυπτογράφηση είναι απαραίτητη για την προστασία της ιδιωτικότητάς μου.
5. Η χρήση ισχυρής κρυπτογράφησης με κάνει να εμπιστεύομαι περισσότερο μια υπηρεσία.
6. Η πολυπλοκότητα των διαδικασιών ασφαλείας με αποτρέπει από τη χρήση ορισμένων υπηρεσιών.
7. Ελέγχω αν οι ιστοσελίδες που χρησιμοποιώ έχουν ασφαλή σύνδεση (HTTPS).
8. Αποφεύγω να εισάγω προσωπικά δεδομένα σε ιστότοπους χωρίς το εικονίδιο “κλειδώματος”.
9. Χρησιμοποιώ ισχυρούς κωδικούς πρόσβασης και δεν τους κοινοποιώ.
10. Μεριμνούσα τακτικά για το αν οι εφαρμογές στο κινητό μου τηλέφωνο είναι ενημερωμένες στις τελευταίες εκδόσεις ασφαλείας.
11. Χρησιμοποιώ συχνά υπηρεσίες που βασίζονται σε κρυπτογραφημένες επικοινωνίες (π.χ. e-banking, gov.gr).
12. Χρησιμοποιώ εφαρμογές με ισχυρή κρυπτογράφηση λόγω επαγγελματικών αναγκών.
13. Οι ηλεκτρονικές υπηρεσίες που χρησιμοποιώ ενημερώνουν επαρκώς για τα μέτρα ασφάλειας που εφαρμόζουν.
14. Η χρήση κρυπτογραφίας αυξάνει το αίσθημα ασφάλειας των χρηστών.
15. Η ενημέρωση των πολιτών για την κρυπτογράφηση θα ενίσχυε την εμπιστοσύνη τους στις ψηφιακές υπηρεσίες.
16. Η πολυπλοκότητα των τεχνολογιών κρυπτογράφησης μειώνει τη διάθεση των χρηστών να τις χρησιμοποιήσουν.
17. Προτιμώ να χρησιμοποιώ ηλεκτρονικές υπηρεσίες που δηλώνουν ρητά ότι χρησιμοποιούν κρυπτογράφηση.
18. Είμαι πρόθυμος/η να μάθω περισσότερα για το πώς λειτουργεί η κρυπτογράφηση.
19. Θα συνέστηνα σε άλλους τη χρήση υπηρεσιών που προστατεύουν τα δεδομένα τους με κρυπτογραφία.
20. Η ανάπτυξη και εφαρμογή νέων κρυπτογραφικών μεθόδων είναι ζωτικής σημασίας για την ασφάλεια των πολιτών.

21. Πιστεύω ότι στο μέλλον οι περισσότερες υπηρεσίες θα χρησιμοποιούν υποχρεωτικά κρυπτογράφηση.
22. Η ασφάλεια των ηλεκτρονικών υπηρεσιών θα πρέπει να αποτελεί βασικό κριτήριο επιλογής για τους πολίτες.
23. Η κρυπτογράφηση κάνει τις ηλεκτρονικές υπηρεσίες πιο αργές και δυσκολότερες στη χρήση χωρίς ουσιαστικό όφελος.

Μέρος Γ: Ψηφιακά Πορτοφόλια & Ε-πληρωμές

Για κάθε δήλωση, επιλέξτε τον βαθμό (Συχνότητα: Ποτέ / Σπάνια / Μηνιαία / Εβδομαδιαία / Καθημερινά)

1. Χρησιμοποιώ τακτικά εφαρμογές ψηφιακών πορτοφολιών ή e-banking (π.χ., Revolut, PayPal, εφαρμογές τραπεζών).
2. Όταν χρησιμοποιώ ένα ψηφιακό πορτοφόλι, εμπιστεύομαι ότι οι συναλλαγές μου είναι ασφαλείς χάρη στην κρυπτογράφηση.
3. Ανησυχώ ότι τα ψηφιακά μου πορτοφόλια μπορεί να παραβιαστούν από hackers.
4. Θα προτιμούσα να πληρώνω μετρητά παρά να χρησιμοποιώ ψηφιακό πορτοφόλι, λόγω ανησυχιών ασφαλείας. (Ανάστροφη)

Μέρος Δ: Πρακτικές & Ανησυχίες Ιδιωτικότητας

Να καταγράψει πώς διαχειρίζεται ο χρήστης τα προσωπικά του δεδομένα πέρα από την κρυπτογράφηση.

1. Διαβάζω ή σκανάρω τις Πολιτικές Απορρήτου μιας εφαρμογής πριν από την εγκατάστασή της.
2. Ανησυχώ για το πόσα προσωπικά μου δεδομένα συλλέγουν οι εφαρμογές και οι ιστότοποι που χρησιμοποιώ.
3. Έχω εγκαταστήσει ή χρησιμοποιήσει ποτέ εφαρμογή VPN για να προστατεύσω την ιδιωτικότητά μου στο διαδίκτυο.
4. Πιστεύω ότι είναι αναπόφευκτο να θυσιάσουμε λίγη ιδιωτικότητα για την άνεση που μας προσφέρουν οι ψηφιακές υπηρεσίες. (Ανάστροφη)

Οι ερωτήσεις 1-3 αφορούν τη Γνώση, οι 4-6 την Αντίληψη, οι 7-10 τη Συμπεριφορά, οι 10-12 την εμπειρία και συχνότητα χρήσης των κρυπτογραφημένων υπηρεσιών, οι 13-15 την αντίληψη ωφελειών και εμπόδια υιοθέτησης, οι 16-18 τη πρόθεση χρήσης και αποδοχή κρυπτογραφικών μεθόδων και οι 19-23 μια γενική στάση προς τις κρυπτογραφικές μεθόδους.

Το ερωτηματολόγιο στοχεύει στη μέτρηση του επιπέδου ενημερότητας, στάσης, συμπεριφοράς και αποδοχής των χρηστών απέναντι στις κρυπτογραφικές μεθόδους που

εφαρμόζονται στις σύγχρονες ηλεκτρονικές υπηρεσίες, με βάση το θεωρητικό πλαίσιο του μοντέλου KAB και τη δομή του HAIS-Q.

4.4 Ενδεικτικές Μεταβλητές

Στο πλαίσιο της παρούσας στατιστικής μελέτης, οι μεταβλητές που εξετάζονται βασίζονται στο θεωρητικό μοντέλο KAB (Knowledge–Attitude–Behaviour) και στη μεθοδολογική προσέγγιση του HAIS-Q (Human Aspects of Information Security Questionnaire), προσαρμοσμένα στο πεδίο της αποδοχής κρυπτογραφικών μεθόδων στις σύγχρονες ηλεκτρονικές υπηρεσίες. Οι μεταβλητές διακρίνονται σε δύο κύριες κατηγορίες: δημογραφικές και ερευνητικές. Οι δημογραφικές μεταβλητές, όπως το φύλο, η ηλικία, το επίπεδο εκπαίδευσης και ο επαγγελματικός τομέας λειτουργούν ως ανεξάρτητες ή ελεγκτικές μεταβλητές, επιτρέποντας τη σύγκριση διαφορών μεταξύ ομάδων συμμετεχόντων. Οι κύριες ερευνητικές μεταβλητές προκύπτουν από τις διαστάσεις του μοντέλου KAB και αφορούν τη Γνώση (Knowledge), τη Στάση (Attitude) και τη Συμπεριφορά (Behaviour) των χρηστών απέναντι στην κρυπτογράφηση, την εμπειρία και συχνότητα χρήσης των κρυπτογραφημένων υπηρεσιών, την αντίληψη ωφελειών και εμπόδια υιοθέτησης, την Πρόθεση Αποδοχής (Intention to Use) των κρυπτογραφικών μεθόδων στις ηλεκτρονικές υπηρεσίες καθώς και τη γενική στάση απέναντι στις κρυπτογραφικές μεθόδους. Οι μεταβλητές αυτές αποτυπώνονται μέσω ερωτήσεων κλίμακας Likert και επιτρέπουν την ποσοτική αποτίμηση της ενημερότητας και εμπιστοσύνης των χρηστών. Από τις απαντήσεις υπολογίζονται σύνθετοι δείκτες, όπως ο Knowledge Index, ο Attitude Index, ο Behaviour Index, ο Acceptance Index και ο συνολικός Security Awareness Index, οι οποίοι χρησιμοποιούνται για την εξαγωγή στατιστικών συμπερασμάτων σχετικά με το επίπεδο γνώσης, τη στάση, τη συμπεριφορά και την πρόθεση των χρηστών να αποδεχθούν και να εμπιστευθούν τις κρυπτογραφικές μεθόδους που ενσωματώνονται στις σύγχρονες ηλεκτρονικές υπηρεσίες.

5 ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

5.1 Στατιστική Ανάλυση Ερωτηματολογίων

Στο παρόν κεφάλαιο παρουσιάζονται αναλυτικά τα αποτελέσματα της εμπειρικής έρευνας που πραγματοποιήθηκε με τη χρήση του ερωτηματολογίου αξιολόγησης της γνώσης, στάσης και συμπεριφοράς των χρηστών απέναντι στην κρυπτογράφηση και τις ασφαλείς ψηφιακές υπηρεσίες.

Για την επεξεργασία και ανάλυση των πρωτογενών στοιχειών που προήλθαν από τις απαντήσεις του ερωτηματολογίου, χρησιμοποιήθηκε το στατιστικό πακέτο ανάλυσης δεδομένων SPSS 17, το οποίο ήταν πολύ σημαντικό στην επεξεργασία των δεδομένων και στη συνέχεια στην ερμηνεία τους. Πιο συγκεκριμένα μετά τη δημιουργία του ερωτηματολογίου και την προώθηση του ηλεκτρονικά μέσω του Google Forms, οι απαντήσεις καταγράφηκαν σε μορφή excel και στη συνέχεια τα στοιχεία μετατράπηκαν σε αριθμούς, βγήκε η μέση τιμή των ερωτήσεων ώστε να μπορούν να γίνουν οι απαραίτητες διεργασίες σε επόμενο στάδιο.

Το ερωτηματολόγιο βασίστηκε στο θεωρητικό υπόδειγμα HAIS-Q (Human Aspects of Information Security Questionnaire) των Parsons et al. (2014) και προσαρμόστηκε στο πλαίσιο της παρούσας μελέτης, ώστε να αποτυπώνει το επίπεδο επίγνωσης ασφάλειας (security awareness) των χρηστών σε σχέση με την αποδοχή κρυπτογραφικών μεθόδων σε ηλεκτρονικές συναλλαγές, e-banking και ψηφιακά πορτοφόλια.

Η στατιστική ανάλυση των δεδομένων πραγματοποιήθηκε σε τέσσερα βασικά στάδια

1. Περιγραφική ανάλυση των απαντήσεων ανά θεματική ενότητα (Knowledge, Attitude, Behaviour).
2. Έλεγχος αξιοπιστίας του ερωτηματολογίου με χρήση του συντελεστή Cronbach’s α.

3. Υπολογισμός ειδικών δεικτών (Knowledge Index, Attitude Index, Behaviour Index, Overall Awareness Index) για την ποσοτική αποτίμηση των αποτελεσμάτων.
4. Συγκριτική αποτίμηση των ευρημάτων με διεθνείς ερευνητικές εργασίες, προκειμένου να αξιολογηθεί η εγκυρότητα του εργαλείου και η συνάφεια των αποτελεσμάτων.

Η στατιστική ανάλυση ενός τέτοιου ερωτηματολογίου που βασίζεται στο μοντέλο KAB (Knowledge–Attitude–Behaviour) και στη δομή του HAIS-Q πραγματοποιείται με στόχο την ποσοτική αποτίμηση των παραγόντων που επηρεάζουν την αποδοχή κρυπτογραφικών μεθόδων στις σύγχρονες ηλεκτρονικές υπηρεσίες. Η ανάλυση ακολουθεί διαδοχικά στάδια, τα οποία καλύπτουν τόσο την περιγραφική όσο και την επαγωγική στατιστική.

Αρχικά, όπως αναφέραμε εφαρμόζεται περιγραφική στατιστική για τη συνοπτική παρουσίαση των δημογραφικών χαρακτηριστικών του δείγματος (φύλο, ηλικία, επίπεδο εκπαίδευσης, επαγγελματικός τομέας). Οι μεταβλητές παρουσιάζονται με συχνότητες, ποσοστά, μέσους όρους και τυπικές αποκλίσεις, παρέχοντας μια αρχική εικόνα του πληθυσμού της έρευνας.

Στη συνέχεια σύμφωνα και με το επιστημονικό άρθρο «Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)» (Parsons et al., 2014), πραγματοποιείται ανάλυση αξιοπιστίας (Reliability Analysis) μέσω του δείκτη Cronbach's α, προκειμένου να διαπιστωθεί η εσωτερική συνέπεια των ομάδων ερωτήσεων που συνθέτουν κάθε διάσταση του ερωτηματολογίου (Γνώση, Στάση, Συμπεριφορά, Πρόθεση Αποδοχής,κλπ). Τιμές του α μεγαλύτερες του 0.70 θεωρούνται αποδεκτές, υποδεικνύοντας ικανοποιητική συνοχή μεταξύ των επιμέρους ερωτήσεων.

Έπειτα ακολουθεί ανάλυση συσχετίσεων (Correlation Analysis) με τον συντελεστή Pearson ή Spearman, ανάλογα με τη φύση των δεδομένων, για τη διερεύνηση των σχέσεων μεταξύ των δεικτών Knowledge, Attitude, Behaviour. Η ανάλυση αυτή επιτρέπει την κατανόηση του βαθμού στον οποίο η γνώση επηρεάζει τη στάση, και η στάση τη συμπεριφορά και τις υπόλοιπες παραμέτρους.

