ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΠΜΣ ΤΡΑΠΕΖΙΚΗ, ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΤΕΧΝΟΛΟΓΙΑ (FINTECH)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ :

«Ηλεκτρονική Τραπεζική: Mobile Banking στην Ελλάδα»
(«E-Banking : Mobile Banking in Greece»)

ΖΑΧΟΣ ΔΗΜΗΤΡΙΟΣ-ΠΑΝΑΓΙΩΤΗΣ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΡΙΑ: **ΜΠΑΛΩΜΕΝΟΥ ΧΡΥΣΑΝΘΗ**

Πίνακας Περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος Συντομογραφιών και Ακρωνύμων

2FA= 2 Factor Authentication

API =Application Programming Interface

AI = Artificial Intelligence

CA = Certificate Authority, CA

DTMF = Dual Tone Multi – Frequency

ΔΙ.Δ.Η.Ε. = Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

HTTPS = Hyper Text Transfer Protocol Secure)

IoT = Internet of Things

IVR = Interactive Voice Response

SMS = Short Messaging Service

SMAC = Standalone Mobile Application Clients

WAP = Wireless Application Protocol

WWW = World Wide Web

Περίληψη

Η παρούσα εργασία εξετάζει την ανάπτυξη και τη χρήση του Mobile Banking στην Ελλάδα, με έμφαση στις τεχνολογικές εξελίξεις, την ασφάλεια και τη συμπεριφορά των χρηστών. Αρχικά, γίνεται αναφορά στην εξέλιξη του τραπεζικού συστήματος υπό το πρίσμα της τεχνολογίας, καθώς και στα κίνητρα και τη σημασία της έρευνας.

Στο θεωρητικό μέρος, αναλύεται η λειτουργία του Mobile Banking, οι υπηρεσίες που παρέχει, καθώς και τα πλεονεκτήματα και μειονεκτήματά του τόσο για τους καταναλωτές όσο και για τις τράπεζες. Παρουσιάζονται οι βασικές τεχνολογίες που το υποστηρίζουν, καθώς και οι μηχανισμοί ασφάλειας που διασφαλίζουν τις συναλλαγές. Επιπλέον, γίνεται καταγραφή των παρεχόμενων υπηρεσιών Mobile Banking από τις τέσσερις συστημικές ελληνικές τράπεζες, με σύγκριση των χαρακτηριστικών και των επιπέδων ασφαλείας τους.

Το εμπειρικό μέρος περιλαμβάνει πρωτογενή έρευνα που πραγματοποιήθηκε μέσω ερωτηματολογίου, με στόχο τη διερεύνηση της χρήσης του Mobile Banking στην Ελλάδα. Η έρευνα παρέχει πολύτιμα δεδομένα σχετικά με τη διείσδυση του Mobile Banking, τη συχνότητα χρήσης του, τις προτιμήσεις και τις ανησυχίες των καταναλωτών, καθώς και τις βελτιώσεις που ζητούν από τις τραπεζικές εφαρμογές.

Τα συμπεράσματα της εργασίας αναδεικνύουν τον αυξανόμενο ρόλο του Mobile Banking στο σύγχρονο τραπεζικό σύστημα και τη σημασία της συνεχούς αναβάθμισης των τραπεζικών υπηρεσιών, τόσο σε επίπεδο λειτουργικότητας όσο και σε θέματα ασφάλειας.

Summary

This paper examines the development and use of Mobile Banking in Greece, focusing on technological advancements, security, and user behavior. Initially, it discusses the evolution of the banking system through the lens of technology, as well as the motivations and significance of the research.

The theoretical section analyzes the operation of Mobile Banking, the services it offers, and its advantages and disadvantages for both consumers and banks. It presents the key technologies supporting Mobile Banking and the security mechanisms ensuring transaction safety. Additionally, it outlines the services provided by the four systemic Greek banks, comparing their features and security levels.

The empirical section includes primary research conducted through a questionnaire aimed at exploring Mobile Banking usage in Greece. The research provides valuable data on its penetration, frequency of use, consumer preferences and concerns, as well as the improvements users seek in banking applications.

The study's conclusions highlight the growing role of Mobile Banking in the modern banking system and the importance of continuously upgrading banking services in terms of both functionality and security.

Ευχαριστίες

Θα ήθελα να εκφράσω την ειλικρινή μου ευγνωμοσύνη στην επιβλέπουσα καθηγήτριά μου, Μπαλωμένου Χρυσάνθη για την πολύτιμη καθοδήγηση, την αμέριστη υποστήριξη και τις εποικοδομητικές παρατηρήσεις της καθ' όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας. Η συμβολή της υπήρξε καθοριστική στη διαμόρφωση του τελικού αποτελέσματος.

Επιπλέον, θα ήθελα να ευχαριστήσω θερμά όλους όσοι συμμετείχαν στην έρευνα και αφιέρωσαν τον χρόνο τους για να συμπληρώσουν το ερωτηματολόγιο. Η συμβολή τους ήταν πολύτιμη για τη συλλογή δεδομένων και την εξαγωγή ουσιαστικών συμπερασμάτων.

Τέλος, εκφράζω τις ευχαριστίες μου σε όσους με στήριξαν με οποιονδήποτε τρόπο κατά τη διάρκεια αυτής της προσπάθειας.

Κεφάλαιο 1ο

«Εισαγωγή»

1.1 Τεχνολογία και Τράπεζες

Η τεχνολογία έχει διαδραματίσει καθοριστικό ρόλο στη διαμόρφωση της σημερινής εικόνας του τραπεζικού τομέα, επηρεάζοντας σε πολύ μεγάλο βαθμό τόσο τον τρόπο λειτουργίας των τραπεζών όσο και την εμπειρία των πελατών τους. Από τις πρώτες ηλεκτρονικές συναλλαγές έως τις σημερινές εφαρμογές Mobile banking, οι τραπεζικές υπηρεσίες έχουν εξελιχθεί ραγδαία, αξιοποιώντας τις δυνατότητες της πληροφορικής και των επικοινωνιών (Molina-Castillo et al., 2020).

Η χρήση της τεχνολογίας στις Τράπεζες άρχισε με την εισαγωγή των αυτόματων ταμειακών μηχανών (ATM) και των ηλεκτρονικών συστημάτων πληρωμών επιτρέποντας στους πελάτες να πραγματοποιούν συναλλαγές χωρίς να απαιτείται η φυσική τους παρουσία στο υποκατάστημα .Η επόμενη μεγάλη αναβάθμιση έγινε με το Internet Banking, το οποίο έδωσε τη δυνατότητα στους χρήστες να διαχειρίζονται τους λογαριασμούς τους και να εκτελούν πληρωμές μέσω διαδικτύου (Zhao et al., 2019).

Σήμερα, η τεχνολογία έχει αναπτύξει το Mobile Banking αρκετά ώστε να επιτρέπει στους πελάτες να πραγματοποιούν τραπεζικές συναλλαγές μέσω των smartphone και των tablet τους (Shaikh & Karjaluoto, 2015). Η υιοθέτηση τεχνολογιών όπως η τεχνητή νοημοσύνη (AI), το blockchain και τα βιομετρικά στοιχεία ασφάλειας έχουν ενισχύσει την ασφάλεια, την ταχύτητα και την αξιοπιστία των ηλεκτρονικών τραπεζικών υπηρεσιών (Chong et al., 2021). Σε δεύτερο χρόνο έχουμε και την ανάπτυξη των Fintech εταιρειών, οι οποίες έχουν δημιουργήσει έναν νέο ανταγωνιστικό τοπίο, προσφέροντας καινοτόμες λύσεις που αλλάζουν τη δυναμική της αγοράς (Gomber et al., 2017).

Η σύγχρονη τραπεζική είναι πλέον «ένα» με την εξέλιξη της τεχνολογίας, προσφέροντας υπηρεσίες που καθιστούν τις συναλλαγές πιο προσβάσιμες, ασφαλείς

και εξατομικευμένες. Η ανάπτυξη του Mobile Banking στην Ελλάδα αποτελεί χαρακτηριστικό παράδειγμα.

1.2 Ιστορική Αναδρομή

Η ηλεκτρονική τραπεζική γνώρισε σημαντική εξέλιξη τις τελευταίες δεκαετίες, επηρεάζοντας τον τρόπο με τον οποίο πραγματοποιούνται οι τραπεζικές συναλλαγές. Η μετάβαση από τις παραδοσιακές τραπεζικές συναλλαγές στις σύγχρονες ψηφιακές υπηρεσίες πραγματοποιήθηκε σταδιακά, ακολουθώντας την ανάπτυξη των τεχνολογιών της πληροφορικής και των επικοινωνιών.

Το ξεκίνημα έγινε τη δεκαετία του 1960, με την ανάπτυξη των πρώτων Αυτόματων Ταμειολογιστικών Μηχανών (ATMs), που αποτέλεσαν μια από τις πρώτες μορφές αυτοματοποίησης στις τραπεζικές υπηρεσίες (Batiz-Lazo & Reid, 2011).

Τη δεκαετία του 1980 εμφανίστηκαν οι πρώτες ηλεκτρονικές μεταφορές χρημάτων και οι πρώτες προσπάθειες υλοποίησης τηλεφωνικής τραπεζικής. Ωστόσο, η ουσιαστική «επανάσταση» ήρθε τη δεκαετία του 1990 με την εξάπλωση του Διαδικτύου και την υιοθέτηση του Internet Banking, που επέτρεψε στους πελάτες να διαχειρίζονται τους λογαριασμούς τους από τον προσωπικό τους υπολογιστή.

Το Mobile Banking έκανε την εμφάνισή του στις αρχές της δεκαετίας του 2000, αρχικά μέσω SMS και αργότερα μέσω ειδικών εφαρμογών για smartphones (Laukkanen, 2007). Σήμερα, η συνεχής πρόοδος στις τεχνολογίες ασφάλειας, τα βιομετρικά δεδομένα και οι τεχνολογίες τεχνητής νοημοσύνης συμβάλλουν στη βελτίωση της αξιοπιστίας και της αποδοτικότητας του Mobile Banking, καθιστώντας το αναπόσπαστο κομμάτι της σύγχρονης τραπεζικής εμπειρίας (Venkatesh et al., 2012).

1.3 Κίνητρα και Στόχοι της Εργασίας

Η ταχύτατη υιοθέτηση των ψηφιακών υπηρεσιών από τις τράπεζες έχουν μεταμορφώσει το τραπεζικό σύστημα, καθιστώντας το Mobile Banking βασικό στοιχείο της καθημερινότητας των πολιτών. Οι προσωπικές και επαγγελματικές συναλλαγές πραγματοποιούνται πλέον με ταχύτητα, ευκολία και αυξημένη ασφάλεια μέσω κινητών συσκευών.

Ένα από τα βασικά κίνητρα για την εκπόνηση της παρούσας εργασίας είναι η ανάγκη κατανόησης του τρόπου με τον οποίο το Ελληνικό κοινό αλληλοεπιδρά με τις εφαρμογές Mobile Banking. Παρά τις προόδους στον τομέα, παραμένουν ερωτήματα σχετικά με την ασφάλεια, την εμπιστοσύνη των χρηστών και το μέλλον αυτής της τεχνολογίας στην Ελλάδα. Η ύπαρξη ερευνών που εξετάζουν τη διείσδυση και αποδοχή του Mobile Banking σε άλλες χώρες (Shaikh & Karjaluoto, 2015 & Laukkanen, 2007) καθιστά αναγκαία την εξέταση του θέματος σε ελληνικό πλαίσιο.

Οι κύριοι στόχοι της εργασίας είναι οι εξής:

1. **Διερεύνηση του βαθμού χρήσης των εφαρμογών Mobile Banking στην Ελλάδα** – Μέσω της ανάλυσης δεδομένων από το ερωτηματολόγιο, θα εξεταστεί πόσοι χρήστες επιλέγουν τις υπηρεσίες Mobile Banking και ποιές είναι αυτές.
2. **Αξιολόγηση της αίσθησης ασφάλειας των χρηστών** – Δεδομένου ότι η ασφάλεια αποτελεί καθοριστικό παράγοντα για την υιοθέτηση ψηφιακών τραπεζικών υπηρεσιών (Zhao et al., 2019), στόχος είναι να αναλυθεί εάν οι χρήστες αισθάνονται ασφαλείς χρησιμοποιώντας αυτές τις εφαρμογές.
3. **Κατανόηση των προβλέψεων των χρηστών για το μέλλον του Mobile Banking στην Ελλάδα** – Η έρευνα επιδιώκει να καταγράψει πώς οι πολίτες βλέπουν την εξέλιξη των τραπεζικών συναλλαγών μέσω κινητών συσκευών και εάν πιστεύουν ότι η τεχνολογία θα εξελιχθεί περαιτέρω στο μέλλον "εκτοπίζοντας" τα φυσικά υποκαταστήματα των Τραπεζών.
4. **Σύγκριση με διεθνείς τάσεις και βέλτιστες πρακτικές** – Η εργασία θα επιχειρήσει να συγκρίνει τα ευρήματα της έρευνας με αντίστοιχες μελέτες που έχουν διεξαχθεί σε άλλες χώρες, προκειμένου να εντοπιστούν διαφορές, ομοιότητες και πιθανές προκλήσεις.

Μέσω της παρούσας μελέτης, επιδιώκεται η δημιουργία ενός ολοκληρωμένου πλαισίου κατανόησης της χρήσης του Mobile Banking, συμβάλλοντας έτσι τόσο στην ακαδημαϊκή κοινότητα όσο και στις ίδιες τις τράπεζες που επιθυμούν να βελτιώσουν τις παρεχόμενες υπηρεσίες τους.

1.4 Ευρήματα Έρευνας

Η παρούσα έρευνα ανέδειξε σημαντικά δεδομένα σχετικά με τη χρήση του Mobile Banking στην Ελλάδα. Από το σύνολο των 118 ερωτηθέντων, προέκυψαν τα εξής:

- Φύλο & Ηλικία: Η πλειοψηφία των χρηστών Mobile Banking είναι άνδρες (54,2%), με κυρίαρχες ηλικιακές ομάδες 28-39 ετών (39,8%) και 18-27 ετών (30,5%).
- Μορφωτικό επίπεδο: Το 55,1% των ερωτηθέντων είναι πτυχιούχοι ΑΕΙ/ΤΕΙ, ενώ ένα σημαντικό ποσοστό (19,5%) διαθέτει μεταπτυχιακό ή διδακτορικό.
- Επαγγελματική κατάσταση & Εισόδημα: Οι περισσότεροι χρήστες είναι ιδιωτικοί υπάλληλοι (31,4%), ενώ το 30,5% έχει εισόδημα 700€ - 1.000€, με το 25,4% να κυμαίνεται στα 1.001€ - 2.000€.
- Υιοθέτηση Mobile Banking: Το 84,7% των ερωτηθέντων δήλωσε ότι χρησιμοποιεί Mobile Banking, αποδεικνύοντας τη μεγάλη διείσδυσή του στην ελληνική αγορά.
- Συχνότητα χρήσης: Το 65,2% συμφωνεί ή συμφωνεί απόλυτα ότι χρησιμοποιεί Mobile Banking συχνά.
- Κύριες χρήσεις: Οι πιο συχνές λειτουργίες είναι ο έλεγχος υπολοίπου (80,5%), οι μεταφορές χρημάτων (69,5%) και η πληρωμή λογαριασμών (60,2%).
- Ευχρηστία & Ασφάλεια: Το 79,6% των χρηστών θεωρεί τις εφαρμογές Mobile Banking εύχρηστες, ενώ το 60,1% δηλώνει ότι νιώθει πάντα ή συχνά ασφαλές στις συναλλαγές του.
- Προτιμώμενες τράπεζες: Οι πιο δημοφιλείς εφαρμογές Mobile Banking ανήκουν στην Τράπεζα Πειραιώς (31,4%) και την Εθνική Τράπεζα (28,8%).
- Βελτιώσεις: Το 51,7% θεωρεί ότι απαιτείται αυξημένη ασφάλεια, ενώ το 41,5% επιθυμεί καλύτερη ταχύτητα.

- Μέλλον Mobile Banking: Το 55,1% πιστεύει ότι το Mobile Banking θα αντικαταστήσει πλήρως τα τραπεζικά καταστήματα στο μέλλον, ενώ ένα 24,6% διαφωνεί.

Τα παραπάνω στοιχεία παρέχουν μια σαφή εικόνα για την αποδοχή, τη χρήση και τις προοπτικές του Mobile Banking στην Ελλάδα, δημιουργώντας τη βάση για περαιτέρω ανάλυση.

Μέρος 1ο Θεωρητική Ανάλυση

Βιβλιογραφική Ανασκόπηση

1. Εισαγωγή

Η ανάπτυξη των ψηφιακών τεχνολογιών έχει επηρεάσει σημαντικά τον τραπεζικό κλάδο, με το Mobile Banking να αποτελεί πλέον βασικό στοιχείο των τραπεζικών συναλλαγών. Η ηλεκτρονική τραπεζική εξελίχθηκε μέσα από διάφορες τεχνολογικές φάσεις, από το Internet Banking μέχρι τις σύγχρονες εφαρμογές κινητής τραπεζικής, προσφέροντας αυξημένη ευκολία και ασφάλεια (Shaikh & Karjaluoto, 2015).

2. Mobile Banking: Ορισμός και Βασικά Στοιχεία

Το Mobile Banking αναφέρεται στη χρήση κινητών συσκευών για τη διεκπεραίωση τραπεζικών συναλλαγών. Οι χρήστες έχουν τη δυνατότητα να διαχειρίζονται τους λογαριασμούς τους, να πραγματοποιούν πληρωμές και να εκτελούν μεταφορές χρημάτων μέσω ειδικών εφαρμογών τραπεζών ή προσαρμοσμένων ιστότοπων (Laukkanen, 2007). Οι βασικοί φορείς περιλαμβάνουν τις εμπορικές τράπεζες, τις εταιρείες τεχνολογίας και τις ρυθμιστικές αρχές που διαμορφώνουν το πλαίσιο ασφάλειας και συμμόρφωσης (Zhao et al., 2019).

3. Παρεχόμενες Υπηρεσίες και Χαρακτηριστικά

Οι βασικές υπηρεσίες που προσφέρονται μέσω Mobile Banking περιλαμβάνουν διαχείριση λογαριασμών, πληρωμές λογαριασμών, μεταφορές χρημάτων και επενδυτικές συναλλαγές (Venkatesh et al., 2012). Το Mobile Banking χαρακτηρίζεται

από ευχρηστία, άμεση πρόσβαση και εξελιγμένα πρωτόκολλα ασφαλείας (Laukkanen, 2007).

4. Οφέλη και Μειονεκτήματα του Mobile Banking

Τα κυριότερα οφέλη του Mobile Banking περιλαμβάνουν την εξοικονόμηση χρόνου, τη μείωση κόστους για τις τράπεζες και τους πελάτες, καθώς και τη βελτιωμένη χρηστικότητα. Ωστόσο, εξακολουθούν να υπάρχουν προκλήσεις όπως θέματα ασφαλείας και περιορισμένη αποδοχή από ορισμένες ομάδες χρηστών (Shaikh & Karjaluoto, 2015).

5. Τεχνολογίες Mobile Banking

Οι τεχνολογίες που χρησιμοποιούνται στο Mobile Banking περιλαμβάνουν:

- *SMS Banking*: Επιτρέπει την αποστολή και λήψη τραπεζικών πληροφοριών μέσω μηνυμάτων SMS.
- *WAP Banking*: Χρησιμοποιεί τεχνολογίες κινητού διαδικτύου για πρόσβαση σε τραπεζικές υπηρεσίες (Cordelia,2020).
- *IVR Banking*: Διαδραστικά φωνητικά συστήματα για τη διεκπεραίωση τραπεζικών συναλλαγών.
- *M-Banking με SMAC*: Ενσωματώνει καινοτόμες τεχνολογίες για βελτιωμένη εμπειρία χρήστη (Zhao et al., 2019).

6. Ζητήματα Ασφάλειας

Η ασφάλεια αποτελεί κρίσιμο ζήτημα στο Mobile Banking, με τεχνολογίες όπως:

- *Κρυπτογράφηση*: Συμμετρική και ασύμμετρη κρυπτογράφηση για την προστασία δεδομένων.
- *Ψηφιακά Πιστοποιητικά και Υπογραφές*: Ενισχύουν την αξιοπιστία των συναλλαγών.
- *Πρωτόκολλα SSL/TLS και SET*: Παρέχουν ασφάλεια στις διαδικτυακές συναλλαγές

7. Απειλές και Κίνδυνοι

Οι βασικές απειλές περιλαμβάνουν:

- *Sniffers* και *Key Loggers*: Παρακολουθούν και καταγράφουν δραστηριότητα των χρηστών.
- *Phishing* και *Pharming*: Απόπειρες εξαπάτησης χρηστών για απόκτηση προσωπικών δεδομένων. (Μαυρογιάννης, 2003).
- *Malware:* Κακόβουλο λογισμικό που στοχεύει τραπεζικές εφαρμογές (Shaikh & Karjaluoto, 2015).

8. Mobile Banking στην Ελλάδα

Η χρήση του Mobile Banking στην Ελλάδα αυξάνεται σταθερά, με τις μεγάλες ελληνικές τράπεζες (Εθνική Τράπεζα, Τράπεζα Πειραιώς, Eurobank, Alpha Bank) να επενδύουν σε καινοτόμες εφαρμογές για βελτιωμένη εμπειρία χρήστη.

Παρόλαυτα, έρευνες τις Eurostat δείχνουν ότι η Ελλάδα ακόμα υστερεί στο να έχει κάποιος πρόσβαση στο Internet στο 100% της γεωγραφικής της έκτασης κάτι που προσθέτει μια αιτία που ακόμα κρατάει πίσω – έστω ελάχιστα – την πλήρη ανάπτυξη του M-Banking στη χώρα μας.

Κεφάλαιο 2ο

«Mobile Banking»

Σε αυτό το κεφάλαιο ο αναγνώστης θα ενημερωθεί για το τί είναι το Mobile Banking. Ακολουθεί μια περιγραφή των βασικών φορέων που το αποτελούν καθώς και μία ανάλυση των χαρακτηριστικών του. Το κεφάλαιο κλείνει με μία αναφορά στα οφέλη και τα μειονεκτήματα για τον καταναλωτή αλλά και την ίδια την Τράπεζα.

2.1 Mobile Banking Ορισμός και Βασικοί Φορείς

Πρώτη μας κίνηση είναι να ορίσουμε το «M-Banking» , μια σύντμηση του όρου Mobile Banking. Η κινητή τραπεζική (m-banking) είναι ένας σύγχρονος τρόπος διεκπεραίωσης τραπεζικών συναλλαγών μέσω κινητών συσκευών, προσφερόμενος από τα τραπεζικά ιδρύματα. Οι υπηρεσίες αυτές λειτουργούν είτε μέσω SMS, είτε μέσω διαδικτυακών εφαρμογών για κινητά (Mobile Web), είτε μέσω ειδικών εφαρμογών που εγκαθίστανται στο κινητό τηλέφωνο (Angelakopoulos & Mihiotis,2011). Πρόκειται για μια τεχνολογία που εντάσσεται στη γενικότερη κατηγορία της Ηλεκτρονικής τραπεζικής (e-banking), αλλά διαφοροποιείται λόγω της ευκολίας χρήσης, της φορητότητας και της δυνατότητας εκτέλεσης συναλλαγών σε πραγματικό χρόνο από οπουδήποτε υπάρχει σύνδεση στο διαδίκτυο. Το M-Banking δεν είναι μόνο οι εξ΄ αποστάσεως πληρωμές · είναι ένας ευρύτερος όρος που καλύπτει όλες τις χρηματοοικονομικές υπηρεσίες και συναλλαγές σε μία Τράπεζα με την προϋπόθεση ο πελάτης να έχει μια κινητή συσκευή στην οποία έχει “κατεβάσει” την αντίστοιχη εφαρμογή (app) και ολοκληρώνοντας την διαδικασία εγγραφής-αυθεντικοποίησης σε αυτή από την εκάστοτε Τράπεζα, να του επιτραπεί η πρόσβαση στο M-Banking.

Εδώ και χρόνια το κινητό τηλέφωνο έχει διεισδύσει στην καθημερινότητά μας και οι τεχνολογίες που το αποτελούν δεν σταματούν να εξελίσσονται, αυξάνοντας κατά αυτόν τον τρόπο και την ανάγκη για την χρήση του από τον μέσο καταναλωτή. Οι υψηλές ταχύτητες σύνδεσης στο Internet, η ευκολία στην χρήση του και η συνεχώς αναπτυσσόμενη κάλυψη των δικτύων μετατρέπει το κινητό σε ένα πολύ σημαντικό εργαλείο για όλους τους χρήστες. (Smutkupt, Krairit & Esichaikul, 2010)

Το M-Banking βασίζεται στην συνεργασία και ομαλή συνύπαρξη σε ένα σύνθετο οικοσύστημα διαφόρων φορέων. Οι παρακάτω φορείς «προετοιμάζουν το έδαφος» και διατηρούν την τάξη για την σωστή λειτουργία για την παροχή κινητών χρηματοοικονομικών υπηρεσιών.

Οι ***κύριοι φορείς*** περιλαμβάνουν:

1. ***Τράπεζες*** : Ο βασικός φορέας που προσφέρει τις υπηρεσίες Mobile Banking.
2. ***Πάροχοι Τεχνολογίας*** : Αυτές οι εταιρείες παρέχουν τις τεχνολογικές λύσεις για την ανάπτυξη των εφαρμογών Mobile Banking, εξασφαλίζοντας την ασφάλεια, τη λειτουργικότητα και την ευχρηστία. Μεγάλοι φορείς αποτελούν και οι εταιρείες ανάπτυξης λογισμικού και πάροχοι υποδομών Cloud.
3. ***Οι εταιρείες κινητής τηλεφωνίας*** : Αυτές σε συνδέουν στο διαδίκτυο για να μπορείς να χρησιμοποιήσεις την εφαρμογή M-Banking. Χάρη στην κινητή σου συσκευή έχεις πρόσβαση στην Τράπεζά σου ανά πάσα στιγμή και από οπουδήποτε
4. ***Πάροχοι Ασφάλειας***: Οι φορείς που εξειδικεύονται σε θέματα ψηφιακής ασφάλειας, όπως κρυπτογράφηση και πιστοποίηση ταυτότητας, διασφαλίζουν την προστασία των δεδομένων των χρηστών και την αποτροπή κυβερνοεπιθέσεων.
5. ***Ρυθμιστικές Αρχές***: Όπως οι Κεντρικές Τράπεζες και οι αρμόδιες ρυθμιστικές υπηρεσίες καθορίζουν τους κανόνες και τις κατευθυντήριες γραμμές που διέπουν τις υπηρεσίες Mobile Banking όπως η προστασία δεδομένων και η διαφάνεια των συναλλαγών.
6. ***Χρήστες*** : Ο τελικός φορέας, καθώς οι χρήστες είναι αυτοί που αξιοποιούν τις υπηρεσίες Mobile Banking για τις χρηματοοικονομικές τους ανάγκες.

