2026-01

þÿ ‘ ¯ Ã ¸ · ¼ ± ± Ã Æ ¬ » µ ¹ ± Â º ± ¹ µ ¼ À ¹ Â

þÿ Ä É ½ À µ » ± Ä Î ½ Ä Á ± À µ ¶ Î ½ Ã Ä ¹ Â

þÿ · » µ º Ä Á ¿ ½ ¹ º - Â Ã Å ½ ± » » ± ³ - Â : ‘ ½

þÿ Ä É ½ ´ · ¼ ¿ ³ Á ± Æ ¹ º Î ½ À ± Á ± ³ Ì ½ Ä É

þÿ ± À ± ² » ± Ã Ì À ¿ Å » ¿ Â , ‘ ¹ ¼ ¯ » ¹ ¿ Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± Ã Ä · ½ • ³ º » · ¼ ± Ä ¿ » ¿ ³ ¹ º ® › ¿ ³ ¹ Ã Ä ¹ º ® º ± ¹ Ä ± § Á · ¼ ±
þÿ £ Ç ¿ » ® Ÿ ¹ º ¿ ½ ¿ ¼ ¹ º Î ½ • À ¹ Ã Ä · ¼ Î ½ º ± ¹ ” ¹ ¿ ¯ º · Ã · Â , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â

Πανεπιστήμιο Νεάπολις Πάφος

Σχολή Οικονομικών, Διοίκησης και Πληροφορικής
Τμήμα Λογιστικής και Χρηματοοικονομικών
Πρόγραμμα Μεταπτυχιακών Σπουδών στην Εγκληματολογική Λογιστική

Αίσθημα ασφάλειας και εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές: Ανάλυση των δημογραφικών παραγόντων

Αιμίλιος Παπαβλασόπουλος

Ιανουάριος, 2026

Σχολή Οικονομικών, Διοίκησης και Πληροφορικής
Τμήμα Λογιστικής και Χρηματοοικονομικών
Πρόγραμμα Μεταπτυχιακών Σπουδών στην Εγκληματολογική Λογιστική

Αίσθημα ασφάλειας και εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές: Ανάλυση των δημογραφικών παραγόντων

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση
Μεταπτυχιακού τίτλου σπουδών
στο Πανεπιστήμιο Νεάπολις Πάφος

Αιμίλιος Παπαβλασόπουλος

Ιανουάριος, 2026

Πνευματικά δικαιώματα

Περιεχόμενα

Λίστα Πινάκων

Λίστα Διαγραμμάτων

Σελίδα Εγκυρότητας

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας:

Αιμίλιος Παπαβλασόπουλος

Τίτλος Διπλωματικής Εργασίας:

Αίσθημα ασφάλειας και εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές: Ανάλυση των δημογραφικών παραγόντων.

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

Εξεταστική Επιτροπή:

Επιβλέπων Καθηγητές (Πανεπιστήμιο Νεάπολις Πάφος)
Νικόλαος Σαριαννίδης
Σοφία Καραγιαννοπούλου

Μέλος Εξεταστικής Επιτροπής: ……Ανδρονίκη Καταραχιά

Μέλος Εξεταστικής Επιτροπής: ……Ηλέκτρα Πιτόσκα

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Ο Αιμίλιος Παπαβλασόπουλος γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Αίσθημα ασφάλειας και εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές: Ανάλυση των δημογραφικών παραγόντων», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

ΟΔηλών

Αιμίλιος Παπαβλασόπουλος

Περίληψη

Με την εξέλιξη της τεχνολογίας, η χρήση των ηλεκτρονικών συναλλαγών έχει γνωρίσει αξιοσημείωτη άνοδο. Η εξέλιξη της ασύρματης τεχνολογίας και του Διαδικτύου έχει δημιουργήσει νέες δυνατότητες, συμβάλλοντας σημαντικά στην ενίσχυση του ηλεκτρονικού εμπορίου και των υπηρεσιών που το συνοδεύουν, όπως οι ηλεκτρονικές πληρωμές, το εμπόριο μέσω κινητών συσκευών, οι ψηφιακές αγορές και άλλες συναφείς εφαρμογές. Τα ηλεκτρονικά συστήματα πληρωμών προσφέρουν έναν αξιόπιστο μηχανισμό για τη μεταφορά χρηματικών ποσών και ταυτόχρονα λειτουργούν ως καταλύτες για την τεχνολογική πρόοδο στον χρηματοοικονομικό τομέα (Poudel et al., 2023). Ωστόσο, η ραγδαία ανάπτυξη των ηλεκτρονικών τραπεζικών υπηρεσιών συνοδεύεται από νέες προκλήσεις, μεταξύ των οποίων ξεχωρίζει το ζήτημα της ασφάλειας και της εμπιστοσύνης των χρηστών. Η αίσθηση ασφάλειας και η εμπιστοσύνη αποτελούν βασικά ψυχολογικά προαπαιτούμενα για την αποδοχή και συνεχή χρήση των ψηφιακών υπηρεσιών (Yousafzai et al., 2009). Σε ένα περιβάλλον όπου οι κυβερνοεπιθέσεις και η παραβίαση προσωπικών δεδομένων αυξάνονται, η εμπιστοσύνη προς την τεχνολογία γίνεται κρίσιμη (Kim et al., 2008).

Ειδικά στην ελληνική πραγματικότητα, όπου η μετάβαση στην ψηφιακή τραπεζική πραγματοποιήθηκε εν μέρει επιτακτικά λόγω των capital controls και της πανδημίας, η ανάγκη κατανόησης των παραγόντων που ενισχύουν ή μειώνουν την εμπιστοσύνη είναι πιο επίκαιρη από ποτέ (Kitsios & Kamariotou, 2019). Επιπλέον, η μελέτη των δημογραφικών παραγόντων συμβάλλει στην αναγνώριση διαφοροποιήσεων μεταξύ πληθυσμιακών ομάδων και στην ανάπτυξη στοχευμένων στρατηγικών εμπιστοσύνης και ασφάλειας (Pikkarainen et al., 2004).

Στο πλαίσιο αυτό, σκοπός της έρευνας είναι η διερεύνηση του αισθήματος ασφάλειας και της εμπιστοσύνης που διαθέτουν οι πελάτες τραπεζών όταν πραγματοποιούν ηλεκτρονικές συναλλαγές, καθώς και η εξέταση της επίδρασης των δημογραφικών χαρακτηριστικών στις δύο αυτές μεταβλητές. Η χρήση ψηφιακών τραπεζικών υπηρεσιών έχει αυξηθεί ραγδαία, ειδικά μετά την πανδημία COVID-19, ενισχύοντας την ανάγκη για κατανόηση των ψυχολογικών και κοινωνικών παραγόντων που επηρεάζουν τη χρήση τους.

Λέξεις – κλειδιά: ηλεκτρονικές συναλλαγές, ασφάλεια, απάτη, τραπεζικό σύστημα

Abstract

With the development of technology, the use of electronic transactions has experienced a remarkable increase. The development of wireless technology and the Internet has created new possibilities, significantly contributing to the strengthening of electronic commerce and the services that accompany it, such as electronic payments, commerce via mobile devices, digital markets and other related applications. Electronic payment systems offer a reliable mechanism for the transfer of funds and at the same time act as catalysts for technological progress in the financial sector (Poudel et al., 2023). However, the rapid development of electronic banking services is accompanied by new challenges, among which the issue of security and user trust stands out. The sense of security and trust are key psychological prerequisites for the acceptance and continued use of digital services (Yousafzai et al., 2009). In an environment where cyberattacks and personal data breaches are increasing, trust in technology is becoming critical (Kim et al., 2008).

Especially in the Greek reality, where the transition to digital banking was partly driven by capital controls and the pandemic, the need to understand the factors that enhance or reduce trust is more relevant than ever (Kitsios & Kamariotou, 2019). Furthermore, the study of demographic factors contributes to the identification of differences between population groups and the development of targeted trust and security strategies (Pikkarainen et al., 2004).

In this context, the purpose of the research is to investigate the sense of security and trust that bank customers have when making electronic transactions, as well as to examine the effect of demographic characteristics on these two variables. The use of digital banking services has increased rapidly, especially after the COVID-19 pandemic, reinforcing the need to understand the psychological and social factors that influence their use.

Keywords: electronic transactions, security, fraud, banking system

Εισαγωγή

Η ασφάλεια και η προστασία των προσωπικών δεδομένων αποτελεί κεντρικό άξονα στη λειτουργία των ψηφιακών συναλλαγών. Ο τρόπος με τον οποίο οι χρήστες αντιλαμβάνονται ζητήματα που αφορούν την ασφάλεια και το απόρρητο, διαδραματίζει καθοριστικό ρόλο στην απόφασή τους να κάνουν χρήση τέτοιων υπηρεσιών. Επομένως, η υποκειμενική αντίληψη της ευκολίας χρήσης και της χρησιμότητας των ηλεκτρονικών συναλλαγών ασκεί σημαντική επιρροή στην πρόθεση υιοθέτησής της.

Οι ανησυχίες των καταναλωτών σχετικά με την ασφάλεια των συστημάτων συνιστούν σημαντικό ανασταλτικό παράγοντα για την ανάπτυξη των ηλεκτρονικών συναλλαγών (Orni et al., 2004). Κατά τη συμμετοχή τους σε διαδικτυακές δραστηριότητες και ηλεκτρονικές συναλλαγές, οι χρήστες εμφανίζουν αυξημένη ανησυχία αναφορικά με ζητήματα ασφαλείας (Zhou, 2011). Όπως αναφέρουν οι Gervey και Lin (2000), η ασφάλεια αποτελεί έναν από τους παράγοντες που επηρεάζουν τη διάθεση των καταναλωτών να εμπιστευτούν τις ηλεκτρονικές πληρωμές. Τα ευρήματα του Lim (2003) επισημαίνουν ότι η ύπαρξη ή η αίσθηση ασφάλειας μπορεί να προκαλέσει ανησυχίες σχετικές με την εμπιστοσύνη, ενώ η ασφάλεια φαίνεται να λειτουργεί ως διαμεσολαβητικός παράγοντας ανάμεσα στην εμπιστοσύνη και την πρόθεση, προωθώντας έτσι μια συμπεριφορά βασισμένη στην εμπιστοσύνη, όταν συνυπάρχουν και οι δύο αυτοί παράγοντες. Παρότι έχουν αναπτυχθεί προηγμένοι μηχανισμοί ασφάλειας, σύμφωνα με τους Suh και Han (2003), οι καταναλωτές εξακολουθούν να εκφράζουν επιφυλάξεις ως προς τη χρήση του διαδικτύου για τραπεζικές συναλλαγές. Η έρευνα των Kumar et al. (2012) αναδεικνύει ότι η αντίληψη των καταναλωτών για την ασφάλεια των ηλεκτρονικών τραπεζικών υπηρεσιών ενισχύει τη θεσμική εμπιστοσύνη και ενθαρρύνει την αποδοχή τους.

Η φύση του κινδύνου που εμπεριέχουν οι ηλεκτρονικές συναλλαγές καθιστά δύσκολη την οικοδόμηση εμπιστοσύνης από την πλευρά των χρηστών. Η εμπιστοσύνη αναδεικνύεται ως βασικός παράγοντας που επηρεάζει την πρόθεση των καταναλωτών να αξιοποιήσουν τις ηλεκτρονικές υπηρεσίες πληρωμών, ενώ έχει διαπιστωθεί ότι άτομα με υψηλά επίπεδα εμπιστοσύνης είναι πιο πιθανό να υιοθετήσουν τις σχετικές τεχνολογίες (Kim et al., 2010). Επιπλέον, η βιβλιογραφία αναδεικνύει θετική συσχέτιση μεταξύ εμπιστοσύνης και υιοθέτησης του ηλεκτρονικού εμπορίου, καθώς και των πληρωμών μέσω φορητών συσκευών. Ωστόσο, παραμένει σε μεγάλο βαθμό αδιευκρίνιστο το πώς

ακριβώς διαμορφώνεται η εμπιστοσύνη και ποιοι παράγοντες συμβάλλουν ουσιαστικά στην ενίσχυσή της.

Η παρούσα εργασία στηρίζεται σε έξι κεφάλαια με το πρώτο να αναφέρεται γενικά στις ηλεκτρονικές τραπεζικές υπηρεσίες, ενώ το δεύτερο εμβαθύνει στην έννοια της ασφάλειας των ηλεκτρονικών συναλλαγών. Το τρίτο κεφάλαιο σχετίζεται με τις προσκλήσεις και τους κινδύνους που εντοπίζονται στις ηλεκτρονικές συναλλαγές. Έπειτα, το ερευνητικό σκέλος της εργασίας ξεκινά με το τέταρτο κεφάλαιο στο οποίο παρουσιάζεται η ταυτότητα της έρευνας. Εντός του κεφαλαίου εντοπίζονται πληροφορίες για τον σκοπό της έρευνας, τον τύπο της, το δείγμα, αλλά και το μέσο συλλογής δεδομένων. Έπειτα, ακολουθούν πληροφορίες για την ερευνητική διαδικασία, την ανάλυση των δεδομένων, τα ηθικά ζητήματα και το κεφάλαιο ολοκληρώνεται με την αναφορά στους περιορισμούς της έρευνας. Στο επόμενο κεφάλαιο, παρουσιάζονται τα αποτελέσματα της έρευνας τα οποία σχεδιάστηκαν για να απαντηθούν τα αντίστοιχα ερευνητικά ερωτήματα και περιλαμβάνουν σημαντικά ευρήματα περιγραφικής και επαγωγικής στατιστικής. Τέλος, ακολουθεί το κεφάλαιο των συμπερασμάτων το οποίο στηρίζεται στα στατιστικά ευρήματα σε συνάρτηση με το θεωρητικό υπόβαθρο της εργασίας.

Κεφάλαιο 1ο: Οι ηλεκτρονικές Τραπεζικές Υπηρεσίες

1.1 Ηλεκτρονικές Τραπεζικές Υπηρεσίες (e-banking) και νέες τεχνολογίες

Η εξέλιξη της τεχνολογίας και η επέκταση των υπηρεσιών που προσφέρονται μέσω Διαδικτύου έχει επιτρέψει σε οργανισμούς και πελάτες να ανακαλύψουν μοναδικούς τρόπους επικοινωνίας, επηρεάζοντας σημαντικά τον τραπεζικό κλάδο και δημιουργώντας τις ηλεκτρονικές τραπεζικές υπηρεσίες (e – banking). Μέσω των ηλεκτρονικών υπηρεσιών, οι τράπεζες προσφέρουν στους πελάτες ευκολία πρόσβασης ανά πάσα στιγμή και από οπουδήποτε, σε σημείο που πλέον μεγαλύτερο βάρος ανάπτυξης δίνεται στα ψηφιακά κανάλια και όχι στα φυσικά καταστήματα των τραπεζών (Groenfeldt, 2014). Οι ηλεκτρονικές τραπεζικές υπηρεσίες μειώνουν το κόστος που σχετίζεται με την αποστολή έντυπων καταστάσεων και εξαλείφουν την ανάγκη για προσωπικές αλληλεπιδράσεις στα υποκαταστήματα, ενώ οι πελάτες δεν χρειάζεται πλέον να περιμένουν το ωράριο λειτουργίας των τραπεζών ή να υπομένουν μεγάλες τηλεφωνικές ουρές για να επικοινωνήσουν με έναν εκπρόσωπο τράπεζας. Επίσης, έχουν εισαχθεί νέοι τρόποι πληρωμής, όπως μετρητά, χρεωστικές κάρτες, πιστωτικές κάρτες, κινητά πορτοφόλια, ηλεκτρονικά πορτοφόλια και άμεσες χρεώσεις (Ungratwar, Sharma&Kumar, 2025).

Τις τελευταίες δεκαετίες, το παγκόσμιο χρηματοπιστωτικό σύστημα υπέστη σημαντικές αλλαγές λόγω διαφόρων παραγόντων, όπως η παγκοσμιοποίηση της αγοράς, η ανάπτυξη των τεχνολογιών πληροφοριών και επικοινωνιών και η απελευθέρωση των χρηματοπιστωτικών αγορών. Αυτές οι αλλαγές έχουν συμβάλλει στον πλήρη μετασχηματισμό του χρηματοπιστωτικού περιβάλλοντος, δίνοντας έμφαση στον τεχνολογικό τομέα. Στο πλαίσιο αυτό, λοιπόν, αναπτύχθηκε η ηλεκτρονική τραπεζική, τα ηλεκτρονικά συστήματα πληρωμών, τα πιστωτικά γραφεία και η FinTech. Ο όρος FinTech δεν έχει ακόμη έναν ενιαίο ορισμό λόγω του γεγονότος ότι χρησιμοποιείται για να δηλώσει διαδικασίες που χαρακτηρίζονται από ταχεία ανάπτυξη και συνεχείς μετασχηματισμούς (Shmuratko&Sheludko, 2019). Σύμφωνα με τον Schueffel (2016), ηFinTech ορίζεται ως μια νέα χρηματοπιστωτική βιομηχανία που χρησιμοποιεί την τεχνολογία για τη βελτίωση της οικονομικής απόδοσης. Επίσης, σύμφωνα με τους Zherdetskaya καιGorodinsky (2017) οι «νεοσύστατες επιχειρήσεις FinTech», χρησιμοποιούν τον συνδυασμό τεχνολογίας, εξυπηρέτησης με επίκεντρο τον πελάτη και ευέλικτων επιχειρηματικών δομών για τη μείωση του κόστους και την αύξηση του πελατολόγιου τους.

Τα τελευταία χρόνια οι τράπεζες εισάγουν έναν αυξανόμενο αριθμό καινοτόμων προϊόντων και υπηρεσιών που, εκ φύσεως, ταιριάζουν με τους παραπάνω ορισμούς, καθώς ολοένα και περισσότερο αξιοποιούν τις τεχνολογικές εξελίξεις, αποσκοπώντας στη βελτίωση των χρηματοπιστωτικών υπηρεσιών. Πιο συγκεκριμένα, αναφέρεται η ανάπτυξη των τεχνολογιών πληροφοριών, με έμφαση στην ταχύτητα επεξεργασίας και μετάδοσης πληροφοριών, καθώς και στη χρήση νέου λογισμικού. Παράλληλα, τα τραπεζικά ιδρύματα αναζητούν τρόπους για την ενσωμάτωση καινοτομιών για την ικανοποίηση των αυξανόμενων αναγκών των χρηστών όσον αφορά την ταχύτητα, την ποικιλομορφία και το κόστος των παρεχόμενων υπηρεσιών (Shmuratko&Sheludko, 2019).

Ο τραπεζικός κλάδος στη σύγχρονη εποχή ενσωματώνει ένα πλήθος καινοτόμων τεχνολογιώνπου ονομάζονται e-finance, συνοψίζονται στην παροχή τραπεζικών υπηρεσιών μέσω ηλεκτρονικών καναλιών επικοινωνίας. Υπάρχουν πολλά τέτοια κανάλια, όπως τα αυτοματοποιημένα τηλεφωνικά κέντρα, τα ATM, το Internet και mobilebanking. Με την εισαγωγή των τεχνολογικών επιτευγμάτων, το εύρος των υπηρεσιών που παρέχονται στον πελάτη μέσω ενός ATM έχει αυξηθεί σημαντικά την τελευταία δεκαετία. Επίσης, με την ραγδαία αύξηση της χρήσης των smartphone και του ηλεκτρονικού υπολογιστή διάδοση, οι τράπεζες ανέπτυξαν τις ηλεκτρονικές τους υπηρεσίες μέσω Διαδικτύου. Οι πελάτες των τραπεζών που χρησιμοποιούν κινητές συσκευές αλληλεπιδρούν με την τράπεζα 3,5 φορές πιο συχνά από τους χρήστες της παραδοσιακής ηλεκτρονικής τραπεζικής (Bonsetal, 2012).

Επιπρόσθετα, μία ακόμη σύγχρονη τεχνολογική καινοτομία που διέπει τη λειτουργία των τραπεζών είναι το blockchain, το οποίο είναι μια πολυλειτουργική και πολυεπίπεδη τεχνολογία πληροφοριών που έχει σχεδιαστεί για να προσφέρει αξιόπιστες πληροφορίες για διάφορα περιουσιακά στοιχεία. Χάρη στα οικονομικά, πολιτικά, ανθρωπιστικά και νομικά πλεονεκτήματά του, το blockchain έχει μετατραπεί σε μια ισχυρή καινοτομία που μπορεί να αλλάξει ριζικά το μεγαλύτερο μέρος των πτυχών της λειτουργίας της κοινωνίας. Η πρακτική εφαρμογή αυτής της τεχνολογίας έχει ποικίλα πλεονεκτήματα, τα οποία διασφαλίζουν τις συναλλαγές μέσω του e–banking (Shmuratko&Sheludko, 2019).

1.2 Ιστορική εξέλιξη και ανάπτυξη του e-banking

Από τα τέλη της δεκαετίας του 1990, η ηλεκτρονική τραπεζική (e-Banking) έχει εξελιχθεί σε πολύ μεγάλο βαθμό με δεκάδες εκατομμύρια χρήστες παγκοσμίως (OECD, 2001). Ωστόσο, η ηλεκτρονική τραπεζική είναι προϊόν διαφορετικών γενεών ηλεκτρονικών συναλλαγών. Το τρέχον διαδικτυακό διαδίκτυο ή e-Banking είναι το τελευταίο στάδιο μιας

εξελικτικής πορείας πολλών ετών. Οι αυτόματες ταμειακές μηχανές (ATM) ήταν οι πρώτες γνωστές μηχανές που παρείχαν ηλεκτρονική πρόσβαση στους πελάτες, ενώ στη συνέχεια κυριάρχησε η τηλεφωνική τραπεζική, κατά την οποία, οι χρήστες είχαν τη δυνατότητα να καλέσουν το σύστημα υπολογιστών της τράπεζάς τους από το συνηθισμένο τους τηλέφωνο και να χρησιμοποιήσουν το πληκτρολόγιο του τηλεφώνου για να πραγματοποιήσουν τραπεζικές συναλλαγές (Mia, Rahman&Uddin, 2007).