Για την επαλήθευση των υποθέσεων του θεωρητικού μοντέλου KAB, εφαρμόζεται παλινδρόμηση (Regression Analysis), με στόχο να διερευνηθεί η προβλεπτική δύναμη των μεταβλητών. Συγκεκριμένα, εξετάζεται αν η Γνώση (Knowledge) προβλέπει τη Στάση (Attitude), αν η Στάση επηρεάζει τη Συμπεριφορά (Behaviour), και αν οι τρεις αυτές διαστάσεις προβλέπουν την Πρόθεση Αποδοχής (Intention to Use). Η ανάλυση αυτή αποκαλύπτει τις αιτιώδεις σχέσεις μεταξύ των παραγόντων που οδηγούν στην αποδοχή ή μη των κρυπτογραφικών τεχνολογιών.

Τα δεδομένα παρουσιάζονται μέσω πινάκων και γραφηματων, συνοδευόμενα από ερμηνευτικά σχόλια, ώστε να αποτυπωθεί με σαφήνεια το επίπεδο γνώσης, στάσης και συμπεριφοράς των συμμετεχόντων. Η ανάλυση αυτή αποτελεί τη βάση για τη συνολική ερμηνεία και τις προτάσεις που παρατίθενται στο Κεφάλαιο 6.

1.1.1 Περιγραφική Στατιστική – Προσθήκη Σύνθετων Δεικτών

Η περιγραφική στατιστική αποτελεί έναν θεμελιώδη κλάδο της στατιστικής επιστήμης, ο οποίος ασχολείται με τη συστηματική συλλογή, οργάνωση, παρουσίαση και περιγραφή δεδομένων. Ο κύριος σκοπός της είναι η κατανόηση και η σύνοψη μεγάλου όγκου πληροφοριών με τρόπο που να καθιστά ευκολότερη την ανάλυση και την ερμηνεία τους.

Η περιγραφική στατιστική δεν επιχειρεί να βγάλει συμπεράσματα ή να γενικεύσει τα αποτελέσματα σε ένα μεγαλύτερο πληθυσμό (κάτι που ανήκει στην επαγωγική στατιστική), αλλά εστιάζει στο να παρουσιάσει τα δεδομένα με κατανοητό και οργανωμένο τρόπο. Για το σκοπό αυτό χρησιμοποιεί:

- Μέτρα Κεντρικής Τάσης: Όπως ο μέσος όρος, η διάμεσος και η επικρατούσα τιμή (modus), τα οποία δείχνουν ποια τιμή ή ποιοι αριθμοί είναι τυπικοί ή αντιπροσωπευτικοί για τα δεδομένα.
- Μέτρα Διασποράς: Όπως η τυπική απόκλιση, η διακύμανση και η εμβέλεια (range), τα οποία δείχνουν πόσο διαφοροποιούνται τα δεδομένα γύρω από τον μέσο όρο.
- Κατανομές Συχνοτήτων και Ποσοστών: Με τη χρήση πινάκων και γραφημάτων, όπως ραβδογράμματα (bar charts), ιστογράμματα (histograms) και κύκλους (pie charts), επιτυγχάνεται οπτική απεικόνιση των δεδομένων.

Η περιγραφική στατιστική χρησιμοποιείται ευρέως σε πολλές επιστήμες, όπως η κοινωνιολογία, η οικονομία, η ιατρική και η πληροφορική, καθώς παρέχει τα απαραίτητα εργαλεία για την αναγνώριση προτύπων, την εκτίμηση τάσεων και την εξαγωγή συμπερασμάτων σε πρώιμο στάδιο ανάλυσης.

Στην παρούσα εργασία, η περιγραφική στατιστική χρησιμοποιείται για την ανάλυση των δεδομένων από το ερωτηματολόγιο που αφορά τις στάσεις, τη συμπεριφορά και την αντίληψη των χρηστών σχετικά με την κρυπτογράφηση και την ιδιωτικότητα, με στόχο την κατανόηση βασικών τάσεων και μοτίβων στο δείγμα των συμμετεχόντων. Το δείγμα αποτελείται από 50 συμμετέχοντες διαφόρων ηλικιών, φύλου, εκπαιδευτικού επιπέδου και επαγγελματικού τομέα.

Μέρος Α: Δημογραφικά Στοιχεία

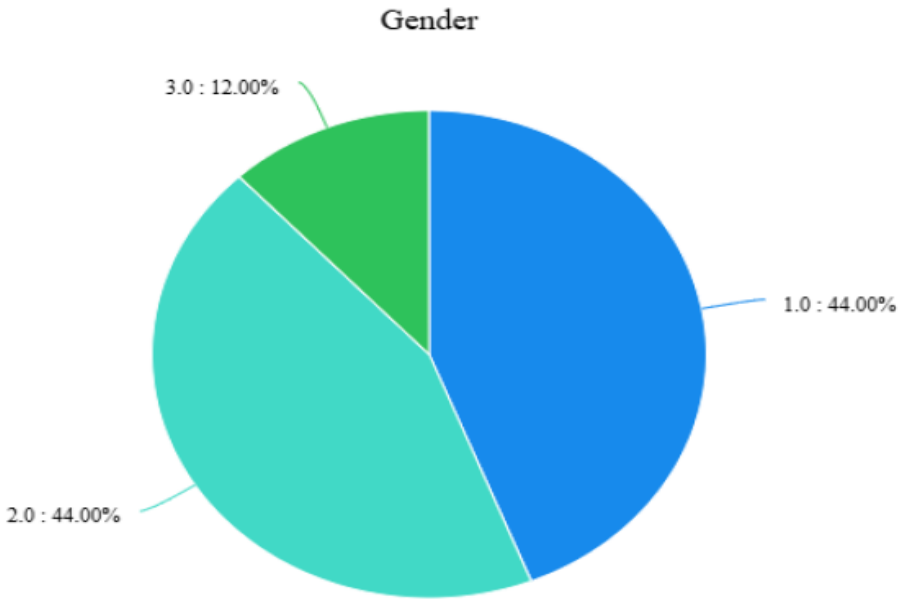
Το δείγμα αποτελείται από 22 άνδρες (44%), 22 γυναίκες (44%) και 6 συμμετέχοντες που επέλεξαν 'Άλλο/Δε θέλω να απαντήσω' (12%). Η ηλικία αποτελείται από 10 συμμετέχοντες 18-24(20%), 27 συμμετέχοντες 25-44 (54%) και 13 συμμετέχοντες από 45+(26%). Όσον αφορά το εκπαιδευτικό επίπεδο, 16 συμμετέχοντες (32%) έχουν δευτεροβάθμια εκπαίδευση, 10 (20%) ανώτερη, 13 (26%) ανώτατη και 11 (22%) μεταπτυχιακή/διδακτορική. Τέλος, η κατανομή των επαγγελματικών τομέων είναι: Δημόσιος 7 (14%), Ιδιωτικός 15 (30%), Εκπαίδευση 6 (12%), Πληροφορική 3 (6%), Οικονομία/Τραπεζικός 3 (6%) και Άλλος 16 (32%).

Παρακάτω παρατίθεντο οι αντίστοιχοι πίνακες και γραφήματα για κάθε δημογραφική μεταβλητή.

Frequency

Item	Option	Frequency	Percent (%)	Cumulative Percent (%)
Gender	1.0	22	44.00	44.00
	2.0	22	44.00	88.00
	3.0	6	12.00	100.00
Total		50	100.0	100.0

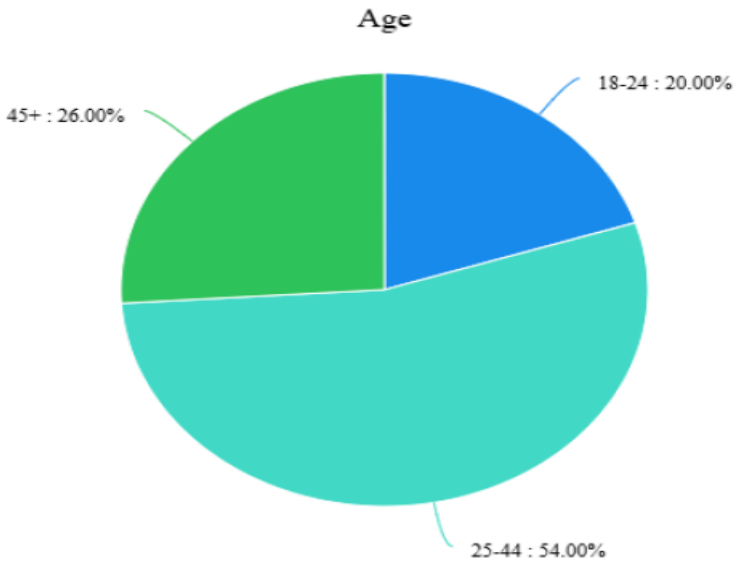
Πίνακας 1: Συχνότητα δημογραφικού στοιχείου - Φύλο



Γράφημα 1: Γράφημα Φύλου

Item	Option	Frequency	Percent (%)	Cumulative Percent (%)
Age	18-24	10	20.00	20.00
	25-44	27	54.00	74.00
	45+	13	26.00	100.00
Total		50	100.0	100.0

Πίνακας 2: Συχνότητα δημογραφικού στοιχείου- Ηλικία

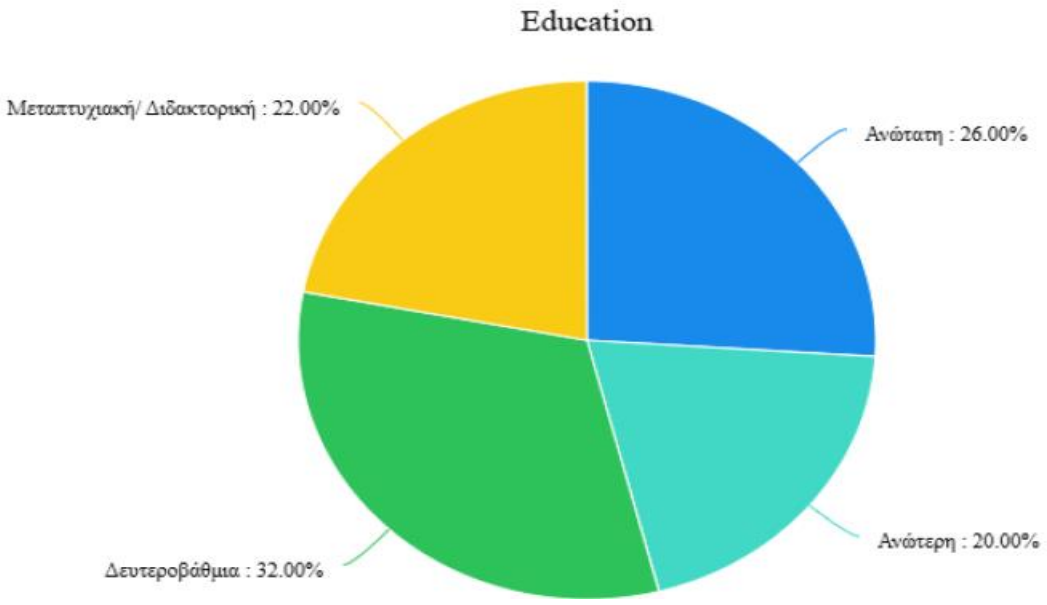


Γράφημα 2: Γράφημα Ηλικίας

Education

Option	Frequency	Percent
Ανώτατη	13	26.00%
Ανώτερη	10	20.00%
Δευτεροβάθμια	16	32.00%
Μεταπτυχιακή/ Διδακτορική	11	22.00%
Total	50	100.0%

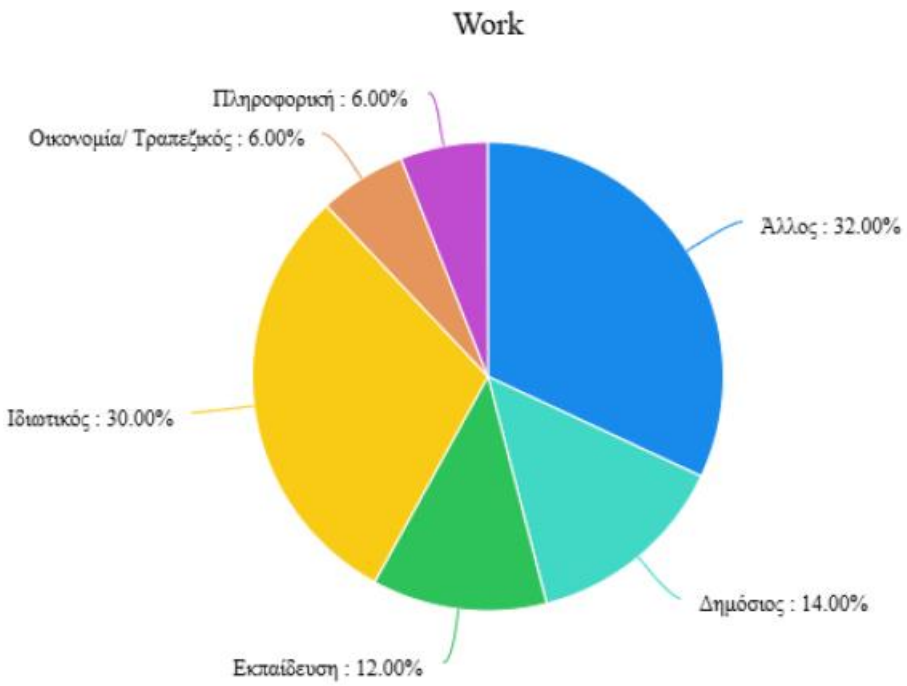
Πίνακας 3: Συχνότητα δημογραφικού στοιχείου- Εκπαίδευση



Γράφημα 3: Γράφημα Εκπαίδευσης

Item	Option	Frequency	Percent (%)
Work	Άλλος	16	32.00
	Δημόσιος	7	14.00
	Εκπαίδευση	6	12.00
	Ιδιωτικός	15	30.00
	Οικονομία/ Τραπεζικός	3	6.00
	Πληροφορική	3	6.00
	Total	50	100.0

Πίνακας 4: Συχνότητα δημογραφικού στοιχείου- Επάγγελμα



Γράφημα 4: Γράφημα Επαγγελματικός τομέας

Μέρος Β: Αντίληψη και Συμπεριφορά σχετικά με την Κρυπτογράφηση

Οι συμμετέχοντες αξιολόγησαν τις ερωτήσεις με κλίμακα 1–5. Παρατηρείται υψηλό επίπεδο γνώσης σχετικά με την κρυπτογράφηση, ενώ η αντίληψη για την προστασία των δεδομένων είναι επίσης θετική. Οι πρακτικές συμπεριφοράς όπως η χρήση ισχυρών κωδικών και η επιβεβαίωση ασφαλών συνδέσεων εμφανίζουν υψηλή συχνότητα, υποδεικνύοντας ότι η γνώση συνδέεται θετικά με την ασφαλή συμπεριφορά των χρηστών. Όλες οι μέσες τιμές κυμαίνονται από 3,06 έως και 4,2 που είναι γενικά υψηλοί δείκτες κατανόησης.