2.2 Παρεχόμενες Υπηρεσίες

Το M-Banking είναι ένας πολύ βολικός τρόπος να διαχειριστείς τα χρήματά σου, χωρίς να χρειαστεί να πας στην Τράπεζα. Οι υπηρεσίες που προσφέρει ποικίλλουν ανάλογα με την Τράπεζα αλλά γενικά μπορούμε να πούμε ότι οι πιο συνηθισμένες-βασικότερες είναι κυρίως αυτές που αφορούν την ανεύρεση πληροφοριών παράδειγμα το υπόλοιπο του τραπεζικού λογαριασμού (Federal Reserve Board,2016). Εμβαθύνοντας έχουμε τις εξής :

α) Πληροφορίες – Ενημέρωση Λογαριασμών – Καταθέσεις

- Καταθέσεις
- Υπόλοιπο Λογαριασμού
- Κινήσεις καταθετικού λογαριασμού
- Κατάσταση Επιταγών / Πάγιες Εντολές
- Alert συναλλαγών
- Δάνεια
- Υπόλοιπο δανειακού λογαριασμού
- Κινήσεις δανειακού λογαριασμού
- Αναλυτικός πίνακας δόσεων δανείου
- Alert συναλλαγών
- Πιστωτικές Κάρτες
- Υπόλοιπο πιστωτικών καρτών
- Τελευταίες κινήσεις πιστωτικών καρτών (statement)
- Επενδύσεις
- Χαρτοφυλάκιο Μετοχών
- Χαρτοφυλάκιο Αμοιβαίων Κεφαλαίων
- Κατάσταση ΧΑΑ
- Κατάσταση αμοιβαίων κεφαλαίων της Τράπεζας
- Τιμές συναλλάγματος

β) Κίνηση Κεφαλαίων

- Μεταφορά χρημάτων μεταξύ των λογαριασμών του ίδιου δικαιούχου
- Μεταφορά χρημάτων μεταξύ των λογαριασμών διαφορετικών δικαιούχων
- Εμβάσματα σε μετρητά
- Διατραπεζική μεταφορά Εσωτερικού Δίας (Dias Transfer)
- Διατραπεζική μεταφορά Εξωτερικού
- Αγορά & Πώληση μετοχών ΧΑΑ
- Αγορά & Εξαγορά μεριδίων της Τράπεζας

γ) Πληρωμές Οφειλών

- Δάνεια – Πιστωτικές Κάρτες

- Δόσεις Δανείου
- Κάρτα εκδόσεως της Τράπεζας ίδιου κατόχου
- Κάρτα εκδόσεως της Τράπεζας τρίτων
- Κάρτα εκδόσεως άλλων Τραπεζών
- Δημόσιο κ΄ ΔΕΚΟ
- Φόρος εισοδήματος Φ.Π., Τέλη κυκλοφορίας
- ΦΠΑ, ΙΚΑ, ΟΑΕΕ
- ΔΕΗ, ΕΥΔΑΠ, ΟΤΕ
- Πάγιες εντολές πληρωμών

δ) Αιτήσεις

- Άνοιγμα λογαριασμού
- Αλλαγή UserID και Password
- Έκδοση καρνέ-μπλοκ επιταγών
- Χορήγηση Δανείου
- Ενεργοποίηση/απενεργοποίηση alert συναλλαγών και γενικών ειδοποιήσεων
- Αποστολή Ενημερώσεων

ε) Γενικές πληροφορίες για προϊόντα και υπηρεσίες της Τράπεζας

Οι προαναφερθείσες υπηρεσίες και η διάθεση αυτών, γίνεται κυρίως με χρήση της τεχνολογίας των SMS ή με το πρωτόκολλο WAP(Wireless Application Protocol) τα οποία θα αναλύσουμε στο 3ο Κεφάλαιο.

Οι υπηρεσίες του M-Banking διακρίνονται σε ***δύο ομάδες***, αναλόγως με το αν η υπηρεσία παρέχεται αυτόματα.

1η Ομάδα "Push" : σε αυτήν την ομάδα η Τράπεζα αποστέλλει ενημερώσεις-πληροφορίες στον πελάτη βασιζόμενη σε προσυμφωνημένους κανόνες μεταξύ των δύο μερών. Αυτό γίνεται χωρίς να το έχει ζητήσει την προκειμένη στιγμή ο πελάτης (πχ. Alert συναλλαγών)

2η Ομάδα "Pull" : εδώ έχουμε το αντίθετο. Αυτό σημαίνει ότι σε αυτή την περίπτωση ο πελάτης αποστέλλει ένα αίτημα στην Τράπεζα και η τελευταία το διεκπεραιώνει, κάτι που αποτελεί και την πλειοψηφία των υπηρεσιών M-Banking.

Ένας άλλος τρόπος κατηγοριοποίησης έχει να κάνει με την φύση της υπηρεσίας γενικά, σχηματίζοντας 2 κατηγορίες :

1) Υπηρεσίες Ελέγχου – Ενημερώσεων (πχ Ερώτηση Υπολοίπου – Κατάσταση ενός λογαριασμού)
2) Υπηρεσίες Συναλλαγών (πχ Μεταφορά κεφαλαίων, πληρωμή λογαριασμών) – Απαιτούν Αυξημένη ασφάλεια όσον αφορά το κανάλι επικοινωνίας πελάτη – Τράπεζας.

Γενικά όμως η επικρατέστερη διαφοροποίηση των υπηρεσιών M-Banking γίνεται λαμβάνοντας υπόψη το αντικείμενο το υπηρεσιών, έτσι έχουμε τα εξής:

α) Κινητή διαχείριση των Τραπεζικών λογαριασμών : Χρήση υπηρεσιών της Τράπεζας χωρίς τη διαμεσολάβηση πληροφορικής για έναν προσωπικό λογαριασμό πχ. ταμιευτήριο.

β) Κινητή διαχείριση των Χρηματιστηριακών λογαριασμών: Πρόκειται για συναλλαγές μη πληροφοριακού χαρακτήρα συνδεδεμένες με λογαριασμό αξιών.

γ) Κινητές Οικονομικές Πληροφορίες: Υπηρεσίες ενημέρωσης αποκλειστικά.

2.3 Χαρακτηριστικά M-Banking

Το κινητό τηλέφωνο προσφέρει όχι μόνο φορητότητα και ευελιξία, αλλά και νέες επαγγελματικές δυνατότητες, ιδιαίτερα σε τομείς όπου η θέση του χρήστη παίζει σημαντικό ρόλο. Διαθέτει επίσης το πλεονέκτημα ευρύτερης συνδεσιμότητας. Επειδή μια φορητή συσκευή συνοδεύει το χρήστη συνεχώς, 24 ώρες την ημέρα και 7 μέρες την εβδομάδα, το M-Banking μπορεί εύκολα να ενσωματωθεί στην καθημερινότητά του, τόσο στην εργασία όσο και στον ελεύθερο χρόνο του. Αυτές οι δυνατότητες δεν είναι άμεσα προσβάσιμες μέσω του Διαδικτύου από έναν σταθερό υπολογιστή. Γι' αυτό, οι υπηρεσίες σχεδιάζονται με τρόπο που αξιοποιεί συγκεκριμένα χαρακτηριστικά τα οποία θα ενισχύσουν την ανάπτυξη του M-Banking και θα προσελκύσουν νέους πελάτες.

1) **Ευκολία εκμάθησης** : Αυτό σημαίνει ότι πρέπει να μπορείς να καταλάβεις πως λειτουργεί η εφαρμογή χωρίς να χρειαστεί πολύς χρόνος και προσπάθεια. Οι χρήστες χρειάζονται σαφείς οδηγίες και υποστήριξη για να κατανοήσουν γρήγορα τις λειτουργίες της εφαρμογής.

2) **Αλληλεπίδραση** : Όταν κάνεις κάτι στην εφαρμογή πρέπει να παίρνεις σαφείς και κατανοητές απαντήσεις. Γενικά, μιλάμε για την ανταπόκριση του συστήματος στις ενέργειες του χρήστη, πχ "καθαρές" ειδοποιήσεις και απαντήσεις στις συναλλαγές.
3) **Ευκολία χρήσης** : Η εφαρμογή πρέπει να είναι σχεδιασμένη με τρόπο που να σε βοηθάει να κάνεις αυτό που θέλεις γρήγορα και εύκολα. Οι διαισθητικές επαφές (interface) είναι κρίσιμες διότι πρέπει να εξυπηρετούν χρήστες με διαφορετικά επίπεδα εξοικείωσης με την τεχνολογία.
4) **Καταλληλότητα σχεδιασμού** : Το M-Banking App πρέπει να είναι σχεδιασμένο έτσι ώστε να ανταποκρίνεται στις προσδοκίες των πελατών, τόσο λειτουργικά όσο και αισθητικά.
5) **Επάρκεια** : Η επάρκεια της υπηρεσίας αφορά την κάλυψη των βασικών αναγκών και απαιτήσεων του χρήστη, προσφέροντας πλήρες φάσμα τραπεζικών λειτουργιών.
6) **Θετική εμπειρία** : Η υπηρεσία πρέπει να προσφέρει μια συνολικά ευχάριστη εμπειρία στο χρήστη, μέσω απρόσκοπτης λειτουργίας και ικανοποίησης των προσδοκιών του.
7) **Ακριβής πληροφόρηση** : Οι πληροφορίες που παρέχονται από την υπηρεσία πρέπει να είναι ακριβείς, ώστε να αποτρέπονται λάθη και παρανοήσεις στις συναλλαγές.
8) **Αξιόπιστη πληροφόρηση** : Η αξιοπιστία είναι κρίσιμη, καθώς οι χρήστες πρέπει να νιώθουν ότι μπορούν να βασίζονται στις πληροφορίες που τους παρέχονται.
9) **Επίκαιρη πληροφόρηση** : Οι πληροφορίες πρέπει να είναι πάντα ενημερωμένες, διασφαλίζοντας ότι ο χρήστης έχει πρόσβαση στα πιο πρόσφατα δεδομένα.
10) **Σχετική πληροφόρηση** : Οι παρεχόμενες πληροφορίες πρέπει να είναι σχετικές με τις ανάγκες και τις ενέργειες του χρήστη, αποφεύγοντας περιττές ή άσχετες λεπτομέρειες.
11) **Κατανοητή πληροφόρηση** : Η πληροφορία πρέπει να παρουσιάζεται με τρόπο που είναι εύκολα αντιληπτός από κάθε χρήστη, ανεξάρτητα από την εξοικείωσή του με την τεχνολογία.

12) **Επαρκής πληροφόρηση** : Η υπηρεσία πρέπει να παρέχει όλες τις απαραίτητες πληροφορίες χωρίς κενά που θα μπορούσαν να προκαλέσουν σύγχυση.
13) **Σωστή παρουσίαση της πληροφόρησης** : Η πληροφορία πρέπει να παρουσιάζεται με σαφή, λογικό και "ελκυστικό" τρόπο, ώστε να είναι εύκολα προσβάσιμη και κατανοητή. Γενικά πρέπει να γίνεται ορθή χρήση των μέσων που χρησιμοποιούνται πχ κείμενο, φωτογραφίες, γραφήματα, μουσική-ήχοι και βίντεο.
14) **Καλή φήμη** : Η φήμη της υπηρεσίας βασίζεται στην εμπιστοσύνη που έχουν οι χρήστες στη σταθερότητα, την ποιότητα και την ασφάλειά της.
15) **Ασφάλεια συναλλαγών** : Οι χρηματοοικονομικές συναλλαγές πρέπει να διασφαλίζουν απόλυτη προστασία έναντι απάτης ή κακόβουλων ενεργειών. Αυτό εξαρτάται και από τις παραμέτρους που δημιουργούν την αίσθηση της ασφάλειας όπως είναι η αξιοπιστία απόκρισης και ο χρόνος αναμονής.
16) **Ασφάλεια ατομικών πληροφοριών** : Η προστασία προσωπικών δεδομένων του χρήστη είναι θεμελιώδης, ενισχύοντας την εμπιστοσύνη στην υπηρεσία. Αυτό εξαρτάται κυρίως από την κρυπτογράφηση που χρησιμοποιείται από την εκάστοτε Τράπεζα αλλά και από τα συστήματα διασφάλισης για κλοπή από τρίτους στην διαδικασία μεταφοράς δεδομένων.
17) **Εξατομίκευση** : Το M-Banking πρέπει να προσαρμόζεται στις ανάγκες και τις προτιμήσεις του χρήστη, προσφέροντας μια προσωποποιημένη εμπειρία.
18) **Αίσθηση συμμετοχής σε κοινότητα** : Η υπηρεσία μπορεί να ενισχύσει την εμπειρία του χρήστη, προσφέροντας δυνατότητες που δημιουργούν αίσθηση σύνδεσης με μια ευρύτερη κοινότητα. Αυτές μπορεί να είναι η επικοινωνία με άλλους χρήστες σε "δωμάτια" (forum) συζητήσεων ή συμμετοχή σε προγράμματα επιβράβευσης.
19) **Διευκόλυνση επικοινωνίας με την Τράπεζα** : Η υπηρεσία πρέπει να παρέχει εύκολους τρόπους επικοινωνίας, όπως ζωντανή συνομιλία, email ή τηλέφωνο, για την εξυπηρέτηση του χρήστη. Σημαντικό είναι και οι πληροφορίες σχετικά με τα τηλέφωνα-email να χωρίζονται και ανά κατάστημα, ανά διεύθυνση και ανά δραστηριότητα.

20) **Εκπλήρωση υποσχέσεων** : Η υπηρεσία πρέπει να ανταποκρίνεται πλήρως στις υποσχέσεις που δίνει τόσο σε επίπεδο λειτουργικότητας όσο και υποστήριξης.
21) **Ευκολία πλοήγησης WAP** : Η πλοήγηση μέσω WAP πρέπει να είναι εύκολη και διαισθητική, επιτρέποντας στους χρήστες να βρίσκουν γρήγορα αυτό που χρειάζονται.
22) **Ελκυστική εμφάνιση WAP** : Η σχεδίαση του περιβάλλοντος WAP πρέπει να είναι αισθητικά ευχάριστη, προσελκύοντας και διατηρώντας το ενδιαφέρον του χρήστη.

Αυτά τα χαρακτηριστικά συνθέτουν μια ολοκληρωμένη εμπειρία χρήστη στο M-Banking, προωθώντας την εμπιστοσύνη, την ευκολία και την ικανοποίηση.

2.4 Οφέλη του M-Banking

Το M-Banking έχει φέρει επανάσταση στον τρόπο που διαχειριζόμαστε τα χρήματά μας, προσφέροντας μια σειρά από πλεονεκτήματα τόσο για τους καταναλωτές όσο και για τις Τράπεζες :

α) Οφέλη για τον καταναλωτή :

Ευκολία και προσβασιμότητα : Ο καταναλωτής μπορεί να εκτελεί συναλλαγές οποιαδήποτε στιγμή από οπουδήποτε χωρίς να επισκέπτεται φυσικό κατάστημα, αρκεί να έχει το κινητό του.

Εξοικονόμηση χρόνου : Οι συναλλαγές ολοκληρώνονται γρήγορα μέσω εφαρμογών, αποφεύγοντας τις ουρές στα υποκαταστήματα, με μερικά μόνο "πατήματα" με το δάχτυλό σου.

Οικονομία χρημάτων : Ο καταναλωτής μειώνει τα έξοδά του πχ από τις μετακινήσεις που έκανε για να πάει σε ένα υποκατάστημα της Τράπεζας. Επίσης, οι Τράπεζες πλέον χρεώνουν πολύ χαμηλές προμήθειες για τις online συναλλαγές.

Ενημέρωση σε Πραγματικό Χρόνο : Ειδοποιήσεις για την κάθε συναλλαγή ή κίνηση στον λογαριασμό και παρακολούθηση των οικονομικών με έξυπνα εργαλεία "budgeting".

Ασφάλεια : Χρήση βιομετρικών δεδομένων (πχ δαχτυλικό αποτύπωμα, αναγνώριση προσώπου) για ασφαλείς συναλλαγές. Εντοπισμός ύποπτων

κινήσεων μέσω ειδοποιήσεων. Δυνατότητα μπλοκαρίσματος της κάρτας σου άμεσα σε περίπτωση απώλεια ή κλοπής.

β) Οφέλη για την <u>Τράπεζα</u> :

Μείωση κόστους λειτουργίας : Λιγότερες συναλλαγές στα υποκαταστήματα μειώνουν τα λειτουργικά έξοδα όπως προσωπικό, εξοπλισμός και ενοίκια. Αυτό βοηθά ταυτόχρονα και στην πιο σωστή αξιοποίηση του προσωπικού που μέχρι σήμερα απασχολούταν με τις συναλλαγές.

Αύξηση εσόδων : Ενίσχυση της χρήσης Τραπεζικών προϊόντων (π.χ. δάνεια, πιστωτικές κάρτες) μέσω των εφαρμογών. Έσοδα από online προμήθειες και συναλλαγές. Η τεχνολογία επίσης οδηγεί και σε προσφορά νέων προϊόντων και υπηρεσιών.

Διατήρηση πελατών και προσέλκυση νέων : Η βελτίωση της εμπειρίας του πελάτη οδηγεί σε αυξημένη ικανοποίηση και πιστότητα. Κάνοντας χρήση της νέας τεχνολογίας και της τεχνητής νοημοσύνης μπορούν να αναπτύξουν στοχευμένο Μάρκετινγκ αλλά και να έχουν εξατομικευμένες προσφορές στους υπάρχον πελάτες μέσω σωστής συλλογής δεδομένων και ανάλυση συμπεριφοράς.

Μείωση του ρίσκου : Πιο αποτελεσματική ανίχνευση απάτης μέσω προηγμένων συστημάτων. Εντοπισμός ύποπτων κινήσεων με αυτοματοποιημένα εργαλεία.

2.5 Μειονεκτήματα του M-Banking

Το Mobile Banking είναι ένα πολύ βολικό "εργαλείο", αλλά χρειάζεται προσοχή. Παρά την πληθώρα πλεονεκτημάτων δεν παύει να υπάρχει και η αρνητική του πλευρά, κάτι που επηρεάζει άμεσα και το Ελληνικό καταναλωτικό κοινό.

α) Μειονεκτήματα για τον <u>Καταναλωτή</u> :

Ασφάλεια – Ιδιωτικότητα : Πρώτο και βασικό, ο κίνδυνος παραβίασης προσωπικών δεδομένων από Hackers με κακόβουλα λογισμικά. Όσον αφορά την ασφάλεια είναι ότι εξαρτάται σε μεγάλο βαθμό και από την ασφάλεια της ίδιας της κινητής συσκευής (πχ ένα μη ενημερωμένο λογισμικό μπορεί να δημιουργήσει ευπάθειες).

Εξάρτηση από την τεχνολογία : Απαιτείται σύνδεση στο διαδίκτυο, που μπορεί να μην είναι πάντα διαθέσιμη. Επίσης, υπάρχουν και προβλήματα στις

λειτουργίες των εφαρμογών λόγω τεχνικών σφαλμάτων ή διακοπών (server downtime) που σε περίπτωση ανάγκης για συναλλαγή θα βρεθούμε εκτεθειμένοι.

Περιορισμένη υποστήριξη : Για την ώρα οι Τράπεζες δυσκολεύονται στην επίλυση σύνθετων θεμάτων μέσω της εφαρμογής καθώς δεν υπάρχει η σωστή εξειδίκευση του προσωπικού, αλλά ταυτόχρονα μιλάμε και για ένα εργαλείο που ακόμα εξελίσσεται.

Πολυπλοκότητα για ορισμένους χρήστες : Οι εφαρμογές αυτές δεν είναι "φιλικές" για ανθρώπους με περιορισμένη τεχνολογική εξοικείωση, όπως οι ηλικιωμένοι. Από την άλλη μεριά μπορεί και κάποιες εφαρμογές να έχουν σχεδιαστικές ατέλειες, κάτι που θα επηρεάζει την ευκολία στη χρήση τους.

Εξάρτηση από τις κινητές συσκευές : Αν χαθεί ή κλαπεί το κινητό, υπάρχει κίνδυνος μη εξουσιοδοτημένης πρόσβασης. Επείγουσες συναλλαγές δεν μπορούν να πραγματοποιηθούν αν η συσκευή δεν λειτουργεί (πχ χαμηλή μπαταρία).

β) Μειονεκτήματα για την <u>Τράπεζα</u> :

Αυξημένο ρίσκο ασφαλείας : Οι κυβερνοεπιθέσεις και οι παραβιάσεις δεδομένων αποτελούν μεγάλη απειλή. Απαίτηση επενδύσεων σε προηγμένα μέτρα ασφαλείας όπως η κρυπτογράφηση και συστήματα ανίχνευσης απάτης.

Υψηλό κόστος υλοποίησης και συντήρησης : Ανάπτυξη, βελτίωση και συντήρηση της εφαρμογής απαιτούν σημαντικούς οικονομικούς και τεχνικούς πόρους. Η συνεχής αναβάθμιση είναι απαραίτητη για την παρακολούθηση τεχνολογικών εξελίξεων και απαιτήσεων της αγοράς.

Μειωμένη επαφή με τον πελάτη : Η μειωμένη φυσική παρουσία πελατών στα υποκαταστήματα περιορίζει την δυνατότητα προσωπικής επικοινωνίας και πώλησης νέων προϊόντων. Επίσης έχουμε μικρότερη ευκαιρία για οικοδόμηση σχέσεων εμπιστοσύνης μεταξύ ιδρύματος και πελάτη.

Πίεση για συνεχή καινοτομία : Ο ανταγωνισμός με άλλες τράπεζες και Fintech εταιρείες απαιτεί συνεχή βελτίωση και καινοτομία. Αυτό για κάποιες μικρές τράπεζες μπορεί να είναι δύσκολο γιατί το κόστος και η ταχύτητα εφαρμογής νέων χαρακτηριστικών μπορεί να είναι αρκετά περιοριστικοί παράγοντες.

Το M-Banking προσφέρει τεράστια οφέλη, αλλά απαιτεί συνεχή προσαρμογή και προσοχή για να αντιμετωπιστούν οι τεχνολογικές και κοινωνικές του προκλήσεις. Με τη σωστή ισορροπία μπορεί να εξυπηρετήσει τόσο τις ανάγκες των καταναλωτών όσο και των τραπεζών, οδηγώντας σε ένα πιο αποτελεσματικό και ασφαλές Τραπεζικό Σύστημα.

Κεφάλαιο 3ο

«Mobile Banking και Τεχνολογία»

3.1 Η Εξέλιξη του Mobile Banking

Η εξέλιξη του Mobile Banking είναι μία δυναμική διαδικασία που αντικατοπτρίζει τις τεχνολογικές και κοινωνικές αλλαγές. Από την αρχική του μορφή μέχρι σήμερα, το M-Banking έχει περάσει από διάφορα στάδια ανάπτυξης τα οποία συνοψίζονται ως εξής :

1. ***Τα Πρώτα Βήματα (1990 – 2000)***

   SMS Banking : Οι πρώτες υπηρεσίες Mobile Banking βασίζονταν σε SMS. Οι χρήστες μπορούσαν να λαμβάνουν ειδοποιήσεις για το υπόλοιπο λογαριασμού ή να πραγματοποιούν βασικές συναλλαγές μέσω γραπτών μηνυμάτων.

   WAP Banking : Με την ανάπτυξη του Mobile Internet εμφανίστηκαν τραπεζικές πλατφόρμες βασισμένες σε WAP (Wireless Application Protocol). Ωστόσο, οι υπηρεσίες αυτές ήταν περιορισμένες λόγω χαμηλής ταχύτητας σύνδεσης και κακής εμπειρίας χρήστη.

2. ***Άνοδος των Εφαρμογών (2010)***

   Εφαρμογές Mobile Banking : Η διάδοση των smartphones και των App Stores (πχ IOS App Store, Playstore) έδωσε ώθηση στη δημιουργία τραπεζικών εφαρμογών.

   Περισσότερες δυνατότητες : Οι εφαρμογές προσέφεραν μεταφορές χρημάτων, πληρωμές λογαριασμών, αναλύσεις δαπανών και υποστήριξη πελατών.

   Ασφάλεια : Ξεκίνησε η ενσωμάτωση ασφαλών μεθόδων όπως PIN, κωδικοί μίας χρήσης (OTP) και αρχικές μορφές βιομετρικής ταυτοποίησης.

3. ***Τεχνολογική Καινοτομία (2020)***

   Βιομετρική Ταυτοποίηση : Αναγνώριση δακτυλικού αποτυπώματος, αναγνώριση προσώπου και ίριδας έχουν γίνει πλέον στάνταρ ασφαλείας.

   Προσωποποιημένη Εμπειρία : Οι Τράπεζες χρησιμοποιούν τεχνητή νοημοσύνη (AI) για να παρέχουν εξατομικευμένες προτάσεις και οικονομικές αναλύσεις.

   Συνδεδεμένα Οικοσυστήματα : Ενσωμάτωση του M-Banking με άλλες πλατφόρμες όπως ψηφιακά πορτοφόλια (πχ Apple Pay, Google Pay), αγορές κρυπτονομισμάτων και επενδυτικές υπηρεσίες.

4. ***Μελλοντικές Τάσεις***

Open Banking : Η χρήση APIs (Application Programming Interfaces) επιτρέπει στις Τράπεζες να συνεργάζονται με τρίτους παρόχους για καινοτόμες υπηρεσίες διευκολύνοντας την πρόσβαση σε χρηματοοικονομικά δεδομένα.

AI και Chatbots : Εξελιγμένα συστήματα εξυπηρέτησης πελατών, μέσω AI, προσφέρουν άμεσες λύσεις σε αιτήματα και ερωτήματα χρηστών.

- ***Πιο ανεπτυγμένα Οικοσυστήματα :***
    a. IoT Banking (Internet of Things) : Δυνατότητα συναλλαγών, μέσω "έξυπνων" συσκευών, όπως wearables.
    b. Φωνητικές Εντολές : Υπηρεσίες φωνητικής αναγνώρισης για γρήγορη πρόσβαση και συναλλαγές.
- ***Ενισχυμένη Ασφάλεια : Η τεχνολογία Blockchain και τα πολυεπίπεδα*** πρωτόκολλα ασφαλείας θα ενισχύσουν την προστασία δεδομένων και συναλλαγών.

5. ***Κοινωνική Επίδραση της Εξέλιξης***

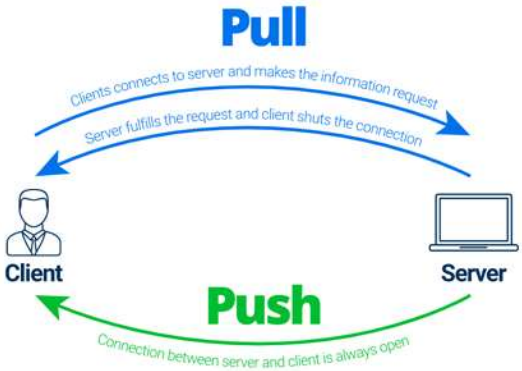
1) Αυξημένη χρήση : Το M-Banking έχει καταστεί βασικό εργαλείο για την διαχείριση χρημάτων, ειδικά μετά την πανδημία COVID-19, που επιτάχυνε τη μετάβαση στις ψηφιακές υπηρεσίες.
2) Πρόσβαση σε Αναπτυσσόμενες Χώρες : Οι κινητές τραπεζικές υπηρεσίες έχουν ενισχύσει την οικονομική ενσωμάτωση ατόμων που δεν έχουν πρόσβαση σε παραδοσιακές τράπεζες.
3) Εξατομικευμένες Υπηρεσίες : Η εμπειρία χρήστη συνεχώς βελτιώνεται, καθώς οι Τράπεζες προσπαθούν να κατανοήσουν τις ανάγκες του πελάτη σε βάθος.

Η εξέλιξη του M-Banking είναι άρρηκτα συνδεδεμένη με τις τεχνολογικές εξελίξεις και τις μεταβαλλόμενες ανάγκες της κοινωνίας.

3.2 Οι τεχνολογίες του M-Banking

Βασικός παράγοντας για την ανάπτυξη των κινητών οικονομικών υπηρεσιών είναι η τεχνολογία. Οι υπηρεσίες αυτές προσφέρονται μέσω πολλών διαφορετικών καναλιών, κάτι που σημαίνει ότι οι Τράπεζες καλούνται να επιλέξουν το καλύτερο για την επικοινωνία με τους πελάτες τους. Το M-Banking στηρίχτηκε σε εφαρμογές των τεσσάρων καναλιών :

- *SMS (Short Messaging Service)*
- *WAP (Wireless Application Protocol)*
- *IVR (Interactive Voice Response)*
- *SMAC (Standalone Mobile Application Clients)*



1. SMS Banking

Το SMS Banking είναι μία από τις πρώτες μορφές ψηφιακής τραπεζικής που χρησιμοποιεί μηνύματα SMS για την εκτέλεση βασικών τραπεζικών λειτουργιών. Γενικά οι υπηρεσίες που καλύπτει έχουν ενημερωτικό χαρακτήρα αλλά υπάρχουν και εξαιρέσεις ορισμένων Τραπεζικών Ιδρυμάτων που φτάνουν να διεκπεραιώνουν μέχρι και συναλλαγές. Η συγκεκριμένη τεχνολογία χρησιμοποιεί τους τύπους μηνυμάτων : Push και Pull.

Push Μηνύματα : Το Τραπεζικό ίδρυμα στέλνει αυτοματοποιημένες ειδοποιήσεις στους πελάτες του. Οι ειδοποιήσεις αυτές αφορούν ενημερώσεις για τα υπόλοιπα των λογαριασμών, ειδοποιήσεις για πληρωμές που εκκρεμούν, ειδοποιήσεις για εισερχόμενα εμβάσματα. Η συγκεκριμένη λειτουργία παρέχει άμεση ενημέρωση 24 ώρες το 24ωρο προσφέροντας και ενισχυμένη ασφάλεια στον καταναλωτή κρατώντας τον σε συνεχή επαφή με τα χρήματά του.