Οι τραπεζικές συναλλαγές μέσω υπολογιστή (PC banking) αντικατέστησαν τις τηλεφωνικές τραπεζικές συναλλαγές και επέτρεψαν στους χρήστες να αλληλεπιδρούν με την τράπεζά τους μέσω ενός υπολογιστή με σύνδεση dial-upmodem στο τηλεφωνικό δίκτυο. Μετά από αυτές τις γενιές, η Deutsche Bank ξεκίνησε το πρώτο έργο διαδικτυακής τραπεζικής στη Λατινική Αμερική το 1996 και η Citibank ανέπτυξε ένα ειδικό «ηλεκτρονικό κιτ εργαλείων» σε όλα τα υποκαταστήματά της παγκοσμίως (UNCTAD, 2002). Η ηλεκτρονική τραπεζική χρησιμοποιεί το Διαδίκτυο για τη διεπαφή χρήστη και για τη μεταφορά δεδομένων και τη λήψη λογισμικού, και έτσι έχει τη δυνατότητα να μειώσει το κόστος συντήρησης. Για τους χρήστες, η ηλεκτρονική τραπεζική παρέχει ενημερωμένες πληροφορίες, 24ωρη πρόσβαση σε τραπεζικές υπηρεσίες. Οι κύριες υπηρεσίες που παρέχονται από τις ηλεκτρονικές τράπεζες είναι η μεταφορά χρημάτων μεταξύ των λογαριασμών, η πληρωμή λογαριασμών και ο έλεγχος υπολοίπων λογαριασμών. Δάνεια, χρηματιστηριακές συναλλαγές, συναλλαγές μετοχών, ομαδοποίηση υπηρεσιών και μια σειρά από άλλες χρηματοοικονομικές υπηρεσίες προστίθενται σε αυτές τις «κύριες υπηρεσίες» (Mia, Rahman&Uddin, 2007).

Η ηλεκτρονική τραπεζική χρησιμοποιείται ευρέως, μεταξύ άλλων, στις σκανδιναβικές χώρες. Το 2001, η ηλεκτρονική τραπεζική (E-Banking) χρησιμοποιούνταν από περισσότερο από το 25% του πληθυσμού στη Νορβηγία, τη Σουηδία και τη Φινλανδία, και από το 15% του πληθυσμού στη Δανία (OECD, 2001). Το 2004, η χρήση της ηλεκτρονικής τραπεζικής στη Δανία αυξήθηκε στο 45%. Ο Nair (1999) επεσήμανε ότι η ηλεκτρονική τραπεζική έγινε γρήγορα στρατηγική αναγκαιότητα για τις περισσότερες εμπορικές τράπεζες, καθώς ο ανταγωνισμός αυξανόταν συνεχώς από τις ιδιωτικές τράπεζες και τα μη χρηματοπιστωτικά ιδρύματα.

Με τη σταδιακή εξάπλωση του Διαδικτύου και των ασύρματων τεχνολογιών επικοινωνίας, όλα τα καθιερωμένα τραπεζικά ιδρύματα που λειτουργούν στην Ελλάδα έχουν αναπτύξει και προσφέρουν υπηρεσίες διαδικτυακής τραπεζικής στους πελάτες τους. Αυτό το γεγονός είναι άρρηκτα συνδεδεμένο με την ραγδαία ανάπτυξη της τεχνολογίας και την παράλληλη ανάπτυξη του διαδικτύου σε κάθε χώρα και γεωγραφική ήπειρο. Οι

προσφερόμενες τραπεζικές υπηρεσίες αποτελούσαν, σχεδόν μέχρι τα τέλη της δεκαετίας του 1990, πόλο έλξης, ιδιαίτερης προσοχής και χρησιμότητας μεταξύ των πελατών των χρηματοπιστωτικών ιδρυμάτων διεθνώς, τόσο ιδιωτών όσο και επιχειρήσεων (Mylonakis, Orfanos&Evripiotis, 2024).

Στο ελληνικό τραπεζικό σύστημα, ο αριθμός των εγχώριων τραπεζικών ιδρυμάτων μειώθηκε δραστικά από 35 το 2009 σε 13 το 2023, εκ των οποίων 9 εμπορικές και 4 συνεταιριστικές τράπεζες. Τα 9 εμπορικά τραπεζικά ιδρύματα λειτουργούν 405 καταστήματα και απασχολούν 28.436 υπαλλήλους τραπεζών. Όσον αφορά τους ενεργούς χρήστες των ηλεκτρονικών υπηρεσιών στο τέλος του 2023, ήταν εγγεγραμμένοι 3,73 εκατομμύρια ενεργοί χρήστες του internetbanking, εκ των οποίων το 64% πραγματοποίησε τουλάχιστον μία συναλλαγή μεταφοράς χρημάτων κάθε μήνα (Mylonakis, Orfanos&Evripiotis, 2024). Οι χρήστες του internetbanking στην Ελλάδα το 2023 ανήλθαν στο 52,01%, σε αντίθεση με το 13,87% το 2015 (Eurostat, 2024), μια αρκετά μεγάλη πρόοδος σε 8 χρόνια. Αξίζει να σημειωθεί ότι αυτή η αύξηση συνδέεται κυρίως, σε σημαντικό βαθμό, με την επιβολή περιορισμών στην κίνηση κεφαλαίων (28-02-2015), μια αύξηση που παρατηρήθηκε γενικά σε όλους τους τύπους ηλεκτρονικών συναλλαγών.

1.3 Νομοθετικό πλαίσιο

Καθώς αυξάνονται οι τεχνολογικές καινοτομίες στον τραπεζικό τομέα, αυξάνεται παράλληλα και η ζήτηση των χρηστών για νέες και αποδοτικότερες υπηρεσίες. Η ευρεία χρήση των ηλεκτρονικών συναλλαγών έχει οδηγήσει στην ανάγκη ανάπτυξης ενός κανονιστικού πλαισίου για τις διαδικτυακές τραπεζικές συναλλαγές στις ευρωπαϊκές χώρες. Ως εκ τούτου,στην Ευρωπαϊκή Ένωση (ΕΕ) δημιουργήθηκε ένα ενιαίο χρηματοοικονομικό πλαίσιο, το οποίο βελτιώνεται συνεχώς καιλαμβάνει υπόψη τις ανάγκες των παρόχων και των χρηστών των διαδικτυακών τραπεζικών συναλλαγών. Σε επίπεδο ΕΕ, η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) είναι η ενιαία ρυθμιστική αρχή, η οποία ρυθμίζει τις διαδικτυακές τραπεζικές συναλλαγές, ενώ οι συναλλαγές πληρωμών και η χρήση ηλεκτρονικού χρήματος απαιτούν εθνική άδεια και εποπτεύονται από εθνικές ρυθμιστικές αρχές (Kapliar, 2022).

Σε εθνικό επίπεδο κάθε κράτους μέλους της Ευρωπαϊκής Ένωσης, υπάρχουναδειοδοτημένα και εποπτευόμενα ιδρύματα που μπορούν να προσφέρουν τις υπηρεσίες τους, χρησιμοποιώντας το σύστημα διαβατηρίων της ΕΕ. Ωστόσο, η διαδικασία αυτή δημιουργεί κίνδυνο εποπτικού κατακερματισμού ή ακόμη και εποπτικού ανταγωνισμού, ο οποίος είναι ορατός καθώς ο τομέας της fintech επικεντρώνεται σε

συγκεκριμένες υπηρεσίες και αναθέτει σε τρίτους μη βασικά μέρη των δραστηριοτήτων. Έτσι, έχει δημιουργηθεί ένα πολύπλοκο δίκτυο διασυνδεδεμένων χρηματοπιστωτικών ιδρυμάτων, τα οποία δραστηριοποιούνται σε ευρωπαϊκές χώρες, χωρίς όμως να υπάρχει ενιαία εποπτεία από την κεντρική διοίκηση της ΕΕ. Για τηνεπίλυση του παραπάνω ζητήματοςθα πρέπει να εναρμονιστεί το κανονιστικό πλαίσιο, να υπάρχει εποπτεία των πληρωμών και των ιδρυμάτων έκδοσης ηλεκτρονικού χρήματος σε επίπεδο ΕΕ, ώστε να διασφαλίζεται η ευθύνη όλων των φορέων. Τα βασικά έγγραφα σε επίπεδο ΕΕ για την κρατική ρύθμιση των ηλεκτρονικών τραπεζικών συναλλαγών είναι οι Οδηγίες της ΕΕ για τις Υπηρεσίες Πληρωμών (PSD1 2007/64, PSD2 2015/2366).

Σύμφωνα με την PSD2 2015/2366 ενημερώθηκε το υπάρχον κανονιστικό πλαίσιο για τις υπηρεσίες πληρωμών στην ΕΕ και εισήχθησαν ενισχυμένες απαιτήσεις διαφάνειας και ασφάλειας. Η ενημερωμένη Οδηγία για τις Υπηρεσίες Πληρωμών PSD2 2021/1230 εναρμονίζει τους επιχειρηματικούς κανόνες για όλους τους παρόχους υπηρεσιών ηλεκτρονικών πληρωμών σε ολόκληρη την ΕΕ και δημιουργεί ένα κλιμακωτό καθεστώς αδειοδότησης για μη τραπεζικούς παρόχους υπηρεσιών πληρωμών, όπως τα ιδρύματα πληρωμών. Ο κανονισμός 2018/389 της Επιτροπής τέθηκε σε ισχύ στις 14 Σεπτεμβρίου 2019, ορίζοντας μηχανισμούς για συναλλαγές ηλεκτρονικών πληρωμών και ηλεκτρονικές τραπεζικές συναλλαγές, ώστε να διασφαλίζονται υψηλότερα επίπεδα ασφάλειας (Kapliar, 2022).

Σκοπός των ΟδηγιώνPSD1 (2007/64/ΕΚ) και PSD2 (2015/2366) είναι να υπάρχει ισότητα ανταγωνισμού για τους παρόχους υπηρεσιών πληρωμών, να ενισχυθεί η προστασία των καταναλωτών και να υποστηριχθεί η συμμετοχή μη τραπεζικών ιδρυμάτων στις υπηρεσίες πληρωμών. Με την Οδηγία PSD2 ενημερώθηκε το προηγούμενο πλαίσιο προωθώντας την ανοιχτή τραπεζική, ενισχύοντας τη διαφάνεια και επιβάλλοντας αυστηρότερες απαιτήσεις ασφαλείας. Παράλληλα, θεσμοθετήθηκαν σαφείς ορισμοί και υποχρεώσεις για τους συμμετέχοντες στην αγορά, συμπεριλαμβανομένης της Ισχυρής Επαλήθευσης Πελάτη (SCA), των Υπηρεσιών Έναρξης Πληρωμής (PIS), των Υπηρεσιών Πληροφοριών Λογαριασμού (AIS), της Επιβεβαίωσης Διαθεσιμότητας Χρημάτων (COFA) και της ρύθμισης των Τρίτων Παρόχων (TPP). Οι TPP επιτρέπουν νέες καινοτόμες χρηματοοικονομικές υπηρεσίες διατηρώντας παράλληλα αυστηρή εποπτεία από τις εθνικές χρηματοοικονομικές αρχές.

Η Οδηγίας PSD2 άρχισε να εφαρμόζεται τον Σεπτέμβριο του 2019, και παράλληλα η Ευρωπαϊκή Επιτροπή ξεκίνησε την προετοιμασία αναθεωρήσεων, εστιάζοντας στις διαδικασίες ελέγχου ταυτότητας, τις υποχρεώσεις διαφάνειας, τις απαιτήσεις αδειοδότησης

και τους κανόνες πρόσβασης για συστήματα πληρωμών και λογαριασμούς. Ο συνοδευτικός κατ' εξουσιοδότηση κανονισμός (ΕΕ) 2018/389 της Επιτροπής εισήγαγε λεπτομερείς κανόνες για την ασφαλή επικοινωνία, καθιστώντας υποχρεωτική την διπλή επαλήθευση για τις περισσότερες ηλεκτρονικές πληρωμές, ορίζοντας παράλληλα αρκετές εξαιρέσεις χαμηλού κινδύνου (OpenbankingPSD2 regulationintheEU, 2022).

Με το ενημερωμένο PSD2 2021/1230 θεσπίστηκε ένακλιμακωτό καθεστώς εξουσιοδότησης για μη τραπεζικές οντότητες και ενισχύοντας τα πρότυπα διαφάνειας και ασφάλειας σε όλες τις ψηφιακές μεθόδους πληρωμής, με εξαίρεση τα φυσικά μετρητά και τα έντυπα μέσα. Πρόσθετοι κανονισμοί της ΕΕ επηρεάζουν τις ηλεκτρονικές τραπεζικές συναλλαγές, όπως ο κανονισμός της Πολυμερούς Νομισματικής Επιτροπής (MMC) του 2016, ο οποίος περιορίζει τις διατραπεζικές προμήθειες για συναλλαγές με χρεωστικές και πιστωτικές κάρτες και διασφαλίζει τον διαρθρωτικό διαχωρισμό εντός των συστημάτων πληρωμών. Πιο πρόσφατα, ο κανονισμός για τις διασυνοριακές πληρωμές εισήγαγε κανόνες που διέπουν τη μετατροπή νομισμάτων και τα τέλη διασυνοριακών συναλλαγών, ενισχύοντας τον θεμιτό ανταγωνισμό και την προστασία των καταναλωτών σε ολόκληρη την Ευρωπαϊκή Ένωση (Kapliar, 2022).

Κεφάλαιο 2ο: Η έννοια της ασφάλειας στις Ηλεκτρονικές Συναλλαγές

2.1 Η ασφάλεια στο διαδίκτυο

Για πολλά χρόνια, οι πλατφόρμες ηλεκτρονικής τραπεζικής έχουν εφαρμοστεί ως τον πιο αποτελεσματικό τρόπο, μέσω του οποίου μπορούν να πραγματοποιούνται τραπεζικές συναλλαγές άμεσα και χωρίς κόπο.Η ιδέα της ηλεκτρονικής τραπεζικής, σύμφωνα με τον Essinger (1999), είναι: «να δίνει στους πελάτες πρόσβαση στους τραπεζικούς τους λογαριασμούς μέσω ενός ιστότοπου και να τους επιτρέπει να πραγματοποιούν ορισμένες συναλλαγές στον λογαριασμό τους, υπό την προϋπόθεση ότι συμμορφώνονται με αυστηρούς ελέγχους ασφαλείας». Σύμφωνα με τον Leow (1999), οι όροι «PC banking», «online banking», «Internet banking», «telephone banking» ή «mobile banking» αναφέρονται σε διάφορους τρόπους με τους οποίους οι πελάτες μπορούν να έχουν πρόσβαση στις τράπεζές τους χωρίς να χρειάζεται να βρίσκονται φυσικά στο τραπεζικό υποκατάστημα.

Οι πλατφόρμες ηλεκτρονικής τραπεζικής είναι ουσιαστικά εφαρμογές που βασίζονται στο Διαδίκτυο. Για το λόγο αυτό, οι χρήστες αυτών των πλατφόρμων καθίστανταιένας πολύ ελκυστικός και εν μέρει ευάλωτος στόχος για άτομα με κακόβουλες προθέσεις. Η ανάγκη εξάλειψης των επιπτώσεων του ταχέως αναπτυσσόμενου κυβερνοεγκλήματος αποτελεί μια σημαντική πρόκληση για την ηλεκτρονική τραπεζική που απαιτεί περαιτέρω καινοτόμες προσεγγίσεις. Εξάλλου, αν δεν αντιμετωπιστούν έγκαιρα και σωστά προβλήματα τέτοιας φύσεως, οι κίνδυνοι που σχετίζονται με την ασφάλεια μπορούν να προκαλέσουν στις τράπεζες την απώλεια κερδών από την ηλεκτρονική τραπεζική (Nilsson, Adams&Herd, 2005).

Οι κύριοι κίνδυνοι που σχετίζονται με την ηλεκτρονική τραπεζική είναι στρατηγικοί, λειτουργικοί, νομικοί και καλής φήμης του εκάστοτε τραπεζικού ιδρύματος. Είναι χαρακτηριστικό ότι η παραβίαση της ασφάλειας που επιτρέπει την μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες πελατών μπορεί να θεωρηθεί ως ένας βασικός λειτουργικός κίνδυνος ηλεκτρονικού τραπεζικού συστήματος. Επίσης, ένα τέτοιο γεγονός μπορεί να εκθέσειτην εκάστοτε τράπεζα σε νομικό κίνδυνο και κίνδυνο κακής φήμης που μπορεί να της στοιχίσει πελάτες. Προκειμένου να προστατευτούν οι ίδιοι οι καταναλωτές, αλλά και η φήμη της εκάστοτε τράπεζας, θα πρέπει να εκπαιδευτούνοι

πελάτες σχετικά με τους κινδύνους ασφαλείας, τις προφυλάξεις και την ενημέρωση για την χρήση των νέων τεχνολογικών μέσων(Kiljanetal., 2016).

Μελετώντας τους διαφαινόμενους κινδύνους, συνήθως αναφέρονται η κλοπή ταυτότητας, η οποία μπορεί να συμβεί με τη χρήση μιας μη συμβατικής επίθεσης όπως το ηλεκτρονικό ψάρεμα (phishing), την μετάβαση σε ψεύτικους ιστότοπους (pharming), την πλαστογράφηση (spoofing), την καταγραφή κλειδιών (key logging), την καταγραφή οθόνης (screen logging), τους λεγόμενους«δούρειους ίππους» (Trojans horses), καθώς και άλλες περιπτώσεις χρήσης κακόβουλου λογισμικού. Ένα άλλο σημαντικό πρόβλημα έγκειταιστα συστήματα ελέγχου ταυτότητας που χρησιμοποιούνται σήμερα και τα οποία βασίζουν την ανθεκτικότητά τους στις αποφάσεις του τελικού χρήστη, γεγονός που τα καθιστά ευάλωτα σε κυβερνοεπιθέσεις (More&Nalawade, 2015).

Για το λόγο αυτό, κάθε τραπεζικό ίδρυμα που προσφέρει ηλεκτρονικές υπηρεσίες έχει δημοσιεύσει στην ιστοσελίδα του συστάσεις προς τους πελάτες σχετικά με τον τρόπο αύξησης της ασφάλειας κατά την πραγματοποίηση συναλλαγών σε διαδικτυακό περιβάλλον. Οι πελάτες συνήθως αντιλαμβάνονται κινδύνους κατά τη διεξαγωγή διαδικτυακών συναλλαγών, ιδιαίτερα εφόσον οι συναλλαγές αφορούν σε χρήματα. Μια άλλη ανησυχία από την άποψη της ασφάλειας είναι το κενό εμπιστοσύνης, το οποίο αφορά ένα σημαντικό αριθμό πολιτών, που δεν χρησιμοποιούν το Διαδίκτυο στις καθημερινές τους συναλλαγές και ως εκ τούτου, είναι καχύποπτοι για τις τραπεζικές τους συναλλαγές. Από την άλλη, για αυτούς που είναι χρήστες του Διαδικτύου, φαίνεται να είναι ευκολότερο να εμπιστευτούν τις ηλεκτρονικές τραπεζικές συναλλαγές. Ωστόσο, σε κάποιες περιπτώσεις, συνεργαζόμενες με τις τράπεζες εταιρίες που αναλαμβάνουν τη διαχείριση των λειτουργικών συστημάτων, ενδεχομένως να μην είναι επαρκώς ενημερωμένες και η μεταφορά πληροφοριών μεταξύ αυτών και των τραπεζών να αυξάνει τον κίνδυνο ασφάλειας (Nilsson, Adams&Herd, 2005).

Καθώς, λοιπόν, οι κίνδυνοι είναι πολλοί, έχουν αναπτυχθεί ποικίλα καινοτόμα σχέδια, τα οποία μπορούν να εφαρμοστούν για την επίλυση των προβλημάτων ασφάλειας. Εξάλλου, η βασική ανάγκη για ένα έξυπνο τραπεζικό σύστημα είναι απαραίτητη για να έχουν οι άνθρωποι εμπιστοσύνη στην προσβασιμότητα του λογαριασμού τους και στην ασφάλεια του απορρήτου τους. Ωστόσο,μερικές φορές είναι πολύ δύσκολο να διασφαλιστεί ο όγκος των δεδομένων στον κυβερνοχώρο από τεράστιο αριθμό κυβερνοεπιθέσεων. Η εξάρτηση από το Διαδίκτυο και η εύκολη πρόσβαση στα τραπεζικά στοιχεία μέσω του διαδικτυακού συστήματος γίνεται απειλή για τους ανθρώπους στη σύγχρονη εποχή (More&Nalawade, 2015).

2.2 Κρυπτογράφηση δεδομένων

Για τη διασφάλιση της ανταλλαγής δεδομένων στο Διαδίκτυο θα πρέπει να αναπτυχθούν μηχανισμοί προστασίας, όπως η κρυπτογράφηση, δηλαδή η μετατροπή των δεδομένων με τέτοιο τρόπο, ώστε να μην μπορούν να διαβαστούν από οποιονδήποτε, χωρίς να έχει την απαραίτητη εξουσιοδότηση. Ουσιαστικά, η κρυπτογράφηση, αποτελεί μια διαδικασία κωδικοποίησης πληροφοριών, μέσω της οποίας ένα κείμενο μετατρέπεται σε ένα κρυπτοκείμενο, δηλαδή σε μία εναλλακτική μορφή ανάγνωσης. Η ασφάλεια βασίζεται στο γεγονός ότι η αποκρυπτογράφησητου κρυπτοκειμένου μπορεί να γίνει μόνο από εξουσιοδοτημένους φορείς, οι οποίοι μπορούν να αποκτήσουν πρόσβαση στις πληροφορίες (Devadigaetal., 2017).