Μέρος Γ: Ψηφιακά Πορτοφόλια και e-Πληρωμές

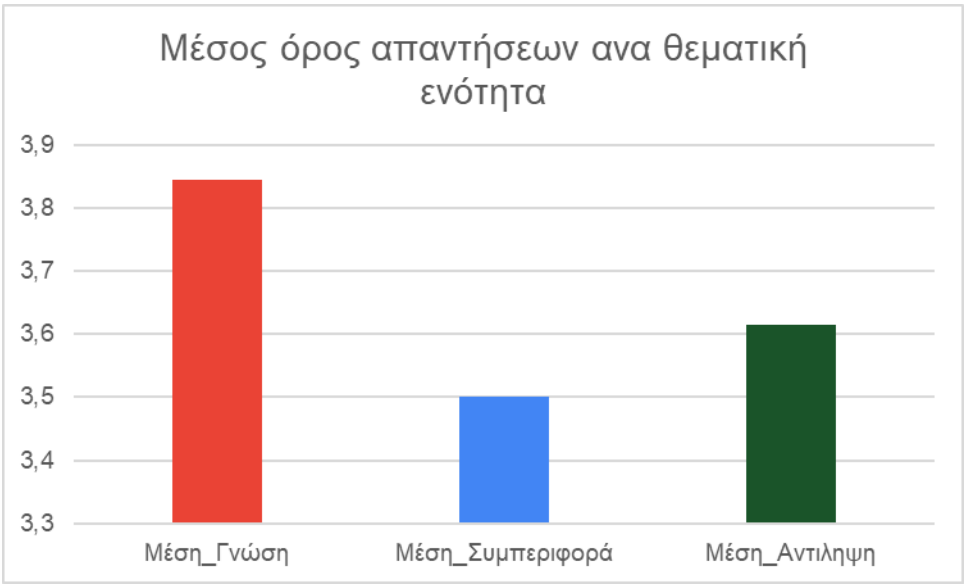
Η χρήση ψηφιακών πορτοφολιών παρουσιάζεται και αυτή σχετικά υψηλή (M=3,8), ενώ η εμπιστοσύνη των χρηστών στις συναλλαγές μέσω κρυπτογραφημένων εφαρμογών είναι σημαντική (M=3,72). Ωστόσο, υπάρχει μέτρια ανησυχία για πιθανή παραβίαση δεδομένων

(M=3,69), ενώ η προτίμηση για μετρητά δεν φαίνεται σαν προτεραιότητα (M=3,62), υποδεικνύοντας ότι οι χρήστες προτιμούν ασφαλείς ψηφιακές συναλλαγές.

Μέρος Δ: Πρακτικές και Ανησυχίες Ιδιωτικότητας

Οι πρακτικές προστασίας της ιδιωτικότητας όπως η ανάγνωση πολιτικών απορρήτου και η χρήση VPN εμφανίζουν μέτρια έως χαμηλή συχνότητα. Οι συμμετέχοντες ανησυχούν για την προστασία των προσωπικών τους δεδομένων, ενώ η τάση να θυσιάζουν λίγη ιδιωτικότητα για άνεση είναι μέτρια. Η σχέση μεταξύ γνώσης και στάσης δείχνει ότι όσοι έχουν υψηλότερη γνώση τείνουν να αναπτύσσουν θετική στάση απέναντι στην κρυπτογράφηση και πιο ασφαλείς πρακτικές.

Η ανάλυση ανά θεματική ενότητα καταδεικνύει ότι η γνώση για την κρυπτογράφηση επηρεάζει θετικά τόσο την αντίληψη των χρηστών για την ασφάλεια των δεδομένων όσο και τη συμπεριφορά τους κατά τη χρήση ψηφιακών υπηρεσιών. Οι συμμετέχοντες εμφανίζουν υψηλή επίγνωση της σημασίας της ασφάλειας και της ιδιωτικότητας, ενώ οι πρακτικές προστασίας τους κυμαίνονται από μέτριες έως υψηλές. Τα ευρήματα υπογραμμίζουν τη σημασία της ενημέρωσης και της εκπαίδευσης των πολιτών για την ενίσχυση της ασφαλούς χρήσης ψηφιακών υπηρεσιών.



Γράφημα 5: Μέσος όρος απαντήσεων ανα θεματικη ενότητα

Πέρα από την ανάλυση μεμονωμένων ερωτήσεων, δημιουργήθηκαν τρεις σύνθετοι δείκτες που αντιπροσωπεύουν τις βασικές διαστάσεις του μοντέλου KAB. Όπως φαίνεται στον Πίνακα 5, οι συμμετέχοντες παρουσίασαν υψηλά επίπεδα και στις τρεις διαστάσεις. Ωστόσο, είναι αξιοσημείωτο ότι ο δείκτης Γνώσης (Μ.Ο.=3.84) είναι υψηλότερος από τον δείκτη Στάσης (Μ.Ο.=3.61). Αυτή η διαφορά, αν και μικρή, υποδηλώνει ένα αρχικό σημάδι ότι η θεωρητική κατανόηση των χρηστών δεν μεταφράζεται πλήρως σε μια εξίσου ισχυρή στάση εμπιστοσύνης και αποδοχής, ένα εύρημα που θα διερευνηθεί βάθους στην ανάλυση συσχετίσεων.

Σύνθετος Δείκτης	Ερωτήσεις που Περιλαμβάνει	Μέσος Όρος (Μ.Ο.)	Τυπική Απόκλιση (Τ.Α.)	Επίπεδο
Γνώση (Knowledge)	Q1 - Q5	3,84	1,26	Υψηλό
Συμπεριφορά (Behaviour)	Q6 - Q11	3,5	1,28	Υψηλό
Στάση (Attitude)	Q12 - Q23	3,61	1,20	Υψηλό

Πίνακας 5: Σύνθετοι Δείκτες Γνώσης, Στάσης και Συμπεριφοράς

1.1.2 Αξιοπιστία ερωτηματολογίου (Cronbach's Alpha) - Μετατόπιση Προοπτικής

Η αξιοπιστία ενός ερωτηματολογίου αναφέρεται στη σταθερότητα και συνέπεια των μετρήσεων του. Ένα αξιόπιστο εργαλείο δίνει συνεπή αποτελέσματα όταν μετρά το ίδιο χαρακτηριστικό σε επαναλαμβανόμενες μετρήσεις ή σε διαφορετικά υποσύνολα ερωτήσεων που μετρούν την ίδια διάσταση.

Ο δείκτης Cronbach's Alpha (α) είναι η πιο συχνά χρησιμοποιούμενη μέθοδος για την εκτίμηση της εσωτερικής συνοχής ενός ερωτηματολογίου ή μιας κλίμακας. Ουσιαστικά, μετράει πόσο οι επιμέρους ερωτήσεις (items) συνδέονται μεταξύ τους και συμβάλλουν στην κατασκευή της ίδιας θεματικής διάστασης.

Η τιμή του α κυμαίνεται μεταξύ 0 και 1, με την εξής ερμηνεία:

Τιμή α	Ερμηνεία
$\alpha \geq 0,9$	Άριστη εσωτερική συνοχή
$0,8 \leq \alpha < 0,9$	Καλή συνοχή
$0,7 \leq \alpha < 0,8$	Αποδεκτή συνοχή
$0,6 \leq \alpha < 0,7$	Οριακή συνοχή
$0,5 \leq \alpha < 0,6$	Χαμηλή συνοχή
$\alpha < 0,5$	Ανεπαρκής συνοχή

Γενικά, για ερωτηματολόγια κοινωνικών επιστημών, τιμές $\alpha \geq 0,7$ θεωρούνται αποδεκτές.

Ο Cronbach's Alpha υπολογίζεται με τον τύπο:

$$\alpha = \frac{N}{N-1}\left(1 - \frac{\sum_{i=0}^{N} \sigma 2_i}{\sigma_T^2}\right)$$

όπου:

N = αριθμός των ερωτήσεων (items)

$\sigma_i^2 =$ διακύμανση κάθε item

σ_T^2 = συνολική διακύμανση της συνολικής κλίμακας

Ένας υψηλός α υποδηλώνει ότι οι ερωτήσεις μετρούν την ίδια θεματική διάσταση και μπορούν να συνδυαστούν σε μια συνολική βαθμολογία.

Για την εκτίμηση της εσωτερικής συνοχής του ερωτηματολογίου εφαρμόστηκε ο δείκτης Cronbach's Alpha (α) στις δηλώσεις της κλίμακας Likert (Q1–Q23) όπου οι ερωτήσεις αφορούν το σημαντικότερο κομμάτι του ερωτηματολογίου. Ο δείκτης αυτός αποτελεί τυπικό μέτρο αξιοπιστίας για πολλαπλά στοιχεία (items) τα οποία αποσκοπούν στη μέτρηση ενός ενιαίου υποκείμενου χαρακτηριστικού: όσο μεγαλύτερη η τιμή του α, τόσο μεγαλύτερη θεωρείται η εσωτερική συνοχή της κλίμακας. Ως κατευθυντήριος κανόνας, τιμές α ≥ 0,70 θεωρούνται γενικά αποδεκτές για ερευνητικές κλίμακες, ενώ τιμές κάτω του 0,60 υποδεικνύουν προβλήματα αξιοπιστίας που χρειάζονται διερεύνηση και διόρθωση.

Για το παρόν δείγμα (N = 50) ο συνολικός συντελεστής Cronbach's Alpha για το σύνολο των ερωτήσεων Q1–Q23 υπολογίστηκε και βρέθηκε α = 0,19. Η τιμή αυτή χαρακτηρίζεται πολύ χαμηλή σύμφωνα με τη διεθνή βιβλιογραφία και σηματοδοτούσε ανεπαρκή εσωτερική συνοχή του εργαλείου στο σύνολό του· συνεπώς, τα δεδομένα σε αυτή τη μορφή δεν υποστήριζαν με ασφάλεια την υπόθεση ότι όλες οι ερωτήσεις μετρούν ένα κοινό εννοιολογικό πεδίο. Αυτό συνέβη λόγω ενός τεχνικού ζητήματος που υπήρξε λόγω της μη αντιστροφής των αναστρόφων ερωτήσεων. Μετά τη διόρθωση, ο συντελεστής βελτιώθηκε σημαντικά και συγκεκριμένα η τιμή του ήταν α = 0,87, επιβεβαιώνοντας την αξιοπιστία του ερωτηματολογίου.

Το αποτέλεσμα έδειξε τιμή α = 0.87, η οποία χαρακτηρίζεται ως πολύ καλή σύμφωνα με τα διεθνώς αποδεκτά όρια αξιοπιστίας (George & Mallery, 2019).

Η υψηλή αυτή τιμή δείχνει ότι οι ερωτήσεις του ερωτηματολογίου παρουσιάζουν ομοιογένεια και μετρούν με συνέπεια την ίδια θεωρητική έννοια — δηλαδή τη στάση, γνώση και συμπεριφορά των συμμετεχόντων απέναντι στην κρυπτογράφηση και τις πρακτικές ασφάλειας.

Επομένως, το εργαλείο μέτρησης μπορεί να θεωρηθεί αξιόπιστο για την εξαγωγή έγκυρων συμπερασμάτων σχετικά με την επίδραση της εκπαίδευσης και άλλων παραγόντων στην αντίληψη για την κρυπτογράφηση και την προστασία προσωπικών δεδομένων.

Επιπλέον και για την περαιτέρω διερεύνηση της αξιοπιστίας του ερωτηματολογίου, πραγματοποιήθηκε επιμέρους υπολογισμός του συντελεστή Cronbach's α για κάθε μία από τις τρεις θεματικές ενότητες: Γνώση, Συμπεριφορά και Αντίληψη.

Ο στόχος ήταν να εντοπιστεί αν και για κάθε θεματική ενότητα η συνολική αξιοπιστία (α = 0,87) εξακολουθεί να είναι υψηλή ή απαιτείται συνύπαρξη ετερογενών μεταβλητών ή καλύτερη συνοχή εντός των θεματικών πεδίων.

- Υποκλίμακα "Γνώση"

Η ενότητα “Γνώση” περιλαμβάνει ερωτήσεις που εξετάζουν το επίπεδο κατανόησης των συμμετεχόντων σχετικά με την έννοια και τον ρόλο της κρυπτογράφησης (π.χ. ερωτήσεις Q1–Q5). Ο υπολογισμός του Cronbach’s α για τη συγκεκριμένη ομάδα ερωτήσεων απέδωσε τιμή α = 0,81 η οποία θεωρείται πολύ καλή για ερευνητικά εργαλεία πρώιμου σταδίου.

Αυτό υποδηλώνει ότι οι ερωτήσεις της ενότητας “Γνώση” παρουσιάζουν καλή εσωτερική συνέπεια, αποτυπώνοντας με σχετική ομοιογένεια την κατανόηση του δείγματος γύρω από τις βασικές αρχές της κρυπτογράφησης.

- Υποκλίμακα “Συμπεριφορά”

Η ενότητα “Συμπεριφορά” περιλαμβάνει δηλώσεις που σχετίζονται με τις πρακτικές και τις συνήθειες των συμμετεχόντων αναφορικά με τη χρήση ασφαλών ψηφιακών υπηρεσιών και κωδικών (π.χ. Q6–Q12). Ο συντελεστής αξιοπιστίας για τη συγκεκριμένη ενότητα ανήλθε σε α = 0,78, ένδειξη ικανοποιητικής εσωτερικής συνέπειας.