Pull Μηνύματα : Από την άλλη πλευρά ο πελάτης στέλνει ερωτήσεις – αιτήματα στην Τράπεζα πχ ρωτάει για το υπόλοιπο του λογαριασμού του ή ακόμα αιτείται και για μεταφορά χρημάτων. Η υπηρεσία αυτή είναι αρκετά χρήσιμη καθώς ο χρήστης μπορεί να κάνει τα παραπάνω χωρίς να είναι απαραίτητη η σύνδεσή του στο διαδίκτυο.

Το SMS Banking έχει πλεονεκτήματα αλλά δεν παύει να έχει και μειονεκτήματα :

Στα ***πλεονεκτήματα*** έχουμε :

- Εύκολη πρόσβαση : Δεν χρειάζεται να έχει κάποιος στην κατοχή του Smartphone· μπορεί με οποιοδήποτε κινητό να κάνει χρήση αυτής της υπηρεσίας. Επίσης δεν χρειάζεται ο χρήστης να είναι "παντογνώστης" της τεχνολογίας καθώς χρειάζεται μόνο κάποιες βασικές γνώσεις αποστολής και ανάγνωσης SMS.
- Άμεση ενημέρωση και εξοικονόμηση χρόνου : Οι χρήστες λαμβάνουν απαντήσεις στα ερωτήματα-αιτήματά τους άμεσα και πραγματικό χρόνο αποφεύγοντας την πολύωρη αναμονή σε Τράπεζες ή ATMς.

Στα ***μειονεκτήματα*** έχουμε :

- "Ξεπερασμένο" σύστημα κινητής τραπεζικής : Οι λειτουργίες και οι δυνατότητες του SMS Banking σε σχέση με τα νέα Apps είναι αρκετά περιορισμένες.
- Έξοδο για τον καταναλωτή : Υπάρχουν περιπτώσεις όπου η χρέωση του SMS επιβαρύνει τον πελάτη.
- Ασφάλεια : Ακόμα και τα SMS είναι ευάλωτα σε υποκλοπές και "Spoofing"

1. Ορισμός "Spoofing" (https://www.investopedia.com)

Για να λειτουργήσει η υπηρεσία του SMS Banking υπάρχει μια σειρά δομικών στοιχείων που λειτουργούν αρμονικά για να πετύχουν αυτό το αποτέλεσμα. Αυτά είναι τα εξής :

1. Κινητός Σταθμός – Mobile Station (MS)

   Πρόκειται για το ίδιο το κινητό τηλέφωνο που είναι απαραίτητο για την αποστολή και λήψη των SMS. Αποτελεί το αρχικό αλλά ταυτόχρονα το τελικό σημείο επαφής χρήστη με το SMS Banking.

2. Κέντρο Μεταγωγής Κινητής Τηλεφωνίας – Mobile Switching Center (MSC)

   Ευθύνη αυτού είναι η διαχείριση των κλήσεων και SMS στο δίκτυο κινητής τηλεφωνίας. Κατόπιν επεξεργασίας προωθεί τα SMS από το MS προς το επόμενο στοιχείο SMSC.

3. Κέντρο Υπηρεσιών Μηνυμάτων Κειμένου – Short Message Service Center (SMSC)

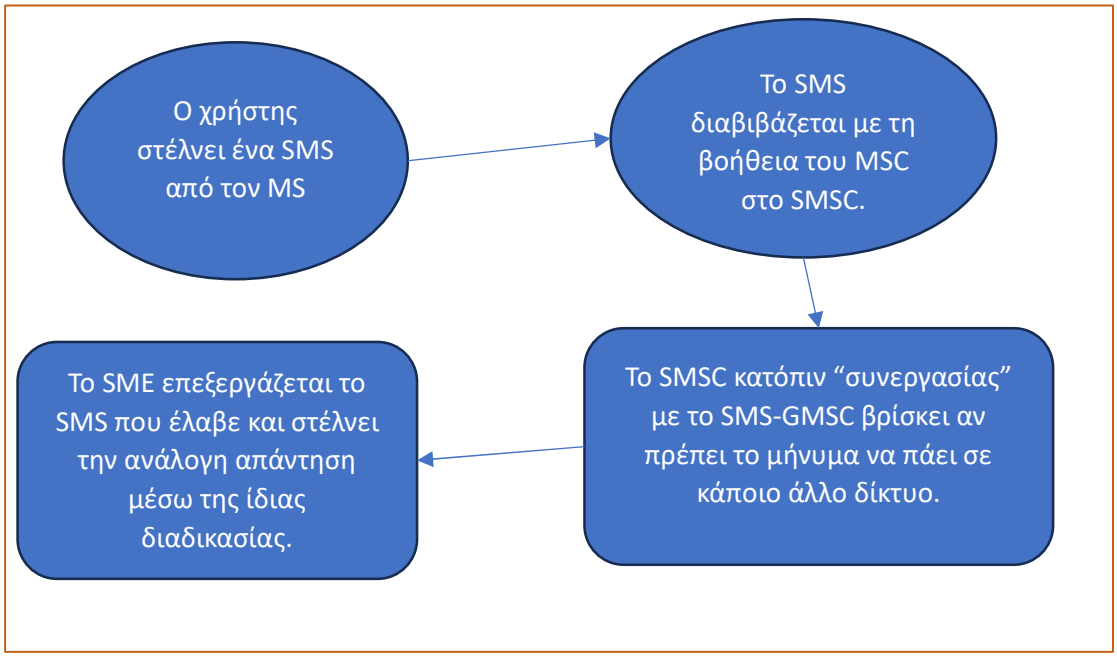
   Αποτελεί τον κεντρικό "κόμβο", καθώς εκεί αποθηκεύονται τα SMS και μετά προωθούνται. Σε περίπτωση που ο παραλήπτης δεν είναι σε θέση να λάβει το SMS, το SMSC αποθηκεύει το μήνυμα μέχρι να παραδοθεί σε αυτόν.

4. SMS Gateway Mobile Switching Center (SMS – GMSC)

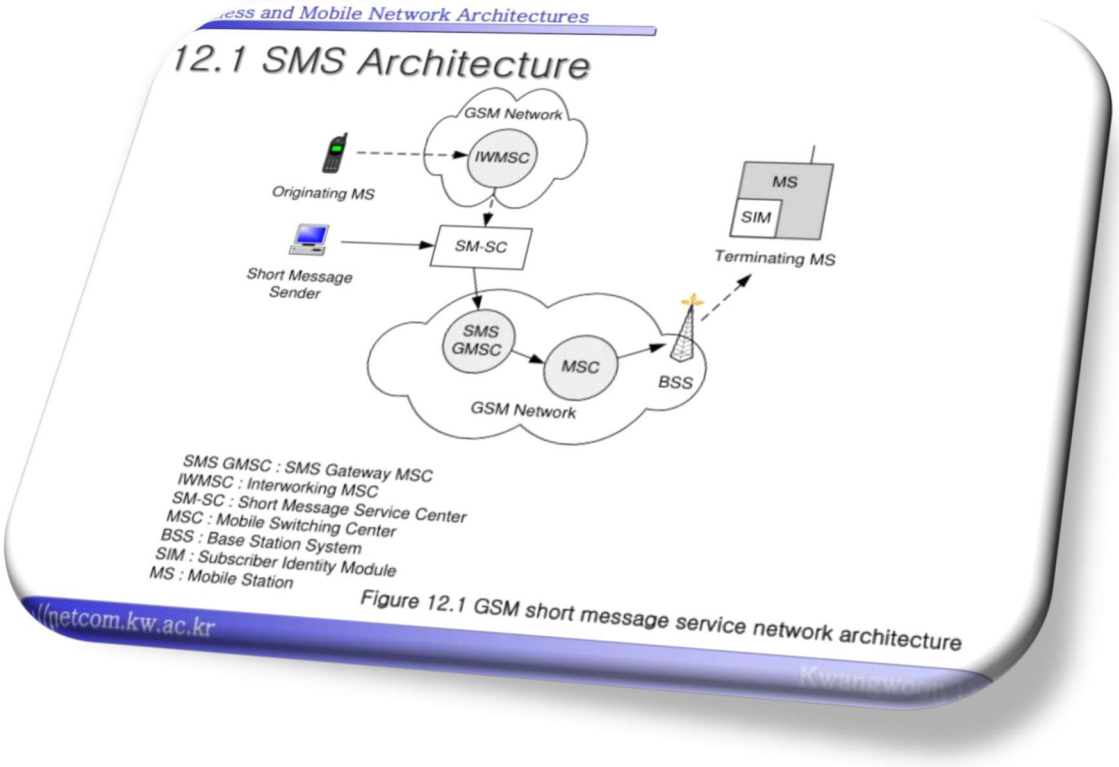
   Ο ρόλος του είναι να λαμβάνει τα μηνύματα από το GMSC – να εξετάζει για τις απαραίτητες πληροφορίες τη βάση HLR (Home Location Register) – και τέλος να τα αποστέλλει στο σωστό MSC.

5. Short Message Entity (SME)

   Είναι η ίδια η Τράπεζα. Αυτή λαμβάνει τα μηνύματα και έπειτα δημιουργεί τις απαντήσεις (Push) και τις αποστέλλει.



2.Περιγραφή διαδικασίας SMS (Συμβολή του συγγραφέα)



3.Αρχιτεκτονική SMS – Banking

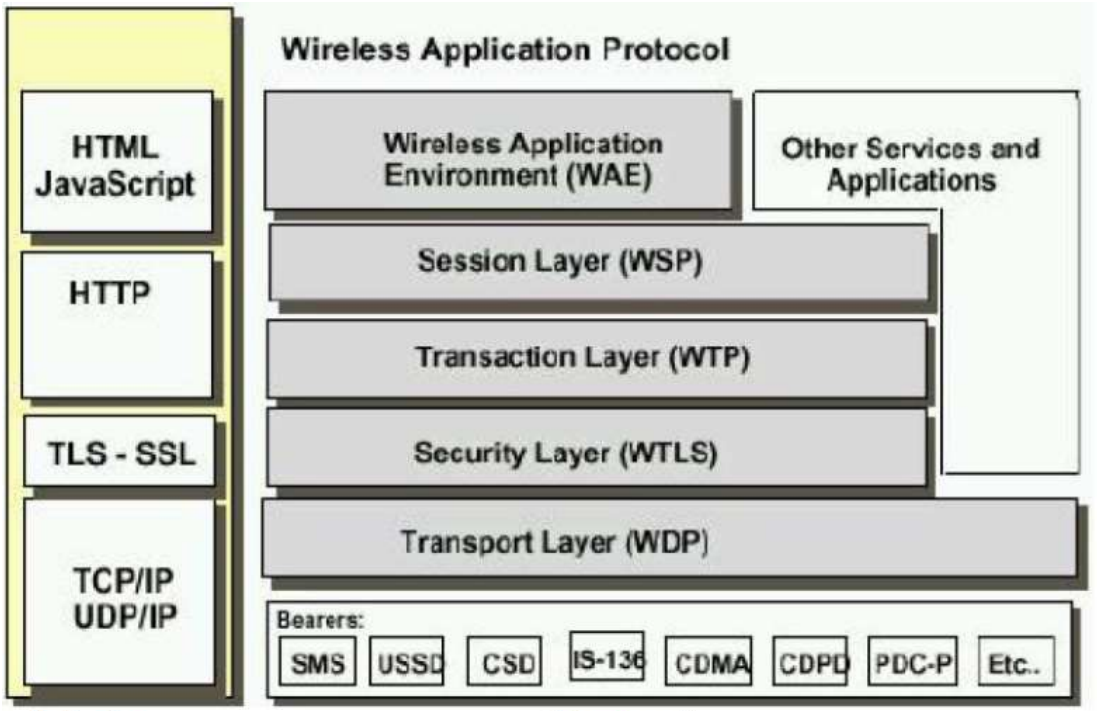
2. *WAP Banking (Wireless Application Protocol)*

Το WAP αποτελεί μια πρώιμη μορφή πρόσβασης σε τραπεζικές υπηρεσίες μέσω του κινητού. Ένα διεθνές πρότυπο για μεταφορά-παρουσίαση δεδομένων σε κινητά και άλλα ασύρματα τερματικά.

Το 1997 μια συνεργασία "γιγάντων" που ακούνε στα ονόματα Nokia, Ericsson, Motorola και Unwired Planet ανάπτυξαν το πρωτόκολλο αυτό μέσω του οργανισμού WAP Forum. Οι εταιρείες αυτές συνειδητοποίησαν ότι για να υπάρξει ανάπτυξη στις εφαρμογές και στις υπηρεσίες των ασύρματων τηλεπικοινωνιακών δικτύων, πρέπει πρώτα να εξασφαλίσουν κοινά αποδεκτές τεχνικές προδιαγραφές – ένα κοινό πλαίσιο και ταυτόχρονα να παρέχεται και η δυνατότητα πρόσβασης στο Διαδίκτυο. Το WAP είναι αποδεκτό ως ένα αρχικό πρότυπο για πρόσβαση στο Διαδίκτυο, άλλωστε πολλοί αναφέρονται σε αυτό σαν το Internet του κινητού τηλεφώνου.

Επηρεαζόμενο από το διαδίκτυο λοιπόν, το WAP είναι ένα μοντέλο μετάδοσης δεδομένων στηριζόμενο στην ανταλλαγή μηνυμάτων Πελάτη(Client) –

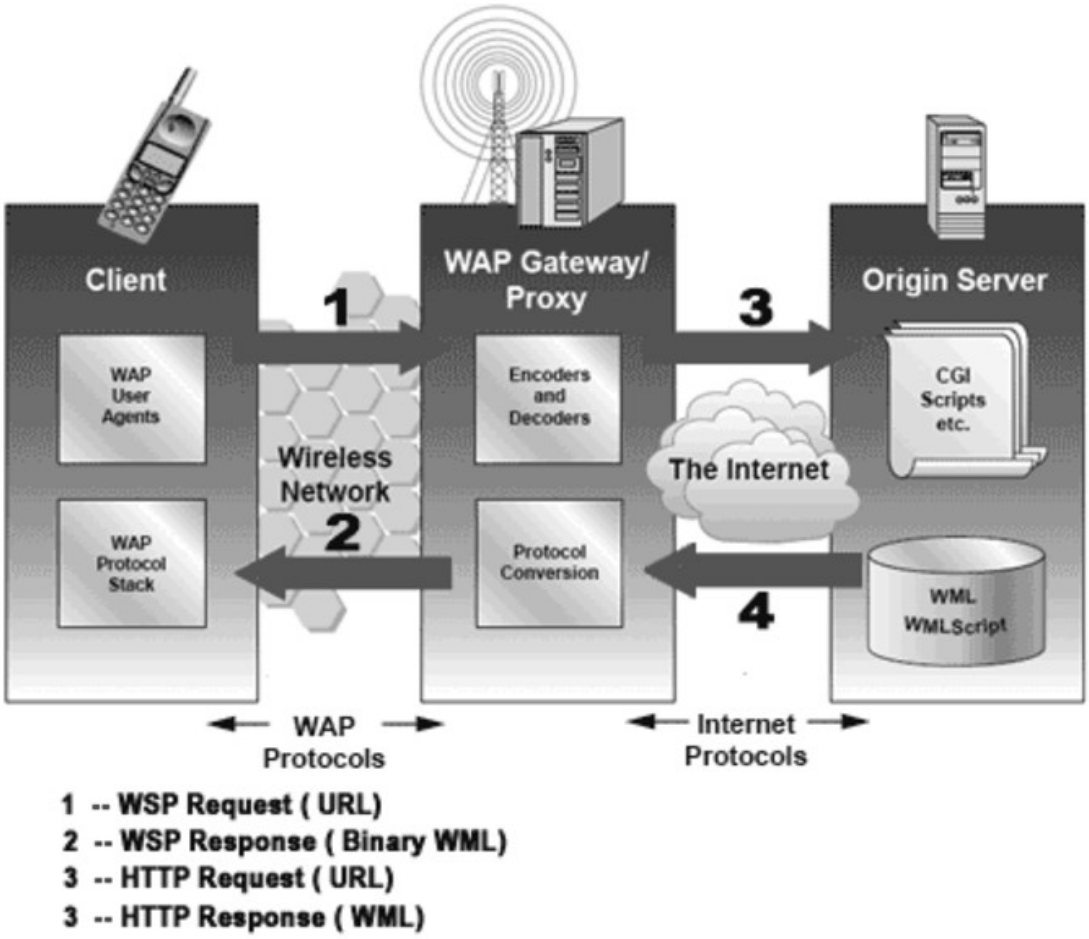
Διακομιστή(Server). Ο πελάτης αιτείται κάτι από τον διακομιστή και αυτός κάνει τις ανάλογες κινήσεις. Για να είναι εφικτή αυτή η επικοινωνία μεταξύ των δύο χρειάζεται μια WAP Proxy (Πύλη WAP) που στην ουσία είναι ο ενδιάμεσος μεταφραστής. Η WAP Proxy επικοινωνεί με το κινητό σταθμό (MS) κάνοντας χρήση των πρωτοκόλλων WAP ενώ αντίθετα με τον διακομιστή κάνει χρήση των πρωτοκόλλων του Internet. Παρακάτω βλέπουμε τα πρωτόκολλα WAP και Internet.



Επίπεδα	Περιγραφή
Application Layer (Εφαρμογής) Wireless Application Environment (WAE)	Περιβάλλον ανάπτυξης κινητών υπηρεσιών. HTML και η WML script (Wireless Mark-up Language) βρίσκονται σε αυτό το επίπεδο.
Session Layer (Συνόδου) Wireless Session Protocol (WSP)	Παρέχει μεθόδους ανταλλαγής περιεχομένων μεταξύ των server ασύρματων συσκευών και εφαρμογών. Η σχέση των ασύρματων συσκευών με το δίκτυο είναι σχέση πελάτη/εξυπηρετητή
Transaction Layer (Συναλλαγών) Wireless Transaction Protocol (WTP)	Παρέχει υποστήριξη για πολλούς τύπους συναλλαγών. Η αξιοπιστία εξαρτάται από τον τύπο της συναλλαγής.
Security Layer (Ασφάλειας) Wireless Transport Layer Security (WTLS)	Διασφαλίζει τα επίπεδα μυστικότητας και πιστοποίησης του χρήστη αλλά και την ασφάλεια της σύνδεσης μέσω του ελέγχου ακεραιότητας των δεδομένων.
Transport Layer (Μεταφοράς) Wireless Transport Layer (WTL)	Είναι το περιβάλλον διεπαφής μεταξύ των ανώτερων στρωμάτων και του στρώματος δικτύου. Είναι υπεύθυνο για τον εντοπισμό και την διόρθωση λαθών κατά την επικοινωνία χρησιμοποιώντας το WDP (Wireless Datagram Protocol)
Network Layer	Αναφέρεται στην φυσική διασύνδεση μεταξύ του δικτύου και των ασύρματων συσκευών.

4.Πρωτόκολλα WAP

Για να κατανοήσουμε καλυτέρα το WAP ακολουθεί μια απλή έκδοση του Client-Server για να δούμε την αρχιτεκτονική του.



5.Αρχιτεκτονική WAP

- **Mobile Station (MS)** : Είναι το πιο βασικό στοιχείο καθώς πρόκειται για το ασύρματο τερματικό που λαμβάνει και στέλνει δεδομένα μέσω προγράμματος περιήγησης (WAP Browser) και έτσι ο χρήστης αποκτά πρόσβαση στις υπηρεσίες.

- **Wap Gateway / Proxy** : Λειτουργεί ως μεσάζοντας μεταξύ κινητού τηλεφώνου και Τραπεζικού διακομιστή. Δουλειά του είναι να μετατρέπει τις αιτήσεις από τα πρωτόκολλα WAP (WSP,WTP,WTLS,WDP) σε αυτά του WWW (HTTP,SSL/TLS και TCP/IP) ώστε να επικοινωνεί με τους web servers της Τράπεζας και αντίστροφα.

- **WAP Server (Origin Server)** : Είναι ο διακομιστής, εδώ η Τράπεζα που στέλνει ή λαμβάνει δεδομένα και κατά αυτό τον τρόπο χειρίζεται τα αιτήματα του πελάτη (Client).

Πώς όμως γίνεται μια συναλλαγή μέσω WAP ;

1) Ο χρήστης συνδέεται στον WAP Browser στην συσκευή του, εισάγει την διεύθυνση URL του εξυπηρετητή (WAP Server) και επιλέγει την υπηρεσία που θέλει.
2) Στην συνέχεια η πύλη WAP (WAP Proxy) μεταφράζει το αίτημα WAP σε HTTP αίτημα και το διακινεί προς τον Server της Τράπεζας.
3) Αφού επεξεργαστεί το αίτημα ο Server της Τράπεζας αποστέλλει την ανάλογη απάντηση πάλι μέσω WAP Gateway. Τώρα η πύλη WAP μετατρέπει το μήνυμα που έλαβε, από HTML/XML σε WML (Wireless Markup Language) για να μπορεί να διαβαστεί από τον WAP Browser.
4) Το αποτέλεσμα εμφανίζεται στην οθόνη του χρήστη.

3. IVR Banking

Πρόκειται για μια καινοτόμο τεχνολογία που αφορά φωνητικές εντολές μέσω τηλεφώνου. Το IVR (Interactive Voice Response) αποτελεί μια υπηρεσία που επιτρέπει στον πελάτη να πλοηγείτε στο σύστημα μια Τράπεζας μέσω φωνητικών οδηγιών ή πατώντας πλήκτρα στο τηλέφωνό του. Για να το πετύχει αυτό γίνεται χρήση της τεχνολογίας TTS (Text to Speech). Η επικοινωνία με ένα σύστημα IVR γίνεται με 2 τρόπους :

α) Σήματα DTMF (Dual Tone Multi – Frequency)

β) Αναγνώριση φωνής του πελάτη

α) Τα DTMF αφορούν τον τόνο-ήχο που “βγάζουν” τα πλήκτρα ενός τηλεφώνου. Κάθε πλήκτρο του τηλεφώνου αντιστοιχεί σε έναν μοναδικό συνδυασμό δύο συχνοτήτων. Πατάς το πλήκτρο και το τηλέφωνο στέλνει τα σήματα αυτά μέσω του μικροφώνου.

Η διαδικασία ξεκινάει με την κλήση σε έναν αριθμό DNIS (Dialed Number Information Service), ακούς το ηχογραφημένο μήνυμα και στη συνέχεια ακολουθώντας

τις οδηγίες επιλέγεις κάποια υπηρεσία με το πάτημα κουμπιών στο πληκτρολόγιο. Μετά η συσκευή-δέκτης (πχ τηλεφωνικό κέντρο) αναλύει τις συχνότητες και μπορεί να προσδιορίσει ποιο πλήκτρο πατήθηκε και να προβεί στην αντίστοιχη ενέργεια. Τα σήματα αυτά είναι γνωστά και σαν Touch Tones.

β) Ο δεύτερος τρόπος λειτουργεί με τον ίδιο τρόπο με μόνη διαφορά ότι ο χρήστης πλοηγείτε στο μενού χρησιμοποιώντας την φωνή του. Εδώ έχουμε 4 ειδών συστήματα

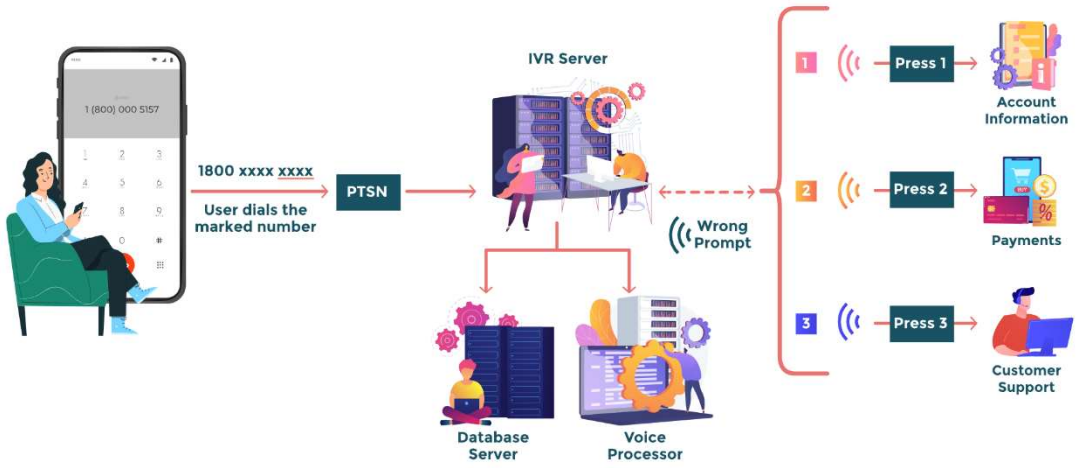
- Speaker – Dependent : σε αυτά πρέπει να "εκπαιδεύσει" κάποιος τον υπολογιστή. Αυτό είναι μια χρονοβόρα διαδικασία καθώς πρέπει να διαβάσει μερικές προτάσεις ή να απαντήσει σε κάποιες ερωτήσεις ώστε να κατανοήσει ο υπολογιστής τον μοναδικό ήχο της φωνής του.
- Speaker – Independent : εδώ ο εξυπηρετητής εκπαιδεύεται από τους ίδιους τους χρήστες οπότε μιλάμε για ένα σύστημα που εξελίσσεται μόνο του.
- Σύστημα συνεχούς ροής φωνής : το σύστημα αντιλαμβάνεται την ομιλία κανονικά ακόμα και με παύσεις.
- Σύστημα μη συνεχούς ροής φωνής : ο χρήστης πρέπει να κάνει παύσεις σε κάθε λέξη για να αντιληφθεί το σύστημα τί είπε.

Το IVR Banking ξεκινά με την πραγματοποίηση κλήσης του πελάτη στον ειδικό αριθμό IVR της Τράπεζας. Έπειτα, γίνεται η ταυτοποίηση του χρήστη (πχ κωδικός PIN) και αφού ολοκληρωθεί αυτό το κομμάτι προχωράει στο μενού επιλογών των υπηρεσιών.

Ο χρήστης παρέχει δεδομένα στην Πύλη φωνής (Voice Gateway) χρησιμοποιώντας φωνητικές εντολές ή το πληκτρολόγιο. Η πύλη επεξεργάζεται τα δεδομένα αυτά τα αποστέλλει στον Server της Τράπεζας για να προβεί στις αντίστοιχες ενέργειες του αιτήματος. Τέλος, ο πελάτης λαμβάνει επιβεβαίωση με φωνητικό μήνυμα, συχνά με ένα αναγνωριστικό και η κλήση ολοκληρώνεται.

Μιλάμε για το πιο παλιό σύστημα τηλεφωνικής Τραπεζικής καθώς η πρόσβαση σε αυτό γινόταν και με σταθερά τηλέφωνα.

Ακολουθεί εικόνα με την αρχιτεκτονική και τα δομικά στοιχεία της υπηρεσίας :



6.Αρχιτεκτονική IVR

4. M-Banking με SMAC

Standalone Mobile Application Clients : εφαρμογές που αφού εγκατασταθούν στην κινητή συσκευή λειτουργούν αυτόνομα. Δεν χρειάζεται να είναι συνέχει συνδεδεμένες με κάποιον διακομιστή (Server) για τις πιο βασικές λειτουργίες τους αλλά παρόλαυτα απαιτείται να έχουν συχνά επικοινωνία με κάποιον server για την σωστή ενημέρωση των δεδομένων ή την διεκπεραίωση συναλλαγών. Αυτά τα Apps σχεδιάζονται με σκοπό την εκτέλεση πολύπλοκων λειτουργιών και προσαρμόζονται στην ανάλογη πολυπλοκότητα της συσκευής στην οποία εγκαθίστανται.