Η κρυπτογράφηση των δεδομένων απαιτεί καλό σχεδιασμό, με τη χρήση κλειδιών κρυπτογράφησης, τα οποία αναπτύσσονται από έναν αλγόριθμο. Οι εξουσιοδοτημένοι παραλήπτες των δεδομένων έχουν πρόσβαση στα κλειδιά κρυπτογράφησης, έτσι ώστε να μπορέσουν να αποκρυπτογραφήσουν τα μήνυμα. Με τον τρόπο αυτό αποκλείεται η πρόσβαση σε μη εξουσιοδοτημένους χρήστες(Malloulietal., 2021).

Για τεχνικούς λόγους, ένα σχήμα κρυπτογράφησης χρησιμοποιεί συνήθως ένα ψευδο-τυχαίο κλειδί κρυπτογράφησης που δημιουργείται από έναν αλγόριθμο. Στο χώρο του Διαδικτύου, είναι αδύνατον να αποκρυπτογραφηθεί το μήνυμα χωρίς να είναι διαθέσιμο το κλειδί. Έτσι,ένας εξουσιοδοτημένος παραλήπτης μπορεί εύκολα να αποκρυπτογραφήσει το μήνυμα με το κλειδί που παρέχεται από τον δημιουργό στους παραλήπτες αλλά όχι σε μη εξουσιοδοτημένους χρήστες.Από τους αλγορίθμους κρυπτογράφησης, αυτό που χρησιμοποιείται περισσότερο από παρόχους υπηρεσιών αποθήκευσης δεδομένων είναι το AES (Σύνθετο Πρότυπο Κρυπτογράφησης). Το κλειδί της κρυπτογράφησης μετριέται σε bit και οι συνήθεις τιμές είναι 128, 192 και 256 bit. Όσο περισσότερα τα bit του κλειδιού, τόσο μεγαλύτερο το μέγεθός του, άρα και πιο δύσκολο «σπάσιμο» του κλειδιού για να αποκτήσει κάποιος χάκερ, πρόσβαση στα δεδομένα. Για αυτό το λόγο, στη σύγχρονη εποχή, τα 256 bit αποτελούν την πιο διαδεδομένη μορφή κρυπτογράφησης. Η κρυπτογράφηση δεδομένων, πλέον, θεωρείται απαραίτητη, ώστε να διασφαλιστεί ότι κανένας μη εξουσιοδοτημένος χρήστης δεν θα αποκτήσει πρόσβαση κατά τη μεταφορά τους μεταξύ των διαφόρων διακομιστών αποθήκευσης (Khelifietal., 2013).

2.3 Η διασφάλιση των ηλεκτρονικών συναλλαγών

Η διασφάλιση υψηλού επιπέδου ασφάλειας για τις πλατφόρμες ηλεκτρονικής τραπεζικής έχει ως τελικό κίνητρο την προστασία των καταναλωτών όσον αφορά τις ηλεκτρονικές υπηρεσίες και κατά συνέπεια την προστασία των συμφερόντων των χρηματοπιστωτικών ιδρυμάτων. Ο τρόπος με τον οποίο ένα χρηματοπιστωτικό ίδρυμα διαχειρίζεται την ασφάλεια των πληροφοριών, στην προκειμένη περίπτωση με βάση τις τεχνολογίες πληροφοριών και επικοινωνιών, είναι απαραίτητος για να διασφαλίσει την αξιοπιστία του όσον αφορά την ικανότητα παροχής υπηρεσιών ηλεκτρονικής τραπεζικής και να προστατεύσει την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών (Choudhurietal., 2024).

Οι περισσότερες νομικές ρυθμίσεις σχετικά με την προστασία των συμφερόντων των καταναλωτών μέσω της διασφάλισης της ασφάλειας των πλατφορμών ηλεκτρονικής τραπεζικής λαμβάνουν υπόψη τη διασφάλιση της ασφάλειας και της εμπιστευτικότητας των πληροφοριών των πελατών, τηνπροστασία από τυχόν αναμενόμενες απειλές ή κινδύνους για την ασφάλεια ή την ακεραιότητα των εν λόγω πληροφοριών και τηνπροστασία από μη εξουσιοδοτημένη πρόσβαση ή χρήση τέτοιων πληροφοριών που θα μπορούσε να οδηγήσει σε σημαντική ζημία ή ταλαιπωρία για οποιονδήποτε πελάτη (Dhoot, Nazarov&Koupaei, 2020).

Κάθε χρηματοπιστωτικό ίδρυμα θα πρέπει να πληροί ένα ελάχιστο σύνολο απαιτήσεων ασφαλείας, όπως η εμπιστευτικότητα και ακεραιότητα των επικοινωνιών και δεδομένων, ηεπαλήθευση ταυτότητας των εμπλεκομένων στις συναλλαγές, η προστασία προσωπικών δεδομένων, η διατήρηση τραπεζικού απορρήτου, η ιχνηλασιμότητα συναλλαγών και ησυνεχής εξυπηρέτηση πελατών. Επίσης, θα πρέπει να προλαμβάνει, να ανιχνεύει και να παρακολουθεί περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στο σύστημα, να διαχειρίζεται το σύστημα πληροφοριών και να μεριμνά για όλα τα απαραίτητα τεχνικά μέτρα που θα πρέπει να λαμβάνονται για την ασφαλή λειτουργία του συστήματος(Ibrahim, 2018).

Τα αξιόπιστα συστήματα ηλεκτρονικών τραπεζικών συναλλαγών βασίζονται στη συνεχή ενδυνάμωση της ασφάλειας των διακομιστών, του δικτύου καθώς και των υπολογιστών των τραπεζών τους, ώστε να διασφαλίζεται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των συναλλαγών των πελατών. Υπάρχουν πολλά μοντέλα ασφάλειας, αν και αρκετά από αυτά είναι ευάλωτα σε επιθέσεις λόγω βλάβης των μηχανισμών ασφαλείας τους. Μερικοί από αυτούς τους μηχανισμούς ασφαλείας

αναφέρονται στη συνέχεια. Αρχικά, η διασφάλιση των ηλεκτρονικών συναλλαγών επιτυγχάνεται με την αποστολή SMS με κωδικό μίας χρήσης (OTP). Το βασικό παράδειγμα του SMS OTP είναι ο Αριθμός Εξουσιοδότησης Συναλλαγής (mTAN) για κινητά που εφαρμόζεται για την εξουσιοδότηση συναλλαγών για το σύστημα ηλεκτρονικής τραπεζικής. Σε αυτόν τον μηχανισμό, το OTP αποστέλλεται ως μήνυμα κειμένου στην κινητή συσκευή του χρήστη. Ωστόσο, η ασφάλεια του SMS OTP εξαρτάται από την εμπιστευτικότητα των μηνυμάτων SMS, η οποία εξαρτάται από την ασφάλεια των δικτύων κινητής τηλεφωνίας (Gomes, Deshmukh&Anute, 2022).

Ένα άλλο μέσο διασφάλισης των ηλεκτρονικών συναλλαγών, είναι οι Κωδικοί πρόσβασης μίας χρήσης (OTP), μέσω μικρών συσκευών που χορηγούνται στους πελάτες και εμφανίζουν αριθμούς, με βάση τη διαμόρφωση των κωδικών, επομένως μπορούν να χρησιμοποιηθούν μόνο μία φορά. Χρησιμοποιούνται γενικά ως δεύτεροι παράγοντες ελέγχου ταυτότητας. Ωστόσο, η επίθεση man-in-the-middle μπορεί να μεταβιβάσει τα διαπιστευτήρια σύνδεσης, συμπεριλαμβανομένης της τιμής OTP, σε πραγματικό χρόνο. Έτσι, μπορεί να ξεπεραστεί η ασφάλεια από την συνεχώς μεταβαλλόμενη τιμή του κωδικού (Muneeswari&Puthussery, 2019).

Επιπρόσθετα, υπάρχει οέλεγχος ταυτότητας πολλαπλών παραγόντων (MFA). Πρόκειται για ένα σύστημα ασφαλείας που προσφέρει διάφορες τεχνικές ελέγχου ταυτότητας. Ο στόχος του MFA είναι να σχηματίσει ένα πολυεπίπεδο αμυντικό μηχανισμό, προκειμένου να καταστήσει σχεδόν αδύνατη για έναν μη εξουσιοδοτημένο χρήστη να συνδεθεί και να εκτελέσει οποιαδήποτε λειτουργία. Ακόμη μέσο διασφάλισης των ηλεκτρονικών συναλλαγών είναι το Secure Sockets Layer (SSL). Το SSL είναι πρωτόκολλα κρυπτογράφησης που χρησιμοποιούνται για την έναρξη μιας κρυπτογραφημένης σύνδεσης μεταξύ ενός διακομιστή ηλεκτρονικών τραπεζικών υπηρεσιών και ενός προγράμματος περιήγησης χρήστη. Αυτή η σύνδεση στοχεύει να εγγυηθεί ότι όλα τα δεδομένα που παραδίδονται παραμένουν ασφαλή (Karimetal., 2023).

Πιο σύγχρονα μέσα διασφάλισης είναι η Τεχνολογία βιομετρικής επαλήθευσης ταυτότητας.Πρόκειται για μια μέθοδο αναγνώρισης των πελατών μέσω των βιολογικών τους χαρακτηριστικών, όπως ο αμφιβληστροειδής χιτώνας, η αναγνώριση προσώπου και τα δακτυλικά αποτυπώματα. Τα βιομετρικά χαρακτηριστικά είναι διαφορετικά για τον καθένα και είναι δύσκολο να πλαστογραφηθούν. Ωστόσο, σε ένα βιομετρικό σύστημα μπορεί να παρατηρηθούν δύο τύποι αποτυχίας ελέγχου ταυτότητας: Η πρώτη είναι η ψευδής μη αντιστοίχιση, η οποία συμβαίνει όταν δύο δείγματα από το ίδιο άτομο έχουν χαμηλή ομοιότητα και το σύστημα δεν μπορεί να τα αντιστοιχίσει σωστά. Αυτή η

αποτυχία οδηγεί σε άρνηση υπηρεσίας σε έναν νόμιμο χρήστη. Η δεύτερη είναι η ψευδής αντιστοίχιση, η οποία μπορεί να οδηγήσει σε εισβολή από έναν απατεώνα (Tassabehji&Kamala, 2012).

Εν συνεχεία οι τραπεζικές ηλεκτρονικές συναλλαγές διασφαλίζονται από την Προστασία Περιήγησης, η οποία εκτός από την ασφαλή περιήγηση στο διαδίκτυο, περιλαμβάνει επίσης βελτιωμένη τραπεζική προστασία, η οποία αποτελεί έναν προσωπικό φύλακα ασφαλείας, διασφαλίζοντας ότι οι τραπεζικές συναλλαγές είναι ασφαλείς και ιδιωτικές. Παράλληλα, υπάρχουν τα Ψηφιακά Πιστοποιητικά, τα οποία χρησιμοποιούνται για τον έλεγχο ταυτότητας τόσο των χρηστών όσο και του ίδιου του τραπεζικού συστήματος. Αυτό το είδος ελέγχου ταυτότητας εξαρτάται από την ύπαρξη μιας υποδομής δημόσιου κλειδιού (PKI) και μιας αρχής έκδοσης πιστοποιητικών (CA) η οποία αντιπροσωπεύει ένα αξιόπιστο στοιχείο που υπογράφει τα πιστοποιητικά βεβαιώνοντας την εγκυρότητά τους (Lee, Lim&Lim, 2013).

Επιπλέον, το Σύστημα Ανίχνευσης και Πρόληψης Εισβολών (IDPS)είναι το λογισμικό μιας συσκευής που εφαρμόζεται συνήθως για την ανίχνευση και την αποτροπή οποιασδήποτε εισβολής που προσπαθεί να εισβάλει στο δίκτυο ή τον κεντρικό υπολογιστή και να απειλήσει την ασφάλεια του συστήματος. Υπάρχουν δύο κύριοι τύποι IDPS, συστήματα ανίχνευσης εισβολών που βασίζονται σε δίκτυο (NIDPS) και συστήματα ανίχνευσης εισβολών που βασίζονται σε κεντρικό υπολογιστή (HIDPS) (Ibrahim, 2018).

Αναφορικά με τις μεθόδους ανίχνευσης και αναγνώρισης επιθέσεων, υπάρχουν τρεις βασικές μέθοδοι, οι οποίες είναι η αναγνώριση υπογραφών, η ανίχνευση ανωμαλιών και η ανάλυση πρωτοκόλλου κατάστασης. Η αναγνώριση υπογραφών είναι γνωστή ως ανίχνευση κακής χρήσης και αποτελεί μια τεχνική που περιέχει μια βάση δεδομένων πληροφοριών με υπογραφές για κακόβουλη, επιβλαβή, παράνομη ή μη εξουσιοδοτημένη δραστηριότητα.Στη συνέχεια γίνεται σύγκριση μεταξύ των τρεχόντων δεδομένων με τη βάση δεδομένων υπογραφών και ανταποκρίνεται όταν αναγνωριστεί μια αντιστοιχία. Η ανίχνευση που βασίζεται σε υπογραφές είναι εξαιρετικά αποτελεσματική στην ανίχνευση γνωστών επιθέσεων, αλλά σε κάποιο βαθμό αδυνατεί να ανακαλύψει και να αναγνωρίσει τις απειλές που είναι άγνωστες και αυτό είναι σίγουρα ένα μειονέκτημα (Choudhurietal., 2024).

Η ανίχνευση ανωμαλιών είναι η διαδικασία παρακολούθησης και ανίχνευσης των αποκλίσεων από τις γνωστές λειτουργίες στα συστήματα ή τα δίκτυα, με βάση τις πληροφορίες που συλλέγονται μέσω των συνηθισμένων λειτουργιών. Το κύριο

πλεονέκτημα των μεθόδων ανίχνευσης ανωμαλιών είναι ότι μπορούν να είναι εξαιρετικά χρήσιμες στην ανίχνευση άγνωστων επιθέσεων. Ωστόσο, υποφέρουν από υψηλό ποσοστό ψευδών συναγερμών (Dhoot, Nazarov&Koupaei, 2020).

Η ανάλυση πρωτοκόλλου κατάστασης είναι μια τεχνική που χρησιμοποιείται για τον έλεγχο των πρωτοκόλλων δικτύου και την αντιστοίχιση προκαθορισμένων προφίλ των πρωτοκόλλων συνήθους δραστηριότητας έναντι εντοπισμένων συμβάντων για την αναγνώριση αποκλίσεων. Αυτό σημαίνει ότι οι IDPS σε αυτήν την τεχνική θα είναι σε θέση να κατανοήσουν και να παρακολουθήσουν την κατάσταση των πρωτοκόλλων δικτύου, εφαρμογής και μεταφοράς που περιέχουν πληροφορίες κατάστασης(Ibrahim, 2018).

Κεφάλαιο 3ο: Προκλήσεις και κίνδυνοι στις Ηλεκτρονικές Συναλλαγές

3.1 Κίνδυνοι και απειλές στις ηλεκτρονικές συναλλαγές

Η ανάπτυξη των ηλεκτρονικών συναλλαγών στον τραπεζικό κλάδο έχει δημιουργήσει νέα δεδομένα ως προς τους κινδύνους, καθώς η υιοθέτηση της ταχέως εξελισσόμενης τεχνολογίας αλλάζει τους παραδοσιακούς κινδύνους. Οι κίνδυνοι στις ηλεκτρονικές τραπεζικές συναλλαγές μπορούν να συνοψιστούν σε α) λειτουργικούς κινδύνους, β)κινδύνους ασφάλειας, γ)κινδύνους σχεδιασμού συστήματος, δ)κινδύνους φήμης και ε)νομικούς κινδύνους (Yadav, 2022).

Οι λειτουργικοί κίνδυνοι προκύπτουν από απάτες, σφάλματα επεξεργασίας, διακοπές συστήματος ή άλλα απρόβλεπτα γεγονότα που έχουν ως αποτέλεσμα την αδυναμία του εκάστοτε τραπεζικού ιδρύματος να παρέχει τις υπηρεσίες του. Το επίπεδο κινδύνου συναλλαγών μπορεί να επηρεαστεί από τη δομή του περιβάλλοντος επεξεργασίας δεδομένων, συμπεριλαμβανομένων των τύπων υπηρεσιών που προσφέρονται, της πολυπλοκότητας των διαδικασιών, καθώς και της υποστηρικτικής τεχνολογίας. Στις περισσότερες περιπτώσεις, οι δραστηριότητες ηλεκτρονικής τραπεζικής αυξάνουν την πολυπλοκότητα των δραστηριοτήτων του ιδρύματος και την ποσότητα του κινδύνου των λειτουργιών του, ειδικά εάν το ίδρυμα προσφέρει καινοτόμες υπηρεσίες που δεν έχουν τυποποιηθεί. Δεδομένου ότι οι πελάτες αναμένουν ότι οι υπηρεσίες ηλεκτρονικής τραπεζικής πρέπει να είναι διαθέσιμες 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, τα χρηματοπιστωτικά ιδρύματα θα πρέπει να διασφαλίζουν ότι οι υποδομές ηλεκτρονικής τραπεζικής τους χαρακτηρίζονται επαρκή, ώστε να διασφαλίσουν αξιόπιστη διαθεσιμότητα υπηρεσιών (Solanki, 2012).

Οι κίνδυνοι ασφαλείας αναφέρονται σε μη εξουσιοδοτημένη πρόσβαση σε κρίσιμες πληροφορίες μιας τράπεζας όπως το λογιστικό σύστημα, το σύστημα διαχείρισης κινδύνων ή το σύστημα διαχείρισης χαρτοφυλακίου. Μια παραβίαση ασφάλειας θα μπορούσε να οδηγήσει σε άμεση οικονομική ζημία για την τράπεζα, καθώς οι εισβολείς θα μπορούσαν να αποκτήσουν πρόσβαση, να ανακτούν και να χρησιμοποιούν εμπιστευτικές πληροφορίες πελατών ή ακόμη και να εγκαταστήσουν ιό στο τραπεζικό λογισμικό. Αυτό μπορεί να οδηγήσει σε απώλεια δεδομένων, κλοπή ή παραβίαση των πληροφοριών των πελατών, απενεργοποίηση σημαντικού μέρους του εσωτερικού συστήματος υπολογιστών της

τράπεζας με αποτέλεσμα την αδυναμία παροχής υπηρεσιών ή το αυξημένο κόστος επισκευής αυτών (Paliwal, 2017).

Η παραβίαση των συστημάτων ασφαλείας μιας τράπεζας επιφέρει και άλλους σχετικούς κινδύνους, όπως είναι η απώλεια φήμης, η παραβίαση του απορρήτου των πελατών και οι νομικές επιπτώσεις. Εξάλλου, ο έλεγχος της πρόσβασης στο σύστημα των τραπεζών έχει γίνει πιο περίπλοκος στο περιβάλλον του Διαδικτύου, το οποίο είναι δημόσιο και οι προσπάθειες μη εξουσιοδοτημένης πρόσβασης θα μπορούσαν να προέρχονται από οποιαδήποτε πηγή και από οπουδήποτε στον κόσμο με ή χωρίς εγκληματική πρόθεση. Επίσης, εκτός από τις εξωτερικές επιθέσεις, οι τράπεζες εκτίθενται σε κίνδυνο ασφαλείας από εσωτερικές πηγές, όπως απάτη εργαζομένων. Η εξοικείωση των εργαζομένων με διαφορετικά συστήματα και τις αδυναμίες τους αποτελούν πιθανές απειλές για την ασφάλεια σε ένα χαλαρά ελεγχόμενο περιβάλλον. Μπορούν να καταφέρουν να αποκτήσουν τα δεδομένα ελέγχου ταυτότητας προκειμένου να έχουν πρόσβαση στους λογαριασμούς των πελατών προκαλώντας απώλειες στην τράπεζα. Εκτός εάν προστατεύονται ειδικά, όλες οι μεταφορές δεδομένων/πληροφοριών μέσω του Διαδικτύου μπορούν να παρακολουθηθούν ή να διαβαστούν από μη εξουσιοδοτημένα άτομα (Alsayed&Bilgrami, 2017).

Εν συνεχεία, επισημαίνονται οι κίνδυνοι σχεδιασμού συστήματος, οι οποίοι σχετίζονται με τη διαχείριση διαφόρων ειδών λειτουργικών κινδύνων που αφορούν την εφαρμογή των τραπεζικών συστημάτων. Πιο συγκεκριμένα, μια τράπεζα αντιμετωπίζει τον κίνδυνο τα συστήματα που επιλέγει να μην είναι καλά σχεδιασμένα ή εφαρμοσμένα και ως εκ τούτου, να εκτεθεί στον κίνδυνο διακοπής ή επιβράδυνσης των υπαρχόντων συστημάτων της, στην περίπτωση που το το σύστημα ηλεκτρονικής τραπεζικής που επιλέγει δεν είναι συμβατό με τις απαιτήσεις των χρηστών. Πολλές τράπεζες στηρίζονται σε εξωτερικούς παρόχους υπηρεσιών για την εφαρμογή και τη λειτουργία των συστημάτων τους, γεγονός που μπορεί να τις εκθέσει σε διάφορους λειτουργικούς κινδύνους. Οι πάροχοι υπηρεσιών ενδέχεται να μην διαθέτουν την απαιτούμενη γνώση για να παρέχουν τις υπηρεσίες που αναμένονται ή ενδέχεται να μην ενημερώνουν την τεχνολογία τους. Οι λειτουργίες ενός παρόχου υπηρεσιών θα μπορούσαν να διακοπούν λόγω βλαβών του συστήματος ή οικονομικών δυσκολιών, θέτοντας σε κίνδυνο την ικανότητα μιας τράπεζας να παρέχει υπηρεσίες. Ως εκ τούτου, ο ταχύς ρυθμός αλλαγής που χαρακτηρίζει την τεχνολογία πληροφοριών παρουσιάζει στις τράπεζες τον κίνδυνο απαξίωσης των συστημάτων (Solanki, 2012).