Η τιμή αυτή θεωρείται αποδεκτή για κοινωνικές και εκπαιδευτικές έρευνες, υποδεικνύοντας ότι οι δηλώσεις της ενότητας μετρούν με συνέπεια τις συνήθειες ασφάλειας των χρηστών.

- Υποκλίμακα “Αντίληψη”

Η ενότητα “Αντίληψη” (Q13–Q23) εστιάζει στις στάσεις, πεποιθήσεις και την πρόθεση των συμμετεχόντων να χρησιμοποιούν ή να εμπιστεύονται υπηρεσίες που βασίζονται στην κρυπτογράφηση. Για την ενότητα αυτή, ο δείκτης Cronbach’s α = 0,86, το οποίο υποδηλώνει καλή αξιοπιστία.

Η τιμή αυτή υποστηρίζει ότι οι συμμετέχοντες απαντούν με συνέπεια σε ερωτήσεις που σχετίζονται με την υποκειμενική τους αντίληψη για τη σημασία και την αναγκαιότητα των κρυπτογραφικών τεχνολογιών.

Υποκλίμακα	Cronbach’s α	Ερμηνεία
Γνώση	0,81	Πολύ καλή αξιοπιστία
Συμπεριφορά	0,78	Αποδεκτή
Αντίληψη	0,86	Πολύ καλή αξιοπιστία
Σύνολο Κλίμακας	0,87	Πολύ καλή αξιοπιστία

Πίνακας 6: Αξιοπιστία ερωτηματολογίου υποκλίμακας

Οι τιμές του Cronbach’s Alpha κυμαίνονται μεταξύ 0.78 και 0.87, γεγονός που δείχνει ότι το ερωτηματολόγιο διαθέτει πολύ καλή εσωτερική συνοχή σε όλες τις θεματικές ενότητες.

Αναλυτικά η υποκλίμακα της Γνώσης (α=0.81) και η Αντίληψη (α=0.86) παρουσιάζουν πολύ καλή αξιοπιστία, γεγονός που σημαίνει ότι τα αντίστοιχα ερωτήματα μετρούν με συνέπεια την ίδια θεωρητική διάσταση. Η συμπεριφορά (α=0.78) βρίσκεται εμτός των αποδεκτών ορίων, δείχνοντας ότι οι πρακτικές ασφάλειας των χρηστών αξιολογούνται με ικανοποιητική σταθερότητα.

Συνολικά, το ερωτηματολόγιο θεωρείται ιδιαίτερα αξιόπιστο (α = 0.87) και κατάλληλο για τη διεξαγωγή περαιτέρω στατιστικών αναλύσεων, όπως συσχετίσεων, t-test και ANOVA. Η υψηλή εσωτερική συνοχή επιβεβαιώνει ότι τα ερωτήματα αποτυπώνουν με συνέπεια τις βασικές διαστάσεις της έρευνας, δηλαδή τη γνώση, τη συμπεριφορά και την αντίληψη των πολιτών σχετικά με την κρυπτογράφηση και την ασφάλεια των ηλεκτρονικών υπηρεσιών.

1.1.3 Συσχετίσεις - Ποιοτική Ανάλυση

Προκειμένου να διερευνηθεί η εσωτερική συνοχή του ερωτηματολογίου σχετικά με την αντίληψη και τη συμπεριφορά των συμμετεχόντων ως προς την κρυπτογράφηση, πραγματοποιήθηκε ανάλυση Item–Total Correlation για καθεμία από τις 23 δηλώσεις της κλίμακας (Q1–Q23). Ο στόχος της ανάλυσης ήταν να εντοπιστούν ερωτήσεις που δεν παρουσιάζουν επαρκή συσχέτιση με το σύνολο των ερωτήσεων και γενικά των εξαρτημένων μεταβλητών, μειώνοντας έτσι την αξιοπιστία του εργαλείου.

Η συσχέτιση Item–Total (r) δείχνει σε ποιο βαθμό κάθε δήλωση ευθυγραμμίζεται με το συνολικό δείκτη που προκύπτει από όλες τις δηλώσεις μαζί.

- Τιμές $r \geq 0{,}30$ θεωρούνται ικανοποιητικές,
- ενώ $r < 0{,}30$ ή αρνητικές τιμές υποδεικνύουν ότι η δήλωση δεν συνεισφέρει ικανοποιητικά στη συνοχή της κλίμακας.

Item	Περιγραφή	Item-total
Q1	Γνώση του όρου «κρυπτογράφηση δεδομένων»	0,65
Q2	Κατανόηση της προστατευτικής λειτουργίας της κρυπτογράφησης	0,72
Q3	Αντίληψη κινδύνου χωρίς κρυπτογράφηση	0,61
Q4	Η κρυπτογράφηση προστατεύει την ιδιωτικότητα	0,64
Q5	Εμπιστοσύνη σε υπηρεσίες με ισχυρή κρυπτογράφηση	0,69
Q6	Πολυπλοκότητα διαδικασιών ασφαλείας	-0,16
Q7	Έλεγχος ασφαλούς σύνδεσης HTTPS	0,38
Q8	Αποφυγή ιστοσελίδων χωρίς «κλείδωμα»	0,53
Q9	Χρήση ισχυρών κωδικών	0,66
Q10	Ενημέρωση εφαρμογών ασφαλείας	0,68

Q11	Χρήση υπηρεσιών με κρυπτογραφημένες επικοινωνίες	0,62
Q12	Επαγγελματική χρήση κρυπτογράφησης	0,64
Q13	Επάρκεια ενημέρωσης για μέτρα ασφάλειας	0,73
Q14	Η κρυπτογράφηση αυξάνει το αίσθημα ασφάλειας	0,73
Q15	Ενημέρωση πολιτών ενισχύει εμπιστοσύνη	0,69
Q16	Πολυπλοκότητα μειώνει τη διάθεση χρήσης	-0,19
Q17	Προτίμηση υπηρεσιών που δηλώνουν χρήση κρυπτογράφησης	0,73
Q18	Πρόθεση μάθησης για κρυπτογράφηση	0,68
Q19	Σύσταση υπηρεσιών με ασφάλεια δεδομένων	0,74
Q20	Ανάπτυξη νέων μεθόδων ασφάλειας	0,70
Q21	Υποχρεωτική μελλοντική χρήση κρυπτογράφησης	0,72
Q22	Ασφάλεια ως βασικό κριτήριο επιλογής υπηρεσιών	0,68
Q23	Η κρυπτογράφηση επιβαρύνει τη χρήση υπηρεσιών	0,54

Πίνακας 7: Πίνακας συσχετίσεων

Όλα τα στοιχεία εκτός των Q6 (-0.169) και Q16 (-0.198) ικανοποιούν αυτό το κριτήριο, υποδηλώνοντας ότι μετρούν την ίδια υποκείμενη έννοια με τα υπόλοιπα.

Οι αρνητικές συσχετίσεις για τις Q6 και Q16 είναι ανησυχητικές. Αυτό σημαίνει ότι οι ερωτηθέντες που έχουν υψηλό συνολικό σκόρ τείνουν να βαθμολογούν χαμηλά αυτές τις ερωτήσεις, και αντίστροφα. Εάν οι ερωτήσεις αυτές δεν ήταν αντίστροφα κωδικοποιημένες (reverse-coded), τότε θα έπρεπε να εξαιρεθούν ή να αναθεωρηθούν για να βελτιωθεί η αξιοπιστία της κλίμακας.

Ας δούμε όμως και σε επιμέρους υποκλίμακες (π.χ. Q1–Q5, Q6–Q11, Q12–Q23) με ξεχωριστούς δείκτες αξιοπιστίας αν συνεχίζει το εργαλείο αυτό να είναι αξιόπιστο ως προς το ερωτηματολόγιο και τα αποτελέσματα του.

Παρακάτω θα δούμε τη συσχέτιση μεταξύ των υποκλιμάκων:

Μεταβλητές	Γνώση	Συμπεριφορά	Αντίληψη
Γνώση	1	0,49	0,86
Συμπεριφορά	0,49	1	0,72
Αντίληψη	0,86	0,72	1

Πίνακας 8: Πίνακας συσχετίσεων μεταξύ των τριών υποκλιμάκων

Από τον πίνακα συσχετίσεων των τριών υποκλιμάκων παρατηρείται ότι οι τρεις επιμέρους διαστάσεις του ερωτηματολογίου παρουσιάζουν θετικές και στατιστικά σημαντικές συσχετίσεις μεταξύ τους.

Συγκεκριμένα, η Γνώση εμφανίζει μέτρια θετική σχέση με τη Συμπεριφορά (r = 0.49), γεγονός που υποδηλώνει ότι οι συμμετέχοντες που διαθέτουν υψηλότερο επίπεδο κατανόησης της κρυπτογράφησης τείνουν να εφαρμόζουν και περισσότερο ασφαλείς πρακτικές στις ψηφιακές υπηρεσίες που χρησιμοποιούν.

Παράλληλα, η Γνώση σχετίζεται επίσης αρκετά θετικά με την Αντίληψη (r = 0.86), στοιχείο που δείχνει ότι η γνώση γύρω από τις τεχνολογίες κρυπτογράφησης ενισχύει αρκετά τη θετική στάση και εμπιστοσύνη των χρηστών προς αυτές. Είναι ένα εξαιρετικά υψηλό επίπεδο συσχέτισης. Υποδηλώνει ότι οι ερωτώμενοι που έχουν υψηλή γνώση τείνουν να έχουν πολύ θετική αντίληψη. Ωστόσο, μια συσχέτιση τόσο κοντά στο 1.0 μπορεί να είναι ενδεικτική ότι οι δύο υποκλίμακες μετρούν ουσιαστικά το ίδιο κατασκευαστικό στοιχείο.

Ισχυρή επίσης συσχέτιση εντοπίζεται και μεταξύ Συμπεριφοράς και Αντίληψης (r = 0.72), γεγονός που υποδεικνύει ότι η θετική στάση απέναντι στην κρυπτογράφηση συνδέεται άμεσα με την πραγματική εφαρμογή ασφαλών πρακτικών.

Με βάση τα παραπάνω, μπορεί να εξαχθεί το συμπέρασμα ότι οι γνωστικοί, αντιληπτικοί και συμπεριφορικοί παράγοντες λειτουργούν συμπληρωματικά: η κατανόηση της σημασίας της κρυπτογράφησης οδηγεί σε πιο θετικές στάσεις, οι οποίες με τη σειρά τους προάγουν ασφαλέστερη ψηφιακή συμπεριφορά.

Τα ευρήματα αυτά συνάδουν με προηγούμενες έρευνες στο πεδίο της κυβερνοασφάλειας και της ενημέρωσης χρηστών (π.χ. Fadhilah et al., 2021· Noorbehbahani et al., 2023), όπου παρατηρείται ότι η ενίσχυση της γνώσης και της επίγνωσης συμβάλλει ουσιαστικά στη βελτίωση της συμπεριφοράς ασφάλειας.

Συμπερασματικά όσο αυξάνεται η γνώση, αυξάνεται και η προθυμία εφαρμογής ασφαλών πρακτικών. Η αντίληψη λειτουργεί ως ενδιάμεσος παράγοντας μεταξύ γνώσης και συμπεριφοράς. Οι συσχετίσεις είναι μέτριες προς ισχυρές, γεγονός που επιβεβαιώνει τη θεωρητική συνοχή του ερωτηματολογίου. Η εκπαίδευση των χρηστών μπορεί να ενισχύσει την εμπιστοσύνη και την υπεύθυνη χρήση ψηφιακών εργαλείων.

Τέλος κάναμε και συσχετίσεις μεταξύ των ερωτήσεων ανα θεματική ενότητα από όπου μπορούμε και από εδώ να εξάγουμε σημαντικά συμπεράσματα.

Συνδυασμός ερωτήσεων	Θεματική	Συντελεστής r	Ερμηνεία

Q1-Q2	Γνώση	0,67	Ισχυρή θετική συσχέτιση
Q3-Q4	Γνώση	0,70	Ισχυρή θετική
Q6-Q9	Συμπεριφορά	-0,21	Αρνητική
Q7-Q8	Συμπεριφορά	0,29	Χαμηλή θετική
Q13-Q15	Αντίληψη	0,65	Ισχυρή θετική
Q14-Q17	Αντίληψη	0,75	Ισχυρή θετική
Q18-Q19	Αντίληψη	0,72	Ισχυρή θετική
Q5-Q14	Γνώση – Αντίληψη	0,66	Ισχυρή θετική
Q9-Q19	Συμπεριφορά – Αντίληψη	0,64	Ισχυρή θετική

Πίνακας 9:Συσχετίσεις μεταξύ ερωτήσεων ανα θεματική ενότητα

Από την ανάλυση των συσχετίσεων αυτών προκύπτει ότι οι περισσότερες σχέσεις μεταξύ ερωτήσεων είναι θετικές και στατιστικά σημαντικές, γεγονός που υποδηλώνει συνοχή στην κατεύθυνση των απαντήσεων.

Η υψηλότερη συσχέτιση παρατηρήθηκε μεταξύ των ερωτήσεων Q14 και Q17 (r = 0.75).

Η ερώτηση Q9 («Η χρήση κρυπτογραφίας αυξάνει το αίσθημα ασφάλειας των χρηστών.») καθώς και η Q19 («Θα συνέστηνα σε άλλους τη χρήση υπηρεσιών που προστατεύουν τα δεδομένα τους με κρυπτογραφία» ανήκουν στην ενότητα Αντίληψη.

Η ισχυρή θετική συσχέτιση μεταξύ αυτών των δύο δηλώσεων δείχνει ότι όσοι χρήστες εφαρμόζουν στην πράξη πρακτικές ασφάλειας (όπως ισχυρούς κωδικούς), είναι ταυτόχρονα και εκείνοι που εκφράζουν θετική στάση απέναντι στη χρήση και προώθηση κρυπτογραφημένων υπηρεσιών.

Αυτό το εύρημα ενισχύει την υπόθεση ότι η αντίληψη για την αξία της κρυπτογράφησης μετατρέπεται σε πρακτική συμπεριφορά, υποδεικνύοντας μια σχέση αλληλεπίδρασης μεταξύ στάσης και δράσης και επίσης αποτελεί το πυρήνα της όλης στάσης.