Η κύρια λοιπόν απαίτηση αυτών των εφαρμογών είναι ότι πρέπει να ληφθούν στη συσκευή του χρήστη, κάτι που σημαίνει ότι η συσκευή πρέπει να υποστηρίζει περιβάλλοντα ανάπτυξης όπως το J2ME ή το BREW. Το J2ME απαιτεί να υποστηρίζει JaVa η εφαρμογή. Η “δουλειά” του J2ME είναι να συνδέει τις API (Application Programming Interface) για τα κινητά με παρόμοια λειτουργικότητα μέσω των λεγόμενων “profiles”. Όμως καθώς η τεχνολογία προοδεύει, αυξάνεται και ο αριθμός των “profiles” καθώς αναπτύσσονται συσκευές με διαφορετικές λειτουργικότητες. Συνέπεια αυτού, είναι η αύξηση του κόστους για να καλυφθούν όλα αυτά τα προφίλ. Για να κατανοήσει κάποιος το μέγεθος του προβλήματος, αρκεί να ειπωθεί ότι οι εταιρείες που υλοποιούν κινητές εφαρμογές μπορεί να φτάσουν να χρησιμοποιούν το 50% των πόρων και του χρόνου τους μόνο για να προσαρμόσουν τις εφαρμογές τους στα διαφορετικά αυτά προφίλ τα οποία αντιστοιχούν σε διαφορετικές δυνατότητες και χαρακτηριστικά συσκευών. Έτσι η ομάδα ανάπτυξης σπαταλάει το χρόνο της για να

διασφαλίσει ότι η εφαρμογή θα λειτουργεί ομαλά σε μια μεγάλη γκάμα συσκευών, αντί να επικεντρωθεί στην προσθήκη νέων λειτουργιών. (Java 2 Micro Edition (J2ME) Developer's Guide. Hardcover – Import, March 31, 2003 by Michael Kroll (Author))

Αρκετές εταιρείες παραγωγής λογισμικού για κινητές συσκευές έχουν κυκλοφορήσει λύσεις που επιτρέπουν τραπεζικές υπηρεσίες με χρήση εφαρμογών J2ME. Παράδειγμα αποτελεί το Wireless I-banco. Ο "πελάτης" J2ME συνδέεται στον server του Wireless I-banco μέσω του δικτύου GSM (Global System for Mobile Communications) και δίνει έτσι πρόσβαση στο χρήστη σε τραπεζικές υπηρεσίες όπως πληροφορίες για το λογαριασμό του ή την εκτέλεση μιας συναλλαγής.

Γενικά οι SMAC εφαρμογές είναι ιδιαίτερα χρήσιμες σε προηγμένες αγορές με τεχνολογικά εξελιγμένες συσκευές, ενώ σε χώρες όπως η Ινδία που θεωρείται μια όχι και τόσο αναπτυσσόμενη χώρα, υπάρχει ο περιορισμός στον αριθμό των συμβατών συσκευών που μπορεί να αποτελέσει μεγάλο εμπόδιο.

Κεφάλαιο 4

«Mobile Banking και Ασφάλεια»

4.1 Το Περιβάλλον Ασφάλειας

Η ασφάλεια του Mobile Banking είναι και θα είναι μια από τις μεγαλύτερες προκλήσεις και ανησυχίες καθώς καλύπτει την προστασία των συναλλαγών, τα προσωπικά δεδομένα των πελατών και γενικά τις τραπεζικές πληροφορίες και της εμπιστευτικότητας αυτών. Η ανάγκη για μια ολοκληρωμένη στρατηγική ασφαλείας κάθε μέρα γίνεται μεγαλύτερη καθώς το M-Banking είναι πλέον αναπόσπαστο κομμάτι της καθημερινότητάς μας.

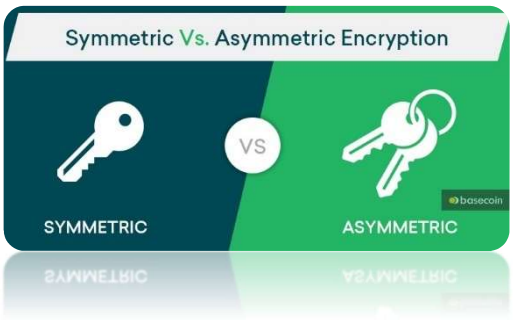
Το περιβάλλον ασφάλειας του Mobile Banking έχει στη διάθεσή του διάφορα τεχνολογικά και οργανωτικά μέτρα σχεδιασμένα για την αποτροπή απειλών όπως είναι η κλοπή δεδομένων, οι κυβερνοεπιθέσεις και οι απάτες (Scheau et al.,2022). Ένα περιβάλλον ασφαλείας πρέπει να κερδίσει την εμπιστοσύνη των πελατών εξασφαλίζοντάς τους μια ασφαλή "συνεργασία" με το εκάστοτε Τραπεζικό Ίδρυμα. Αν μπορούσαμε να απαριθμήσουμε τις βασικές απαιτήσεις ασφαλείας ενός χρήστη αλλά και της ίδιας της Τράπεζας θα ήταν οι εξής :

1. ***Απόρρητο = Εμπιστοσύνη*** : Επεξεργασία δεδομένων των πελατών μόνο από εγκεκριμένους χρήστες. Εδώ έχουμε πχ την κρυπτογράφηση που κάνει χρήση σύγχρονων πρωτοκόλλων όπως το TLS και έτσι προστατεύεται η επικοινωνία εφαρμογής και διακομιστή.
2. ***Ακεραιότητα των συναλλαγών*** : Διασφάλιση ότι δεν θα υπάρξει κάποια μη εξουσιοδοτημένη (ή κακόβουλη) μεταβολή ή αλλοίωση των δεδομένων κατά τη διάρκεια μιας συναλλαγής. Τακτικοί έλεγχοι για rooting ή jailbreaking στις κινητές συσκευές αλλά και τεχνολογίες όπως το Trusted Execution Environment (TEE) βοηθούν για την αντιμετώπιση/πρόληψη του φαινομένου αυτού.
3. ***Πιστοποίηση και Αυθεντικοποίηση Χρήστη*** : Οι ταυτότητες των συναλλασσόμενων μερών πρέπει να επιβεβαιώνονται και επαληθεύονται. Εφαρμογή μεθόδων ισχυρής πιστοποίησης όπως η Διπλή Αυθεντικοποίηση (2FA) με PIN ή χρήση βιομετρικών στοιχείων (όπως αναγνώριση προσώπου ή

δακτυλικού αποτυπώματος), συμβάλλει στην προστασία από μία μη εξουσιοδοτημένη πρόσβαση.

4.2 Κρυπτογράφηση

Όταν μιλάμε για εμπιστευτικότητα και ακεραιότητα δεδομένων οδηγούμαστε στην κρυπτογράφηση · την θεμελειώδη τεχνολογία που διασφαλίζει τα παραπάνω. Η διαδικασία της κρυπτογράφησης είναι η μετατροπή των δεδομένων, με χρήση αλγορίθμων, σε μια μορφή που δεν μπορεί να διαβαστεί από κάποιον που δεν έχει το "κλειδί" της αποκρυπτογράφησης. Υπάρχουν δύο είδη κρυπτογράφησης που χρησιμοποιούνται :



Α) Η συμμετρική

Β) Η ασύμμετρη

Α) Συμμετρική (Symmetric key encryption)

Στη συμμετρική κρυπτογράφηση έχουμε ένα "κοινό κλειδί" που χρησιμοποιείται τόσο στην κρυπτογράφηση, όσο και στην αποκρυπτογράφηση των δεδομένων.

Πλεονεκτήματα

1. Απλό και γρήγορο : Λιγότερο απαιτητική σε υπολογιστική ισχύ κάνοντάς την κατάλληλη για μεγάλα δεδομένα αφού είναι δομημένη πάνω σε απλές μαθηματικές σχέσεις.
2. Χρήση σε σταθερές συνδέσεις : Ιδανική για ασφαλείς συνδέσεις όπως η αποθήκευση δεδομένων στη συσκευή του χρήστη.

Μειονεκτήματα

1. "Το κοινό κλειδί" : Οι συμμετέχοντες στην συναλλαγή πρέπει να έχουν το ίδιο κλειδί με αποτέλεσμα να αυξάνεται ο κίνδυνος παραβίασης.
2. Η διάθεση-διανομή του κλειδιού : Η ασφάλεια της διανομής του κλειδιού είναι απόλυτα σημαντική και μπορεί να αποτελέσει σημείο αδυναμίας.

Παραδείγματα τέτοιων αλγορίθμων :

AES (Advanced Encryption Standard)

DES (Data Encryption Standard)

Β) Ασύμμετρη (Asymmetric key encryption)

Η ασύμμετρη κρυπτογράφηση βασίζεται σε δύο κλειδιά

- Δημόσιο κλειδί (για κρυπτογράφηση)
- Ιδιωτικό κλειδί (για αποκρυπτογράφηση)

Πλεονεκτήματα

1. Ασφαλής Διανομή : αφού το δημόσιο κλειδί δεν απαιτεί κρυπτογράφηση
2. Εύκολο στην επικοινωνία : ειδικά στο M-Banking όπου πολλοί χρήστες αλληλοεπιδρούν με τον διακομιστή

Μειονεκτήματα

1. Πολύπλοκη και Αργή : πιο απαιτητική σε πόρους σε σύγκριση με την συμμετρική
2. Εφαρμόζεται σε μικρά δεδομένα : η πολυπλοκότητά της έχει ως αποτέλεσμα να χρησιμοποιείται κυρίως για μικρές ποσότητες δεδομένων

Παραδείγματα

RSA (Rivest – Shamir – Adleman)

ECC (Elliptic Curve Cryptography)

Στο Mobile Banking ***τα δύο αυτά είδη συνδυάζονται***.

Πως ; -> Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται για την ασφαλή διανομή ενός συμμετρικού κλειδιού και έπειτα γίνεται χρήση συμμετρικής κρυπτογράφησης για να εξασφαλιστεί γρήγορη και ασφαλή επικοινωνία Τράπεζας με πελάτη.

4.3 Ψηφιακά Πιστοποιητικά

Σε συνέχεια λοιπόν, της κρυπτογράφησης δημοσίου κλειδιού έχουμε ότι για να λειτουργήσει σωστά πρέπει να παράγουμε ένα δημόσιο και ένα ιδιωτικό κλειδί. Ποιος όμως είναι αυτός που κατέχει το ιδιωτικό κλειδί ;

Σε αυτό το σημείο έρχονται τα *Ψηφιακά Πιστοποιητικά*.

Πρόκειται για ηλεκτρονικά έγγραφα που :

α) Πιστοποιούν την ταυτότητα της οντότητας / Τραπεζικού Ιδρύματος.

β) Συσχετίζουν την ταυτότητα αυτή με ένα ζεύγος κλειδιών δημόσιο και ιδιωτικό.

γ) Τέλος τα Πιστοποιητικά αυτά υπογράφονται από μία αξιόπιστη Τρίτη οντότητα, την Αρχή Πιστοποίησης (Certificate Authority, CA). Η CA εκδίδει τα ψηφιακά πιστοποιητικά υπογεγραμμένα με το ιδιωτικό κλειδί της στα οποία εμπεριέχουν το δημόσιο κλειδί και το όνομα κάποιας οντότητας.

Ένα τυπικό ψηφιακό πιστοποιητικό περιλαμβάνει λοιπόν με βάση τα παραπάνω :

1) Το όνομα της οντότητας
2) Το δημόσιο κλειδί της οντότητας
3) Το όνομα της Αρχής Πιστοποίησης που το εξέδωσε
4) Ημερομηνίες έναρξης και λήξης ισχύος
5) Την ψηφιακή υπογραφή της CA

Ας δούμε αναλυτικά τη διαδικασία για να κατανοήσουμε πως λειτουργεί :

- ✓ Η οντότητα/Τραπεζικό Ίδρυμα δημιουργεί ένα ιδιωτικό κλειδί και ένα δημόσιο.

- ✓ "Κρατάει" το ιδιωτικό για αυτήν και το δημόσιο + πληροφορίες για την ταυτότητά της το δίνει σε μια Αρχή Έκδοσης Πιστοποιητικών.

- ✓ Η CA ανάλογα με τον τύπο του πιστοποιητικού προβαίνει στις αντίστοιχες μεθόδους για να επαληθεύσει την ταυτότητα της οντότητας.

- ✓ Στη συνέχεια φτιάχνει το Ψηφιακό Πιστοποιητικό το οποίο εμπεριέχει την ταυτότητα και το δημόσιο κλειδί της οντότητας.

- ✓ Τέλος, μπαίνει η υπογραφή της CA κάνοντας χρήση του δικού της ιδιωτικού κλειδιού.

- ✓ Το πλέον, γνήσιο πιστοποιητικό **"γυρίζει"** στην οντότητα και αρχίζει να το διανέμει κανονικά.

Πλεονεκτήματα

- Υψηλό επίπεδο ασφάλειας : Απειλές όπως το phising και το man-in-the-middle attack ελαχιστοποιούνται.
- Απλότητα : Ενσωματώνονται σε όλες τις εφαρμογές, οπότε ο χρήστης δεν χρειάζεται να προβεί σε κάποια πολύπλοκη διαδικασία.

Προβληματισμοί – Περιορισμοί

- Εξάρτηση από την αξιοπιστία της CA. Υπάρχουν και CA οι οποίες δρουν "αντίθετα" δημιουργώντας δόλια πιστοποιητικά θέτοντας σε κίνδυνο όλο το σύστημα.
- Το ιδιωτικό κλειδί πρέπει να διατηρείται μυστικό, καθώς το πιστοποιητικό, όπως είπαμε βασίζεται στο ζεύγος δημοσίου-ιδιωτικού κλειδιού.

Ψηφιακά Πιστοποιητικά στο Mobile Banking

- SSL/TLS Certificates : Διασφαλίζουν την ασφαλή επικοινωνία χρήστη-διακομιστή του Τραπεζικού Ιδρύματος μέσω της τεχνολογίας HTTPS.
- Client Certificates : Αφορούν την πιστοποίηση του χρήστη δίνοντας ένα υψηλό επίπεδο αυθεντικοποίησης.
- Code Signing Certificates : Παρέχουν εγγύηση ότι η εκάστοτε Mobile Banking App είναι γνήσια χωρίς να ενέχει κίνδυνο ο πελάτης από κάποιο κακόβουλο λογισμικό.

4.4 Διασφάλιση της ακεραιότητας των συναλλαγών και Ψηφιακή Υπογραφή

Η διασφάλιση της ακεραιότητας των συναλλαγών αποτελεί κομμάτι ζωτικής σημασίας για την προστασία των συναλλασσόμενων από τυχόν αλλοιώσεις στα δεδομένα που ανταλλάσσονται ή ακόμα και υποκλοπής προσωπικών δεδομένων. Για αυτό το λόγο οι Τράπεζες θα πρέπει να είναι 100% σίγουρες ότι όλες οι εντολές που λαμβάνουν ή δίνουν προέρχονται από τον εκάστοτε πελάτη και δεν έχουν παραποιηθεί στο "δρόμο".

Πώς όμως το πετυχαίνουν αυτό οι Τράπεζες ;

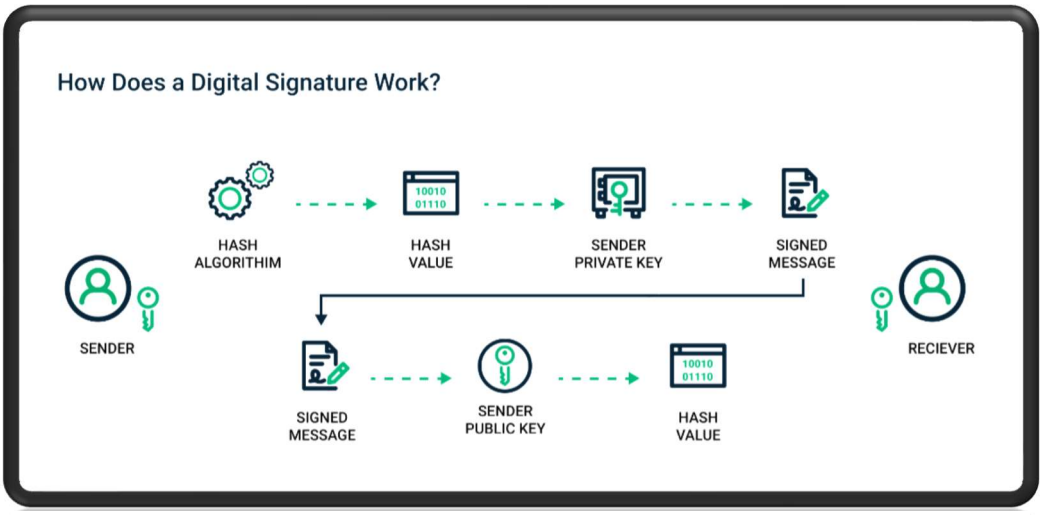
Σε αυτό λοιπόν, έρχεται να βοηθήσει η ***Ψηφιακή Υπογραφή***, η οποία καλύπτει :

α) Την Αυθεντικότητα : Το μήνυμα προέρχεται από τον "σωστό" αποστολέα.

β) Την Ακεραιότητα : Η παραμικρή τροποποίηση μηνύματος καθιστά άκυρη την υπογραφή και έτσι εκμηδενίζεται οποιαδήποτε κακόβουλη προσπάθεια παραποίησης.

γ) Μη-Αποποίηση Ευθύνης : Η υπογραφή αυτή συνδέεται με το ιδιωτικό κλειδί του χρήστη, όπως θα αναφέρουμε και παρακάτω, οπότε ο αποστολέας δεν μπορεί να αρνηθεί ότι υπέγραψε την εντολή.

Στη λειτουργία αυτού του συστήματος γίνεται χρήση ασύμμετρης κρυπτογράφησης.



7.Πώς λειτουργεί η Ψηφιακή Υπογραφή (Πηγή : www.investopedia.com)

- Ο χρήστης δημιουργεί τη συναλλαγή ή το μήνυμα που επιθυμεί με τις λεπτομέρειες.
- Το μήνυμα αυτό περνά μέσα από έναν αλγόριθμο Hash (πχ SHA-256) και παράγει ένα μοναδικό "αποτύπωμα" δεδομένων γνωστό ως Hash Value
- Το Hash Value κάνοντας χρήση του ιδιωτικού κλειδιού του αποστολέα κρυπτογραφείται δημιουργώντας έτσι την ψηφιακή υπογραφή.
- Έτσι η ψηφιακή υπογραφή επισυνάπτεται στο μήνυμα και αποστέλλεται στην Τράπεζα.
- Τέλος, η Τράπεζα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα αποκρυπτογραφεί την υπογραφή και υπολογίζει το Hash Value που έλαβε. Αν το Hash Value που υπολόγισε ισούται με το αποκρυπτογραφημένο Hash της υπογραφής τότε το μήνυμα είναι "ΑΥΘΕΝΤΙΚΟ".

4.5 Πρωτόκολλα SSL/TLS και SET

Η Ασφάλεια του Mobile Banking στηρίζεται σε διάφορα πρωτόκολλα για να λειτουργήσει ορθά. Τα δύο βασικά εξ αυτών που διασφαλίζουν τις ασφαλείς Ηλεκτρονικές συναλλαγές είναι :

- SSL/TLS (Secure Locket Layer / Transport Layer Security
- SET (Secure Electronic Transactions)

4.5.1. SSL/TLS Ανάλυση – Περιγραφή

Το SSL είναι από τα πιο διαδεδομένα πρωτόκολλα ασφαλείας για την δημιουργία ασφαλής σύνδεσης μεταξύ mobile app-server. Χρησιμοποιείται επί το πλείστων από τα Εικονικά Ιδιωτικά Δίκτυα (VPN) και παρέχει στους χρήστε πρόσβαση σε εφαρμογές όπως HTTP, client/server ή File Sharing.

Ο Taher Elgamal γνωστός ως ο "πατέρας του SSL" ηγήθηκε της ανάπτυξης αυτού του πρωτοκόλλου και το 1995 δημοσιοποίησε το SSL 2.0 και μια χρονιά αργότερα είχαμε το SSL 3.0. Από το 1996 και έπειτα δεν υπήρξε αναβάθμιση οπότε πλέον θεωρείται ξεπερασμένο. Σε αυτό το σημείο, έρχονται οι Tim Dierks και Christopher Allen το 1999 να δημιουργήσουν τον διάδοχο του SSL 3.0 -> το TLS 1.0. Κατ' ουσίαν τα δύο αυτά πρωτόκολλα δεν έχουν κάποια διαφορά στην λειτουργία, απλά το TLS καλύπτει κάποια "μικροπροβλήματα" και αδυναμίες του SSL. Παρόλαυτα, πολύς κόσμος ακόμα αναφέρεται στο TLS σαν SSL λόγω της αναγνωρισημότητας του τελευταίου ή γενικά πρωτόκολλα SSL/TLS σαν να είναι το ίδιο.

Για να κατανοήσουμε πως γίνεται μια σύνδεση SSL ακολουθεί μια σύντομη περιγραφή της διαδικασίας :

HANDSHAKE	❖ Όλα ξεκινάνε με την χειραψία (Handshake). Ο πελάτης της (client) στέλνει στον server ένα αίτημα, την έκδοση SSL που χρησιμοποιεί καθώς και την προτίμησή του για τον αλγόριθμο της κρυπτογράφησης – πληροφορίες αναγκαίες για τον server ώστε να ξεκινήσει η σύνδεση. ❖ Ο server απαντά παρέχοντας τις αντίστοιχες πληροφορίες μαζί με το ψηφιακό πιστοποιητικό του.

ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ	❖ Με την βοήθεια μιας Αρχής Πιστοποίησης (CA) επαληθεύεται το πιστοποιητικό του server από το εκάστοτε Mobile App. Αν δεν ολοκληρωθεί η πιστοποίηση εμφανίζεται μήνυμα σφάλματος και διακόπτεται η σύνδεση.
ΚΡΥΠΤΟΓΡΑΦΗΣΗ	❖ Εφόσον ολοκληρωθούν τα προηγούμενα, έχουμε την καθιέρωση ενός συμμετρικού κλειδιού για την κρυπτογράφηση της επικοινωνίας. Με χρήση ασύμμετρης κρυπτογράφησης το κλειδί αυτό ανταλλάσσεται κατά τη διάρκεια της "χειραψίας". ❖ Ο client με το δημόσιο κλειδί του server, κρυπτογραφεί το συμμετρικό κλειδί και του το στέλνει με ασφάλεια.
ΑΣΦΑΛΗΣ ΕΠΙΚΟΙΝΩΝΙΑ	❖ Ολοκλήρωση σύνδεσης SSL ❖ Πλέον έχουμε επικοινωνία κρυπτογραφημένη και προστατευμένη από απειλές.

1 Συμβολή του συγγραφέα (Διαδικασία σύνδεσης SSl)

4.5.2. SSL/TLS Εφαρμογές

- ***Ασφαλείς Ιστοσελίδες (HTTPS)***

Πρόκειται για την πιο κοινή εφαρμογή του πρωτοκόλλου SSL/TLS, η οποία είναι να παρέχει ασφάλεια στις ιστοσελίδες μέσω του HTTPS (Hyper Text Transfer Protocol Secure). Αυτό που κάνει στην ουσία είναι να διατηρεί μια κρυπτογραφημένη σύνδεση για την επικοινωνία των Browsers και Servers του ιστού.

Παραδείγματα αποτελούν το e-Banking, Paypal αλλά και διάσημες εμπορικές πλατφόρμες όπως η Amazon.

- ***Email Clients και Servers***

Χρησιμοποιείται για τη διασφάλιση ασφαλής αποστολής και λήψης μηνυμάτων στα email πελατών-διακομιστών με πρωτόκολλα όπως SMTP,IMAP και POP3.

Παραδείγματα αποτελούν το Gmail και το Outlook.

- ***VPN (Virtual Private Network)***

Ασφαλή μεταφορά δεδομένων μέσω δημοσίων ή μη αξιόπιστων δικτύων.

Παράδειγμα είναι η χρήση για να παρακαμφθεί ο γεωγραφικός περιορισμός για κάποιο συγκεκριμένο περιεχόμενο.

- ***Mobile Banking – Διάφορες Οικονομικές Εφαρμογές***

Και εδώ πάλι το SSL/TLS προστατεύει τα Apps από διάφορες "επιθέσεις".

Παραδείγματα είναι τα App και των Ελληνικών Τραπεζών .

- ***Ηλεκτρονικό εμπόριο (e-Commerce)***

Αναφέρεται στις πληρωμές μέσω πιστωτικών καρτών, διατηρώντας την ακεραιότητα των δεδομένων των τελευταίων.

Παράδειγμα αποτελούν τα συστήματα πληρωμών Visa και Mastercard.

4.5.3. SSL/TLS Μηχανισμοί Ασφάλειας

Έχοντας αναφερθεί στην λέξη "ΑΣΦΑΛΕΙΑ" αρκετές φορές στο προηγούμενο κομμάτι ας μιλήσουμε εν συντομία για το πως αυτή επιτυγχάνεται και με ποιους τρόπους. Το πρωτόκολλο SSL/TLS λοιπόν, παρέχει ασφάλεια σύνδεσης TCP/IP (Transmission Control Protocol / Internet Protocol). Αυτό το πετυχαίνει :

1. Με κρυπτογράφηση : Ισχυροί αλγόριθμοι όπως AES (Advanced Encryption Standard) και RSA συμβάλλουν στην ενίσχυση της εμπιστευτικότητας της επικοινωνίας.
2. Με αυθεντικοποίηση : Πιστοποιητικά SSL/TLS εξασφαλίζουν την αυθεντικότητα της ταυτότητας του server.
3. Με ακεραιότητα : Επιβεβαιώνει ότι τα δεδομένα δεν έχουν τροποποιηθεί κατά την μεταφορά, χρησιμοποιώντας MACs (Message Authentication Codes).
4. Με την χειραψία : Η οποία δημιουργεί στην ουσία τις συνθήκες για την όλη επικοινωνία αφού συμπεριλαμβάνει πιστοποιητικά και συμμετρικά κλειδιά και όλα αυτά μέσω ασύμμετρης κρυπτογράφησης.

4.5.4. SSL/TLS Αντοχή σε επιθέσεις

Το πρωτόκολλο SSL/TLS είναι μια αρκετά ισχυρή λύση όσον αφορά την ασφάλεια των εφαρμογών του M-Banking. Παρόλο όμως την ανθεκτικότητά του έχουμε κατά καιρούς ορισμένες επιθέσεις όπως :

1) Dictionary Attack (Επίθεση Λεξικού)

Πρόκειται για μια από τις πιο επικίνδυνες επιθέσεις για εφαρμογές του Διαδικτύου καθώς πολλά μηνύματα περιέχουν αρκετά προβλέψιμα στοιχεία όπως πχ η εντολή HTTP Get. Η ιδανική συνθήκη για να πετύχει αυτή η επίθεση είναι να χρησιμοποιούνται λίγα μυστικά κρυπτογραφικά κλειδιά. Με την δημιουργία ενός λεξικού το οποίο περιλαμβάνει κάθε πιθανή κρυπτογράφηση του "γνωστού" μηνύματος, οι επιτιθέμενοι μπορούν να προσδιορίσουν το σωστό μυστικό κλειδί κατόπιν μιας αντιστοιχίας που θα εντοπίσει το κρυπτογράφημά τους.

Το SSL/TLS μπορεί εύκολα να αντιμετωπίσει αυτή την κατάσταση χρησιμοποιώντας ένα κλειδί με 128 bits και όχι ένα απλό με 40 bits.

2) Replay Attack (Επίθεση Επανάληψης)

Σε αυτή την επίθεση, ο "κακόβουλος" χρήστης χρησιμοποιώντας τα ήδη υπάρχοντα μηνύματα μεταξύ client και server προσπαθεί να ξεγελάσει τον τελευταίο και να αποκτήσει πρόσβαση.

Εδώ το πρωτόκολλο SSL/TLS κατά τη διαδικασία της χειραψίας (Handshake) έχει δημιουργήσει ένα μοναδικό Nonce Value(τυχαίος αριθμός) μεγέθους 128 bits για κάθε συνεδρία και έτσι δεν γίνεται να αντιγραφεί και να επαναχρησιμοποιηθεί.

3) Man In The Middle

Όπως και σε απλή μετάφραση έχουμε τον ενδιάμεσο σε μια συζήτηση μεταξύ των client-server. Ο επιτιθέμενος τρίτος παρεμβαίνει στην επικοινωνία αυτών και προσποιείται τον έναν ή τον άλλον, προσπαθώντας να μπερδέψει τον εκάστοτε λήπτη με μηνύματα αυτού που προσποιείται.

Όπως ήδη αναφέραμε το SSL/TLS υποχρεώνει τον server να προβαίνει σε απόδειξη της ταυτότητάς του σε κάθε μήνυμα οπότε ο επιτιθέμενος "βαράει σε τοίχο".

4) Brute Force Attack

Οι επιθέσεις αυτές βασίζονται στη συστηματική δοκιμή όλων τον πιθανών συνδυασμών για την αποκρυπτογράφηση των μηνυμάτων.

Η χρήση ισχυρών αλγορίθμων που χρησιμοποιούν μεγάλα κλειδιά των 128 bits όπως ο AES-256 καθιστούν πρακτικά αδύνατη μια τέτοια επίθεση.