Επιπλέον οι κίνδυνοι φήμης επηρεάζουν σημαντικάτην κοινή γνώμη, η οποία μπορεί να οδηγήσει σε σοβαρή απώλεια χρηματοδότησης ή πελατών. Οι κύριοι λόγοι για αυτόν τον κίνδυνο μπορεί να είναι η ελλιπής λειτουργία των συστημάτων σύμφωνα με τις προσδοκίες των πελατών, σημαντικές παραβιάσεις ασφάλειας, λόγω επιθέσεων, η ανεπαρκής ενημέρωση των πελατών σχετικά με τα τραπεζικά προϊόντα, οι διαδικασίες επίλυσης προβλημάτων καιη ελλιπής επικοινωνία. Πελάτες που επηρεάζονται άμεσα από τέτοια ζητήματα ενδέχεται να εγκαταλείψουν την τράπεζα, ενώ η δημοσιοποίηση τέτοιων φαινομένων μπορεί να επιφέρουν αλυσιδωτές επιπτώσεις (Yadav, 2022).

Οι νομικοί κίνδυνοι αφορούν τις περιπτώσεις μη συμμόρφωσης με τις νομικές ή κανονιστικές απαιτήσεις. Οι νομικοί κίνδυνοι σχετίζονται άμεσα με την ηλεκτρονική τραπεζική και αυξάνονται καθώς η χρήση της επεκτείνεται. Προκύπτουν κυρίως από την αβεβαιότητα που υπάρχει στο νομικό - κανονιστικό πλαίσιο που αφορά την ηλεκτρονική τραπεζική. Στις περισσότερες χώρες δεν υπάρχει σαφές ρυθμιστικό πλαίσιο, η αναπτύσσεται με βραδείς ρυθμούς,γεγονός που οφείλεται στη μικρή εμπειρία στον τομέα της ηλεκτρονικής τραπεζικής.Ένας βασικός νομικός κίνδυνος σχετίζεται με την προστασία των προσωπικών δεδομένων των πελατών. Η κακή χρήση από τοπροσωπικό της τράπεζας ή από εξωτερικούς κακόβουλους εισβολείς μπορεί να εκθέσει μια τράπεζα σε σοβαρούς νομικούς κινδύνους.Είναι πιθανό οι εισβολείς να αποκτήσουν πρόσβαση στις βάσεις δεδομένων των τραπεζών και να χρησιμοποιήσουν τα δεδομένα τωνπελατών για να διαπράξουν απάτη. Σε αυτήν την περίπτωση, δημιουργείται νομικός κίνδυνος από την κακή ή μηπιστοποιημένη χρήση των δεδομένων των πελατών (Alsayed&Bilgrami, 2017).

Σε όρους Ευρωπαϊκής Ένωσης, έχει αναπτυχθεί ένα ρυθμιστικό πλαίσιο που ασχολείται με ζητήματα όπως οι ηλεκτρονικές (ψηφιακές) υπογραφές, η εξ αποστάσεως παροχή χρηματοοικονομικών υπηρεσιών, καθώς και η Οδηγία για το ηλεκτρονικό εμπόριο.Ένας πελάτης που δεν είναι επαρκώς ενημερωμένος για τα δικαιώματα και τις υποχρεώσεις του, ενδέχεται να μην λάβει τα κατάλληλα μέτρα προφύλαξης κατά τη χρήση προϊόντων ή υπηρεσιών ηλεκτρονικής τραπεζικής, οδηγώντας σε αμφισβητούμενες συναλλαγές, ανεπιθύμητες αγωγές κατά της τράπεζας ή άλλες κανονιστικές κυρώσεις (Mylonakis, Orfanos&Evripiotis, 2024).

3.2 Παράγοντες που επηρεάζουν το αίσθημα ασφαλείας

Η ασφάλεια των τραπεζικών συναλλαγών αποτελεί το κύριο μέλημα των τραπεζικών ιδρυμάτων, καθώς η απουσία ασφάλειας μπορεί να οδηγήσει σε σοβαρή ζημιά του τραπεζικού τομέα. Ως εκ τούτου, οι περισσότεροι πελάτες ελπίζουν ότι υπάρχει

ασφάλεια στις συναλλαγές τους και ότι τα χρήματά τους προστατεύονται. Επίσης, σημαντική για τους πελάτες είναι και η προστασία των πληροφοριών τους και των προσωπικών τους δεδομένων (Jaliletal., 2014).

Στην έρευνα τους, οιMauro Hernandez και Mazzon (2006) έδειξαν ότι στοιχεία, όπως η αποτελεσματικότητα, η ασφάλεια και η ιδιωτικότητα επηρεάζουν συλλογικά τους καταναλωτές αναφορικά με τη χρήση των ηλεκτρονικών τραπεζικών συναλλαγών. Ορισμένοι χρήστες δεν ήταν απόλυτα ικανοποιημένοι με τις ηλεκτρονικές συναλλαγές λόγω της πιθανότητας μη ασφαλούς πρόσβασης σε λογαριασμούς, λόγω έλλειψης αξιόπιστης ταυτοποίησης του αποστολέα των ηλεκτρονικών τραπεζικών συναλλαγών. Επομένως, είναι εξαιρετικά απαραίτητο να υπάρχει ένας αξιόπιστος τρίτοςφορέας που να κατέχει τα πιστοποιητικά ταυτότητας τόσο του αποστολέα όσο και του παραλήπτη στις ηλεκτρονικές συναλλαγές, προκειμένου να ενισχυθεί το αίσθημα ασφάλειας.

Γενικότερα, το αίσθημα ασφαλείας και εμπιστοσύνης από τους καταναλωτές προς τις τράπεζες μπορεί να επηρεαστεί όταν οι τράπεζες δεν φαίνεται να ενδιαφέρονται και να προστατεύουν τους μηχανισμούς ηλεκτρονικών συναλλαγών. Είναι γεγονός ότι η καλά σχεδιασμένη ασφάλεια μπορεί να οδηγήσει τους καταναλωτές να υιοθετήσουν μια πιο σίγουρη προσέγγιση στην ηλεκτρονική τραπεζική. Ως εκ τούτου, μια τράπεζα πρέπει να μειώσει το άγχος ενός πελάτη σχετικά με την ασφάλειατων ηλεκτρονικών χρηματοοικονομικών συναλλαγών της, παρέχοντας κατάλληλα σχετικές πληροφορίεςσχετικά με την αξιοπιστία της τεχνολογίας που χρησιμοποιείται. Οι εταιρείες ηλεκτρονικής τραπεζικής τονίζουν ότιπαρέχουν ασφαλείς εσωτερικούς λειτουργικούς ελέγχους με ένα πολυεπίπεδο σύστημα ασφαλείας μέσωτης ενσωμάτωσης προηγμένης τραπεζικής τεχνολογίας που παρακολουθεί συνεχώς τις διαδικτυακές συναλλακτικές δραστηριότητες μέσω μιας ποικιλίας πακέτων λογισμικού (Wongetal., 2009).

Εν συνεχεία, σύμφωνα με την μελέτητου Chuang (2011) φαίνεται ότι η ασφάλεια και η ιδιωτικότητα έχουν ισχυρή επίδραση στην εμπιστοσύνη των πελατών κατά την περίοδο των ηλεκτρονικών συναλλαγών. Η ασφάλεια γίνεται αντιληπτή σε τρεις διαστάσεις, δηλαδή, την αξιοπιστία, την ασφάλεια και την ιδιωτικότητα. Μια καλή εμπειρίαμε την ασφάλεια και την ιδιωτικότητα σε ιστότοπους ηλεκτρονικής τραπεζικής μπορεί να έχει θετική επίδραση στηνεμπιστοσύνη των πελατών

3.3 Μέτρα προστασίας

Κάθε τραπεζικό ίδρυμα στο πλαίσιο των μέτρων προστασίας θα πρέπει να προωθήσει την διαχείριση και τον έλεγχο κινδύνων. Έτσι, λοιπόν, αφού πραγματοποιήσει μια αξιολόγηση των κινδύνων και της ανοχής κινδύνου, η διοίκηση της τράπεζας θα πρέπει να λάβει τα κατάλληλα μέτρα. Αυτή η φάση της διαδικασίας διαχείρισης κινδύνων περιλαμβάνει δραστηριότητες όπως η εφαρμογή πολιτικών και μέτρων ασφαλείας, ο συντονισμός της εσωτερικής επικοινωνίας, η αξιολόγηση και η αναβάθμιση προϊόντων και υπηρεσιών, η εφαρμογή μέτρων για να διασφαλιστεί ότι οι κίνδυνοι εξωτερικής ανάθεσης ελέγχονται και διαχειρίζονται, η παροχή γνωστοποιήσεων και η εκπαίδευση των πελατών, καθώς και η ανάπτυξη σχεδίων έκτακτης ανάγκης (Vrîncianu&Popa, 2010).

Οιδιοικήσεις των τραπεζικών ιδρυμάτων θα πρέπει να διασφαλίζουν ότι το προσωπικό που είναι υπεύθυνο για την επιβολή ορίων κινδύνου έχει εξουσία ανεξάρτητη από τον φορέα που αναλαμβάνει την ηλεκτρονική τραπεζική ή τη δραστηριότητα ηλεκτρονικού χρήματος. Οι τράπεζες αυξάνουν την ικανότητά τους να ελέγχουν και να διαχειρίζονται τους διάφορους κινδύνους που ενυπάρχουν σε οποιαδήποτε δραστηριότητα όταν οι πολιτικές και οι διαδικασίες καθορίζονται σε γραπτή τεκμηρίωση και διατίθενται σε όλο το σχετικό προσωπικό (Chaimaa, Najib&Rachid, 2021).

Η ασφάλεια βασίζεταιστον συνδυασμό συστημάτων, εφαρμογών και εσωτερικών ελέγχων που χρησιμοποιούνται για την προστασία της ακεραιότητας, της αυθεντικότητας και της εμπιστευτικότητας των δεδομένων και των λειτουργικών διαδικασιών. Η σωστή ασφάλεια βασίζεται στην ανάπτυξη και εφαρμογή επαρκών πολιτικών ασφαλείας και μέτρων για τις διαδικασίες εντός της τράπεζας και για την επικοινωνία μεταξύ της τράπεζας και των εξωτερικών φορέων. Οι πολιτικές και τα μέτρα ασφαλείας μπορούν να περιορίσουν τον κίνδυνο εξωτερικών και εσωτερικών επιθέσεων σε συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικού χρήματος, καθώς και τον κίνδυνο δυσφήμισης που προκύπτει από παραβιάσεις ασφαλείας. Τα μέτρα ασφαλείας προϋποθέτουν τον συνδυασμό εργαλείων υλικού και λογισμικού, καθώς και διαχείρισης προσωπικού, ώστε να συμβάλλουν στη δημιουργία ασφαλών συστημάτων και λειτουργιών. Τέτοια μέτρα περιλαμβάνουν κρυπτογράφηση, κωδικούς πρόσβασης, τείχη προστασίας, ελέγχους ιών και έλεγχο εργαζομένων (Vrîncianu&Popa, 2010).

Η κρυπτογράφηση είναι η χρήση κρυπτογραφικών αλγορίθμων για την κωδικοποίηση δεδομένων απλού κειμένου σε κρυπτογραφημένο κείμενο για την αποτροπή μη εξουσιοδοτημένης παρατήρησης. Οι κωδικοί πρόσβασης, οι φράσεις πρόσβασης, οι

προσωπικοί αριθμοί αναγνώρισης, τα διακριτικά που βασίζονται στο υλικό και τα βιομετρικά στοιχεία είναι τεχνικές για τον έλεγχο της πρόσβασης και την αναγνώριση χρηστών. Τα τείχη προστασίας είναι συνδυασμοί υλικού και λογισμικού που ελέγχουν και περιορίζουν την εξωτερική πρόσβαση σε εσωτερικά συστήματα που συνδέονται με ανοιχτά δίκτυα όπως το Διαδίκτυο. Τα τείχη προστασίας μπορούν επίσης να διαχωρίζουν τμήματα εσωτερικών δικτύων χρησιμοποιώντας τεχνολογία Διαδικτύου. Η τεχνολογία τείχους προστασίας, εάν σχεδιαστεί και εφαρμοστεί σωστά, μπορεί να αποτελέσει ένα αποτελεσματικό μέσο ελέγχου της πρόσβασης και διαφύλαξης της εμπιστευτικότητας και της ακεραιότητας των δεδομένων. Ωστόσο, επειδή τα τείχη προστασίας μπορεί να ξεπεραστούν, οι τράπεζες θα πρέπει να αναπτύξουν μέτρα πρόληψης και ανίχνευσης για να μειώσουν την πιθανότητα επίθεσης από ιούς και καταστροφής δεδομένων, ιδιαίτερα για τις απομακρυσμένες τραπεζικές συναλλαγές (Chaimaa, Najib&Rachid, 2021).

Εν συνεχεία, αναμένεται ότι μία σειρά λειτουργικών, νομικών και άλλων κινδύνων μπορούν να διαχειριστούν και να ελεγχθούν εάν η διοίκηση θέσει ως βασική θέση ότι οι υπηρεσίες ηλεκτρονικής τραπεζικής προορίζονται για να υποστηρίξουν τους συνολικούς στόχους της τράπεζας. Ταυτόχρονα, το τεχνικό προσωπικό θα πρέπει να επικοινωνεί με σαφήνεια στην ανώτερη διοίκηση τον τρόπο λειτουργίας των ηλεκτρονικών συστημάτων, καθώς επίσης, να ενημερώνει για αδυναμίες και πλεονεκτήματα των συστημάτων. Τέτοιες διαδικασίες μπορούν να μειώσουν τους λειτουργικούς κινδύνους του κακού σχεδιασμού των συστημάτων, συμπεριλαμβανομένης της ασυμβατότητας διαφορετικών συστημάτων εντός ενός τραπεζικού οργανισμού, τα προβλήματα ακεραιότητας δεδομένων, τον κίνδυνο δυσφήμισης, ο οποίος σχετίζεται με τη δυσαρέσκεια των πελατών λόγω της μη αναμενόμενης λειτουργίας των συστημάτων (Mogos&Jamail, 2021).

Σημαντική παράμετρος για τη λήψη μέτρων προστασίας είναι η αξιολόγηση προϊόντων και υπηρεσιών πριν από την χρήση τους. Οι δοκιμές επικυρώνουν ότι ο εξοπλισμός και τα συστήματα λειτουργούν σωστά και οδηγούνστα επιθυμητά αποτελέσματα. Στο πλαίσιο αυτό, οι τράπεζες αναθέτουν σε εξωτερικούς φορείς τη διαχείριση και το έλεγχο λειτουργιών, χωρίς, ωστόσο, αυτό να μειώνει την ευθύνη του εκάστοτε τραπεζικού ιδρύματος για τους τελικούς ελέγχους που επηρεάζουν τις λειτουργίες του (Chaimaa, Najib&Rachid, 2021).

Σημαντική παράμετρος για την προστασία είναι η εκπαίδευση των πελατών, έτσι ώστε να οικειοποιηθούντον τρόπο χρήσης νέων προϊόντων και υπηρεσιών, να ενημερωθούν για τις χρεώσεις των υπηρεσιών και προϊόντων, καθώς επίσης να γνωρίζουν τις διαδικασίες επίλυσης προβλημάτων και σφαλμάτων. Με τον τρόπο αυτό και οι

τράπεζεσσυμμορφώνονται με τους νόμους και τους κανονισμούς περί προστασίας των πελατών και απορρήτου (Vrîncianu&Popa, 2010).

Κάθε τράπεζα οφείλει να έχει ένα σχέδιο έκτακτης ανάγκης, το οποίοθα αφορά την ανάκτηση δεδομένων, τις εναλλακτικές δυνατότητες επεξεργασίας δεδομένων, την στελέχωση έκτακτης ανάγκης και την υποστήριξη εξυπηρέτησης πελατών. Στο πλαίσιο αυτό, τα συστήματα δημιουργίας αντιγράφων ασφαλείας θα πρέπει να δοκιμάζονται περιοδικά για να διασφαλίζεται η αποτελεσματικότητά τους. Επιπλέον, θα πρέπει να υπάρχουν αντισταθμιστικές ενέργειες και εναλλακτικές δράσεις στην περίπτωση που οι πάροχοι υπηρεσιών υποστούν βλάβη (Mogos&Jamail, 2021).

Κεφάλαιο 4ο: Μεθοδολογία έρευνας

4.1 Σκοπός και ερευνητικά ερωτήματα

Ο πρωταρχικός σκοπός της παρούσας έρευνας εστίαζε στη διεξοδική διερεύνηση δύο κρίσιμων παραγόντων που καθορίζουν τη συμπεριφορά των καταναλωτών στο ψηφιακό περιβάλλον. Το πρώτο αφορούσε στο αίσθημα ασφάλειας και το δεύτερο σχετίζονταν με την εμπιστοσύνη που διέθεταν οι πελάτες τραπεζών κατά την πραγματοποίηση ηλεκτρονικών συναλλαγών. Παράλληλα, βασική επιδίωξη αποτέλεσε η εξέταση της επίδρασης των δημογραφικών και κοινωνικών χαρακτηριστικών στην διαφοροποίηση των δύο αυτών μεταβλητών.

Ειδικότερα, μέσω της παρούσας μελέτης επιδιώχθηκε:

- Η λεπτομερής αποτύπωση του επιπέδου ασφάλειας που αντιλαμβάνονται οι πελάτες όταν αλληλεπιδρούν με τα ηλεκτρονικά συστήματα των τραπεζών.
- Η πολυδιάστατη αξιολόγηση της εμπιστοσύνης προς τις ψηφιακές πλατφόρμες, εξετάζοντας παραμέτρους όπως η ακεραιότητα, η καλοσύνη και η ικανότητα των συστημάτων.
- Η διερεύνηση της συσχέτισης και της αλληλεπίδρασης μεταξύ της υποκειμενικής αίσθησης ασφάλειας και της εμπιστοσύνης των πελατών τραπεζών που πραγματοποιούν ηλεκτρονικές συναλλαγές.
- Η ανάλυση του βαθμού στον οποίο τα δημογραφικά χαρακτηριστικά (φύλο, ηλικία, επίπεδο εκπαίδευσης, επαγγελματική ιδιότητα, συχνότητα ηλεκτρονικών συναλλαγών) διαφοροποιούν τις στάσεις των χρηστών αναφορικά με τη ασφάλεια και την εμπιστοσύνη.

Βάσει των ανωτέρω, τα ερευνητικά ερωτήματα της έρευνας διαμορφώθηκαν ως εξής:

1. Σε ποια επίπεδα κινείται το αίσθημα ασφάλειας των πελατών τραπεζών κατά τη χρήση ηλεκτρονικών συναλλαγών;
2. Ποιο είναι το επίπεδο εμπιστοσύνης των πελατών στις ηλεκτρονικές τραπεζικές υπηρεσίες και τις επιμέρους διαστάσεις της;
3. Υφίσταται στατιστικά σημαντική συσχέτιση μεταξύ της αίσθησης ασφάλειας και της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές;

4. Πώς και σε ποιο βαθμό επηρεάζουν τα δημογραφικά χαρακτηριστικά των πελατών (φύλο, ηλικία, επίπεδο εκπαίδευσης, επαγγελματική ιδιότητα, συχνότητα ηλεκτρονικών συναλλαγών) το αίσθημα ασφάλειας και την εμπιστοσύνη;

4.2 Τύπος έρευνας

Για την επίτευξη των στόχων της μελέτης υιοθετήθηκε η ποσοτική μεθοδολογική προσέγγιση με συγχρονικό (cross-sectional) σχεδιασμό. Η επιλογή της ποσοτικής μεθόδου κρίθηκε ως η πλέον κατάλληλη, καθώς επιτρέπει τη συλλογή αριθμητικών δεδομένων από ικανό δείγμα συμμετεχόντων, παρέχοντας τη δυνατότητα γενίκευσης τάσεων και εντοπισμού αιτιακών ή συσχετιστικών δεσμών μεταξύ μεταβλητών (Creswell & Creswell, 2018).

Επιπροσθέτως, η χρήση δομημένου ερωτηματολογίου διασφαλίζει την τυποποίηση της διαδικασίας συλλογής δεδομένων, ελαχιστοποιώντας την υποκειμενικότητα του ερευνητή και επιτρέποντας την αντικειμενική μέτρηση αφηρημένων εννοιών, όπως η «εμπιστοσύνη» και η «ασφάλεια» (Bryman, 2016). Ο συγχρονικός σχεδιασμός επιλέχθηκε λόγω των χρονικών περιορισμών της μελέτης, καθώς επιτρέπει την αποτύπωση της υφιστάμενης κατάστασης σε μια συγκεκριμένη χρονική στιγμή.

4.3 Πληθυσμός και δείγμα

Ο πληθυσμός στόχος της έρευνας περιλάμβανε πελάτες ελληνικών τραπεζών οι οποίοι είναι ενεργοί χρήστες ηλεκτρονικών τραπεζικών υπηρεσιών (e-banking, mobile banking). Το τελικό δείγμα της έρευνας αποτελείται από 151 μεταπτυχιακούς φοιτητές.

Η μέθοδος επιλογής του δείγματος ήταν η δειγματοληψία ευκολίας (convenience sampling). Η συγκεκριμένη μη πιθανοτική μέθοδος επιλέχθηκε διότι επιτρέπει την ταχεία, οικονομική και αποτελεσματική συλλογή δεδομένων από άτομα που είναι άμεσα προσβάσιμα στον ερευνητή (Etikan et al., 2016). Παρόλο που η δειγματοληψία ευκολίας ενέχει περιορισμούς ως προς την αντιπροσωπευτικότητα του γενικού πληθυσμού, θεωρείται αποδεκτή και ευρέως διαδεδομένη σε ακαδημαϊκές έρευνες όπου η τυχαιοποίηση είναι πρακτικά δύσκολη, αρκεί να αναγνωρίζονται οι περιορισμοί της (Stratton, 2021). Η επιλογή φοιτητών, ειδικά σε συναφές αντικείμενο (Λογιστική), εξασφαλίζει επίσης ότι οι συμμετέχοντες έχουν ικανό επίπεδο εξοικείωσης με τις τραπεζικές συναλλαγές.

