ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΤΡΑΠΕΖΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
MBA-2011-2012

«Η ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ (ELECTRONIC BANKING) ΣΤΟ ΔΙΑΔΙΚΤΥΟ.ΤΡΟΠΟΙ ΥΛΟΠΟΙΗΣΗΣ, ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΧΡΗΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ EBANKING ΚΑΙ M-BANKING»

ΜΠΟΥΣΙΟΣ ΜΙΧΑΗΛ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΓΕΩΡΓΟΠΟΥΛΟΣ ΑΝΤΩΝΗΣ

ΑΘΗΝΑ 2012

Διπλωματική Εργασία *MBA-2011-2012*

Η ηλεκτρονική τραπεζική (electronic banking) στο διαδίκτυο. Τρόποι υλοποίησης, ασφάλειας και χρήση των ηλεκτρονικών υπηρεσιών e-banking και m-banking.

Μπούσιος Μιχαήλ

Περίληψη

Η ραγδαία εξέλιξη της τεχνολογίας και ο συνεχής ρυθμός αύξησης των χρηστών του διαδικτύου έχει φέρει μια αλλαγή στις συνήθειες και στον τρόπο λειτουργίας πολλών ανθρώπων. Νέες δυνατότητες και νέες ειδικότητες έχουν αναπτυχθεί στον εργασιακό τομέα, ειδικά με τη χρήση της πληροφορικής και με την ενοποίηση της παγκόσμιας αγοράς παρατηρείται ότι πλέον η αγορά εργασίας τείνει να μην έχει ανάγκη την ύπαρξη προσωπικής επαφής εργοδοτών και εργαζομένων γεγονός ότι έχει ωθήσει την αγορά στην παροχή περισσότερων υπηρεσιών μιας και το διαδίκτυο προσφέρεται σε πάνω από δύο (2) δισεκατομμύρια ενεργούς χρήστες του διαδικτύου. Ο αριθμός αυτός είναι σημαντικός καθώς μέρα με τη μέρα αυξάνεται λογαριθμικά, γεγονός που το διαδίκτυο αποτελεί έναν πόλο έλξης πολλών επαγγελματιών στο χώρο των χρηματοοικονομικών υπηρεσιών αλλά και πέραν από αυτόν. Μέσα σε αυτή την εξέλιξη, δε θα μπορούσαν να λείψουν και τα χρηματοπιστωτικά ιδρύματα με τη δημιουργία και την προβολή των προϊόντων τους δημιουργώντας τα κατάλληλα κανάλια επικοινωνίας μέσω διαδικτύου όπως είναι το e-banking αλλά και το mobile banking.

Η παρούσα διπλωματική επιχειρεί την ανάλυση των δύο καναλιών επικοινωνίας ώστε να γίνει κατανοητή η χρήση τους από τους αναγνώστες δηλαδή πώς ένας χρηματοοικονομικός φορέας όπως είναι και μια Τράπεζα, προσφέρει τις υπηρεσίες της μέσω κατάλληλων ενεργειών στους χρήστες διαμέσου του e-banking και mobile banking.

Στο πρώτο μέρος της εργασίας, έχει γίνει μια βιβλιογραφική ανασκόπηση στο ρόλο της τραπεζικής πληροφορικής, μια γενική ανασκόπηση από την εισαγωγή της πληροφορικής στα χρηματοπιστωτικά ιδρύματα και την εξέλιξη τους από εργαλείο μηχανογράφησης και αρχειοθέτησης εγγράφων σε εργαλείο παραγωγής συναλλαγών μέσω της διεύρυνσης της επιχειρηματικής λογικής με την παραγωγή κέρδους. Στη συνέχεια, γίνεται μια αναφορά στα ηλεκτρονικά συστήματα που χρησιμοποιεί μια τράπεζα με σκοπό ο αναγνώστης να κατανοήσει τη σπουδαιότητα της πληροφορικής στον τραπεζικό χώρο, αναφέρονται δηλαδή τα τμήματα που συνθέτουν έναν φορέα όπως επίσης και τα συστήματα πληρωμών που χρησιμοποιούνται εκτός τράπεζας με σκοπό τη μεταφορά χρημάτων μέσω τραπεζικών εντολών και μέσω εσωτερικού δικτύου των τραπεζών.