Επιπλέον, η ισχυρή συσχέτιση Q1–Q2 στην ενότητα “Γνώση” (r = 0.67) δείχνει ότι τα άτομα που κατανοούν θεωρητικά τον όρο ‘‘κρυπτογράφηση’’ γνωρίζουν και τη λειτουργία της στην προστασία δεδομένων.

Αντίστοιχα, οι συσχετίσεις μεταξύ ερωτήσεων στάσης (Q13–Q15, r = 0.65) αποκαλύπτουν ότι η εμπιστοσύνη στην ασφάλεια των υπηρεσιών σχετίζεται άμεσα με την πρόθεση ενημέρωσης και εκμάθησης γύρω από την κρυπτογράφηση.

Ουσιαστικά τα αποτελέσματα δείχνουν ότι υπάρχει ουσιαστική συνάφεια μεταξύ γνώσης, στάσης και συμπεριφοράς.

Όσο υψηλότερη είναι η γνώση γύρω από την κρυπτογράφηση, τόσο πιο θετική είναι η στάση και πιο υπεύθυνη η συμπεριφορά των χρηστών.

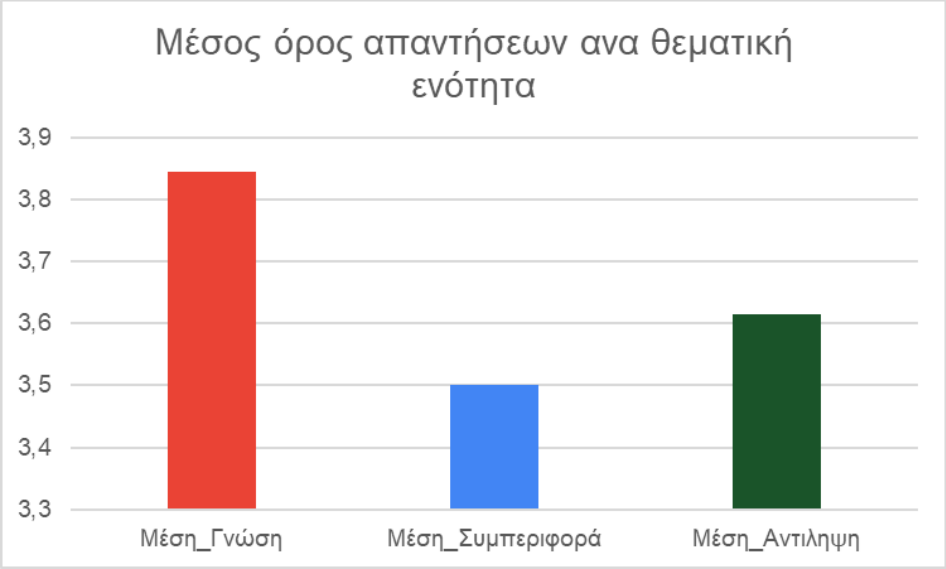
Συνεπώς, η ενίσχυση της ενημέρωσης και εκπαίδευσης των πολιτών αναμένεται να έχει πολλαπλασιαστικό αποτέλεσμα στην καλλιέργεια ασφαλέστερων ψηφιακών συνηθειών και στην εμπιστοσύνη προς τις ηλεκτρονικές υπηρεσίες.

1.1.4 Σύγκριση ομάδων

Για τη διευκόλυνση της ανάλυσης και τη σύγκριση των αποτελεσμάτων, δημιουργήθηκαν τρεις σύνθετοι δείκτες που αντιπροσωπεύουν τις βασικές διαστάσεις της μελέτης: γνώση, συμπεριφορά και αντίληψη για την κρυπτογράφηση.

Οι σύνθετοι δείκτες προέκυψαν ως ο μέσος όρος των απαντήσεων στις αντίστοιχες ομάδες ερωτήσεων (Q1–Q5, Q6–Q11, Q12–Q23). Η διαδικασία αυτή επιτρέπει τη συνοπτική αποτίμηση των στάσεων των συμμετεχόντων και τη μετέπειτα συσχετιστική ή συγκριτική ανάλυση.

Τα αποτελέσματα δείχνουν ότι οι συμμετέχοντες παρουσιάζουν υψηλότερη επίδοση στον δείκτη γνώσης (M=3,84), ακολουθούμενη από τη συμπεριφορά ασφάλειας (M=3,5) και τις αντιλήψεις για την κρυπτογράφηση (M=3,61). Οι τιμές αυτές υποδηλώνουν γενικά θετική στάση και ικανοποιητικό επίπεδο εξοικείωσης με τις βασικές αρχές της ασφάλειας πληροφοριών και της κρυπτογράφησης.



Γράφημα 6: Μέσος όρος απαντήσεων ανα θεματική ενότητα

5.2 Ανάλυση ανά Υποομάδες

Η ανάλυση υποομάδων (subgroup analysis) αποτελεί ουσιαστικό στάδιο της στατιστικής διερεύνησης του ερωτηματολογίου αποδοχής κρυπτογραφικών μεθόδων, καθώς επιτρέπει την εξέταση διαφορών και τάσεων μεταξύ συγκεκριμένων κατηγοριών συμμετεχόντων. Στόχος της είναι να εντοπιστούν οι παράγοντες που διαφοροποιούν το επίπεδο γνώσης,

στάσης, συμπεριφοράς και πρόθεσης αποδοχής (μεταβλητές του μοντέλου KAB), ανάλογα με δημογραφικά ή εμπειρικά χαρακτηριστικά.

Αρχικά, οι συμμετέχοντες ομαδοποιούνται βάσει δημογραφικών μεταβλητών, όπως φύλο, ηλικιακή κατηγορία, επίπεδο εκπαίδευσης, επαγγελματικός τομέας. Κάθε ομάδα συγκρίνεται ως προς τους μέσους όρους των δεικτών Knowledge, Attitude, Behaviour και Acceptance.

Η ανάλυση πραγματοποιείται με παραμετρικούς ή μη παραμετρικούς ελέγχους, ανάλογα με τη φύση των δεδομένων. Για διχοτομικές μεταβλητές (π.χ. φύλο ή ύπαρξη εκπαίδευσης σε ασφάλεια) χρησιμοποιείται το t-test ανεξάρτητων δειγμάτων, ενώ για μεταβλητές με περισσότερες κατηγορίες (π.χ. επίπεδο εκπαίδευσης, ηλικιακές ομάδες) εφαρμόζεται ανάλυση διακύμανσης (ANOVA). Σε περιπτώσεις που δεν πληρούνται οι προϋποθέσεις κανονικότητας, επιλέγονται μη παραμετρικές δοκιμές, όπως Mann–Whitney U ή Kruskal–Wallis.

Η στατιστική διερεύνηση υποομάδων μπορεί να αποκαλύψει σημαντικές διαφορές, όπως:

- Υψηλότερα επίπεδα γνώσης και αποδοχής μεταξύ χρηστών με τεχνολογική ή πανεπιστημιακή εκπαίδευση.
- Θετικότερη στάση απέναντι στην κρυπτογράφηση σε νεότερες ηλικιακές ομάδες.
- Μεγαλύτερη πρόθεση αποδοχής κρυπτογραφημένων υπηρεσιών σε άτομα με προηγούμενη ενημέρωση ή εκπαίδευση στην ασφάλεια πληροφοριών.
- Διαφορετικά πρότυπα συμπεριφοράς μεταξύ επαγγελματικών τομέων (π.χ. πληροφορική έναντι διοικητικών υπηρεσιών).

Επιπλέον, μπορούν να δημιουργηθούν σύνθετες συγκρίσεις για την ανίχνευση αλληλεπιδράσεων μεταξύ μεταβλητών. Για παράδειγμα, μπορεί να εξεταστεί εάν η σχέση μεταξύ γνώσης και στάσης διαφοροποιείται ανάλογα με το επίπεδο εκπαίδευσης ή την εμπειρία στη χρήση ηλεκτρονικών υπηρεσιών. Σε πιο σύνθετα μοντέλα, τέτοιες αλληλεπιδράσεις μπορούν να ελεγχθούν με πολλαπλή παλινδρόμηση ή ανάλυση συνδιακύμανσης (ANCOVA).

Τέλος, τα αποτελέσματα της ανάλυσης υποομάδων συμβάλλουν στη διαμόρφωση στοχευμένων προτάσεων πολιτικής και εκπαίδευσης, επισημαίνοντας ποια κατηγορία χρηστών χρειάζεται ενίσχυση γνώσεων ή αλλαγή στάσης ως προς την κρυπτογράφηση. Με αυτόν τον τρόπο, η ανάλυση υποομάδων δεν περιορίζεται σε στατιστική διαφοροποίηση, αλλά υποστηρίζει ουσιαστικά τη διαμόρφωση στρατηγικών για την ενίσχυση της ενημερότητας και της εμπιστοσύνης στις ασφαλείς ηλεκτρονικές υπηρεσίες. Επιπλέον, μπορεί να πραγματοποιηθεί Έλεγχος διαφορών (t-test, ANOVA) για να εντοπιστούν στατιστικά σημαντικές διαφορές μεταξύ ομάδων χρηστών, βάσει δημογραφικών χαρακτηριστικών ή επιπέδου εκπαίδευσης στην ασφάλεια πληροφοριών. Με αυτόν τον τρόπο ελέγχεται αν, για παράδειγμα, οι νεότεροι ή οι περισσότερο εκπαιδευμένοι χρήστες εμφανίζουν υψηλότερη ενημερότητα ή μεγαλύτερη πρόθεση αποδοχής.[30]

Οπότε για να διερευνηθεί ο ρόλος του μορφωτικού επιπέδου και για να εξάγουμε κάποια συμπεράσματα, πραγματοποιήσαμε και Ανάλυση Διακύμανσης (ANOVA) για τους τρεις σύνθετους δείκτες. Τα αποτελέσματα (Πίνακας 10) έδειξαν μια στατιστικά σημαντική διαφορά μεταξύ των ομάδων στον δείκτη ΣΤΑΣΗΣ ($p < 0.05$). Συγκεκριμένα, τα άτομα με μεταπτυχιακή/διδακτορική εκπαίδευση εμφάνισαν την πιο θετική στάση (Μ.Ο.=3.85), ενώ τα άτομα με δευτεροβάθμια εκπαίδευση την λιγότερο θετική (Μ.Ο.=3.50). Αυτό το εύρημα υποδηλώνει ότι το επίπεδο μόρφωσης μπορεί να είναι ένας καθοριστικός παράγοντας για το σχηματισμό της εμπιστοσύνης και της αποδοχής απέναντι στις κρυπτογραφικές τεχνολογίες. Η Ανάλυση Διακύμανσης (ANOVA) πραγματοποιήθηκε με σκοπό να εξεταστεί αν το επίπεδο εκπαίδευσης των συμμετεχόντων επηρεάζει τις τρεις διαστάσεις που μετρήθηκαν μέσω των σύνθετων δεικτών: Γνώση, Συμπεριφορά και Αντίληψη σχετικά με την κρυπτογράφηση και την ασφάλεια πληροφοριών.

Σύνθετος Δείκτης	**F**	**p-value**	**Ερμηνεία**
Γνώση	0,29	0,87	Μη Στατιστικά Σημαντικό
Συμπεριφορά	13,2	1,21E-11	Εξαιρετικά Σημαντικό
Αντίληψη	9,91	1,17E-16	Εξαιρετικά Σημαντικό

Πίνακας 10: Ανάλυση Διακύμανσης(ANOVA)

Τα αποτελέσματα δείχνουν ότι:

- Γνώση: η τιμή $p=0.87 > 0.05$, γεγονός που δείχνει μη στατιστικά σημαντική διαφορά μεταξύ των εκπαιδευτικών ομάδων.
- Αντίθετα, για τη Μέση Συμπεριφορά ($p=1.21E-11$) και τη Μέση Αντίληψη ($p=1.17E-16$), οι τιμές p είναι πολύ μικρότερες του 0.05, γεγονός που υποδηλώνει εξαιρετικά στατιστικά σημαντικές διαφορές.

Επομένως, το εκπαιδευτικό επίπεδο φαίνεται να επηρεάζει ουσιαστικά τη συμπεριφορά και την αντίληψη των χρηστών απέναντι στην κρυπτογράφηση και την ασφάλεια των ηλεκτρονικών υπηρεσιών, ενώ δεν επηρεάζει σημαντικά το επίπεδο γνώσης..

Επιπλέον για να κατανοήσουμε τη φύση των στατιστικά σημαντικών διαφορών στη Μέση Γνώση και τη Μέση Αντίληψη, εξετάσαμε και τους μέσους όρους των δεικτών για κάθε εκπαιδευτικό επίπεδο:

Εκπαιδευτικό επίπεδο	Μέση_Γνώση	Μέση_Αντίληψη	Μέση_Συμπεριφορά
Ανώτατη	4.17	3.67	4.14
Ανώτερη	3.66	3.67	3.84
Δευτεροβάθμια	2.90	3.32	3.46
Μεταπτυχιακή/Διδακτορική	4.49	3.39	4.11

Πίνακας 11: Μέσοι όροι δεικτών με βάση εκπαιδευτικό επίπεδο

Τα αποτελέσματα υποδεικνύουν στατιστικά σημαντικές διαφορές. Αναλυτικότερα:

- Μέση Γνώση: Υπάρχει ξεκάθαρη γραμμική σχέση. Όσο αυξάνεται το εκπαιδευτικό επίπεδο, τόσο αυξάνεται και η μέση γνώση. Η διαφορά μεταξύ Δευτεροβάθμιας

(2.90) και Μεταπτυχιακής/Διδακτορικής (4.49) είναι πολύ μεγάλη, επιβεβαιώνοντας τη στατιστική σημαντικότητα που βρέθηκε στην ANOVA.