4.4 Μέσο συλλογής δεδομένων

Το ερευνητικό εργαλείο που χρησιμοποιήθηκε ήταν ένα δομημένο ερωτηματολόγιο, χωρισμένο σε τρεις διακριτές ενότητες, οι οποίες σχεδιάστηκαν για να καλύψουν πλήρως τα ερευνητικά ερωτήματα.

Η πρώτη ενότητα αφορούσε τα δημογραφικά και ατομικά χαρακτηριστικά των συμμετεχόντων. Συγκεκριμένα, ζητήθηκαν πληροφορίες σχετικά με το φύλο, την ηλικία, την επαγγελματική ιδιότητα, καθώς και τη συχνότητα με την οποία πραγματοποιούν ηλεκτρονικές συναλλαγές, προκειμένου να σκιαγραφηθεί το προφίλ του δείγματος.

Η δεύτερη ενότητα εστίασε στη μέτρηση της αίσθησης ασφάλειας. Για τον σκοπό αυτό, αξιοποιήθηκε η κλίμακα "Perceived Security Scale" των Salisbury et al. (2001), προσαρμοσμένη στα ελληνικά δεδομένα. Το εργαλείο αυτό αποτελείται από 5 ερωτήσεις που διερευνούν τις αντιλήψεις του χρήστη σχετικά με την ασφάλεια των μηχανισμών πληρωμής και την προστασία των προσωπικών του δεδομένων κατά τη διαδικασία της συναλλαγής. Οι συμμετέχοντες κλήθηκαν να απαντήσουν σε κλίμακα Likert 7 βαθμίδων (1 = Διαφωνώ απόλυτα έως 7 = Συμφωνώ απόλυτα).

Η τρίτη ενότητα αφορούσε την πολυδιάστατη έννοια της εμπιστοσύνης και βασίστηκε στην κλίμακα "Trust in Online Banking Scale" των Yousafzai et al. (2009). Το συγκεκριμένο εργαλείο επιλέχθηκε διότι δεν αντιμετωπίζει την εμπιστοσύνη ως μονοδιάστατη έννοια, αλλά αξιολογεί τόσο τις γνωστικές όσο και τις συναισθηματικές της πτυχές. Περιλαμβάνει συνολικά 18 ερωτήσεις που κατανέμονται σε έξι υπο-κλίμακες:

1. Αντιληπτός κίνδυνος (Perceived Risk): 3 ερωτήσεις για την αίσθηση ρίσκου κατά τη συναλλαγή.
2. Γενική Εμπιστοσύνη (Trust): 3 ερωτήσεις για τη συνολική στάση εμπιστοσύνης.
3. Αντιληπτή Ιδιωτικότητα (Perceived Privacy): 5 ερωτήσεις για την πεποίθηση ότι η τράπεζα προστατεύει το απόρρητο.
4. Αντιληπτή Ικανότητα (Perceived Competence): 3 ερωτήσεις για την τεχνική επάρκεια της τράπεζας.
5. Αντιληπτή Ακεραιότητα (Perceived Integrity): 2 ερωτήσεις για την τιμιότητα και την ηθική στάση της τράπεζας.
6. Αντιληπτή Καλοσύνη (Perceived Benevolence): 2 ερωτήσεις για το αν η τράπεζα δρα προς το συμφέρον του πελάτη.

Και σε αυτή την ενότητα χρησιμοποιήθηκε κλίμακα Likert 7 βαθμίδων.

4.5 Ερευνητική διαδικασία

Η διαδικασία συλλογής των δεδομένων υλοποιήθηκε σε στάδια, διασφαλίζοντας την επιστημονική εγκυρότητα της έρευνας. Αρχικά, κατατέθηκε η ερευνητική πρόταση στο πλαίσιο της διπλωματικής εργασίας. Ακολούθησε επικοινωνία με την επιβλέπουσα καθηγήτρια, η οποία προχώρησε σε έλεγχο του ερωτηματολογίου και παρείχε την τελική έγκριση για τη διεξαγωγή της έρευνας.

Πριν την κύρια φάση της συλλογής, πραγματοποιήθηκε πιλοτική έρευνα (pilot study) σε δείγμα πέντε (5) φοιτητών. Σκοπός της πιλοτικής φάσης ήταν ο έλεγχος της σαφήνειας των ερωτήσεων, ο εντοπισμός τυχόν συντακτικών λαθών και η εκτίμηση του απαιτούμενου χρόνου συμπλήρωσης. Οι παρατηρήσεις των συμμετεχόντων οδήγησαν σε μικρές διορθωτικές παρεμβάσεις, διαμορφώνοντας την τελική έκδοση του εργαλείου.

Η κύρια φάση συλλογής δεδομένων πραγματοποιήθηκε μέσω της πλατφόρμας Google Forms. Εφαρμόστηκε μικτή μέθοδος προσέγγισης για τη μεγιστοποίηση της συμμετοχής. Αρχικά, ο σύνδεσμος που οδηγούσε στην συμπλήρωση του ερωτηματολογίου διανεμήθηκε διαδικτυακά μέσω κοινωνικών δικτύων και προσωπικών επαφών, ενώ παράλληλα διαμοιράστηκε και δια ζώσης στις αίθουσες διδασκαλίας των πανεπιστημίων. Για τη διευκόλυνση των φοιτητών στις αίθουσες, χρησιμοποιήθηκε κωδικός QR (QR code), επιτρέποντας την άμεση πρόσβαση στο ερωτηματολόγιο μέσω κινητών συσκευών. Η διαδικασία συλλογής δεδομένων ξεκίνησε στις 06/11/2025 και ολοκληρώθηκε στις 09/12/2025.

4.6 Διαδικασία ανάλυσης δεδομένων

Η στατιστική επεξεργασία και ανάλυση των δεδομένων πραγματοποιήθηκε με τη χρήση του λογισμικού IBM SPSS Statistics (έκδοση 25.0.0).

Σε πρώτο στάδιο, εφαρμόστηκε η Περιγραφική Στατιστική. Δημιουργήθηκαν πίνακες συχνοτήτων και ποσοστιαίες κατανομές για την παρουσίαση του προφίλ του δείγματος, ενώ χρησιμοποιήθηκαν γραφήματα για την οπτικοποίηση των δημογραφικών δεδομένων. Για τις κύριες μεταβλητές (Ασφάλεια, Εμπιστοσύνη και οι υποκατηγορίες της), υπολογίστηκαν οι μέσοι όροι (Mean) και οι τυπικές αποκλίσεις (Standard Deviation), ώστε να διαπιστωθεί η κεντρική τάση και η διασπορά των απαντήσεων.

Σε δεύτερο στάδιο, ακολούθησε η Επαγωγική Στατιστική για τον έλεγχο των ερευνητικών υποθέσεων. Αρχικά, πριν την εφαρμογή των τεστ, ελέγχθηκε η κανονικότητα της κατανομής των δεδομένων με τη χρήση του ελέγχου Kolmogorov-Smirnov. Έπειτα, για τη διερεύνηση του τρίτου ερευνητικού ερωτήματος (σχέση ασφάλειας και εμπιστοσύνης), διενεργήθηκε ανάλυση συσχέτισης (Pearson correlation για κανονικές κατανομές ή Spearman's rho για μη κανονικές). Τέλος, για το τέταρτο ερευνητικό ερώτημα (επίδραση δημογραφικών), πραγματοποιήθηκαν έλεγχοι σύγκρισης μέσων όρων. Συγκεκριμένα, για ανεξάρτητες μεταβλητές με δύο επίπεδα (π.χ. φύλο) χρησιμοποιήθηκε το Independent Samples t-test (ή το μη παραμετρικό Mann-Whitney U). Για μεταβλητές με τρία ή περισσότερα επίπεδα, εφαρμόστηκε Ανάλυση Διακύμανσης Μονής Κατεύθυνσης (One-Way ANOVA) ή το αντίστοιχο μη παραμετρικό τεστ Kruskal-Wallis. Το επίπεδο στατιστικής σημαντικότητας για όλους τους ελέγχους ορίστηκε στο a = 0,05.

4.7 Ηθικά ζητήματα

Η έρευνα σχεδιάστηκε και υλοποιήθηκε με αυστηρή προσήλωση στους κανόνες της ερευνητικής δεοντολογίας. Πρωταρχικό μέλημα αποτέλεσε η εξασφάλιση της ενημερωμένης συγκατάθεσης (informed consent) των συμμετεχόντων. Στην εισαγωγή του ερωτηματολογίου υπήρχε σαφής ενημέρωση για τον σκοπό της έρευνας, τον ακαδημαϊκό της χαρακτήρα και την εθελοντική φύση της συμμετοχής.

Επιπλέον, διασφαλίστηκε πλήρως η ανωνυμία και η εμπιστευτικότητα. Δεν ζητήθηκε κανένα προσωπικό στοιχείο που θα μπορούσε να οδηγήσει στην άμεση ή έμμεση ταυτοποίηση των συμμετεχόντων (όπως ονοματεπώνυμο ή διεύθυνση IP). Η διαχείριση και αποθήκευση των δεδομένων έγινε αποκλειστικά για τους σκοπούς της παρούσας εργασίας, χωρίς κοινοποίηση σε τρίτους, σε πλήρη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).

4.8 Περιορισμοί της έρευνας

Παρά τον προσεκτικό σχεδιασμό, η έρευνα υπόκειται σε συγκεκριμένους περιορισμούς που πρέπει να συνεκτιμηθούν κατά την ερμηνεία των ευρημάτων. Ο βασικότερος περιορισμός αφορά τη μέθοδο δειγματοληψίας (ευκολίας) και τη σύνθεση του δείγματος. Το γεγονός ότι οι συμμετέχοντες είναι αποκλειστικά μεταπτυχιακοί φοιτητές οικονομικής κατεύθυνσης σημαίνει ότι ενδέχεται να διαθέτουν υψηλότερο επίπεδο ψηφιακού γραμματισμού και εξοικείωσης με τραπεζικά θέματα σε σχέση με τον

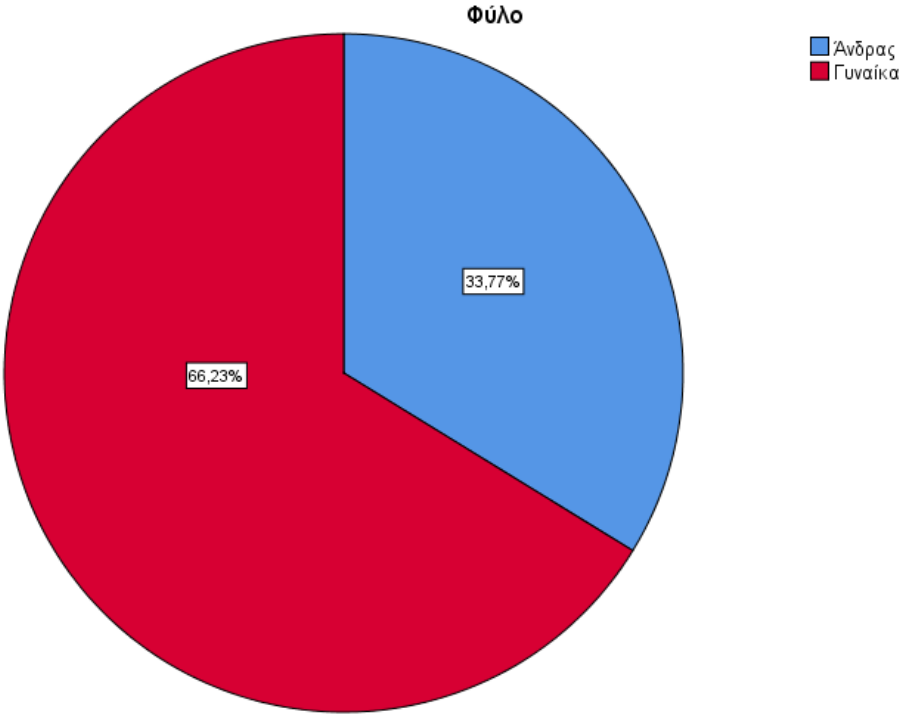
γενικό πληθυσμό, περιορίζοντας τη δυνατότητα γενίκευσης των συμπερασμάτων στο ευρύ κοινό.

Επιπλέον, το μέγεθος του δείγματος (N=151), αν και επαρκές για τις στατιστικές αναλύσεις που διενεργήθηκαν, παραμένει σχετικά μικρό. Ένας ακόμη περιορισμός σχετίζεται με τη φύση των ερωτηματολογίων αυτοαναφοράς, όπου οι απαντήσεις ενδέχεται να επηρεάζονται από την υποκειμενικότητα ή την τάση για κοινωνικά επιθυμητές απαντήσεις. Τέλος, ο συγχρονικός χαρακτήρας της έρευνας δεν επιτρέπει την εξαγωγή συμπερασμάτων για τη διαχρονική εξέλιξη της εμπιστοσύνης, αλλά παρέχει μόνο μια «εικόνα» της συγκεκριμένης στιγμής στην οποία συλλέχθηκαν τα δεδομένα.

Κεφάλαιο 5ο : Αποτελέσματα έρευνας

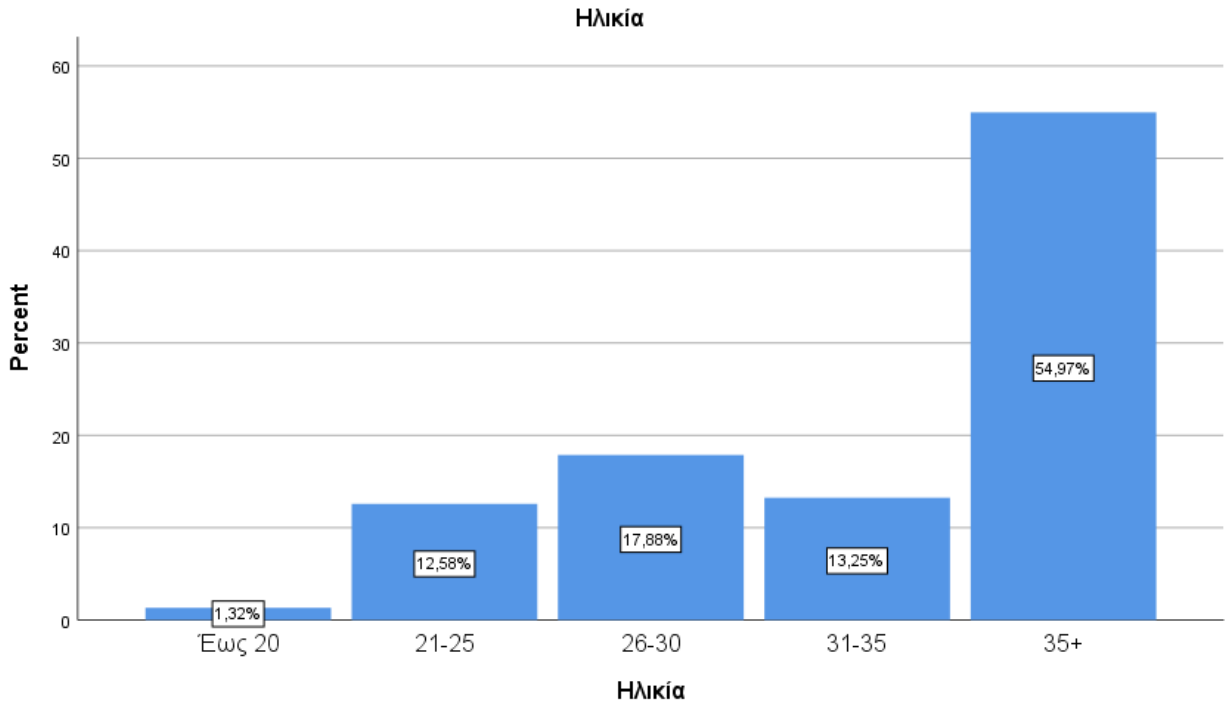
5.1 Δημογραφικά στοιχεία

Το δείγμα της έρευνας στηρίχθηκε σε ένα σύνολο 151 φοιτητών. Από το σύνολο αυτό, το 66,2% (n = 100) ανήκε σε γυναίκες και το υπόλοιπο 33,8% (n = 51) ανήκε σε άνδρες.



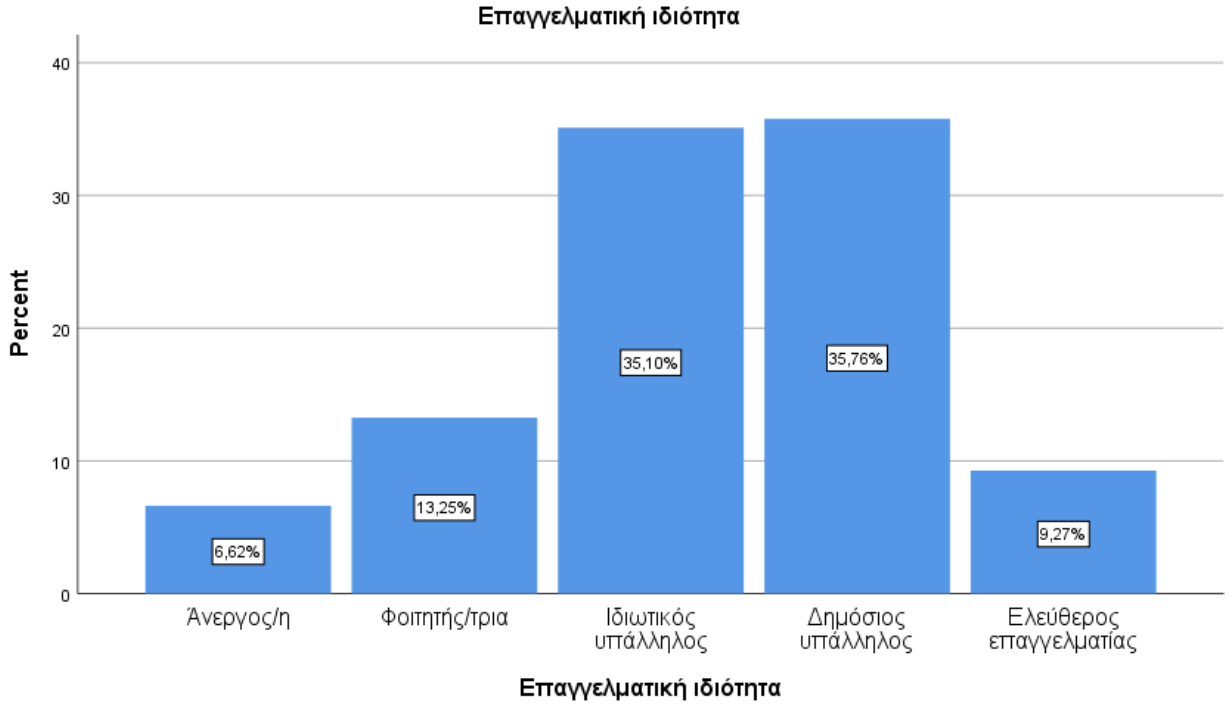
Διάγραμμα 1: Κατανομή φύλου

Στη συνέχεια, ζητήθηκε από τους ερωτηθέντες να σημειώσουν την ηλικία τους. Σύμφωνα με τα αποτελέσματα, η πλειοψηφία φτάνοντας το 55% (n = 83) ανήκε σε άτομα μεγαλύτερα των 35 ετών. Παράλληλα, το 31,1% (n = 47) ανήκε σε άτομα από 26 έως 35 ετών.



Διάγραμμα 2: Κατανομή ηλικίας

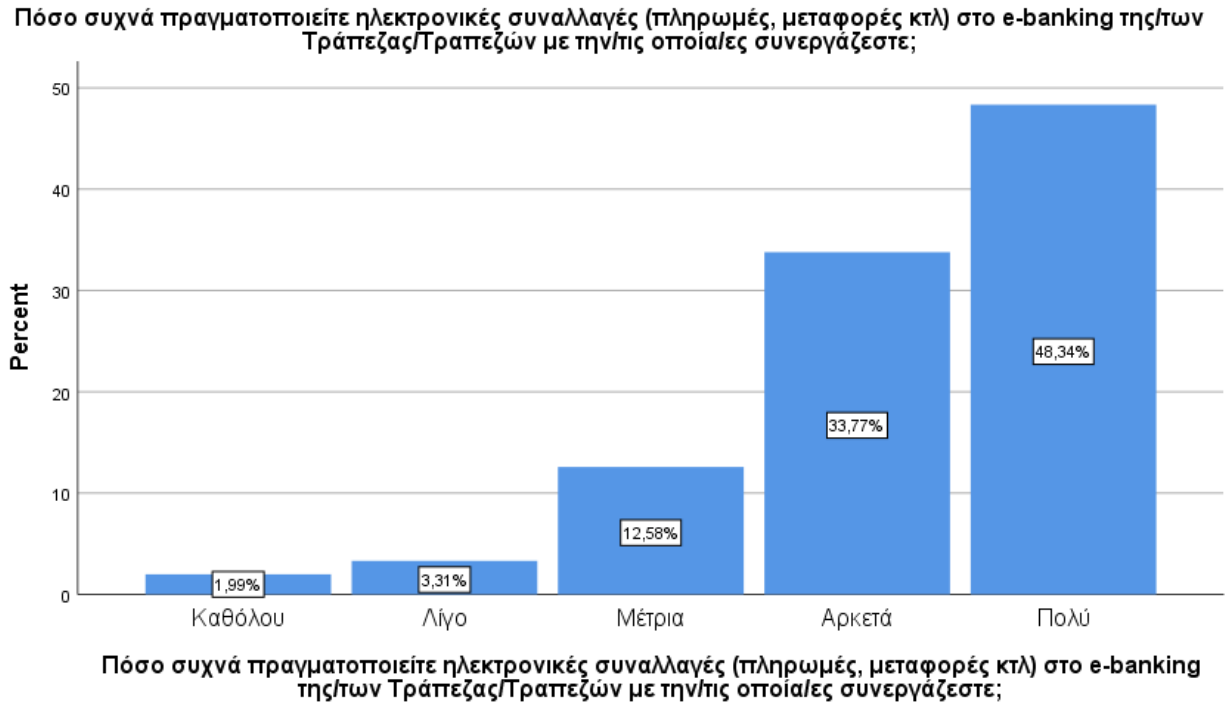
Ως προς την επαγγελματική ιδιότητα, δύο κατηγορίες ξεχώρισαν, οι δημόσιοι και οι ιδιωτικοί υπάλληλοι. Οι μεν αφορούσαν το 35,8% του δείγματος (n = 54) και οι δε αφορούσαν το 35,1% του δείγματος (n = 53).