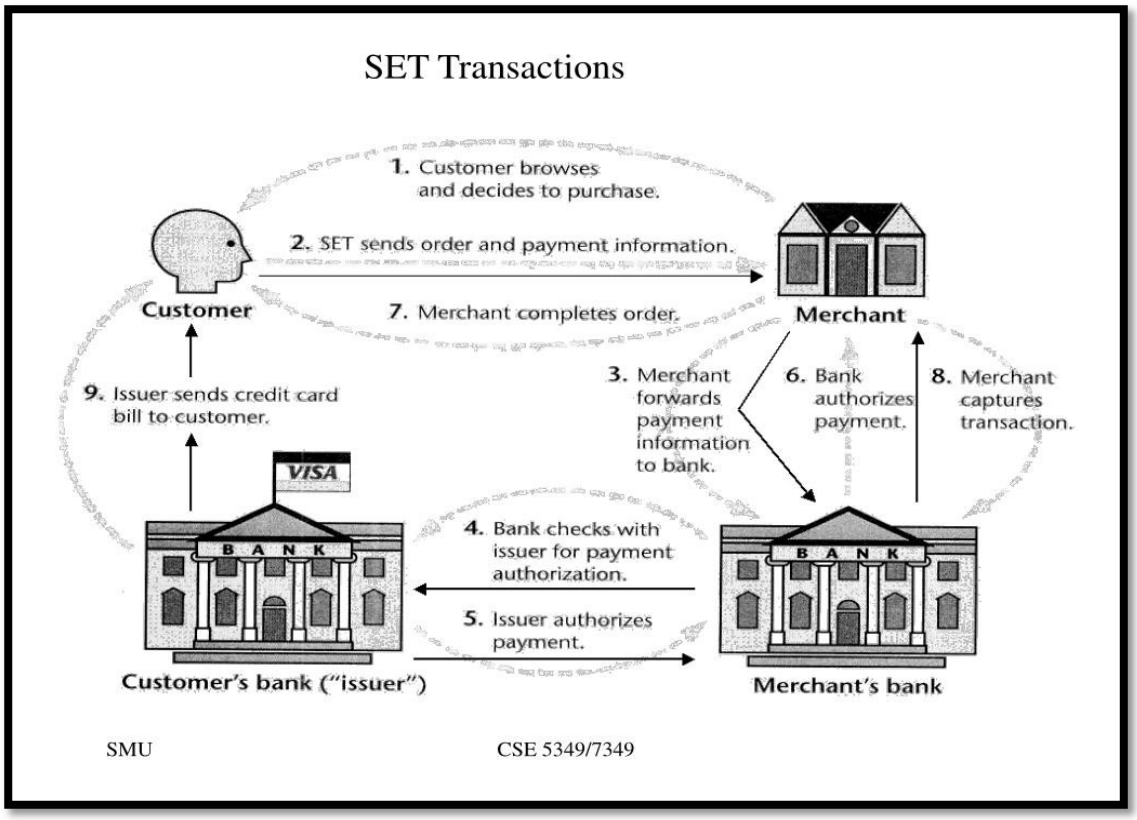
4.5.5. SET Ανάλυση – Περιγραφή

SET (Secure Electronic Transactions) : Πρωτόκολλο ασφαλείας σχεδιασμένο το 1990 από την Visa και Mastercard με στόχο την προστασία των ηλεκτρονικών συναλλαγών με πιστωτικές και χρεωστικές κάρτες. Εστιάζοντας στην διασφάλιση της εμπιστευτικότητας και της αυθεντικότητας των δεδομένων σε μια online πληρωμή δημιουργεί ένα ασφαλές περιβάλλον για τις συναλλαγές του ηλεκτρονικού εμπορίου (e-Commerce).

Για να κατανοήσουμε πως λειτουργεί ξεκινάμε με τα μέρη που εμπλέκονται σε μια τέτοια συναλλαγή :

- Κάτοχος Κάρτας (Card Holder) : Είναι ο εξουσιοδοτημένος κάτοχος της κάρτας πληρωμής και επιθυμεί να πραγματοποιήσει μια συναλλαγή με αυτήν.
- Έμπορος (Merchant) : Αυτός που παρέχει το προϊόν/υπηρεσία στον Card Holder.
- Τράπεζα Κατόχου Κάρτας (Issuer Bank) : Το χρηματοπιστωτικό ίδρυμα που επιβεβαιώνει την εγκυρότητα της κάρτας και εν τέλη εγκρίνει τη συναλλαγή.
- Τράπεζα Εμπόρου (Acquirer Bank) : Η Τράπεζα με την οποία “εμπλέκεται” ο έμπορος και διεκπεραιώνει τις πληρωμές.
- Πύλη πληρωμής (Payment GateWay) : Είναι ο διαμεσολαβητής μεταξύ SET και των δικτύων πληρωμών με κάρτα. Δουλειά του είναι να διασφαλίζει την ασφάλεια στην επικοινωνία πελάτη-εμπόρου.
- Αρχή Πιστοποίησης (Certification Authority) : Η οντότητα που παρέχει τα πιστοποιητικά που διασφαλίζουν την αυθεντικότητα όλων των μερών στη συναλλαγή SET.

Στην παρακάτω εικόνα βλέπουμε πως λειτουργούν αρμονικά τα εμπλεκόμενα μέρη σε μια τέτοιου είδους συναλλαγή.



8.Αρχιτεκτονική SET (Πηγή: Ahmed, A., Aziz, A. and Muneeb, M. (2019) 'Electronic payment system: A complete guide', Journal of Management Studies)

4.5.6. SET Εφαρμογές – Λειτουργίες

Εφαρμογές του SET

Το πρωτόκολλο SET έχει εφαρμογή σε :

1. Ηλεκτρονικές Αγορές (E-Commerce) : Γενικά εφαρμόζεται στα καταστήματα που υποστηρίζουν τις online πληρωμές μέσω πιστωτικών και χρεωστικών καρτών και παρέχει ασφάλεια.
2. Mobile Banking : Χρήση του στις συναλλαγές όπως πληρωμές λογαριασμών, μεταφορές χρημάτων και αγορές μέσω κινητού τηλεφώνου.
3. Υπηρεσίες Επιχειρήσεων – B2B Transactions : Παρέχει ασφαλή επικοινωνία και υποστήριξη σε εταιρείες που διεκπεραιώνουν πληρωμές μεταξύ επιχειρήσεων.
4. Εξασφάλιση των πληρωμών σε Δημόσιες Υπηρεσίες : Έχει εφαρμογή και στο δημόσιο τομέα σε πληρωμές φόρων/τελών.
5. Συστήματα ERP και CRM : Εφαρμογές που διαχειρίζονται επιχειρησιακές διαδικασίες κάνουν χρήση SET για ασφαλή οικονομική διαχείριση.

Λειτουργίες SET

Το πρωτόκολλο αυτό βασίζεται σε μια σειρά από λειτουργίες για την ολοκληρωμένη προστασία των συναλλαγών :

1. Αυθεντικοποίηση (Authentication)
   Επιβεβαιώνει τις ταυτότητες όλων των μερών με την βοήθεια των Αρχών Πιστοποίησης
2. Εμπιστευτικότητα (Confidentiality)
   Με την κρυπτογράφηση των δεδομένων της συναλλαγής επιτυγχάνεται η διατήρηση της ασφάλειας των "ευαίσθητων" πληροφοριών (πχ αριθμοί κάρτας).
3. Ψηφιακή Υπογραφή (Digital Signature)
   Με αυτή τη λειτουργία επιβεβαιώνεται η ταυτότητα του εκάστοτε αποστολέα και έτσι δεν μπορεί να αμφισβητηθεί η συναλλαγή.
4. Επικύρωση Συναλλαγών (Transaction Validation)
   Τέλος, όλες οι πληρωμές επικυρώνονται από το χρηματοπιστωτικό ίδρυμα του κατόχου της κάρτας, πριν την ολοκλήρωση της κάθε συναλλαγής.

4.5.7. Διαφορές SSL/TLS – SET

Συγκρίνοντας SET με SSL/TLS μπορούμε να εστιάσουμε στις βασικές διαφορές, στις λειτουργίες και τους στόχους τους :

1. ***Σκοπός και πού εφαρμόζονται***
   - SSL/TLS – Ευρεία χρήση σε διάφορες εφαρμογές όπως ιστοσελίδες,email αλλά και VPNs.
   - Σκοπός η δημιουργία ενός ασφαλούς καναλιού επικοινωνίας για τον χρήστη και τον διακομιστή.
   - SET – Αφορά κυρίως εφαρμογές e-Commerce και συστήματα πληρωμών τα οποία περιλαμβάνουν πολλά εμπλεκόμενα μέρη (καταναλωτές, εμπόρους, τράπεζες).
   - Σχεδιάστηκε για την ασφαλή διεξαγωγή των ηλεκτρονικών πληρωμών με έμφαση στις πιστωτικές/χρεωστικές κάρτες.
2. ***Διαφορές στην Τεχνολογία***
   - SSL/TLS – Χρησιμοποιεί ασύμμετρη κρυπτογράφηση για τη δημιουργία ενός συμμετρικού κλειδιού με το οποίο διασφαλίζεται η

εμπιστευτικότητα της επικοινωνίας. Επειδή αφορά κυρίως την αποφυγή της αλλοίωσης των δεδομένων στην επικοινωνία μόνο 2 μερών χρησιμοποιεί ασθενέστερη κρυπτογράφηση μέχρι 128 bits.

- SET – Από την άλλη μεριά το πρωτόκολλο SET κάνει χρήση κρυπτογράφησης 1024 bits καθώς εμπλέκονται περισσότερα μέρη στη συναλλαγή. Επίσης, χρησιμοποιεί τα ψηφιακά πιστοποιητικά για να αυθεντικοποιεί και τον έμπορο αλλά και τον κάτοχο της κάρτας.

Με μια γρήγορη ματιά έχουμε συγκεντρωτικά τα εξής :

	SET	*SSL/TLS*
Που εστιάζει	Ηλεκτρονικές Πληρωμές	Ασφάλεια Επικοινωνίας
Ποιον αυθεντικοποιεί	Πολλαπλά μέρη	Κυρίως τον διακομιστή στον πελάτη
Τι κρυπτογραφεί	Συναλλαγές	Δεδομένα
Κύριο Πλεονέκτημα	Υψηλή ασφάλεια πληρωμών	Εύκολη Εφαρμογή
Κύριο Μειονέκτημα	Πολυπλοκότητα, Κοστοβόρο	Μειωμένη εξειδίκευση στις πληρωμές

2 Συμβολή του συγγραφέα (σύγκριση – SET – SSL/TLS)

4.6 Απειλές και κίνδυνοι από την χρήση του Mobile Banking

Το Mobile Banking μπορεί να φέρει πληθώρα πλεονεκτημάτων αλλά αυτό δεν σημαίνει ότι είναι απαλλαγμένο από κινδύνους και απειλές. Γενικά τα πάντα έχουν να κάνουν με τις ευπάθειες των λειτουργικών συστημάτων των ίδιων των κινητών συσκευών που χρησιμοποιούνται για την εκτέλεση εφαρμογών Mobile Banking. Επιπλέον κίνδυνο έρχονται να προσθέσουν και οι πλατφόρμες Playstore και AppStore που μπορεί να περιέχουν κακόβουλο λογισμικό, μέσω των οποίων γίνεται και η λήψη των M-Banking Apps. Οι εφαρμογές που μπορούν να μας υποκλέψουν κωδικούς σύνδεσης είναι πάρα πολλές (Zitmo, Banker, Perkel, DroidDream, Keyloggers κ.α.). (Webroot,2014)

Αναλυτικότερα έχουμε:

1. **Sniffers** : Κακόβουλες εφαρμογές/λογισμικά υποκλοπής δεδομένων. Συνήθως συνδέονται σε μη ασφαλή δίκτυα Wi Fi και προσπαθούν να αποσπάσουν πληροφορίες που "ταξιδεύουν" σε αυτό.

   Σαν μέτρα προστασίας, μπορούμε να αποφεύγουμε γενικά την χρήση δημοσίων Wi Fi σαν χρήστες και να κατεβάζουμε τις εφαρμογές Mobile Banking μόνο από επίσημες πλατφόρμες όπως το Google Play.
2. **Key Loggers** : Πρόκειται για προγράμματα που καταγράφουν την πληκτρολόγηση που κάνει ο χρήστης εν αγνοία του φυσικά. Πρωταρχικός τους στόχος τα Usernames και τα Passwords.

   Με εγκατάσταση κάποιου εγκεκριμένου λογισμικού προστασίας από Malware/Virus και με συνεχή ενημέρωση της συσκευής μας και των λογισμικών ασφαλείας που διακατέχει, θα έχουμε ένα μεγάλο ποσοστό προστασίας απέναντι σε αυτού του είδους τον κίνδυνο.
3. **Phishing** : "Ηλεκτρονικό Ψάρεμα" μια μορφή εξαπάτησης του χρήστη μέσω ψεύτικων email,SMS ή ιστοσελίδων, πάντα με στόχο την υποκλοπή προσωπικών δεδομένων.

   Βασικός τρόπος αντιμετώπισης είναι για αρχή να αποκτήσουμε, εμείς σαν χρήστες εμπειρία και να μπορούμε να αναγνωρίζουμε το ψεύτικο μήνυμα ή site και να μην πατάμε ότι link μας αποστέλλονται χωρίς να έχουμε διασταυρώσει από που προέρχονται.

4. **Pharming** : Ανακατεύθυνση του χρήστη σε ψεύτικη/απάτη ιστοσελίδα με τέτοιο τρόπο που νομίζει ότι ακόμα περιηγείται στην γνήσια. Αυτή η απάτη γίνεται μέσω παραβιασμένων DNS (Domain Name Systems), (Μαυρογιάννης, 2003).

   «Φύλακας άγγελος» του χρήστη στην προκειμένη περίπτωση αποτελεί το πρωτόκολλο SSL/TLS καθώς οι ιστοσελίδες που το ακολουθούν δεν μπορούν να πέσουν θύματα αυτής της απάτης.

5. **Malware** : Κακόβουλο λογισμικό σχεδιασμένο για την εξαπάτηση του χρήστη. Συχνά τα λογισμικά αυτά έχουν τη "μορφή" χρήσιμων προγραμμάτων για το εκάστοτε θύμα ώστε να τον προκαλέσουν να τα ενεργοποιήσει στο σύστημά του. Δύο υποκατηγορίες Malware :

   A. A) Trojan Horse : Σε μετάφραση «Δούρειος Ίππος». Κυρίως εφαρμογές/αρχεία που παρουσιάζονται ως νόμιμες και μόλις εγκατασταθούν στην συσκευή αποκτούν πλήρη πρόσβαση σε δεδομένα και κινήσεις του θύματος.

      Εδώ πάλι ο ανθρώπινος παράγοντας παίζει βασικό ρόλο στην αντιμετώπιση αυτής της απειλής καθώς πρέπει οι ίδιοι να προσέχουμε τί κατεβάζουμε και από πού. (Gao,2015)

   B. B) Virus : Προγράμματα υπολογιστή που "μολύνουν" το σύστημά μας χωρίς την άδειά μας και φυσικά χωρίς να έχουμε επίγνωση αυτών των κινήσεών τους. Κύριος τρόπος μετάδοσης των "ιών" αυτών είναι τα email.

Δυστυχώς με την νέα τεχνολογία έχουν αναβαθμιστεί και αυτού του είδους τα λογισμικά με συνέπεια να έχουμε αυξήσει το εύρος της δράσης τους.

Γενικά όπως βλέπουμε δύο είναι οι βασικές συστάσεις που μπορούμε να επικεντρωθούμε για περαιτέρω Ασφάλεια στο Mobile Banking

A) Συνεχής ενημέρωση/αναβάθμιση των λειτουργικών συστημάτων και των εφαρμογών.

B) Ενίσχυση ευαισθητοποίησης των χρηστών.

4.7 Δίωξη Ηλεκτρονικού Εγκλήματος – Ελληνική Αστυνομία

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.) της Ελληνικής Αστυνομίας αναλαμβάνει ποικίλες δράσεις για την αντιμετώπιση των παραπάνω απειλών καθώς είναι υπεύθυνη για την πρόληψη, διερεύνηση αλλά και καταστολή των εγκλημάτων που διαπράττονται μέσω διαδικτύου, πόσο μάλλον στο τομέα Mobile Banking. Ας δούμε εν συντομία τις δράσεις αυτές :

1. **<u>Ενημέρωση και Ευαισθητοποίηση του κοινού</u>**

Η ΔΙ.Δ.Η.Ε. διοργανώνει συνεχώς Ημερίδες Ασφαλούς Πλοήγησης σε όλη τη χώρα με στόχο την ενημέρωση των πολιτών μικρών και μεγάλων, για τους κινδύνους του Διαδικτύου και τις μεθόδους προστασίας από αυτούς.

Πραγματοποιεί Τηλεδιασκέψεις με καινοτόμες τεχνολογίες σε πραγματικό χρόνο επιτρέποντας κατά αυτό τον τρόπο την αλληλεπίδραση μεταξύ ομιλητών και ακροατών.

Δέχεται Εκπαιδευτικές Επισκέψεις από διάφορα σχολεία/φορείς προσφέροντας ενημέρωση σε μαθητές και εκπαιδευτικούς.

Τέλος, έχει "εισβάλλει" η ΔΙ.Δ.Η.Ε. και στα μέσα κοινωνικής δικτύωσης με την σελίδα Cyberalert.gr , την οποία μπορούμε να την βρούμε πλέον σε Facebook, Twitter, Instagram και Youtube.

2. **<u>Συνεργασία με Χρηματοπιστωτικά Ιδρύματα</u>**

Γενικά η συγκεκριμένη Υπηρεσία είναι σε "στενή" συνεργασία με τις Τράπεζες για ανίχνευση και αντιμετώπιση περιστατικών απάτης καθώς διακυβεύονται τα πολύτιμα προσωπικά δεδομένα αλλά και οι περιουσίες των χρηστών.

3. Συνεχή Διερεύνηση των Καταγγελιών

Η ΔΙ.Δ.Η.Ε. δυστυχώς δέχεται συνεχώς καταγγελίες από πολίτες αλλά και επιχειρήσεις για περιστατικά ηλεκτρονικής απάτης και κατόπιν έρευνας - > προχωρά στον εντοπισμό και σύλληψη του δράστη.

4. Εκπαίδευση και Κατάρτιση του Στόλου της

Η Δίωξη Ηλεκτρονικού Εγκλήματος διαθέτει αρκετούς από τους πόρους της για την εκπαίδευση του προσωπικού της καθώς αποτελεί βασικό παράγοντα για την αντιμετώπιση των απειλών, αφού η τεχνολογία αλλάζει μέρα με τη μέρα, δίνοντας την ευκαιρία στους εγκληματίες να βρίσκουν νέους μεθόδους επίθεσης.

5. Διεθνής Συνεργασία

Πλέον η Ελλάδα συμμετέχει στις προτεραιότητες του κύκλου EMPACT 2022-2025 μαζί με τα υπόλοιπα κράτη-μέλη της Ε.Ε. με κοινό σκοπό την καταπολέμηση του οργανωμένου εγκλήματος. Κατά αυτόν τον τρόπο έχουμε διασυνοριακή συνεργασία της ΔΙ.Δ.Η.Ε. με Διεθνείς οργανισμούς και Αρχές ανταλλάσσοντας πληροφορίες και μεθόδους.

Κεφάλαιο 5

«Mobile Banking – Συστημικές Ελληνικές Τράπεζες»

Στο κεφάλαιο αυτό θα μιλήσουμε περιληπτικά για τις 4 κύριες (συστημικές) Ελληνικές Τράπεζες και για το πως προσφέρουν τους προηγμένες υπηρεσίες Mobile Banking στο Ελληνικό τραπεζικό κοινό.

5.1 Εθνική Τράπεζα – NBG

Μια ισορροπημένη εφαρμογή με βασικές υπηρεσίες/λειτουργίες αλλά με λιγότερες καινοτομίες σε σχέση με τον ανταγωνισμό.

Α) Η Εθνική Τράπεζα κατέχει την εφαρμογή NBG Mobile Banking την οποία μπορούμε να κατεβάσουμε στις κινητές μας συσκευές μέσω των γνωστών πλατφορμών Playstore (Android) και AppStore (Ios). Μόλις εγκαταστήσουμε το App απαιτείται φυσικά εγγραφή του χρήστη. Από εκεί και έπειτα αρκεί μόνο η σύνδεση στο Διαδίκτυο για να λάβεις τις υπηρεσίες και τα προϊόντα της ΕΤΕ.

Υπηρεσίες Mobile Banking που προσφέρει

Άνοιγμα νέου λογαριασμού και απόκτηση κάρτας : Πλέον η διαδικασία γίνεται ακόμα πιο εύκολη καθώς και τα δικαιολογητικά για την ολοκλήρωση του λογαριασμού μπορούν να σταλούν μέσω του eGov-KYC.

- Διαχείριση λογαριασμών και καρτών 24/7.
- Πληρωμές οφειλών-λογαριασμών αλλά και τραπεζικές συναλλαγές (εμβάσματα-μεταφορές)
- Ενημέρωση για το αφορολόγητο ποσό που έχουν για να καλύψουν οι πελάτες της, μέσω εξόδων με τις κάρτες τους.

Β) Ασφάλεια NBG

Η ΕΤΕ δίνει ιδιαίτερη έμφαση όσον αφορά το θέμα Ασφάλεια στις συναλλαγές μέσω της εφαρμογής της. Κάνοντας χρήση του πρωτοκόλλου SSL/TLS και με τη βοήθεια ισχυρής κρυπτογράφησης διασφαλίζει την προστασία των δεδομένων των χρηστών της. Η Αρχή Πιστοποίησης (CA) που χρησιμοποιεί είναι η Verisign η οποία επικυρώνει την αυθεντικότητα των ψηφιακών πιστοποιητικών της.

Όσον αφορά τον ίδιο τον πελάτη, παρέχει δυνατότητα διαχείρισης στον ίδιο, για τις κάρτες του και το λογαριασμό του, όπως "πάγωμα" της κάρτας αλλά και καθορισμό ανωτάτων ορίων συναλλαγών.

5.2 Τράπεζα Πειραιώς – Piraeus App

Εφαρμογή με έμφαση στην ευαισθητοποίηση και καθοδήγηση του κοινού με εκπαίδευση και προσωποποιημένες συμβουλές.

Α) Η Τράπεζα Πειραιώς γνωστή για τα καινοτόμα προϊόντα και τις υπηρεσίες της έχει την εφαρμογή Piraeus App. Οι χρήστες της μπορούν να αξιοποιούν τις λειτουργίες της και να οργανώνουν τα οικονομικά τους από όπου και αν βρίσκονται.

Υπηρεσίες που προσφέρει

- Πλήρης Διαχείριση λογαριασμών και καρτών
- Μεταφορές χρημάτων – Εμβάσματα σε άλλα Τραπεζικά Ιδρύματα
- Πληρωμές λογαριασμών και με χρήση κωδικού RF
- Χρηματιστηριακές συναλλαγές
- Παρακολούθηση των δαπανών μέσω κάρτας για το αφορολόγητο – Στόχους Αποταμίευσης

Επιπλέον διαθέτει και το γνωστό σε όλους τους Έλληνες **"Πρόγραμμα Επιβράβευσης Yellow"**. Οι πελάτες της Τράπεζας Πειραιώς έχουν το προνόμιο να μαζεύουν πόντους απλά κάνοντας τις καθημερινές τους συναλλαγές και στη συνέχεια να τους εξαργυρώσουν σε μορφή έκπτωσης αγορών σε συνεργάτες του προγράμματος.

Β) Ασφάλεια – Piraeus App

Η Τράπεζα Πειραιώς εφαρμόζοντας προηγμένες μεθόδους και πρωτόκολλα ασφαλείας με κρυπτογράφηση 256 bits καλύπτει πλήρως τους πελάτες της όσον αφορά τον τομέα της ασφάλειας. Για έξτρα ασφάλεια απαιτεί από τον εκάστοτε νέο χρήστη υποβολή αίτησης ή επίσκεψη σε κάποιο φυσικό υποκατάστημά της.

Όσον αφορά το Interface της εφαρμογής έχουμε είσοδο με τετραψήφιο κωδικό που απαιτεί αλλαγή ανά τακτά χρονικά διαστήματα και βιομετρικά στοιχεία, πράγματα που υποστηρίζουν και οι υπόλοιπες Τραπεζικές Εφαρμογές του ανταγωνισμού.

5.3 Alpha Bank – MyAlpha Mobile

Εμπλουτισμένες υπηρεσίες με σταθερά κορυφαία υποστήριξη πελατών και βασικό μέλημα την διαφάνεια.

Α) Η MyAlpha Mobile App, πάλι διαθέσιμη όπως και οι υπόλοιπες εφαρμογές για λειτουργικά Android και Ios μέσω των αντίστοιχων πλατφορμών, εφόσον κατεβαστεί και εγκατασταθεί στη συσκευή μας, αποκτούμε τη δυνατότητα να διεκπεραιώσουμε τις συναλλαγές μας στο ασφαλές περιβάλλον της Alpha Bank.

Υπηρεσίες που προσφέρει

- Διαχείριση λογαριασμών/καρτών
- Ενημέρωση κινήσεων και υπολοίπων μέσω SMS
- Μεταφορές – πληρωμές μέσω συστήματος Dias Transfer
- Πρόγραμμα επιβράβευσης “Bonus” (αντίστοιχο με Yellow της Πειραιώς)

Μια καινοτομία της Alpha Bank για κινητά αποτελεί το **myAlpha Wallet**, το ψηφιακό πορτοφόλι που με χρήση λειτουργίας tap n’ pay παρέχει τη δυνατότητα να γίνονται οι ανέπαφες συναλλαγές στα τερματικά POS με χρήση της κινητής συσκευής ή κάποιου wearable (smartwatch) για όλες τις κάρτες της Τράπεζας Alpha.

Β) Ασφάλεια

Όπως όλα τα Τραπεζικά Ιδρύματα έτσι και η Alpha Bank οφείλει να κάνει τον πελάτη της να νιώθει ασφαλής κατά την περιήγησή του στην εφαρμογή της. Αυτό το πετυχαίνει με λειτουργίες όπως :

Συχνή απαίτηση αλλαγής password από τον χρήστη για να μην είναι εύκολο να βρεθεί από κακόβουλο λογισμικό.

- Push Notifications για να είναι ενήμερος ο πελάτης για οποιαδήποτε δραστηριότητα στο λογαριασμό του.
- Διαχείριση συνδεδεμένων συσκευών στο e-Banking κάθε χρήστη.
- Χρήση PIN/βιομετρικών στοιχείων, ανάλογα πάντα τη συσκευή, για είσοδο στην εφαρμογή.

5.4 Eurobank – Eurobank Mobile App

Εξαιρετική εμπειρία για τον χρήστη με ισχυρή ασφάλεια, για ολοκληρωμένη προστασία στις πληρωμές.

Α) Ομοίως με τις προαναφερθέν εφαρμογές του ανταγωνισμού η Eurobank έρχεται με τη σειρά της να εξυπηρετήσει το κοινό της με παρόμοιες υπηρεσίες 24/7, απλά και μόνο με τη χρήση ενός κινητού τηλεφώνου ανεξαρτήτως λογισμικού, με σύνδεση στο Internet.

Υπηρεσίες που προσφέρει

- ✓ Συνεχή online ενημέρωση για κινήσεις, λογαριασμούς, κάρτες, επενδύσεις κ.α.
- ✓ Μεταφορές χρημάτων μεταξύ λογαριασμών αλλά και άλλων Τραπεζών
- ✓ Εξόφληση λογαριασμών ΔΕΚΟ αλλά και οφειλών προς Δημοσίους φορείς
- ✓ Επίσης, έχουμε και εδώ πρόγραμμα επιβράβευσης "€πιστροφή" το οποίο λειτουργεί κατά τον ίδιο τρόπο με τα προηγούμενα, αλλά με κύρια διαφορά ότι αντί για πόντους επιστρέφει χρήματα ανάλογα με τις αγορές του πελάτη στις συμβεβλημένες επιχειρήσεις.

Β) Ασφάλεια

Η εφαρμογή της Eurobank ενισχυμένη και αυτή με πρωτόκολλα ασφαλείας και ισχυρή κρυπτογράφηση 256 bit έρχεται να παρέχει ένας ασφαλές περιβάλλον για τον χρήστη. Παρεμφερή λειτουργίες με τον ανταγωνισμό, έχουμε απαίτηση αλλαγής password από τον χρήστη ανά 6 μήνες και χρόνο αδράνειας στης εφαρμογή με την παρέλευση του οποίου γίνεται αυτόματη αποσύνδεση χρήστη.