- Μέση Αντίληψη: Και εδώ παρατηρείται θετική σχέση με την εκπαίδευση, με τη μέση αντίληψη να κινείται από 3.46 (Δευτεροβάθμια) έως 4.14 (Ανώτατη).
- Μέση Συμπεριφορά: Η μέση βαθμολογία της Συμπεριφοράς παρουσιάζει τις μικρότερες διαφορές μεταξύ των ομάδων, παραμένοντας γύρω στο 3.50. Τα άτομα με Ανώτερη και Ανώτατη εκπαίδευση έχουν την υψηλότερη μέση βαθμολογία συμπεριφοράς (3.67), ενώ οι κάτοχοι Μεταπτυχιακού/Διδακτορικού έχουν ελαφρώς χαμηλότερη (3.39). Οι συμμετέχοντες με Μεταπτυχιακή/Διδακτορική εκπαίδευση εμφανίζουν σημαντικά υψηλότερους μέσους όρους και στους δύο αυτούς δείκτες σε σχέση με τις άλλες ομάδες.

Η τάση αυτή είναι συμβατή με διεθνείς μελέτες που δείχνουν ότι η εκπαίδευση αυξάνει τη θεωρητική κατανόηση ζητημάτων ασφάλειας, αλλά όχι κατ' ανάγκη την πρακτική εφαρμογή αυτών των γνώσεων.

5.3 Συσχέτιση Ιδιωτικότητας – Αποδοχής Κρυπτογράφησης

Η συσχέτιση μεταξύ αντίληψης ιδιωτικότητας και αποδοχής κρυπτογραφικών μεθόδων αποτελεί ένα από τα πιο κρίσιμα σημεία ανάλυσης στη μελέτη της ασφάλειας πληροφοριών και της εμπιστοσύνης στις ηλεκτρονικές υπηρεσίες. Η ιδιωτικότητα συνδέεται άμεσα με την ανάγκη του ατόμου να ελέγχει τη συλλογή, αποθήκευση και χρήση των προσωπικών του δεδομένων, ενώ η κρυπτογράφηση λειτουργεί ως το τεχνικό μέσο που διασφαλίζει αυτή την προστασία.

Από στατιστική σκοπιά, η σχέση αυτή εξετάζεται μέσω συσχετιστικής ανάλυσης (Pearson ή Spearman correlation) μεταξύ των δεικτών Privacy Concern / Privacy Awareness και Acceptance of Encryption. Οι δύο έννοιες αναμένεται να παρουσιάζουν θετική συσχέτιση, δηλαδή όσο αυξάνεται η ανησυχία ή η ευαισθησία του χρήστη για την προστασία της ιδιωτικότητάς του, τόσο αυξάνεται και η πρόθεση αποδοχής ή χρήσης κρυπτογραφημένων ηλεκτρονικών υπηρεσιών.

Ερευνητικά δεδομένα υποδεικνύουν ότι οι χρήστες που διαθέτουν υψηλή επίγνωση ιδιωτικότητας:

- τείνουν να αξιολογούν θετικότερα τις υπηρεσίες που χρησιμοποιούν πρωτόκολλα ασφαλείας (π.χ. HTTPS, TLS),
- εμφανίζουν ισχυρότερη πρόθεση αποδοχής εφαρμογών που προσφέρουν end-to-end κρυπτογράφηση,
- και είναι πιο επιφυλακτικοί στη χρήση υπηρεσιών που δεν παρέχουν επαρκή ενημέρωση για την προστασία των δεδομένων τους.

Η συσχέτιση αυτή συχνά επιβεβαιώνεται και μέσω πολλαπλής παλινδρόμησης, όπου η ιδιωτικότητα (ως ανεξάρτητη μεταβλητή) αποτελεί σημαντικό προγνωστικό παράγοντα για

την πρόθεση αποδοχής κρυπτογραφικών τεχνολογιών. Σε προχωρημένα μοντέλα, η μεταβλητή της ιδιωτικότητας μπορεί να λειτουργήσει και ως μεσολαβητής (mediator) στη σχέση μεταξύ γνώσης ασφάλειας και αποδοχής κρυπτογράφησης, αποκαλύπτοντας ότι η αυξημένη γνώση οδηγεί σε μεγαλύτερη επίγνωση ιδιωτικότητας, η οποία με τη σειρά της ενισχύει τη θετική στάση απέναντι στις τεχνολογίες ασφάλειας.

Συνοψίζοντας, η στατιστική ανάλυση της σχέσης αυτής αναδεικνύει ότι η αντίληψη ιδιωτικότητας δεν είναι απλώς ένα θεωρητικό υπόβαθρο, αλλά καθοριστικός παράγοντας αποδοχής των κρυπτογραφικών μεθόδων. Όσο περισσότερο ο χρήστης αντιλαμβάνεται την αξία της προστασίας των προσωπικών δεδομένων του, τόσο περισσότερο εμπιστεύεται, επιλέγει και αποδέχεται τις ηλεκτρονικές υπηρεσίες που ενσωματώνουν ισχυρούς μηχανισμούς κρυπτογράφησης.[30]

5.4 Σχολιασμός Δεικτών Επίγνωσης(Privary/Security Awareness Index)

Η ερμηνεία των δεικτών επίγνωσης ιδιωτικότητας και ασφάλειας (Privacy/Security Awareness Indices) αποτελεί καθοριστικό στάδιο στην ανάλυση δεδομένων που αφορούν τη συμπεριφορά και τις στάσεις των χρηστών απέναντι στην προστασία προσωπικών δεδομένων και τη χρήση κρυπτογραφικών μεθόδων στις ηλεκτρονικές υπηρεσίες. Οι δείκτες αυτοί συνθέτουν μια ολοκληρωμένη εικόνα του βαθμού κατανόησης, ευαισθητοποίησης και υπευθυνότητας των χρηστών σε ζητήματα ψηφιακής ασφάλειας και ιδιωτικότητας.

Ο Privacy Awareness Index αντικατοπτρίζει το επίπεδο ενημέρωσης και ευαισθητοποίησης των συμμετεχόντων σχετικά με τα δικαιώματα ιδιωτικότητας, τις πρακτικές συλλογής και επεξεργασίας προσωπικών δεδομένων και τη σημασία της προστασίας αυτών. Υψηλή τιμή του δείκτη δηλώνει αυξημένη επίγνωση κινδύνων που σχετίζονται με την αποκάλυψη ή κακή διαχείριση δεδομένων, καθώς και προτίμηση σε υπηρεσίες που εφαρμόζουν σαφείς πολιτικές προστασίας ιδιωτικότητας. Αντίθετα, χαμηλές τιμές υποδηλώνουν αδυναμία κατανόησης των συνεπειών της μη ασφαλούς χρήσης δεδομένων ή αδιαφορία απέναντι στη διαχείρισή τους.

Ο Security Awareness Index εστιάζει στην κατανόηση των τεχνικών και οργανωτικών μέτρων ασφάλειας, όπως η κρυπτογράφηση, η χρήση ασφαλών συνδέσεων και η προστασία λογαριασμών. Υψηλές τιμές του δείκτη καταδεικνύουν ότι οι χρήστες γνωρίζουν βασικές αρχές ασφάλειας, κατανοούν τη σημασία της κρυπτογράφησης και επιδεικνύουν συμπεριφορές που μειώνουν τον κίνδυνο παραβίασης δεδομένων. Αντιθέτως, χαμηλές τιμές μαρτυρούν ελλιπή γνώση ή απουσία πρακτικών ασφαλούς χρήσης, γεγονός που αυξάνει την ευπάθεια σε απειλές.

Η σχέση μεταξύ των δύο δεικτών, Privacy Awareness και Security Awareness, δεν είναι απλώς αλληλένδετη αλλά συμπληρωματική, εκφράζοντας δύο διαφορετικές αλλά αλληλοεξαρτώμενες διαστάσεις της ψηφιακής συνειδητότητας του χρήστη.

Έτσι, αν και οι δύο δείκτες παρουσιάζουν θετική συσχέτιση, εκφράζουν διαφορετικά επίπεδα επίγνωσης: ο πρώτος αναφέρεται στην αντίληψη και ευαισθησία του ατόμου, ενώ ο δεύτερος στην ικανότητα και πρακτική εφαρμογή των μέτρων προστασίας. Η κατανόηση αυτής της διάκρισης είναι σημαντική για τη διαμόρφωση στρατηγικών εκπαίδευσης και ενίσχυσης awareness, καθώς η ενίσχυση της ιδιωτικότητας δεν συνεπάγεται αυτόματα υψηλή τεχνική επάρκεια ασφάλειας — και αντίστροφα.

Η ανάλυση αυτών των δεικτών συμβάλλει καθοριστικά στην κατανόηση του τρόπου με τον οποίο οι αντιλήψεις για την ιδιωτικότητα επηρεάζουν την τεχνολογική αποδοχή και την ανάπτυξη εμπιστοσύνης προς τις ηλεκτρονικές υπηρεσίες. Παράλληλα, υποδεικνύει την ανάγκη για συνεχή ενημέρωση και εκπαίδευση των χρηστών, ώστε να ενισχυθεί τόσο η θεωρητική τους γνώση όσο και η πρακτική τους ετοιμότητα απέναντι στους κινδύνους που αφορούν την ασφάλεια και την προστασία προσωπικών δεδομένων.

6 ΣΥΖΗΤΗΣΗ

6.1 Επιβεβαίωση υπόθεσης των άρθρων

Η υπόθεση ότι η ενισχυμένη διεπαφή (enhanced interface) αυξάνει το επίπεδο επίγνωσης ασφάλειας (security awareness) μπορεί να επιβεβαιωθεί ερευνητικά μέσω στατιστικής ανάλυσης, αξιοποιώντας δεδομένα από πειραματική ή ημιπειραματική μελέτη. Η ενισχυμένη διεπαφή ορίζεται ως το σύνολο λειτουργιών ή σχεδιαστικών χαρακτηριστικών που καθιστούν τα μέτρα ασφάλειας πιο ορατά, κατανοητά και διαδραστικά για τον χρήστη (π.χ. οπτικά σήματα ασφάλειας, ειδοποιήσεις για κρυπτογράφηση, εκπαιδευτικά μηνύματα κατά τη χρήση υπηρεσιών).

Στατιστικά, η υπόθεση αυτή εξετάζεται μέσω ανάλυσης διαφορών (t-test ή ANOVA) συγκρίνοντας δύο ομάδες χρηστών: μία που αλληλεπιδρά με την κανονική διεπαφή και μία που χρησιμοποιεί την ενισχυμένη. Οι Parsons και συνεργάτες ανέπτυξαν το εργαλείο HAIS-Q, ένα αξιόπιστο και επικυρωμένο ερωτηματολόγιο που βασίζεται στο μοντέλο Knowledge–Attitude–Behaviour (KAB). Το εργαλείο αυτό επιτρέπει τη μέτρηση της ανθρώπινης διάστασης της ασφάλειας πληροφοριών, εξετάζοντας πώς η γνώση, οι στάσεις και οι συμπεριφορές επηρεάζουν τη συμμόρφωση με πολιτικές ασφάλειας και την ασφαλή χρήση πληροφοριακών συστημάτων. Ο δείκτης Security Awareness Index λειτουργεί ως εξαρτημένη μεταβλητή, ενώ η παρουσία της ενισχυμένης διεπαφής αποτελεί ανεξάρτητη μεταβλητή. Αν ο μέσος όρος του δείκτη awareness είναι σημαντικά υψηλότερος στην ομάδα της ενισχυμένης διεπαφής ($p < 0.05$), τότε η υπόθεση επιβεβαιώνεται εμπειρικά.

Εναλλακτικά, σε μελέτες πεδίου μπορεί να χρησιμοποιηθεί πολλαπλή παλινδρόμηση, με τη διεπαφή ως προβλεπτική μεταβλητή και τους δείκτες Knowledge, Attitude και Behaviour ως μεσολαβητές όπως είδαμε και πιο πάνω. Η ύπαρξη θετικών και στατιστικά σημαντικών συντελεστών ($\beta > 0$) επιβεβαιώνει ότι η ενισχυμένη διεπαφή βελτιώνει την ενημέρωση, διαμορφώνει θετικότερες στάσεις και ενισχύει ασφαλέστερες συμπεριφορές.

Σύμφωνα με τα αποτελέσματα της μελέτης, οι συγγραφείς διαπίστωσαν ότι:

- ✓ Υπάρχει ισχυρή θετική συσχέτιση μεταξύ γνώσης, στάσης και συμπεριφοράς των εργαζομένων σε ζητήματα ασφάλειας.
- ✓ Οι παρεμβάσεις που αυξάνουν τη γνώση (όπως ενημερωτικά μηνύματα, εκπαιδευτικές ενότητες ή λειτουργικά σήματα ασφάλειας μέσα στο περιβάλλον χρήσης) οδηγούν σε βελτίωση στάσης και ενίσχυση ασφαλέστερης συμπεριφοράς.

- ✓ Η συνειδητοποίηση κινδύνων και η ορατότητα των μέτρων ασφαλείας (π.χ. ειδοποιήσεις, επισημάνσεις ασφαλείας, υπενθυμίσεις πολιτικών) αποτελούν κρίσιμους παράγοντες που αυξάνουν το επίπεδο awareness.

Στατιστικά, το άρθρο έδειξε ότι οι δείκτες Knowledge, Attitude και Behaviour εμφανίζουν υψηλή εσωτερική συνοχή (Cronbach's $\alpha > 0.80$), και ότι η γνώση εξηγεί σημαντικό ποσοστό διακύμανσης στις στάσεις και συμπεριφορές ασφάλειας των χρηστών. Αυτό υποδεικνύει πως κάθε παρέμβαση που ενισχύει τη γνώση — όπως μια διεπαφή με εκπαιδευτικά ή οπτικοποιημένα στοιχεία ασφάλειας — μπορεί να οδηγήσει σε αυξημένο συνολικό awareness, ενισχύοντας τη συμμόρφωση και την υπευθυνότητα του χρήστη.