Διάγραμμα 3: Κατανομή επαγγελματικής ιδιότητας

Το τελευταίο στοιχείο που ζητήθηκε από τους ερωτηθέντες πριν συμπληρώσουν το βασικό τμήμα του ερωτηματολογίου ήταν η συχνότητα πραγματοποίησης ηλεκτρονικών συναλλαγών στο e-banking της συνεργαζόμενης τράπεζας. Τα αποτελέσματα έδειξαν πως

η συντριπτική πλειοψηφία του δείγματος, η οποία έφτασε το 82,1% (n = 124) δήλωσε πως πραγματοποιεί τέτοιες συναλλαγές αρκετά ή πολύ συχνά.



Διάγραμμα 4: Κατανομή συχνότητας πραγματοποίησης ηλεκτρονικών συναλλαγών στο e-banking της συνεργαζόμενης τράπεζας

5.2 Ανάλυση αξιοπιστίας

Για τον έλεγχο της εσωτερικής συνέπειας (internal consistency) των κλιμάκων που χρησιμοποιήθηκαν στο ερωτηματολόγιο, υπολογίστηκε ο συντελεστής αξιοπιστίας Cronbach's alpha. Ο συγκεκριμένος δείκτης αποτελεί το πλέον διαδεδομένο μέτρο για την εκτίμηση της αξιοπιστίας σε ψυχομετρικά εργαλεία και κλίμακες Likert. Σύμφωνα με τη διεθνή βιβλιογραφία, τιμές του δείκτη άνω του 0,70 θεωρούνται αποδεκτές, ενώ τιμές άνω του 0,80 χαρακτηρίζονται ως πολύ ικανοποιητικές (Hair et al., 2019).

Όπως φαίνεται και από τα αντίστοιχα αποτελέσματα, όλες οι μεταβλητές της έρευνας εμφάνισαν τιμές για τον δείκτη Cronbach's alpha σημαντικά υψηλότερες από το ελάχιστο αποδεκτό όριο του 0,70. Συγκεκριμένα, η κλίμακα της «Ασφάλειας» σημείωσε εξαιρετικά υψηλή αξιοπιστία (alpha = 0,954), όπως και η «Αντιληπτή Ιδιωτικότητα» (alpha = 0,936). Ακόμη και η κλίμακα με τη χαμηλότερη τιμή, η «Αντιληπτή Καλοσύνη» (alpha = 0,777), κυμάνθηκε σε ικανοποιητικά επίπεδα. Τα αποτελέσματα αυτά επιβεβαιώνουν ότι οι ερωτήσεις που συγκροτούν την κάθε μεταβλητή παρουσιάζουν υψηλή συνοχή μεταξύ τους και μετρούν με συνέπεια την ίδια έννοια.

Πίνακας 1: Αξιοπιστία μεταβλητών έρευνας

Μεταβλητή	Αριθμός ερωτήσεων	Cronbach's alpha
Ασφάλεια	5	0,954
Αντιληπτός κίνδυνος	3	0,894
Εμπιστοσύνη	3	0,910
Αντιληπτή ιδιωτικότητα	5	0,936
Αντιληπτή ικανότητα	3	0,876
Αντιληπτή ακεραιότητα	2	0,920
Αντιληπτή καλοσύνη	2	0,777

5.3 Περιγραφικά στοιχεία ασφάλειας

Όπως παρατηρείται από τα σχετικά αποτελέσματα, ο μέσος όρος της αίσθησης ασφάλειας στην πραγματοποίηση ηλεκτρονικών συναλλαγών διαμορφώνεται στο 3,40 (M=3,40), με τυπική απόκλιση 1,62 (SD=1,62). Λαμβάνοντας υπόψη ότι η κλίμακα μέτρησης ήταν επταβάθμια (1-7), η τιμή αυτή βρίσκεται κάτω από το θεωρητικό μέσο της κλίμακας (το 4). Το εύρημα αυτό υποδηλώνει ότι οι συμμετέχοντες διατηρούν, κατά μέσο όρο, μια μέτρια προς χαμηλή αίσθηση ασφάλειας κατά τη διενέργεια ηλεκτρονικών συναλλαγών, εκφράζοντας έναν βαθμό επιφυλακτικότητας.

Επιπρόσθετα, η σχετικά υψηλή τυπική απόκλιση (1,62) υποδεικνύει σημαντική διασπορά στις απαντήσεις του δείγματος, γεγονός που σημαίνει ότι δεν υπάρχει ομοφωνία μεταξύ των φοιτητών, καθώς παρατηρούνται διακυμάνσεις από την απόλυτη διαφωνία (Min = 1) έως την απόλυτη συμφωνία (Max = 7).

Πίνακας 2: Περιγραφικά στοιχεία ασφάλειας

	N	Minimum	Maximum	Mean	Std. Deviation
Ασφάλεια	151	1,00	7,00	3,3987	1,61963
Valid N (listwise)	151				

5.4 Περιγραφικά στοιχεία εμπιστοσύνης

Στη συνέχεια παρουσιάζονται τα περιγραφικά στατιστικά αποτελέσματα για τη μεταβλητή της εμπιστοσύνης οι οποία εκφράζεται από τις έξι επιμέρους διαστάσεις της (Αντιληπτός Κίνδυνος, Εμπιστοσύνη, Αντιληπτή Ιδιωτικότητα, Αντιληπτή Ικανότητα, Αντιληπτή Ακεραιότητα, Αντιληπτή Καλοσύνη). Οι απαντήσεις δόθηκαν σε επταβάθμια κλίμακα, όπου η τιμή 4 αντιπροσωπεύει το ουδέτερο σημείο.

Παρατηρώντας τα δεδομένα, διαπιστώνεται μια σαφής διαφοροποίηση στις αντιλήψεις των συμμετεχόντων ανάλογα με τη διάσταση που εξετάζεται. Συγκεκριμένα παρατηρείται πως για την Αντιληπτή Ικανότητα (M=4,32) και Ακεραιότητα (M=4,29) καταγράφονται οι υψηλότερες μέσες τιμές, όντας οι μοναδικές που υπερβαίνουν το ουδέτερο σημείο της κλίμακας (4). Αυτό υποδηλώνει ενδεχομένως ότι οι φοιτητές αναγνωρίζουν την τεχνική επάρκεια των τραπεζικών συστημάτων και θεωρούν ότι οι τράπεζες λειτουργούν με έναν βαθμό εντιμότητας.

Προχωρώντας στην Εμπιστοσύνη (M=3,84) φαίνεται πως η συνολική αίσθηση εμπιστοσύνης κινείται οριακά κάτω από το μέσο της κλίμακας. Το γεγονός αυτό φανερώνει μια στάση επιφυλακτικότητας και δισταγμού από την πλευρά των χρηστών, οι οποίοι δεν δηλώνουν απόλυτα πεπεισμένοι για την αξιοπιστία των ηλεκτρονικών υπηρεσιών. Η μέση τιμή για την Αντιληπτή Καλοσύνη έφτασε τις 3,74 μονάδες. Η τιμή αυτή υποδεικνύει ότι οι συμμετέχοντες αμφιβάλλουν μετριοπαθώς για το κατά πόσο οι τράπεζες δρουν με γνώμονα το συμφέρον και την ευημερία του πελάτη. Ομοίως, στην περίπτωση της Αντιληπτής Ιδιωτικότητας η μέση τιμή ήταν οι 3,42 μονάδες καταγράφοντας έτσι μια από τις χαμηλότερες τιμές, εύρημα που συνάδει με το χαμηλό αίσθημα ασφάλειας που εντοπίστηκε προηγουμένως. Οι χρήστες φαίνεται να ανησυχούν σημαντικά για την προστασία των προσωπικών τους δεδομένων.

Τέλος, στην διάσταση του Αντιληπτού Κινδύνου η μέση τιμή ήταν 3,24. Η χαμηλή αυτή τιμή και σε συνδυασμό με τη μέτρια εμπιστοσύνη, δείχνει ότι οι χρήστες αντιλαμβάνονται την ύπαρξη κινδύνου σε μέτριο βαθμό αλλά με μια τάση προς την αρνητική πλευρά. Γενικότερα, σε όλες τις μεταβλητές, οι τυπικές αποκλίσεις κυμαίνονται σε υψηλά επίπεδα (από 1,51 έως 1,62), γεγονός που επιβεβαιώνει την ύπαρξη σημαντικής ανομοιογένειας στις απόψεις του δείγματος.

Συνοψίζοντας λοιπόν, προκύπτει μια ενδιαφέρουσα αντίφαση στις στάσεις των φοιτητών. Από τη μία πλευρά, αναγνωρίζουν την τεχνική επάρκεια και την ακεραιότητα των τραπεζικών συστημάτων (υψηλότεροι μέσοι όροι), γεγονός που υποδηλώνει ότι

θεωρούν τις πλατφόρμες λειτουργικές και τις τράπεζες θεσμικά έντιμες. Από την άλλη πλευρά, ωστόσο, αυτή η αναγνώριση δεν μεταφράζεται σε υψηλά επίπεδα συνολικής εμπιστοσύνης ή αισθήματος ασφάλειας.

Οι χαμηλότερες τιμές στην ιδιωτικότητα και την ασφάλεια, σε συνδυασμό με τη μέτρια γενική εμπιστοσύνη, φανερώνουν ότι οι ανησυχίες των χρηστών δεν εστιάζονται στο αν λειτουργεί ομαλά το κάθε σύστημα, αλλά στο αν τα δεδομένα παραμένουν ουσιαστικά προστατευμένα. Συνεπώς, φαίνεται πως το έλλειμμα εμπιστοσύνης πηγάζει κυρίως από τον φόβο παραβίασης της ιδιωτικότητας και όχι από αμφισβήτηση της ομαλής λειτουργίας των τραπεζικών συστημάτων.

Πίνακας 3: Περιγραφικά στοιχεία εμπιστοσύνης

	N	Minimum	Maximum	Mean	Std. Deviation
Αντιληπτός Κίνδυνος	151	1,00	7,00	3,2428	1,57712
Εμπιστοσύνη	151	1,00	7,00	3,8389	1,56813
Αντιληπτή ιδιωτικότητα	151	1,00	7,00	3,4212	1,53469
Αντιληπτή ικανότητα	151	1,00	7,00	4,3245	1,53089
Αντιληπτή ακεραιότητα	151	1,00	7,00	4,2914	1,51146
Αντιληπτή καλοσύνη	151	1,00	7,00	3,7384	1,61538
Valid N (listwise)	151				

5.5 Έλεγχος κατανομής μεταβλητών έρευνας

Σε αυτή την ενότητα, παρουσιάζονται τα αποτελέσματα του ελέγχου για την κανονικότητα της κατανομής των μεταβλητών, ο οποίος είναι απαραίτητος για την επιλογή των κατάλληλων στατιστικών ελέγχων (παραμετρικών ή μη-παραμετρικών) που θα ακολουθήσουν.

Για τον έλεγχο της κανονικότητας των δεδομένων, εφαρμόστηκε το τεστ Kolmogorov-Smirnov (K-S) για κάθε μία από τις μεταβλητές της έρευνας. Η μηδενική υπόθεση (H0) του τεστ είναι ότι τα δεδομένα ακολουθούν κανονική κατανομή. Εάν η σημαντικότητα (Sig. ή p-value) είναι μικρότερη από το επίπεδο σημαντικότητας alpha = 0.05, η H0 απορρίπτεται, υποδεικνύοντας ότι η κατανομή δεν είναι κανονική.

Επομένως, απορρίπτεται η Η0 για όλες τις μεταβλητές και όλες οι εξεταζόμενες μεταβλητές παρουσίασαν στατιστικά σημαντική απόκλιση από την κανονική κατανομή. Άρα, δεν μπορεί να υποτεθεί κανονικότητα για καμία από τις μεταβλητές που μελετήθηκαν.

Δεδομένου ότι το σύνολο των μεταβλητών απέτυχε στον έλεγχο κανονικότητας, η απαίτηση για χρήση παραμετρικών ελέγχων (όπως t-test, ANOVA) δεν πληρείται.

Ως εκ τούτου, για τις περαιτέρω αναλύσεις και την εξέταση των ερευνητικών ερωτημάτων της έρευνας, θα χρησιμοποιηθούν μη παραμετρικές στατιστικές μέθοδοι, οι οποίες δεν απαιτούν την προϋπόθεση της κανονικής κατανομής των δεδομένων. Έτσι, αντί για t-tests ή ANOVA, θα χρησιμοποιηθούν οι μη-παραμετρικοί ισοδύναμοί τους, όπως το τεστ Mann-Whitney U ή το Kruskal-Wallis H. Για την περίπτωση συσχετίσεων θα χρησιμοποιηθεί ο δείκτης rho του Spearman αντίστοιχα.

Πίνακας 4: Έλεγχος κατανομής μεταβλητών έρευνας

	Kolmogorov-Smirnov		
	Statistic	df	Sig.
Ασφάλεια	,120	151	,000
Αντιληπτός Κίνδυνος	,124	151	,000
Εμπιστοσύνη	,101	151	,001
Αντιληπτή ιδιωτικότητα	,093	151	,003
Αντιληπτή ικανότητα	,134	151	,000
Αντιληπτή ακεραιότητα	,137	151	,000
Αντιληπτή καλοσύνη	,120	151	,000

5.6 Συσχέτιση ασφάλειας και διαστάσεωνεμπιστοσύνης

Στη συνέχεια παρουσιάζονται οι συντελεστές συσχέτισης (Spearman'srho) μεταξύ όλων των μελετώμενων μεταβλητών. Όπως φαίνεται από τα αποτελέσματα, όλες οι συσχετίσεις είναι στατιστικά σημαντικές στο επίπεδο $p < 0.01$, γεγονός που επιβεβαιώνει την ύπαρξη ισχυρών γραμμικών σχέσεων μεταξύ των μεταβλητών.

Αναλυτικότερα, εξετάζοντας τον πίνακα συσχετίσεων, η μεταβλητή Ασφάλεια παρουσιάζει στατιστικά σημαντικές και θετικές συσχετίσεις ($p < 0.01$) με όλες τις υπόλοιπες μεταβλητές. Αυτό επιβεβαιώνει τη θέση της Ασφάλειας ως κεντρικού παράγοντα που συνδέεται άμεσα με τις αντιλήψεις κινδύνου, ιδιωτικότητας και εμπιστοσύνης.

Αναλυτικότερα, η Ασφάλεια συσχετίζεται σε ισχυρότερο βαθμό με την Εμπιστοσύνη (rho = 0.660). Αυτή η ισχυρή, θετική συσχέτιση υποδηλώνει ότι όσο υψηλότερα αντιλαμβάνονται οι χρήστες το επίπεδο ασφάλειας ενός συστήματος ή μιας υπηρεσίας, τόσο αυξάνεται και η συνολική τους εμπιστοσύνη προς αυτόν τον φορέα.

Σε επίπεδο επιμέρους διαστάσεων, η Ασφάλεια συνδέεται σημαντικά με την Αντιληπτή ιδιωτικότητα (rho = 0.614). Αυτό το εύρημα υπογραμμίζει την αλληλεξάρτηση μεταξύ της τεχνικής προστασίας (Ασφάλεια) και της προστασίας των προσωπικών δεδομένων (Ιδιωτικότητα), θέτοντας την ασφάλεια ως προϋπόθεση για την αίσθηση ιδιωτικότητας.

Ακόμα, η Ασφάλεια συσχετίζεται μέτρια με την Αντιληπτή ικανότητα (rho = 0.565), την Αντιληπτή ακεραιότητα (r = 0.549) και τον Αντιληπτό Κίνδυνο (rho = 0.531). Η μέτρια ένταση αυτών των συσχετίσεων δείχνει ότι η αντίληψη για την Ασφάλεια ενισχύει την πεποίθηση ότι το σύστημα της τράπεζας είναι τεχνικά επαρκές (αφορώντας την μεταβλητή της Ικανότητας) και δίκαιο/έντιμο (αφορώντας την μεταβλητή της Ακεραιότητας). Η θετική συσχέτιση με τον Αντιληπτό Κίνδυνο είναι ιδιαίτερα ενδιαφέρουσα, καθώς, αν και οι έννοιες είναι εννοιολογικά αντίθετες, η αύξηση της Ασφάλειας μπορεί να οδηγεί σε μεγαλύτερη συνειδητοποίηση των κινδύνων που διαχειρίζεται το σύστημα, καθιστώντας τον κίνδυνο πιο αντιληπτό, ή να αντικατοπτρίζει την αντίληψη ότι η ασφάλεια είναι απαραίτητη ακριβώς επειδή ο κίνδυνος είναι υψηλός.

Τέλος, η ασθενέστερη αλλά και πάλι σημαντική συσχέτιση παρατηρείται με την Αντιληπτή καλοσύνη (rho = 0.364). Αυτό υποδηλώνει ότι, αν και η Ασφάλεια συμβάλλει στην αντίληψη ότι η τράπεζα ενδιαφέρεται για τον χρήστη, ο παράγοντας της Καλοσύνης επηρεάζεται σε μεγαλύτερο βαθμό από άλλες διαστάσεις ή συναισθηματικούς παράγοντες, πέρα από τα καθαρά τεχνικά μέτρα ασφάλειας.

Συνολικά, η ανάλυση επιβεβαιώνει τον πολυδιάστατο ρόλο της Ασφάλειας στο πλαίσιο της έρευνας, καθώς η αντίληψη για αυτήν επηρεάζει θετικά τόσο την ιδιωτικότητα όσο και όλες τις μορφές εμπιστοσύνης, ενώ παράλληλα διατηρεί στενή σχέση με τον αντιληπτό κίνδυνο.

Πίνακας 5: Συσχετίσεις ασφάλειας και διαστάσεων εμπιστοσύνης

	1	2	3	4	5	6	7
Ασφάλεια	1,000						
Αντιληπτός Κίνδυνος	,531**	1,000					
Εμπιστοσύνη	,660**	,694**	1,000				
Αντιληπτή ιδιωτικότητα	,614**	,681**	,818**	1,000			
Αντιληπτή ικανότητα	,565**	,584**	,790**	,689**	1,000		
Αντιληπτή ακεραιότητα	,549**	,535**	,656**	,614**	,855**	1,000	,*
Αντιληπτή καλοσύνη	,364**	,376**	,494**	,530**	,656**	,693**	1,000

**. Correlation is significant at the 0.01 level (2-tailed).

5.7 Διαφοροποίηση μεταβλητών έρευνας από τα δημογραφικά στοιχεία

5.7.1 Φύλο

Για την διερεύνηση της διαφοροποίηση που προκαλεί το φύλο των συμμετεχόντων στις μεταβλητές της έρευνας χρησιμοποιήθηκε ο έλεγχος MannWhitneyU. Η κατανομή των μεταβλητών δεν θεωρείται κανονική και το φύλο χωρίζεται σε δύο κατηγορίες. Έτσι, επιλέχθηκε ο συγκεκριμένος έλεγχος για την διερεύνηση της διαφοροποίησης των μεταβλητών εξαιτίας του φύλου.

Τα αποτελέσματα που προέκυψαν δεν ήταν στατιστικά σημαντικά σε καμία περίπτωση. Η μηδενική υπόθεση (H0) του τεστ είναι ότι το φύλο δεν επηρεάζει τις μεταβλητές της έρευνας. Επομένως, εφόσον τα αποτελέσματα δεν είναι στατιστικά σημαντικά, προκύπτει το συμπέρασμα πως το φύλο δεν διαφοροποιεί στατιστικά σημαντικά τις μεταβλητές της έρευνας.

Πίνακας 6: Αποτελέσματα επιρροής φύλου στις μεταβλητές της έρευνας

	Ασφάλεια	Αντιληπτός Κίνδυνος	Εμπιστοσύνη	Αντιληπτή ιδιωτικότητα	Αντιληπτή ικανότητα	Αντιληπτή ακεραιότητα	Αντιληπτή καλοσύνη
Mann-Whitney U	2296,000	2139,000	2446,500	2441,000	2388,000	2544,500	2428,500
Wilcoxon W	7346,000	7189,000	7496,500	7491,000	7438,000	7594,500	3754,500
Z	-1,001	-1,622	-,408	-,429	-,640	-,022	-,480
Asymp. Sig. (2-tailed)	,317	,105	,683	,668	,522	,983	,631

a. Grouping Variable: Φύλο

5.7.2 Ηλικία

Η διαφοροποίηση που προκαλεί η ηλικία των συμμετεχόντων στις μεταβλητές της έρευνας διερευνήθηκε μέσω του ελέγχου KruskalWallis. Εφόσον, η κατανομή των μεταβλητών δεν θεωρείται κανονική και ηλικία χωρίζεται σε πάνω από δύο κατηγορίες, προτιμήθηκε ο έλεγχος αυτός για τον έλεγχο της διαφοροποίησης των μεταβλητών εξαιτίας της ηλικίας.