5.5 Σύγκριση

Κλείνοντας το Κεφάλαιο των Ελληνικών Συστημικών Τραπεζών καταλήγουμε ότι οι προσφερόμενες υπηρεσίες Mobile Banking είναι σχεδόν ίδιες σε κάθε εφαρμογή. Με γοργούς ρυθμούς το καταναλωτικό κοινό δείχνει να αγκαλιάζει το M-Banking και να εξοικειώνεται με αυτό.

Στον τομέα της ασφάλειας, επίσης έχουμε ομοιότητες καθώς η τεχνολογία ακμάζει και όποιος μείνει πίσω δέχεται τις συνέπειες. Διακρίνουμε ίδιες μεθόδους κρυπτογράφησης και διαδικασιών ασφαλείας που έχουν να κάνουν με την πρόσβαση στην εφαρμογή αλλά και γενικά με την συνεχή ενημέρωση του χρήστη για τις κινήσεις του λογαριασμού του.

Ακολουθεί μια σύντομη συγκριτική ανάλυση των τεσσάρων βασικών Τραπεζών της Ελληνικής Επικράτειας.

Διαχείριση Λογαριασμών και Καρτών				
Τράπεζα	Εθνική Τράπεζα	Τράπεζα Πειραιώς	Eurobank	Alpha Bank
Παρακολούθηση Υπολοίπων	✓	✓	✓	✓
Διαχείριση Καρτών	✓ (Νέες κάρτες, όρια)	✓ (Ενεργοποίηση/ Μπλοκάρισμα)	✓ (Όρια και μπλοκάρισμα)	✓ (Ρυθμίσεις ασφαλείας)
Επενδύσεις	✓	✓	✓	✓
Μεταφορές και Πληρωμές				
Τράπεζα	Εθνική Τράπεζα	Τράπεζα Πειραιώς	Eurobank	Alpha Bank
Εσωτερικές Μεταφορές	✓	✓	✓	✓
Εξωτερικές Μεταφορές	✓	✓	✓	✓
IRIS Payments	✓	✓	✓	✓

Ασφάλεια				
Τράπεζα	Εθνική Τράπεζα	Τράπεζα Πειραιώς	Eurobank	Alpha Bank
Κρυπτογράφηση	256 bit	256 bit	256 bit	256 bit
Πολυπαραγοντική Επαλήθευση	✓ (SMS/Email)	✓ (SMS/Push)	✓ (SMS/Push)	✓ (SMS/Push)
Βιομετρικά	✓	✓	✓	✓

Καινοτομίες				
Τράπεζα	Εθνική Τράπεζα	Τράπεζα Πειραιώς	Eurobank	Alpha Bank
Διαχείριση Επενδύσεων	✓	✓	✓	✓
Εκπαιδευτικά Εργαλεία	✗	✓ (Συμβουλές Smart Tips)	✗	✓ (Οδηγίες Χρήσης)
Φιλικό UI/UX	✓	✓	✓	✓

Δυνατότητες Χρήστη				
Τράπεζα	Εθνική Τράπεζα	Τράπεζα Πειραιώς	Eurobank	Alpha Bank
Υποστήριξη Πελατών	Live Chat	Live Chat/Video Call	Live Chat	Live Chat
Ευκολία Πλοήγησης	Πολύ Καλή	Εξαιρετική	Πολύ Καλή	Εξαιρετική
Push Ειδοποιήσεις	✓	✓	✓	✓

(Πηγή: Επεξεργασία στοιχείων από τα επίσημα site των Τράπεζων και Ελληνική Ένωση Τραπεζών (Hellenic Bank Association - HBA) https://www.hba.gr από τον συγγραφέα.)

Μέρος 2ο Εμπειρικό Τμήμα

- *Εμπειρική Βιβλιογραφική Ανασκόπηση*

Διεθνή Εμπειρικά Ευρήματα

Μελέτες όπως αυτή του Shaikh & Karjaluoto (2015) έχουν δείξει ότι η ευκολία χρήσης και η πρόσβαση σε τραπεζικές συναλλαγές είναι οι κύριοι παράγοντες που οδηγούν τους καταναλωτές να υιοθετήσουν εφαρμογές Mobile Banking. Από την άλλη πλευρά, η μελέτη του Zhao et al. (2019) έδειξε πως οι ανησυχίες για την ασφάλεια επηρεάζουν αρνητικά την εμπιστοσύνη των χρηστών, ακόμα και όταν η τεχνολογία βελτιώνεται συνεχώς.

Εμπειρικά Δεδομένα για το Ελληνικό Περιβάλλον

Στην Ελλάδα, διάφορες έρευνες έχουν καταγράψει μια ραγδαία αύξηση στη χρήση του Mobile Banking. Έρευνες από το Ευρωβαρόμετρο που δημοσιεύονται σε πλατφόρμες όπως το Powergame.gr (2023) καταδεικνύουν ότι 8 στους 10 Έλληνες έχουν ενσωματώσει τις ψηφιακές τραπεζικές υπηρεσίες στην καθημερινότητά τους. Αυτά τα δεδομένα επιβεβαιώνουν την ευρεία αποδοχή αλλά και τις ανησυχίες για την ασφάλεια που παρατηρούνται στο ελληνικό κοινό.

Σύνδεση Διεθνών και Εθνικών Ευρημάτων

Η σύγκριση των διεθνών εμπειρικών δεδομένων με τα ελληνικά ευρήματα αποκαλύπτει ομοιότητες και διαφορές που είναι κρίσιμες για την κατανόηση του φαινομένου. Ενώ οι διεθνείς έρευνες επισημαίνουν την κεντρική σημασία της ευκολίας πρόσβασης και της τεχνολογικής καινοτομίας, στο ελληνικό περιβάλλον παρατηρείται ιδιαίτερη έμφαση στην ασφάλεια και την εμπιστοσύνη. Η διαπίστωση ότι οι Έλληνες χρήστες, παρά την αυξημένη χρήση, διατηρούν ανησυχίες για την προστασία των προσωπικών τους δεδομένων, υποδηλώνει την ανάγκη περαιτέρω μελέτης αυτών των παραγόντων στο ελληνικό πλαίσιο.

Συμπεράσματα και Εμπειρικές Προοπτικές

- **Ευκολία και Πρόσβαση:** Η απρόσκοπτη πρόσβαση στις τραπεζικές συναλλαγές αποτελεί ισχυρό κίνητρο για τη χρήση του Mobile Banking (Shaikh & Karjaluoto, 2015).
- **Ασφάλεια:** Τα εμπειρικά δεδομένα δείχνουν ότι οι ανησυχίες για την ασφάλεια επηρεάζουν σημαντικά την εμπιστοσύνη και την υιοθέτηση, απαιτώντας συνεχή επενδύσεις σε τεχνολογίες προστασίας (Zhao et al., 2019).
- **Ελληνική Πραγματικότητα:** Τα δεδομένα από ελληνικές πηγές επιβεβαιώνουν μια δυναμική ανάπτυξης, αλλά ταυτόχρονα επισημαίνουν την ανάγκη για ενίσχυση των μέτρων ασφαλείας, ώστε να αντιμετωπιστούν οι ιδιαίτερες προκλήσεις του ελληνικού περιβάλλοντος (Powergame.gr, Παρουσίαση Έρευνας του Ευρωβαρόμετρου, 2023).

Κεφάλαιο 6ο

«Έρευνα για το Mobile Banking στην Ελλάδα»

6.1 Σκοπός της Έρευνάς μου

Η χρήση του Mobile Banking στην Ελλάδα έχει αυξηθεί σημαντικά τα τελευταία χρόνια, όπως δείχνουν επίσημες έρευνες. Το Ευρωβαρόμετρο αναφέρει ότι οκτώ στους δέκα Έλληνες χρησιμοποιούν εφαρμογές Mobile και Internet Banking (Powergame.gr, Παρουσίαση Έρευνας του Ευρωβαρόμετρου, 2023). Αυτή η ραγδαία αύξηση καθιστά επιτακτική την ανάγκη μελέτης της αντίληψης των χρηστών για την ασφάλεια και τις μελλοντικές προοπτικές του.

Σκοπός της παρούσας έρευνας είναι να διερευνηθεί η χρήση του Mobile Banking στην Ελλάδα, εστιάζοντας στα εξής ερωτήματα:

- Ποιες εφαρμογές Mobile Banking χρησιμοποιούνται περισσότερο;
- Πόσο συχνά και για ποιες υπηρεσίες;
- Πόσο ασφαλείς νιώθουν οι χρήστες κατά τη χρήση των Mobile Banking Apps;
- Πώς προβλέπουν οι χρήστες το μέλλον του Mobile Banking στην Ελλάδα και τί θέλουν να βελτιωθεί;

6.2 Μεθοδολογία

Για την επίτευξη αυτού του σκοπού, ακολουθήθηκε μια ποσοτική ερευνητική προσέγγιση, βασισμένη στη χρήση ερωτηματολογίου.

Μια τέτοιου είδους έρευνα επιτρέπει τη συλλογή δεδομένων από μεγάλο αριθμό συμμετεχόντων και τη στατιστική ανάλυση των αποτελεσμάτων (Bryman, 2016). Η χρήση ερωτηματολογίου επιλέχθηκε λόγω της δυνατότητάς του να συγκεντρώνει πληροφορίες με δομημένο και συστηματικό τρόπο, διασφαλίζοντας την αξιοπιστία και την εγκυρότητα των απαντήσεων (Saunders et al., 2019).

6.3 Δείγμα

Το δείγμα της έρευνας αποτελείται από Έλληνες χρήστες Mobile Banking, ηλικίας 18 ετών και άνω. Η μέθοδος δειγματοληψίας που χρησιμοποιήθηκε είναι η δειγματοληψία ευκολίας (convenience sampling), δεδομένου ότι το ερωτηματολόγιο διανεμήθηκε διαδικτυακά μέσω πλατφορμών κοινωνικής δικτύωσης και ηλεκτρονικού ταχυδρομείου. Ο στόχος ήταν η συλλογή τουλάχιστον 100 απαντήσεων, ώστε να διασφαλιστεί η επαρκής στατιστική ισχύς της έρευνας (Creswell & Creswell, 2018).

6.4 Ερωτηματολόγιο

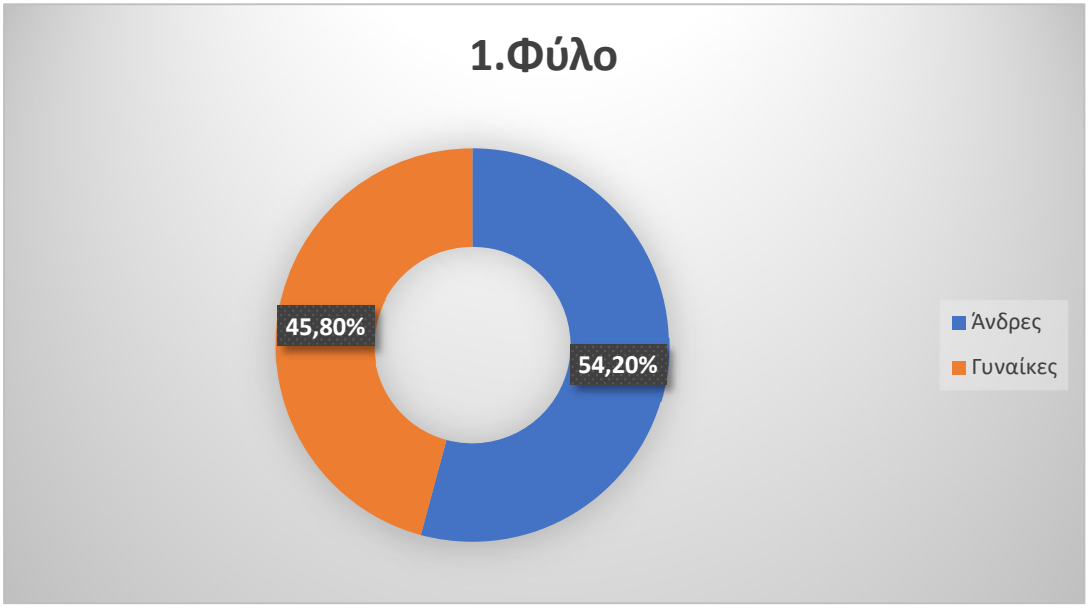
Το βασικό εργαλείο για τη συλλογή των δεδομένων ήταν ένα δομημένο ερωτηματολόγιο, με λίγες αλλά στοχευμένες ερωτήσεις.

Η διανομή του ερωτηματολογίου πραγματοποιήθηκε διαδικτυακά, καθώς αυτή η μέθοδος επιτρέπει τη γρήγορη και οικονομικά αποδοτική συλλογή δεδομένων (Evans & Mathur, 2018). Οι συμμετέχοντες ενημερώθηκαν για τον σκοπό της έρευνας, τη διασφάλιση της ανωνυμίας τους και τη δυνατότητα απόσυρσης από τη μελέτη ανά πάσα στιγμή.

6.5 Παρουσίαση αποτελεσμάτων

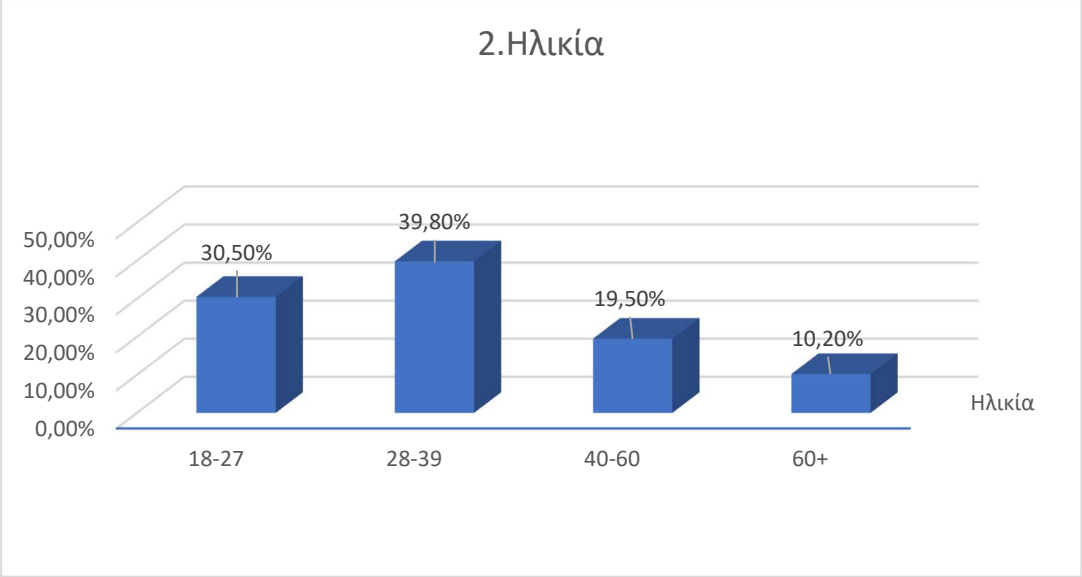
"Όλα τα διαγράμματα που παρουσιάζονται στο παρόν κεφάλαιο βασίζονται σε πρωτογενή δεδομένα της έρευνας του συγγραφέα."

Γενικές Πληροφορίες Ερωτηθέντα



🔎 **Συμπέρασμα**: Η αναλογία φύλου είναι αρκετά ισορροπημένη, με μια μικρή υπεροχή των ανδρών.

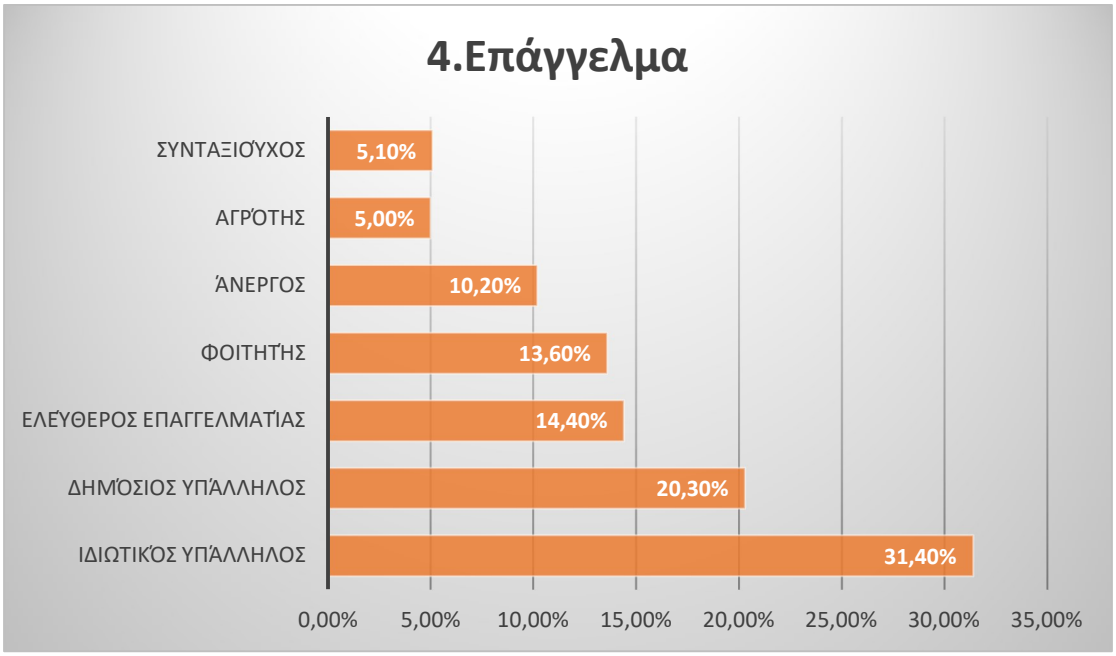
📈 **Σύγκριση με άλλες μελέτες**: Τα ευρήματα της έρευνας Laukkanen δείχνουν ότι οι άνδρες είναι πιο πιθανό να χρησιμοποιήσουν τις υπηρεσίες κινητής τραπεζικής σε σχέση με τις γυναίκες. Αντίθετα, οι γυναίκες τείνουν να είναι πιο επιφυλακτικές και είναι πιο πιθανό να απορρίψουν την κινητή τραπεζική σε σύγκριση με τους άνδρες (Laukkanen, 2007).



🔎 **Συμπέρασμα**: Οι ηλικίες 28-39 είναι η κυρίαρχη ομάδα χρήσης Mobile Banking, ακολουθούμενη από τη νεότερη ομάδα 18-27. Οι μεγαλύτερες ηλικίες (40+) έχουν μικρότερη παρουσία.

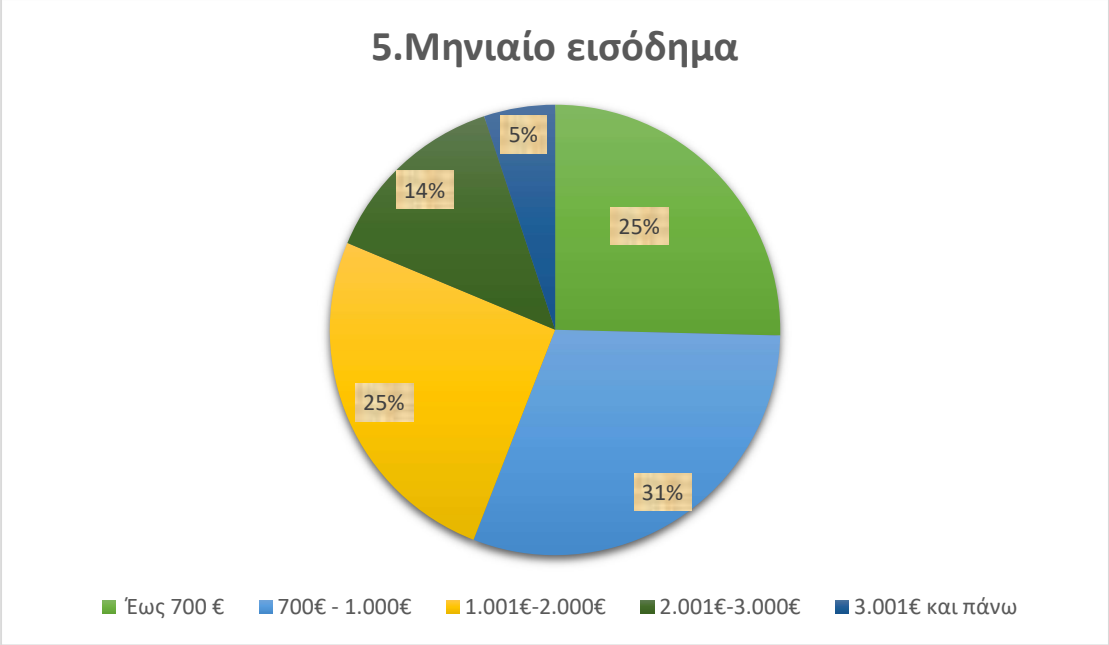
📈 **Σύγκριση με άλλες μελέτες**: Ο Laukkanen (2007) αναφέρει ότι τα άτομα ηλικίας 55 ετών και άνω είναι λιγότερο πιθανό να υιοθετήσουν την κινητή τραπεζική, καθώς έχουν χαμηλότερη πρόθεση να τη χρησιμοποιήσουν.

🔎 **Συμπέρασμα**: Το μεγαλύτερο ποσοστό των χρηστών Mobile Banking έχει πανεπιστημιακή εκπαίδευση, κάτι που δείχνει ότι η τεχνολογία προσελκύει άτομα με υψηλότερο μορφωτικό επίπεδο.



🔎 **Συμπέρασμα**: Οι εργαζόμενοι στον ιδιωτικό τομέα αποτελούν τη μεγαλύτερη ομάδα χρηστών, με δημόσιους υπαλλήλους και φοιτητές να ακολουθούν.

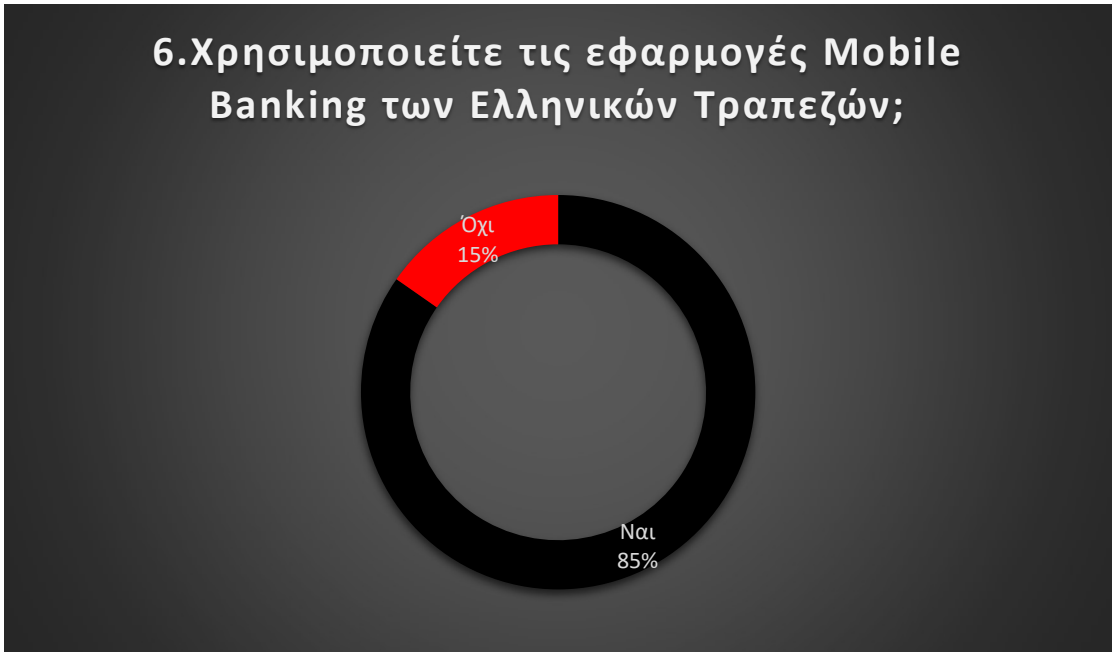
📈 **Σύγκριση με άλλες μελέτες**: Σε αντίστοιχες έρευνες (Deloitte, 2022), οι φοιτητές και οι ιδιωτικοί υπάλληλοι είναι οι πιο συχνοί χρήστες Mobile Banking.



🔎 **Συμπέρασμα**: Το Mobile Banking χρησιμοποιείται ευρέως από άτομα με μεσαίο εισόδημα, αλλά λιγότερο από υψηλόμισθους.

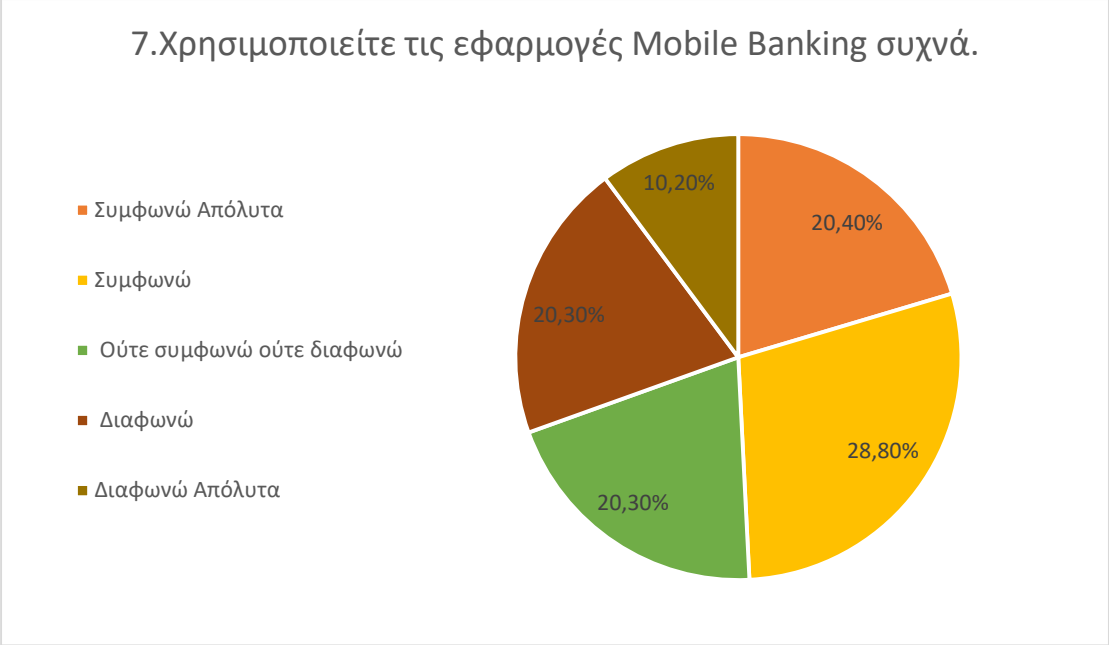
📈 **Σύγκριση με άλλες μελέτες**: Η έρευνα του Fonseca, J. R. S. (2014) δείχνει ότι οι πολίτες με υψηλότερα επίπεδα εκπαίδευσης είναι πιο επιφυλακτικοί και λιγότερο πιθανό να αναλάβουν κινδύνους, κάτι που ισχύει επίσης για τους πολίτες με υψηλότερα εισοδήματα.