Στο δεύτερο μέρος της διπλωματικής, αναφερόμαστε στην ηλεκτρονική τραπεζική μέσω διαδικτύου (e-banking), από τον τρόπο που ένα σύστημα ηλεκτρονικής τραπεζικής συνδέεται στο διαδίκτυο μέχρι το τι βλέπει ένας τελικός χρήστης. Θέλουμε με αυτόν τον τρόπο να περάσουμε στον αναγνώστη τη στοιχειώδη γνώση εκείνη ώστε να κατανοήσει τον τρόπο που εκτελεί τις συναλλαγές του μέσω του διαδικτύου ώστε να είναι πιο «ασφαλής» στις επιλογές του και στον τρόπο χρήσης των υπηρεσιών.

Στο τρίτο μέρος της διπλωματικής, αναφερόμαστε στη χρήση του διαδικτύου μέσω κινητών και ιδίως των «έξυπνων κινητών» ή αλλιώς smartphones. Θέλουμε να εμβαθύνουμε τη γνώση του χρήστη στην λογική ότι πλέον η συσκευή κινητής τηλεφωνίας μπορεί να χρησιμοποιηθεί σε καθημερινές συναλλαγές με την Τράπεζα. Αναφερόμαστε σε αυτή την ενότητα στα είδη των προσφερόμενων εφαρμογών που παρέχουν οι Τράπεζες όπως επίσης και μια ανασκόπηση του mobile banking στις Ελληνικές Τράπεζες.

Στο τέταρτο μέρος αναφερόμαστε στην ασφάλεια των συναλλαγών. Προκειμένου ο χρήστης να εξοικειωθεί με τους κινδύνους που μπορεί να υπάρχουν όταν συναλλάσσεται μέσω διαδικτύου. Στη συγκεκριμένη ενότητα γίνεται μια αναφορά για τους τρόπους που κάποιος «ηλεκτρονικός εγκληματίας» προσπαθεί να αποσπάσει προσωπικά στοιχεία με σκοπό τη μεταφορά ποσών προς όφελός του είτε να κάνει «ζημιά» στα επιτιθέμενα συστήματα. Επιπλέον αναφέρουμε ενδεικτικά τι μέτρα λαμβάνει ένα χρηματοπιστωτικό ίδρυμα προκειμένου να προστατέψει τους πελάτες της, τα συστήματα της και σε τελική ανάλυση τη φήμη της. Τέλος, στο συγκεκριμένο κεφάλαιο, προτείνουμε στον χρήστη μερικές συμβουλές προκειμένου να φυλαχθεί από τους προαναφερόμενους κινδύνους.

Στο πέμπτο κεφάλαιο και τελευταίο, διεξήγαμε μια έρευνα με τη χρήση ηλεκτρονικού ερωτηματολογίου ανάμεσα στους χρήστες που κάνουν χρήση ηλεκτρονικών τραπεζικών συναλλαγών με σκοπό να δούμε κατά πόσο οι χρήστες είναι ενημερωμένοι και εξοικειωμένοι με τη χρήση του διαδικτύου για τη διεξαγωγή τραπεζικών συναλλαγών.

Λέξεις-κλειδιά: Τραπεζική πληροφορική, e-banking, m-banking, ασφάλεια δεδομένων, επιθέσεις συστημάτων, χρήση διαδικτυακών υπηρεσιών

Abstract

The rapid evolution of technology and the perpetually increasing number of internet users has brought a tremendous change in the habits and everyday activities of the people around the world. New capabilities and specialties have developed as far as the workforce is concerned, especially by the use of IT, and through the unification of the global economy it can be observed that the labor market tends to have less physical touch between the employers and the employees; thus more services are provided since internet is available to more than two (2) billion active users. This number is quite important because it rises every day logarithmically, making the internet an attractive place for many professionals in the area of the financial services and not only. Throughout this evolution, the financial institutions have also played a great role through the creation and presentation of their products by creating appropriate internet communication channels such as e–banking and mobile banking.

This project aims to analyze the above communication channels in order the readers can understand their usage; how a financial institute such as a Bank can provide services to its users by proper actions through e – banking and mobile banking. In the first part of the project there is a literature review of the role of internet banking, a general review of the introduction of IT in financial institutes and their evolution from a tool which provided paper based ways of working and archiving to a tool of transactional acts through the enlargement of the business logic to that of profit creation. Next, there is a reference to the electronic systems bank use so that the reader can understand the importance of IT in the banking area. Last but not least, the parts that constitute the bank and the transactional systems which are used outside the bank in order to transfer money through banking orders and through internal networks are mentioned.

In the second part of this project, electronic banking through internet (e – banking) is cited, beginning from the way an electronic banking system is connected on the internet to what the final user can see. The main purpose is to provide the reader the elementary knowledge he/she needs in order to understand the way transactions are performed through the internet and therefore be more ‘safe’ according to his/her choices and the way he/she uses the services.