Όπως και στην περίπτωση της ηλικίας, τα αντίστοιχα αποτελέσματα δεν θεωρούνται στατιστικά σημαντικά για καμία μεταβλητή που ελέγχθηκε. Η μηδενική υπόθεση (H0) του τεστ είναι ότι η ηλικία δεν διαφοροποιεί τις μεταβλητές της έρευνας. Επομένως, μιας και τα αποτελέσματα δεν είναι στατιστικά σημαντικά, μπορεί να ειπωθεί πως η ηλικία δεν διαφοροποιεί με στατιστικά σημαντικό τρόπο τις μεταβλητές της έρευνας.

Πίνακας 7: Αποτελέσματα επιρροής ηλικίας στις μεταβλητές της έρευνας

	Ασφάλεια	Αντιληπτός Κίνδυνος	Εμπιστοσύνη	Αντιληπτή ιδιωτικότητα	Αντιληπτή ικανότητα	Αντιληπτή ακεραιότητα	Αντιληπτή καλοσύνη
Kruskal-Wallis H	5,251	2,542	5,022	3,923	9,049	3,144	4,650
df	4	4	4	4	4	4	4
Asymp. Sig.	,263	,637	,285	,417	,060	,534	,325

a. Kruskal Wallis Test

b. Grouping Variable: Ηλικία

5.7.3 Επαγγελματική ιδιότητα

Η διαφοροποίηση των μεταβλητών της έρευνας εξαιτίας της επαγγελματικής τους ιδιότητας διερευνήθηκε μέσω του ελέγχου KruskalWallis και πάλι. Ο έλεγχος αυτός προτιμήθηκε εφόσον οι μεταβλητές της έρευνας δεν ακολουθούν την κανονική κατανομή και η μεταβλητή της επαγγελματικής ιδιότητας περιείχε περισσότερες από δύο κατηγορίες.

Τα αποτελέσματα που επέστρεψε ο έλεγχος που πραγματοποιήθηκε δεν θεωρούνται στατιστικά σημαντικά σε καμία από τις μεταβλητές της έρευνας που ελέγχθηκαν. Η μηδενική υπόθεση (H0) του τεστ είναι ότι η επαγγελματική ιδιότητα δεν διαφοροποιεί τις μεταβλητές της έρευνας. Επομένως, εφόσον ο έλεγχος δεν επέστρεψε στατιστικά σημαντικά αποτελέσματα, συμπεραίνεται πως η επαγγελματική ιδιότητα δεν διαφοροποιεί με στατιστικά σημαντικό τρόπο τις μεταβλητές της έρευνας.

Πίνακας 8: Αποτελέσματα επιρροής επαγγελματικής ιδιότητας στις μεταβλητές της έρευνας

	Ασφάλεια	Αντιληπτός Κίνδυνος	Εμπιστοσύνη	Αντιληπτή ιδιωτικότητα	Αντιληπτή ικανότητα	Αντιληπτή ακεραιότητα	Αντιληπτή καλοσύνη
Kruskal-Wallis H	3,747	2,645	2,429	1,873	4,018	3,917	2,619
df	4	4	4	4	4	4	4
Asymp. Sig.	,441	,619	,657	,759	,404	,417	,623

a. Kruskal Wallis Test

b. Grouping Variable: Επαγγελματική ιδιότητα

5.7.4 Συχνότητα πραγματοποίησης ηλεκτρονικών συναλλαγών

Για την διερεύνηση της διαφοροποίηση που προκαλεί η συχνότητα με την οποία οι συμμετέχοντες πραγματοποιούν ηλεκτρονικές συναλλαγές στο e-banking της τράπεζάς τους στις μεταβλητές της έρευνας χρησιμοποιήθηκε ο έλεγχος KruskalWallis. Η κατανομή των μεταβλητών δεν θεωρείται κανονική και η συχνότητα συναλλαγών χωρίζεται σε περισσότερες των δύο κατηγορίες. Έτσι, επιλέχθηκε ο συγκεκριμένος έλεγχος για την διερεύνηση της διαφοροποίησης των μεταβλητών εξαιτίας της συχνότητας συναλλαγών.

Τα αποτελέσματα που επέστρεψε ο έλεγχος που πραγματοποιήθηκε θεωρούνται στατιστικά σημαντικά σε κάποιες από τις μεταβλητές της έρευνας που ελέγχθηκαν. Η μηδενική υπόθεση (H0) του τεστ είναι ότι η συχνότητα συναλλαγών δεν διαφοροποιεί τις μεταβλητές της έρευνας. Επομένως, εφόσον ο έλεγχος επέστρεψε στατιστικά σημαντικά αποτελέσματα σε ορισμένες μεταβλητές, συμπεραίνεται πως η συχνότητα συναλλαγών διαφοροποιεί με στατιστικά σημαντικό τρόπο τις μεταβλητές της Ασφάλειας (p = .003), της Εμπιστοσύνης (p = .002), της Αντιληπτής ιδιωτικότητας (p = .017) και της Αντιληπτής ικανότητας (p = .017).

Πίνακας 9: Αποτελέσματα επιρροής συχνότητας συναλλαγών στις μεταβλητές της έρευνας

	Ασφάλεια	Αντιληπτός Κίνδυνος	Εμπιστοσύνη	Αντιληπτή ιδιωτικότητα	Αντιληπτή ικανότητα	Αντιληπτή ακεραιότητα	Αντιληπτή καλοσύνη
Kruskal-Wallis H	15,798	7,166	17,478	11,982	12,098	6,559	7,463
df	4	4	4	4	4	4	4
Asymp. Sig.	,003	,127	,002	,017	,017	,161	,113

a. Kruskal Wallis Test

b. Grouping Variable: Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο e-banking της συνεργαζόμενης τράπεζας

Προκειμένου να διερευνηθεί ανάμεσα σε ποιες κατηγορίες συχνότητας συναλλαγών υπήρχαν οι στατιστικά σημαντικές διαφοροποιήσεις των μεταβλητών της έρευνας, έγιναν ζευγαρωτές συγκρίσεις για όλες τις περιπτώσεις.

Αρχικά, παρατηρείται πως τα επίπεδα ασφάλειας σύμφωνα με τους συμμετέχοντες, είναι στατιστικά σημαντικά μεγαλύτερα για τα άτομα που πραγματοποιούν πολύ συχνά ηλεκτρονικές συναλλαγές στο ebanking της συνεργαζόμενης τράπεζας, σε σύγκριση με τα άτομα που πραγματοποιούν μέτρια ή και αρκετά συχνά αντίστοιχες ηλεκτρονικές συναλλαγές. Άρα η αίσθηση ασφάλειας είναι μεγαλύτερα στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά ηλεκτρονικές συναλλαγές.

Πίνακας 10: Ζευγαρωτές συγκρίσεις Ασφάλειας ως προς την συχνότητα συναλλαγών

Dependent Variable	(I) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	(J) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	Mean Difference (I-J)	Sig.
Ασφάλεια	Καθόλου	Λίγο	-,66667	,460
		Μέτρια	-1,11930	,210
		Αρκετά	-1,39216	,101
		Πολύ	-2,13516	,151
	Λίγο	Καθόλου	,66667	,460
		Μέτρια	-,45263	,634
		Αρκετά	-,72549	,353
		Πολύ	-1,46849	,054
	Μέτρια	Καθόλου	1,11930	,210
		Λίγο	,45263	,634
		Αρκετά	-,27286	,466
		Πολύ	**-1,01586**	**,011**

	Αρκετά	Καθόλου	1,39216	,634
		Λίγο	,72549	,353
		Μέτρια	,27286	,466
		Πολύ	**-,74300**	**,012**
	Πολύ	Καθόλου	2,13516	,151
		Λίγο	1,46849	,054
		Μέτρια	1,01586	,011
		Αρκετά	,74300	,012

Ακόμα, παρατηρείται πως τα επίπεδα εμπιστοσύνης σύμφωνα με τους συμμετέχοντες, είναι στατιστικά σημαντικά μεγαλύτερα για τα άτομα που πραγματοποιούν μέτρια συχνά, αρκετά συχνά ή πολύ συχνά ηλεκτρονικές συναλλαγές στο ebanking της συνεργαζόμενης τράπεζας, σε σύγκριση με τα άτομα που δεν πραγματοποιούν καθόλου συχνά αντίστοιχες ηλεκτρονικές συναλλαγές. Το ίδιο ισχύει και για τα άτομα που πραγματοποιούν πολύ συχνά ηλεκτρονικές συναλλαγές του ebanking, σε σύγκριση με τα άτομα που πραγματοποιούν αρκετά ή και μέτρια συχνά τέτοιες συναλλαγές. Επομένως, η αίσθηση εμπιστοσύνης γενικότερα είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά ηλεκτρονικές συναλλαγές.

Πίνακας 11: Ζευγαρωτές συγκρίσεις Εμπιστοσύνης ως προς την συχνότητα συναλλαγών

Dependent Variable	(I) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	(J) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	Mean Difference (I-J)	Sig.
Εμπιστοσύνη	**Καθόλου**	Λίγο	-1,95556	,117
		Μέτρια	**-2,23977**	**,034**
		Αρκετά	**-2,55556**	**,010**
		Πολύ	**-3,14003**	**,001**
	Λίγο	Καθόλου	1,95556	**,748**
		Μέτρια	-,28421	,738

		Αρκετά	-,60000	,420
		Πολύ	-1,18447	,097
	Μέτρια	Καθόλου	2,23977	,034
		Λίγο	,28421	,738
		Αρκετά	-,31579	,434
		Πολύ	**-,90026**	**,020**
	Αρκετά	Καθόλου	2,55556	,010
		Λίγο	,60000	,420
		Μέτρια	,31579	,434
		Πολύ	**-,58447**	**,033**
	Πολύ	Καθόλου	3,14003*	,001
		Λίγο	1,18447	097
		Μέτρια	,90026	,020
		Αρκετά	,58447	,033

Παρομοίως, παρατηρείται πως τα επίπεδα Αντιληπτής ιδιωτικότητας, είναι στατιστικά σημαντικά μεγαλύτερα στα άτομα που πραγματοποιούν μέτρια συχνά, αρκετά συχνά ή πολύ συχνά ηλεκτρονικές συναλλαγές, σε σχέση με τα άτομα που δεν πραγματοποιούν καθόλου συχνά τέτοιες ηλεκτρονικές συναλλαγές.

Αυτό οδηγεί στο συμπέρασμα πως η αίσθηση ιδιωτικότητας είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές στο ebanking, σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά τέτοιες ηλεκτρονικές συναλλαγές.

Πίνακας 12: Ζευγαρωτές συγκρίσεις Αντιληπτής ιδιωτικότητας ως προς την συχνότητα συναλλαγών

Dependent Variable	(I) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	(J) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	Mean Difference (I-J)	Sig.
Αντιληπτή ιδιωτικότητα	**Καθόλου**	Λίγο	-1,62667	,095
		Μέτρια	**-1,78246**	**,046**

	Αρκετά	**-1,89020**	**,024**
	Πολύ	**-2,42283**	**,004**
Λίγο	Καθόλου	1,62667	,095
	Μέτρια	-,15579	,968
	Αρκετά	-,26353	,791
	Πολύ	-,79616	,314
Μέτρια	Καθόλου	1,78246	,046
	Λίγο	,15579	,968
	Αρκετά	-,10774	,699
	Πολύ	-,64037	,084
Αρκετά	Καθόλου	1,89020	,024
	Λίγο	,26353	,791
	Μέτρια	,10774	,699
	Πολύ	-,53263	,062
Πολύ	Καθόλου	2,42283	,004
	Λίγο	,79616	,314
	Μέτρια	,64037	,084
	Αρκετά	,53263	,062

Όμοια δεδομένα έδειξαν και οι έλεγχοι για την Αντιληπτή ικανότητα. Αναλυτικότερα, παρατηρείται πως τα επίπεδα Αντιληπτής ικανότητας, είναι στατιστικά σημαντικά μεγαλύτερα στα άτομα που πραγματοποιούν μέτρια συχνά, αρκετά συχνά ή πολύ συχνά ηλεκτρονικές συναλλαγές, σε σχέση με τα άτομα που δεν πραγματοποιούν καθόλου συχνά τέτοιες ηλεκτρονικές συναλλαγές.

Αυτό οδηγεί στο συμπέρασμα πως αίσθηση για την ικανότητα της τράπεζας να παρέχει αποδοτικές και αξιόπιστες υπηρεσίες online τραπεζικής είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές στο ebanking, σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά τέτοιες ηλεκτρονικές συναλλαγές.

Πίνακας 13: Ζευγαρωτές συγκρίσεις Αντιληπτής ιδιωτικότητας ως προς την συχνότητα συναλλαγών

Dependent Variable	(I) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	(J) Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές στο ebanking	Mean Difference (I-J)	Sig.
Αντιληπτή ικανότητα	**Καθόλου**	Λίγο	-1,60000	,292
		Μέτρια	**-2,08772**	**,053**
		Αρκετά	**-2,15686**	**,036**
		Πολύ	**-2,64840**	**,007**
	Λίγο	Καθόλου	1,60000	,292
		Μέτρια	-,48772	,391
		Αρκετά	-,55686	,312
		Πολύ	-1,04840	,078
	Μέτρια	Καθόλου	2,08772	,053
		Λίγο	,48772	,391
		Αρκετά	-,06914	,873
		Πολύ	-,56068	,138
	Αρκετά	Καθόλου	2,15686	,036
		Λίγο	,55686	,312
		Μέτρια	,06914	,873
		Πολύ	-,49154	,063
	Πολύ	Καθόλου	2,64840	,007
		Λίγο	1,04840	,078
		Μέτρια	,56068	,138
		Αρκετά	,49154	,720

Κεφάλαιο 6ο: Συμπεράσματα – Συζήτηση

Ο σκοπός της παρούσας έρευνας εστίαζε στη διερεύνηση δύο βασικών παραγόντων που σχετίζονται άμεσα με τη συμπεριφορά των καταναλωτών στο ψηφιακό περιβάλλον. Ο πρώτος παράγοντας σχετίζονταν με το αίσθημα ασφάλειας και ο δεύτερος αφορούσε την εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές. Παράλληλα, βασικός στόχος της έρευνας ήταν και η διερεύνηση της επιρροής των κοινωνικοδημογραφικών χαρακτηριστικών στις δύο αυτές έννοιες.

Από την έρευνα, η οποία έγινε σε ένα δείγμα 151 ατόμων, προκύπτει ότι το ποσοστό των πολιτών που πραγματοποιούν συχνά η πολύ συχνά ηλεκτρονικές συναλλαγές είναι υψηλό. Τα στοιχεία αυτά δείχνουν αφενός ότι οι ηλεκτρονικές συναλλαγές αποτελούν μια παγιωμένη συνήθεια τη σύγχρονης εποχής, και αφετέρου ότι τα δεδομένα που συλλέχθηκαν από την έρευνα είναι έγκυρα.

Κάνοντας μια γενική προσέγγιση φαίνεται ως βασικό εύρημα ότι η εμπειρία και η εξοικείωση με τις ηλεκτρονικές συναλλαγές λειτουργούν ως καθοριστικός παράγοντας. Στο πλαίσιο αυτό, λοιπόν, προκύπτει ότι η συχνή πραγματοποίηση ηλεκτρονικών συναλλαγών, δημιουργεί μεγαλύτερη αίσθηση ασφάλειας, εμπιστοσύνης και ιδιωτικότητας. Τα στοιχεία αυτά συνάδουν με παρόμοιες βιβλιογραφικές έρευνες, στις οποίες αναδεικνύεται το γεγονός ότι η επαναλαμβανόμενη χρήση ψηφιακών τραπεζικών υπηρεσιών, επιφέρει εξοικείωση, μειώνει την αβεβαιότητα και δημιουργεί σχέσεις (Gefen, Karahanna & Straub, 2003· Kim, Ferrin & Rao, 2008).

Αναφορικά με την ασφάλεια των ηλεκτρονικών συναλλαγών, οι συμμετέχοντες διατηρούν, κατά μέσο όρο, μια μέτρια προς χαμηλή αίσθηση ασφάλειας κατά τη διενέργεια ηλεκτρονικών συναλλαγών, εκφράζοντας έναν βαθμό επιφυλακτικότητας. Ανάλογα είναι και τα πορίσματα όμοιων ερευνών, των οποίων οι συμμετέχοντες, ναι μεν αναγνωρίζουν την τεχνολογική πρόοδο και την ευκολία που παρέχεται από τα ηλεκτρονικά συστήματα, αλλά δεν παύουν να διατηρούν επιφυλάξεις για την ασφάλεια, λόγω της πιθανότητας εξαπάτησης και παραβίασης δεδομένων (Yousafzai, Pallister & Foxall, 2009· Liao & Cheung, 2002).

Εμβαθύνοντας στον τομέα της εμπιστοσύνης, αναφέρεται ότι η Αντιληπτή Ικανότητα και η Ακεραιότητα έχουν ανώτερες τιμές στο μέσο όρο από το μέσο της 7βαθμης κλίμακας. Αυτό υποδηλώνει ενδεχομένως ότι οι φοιτητές αναγνωρίζουν την τεχνική επάρκεια των τραπεζικών συστημάτων και θεωρούν ότι οι τράπεζες λειτουργούν με έναν βαθμό εντιμότητας.Η εμπιστοσύνη κινείται οριακά κάτω από το μέσο της

κλίμακας. Το γεγονός αυτό αναδεικνύει επιφυλακτική στάση και δισταγμό από την πλευρά των χρηστών, οι οποίοι δεν είναι απόλυτα βέβαιοι για την αξιοπιστία των ηλεκτρονικών υπηρεσιών.

Εν συνεχεία, στην παρούσα έρευνα, ηΑντιληπτή Καλοσύνη κυμάνθηκε κατά μέσο όρο κάτω από το μέσο της κλίμακας. Τα δεδομένα αυτά, δείχνουν την μετριοπαθή αμφιβολίασχετικά με το πόσο οι τράπεζες δρουν με βάση το συμφέρον και την ευημερία του πελάτη. Το ίδιο ίσχυσε για την περίπτωση της Αντιληπτής Ιδιωτικότητας, εύρημα που συνάδει με το χαμηλό αίσθημα ασφάλειας. Τέλος, στην διάσταση του Αντιληπτού Κινδύνου πάλι παρατηρήθηκαν χαμηλές τιμές στον μέσο όρο, στοιχείο που δείχνει ότι οι χρήστες αντιλαμβάνονται την ύπαρξη κινδύνου σε μέτριο βαθμό αλλά με μια τάση προς την αρνητική πλευρά.

Συνοψίζοντας λοιπόν, προκύπτει μια ενδιαφέρουσα αντίφαση στις στάσεις των φοιτητών. Από τη μία πλευρά, αναγνωρίζουν την τεχνική επάρκεια και την ακεραιότητα των τραπεζικών, γεγονός που υποδηλώνει ότι θεωρούν τις πλατφόρμες λειτουργικές και τις τράπεζες θεσμικά έντιμες. Από την άλλη πλευρά, ωστόσο, αυτή η αναγνώριση δεν μεταφράζεται σε υψηλά επίπεδα συνολικής εμπιστοσύνης ή αισθήματος ασφάλειας. Γενικά φαίνεται πως το έλλειμμα εμπιστοσύνης πηγάζει κυρίως από τον φόβο παραβίασης της ιδιωτικότητας και όχι από αμφισβήτηση της ομαλής λειτουργίας των τραπεζικών συστημάτων.

Η μετριοπάθεια που παρατηρείται στην Αντιληπτή Καλοσύνη και στην Ιδιωτικότητα είναι ανάλογη με άλλες έρευνες, στις οποίες φαίνεται η δυσκολία των χρηστών να προσεγγίσουν ανθρωποκεντρικά, τα αυτοματοποιημένα ψηφιακά συστήματα. Επιπρόσθετα, η καλοσύνη, ως διάσταση εμπιστοσύνης, συσχετίζεται με συναισθηματικούς και διαπροσωπικούς παράγοντες, οι οποίοι, ωστόσο, δεν χαρακτηρίζουν σε μεγάλο βαθμό την ηλεκτρονική τραπεζική (Gefen, 2002). Παράλληλα, ένας από τους βασικότερους παράγοντες που θεωρείται ανασταλτικός για την χρήση ηλεκτρονικών τραπεζικών υπηρεσιών είναι η ανησυχία για την προστασία των προσωπικών δεδομένων (Pavlou, 2003).

Από τις συσχετίσεις της Ασφάλειας επιβεβαιώνεται η θέση της Ασφάλειας ως κεντρικού παράγοντα που συνδέεται άμεσα με τις αντιλήψεις κινδύνου, ιδιωτικότητας και εμπιστοσύνης. Επίσης βρέθηκε αλληλεξάρτηση μεταξύ της τεχνικής προστασίας (Ασφάλεια) και της προστασίας των προσωπικών δεδομένων (Ιδιωτικότητα), θέτοντας την ασφάλεια ως προϋπόθεση για την αίσθηση ιδιωτικότητας. Παράλληλα, φάνηκε ότι η αντίληψη για την Ασφάλεια ενισχύει την πεποίθηση ότι το σύστημα της τράπεζας είναι

τεχνικά επαρκές (αφορώντας την μεταβλητή της Ικανότητας) και δίκαιο/έντιμο (αφορώντας την μεταβλητή της Ακεραιότητας). Επίσης, η αύξηση της Ασφάλειας μπορεί να οδηγεί σε μεγαλύτερη συνειδητοποίηση των κινδύνων που διαχειρίζεται το σύστημα, καθιστώντας τον κίνδυνο πιο αντιληπτό, ή να αντικατοπτρίζει την αντίληψη ότι η ασφάλεια είναι απαραίτητη ακριβώς επειδή ο κίνδυνος είναι υψηλός.Τέλος, αν και η Ασφάλεια συμβάλλει στην αντίληψη ότι η τράπεζα ενδιαφέρεται για τον χρήστη, ο παράγοντας της Καλοσύνης επηρεάζεται σε μεγαλύτερο βαθμό από άλλες διαστάσεις ή συναισθηματικούς παράγοντες, πέρα από τα καθαρά τεχνικά μέτρα ασφάλειας.