Συχνότητα και είδος χρήσης εφαρμογώνMobile Banking



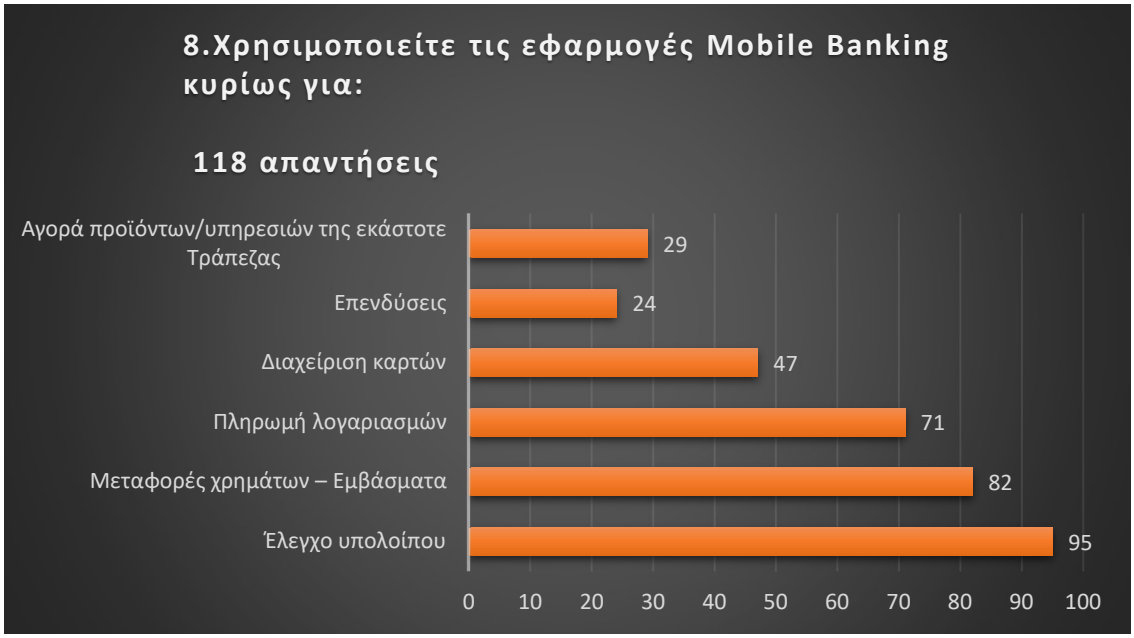
🔎 **Συμπέρασμα**: Η συντριπτική πλειοψηφία χρησιμοποιεί Mobile Banking, επιβεβαιώνοντας τη διαδεδομένη χρήση του.

📈 **Σύγκριση**: Σύμφωνα με την έκθεση της UK Finance με τίτλο "UK Payment Markets 2021" το 2020 περίπου το 72% των ενηλίκων στο Ηνωμένο Βασίλειο χρησιμοποιούσαν υπηρεσίες mobile banking, με τις ημερήσιες συνδέσεις να ξεπερνούν τα 7,4 εκατομμύρια.



🔎 **Συμπέρασμα**: Οι περισσότεροι χρήστες το χρησιμοποιούν τακτικά, αν και ένα 20% δεν είναι τόσο ενεργοί.

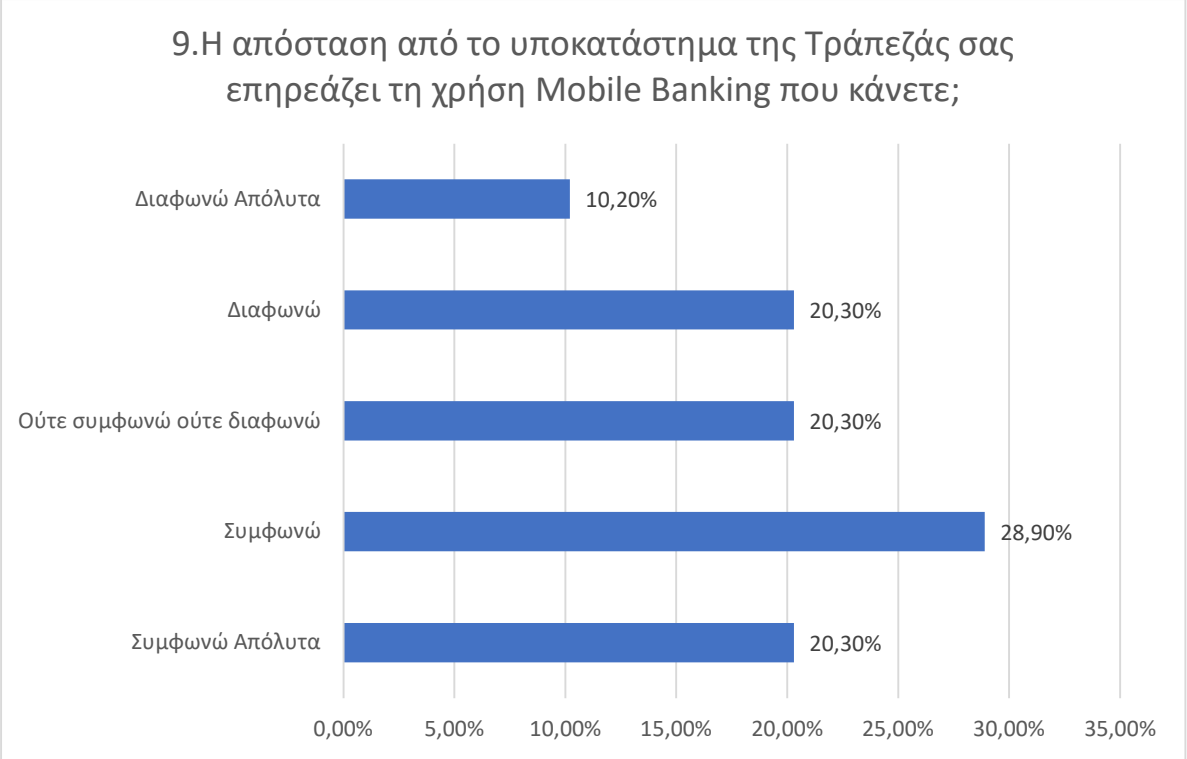
📈 **Σύγκριση**: Σύμφωνα με την έκθεση "Digital Banking Maturity 2020" της Deloitte, η συχνότητα χρήσης των υπηρεσιών mobile banking ποικίλλει ανά χώρα. Συγκεκριμένα, σε παγκόσμιο επίπεδο, το 38% των πελατών χρησιμοποιούν mobile banking τουλάχιστον μία φορά την εβδομάδα. Στην Ευρώπη, το ποσοστό αυτό ανέρχεται στο 36%, ενώ στην Ασία φτάνει το 47%. Αυτά τα στοιχεία υποδεικνύουν ότι η υιοθέτηση του mobile banking είναι υψηλότερη σε ασιατικές χώρες σε σύγκριση με την Ευρώπη (Deloitte,2020).



🔎 **Συμπέρασμα**: Οι βασικές λειτουργίες είναι η παρακολούθηση υπολοίπου και οι πληρωμές.

📈 **Σύγκριση**:

Στην Ισπανία, η χρήση πληρωμών μέσω κινητού έχει αυξηθεί σημαντικά. Σύμφωνα με στοιχεία της Kutxabank, οι πληρωμές με κινητό σε καταστήματα αυξήθηκαν κατά 37% το πρώτο εξάμηνο του 2024 σε σύγκριση με το ίδιο διάστημα το 2023.

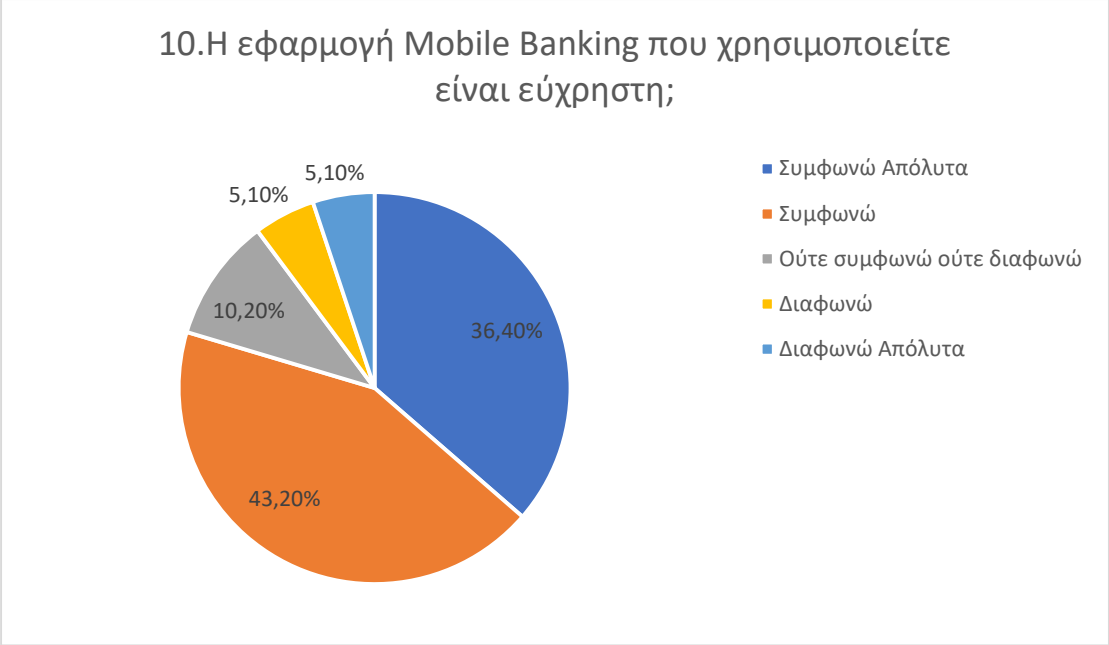


Ερμηνεία: Περίπου το 50% των ερωτηθέντων δηλώνει ότι η απόσταση από το τραπεζικό κατάστημα επηρεάζει τη χρήση Mobile Banking.

🔎 **Συμπέρασμα**: Οι απομακρυσμένες περιοχές στηρίζονται περισσότερο στο Mobile Banking, καθώς δεν έχουν άμεση πρόσβαση σε φυσικά καταστήματα.

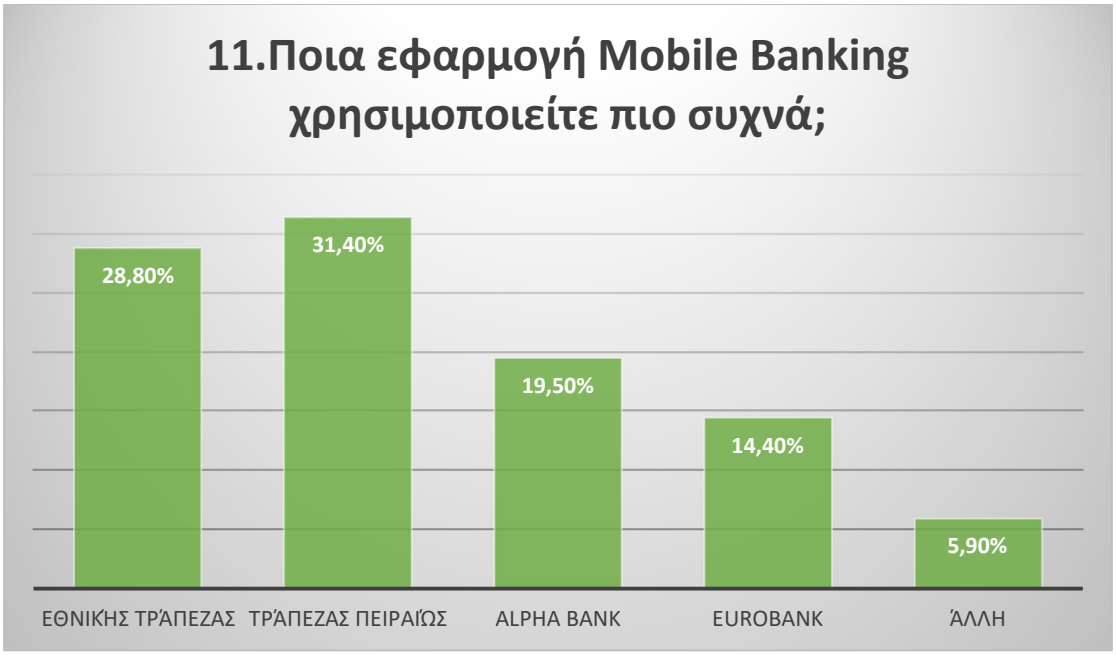
📈 **Σύγκριση με άλλες μελέτες**: Σύμφωνα με στοιχεία της Eurostat (ΕΕ-28), η πρόσβαση στο διαδίκτυο είναι μειωμένη στις αγροτικές περιοχές σε σύγκριση με τις αστικές περιοχές, ιδιαίτερα στην Ελλάδα. Το 2022, το 85% των ελληνικών νοικοκυριών είχε πρόσβαση στο διαδίκτυο, ενώ στις αγροτικές περιοχές το ποσοστό ήταν 76%, υπολείπεται δηλαδή κατά 14,4 ποσοστιαίες μονάδες του ευρωπαϊκού μέσου όρου.

Επιπλέον, η Ελλάδα κατατάσσεται μεταξύ των χωρών της ΕΕ με τα χαμηλότερα ποσοστά νοικοκυριών με πρόσβαση στο διαδίκτυο, μαζί με την Κροατία, και βρίσκεται 4,7 ποσοστιαίες μονάδες κάτω από τον ευρωπαϊκό μέσο όρο.



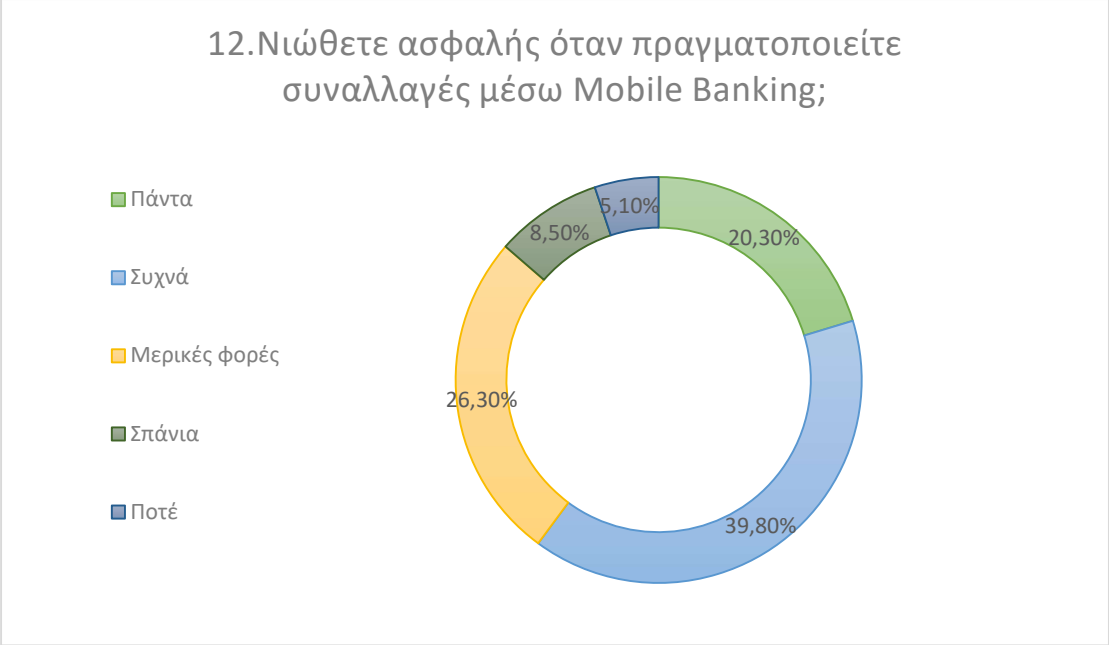
🔎 **Συμπέρασμα**: Η πλειοψηφία των χρηστών αξιολογεί θετικά τη χρηστικότητα των εφαρμογών, γεγονός που ενισχύει την αποδοχή τους.

📈 **Σύγκριση με άλλες μελέτες**: Αυτό το αποτέλεσμα συμφωνεί με την έρευνα του Venkatesh, 2000. Η αντίληψη της χρησιμότητας παίζει σημαντικό ρόλο στην ενθάρρυνση των καταναλωτών να υιοθετήσουν την υπηρεσία. Όσο περισσότερο θεωρούν ότι η υπηρεσία είναι χρήσιμη για τις τραπεζικές τους συναλλαγές, τόσο μεγαλύτερη είναι η πιθανότητα να τη χρησιμοποιήσουν.



🔎 **Συμπέρασμα**: Η δημοτικότητα των εφαρμογών σχετίζεται τόσο με την τεχνολογική υποδομή όσο και με τις συνήθειες των πελατών κάθε τράπεζας.

📈 **Σύγκριση με άλλες μελέτες**: Στις ΗΠΑ, οι mobile banking εφαρμογές των μεγάλων τραπεζών (π.χ. Bank of America) έχουν κυρίαρχη θέση, αλλά η χρήση fintech εφαρμογών όπως Revolut αυξάνεται (Deloitte, 2022).

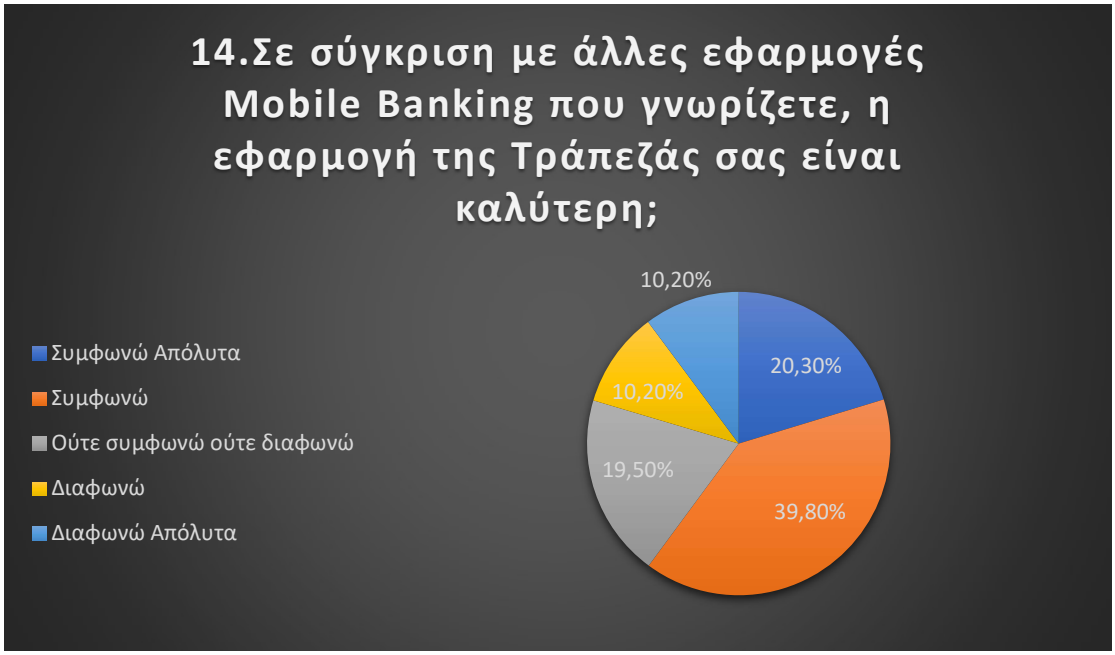


🔎 **Συμπέρασμα**: Παρόλο που η πλειοψηφία αισθάνεται ασφαλής, υπάρχει ένα 13,6 % που εκφράζει ανησυχίες. Αυτό μπορεί να σχετίζεται με περιπτώσεις διαδικτυακής απάτης ή ελλιπή γνώση των μέτρων ασφαλείας.

📈 **Σύγκριση**: Στην έρευνα των Zhao et al. (2019), η ασφάλεια αναφέρθηκε ως βασικός παράγοντας στην υιοθέτηση Mobile Banking, με παρόμοια ποσοστά χρηστών να εκφράζουν επιφυλάξεις.

🔎 **Συμπέρασμα**: Οι χρήστες αντιλαμβάνονται την ασφάλεια ως προτεραιότητα και αξιολογούν θετικά τις νέες τεχνολογίες προστασίας. Οι χρήστες θεωρούν την κρυπτογράφηση και την πολυπαραγοντική ταυτοποίηση ως τα πιο σημαντικά μέτρα ασφαλείας.

📈 **Σύγκριση με άλλες μελέτες**: Στην Πολωνία σε μελέτη των Wodo W. και Blaskiewicz P , κατόπιν εκτενούς συνέντευξης σε 60 άτομα ηλικίας 16-72 ετών συμπέραναν ότι υπάρχει ένα μεγάλο κενό ενημέρωσης σχετικά με τις απειλές από τον κυβερνοχώρο. Επίσης οι πελάτες της Ηλεκτρονικής Τραπεζικής δεν έχουν ακόμα κατανοήσει συγκεκριμένες μεθόδους πληρωμής και δεν αναγνωρίζουν σημαντικά οφέλη λύσεων όπως η 2FA καθώς πιστεύουν ότι δεν αποτελούν στόχο για τους επιτιθέμενους. (Wodo W. ,2021)



🔎 **Συμπέρασμα**:

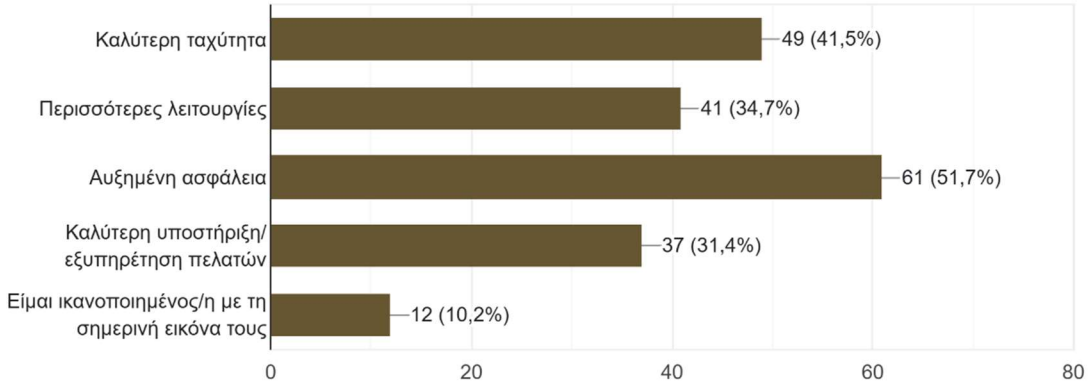
- Το 60,1% των χρηστών πιστεύει ότι η εφαρμογή της τράπεζάς τους είναι καλύτερη από άλλες.
- Ωστόσο, ένα 19,5% κρατά ουδέτερη στάση και το 20,3% διαφωνεί, δείχνοντας ότι υπάρχει περιθώριο για βελτιώσεις και ανταγωνισμό μεταξύ των τραπεζών.

📈 **Σύγκριση με άλλες μελέτες**:

Σύμφωνα με την Mirian de Guerreiro (2011), υπεύθυνη του Λογιστηρίου στην εταιρεία ACI, η οποία ειδικεύεται στον τομέα των ηλεκτρονικών πληρωμών για χρηματοοικονομικά ιδρύματα, το τοπίο των κινητών πληρωμών είναι αρκετά περίπλοκο. Αυτό οφείλεται στο γεγονός ότι υπάρχουν πολλαπλά συστήματα που συνυπάρχουν και συχνά αλληλεπικαλύπτονται. Η επιλογή του κατάλληλου συστήματος από τον χρήστη εξαρτάται από παράγοντες όπως η γεωγραφική τοποθεσία του, ποιος είναι ο παραλήπτης της πληρωμής, καθώς και ***οι υπηρεσίες που προσφέρει ο τραπεζικός του πάροχος***.

15.Ποιες βελτιώσεις θεωρείτε απαραίτητες στις εφαρμογές Mobile Banking; (Πολλαπλές επιλογές)

118 απαντήσεις



🔎 **Συμπέρασμα**:

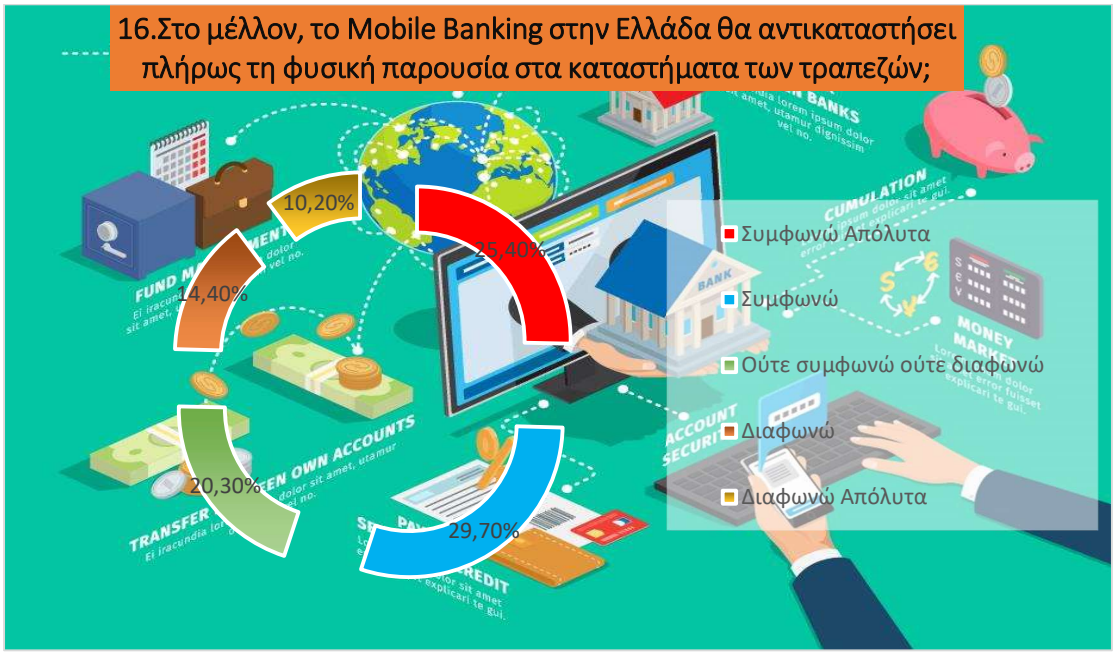
- Η **ασφάλεια** είναι ο κύριος τομέας που χρειάζεται βελτίωση (51,7%).
- Η **ταχύτητα** έρχεται δεύτερη, δείχνοντας ότι οι χρήστες θέλουν γρήγορες και αξιόπιστες εφαρμογές.
- Μόνο το 10,2% είναι απόλυτα ικανοποιημένο, κάτι που υποδεικνύει ότι οι τράπεζες πρέπει να συνεχίσουν να επενδύουν σε αναβαθμίσεις.

📈 **Σύγκριση με άλλες μελέτες:**

Ορισμένες τράπεζες δεν παρέχουν το ίδιο επίπεδο ασφάλειας για τις υπηρεσίες κινητής τραπεζικής όπως προσφέρουν για τις ηλεκτρονικές ή προσωπικές συναλλαγές (Chandran, 2014), κάτι που έρχεται σε συμφωνία με το αποτέλεσμα της έρευνάς μας καθώς 61 από τους 118 ερωτηθέντες αποζητά την ασφάλεια για το Mobile Banking App που χρησιμοποιεί.

Σύμφωνα με τους Wan-Rung, Wang & Hung (2012), τρεις βασικοί παράγοντες που επηρεάζουν την αποδοχή των πληρωμών μέσω κινητών είναι η ικανότητα, δηλαδή ο βαθμός εξοικείωσης των χρηστών με τις κινητές συσκευές και τις σχετικές τεχνολογίες, η παρότρυνση και η ευκαιρία, δηλαδή η δημιουργία συνθηκών που διευκολύνουν τη χρήση της υπηρεσίας και ενισχύουν την εξοικείωση. Οι εταιρείες πρέπει να καλλιεργούν συστηματικά αυτούς τους παράγοντες για να προωθήσουν τις κινητές πληρωμές και να ενισχύσουν την αποδοχή τους από το κοινό. Εδώ έρχεται να

ταιριάξει το ποσοστό 31,4% που αποζητά καλύτερη υποστήριξη από την Τράπεζά του , καθώς η εξοικείωση και η εκμάθηση δεν παύει να είναι ένας ουσιώδης παράγοντας για τα Mobile Banking Apps.



🔎 **Συμπέρασμα**:

- Το 55,1% των ερωτηθέντων πιστεύει ότι το Mobile Banking θα αντικαταστήσει τα φυσικά καταστήματα στο μέλλον.
- Ωστόσο, το 24,6% διαφωνεί, κάτι που δείχνει ότι υπάρχει ακόμα ανάγκη για φυσική παρουσία των τραπεζών.

📈 **Σύγκριση με άλλες μελέτες**: Η Ομοσπονδιακή Εταιρεία Ασφάλισης Καταθέσεων (2019) αναφέρει ότι το 2019, το 34% των πελατών προτιμούσαν την εφαρμογή κινητού για να έχουν πρόσβαση στους λογαριασμούς τους, ενώ το 2015 το ποσοστό ήταν 9,5% και το 2017 ανήλθε στο 15,6%, γεγονός που αποδεικνύει ότι σιγά σιγά ο κόσμος έχει αρχίσει να μην προσέρχεται στα Τραπεζικά παραρτήματα για διάφορες υπηρεσίες.