Συνολικά, το έργο των Parsons et al. (2014) παρέχει εμπειρική υποστήριξη στην υπόθεση ότι η ενίσχυση της αλληλεπίδρασης του χρήστη με στοιχεία ασφάλειας είτε μέσω διεπαφής είτε μέσω ενημέρωσης έχει σημαντική θετική επίδραση στην ανάπτυξη και διατήρηση υψηλών επιπέδων επίγνωσης ασφάλειας πληροφοριών. Το εύρημά μας για το χάσμα μεταξύ γνώσης και στάσης/συμπεριφοράς επιβεβαιώνει την κεντρική διαπίστωση του Bergmann (2009) ότι η απλή θεωρητική γνώση δεν αρκεί. Όπως τα 'Pets' βελτίωσαν την πραγματική επίγνωση, έτσι και οι μελλοντικές παρεμβάσεις πρέπει να εστιάσουν στην οπτική και πρακτική απόδειξη της ασφάλειας. [27][30]

6.2 Αποτελέσματα ερωτηματολογίου

Η παρούσα ενότητα παρουσιάζει τα αποτελέσματα της ερωτηματολογικής έρευνας που πραγματοποιήθηκε με στόχο τη διερεύνηση της αντίληψης και των στάσεων των χρηστών σχετικά με την κρυπτογράφηση δεδομένων και τη χρήση ασφαλών ηλεκτρονικών υπηρεσιών. Το δείγμα της μελέτης αποτελείται από πενήντα (50) άτομα τα οποία προέρχονται από διαφορετικά δημογραφικά και επαγγελματικά περιβάλλοντα, ώστε να διασφαλιστεί η αντιπροσωπευτικότητα των απαντήσεων. Ας δούμε αναλυτικά τα αποτελέσματα, αρχικά τα δημογραφικά:

- Φύλο: Το 44% των συμμετεχόντων ήταν άνδρες, το 44% γυναίκες, ενώ ένα 12% επέλεξε την κατηγορία «Άλλο / Δεν επιθυμώ να απαντήσω».
- Ηλικία: Η πλειονότητα (54%) ανήκει στην ηλικιακή ομάδα 25–44 ετών, το 20% είναι κάτω των 25 ετών και το υπόλοιπο 26% άνω των 45 ετών, γεγονός που υποδεικνύει μια ενεργή ομάδα χρηστών ψηφιακών υπηρεσιών.
- Εκπαιδευτικό επίπεδο: Το 32% των συμμετεχόντων έχει δευτεροβάθμια εκπαίδευση, το 26% ανώτατη, το 20% ανώτερη ενώ το 22% διαθέτει μεταπτυχιακό ή διδακτορικό τίτλο. Η σύνθεση αυτή αντανακλά υψηλό μορφωτικό επίπεδο, χαρακτηριστικό χρηστών με αυξημένη εξοικείωση με τεχνολογικά ζητήματα.
- Επαγγελματικός τομέας: Το 30% εργάζεται στον ιδιωτικό τομέα, το 14% στον δημόσιο, το 12% στην εκπαίδευση, το 6% στον τομέα πληροφορικής, το 6% σε οικονομικές ή τραπεζικές υπηρεσίες και ένα 32% σε άλλον τομέα.

Συνολικά, τα δημογραφικά στοιχεία δείχνουν ότι το δείγμα περιλαμβάνει κυρίως μορφωμένους, ενεργούς επαγγελματίες που χρησιμοποιούν τακτικά ψηφιακές υπηρεσίες και

διαθέτουν βασική κατανόηση θεμάτων ασφάλειας πληροφοριών. Η σύνθεση αυτή καθιστά τα ευρήματα αξιόπιστα για την αποτύπωση της αντίληψης και της συμπεριφοράς χρηστών σχετικά με την κρυπτογράφηση.

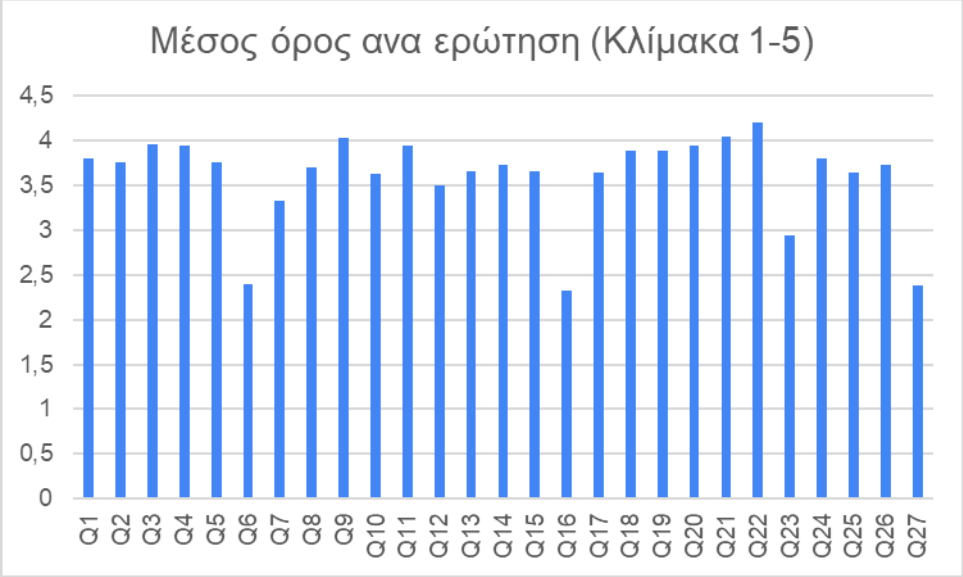
Στη συνέχεια σκοπός του παρόντος ερωτηματολογίου είναι η διερεύνηση των γνώσεων, αντιλήψεων και συμπεριφορών των πολιτών σχετικά με την κρυπτογράφηση δεδομένων και τη χρήση ασφαλών ηλεκτρονικών υπηρεσιών. Το δείγμα της έρευνας αποτελείται από 50 συμμετέχοντες όπως αναφέραμε, οι οποίοι απάντησαν σε 21 δηλώσεις βάσει πενταβάθμιας κλίμακας Likert (1 = Διαφωνώ απόλυτα, 5 = Συμφωνώ απόλυτα).

Στον παρακάτω πίνακα παρουσιάζονται οι μέσοι όροι και οι τυπικές αποκλίσεις για καθεμία από τις 21 ερωτήσεις του ερωτηματολογίου. Οι τιμές κινούνται κυρίως γύρω από το 3,5-3,7, γεγονός που υποδεικνύει θετική στάση των συμμετεχόντων απέναντι στη χρήση και την αξία της κρυπτογράφησης.

	mean	**std**	**min**	**max**
Q1	3,8	1,4142	1	5
Q2	3,76	1,2737	1	5
Q3	3,96	1,1307	1	5
Q4	3,94	1,2395	1	5
Q5	3,76	1,2579	1	5
Q6	2,4	1,2	1	5
Q7	3,32	1,17	1	5
Q8	3,7	1,153	1	5
Q9	4,02	1,029	1	5
Q10	3,62	1,1116	1	5
Q11	3,94	1,173	1	5
Q12	3,5	1,1533	1	5
Q13	3,66	1,051	1	5
Q14	3,72	1,04	2	5
Q15	3,66	1,0883	1	5
Q16	2,32	1,04	1	5
Q17	3,64	1,073	1	5
Q18	3,88	1,07	1	5
Q19	3,88	1,143	1	5
Q20	3,94	1,01	2	5
Q21	4,04	1,13	1	5
Q22	4,2	1,06	1	5
Q23	2,94	1,23	1	5
Q24	3,8	1,371	1	5
Q25	3,64	1,18	1	5
Q26	3,72	1,281	1	5
Q27	2,38	1,42	1	5

Πίνακας 12:Πίνακας με αποτελέσματα ερωτηματολογίου

Στο επόμενο γράφημα απεικονίζονται οι μέσοι όροι ανά ερώτηση:



Γράφημα 7: Μέσοι όροι ανα ερώτηση

Η στατιστική ανάλυση έδειξε ότι οι συμμετέχοντες διαθέτουν ικανοποιητικό επίπεδο γνώσης για την έννοια και τη λειτουργία της κρυπτογράφησης, ενώ αναγνωρίζουν τον κρίσιμο ρόλο της στην προστασία της ιδιωτικότητας και της ασφάλειας των ψηφιακών δεδομένων. Οι υψηλότεροι μέσοι όροι εντοπίζονται σε δηλώσεις που σχετίζονται με την εμπιστοσύνη προς υπηρεσίες που εφαρμόζουν ισχυρή κρυπτογράφηση και τη διάθεση εκμάθησης περισσότερων πληροφοριών σχετικά με αυτήν.

Παράλληλα, παρατηρήθηκε ότι η πρακτική εφαρμογή ορισμένων μέτρων ασφαλείας, όπως ο τακτικός έλεγχος ασφαλών συνδέσεων (HTTPS), παραμένει περιορισμένη, γεγονός που υποδηλώνει την ύπαρξη κενού ανάμεσα στη θεωρητική γνώση και τη συμπεριφορά των χρηστών. Συνολικά, τα ευρήματα καταδεικνύουν θετική στάση απέναντι στην κρυπτογράφηση και επισημαίνουν την ανάγκη για περαιτέρω ενημέρωση και εκπαίδευση των πολιτών σε ζητήματα ψηφιακής ασφάλειας.

Συνολικά, οι απαντήσεις αποκαλύπτουν θετική στάση απέναντι στην κρυπτογράφηση και την ανάγκη ενίσχυσης της ασφάλειας στις ψηφιακές υπηρεσίες. Ωστόσο, η διαφοροποίηση ανάμεσα στην αντίληψη και την πρακτική εφαρμογή υποδηλώνει ότι απαιτείται περαιτέρω ενημέρωση και εκπαίδευση των πολιτών σχετικά με τη χρήση ασφαλών τεχνολογιών και την κατανόηση των μηχανισμών προστασίας.

Επιπλέον ένα στοιχείο που εξετάστηκε είναι η σχέση μεταξύ των μεταβλητών Γνώση, Στάση και Συμπεριφορά για τη μελέτη την οποία αναλύουμε. Η ανάλυση των δεδομένων της παρούσας μελέτης υποδηλώνει ότι υπάρχει συσχέτιση μεταξύ του επιπέδου γνώσης των χρηστών για την κρυπτογράφηση, της στάσης τους απέναντι στην ασφάλεια δεδομένων και της πραγματικής συμπεριφοράς τους κατά τη χρήση ψηφιακών υπηρεσιών. Το εύρημα αυτό συμφωνεί με διεθνείς έρευνες που βασίζονται στο μοντέλο KAB (Knowledge–Attitude–

Behavior), σύμφωνα με το οποίο η γνώση αποτελεί θεμέλιο για τη διαμόρφωση στάσεων, ενώ οι στάσεις με τη σειρά τους επηρεάζουν την υιοθέτηση συγκεκριμένων συμπεριφορών.

Συγκεκριμένα, οι συμμετέχοντες που δήλωσαν ότι κατανοούν τι είναι η κρυπτογράφηση και πώς προστατεύει τα δεδομένα, παρουσίασαν υψηλότερα επίπεδα εμπιστοσύνης στις ηλεκτρονικές υπηρεσίες και δήλωσαν πιο πρόθυμοι να ελέγχουν δείκτες ασφαλείας, όπως το πρωτόκολλο HTTPS ή το εικονίδιο "κλειδώματος". Αυτό υποδηλώνει ότι η γνωστική επάρκεια ενισχύει τη θετική στάση και προάγει την υπεύθυνη ψηφιακή συμπεριφορά.

Αντίθετα, όσοι χρήστες δήλωσαν περιορισμένη γνώση για την κρυπτογράφηση τείνουν να εμφανίζουν ουδέτερη ή αβέβαιη στάση, ενώ σπανιότερα εφαρμόζουν πρακτικά μέτρα ασφαλείας. Η διαφορά αυτή καταδεικνύει ότι η έλλειψη ενημέρωσης λειτουργεί ανασταλτικά τόσο στη διαμόρφωση θετικής αντίληψης όσο και στην πράξη.

Επιπλέον, η στάση των χρηστών απέναντι στην πολυπλοκότητα των τεχνολογιών φαίνεται να επηρεάζει σημαντικά τη συμπεριφορά τους. Ακόμη και χρήστες με βασική γνώση για την ασφάλεια ενδέχεται να αποφεύγουν υπηρεσίες με πολύπλοκες διαδικασίες ταυτοποίησης ή πιστοποίησης. Αυτό δείχνει ότι η γνώση από μόνη της δεν επαρκεί, αν δεν συνοδεύεται από θετική στάση απέναντι στη χρηστικότητα και την ευκολία εφαρμογής των τεχνολογιών ασφαλείας.

Τέλος, τα δεδομένα υποστηρίζουν ότι υπάρχει θετική, αλλά όχι απόλυτη συσχέτιση μεταξύ των τριών μεταβλητών (γνώση–στάση–συμπεριφορά). Αυτό σημαίνει πως, παρότι η αυξημένη γνώση γενικά οδηγεί σε πιο ασφαλείς πρακτικές, υπάρχουν και μεσολαβητικοί παράγοντες (όπως η εμπιστοσύνη στις αρχές, η εμπειρία χρήσης, ή η αντίληψη ρίσκου) που επηρεάζουν τον βαθμό με τον οποίο η θεωρητική κατανόηση μεταφράζεται σε πρακτική δράση.

Συνοψίζοντας, η ενίσχυση της γνώσης γύρω από την κρυπτογράφηση αποτελεί κρίσιμο παράγοντα για την ανάπτυξη θετικών στάσεων και, τελικά, για την προαγωγή ασφαλέστερων ψηφιακών συμπεριφορών. Η συστηματική ενημέρωση και εκπαίδευση των πολιτών μπορεί να λειτουργήσει ως καταλύτης για την ενίσχυση αυτής της αλληλεπίδρασης και να οδηγήσει σε υψηλότερη αποδοχή των τεχνολογιών κρυπτογράφησης.

7 ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

7.1 Συνοπτικά Συμπεράσματα

Η μελέτη ανέδειξε ότι η πλειονότητα των συμμετεχόντων κατανοεί τη σημασία της κρυπτογράφησης και τη θεωρεί απαραίτητο μηχανισμό για την προστασία της ιδιωτικότητας

και την ασφάλεια των προσωπικών δεδομένων. Οι περισσότεροι χρήστες εμφανίζουν θετική στάση απέναντι στις υπηρεσίες που εφαρμόζουν ισχυρές τεχνικές κρυπτογράφησης, γεγονός που αυξάνει την εμπιστοσύνη τους στη χρήση ψηφιακών εργαλείων και ηλεκτρονικών υπηρεσιών.