Ο θεμελιώδης ρόλος της Ασφάλειας στις συσχετίσεις με την εμπιστοσύνη, την ιδιωτικότητα και τον αντιλαμβανόμενο κίνδυνο, αναδεικνύει τη σημασία της ασφάλειας, προκειμένου οι χρήστες να σχηματίσουν θετικές απόψεις για την ηλεκτρονική τραπεζική. Αυτό εξάλλου επιβεβαιώνεται και από άλλες έρευνες στις οποίες φαίνεται ότι η ασφάλεια συμβάλλει στην αύξηση της γνωστικής και συναισθηματικής εμπιστοσύνης (Kim et al., 2008).

Τα επίπεδα ασφάλειας σύμφωνα με τους συμμετέχοντες, είναι στατιστικά σημαντικά μεγαλύτερα για τα άτομα που πραγματοποιούν πολύ συχνά ηλεκτρονικές συναλλαγές στο e - bankingτης συνεργαζόμενης τράπεζας, σε σύγκριση με τα άτομα που πραγματοποιούν μέτρια ή και αρκετά συχνά αντίστοιχες ηλεκτρονικές συναλλαγές. Άρα η αίσθηση ασφάλειας είναι μεγαλύτερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά ηλεκτρονικές συναλλαγές.

Επίσης, τα επίπεδα εμπιστοσύνης είναι στατιστικά σημαντικά μεγαλύτερα για τα άτομα που πραγματοποιούν μέτρια συχνά, αρκετά συχνά ή πολύ συχνά ηλεκτρονικές συναλλαγές στο e-banking της συνεργαζόμενης τράπεζας, σε σύγκριση με τα άτομα που δεν πραγματοποιούν καθόλου συχνά αντίστοιχες ηλεκτρονικές συναλλαγές. Το ίδιο ισχύει και για τα άτομα που πραγματοποιούν πολύ συχνά ηλεκτρονικές συναλλαγές του e-banking, σε σύγκριση με τα άτομα που πραγματοποιούν αρκετά ή και μέτρια συχνά τέτοιες συναλλαγές. Επομένως, η αίσθηση εμπιστοσύνης γενικότερα είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά ηλεκτρονικές συναλλαγές.

Ακόμα, η αίσθηση ιδιωτικότητας είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές στο e-banking, σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά τέτοιες ηλεκτρονικές συναλλαγές. Η αίσθηση για την

ικανότητα της τράπεζας να παρέχει αποδοτικές και αξιόπιστες υπηρεσίες online τραπεζικής (Αντιληπτή ικανότητα) είναι ισχυρότερη στα άτομα που κάνουν συχνότερα ηλεκτρονικές συναλλαγές στο e-banking, σε σχέση με τα άτομα που πραγματοποιούν λιγότερο συχνά τέτοιες ηλεκτρονικές συναλλαγές.

Οι διαφοροποιήσεις που παρατηρούνται ως προς τη συχνότητα χρήσης επιβεβαιώνονται και από την έρευνα του Venkatesh και συνεργατών (2003), στην οποία φαίνεται ότι ηαυξημένη χρήση της τεχνολογίας οδηγεί σε μεγαλύτερη εμπιστοσύνη. Η συχνότερη αλληλεπίδραση με τα ηλεκτρονικά τραπεζικά συστήματα μειώνει τον αντιλαμβανόμενο κίνδυνο και ενισχύει όχι μόνο την αντίληψη ικανότητας, αλλά και την αίσθηση ιδιωτικότητας.

Στο σημείο αυτό θα πρέπει να γίνει αναφορά στους περιορισμούς της έρευνας. Αρχικά,ο βασικότερος περιορισμός αφορά την δειγματοληψία ευκολίας και έτσι το δείγμα δεν θεωρείται αντιπροσωπευτικό έτσι ώστε να γίνουν γενικεύσεις των συμπερασμάτων με ασφάλεια. Επίσης, το μέγεθος του δείγματος παραμένει σχετικά μικρό, αν και είναι ικανοποιητικό στα πλαίσια της παρούσας εργασίας. Ένας ακόμη περιορισμός αφορά το ερωτηματολόγιο που μέσω ερωτήσεων αυτοαναφοράς, εισάγει τον περιορισμό της υποκειμενικότητας ή της τάσης για κοινωνικά επιθυμητές απαντήσεις. Τέλος, το γεγονός πως ο τύπος της έρευνας ήταν συγχρονικόςοδηγεί στον περιορισμό πως δεν οδηγεί σε συμπεράσματα για τη διαχρονική εξέλιξη των μεταβλητών της έρευνας.

Για την αντιμετώπιση, λοιπόν, των παραπάνω περιορισμών, προτείνεται να χρησιμοποιηθεί μελλοντικά μια τυχαία δειγματοληψία και η σύσταση ενός αριθμητικά μεγαλύτερου δείγματος με σκοπό την επίτευξη αντιπροσωπευτικότητας. Επιπλέον, προτείνεται και η ποιοτική προσέγγιση σε μελλοντική έρευνα για να διερευνηθούν τα αίτια που οδήγησαν στα συμπεράσματα της παρούσας έρευνας. Τέλος, θα μπορούσαν να εισαχθούν μεταβλητές όπως η κυβερνοασφάλεια με σκοπό την επιρροή αυτής στην εμπιστοσύνη των πελατών τραπεζών.

Βιβλιογραφία

Alsayed, A., &Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, *7*(1), 109-115.

Bons, R. W., Alt, R., Lee, H. G., &Weber, B. (2012). Banking in the Internet and mobile era. *Electronic markets*, *22*(4), 197-202.

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking overview: concepts, challenges and solutions. *Wireless Personal Communications*, *117*(2), 1059-1078.

Choudhuri, S., Singh, A., Ravi, R., & Badhusha, M. H. N. (2024). An analysis of factors influencing consumer trust in online banking security measures. *Educational Administration: Theory And Practice*, *30*(2), 660-666.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Devadiga, N., Kothari, H., Jain, H., & Sankhe, S. (2017). E-banking security using cryptography, steganography and data mining. *International Journal of Computer Applications*, *164*(9), 26-30.

Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020, March). A security risk model for online banking system. In *2020 Systems of Signals Generating and Processing in the Field of on Board Communications* (pp. 1-4). IEEE.

Essinger, J., (1999).*The Virtual Banking Revolution. The Customer the Bank and the Future.* International Thomson Publishing Company. London.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

Eurostat, A. (2025). *Individuals using the internet for internet banking*. https://ec.europa.eu/eurostat/databrowser/view/tin00099/default/table?lang=en

Europe: online banking penetration by country 2021 (n.d.). Statista. E-source: https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *Database for Advances in Information Systems, 33*(3), 38–53.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

Gervey, B., & Lin, J. (2000). Obstacles on the Internet. *Advertising Age*, *71*(16), 12-17.

Gomes, L., Deshmukh, A., & Anute, N. (2022). Cyber security and internet banking: issues and preventive measures. *Journal of Information Technology and Sciences*, *8*(2), 31-42.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

Ibrahim, R. M. (2018, January). A review on online-banking security models, successes, and failures. In *Proceedings of the 2018 International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC), Tamil Nadu, India* (pp. 28-29).

Jalil, M. A., Talukder, M., & Rahman, M. K. (2014). Factors affecting Customer's perceptions towards online banking transactions in Malaysia. *Journal of Business and Management*, *20*(1), 25-44.

Kapliar, K. (2022). State regulation of internet banking in European countries. *Economics and Education*, *7*(3), 20-26.

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A. K. (2023). Online banking user authentication methods: a systematic literature review. *Ieee Access*, *12*, 741-757.

Khelifi, A., Aburrous, M., Talib, M. A., & Shastry, P. V. S. (2013, July). Enhancing protection techniques of e-banking security services using open source cryptographic algorithms. In *2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (pp. 89-95). IEEE.

Kiljan, S., Simoens, K., Cock, D. D., Eekelen, M. V., & Vranken, H. (2016). A survey of authentication and communications security in online banking. *ACM Computing Surveys (CSUR)*, *49*(4), 1-35.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001.

Kim, C., Tao, W., Shin, N., & Kim, K. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84-95

Kitsios, F., & Kamariotou, M. (2019). Digital transformation and strategy in the banking sector. *Proceedings of the 20th European Conference on Knowledge Management*. https://doi.org/10.3390/joitmc7030204.

Kumar, M., Sareen, M., & Barquissau, E. (2012). Relationship between types of trust and level of adoption of Internet banking. *Problems and Perspectives in Management*, *10*(1), 82-92.

Lee, J. H., Lim, W. G., & Lim, J. I. (2013). A study of the security of Internet banking and financial private information in South Korea. *Mathematical and Computer Modelling*, *58*(1-2), 117-131.

Leow, H. B. (1999). New distribution channels in banking Services. *Banker's Journal Malaysia*, 110, 48-56.

Liao, Z., & Cheung, M. T. (2002). Internet-based e-banking and consumer attitudes: An empirical study. *Information & Management*, *39*(4), 283–295.

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic commerce research and applications*, *2*(3), 216-228.

Mallouli, F., Khelifi, N., Hellal, A., Ferjani, E., Gmach, I., Chaabane, N., ... & Amami, R. (2021, December). Cryptocurrency bounced back based on cryptography technology during the COVID-19 pandemic. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 609-614). IEEE.

Mauro C. Hernandez, J., & Afonso Mazzon, J. (2007). Adoption of internet banking: proposition and implementation of an integrated methodology approach. *International journal of bank marketing*, *25*(2), 72-88.

Mia, M. A. H., Rahman, M. A., & Uddin, M. M. (2007). E-banking: evolution, status and prospect. *The Cost and Management*, *35*(1).

Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 1065-1072.

More, D. M. M., & Nalawade, M. P. J. D. K. (2015). Online banking and cyber-attacks: the current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*, *60*.

Muneeswari, G., & Puthussery, A. (2019, December). Multilevel security and dual OTP system for online transaction against attacks. In *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 221-225). IEEE.

Mylonakis, J., Orfanos, V., &Evripiotis, M. (2024). Internet Banking development and Greek Users' behaviour. *Journal of Banking and Finance*, *5*(I1), 20.

Nair, A. (1999). Indian Internet banking still nascent. *Asia Internetnews, May 12th, Available [online] http://www. asia. internet. com/asia-news/print/0,, 161_648221, 00. html*.

Nilsson, M., Adams, A., & Herd, S. (2005, April). Building security and trust in online banking. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems* (pp. 1701-1704).

Organization for Economic Co-operation and Development (OECD). (2001).*Electronic Finance: Economics and Institutional Factors*. Occasional Papers No. 2, Financial Affairs Division, OECD, Paris

Orni, K., Kaleva, S., Hirvasniemi, S., & Kortelainen, T. (2004). Usability of websites contributing to trust in e-commerce. In *Trust in Knowledge Management and Systems in Organizations* (pp. 125-146). IGI Global Scientific Publishing.

Open banking PSD2 regulation in the EU (2022, July 14). FinTech Legal Center. E-source: https://fintechlegal.center/open-banking-psd2-regulation-in-the-eu/

Paliwal, N. (2017). E-banking-influence, threats and security. *Journal of Advanced Computing and Communication Technologies*, *5*(3).

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 101–134.

Payment services (PSD 1) – Directive 2007/64/EC. (2007). European Commission website. Europa.Eu.E-source: https://ec.europa.eu/info/law/payment-services-psd-1-directive-2007-64-ec_en

Payment services (PSD 2) – Directive (EU) 2015/2366. (2015). European Commission website. Europa.Eu.E-source: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. *Internet Research, 14*(3), 224–235. https://doi.org/10.1108/10662240410542652.

Poudel, O., Acharya, P., & Simkhada, D. (2023). Customers' Trust in E-payment: The Influence of Security and Privacy. *BMC Journal of Scientific Research*, *6*(1), 97-112.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, *101*(4), 165–177. https://doi.org/10.1108/02635570110390071

Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. *Journal of Innovation Management*, *4*(4), 32-54.

Shmuratko, Y. A., &Sheludko, S. A. (2019). Financial Technologies'impactOnThe Development Of Banking. *Financial and credit activity problems of theory and practice*, *4*(31), 61-69.

Solanki, V. S. (2012). Risks in e-banking and their management. *International Journal of Marketing, Financial Services & Management Research, 1*(9), 164-178.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*(3), 135-161

Stratton, S. J. (2021). Population research: Convenience sampling strategies. *Prehospital and Disaster Medicine*, *36*(4), 373–374. https://doi.org/10.1017/S1049023X2100064X

Tassabehji, R., & Kamala, M. A. (2012). Evaluating biometrics for online banking: The case for usability. *International Journal of Information Management*, *32*(5), 489-494.

Ungratwar, S., Sharma, D., &Kumar, S. (2025). Mapping the digital banking landscape: a multi-dimensional exploration of fintech, digital payments, and e-wallets, with insights into current scenarios and future research. *Humanities and Social Sciences Communications*, *12*(1), 1-22.

United Nations Conference on Trade and Development (UNCTAD). (2002). E-*Commerce and Development Report 2002* (NewYork & Geneva: United Nations).

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Vrîncianu, M., & Popa, L. A. (2010). Considerations regarding the security and protection of e-banking services consumers' interests. *The Amfiteatru Economic Journal*, *12*(28), 388-403.

Wong, D. H., Loh, C., Yap, K. B., & Bak, R. (2009). To trust or not to trust: The consumers dilemma with e-banking. *Journal of Internet Business*, (6), 1-27.

Yadav, V. (2022). E-Banking: Risks and Their Management. *Issue 4 Indian JL & Legal Rsch.*, *4*, 1.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2009). Multi-dimensional role of trust in e-banking. *The Service Industries Journal*, *29*(5), 591–605. https://doi.org/10.1080/02642060902720163

Zherdetskaya, L.V. & Gorodinsky, D.I. (2017). Development ofbanking technologies: threats and opportunities for banks, *Economy and society, 10*, 583– 588.

Zhou, T. (2011). The effect of initial trust on user adoption of mobile payment. *Information Development*, *27*(4), 290-300

Παράρτημα

Ερωτηματολόγιο

Έντυπο ενημέρωσης

Αγαπητοί φοιτητές/φοιτήτριες,

Στο πλαίσιο των μεταπτυχιακών μου σπουδών κάνω μια έρευνα με τίτλο «Αίσθημα ασφάλειας και εμπιστοσύνη των πελατών τραπεζών στις ηλεκτρονικές συναλλαγές: Ανάλυση των δημογραφικών παραγόντων». Σκοπός της εν λόγω επιστημονικής έρευνας είναι η διερεύνηση του αισθήματος ασφάλειας και της εμπιστοσύνης που διαθέτουν οι πελάτες τραπεζών όταν πραγματοποιούν ηλεκτρονικές συναλλαγές, καθώς και η εξέταση της επίδρασης των δημογραφικών χαρακτηριστικών στις δύο αυτές μεταβλητές.

Προκειμένου να φτάσουμε σε συμπεράσματα, διαμορφώσαμε ένα σύντομο ερωτηματολόγιο και σας παρακαλούμε να απαντήσετε σε αυτό με ειλικρίνεια. Η άποψή σας είναι πολύ σημαντική για το θέμα καθώς αφενός χωρίς αυτήν δεν μπορεί να γίνει έρευνα και αφετέρου θα συνεισφέρει στην ανακάλυψη σημαντικών ευρημάτων. Η ανωνυμία του ερωτηματολογίου είναι δεδομένη και θα χρειαστείτε 7’ περίπου για να απαντήσετε σε όλες τις ερωτήσεις.

Σας ευχαριστούμε εκ των προτέτων

Ερωτηματολόγιο

Δημογραφικά στοιχεία

Στις ερωτήσεις που ακολουθούν, σημειώστε μόνο μία απάντηση.

Φύλο

Άνδρας	
Γυναίκα	
Άλλο	

Ηλικία

Έως 20	
21-25	
26-30	
31-35	
35+	

Επαγγελματική ιδιότητα	
Άνεργος/η	
Φοιτητής/τρια	
Ιδιωτικός υπάλληλος	
Δημόσιος υπάλληλος	
Ελεύθερος επαγγελματίας	
Άλλο	

Πόσο συχνά πραγματοποιείτε ηλεκτρονικές συναλλαγές (πληρωμές, μεταφορές κτλ) στο e-banking της/των Τράπεζας/Τραπεζών με την/τις οποία/ες συνεργάζεστε;	
Καθόλου	
Λίγο	
Μέτρια	
Αρκετά	
Πολύ	

Κλίμακα αντιληπτής ασφάλειας - Salisbury et al. (2001)

Στις ερωτήσεις που ακολουθούν καλείστε να σημειώσετε μόνο μια απάντηση σύμφωνα με την κλίμακα που ακολουθεί:

1	2	3	4	5	6	7
Διαφωνώ απόλυτα	Διαφωνώ αρκετά	Διαφωνώ λίγο	Ουδέτερος/η	Συμφωνώ λίγο	Συμφωνώ αρκετά	Συμφωνώ απόλυτα

Θα ένιωθα ασφαλής να στείλω ευαίσθητες πληροφορίες μέσω ηλεκτρονικών τραπεζικών συναλλαγών							
Οι ηλεκτρονικές υπηρεσίες των τραπεζών για συναλλαγές είναι ένα ασφαλές μέσο για την αποστολή πληροφοριών							
Θα ένιωθα απόλυτα ασφαλής να παρέχω ευαίσθητες πληροφορίες για τον εαυτό μου μέσω ηλεκτρονικών τραπεζικών συναλλαγών							
Τα περιβάλλοντα που εκτελούνται οι ηλεκτρονικές τραπεζικές συναλλαγές είναι ασφαλή για την αποθήκευση ευαίσθητων πληροφοριών							
Συνολικά, οι ηλεκτρονικές τραπεζικές συναλλαγές είναι ένα ασφαλές μέσο για τη μετάδοση ευαίσθητων πληροφοριών							

Κλίμακα εμπιστοσύνης ηλεκτρονικής τραπεζικής - Yousafzai et al. (2009)

Στις ερωτήσεις που ακολουθούν καλείστε να σημειώσετε μόνο μια απάντηση σύμφωνα με την κλίμακα που ακολουθεί:

1	2	3	4	5	6	7
Διαφωνώ απόλυτα	Διαφωνώ αρκετά	Διαφωνώ λίγο	Ουδέτερος/η	Συμφωνώ λίγο	Συμφωνώ αρκετά	Συμφωνώ απόλυτα

Αντιληπτός κίνδυνος							
Κατά την εκτέλεση συναλλαγών μέσω διαδικτυακής τραπεζικής, θα χαρακτήριζα απίθανο να συμβεί μια οικονομική απώλεια							
Κατά την εκτέλεση συναλλαγών μέσω διαδικτυακής τραπεζικής, θα χαρακτήριζα απίθανο να συμβεί απώλεια προσωπικών πληροφοριών							
Η απόφασή μου να εκτελέσω τραπεζικές συναλλαγές μέσω Διαδικτύου δεν παρουσιάζει σημαντικούς κινδύνους							
Εμπιστοσύνη							
Εμπιστεύομαι τις τραπεζικές συναλλαγές μέσω Διαδικτύου							
Εμπιστεύομαι την τράπεζά μου							
Εμπιστεύομαι το Διαδίκτυο για τραπεζικές συναλλαγές							
Αντιληπτή ιδιωτικότητα							
Κατά τη χρήση των διαδικτυακών τραπεζικών υπηρεσιών, πιστεύω ότι γνωρίζω ακριβώς ποιες πληροφορίες συλλέγονται							
Πιστεύω ότι οι πληροφορίες των διαδικτυακών τραπεζικών συναλλαγών μου θα χρησιμοποιηθούν μόνο για τον σκοπό της εκάστοτε συναλλαγής							
Πιστεύω ότι οι πληροφορίες των διαδικτυακών τραπεζικών συναλλαγών μου θα κοινοποιηθούν σε τρίτους μόνο με τη συγκατάθεσή μου							
Κατά τη χρήση των διαδικτυακών τραπεζικών υπηρεσιών, πιστεύω ότι έχω πλήρη γνώση για τα άτομα που έχουν πρόσβαση στις πληροφορίες του διαδικτυακού λογαριασμού μου							
Κατά τη χρήση των διαδικτυακών τραπεζικών υπηρεσιών,							

πιστεύω ότι ελέγχω τη χρήση των πληροφοριών μου							
Αντιληπτή ικανότητα							
Πιστεύω ότι η τράπεζά μου παρέχει εξαιρετικές υπηρεσίες διαδικτυακής τραπεζικής							
Πιστεύω ότι η τράπεζά μου επεξεργάζεται τις συναλλαγές μου με ακρίβεια και εγκαίρως							
Πιστεύω ότι η τράπεζά μου παρέχει 24ωρη πρόσβαση στη διαδικτυακή τραπεζική							
Αντιληπτή ακεραιότητα							
Πιστεύω ότι η τράπεζά μου είναι δίκαιη με τους πελάτες της που χρησιμοποιούν τις υπηρεσίες διαδικτυακής τραπεζικής							
Πιστεύω ότι η τράπεζά μου έχει συνεπείς διαδικτυακές πρακτικές και πολιτικές							
Αντιληπτή καλοσύνη							
Πιστεύω ότι η τράπεζά μου θα μου επιστρέψει χρήματα αν αυτά αφαιρεθούν από τον λογαριασμό μου μέσω μη εξουσιοδοτημένων συναλλαγών							
Πιστεύω ότι η τράπεζά μου ενεργεί προς το συμφέρον μου							

Ευχαριστώ για τον χρόνο σας!