6.6 Συζήτηση - Συγκριτική Ανάλυση

Με την παρούσα έρευνα αναδείχθηκαν σημαντικά ευρήματα σχετικά με τη χρήση και την αντίληψη του Mobile Banking στην Ελλάδα. Τα δεδομένα μας δείχνουν ότι η ψηφιακή τραπεζική έχει εδραιωθεί σημαντικά στη χώρα, καθώς το 84,7% των

ερωτηθέντων χρησιμοποιεί Mobile Banking, γεγονός που επιβεβαιώνει τη γενικότερη στροφή των χρηστών προς τις ψηφιακές υπηρεσίες. Ωστόσο, παρόλο που η υιοθέτηση είναι υψηλή, υπάρχουν ακόμα ανησυχίες, κυρίως σε θέματα ασφάλειας (51,7%) και ταχύτητας (41,5%), κάτι που υποδηλώνει ότι οι τράπεζες οφείλουν να συνεχίσουν να βελτιώνουν τις εφαρμογές τους.

Σύγκριση με διεθνείς μελέτες

Τα αποτελέσματά μας συγκρίθηκαν με αντίστοιχες έρευνες από άλλες χώρες, προκειμένου να εντοπιστούν ομοιότητες και διαφορές. Μία πολύ καλή έρευνα για σύγκριση αποτελεί αυτή της **ING, International Survey on Mobile Banking 2016**, η οποία έχει λάβει δεδομένα από όλη την Ευρώπη. Σύμφωνα με αυτή λοιπόν, το **47%** των Ευρωπαίων χρηστών κινητών χρησιμοποιεί mobile banking, με ένα **16%** να σχεδιάζει να το υιοθετήσει μέσα στον επόμενο χρόνο. Σε σχέση με το **2015**, όπου το ποσοστό ήταν **41%**, η αύξηση είναι εμφανής. Ωστόσο, η ανάπτυξη δεν είναι ομοιόμορφη: χώρες όπως η **Ολλανδία** πλησιάζουν το όριο υιοθέτησης, ενώ σε **Ρουμανία, Ιταλία και Πολωνία**, η χρήση αναμένεται να αυξηθεί σημαντικά. Η μεγαλύτερη άνοδος χρήσης του M-Banking το 2016 σημειώθηκε σε **Αυστρία, Λουξεμβούργο και Τσεχία**. Οι **Τούρκοι** είναι οι πιο θετικοί, ενώ οι κάτοικοι του **Λουξεμβούργου** είναι λιγότερο ενθουσιώδεις. Θετικούς λοιπόν, βλέπουμε και τους Έλληνες στην έρευνά μας, οπότε μπορούμε να πούμε άφοβα ότι η χώρα μας ακολουθεί το κλίμα της Ευρώπης όσον αφορά την χρήση των M-Banking Apps.

Οι κύριοι χρήστες της κινητής τραπεζικής, στην έρευνά μας είναι νεαρά άτομα έως 45 ετών, που εργάζονται στον ιδιωτικό τομέα. Το εύρημα αυτό ευθυγραμμίζεται με διεθνείς μελέτες, ιδιαίτερα από την αμερικανική αγορά, οι οποίες δείχνουν ότι οι νεότερες γενιές είναι πιο πιθανό να πραγματοποιούν πληρωμές μέσω κινητού τηλεφώνου. Σύμφωνα με στοιχεία το 2015, το 30% των ατόμων ηλικίας 18-29 ετών και το 32% των ατόμων ηλικίας 30-44 ετών έκαναν χρήση του κινητού τους τηλεφώνου για πληρωμές αγαθών/υπηρεσιών.

Η έρευνα της Διεύθυνσης Καταναλωτών και Κοινοτικών Υποθέσεων της Ομοσπονδιακής Τράπεζας των ΗΠΑ (Federal Reserve Board) το 2016 έδειξε ότι η πιο διαδεδομένη χρήση της κινητής τραπεζικής είναι ο έλεγχος των υπολοίπων και των συναλλαγών, ενώ ακολουθεί η μεταφορά χρημάτων μεταξύ λογαριασμών, την οποία

πραγματοποίησε το 58% των χρηστών. Παρά το γεγονός ότι η διείσδυση της κινητής τραπεζικής στην Ελλάδα παραμένει σχετικά περιορισμένη και το κοινό δείχνει επιφυλακτικότητα, η συχνότητα χρήσης όσων την επιλέγουν είναι υψηλή, με το 49,2% των χρηστών να τη χρησιμοποιεί συχνά.

Ουκ ολίγες φορές έχουν πραγματοποιηθεί έρευνες σε διάφορες χώρες για να κατανοηθεί καλύτερα η στάση των καταναλωτών απέναντι στην εξελισσόμενη κινητή τεχνολογία. Για παράδειγμα, ο Mattila το 2003 διαπίστωσε ότι οι κύριοι παράγοντες που επηρεάζουν τις αποφάσεις των καταναλωτών στην υιοθέτηση τραπεζικών συστημάτων είναι η πολυπλοκότητα, η συμβατότητα, το συγκριτικό πλεονέκτημα, η παρατηρησιμότητα και η δυνατότητα δοκιμής. Επίσης, η ασφάλεια και η εμπιστευτικότητα των πληροφοριών είναι κρίσιμες για την επιτυχία των υπηρεσιών κινητής τραπεζικής (m-banking) (Mattila, 2003). Η κοινή αυτή ανησυχία υποδηλώνει ότι ανεξαρτήτως χώρας, οι καταναλωτές εξακολουθούν να θεωρούν την ασφάλεια κρίσιμο παράγοντα για τη χρήση των ψηφιακών τραπεζικών υπηρεσιών.

Ένα ακόμα σημαντικό εύρημα αφορά την πιθανότητα πλήρους αντικατάστασης των φυσικών καταστημάτων από το Mobile Banking. Η μικρότερη αποδοχή στη χώρα μας μπορεί να οφείλεται σε πολιτισμικούς και τεχνολογικούς παράγοντες, καθώς και στο γεγονός ότι ένα μέρος του πληθυσμού εξακολουθεί να προτιμά τις προσωπικές συναλλαγές στα τραπεζικά καταστήματα.

Συμπερασματικά

Η ανάλυση των δεδομένων υποδηλώνει ότι η Ελλάδα ακολουθεί τις διεθνείς τάσεις στον τομέα του Mobile Banking, αν και με ελαφρώς χαμηλότερους ρυθμούς αποδοχής σε ορισμένα σημεία, όπως η αντικατάσταση των φυσικών καταστημάτων. Οι κύριες προκλήσεις που καταγράφονται – ασφάλεια, ταχύτητα και ανάγκη για περισσότερες λειτουργίες – είναι παγκόσμια ζητήματα, γεγονός που δείχνει ότι οι ελληνικές τράπεζες δεν διαφέρουν σημαντικά από τις αντίστοιχες του εξωτερικού όσον αφορά τις προκλήσεις που αντιμετωπίζουν.

Τα ευρήματα αυτά μπορούν να αξιοποιηθούν από τον τραπεζικό κλάδο για να προσαρμόσουν τις στρατηγικές τους και να βελτιώσουν τις εφαρμογές Mobile Banking, ενισχύοντας την εμπιστοσύνη των καταναλωτών και βελτιώνοντας την

εμπειρία τους. Μελλοντικές έρευνες θα μπορούσαν να εξετάσουν πιο εις βάθος τους λόγους που κάποιοι χρήστες παραμένουν επιφυλακτικοί απέναντι στις ψηφιακές τραπεζικές συναλλαγές, καθώς και τις δυνατότητες περαιτέρω ανάπτυξης των Mobile Banking υπηρεσιών στην ελληνική αγορά.

Κεφάλαιο 7ο

«Γενικά Συμπεράσματα»

7.1 Γενικά Συμπεράσματα

Η παρούσα μελέτη ανέδειξε τη **σημαντική διείσδυση του Mobile Banking στην Ελλάδα**, με ποσοστό χρήσης που φτάνει το **84,7%**. Η τάση αυτή συμβαδίζει με τη **διεθνή στροφή προς την ψηφιοποίηση των τραπεζικών υπηρεσιών**, επιβεβαιώνοντας ότι οι Έλληνες καταναλωτές έχουν αποδεχθεί τις τεχνολογικές αλλαγές στον τραπεζικό τομέα.

Δημογραφικά στοιχεία και επίδρασή τους στη χρήση Mobile Banking

Η έρευνα κατέδειξε ότι το Mobile Banking χρησιμοποιείται κυρίως από **νεότερες ηλικιακές ομάδες (18-39 ετών)**, που συνιστούν σχεδόν το **70% των χρηστών**. Αυτό δείχνει ότι η **τεχνολογική εξοικείωση** παίζει καθοριστικό ρόλο στην υιοθέτηση αυτών των υπηρεσιών. Επιπλέον, το υψηλό μορφωτικό επίπεδο των χρηστών (πάνω από **74,6% κατέχει τουλάχιστον πτυχίο ΑΕΙ/ΤΕΙ**) υποδηλώνει ότι η εκπαίδευση λειτουργεί ως **καταλυτικός παράγοντας υιοθέτησης ψηφιακών χρηματοοικονομικών υπηρεσιών**.

Συχνότητα και είδος χρήσης

Οι κύριες λειτουργίες που χρησιμοποιούνται στο Mobile Banking είναι:

- **Έλεγχος υπολοίπου (80,5%)**
- **Μεταφορές χρημάτων (69,5%)**
- **Πληρωμές λογαριασμών (60,2%)**

Αυτό επιβεβαιώνει ότι η πλειοψηφία των χρηστών επιλέγει Mobile Banking κυρίως για **βασικές τραπεζικές συναλλαγές**, ενώ πιο σύνθετες υπηρεσίες (όπως επενδύσεις ή αγορές χρηματοοικονομικών προϊόντων) έχουν χαμηλότερη χρήση.

Ευχρηστία και Ασφάλεια: Παράγοντες αποδοχής και δισταγμού

Η έρευνα κατέδειξε ότι το **79,6% των χρηστών** βρίσκει τις εφαρμογές Mobile Banking εύχρηστες, γεγονός που συνάδει με παγκόσμιες τάσεις και δείχνει ότι οι τράπεζες έχουν βελτιώσει σημαντικά τη σχεδίαση των εφαρμογών τους. Παρ' όλα αυτά, **μόλις το 60,1% νιώθει πάντα ή συχνά ασφαλές** στις συναλλαγές του, υποδεικνύοντας ότι η ασφάλεια παραμένει ένας σημαντικός προβληματισμός.

Η σημασία της απόστασης από τα τραπεζικά καταστήματα

Ένα ενδιαφέρον εύρημα είναι ότι το **49,1% των ερωτηθέντων** δήλωσε ότι η **απόσταση από το τραπεζικό κατάστημα επηρεάζει τη χρήση του Mobile Banking**. Αυτό δείχνει ότι παρόλο που το Mobile Banking προσφέρει ανεξαρτησία από τη φυσική παρουσία σε ένα κατάστημα, εξακολουθεί να υπάρχει μια **ψυχολογική ή πρακτική σύνδεση με τις φυσικές τράπεζες**.

Προοπτικές και μελλοντικές τάσεις

Η έρευνα έδειξε ότι το **55,1% των χρηστών πιστεύει πως το Mobile Banking θα αντικαταστήσει πλήρως τα φυσικά τραπεζικά καταστήματα**. Ωστόσο, ένα **24,6% διαφωνεί**, δείχνοντας ότι παρόλο που το Mobile Banking αναπτύσσεται, οι φυσικές τράπεζες πιθανώς θα συνεχίσουν να έχουν ρόλο στο μέλλον, ιδιαίτερα για πιο **εξειδικευμένες ή πολύπλοκες τραπεζικές συναλλαγές**.

Βελτιώσεις και προσδοκίες των χρηστών

Οι ερωτηθέντες θεωρούν ότι οι τράπεζες θα πρέπει να επικεντρωθούν σε:

- **Ασφάλεια (51,7%)**
- **Ταχύτητα (41,5%)**
- **Πρόσθετες λειτουργίες (34,7%)**

Αυτό αποκαλύπτει ότι ενώ το Mobile Banking έχει ήδη υψηλή αποδοχή, υπάρχουν ακόμα **περιθώρια βελτίωσης**, ειδικά στον τομέα της ασφάλειας.

Τελικό Συμπέρασμα

Η μελέτη καταδεικνύει ότι το Mobile Banking στην Ελλάδα έχει **υψηλή διείσδυση και αποδοχή**, κυρίως από νεότερους και τεχνολογικά καταρτισμένους χρήστες. Ωστόσο, παρά τη λειτουργικότητα και ευκολία χρήσης, η **ανησυχία για την ασφάλεια** και η **συνεχιζόμενη ανάγκη για φυσικά καταστήματα** δείχνουν ότι το παραδοσιακό τραπεζικό μοντέλο δεν θα εξαλειφθεί άμεσα. Παρόλα αυτά, οι τάσεις δείχνουν ότι το Mobile Banking αποτελεί το **μέλλον των τραπεζικών συναλλαγών**, με **διαρκείς εξελίξεις στον τομέα της τεχνολογίας και της ασφάλειας**.

7.2 Περιορισμοί Έρευνας

Όπως κάθε ερευνητική μελέτη, έτσι και η παρούσα αντιμετώπισε ορισμένους περιορισμούς που πρέπει να ληφθούν υπόψη:

- **Περιορισμένο δείγμα**: Η έρευνα βασίστηκε σε **118 συμμετέχοντες**, γεγονός που περιορίζει τη γενίκευση των αποτελεσμάτων στον ευρύτερο ελληνικό πληθυσμό.
- **Συγκέντρωση δεδομένων μέσω ερωτηματολογίου**: Η μέθοδος αυτή αν και αξιόπιστη, επηρεάζεται από υποκειμενικές απαντήσεις των ερωτηθέντων.
- **Έλλειψη δεδομένων από μη χρήστες Mobile Banking**: Το ερωτηματολόγιο ήταν διαμορφωμένο έτσι ώστε να απαντήσει γενικά ερωτήματα για το M-Banking και κυρίως να αποκτήσουμε μια πολύ γενική εικόνα αυτού στην Ελλάδα. Παρόλαυτα, δεν εξετάζει τους μη χρήστες του M-Banking και τις αιτίες που τους οδήγησαν σε αυτή την απόφαση.
- **Δεν αναλύθηκαν τεχνικοί παράγοντες**: Παρά την έμφαση σε θέματα ασφάλειας και ευχρηστίας, δεν εξετάστηκε σε βάθος η τεχνική πλευρά των εφαρμογών Mobile Banking (π.χ. αρχιτεκτονική συστημάτων, χρήση τεχνητής νοημοσύνης κ.λπ.).

7.3 Προτάσεις – Research Proposal

Βάσει των ευρημάτων, προτείνεται:

- **Ενίσχυση της ασφάλειας στις εφαρμογές Mobile Banking**, π.χ. μέσω **βελτιωμένων συστημάτων ελέγχου ταυτότητας και κρυπτογράφησης δεδομένων**.
- **Βελτίωση της ταχύτητας και της ευχρηστίας των εφαρμογών**, ώστε να ανταποκρίνονται καλύτερα στις ανάγκες των χρηστών.
- **Προσθήκη προηγμένων λειτουργιών**, όπως **εξατομικευμένες συμβουλές για διαχείριση χρημάτων** μέσω τεχνητής νοημοσύνης.
- **Εκστρατείες ενημέρωσης** για την αύξηση της εμπιστοσύνης των χρηστών στην ασφάλεια του Mobile Banking.
- **Επέκταση της έρευνας σε ευρύτερο δείγμα** και σύγκριση με δεδομένα από άλλες χώρες, ώστε να κατανοηθεί καλύτερα η θέση της Ελλάδας στο παγκόσμιο τραπεζικό περιβάλλον.

7.4 Συνεισφορά της Έρευνας στο Fintech και στην Ηλεκτρονική Τραπεζική

Η έρευνα συμβάλλει σημαντικά στον τομέα του **Fintech και της ηλεκτρονικής τραπεζικής**, καθώς:

- Παρέχει **συγκεκριμένα δεδομένα για τη χρήση Mobile Banking στην Ελλάδα**, επιτρέποντας τη σύγκριση με διεθνείς τάσεις.
- Αναδεικνύει τους **κύριους παράγοντες που επηρεάζουν την αποδοχή και τη χρήση των εφαρμογών Mobile Banking**.
- Εντοπίζει **κρίσιμους τομείς βελτίωσης**, που μπορούν να αξιοποιηθούν από τις τράπεζες και τις Fintech εταιρείες για την ανάπτυξη καλύτερων προϊόντων.
- Παρέχει μια βάση για μελλοντικές μελέτες που θα μπορούσαν να επεκταθούν σε **νέες τεχνολογίες, όπως το Open Banking και τα Ψηφιακά Πορτοφόλια (Digital Wallets)**.

7.5 Ιδέες για μελλοντική Έρευνα

Με βάση τα αποτελέσματα, προτείνονται οι εξής κατευθύνσεις για μελλοντική έρευνα:

1. **Ποιοτική ανάλυση αυτών που δεν κάνουν χρήση Mobile Banking**: Συνεντεύξεις και focus groups θα μπορούσαν να αποκαλύψουν βαθύτερους λόγους μη χρήσης.
2. **Σύγκριση μεταξύ διαφορετικών ηλικιακών ομάδων**: Πώς διαφέρει η αντίληψη για το Mobile Banking μεταξύ νεότερων και μεγαλύτερων ηλικιών;
3. **Ανάλυση της σχέσης Mobile Banking και Ψηφιακών Πορτοφολιών**: Πόσο πιθανό είναι το Mobile Banking να εξελιχθεί σε ένα ολοκληρωμένο χρηματοοικονομικό οικοσύστημα;
4. **Εκτίμηση του μέλλοντος των φυσικών τραπεζικών καταστημάτων**: Πώς μπορεί το Mobile Banking να συνυπάρξει με τα υποκαταστήματα ή να τα αντικαταστήσει πλήρως στο μέλλον;

Η παρούσα μελέτη ανοίγει νέους δρόμους για την κατανόηση της **κινητής τραπεζικής στην Ελλάδα**, ενώ θέτει τις βάσεις για περαιτέρω έρευνα, που θα επιτρέψει στις τράπεζες και τις Fintech εταιρείες να προσαρμόσουν τις στρατηγικές τους στις πραγματικές ανάγκες των καταναλωτών.

Βιβλιογραφία

Ελληνική

- Αγγέλης, Β. (2005). *Η Βίβλος του e-banking*. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.
- Angelakopoulos, G. & Mihiotis (2011). E-banking: challenges and opportunities in the Greek banking sector. *Electronic Commerce Research, Volume 11, Issue 3*, 297–319.
- Αριστέα Σινανιώτη – Μαρούδη και Ιωάννης Δ. Φαρσαρώτας, «Ηλεκτρονική Τραπεζική», Εκδόσεις ΑΝΤ.Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2005.
- Μυρτίδης, Δ. (2008). *Τραπεζική Πληροφορική: Μέσα Τραπεζικής Εργασίας*. Τόμος Β', έκδ. 2η, Πάτρα: ΕΑΠ.

Ξενόγλωσση

- Brar, T.P.S., Sharma, D. & Khurmi, S.S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *International Journal of Computing & Business Research*, Proceedings of 'I-Society 2012' at GKU, Talwandi Sabo Bathinda (Punjab).
- Bryman, A., 2016. *Social research methods*. 5th ed. Oxford: Oxford University Press.
- Creswell, J.W. & Creswell, J.D., 2018. *Research design: Qualitative, quantitative, and mixed methods approaches*. 5th ed. Thousand Oaks, CA: SAGE Publications.
- Saunders, M., Lewis, P. & Thornhill, A., 2019. *Research methods for business students*. 8th ed. Harlow: Pearson Education.
- Smith, R.E., 1997. *Internet Cryptography*. Boston: Addison-Wesley.

Άρθρα / Έρευνες / Εργασίες

- Batiz-Lazo, B., & Reid, R. J. (2011). The development of cash dispensers and ATMs in the UK, 1967–2005. IEEE Annals of the History of Computing, 33(3), 32–45.
- Chandran, R. (2014). Pros and cons of Mobile banking. International Journal of Scientific and Research Publications, Volume 4, Issue 10. Διαθέσιμο στο

διαδικτυακό τόπο: https://www.ijsrp.org/research-paper-1014/ijsrp-p34115.pdf [Πρόσβαση 25/1/2025]

- Chong, A. Y. L., Li, B., Ngai, E. W. T., Ch'ng, E., & Lee, F. (2021). Predicting online product sales via online reviews, sentiments, and promotion strategies: A big data architecture and neural network approach. *International Journal of Operations & Production Management*, 41(4), 444-468.
- Cordelia Jemima G.Y & Kavitha, V., 2020. Mobile Banking - Security Risks and Security Preventions. *International Journal of Computer Trends and Technology*, 68(11), pp.49-52. Διαθέσιμο στο διαδικτυακό τόπο: https://ijcttjournal.org/helium/ijctt/ijctt-v68i11p106 [Πρόσβαση 29/1/2025].
- Deloitte, 2020. *Digital Banking Maturity 2020*. Διαθέσιμο στο διαδικτυακό τόπο: https://www2.deloitte.com/global/en/pages/financial-services/articles/digital-banking-maturity.html [Πρόσβαση 20/1/2025]
- Deloitte, 2022. *Digital Banking Maturity 2022*. Deloitte. Διαθέσιμο στο διαδικτυακό τόπο: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-digital-banking-maturity-report-sep-22.pdf [Πρόσβαση 10/1/2025]
- Evans, J.R. & Mathur, A., 2018. The value of online surveys: A look back and a look ahead. *Internet Research*, 28(4), pp. 854-887. Διαθέσιμο στο διαδικτυακό τόπο: https://www.emerald.com/insight/content/doi/10.1108/intr-03-2018-0089/full/html [Πρόσβαση 15/1/2025]
- Federal Reserve Board. (2016). *Consumers and Mobile Financial Services.* Διαθέσιμο στο διαδικτυακό τόπο: https://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf [Πρόσβαση 20/1/2025]
- Fonseca, J. R. S. (2014), e-banking Culture: a Comparison of EU 27 Countries and Portuguese case in the EU 27 Retail Banking Context, Journal of Retailing and Consumer Services Volume 21, Issue 5, Pages 708-716)
- GAO, 2015. Cybersecurity: Bank and other depository regulators need to enhance oversight of financial institutions' cybersecurity programs. *U.S. Government Accountability Office (GAO)*. Διαθέσιμο στο διαδικτυακό τόπο: https://www.gao.gov/assets/gao-15-509.pdf [Πρόσβαση 20/12/2024].

- Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: Current Research and Future Research Directions. Journal of Business Economics, 87(5), 537–580.
- Guerreiro, M. (2011). Financial services innovation: the mobile dimension. ACI Payment System.
- ING International Survey. (2016). World on the move for mobile banking-Mobile Banking July 2016. ING.
- Laukkanen, T., 2007. Internet vs mobile banking: Comparing customer value perceptions. *Business Process Management Journal*, 13(6), pp. 788-797. Διαθέσιμο στο διαδικτυακό τόπο: https://www.researchgate.net/publication/242335914_Internet_vs_mobile_banking_Comparing_customer_value_perceptions [Πρόσβαση 10/1/2025].
- Μαυρογιάννης, Δ. (2003). *Ασφάλεια ηλεκτρονικών συναλλαγών.* Δελτίο ΕΕΤ, Γ' Τριμηνία
- Mattila, M. (2003). Factors Affecting The Adoption Of Mobile Banking Services. Journal of Internet Banking and Commerce, 149-160. Διαθέσιμο στο διαδικτυακό τόπο: https://www.researchgate.net/publication/26433997_Factors_Affecting_The_Adoption_Of_Mobile_Banking_Services [Πρόσβαση 13/12/2024]
- Molina-Castillo, F. J., López-Nicolás, C., & de Reuver, M. (2020). Mobile Payment: The Hiding Impact of Learning Costs on User Intentions. Electronic Commerce Research and Applications, 39, 100901.
- Scheau, M.C., Gabudeanu, L., Bricic, I., Apetri, L. & Bodescu, C.N., 2022. Risk-based approach in preventing mobile banking cyber-attacks. *25th RSEP International Conference on Economics, Finance & Business*, pp.52-68. Διαθέσιμο στο διαδικτυακό τόπο: https://doi.org/10.19275/RSEPCONFERENCES174 [Πρόσβαση 25/1/2025]
- Shaikh, A.A. & Karjaluoto, H. Mobile banking adoption: A literature review. *Telematics and Informatics,* 32 (2015), 129–142. Διαθέσιμο στο δικτυακό τόπο: https://jyx.jyu.fi/jyx/Record/jyx_123456789_45299 [Πρόσβαση 13/12/2024]
- Smutkupt, M., Krairit, D. & Esichaikul, V., 2010. Mobile marketing: Implications for marketing strategies. *International Journal of Mobile Marketing*, 5(2), pp. 1-16. Διαθέσιμο στο διαδικτυακό τόπο: https://www.researchgate.net/publication/312550624_Mobile_marketing_Implications_for_marketing_strategies [Πρόσβαση 25/1/2025].

- Venkatesh V., Davis F.D., (2000), A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science 46(2):186-204
- Venkatesh, V., Thong, J.Y.L. & Xu, X., 2012. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), pp. 157-178. Διαθέσιμο στο διαδικτυακό τόπο: https://aisel.aisnet.org/misq/vol36/iss1/13/ [Πρόσβαση 13/12/2024].
- Wan-Rung Lin Yi-Hsien Wang & Tzu-En Hung. (2012). Selecting Mobile Banking System Service for Consumers by Using a Combined DEMATEL and ANP Approach . *Journal of Accounting, Finance & Management Strategy, Vol. 7, No. 1,* , 1-14
- Webroot, 2014. The Risks and Rewards of Mobile Banking Apps. Διαθέσιμο στο διαδικτυακό τόπο: https://webroot-cms-cdn.s3.amazonaws.com/2914/5764/5019/risks_rewards_of_mobile_banking_apps_wp_us.pdf [Πρόσβαση 17/1/ 2025].
- Wodo, W., Blaskiewicz, P., Stygar, D. and Kuzma, N., 2021**.** Evaluating the security of electronic and mobile banking. *Διαθέσιμο στο διαδικτυακό τόπο :*, https://www-sciencedirect-com.proxy.eap.gr/science/article/pii/S136137232100107X [Πρόσβαση 20/1/2025]
- Zhao, Y., Teng, L., & Li, C. (2019). Online banking adoption in the age of Fintech: Evidence from an emerging economy. *Electronic Commerce Research and Applications, 38*, 100949.

Ηλεκτρονικές Πηγές Πληροφόρησης

Για ορισμούς και πληροφορίες χρησιμοποιήθηκε:

- ***https://www.investopedia.com/***
- **Ευρωβαρόμετρο (Eurobarometer)** *Ευρωπαϊκή Επιτροπή (European Commission). Ευρωβαρόμετρο: Χρήση ψηφιακών τραπεζικών υπηρεσιών στην Ευρώπη.* Διαθέσιμο στο: https://europa.eu/eurobarometer

- **Τράπεζα της Ελλάδος (Bank of Greece)** Τράπεζα της Ελλάδος, Εκθέσεις & Στατιστικά για τις ηλεκτρονικές συναλλαγές και το ψηφιακό τραπεζικό σύστημα. Διαθέσιμο στο: https://www.bankofgreece.gr
- **Ελληνική Ένωση Τραπεζών (Hellenic Bank Association - HBA),** Στατιστικά δεδομένα και αναφορές για την ανάπτυξη της ηλεκτρονικής τραπεζικής στην Ελλάδα. Διαθέσιμο στο: https://www.hba.gr
- **Powergame.gr (Οικονομικές αναλύσεις & τραπεζικά δεδομένα)** Άρθρα και αναφορές σχετικά με την εξέλιξη των ψηφιακών τραπεζικών υπηρεσιών στην Ελλάδα. Διαθέσιμο στο: https://www.powergame.gr

Για τις αντίστοιχες ενότητες στην εργασία χρησιμοποιήθηκαν :

- Alpha Bank, Διαθέσιμο στον δικτυακό τόπο: https://www.alpha.gr/
- Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στους δικτυακούς τόπους :
  - https://www.astynomia.gr/elliniki-astynomia/eidikes-ypiresies/diefthynsi-dioxis-ilektronikou-egklimatos/
  - https://cyberalert.gr/
- Εθνική Τράπεζα, Διαθέσιμο στον δικτυακό τόπο: https://www.nbg.gr/
- Eurobank, Διαθέσιμο στον δικτυακό τόπο: https://www.eurobank.gr/
- Πειραιώς Τράπεζα, Διαθέσιμο στον δικτυακό τόπο: https://www.ebanking.piraeusbank.gr/