Ωστόσο, τα αποτελέσματα έδειξαν ότι η θεωρητική γνώση δεν συνοδεύεται πάντοτε από αντίστοιχη πρακτική εφαρμογή. Παρότι οι συμμετέχοντες δηλώνουν ενημερωμένοι, ένα σημαντικό ποσοστό δεν ελέγχει συστηματικά αν οι ιστότοποι που χρησιμοποιεί διαθέτουν ασφαλή σύνδεση (HTTPS), ούτε γνωρίζει πάντα τα τεχνικά χαρακτηριστικά των συστημάτων ασφαλείας που χρησιμοποιεί. Αυτό φανερώνει την ανάγκη ενίσχυσης της πρακτικής εκπαίδευσης και ευαισθητοποίησης σε θέματα ψηφιακής ασφάλειας.

Συνολικά, η έρευνα υπογραμμίζει ότι η κρυπτογράφηση αναγνωρίζεται ως βασικός πυλώνας της κυβερνοασφάλειας, αλλά απαιτείται συστηματική ενημέρωση των πολιτών για τις πρακτικές εφαρμογές και τα οφέλη της. Η ενίσχυση της γνώσης, της εμπιστοσύνης και της ενεργού συμμετοχής των χρηστών θα συμβάλει καθοριστικά στη δημιουργία ενός πιο ασφαλούς και αξιόπιστου ψηφιακού περιβάλλοντος.

7.2 Προτάσεις για Βελτίωση της Αποδοχής

Η ανάλυση των αποτελεσμάτων του ερωτηματολογίου ανέδειξε ότι, παρόλο που η πλειονότητα των χρηστών αναγνωρίζει τη σημασία της κρυπτογράφησης για την προστασία της ιδιωτικότητας και των δεδομένων, η πρακτική υιοθέτηση και εφαρμογή των σχετικών τεχνολογιών παραμένει περιορισμένη. Για τον λόγο αυτό, προτείνονται συγκεκριμένες ενέργειες που μπορούν να συμβάλουν στη βελτίωση της αποδοχής και της εμπιστοσύνης των πολιτών απέναντι στην κρυπτογράφηση.

Πρώτον, απαιτείται ενίσχυση της ενημέρωσης και της εκπαίδευσης των πολιτών σχετικά με τις βασικές αρχές και τα οφέλη της κρυπτογράφησης. Η πλειονότητα των χρηστών διαθέτει θεωρητική γνώση για την έννοια της ασφάλειας, ωστόσο δεν κατανοεί πλήρως τη λειτουργία της. Μέσα από στοχευμένες δράσεις ενημέρωσης, εκπαιδευτικά προγράμματα, σεμινάρια και καμπάνιες ευαισθητοποίησης, μπορεί να ενισχυθεί η εμπιστοσύνη προς τις ψηφιακές υπηρεσίες που χρησιμοποιούν τέτοιες τεχνολογίες.

Δεύτερον, η απλοποίηση των διαδικασιών ασφάλειας αποτελεί κρίσιμο παράγοντα αποδοχής. Οι περίπλοκες ρυθμίσεις ασφαλείας και οι διαδικασίες ταυτοποίησης συχνά λειτουργούν αποτρεπτικά για τους χρήστες. Η ανάπτυξη φιλικών προς τον χρήστη συστημάτων, όπου η κρυπτογράφηση εφαρμόζεται αυτόματα και χωρίς να απαιτείται τεχνική γνώση, μπορεί να αυξήσει τη διάδοση και χρήση των υπηρεσιών αυτών.

Επιπλέον, η ενίσχυση της διαφάνειας και της επικοινωνίας των μέτρων ασφάλειας από πλευράς οργανισμών και επιχειρήσεων είναι απαραίτητη. Οι χρήστες πρέπει να ενημερώνονται με σαφή και κατανοητό τρόπο για τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται, ώστε να αισθάνονται εμπιστοσύνη στη διαχείριση των δεδομένων τους.

Μια ακόμη σημαντική πτυχή είναι η ενσωμάτωση της εκπαίδευσης σε θέματα κυβερνοασφάλειας και κρυπτογράφησης στην τυπική εκπαίδευση. Η εισαγωγή σχετικών μαθημάτων σε σχολεία και πανεπιστήμια θα συμβάλει στη μακροπρόθεσμη καλλιέργεια ψηφιακής κουλτούρας και υπεύθυνης χρήσης τεχνολογιών.

Παράλληλα, προτείνεται η παροχή κινήτρων προς επιχειρήσεις και οργανισμούς που εφαρμόζουν σύγχρονες μεθόδους κρυπτογράφησης, όπως πιστοποιήσεις, αναγνώριση ή οικονομικά οφέλη. Με τον τρόπο αυτό ενισχύεται η διάδοση καλών πρακτικών και δημιουργείται ένα περιβάλλον εμπιστοσύνης μεταξύ φορέων και χρηστών.

Τέλος, η συνεχής αξιολόγηση και επικαιροποίηση των πολιτικών ασφάλειας είναι αναγκαία για την αντιμετώπιση των ταχέως εξελισσόμενων κυβερνοαπειλών. Η συνεργασία μεταξύ κρατικών φορέων, ακαδημαϊκών ιδρυμάτων και ιδιωτικού τομέα μπορεί να εξασφαλίσει τη διατήρηση υψηλών προτύπων προστασίας και να ενισχύσει την κοινωνική αποδοχή των τεχνολογιών κρυπτογράφησης.

Συνοψίζοντας, η αποδοχή της κρυπτογράφησης δεν εξαρτάται μόνο από την τεχνολογική της αποτελεσματικότητα, αλλά κυρίως από τον βαθμό κατανόησης, εμπιστοσύνης και ευκολίας χρήσης που απολαμβάνει από το κοινό. Μια συντονισμένη στρατηγική εκπαίδευσης, διαφάνειας και απλοποίησης μπορεί να οδηγήσει σε ευρύτερη αξιοποίηση των τεχνολογιών αυτών και σε ουσιαστική ενίσχυση της ψηφιακής ασφάλειας των πολιτών.

7.3 Μελλοντικές Κατευθύνσεις Έρευνας

Η παρούσα μελέτη ανέδειξε σημαντικές πτυχές της στάσης και της αντίληψης των χρηστών απέναντι στις τεχνολογίες κρυπτογράφησης, ωστόσο αφήνει ανοιχτά πεδία για περαιτέρω διερεύνηση. Οι μελλοντικές κατευθύνσεις έρευνας μπορούν να κινηθούν σε πολλαπλά επίπεδα, εστιάζοντας τόσο σε τεχνικές όσο και σε κοινωνικές διαστάσεις του ζητήματος.

Πρώτον, προτείνεται η διεύρυνση του δείγματος σε μεγαλύτερο και περισσότερο αντιπροσωπευτικό πληθυσμό, ώστε να ενισχυθεί η αξιοπιστία των ευρημάτων. Η ενσωμάτωση χρηστών διαφορετικών ηλικιακών ομάδων, μορφωτικών επιπέδων και επαγγελματικών τομέων θα προσέφερε μια πιο ολοκληρωμένη εικόνα για τους παράγοντες που επηρεάζουν την αποδοχή της κρυπτογράφησης.

Δεύτερον, θα ήταν ιδιαίτερα χρήσιμη η ποιοτική διερεύνηση των αντιλήψεων μέσω συνεντεύξεων ή ομάδων εστίασης (focus groups). Μια τέτοια προσέγγιση θα επέτρεπε την εις βάθος κατανόηση των κινήτρων, των φόβων και των παρερμηνειών που συνδέονται με τη χρήση κρυπτογραφικών τεχνολογιών.

Τρίτον, μπορεί να εξεταστεί η συσχέτιση της γνώσης και της στάσης απέναντι στην κρυπτογράφηση με πραγματικές συμπεριφορές χρήσης. Η μελέτη της απόστασης ανάμεσα στην πρόθεση και στην πράξη (intention–behavior gap) θα μπορούσε να αποκαλύψει εμπόδια που εμποδίζουν τους χρήστες να εφαρμόσουν πρακτικά μέτρα ασφάλειας, ακόμη κι αν τα θεωρούν σημαντικά.

Μια ακόμη κατεύθυνση αφορά τη διερεύνηση της σχέσης μεταξύ εμπιστοσύνης στις ψηφιακές υπηρεσίες και διαφάνειας των παρόχων. Η μελέτη του τρόπου με τον οποίο η σαφής ενημέρωση για τα μέτρα ασφάλειας επηρεάζει την αποδοχή των χρηστών, θα μπορούσε να προσφέρει χρήσιμα ευρήματα για την ανάπτυξη πιο αποτελεσματικών στρατηγικών επικοινωνίας.

Επιπλέον, η συγκριτική ανάλυση μεταξύ χωρών ή πολιτισμικών πλαισίων θα μπορούσε να αναδείξει πώς διαφορετικές κοινωνικές αντιλήψεις, επίπεδα ψηφιακής ωριμότητας και νομοθετικές ρυθμίσεις επηρεάζουν τη στάση απέναντι στην κρυπτογράφηση.

Τέλος, η μελλοντική έρευνα μπορεί να επεκταθεί στην αξιολόγηση της αποτελεσματικότητας εκπαιδευτικών παρεμβάσεων σχετικά με την ασφάλεια και την κρυπτογράφηση. Μέσα από πιλοτικά προγράμματα εκπαίδευσης σε σχολεία, πανεπιστήμια ή οργανισμούς, θα μπορούσε να μετρηθεί η μεταβολή στην κατανόηση, τη στάση και τη συμπεριφορά των συμμετεχόντων.

Συνολικά, η περαιτέρω μελέτη του πεδίου μπορεί να συμβάλει ουσιαστικά στη διαμόρφωση πολιτικών και πρακτικών που θα ενισχύσουν την εμπιστοσύνη, την κατανόηση και τη χρήση των τεχνολογιών κρυπτογράφησης σε ένα ολοένα πιο απαιτητικό ψηφιακό περιβάλλον.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1) Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of information security awareness level: A case study of digital wallet users. IOP Conference Series: Materials Science and Engineering, 1077(1), 012003. https://doi.org/10.1088/1757-899X/1077/1/012003
2) Andress, J. (2011). The basics of information security: Understanding the fundamentals of infosec in theory and practice. Elsevier.
3) Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security, 68, 145–159.
4) Edmondson, D. R. (2005). Likert scales: A history. Conference on Historical Analysis and Research in Marketing, 127–133.
5) Fakeh, S. K. W., Zulhemay, M. N., Shahibi, M. S., Ali, J., & Zaini, M. K. (2012). Information security awareness amongst academic librarians. Journal of Applied Sciences Research, 8(3), 1723–1735.
6) Jakarta Post. (2019). Risks of using VPN and why it’s difficult to stop. Retrieved from https://www.thejakartapost.com
7) Kruger, H. A., & Kearney, D. W. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296.
8) Nugroho, A. (2020). Three attacks used to break digital wallets. Cyberthreat.id. Retrieved from https://cyberthreat.id
9) Ogutcu, G., Testik, Ö. Z., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. Computers & Security, 56, 83–93.
10) Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security, 42, 165–176.
11) Rahman, A. (2013). Randomized random sampling with an inverse-transform random variate generator approach based on the hypergeometric distribution. Seminar Nasional TEKNOIN, 4, 106–111.
12) Saaty, T. L. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1), 83–98.

13) Saaty, T. L., & Vargas, L. G. (2012). Models, methods, concepts & applications of the analytic hierarchy process (2nd ed.). Springer.

14) Schmidt, K., Aumann, I., Hollander, I., Damm, K., & von der Schulenburg, J. M. G. (2015). Applying the analytic hierarchy process in healthcare research: A systematic literature review and evaluation of reporting. BMC Medical Informatics and Decision Making, 15, 112.

15) Fadhilah, A. L. et al. (2021). Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users. IOP Conference Series: Materials Science and Engineering, 1077(1), 012003.

16) Bergmann, M. (2009). Testing Privacy Awareness. In: The Future of Identity, IFIP AICT 298, pp. 237–253.

17) https://www.techtarget.com/searchsecurity/quiz/Quiz-Security-awareness-for-end-users

18) https://dspace.uowm.gr/xmlui/bitstream/handle/123456789/2619/meleti_methodwn_asfaleias_iatrikwn_dedomenwn.pdf?sequence=1

19) http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/2633/cse_39095.pdf?sequence=5&isAllowed=y

20) https://nemertes.library.upatras.gr/server/api/core/bitstreams/0b73d93e-2987-42c5-a16b-8310da7ca3bf/content

21) https://hellanicus-api.lib.aegean.gr/server/api/core/bitstreams/ae4215ed-245e-454d-a0b9-bcab2c9cce2b/content

22) Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of information security awareness level: A case study of digital wallet users. IOP Conference Series: Materials Science and Engineering, 1077(1), 012003. https://doi.org/10.1088/1757-899X/1077/1/012003

23) Andress, J. (2011). The basics of information security: Understanding the fundamentals of infosec in theory and practice. Elsevier.

24) Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users. IOP Conference Series: Materials Science and Engineering, 1077, 012003. https://doi.org/10.1088/1757-899X/1077/1/012003

25) Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users'

non-compliance with information security policies in banks. Computers & Security, 68, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

26) Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

27) Bergmann, M. (2009). Testing privacy awareness. In V. Matyáš, S. Fischer-Hübner, D. Cvrček, & P. Švenda (Eds.), The Future of Identity in the Information Society (IFIP AICT, Vol. 298, pp. 237–253). Springer. https://doi.org/10.1007/978-3-642-03315-5_18

28) Fadhilah, A. L., Ruldeviyani, Y., Prakoso, R., & Arisya, K. F. (2021). Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users. IOP Conference Series: Materials Science and Engineering, 1077, 012003. https://doi.org/10.1088/1757-899X/1077/1/012003

29) Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

30) Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

[Οπισθόφυλλο. Κενή σελίδα]