In the third part, the use of internet through mobile phones and especially through smartphones is mentioned. The reason is to deepen the knowledge of the user and

make him/her understand that mobile phones can also be used through daily transactions with a Bank. Through this unit the different kinds of applications Banks offer are referred and a review of mobile banking (m – banking) in Greek Banks is developed.

In the fourth part transaction safety issues are cited so that the user can be familiarized with the dangers he/she might have to deal while trading online. In this unit the different ways a 'digital criminal' can obtain personal data in order to harm transaction systems for personal profit are presented. Some indicative measures a bank can take in order to protect its clients, systems and reputation are mentioned and last, advice for the users in order to protect themselves from the dangers mentioned above is given.

In the last unit, a survey through the use of a questionnaire is conducted in a reasonable number of users who make use of electronic banking transactions in order to understand how informed and familiar are in the use of internet for their transactions.

Περιεχόμενα

Εισαγωγή

Οι περισσότεροι επαγγελματικοί κλάδοι και ειδικότερα ο Τραπεζικός κλάδος στην προσπάθεια εξέλιξης και βελτίωσης των υπηρεσιών τους, εισήγαγαν στην επιχειρηματική τους στρατηγική και υπηρεσίες πληροφορικής αναπτύσσοντας νέες μεθόδους επιχειρηματικών δράσεων. Η «Τραπεζική πληροφορική» όπως μπορούμε να ονομάσουμε τον αντίστοιχο κλάδο, είναι βασικό πλέον κομμάτι κάθε τράπεζας στις καθημερινές συναλλαγές είτε με τους πελάτες της, είτε με τους εσωτερικούς της πελάτες (διάφορες υπηρεσίες της τράπεζας), είτε με εξωτερικές υπηρεσίες (π.χ. συστήματα πληρωμών, ισοτιμία νομισμάτων, συνεδριάσεις χρηματιστηρίων κλπ).

Σκοπός της διπλωματικής εργασίας είναι να εξετάσουμε τους τομείς της τραπεζικής πληροφορικής και ειδικότερα εκείνους τους τομείς που αφορούν νέες τεχνολογίες αλληλεπίδρασης με τους πελάτες της τράπεζας μέσω διαδικτύου όπως είναι το e-banking και mobile banking. Η απεικόνιση της σωστής πληροφορίας προς αυτά τα δύο κανάλια επικοινωνίας όπως και η μετέπειτα υποστήριξη των πελατών, στηρίζεται σε διάφορα επιμέρους συστήματα τα οποία αλληλεπιδρούν («συνεργάζονται») προκειμένου ο τελικός χρήστης (πελάτης της τράπεζας) να έχει πλήρη εικόνα του χαρτοφυλακίου που διαθέτει στην τράπεζα.

Στη συγκεκριμένη διατριβή θα αναφερθούμε στα συστήματα και τα τμήματα της τράπεζας τα οποία εμπλέκονται προκειμένου να εκτελεστούν οι τραπεζικές εργασίες μέσω του e-banking και m-banking. Ένα σύστημα ηλεκτρονικής τραπεζικής όπως είναι το e-banking χρησιμοποιεί επιμέρους συστήματα τα ώστε να ολοκληρώσει τις συναλλαγές. Τα συστήματα που θα αναφερθούμε είναι τα συστήματα πληρωμών και μεταφορά χρημάτων όπως το διατραπεζικό σύστημα ΔΙΑΣ, σύστημα πληρωμών SWIFT και το Ευρωπαϊκό σύστημα SEPA. Τα συστήματα e-banking και m-banking λόγω της άμεσης πρόσβασης στα συστήματα των τραπεζών, θα πρέπει να διαθέτει παράλληλα και μηχανισμούς ασφαλείας ώστε να διασφαλίζεται η σωστή μετάδοση της πληροφορίας με ασφάλεια στον τελικό αποδέκτη. Λόγω της έκθεσης στο διαδίκτυο, τα συστήματα των τραπεζών, δέχονται τακτικά επιθέσεις, στη συγκεκριμένη διπλωματική κρίνουμε σκόπιμο να αναφερθούμε στις μεθόδους ασφαλείας που παρέχουν τα τραπεζικά συστήματα όπως επίσης και οι μέθοδοι και κανόνες προφύλαξης που ένας χρήστης θα πρέπει τηρεί στα δικά του συστήματα πρόσβασης στο διαδίκτυο. Προκειμένου ο αναγνώστης να αντιληφθεί το πως μια οποιαδήποτε συναλλαγή υλοποιείται στα πλαίσια της ενημέρωσης, θεωρούμε ότι

πρέπει να αναφέρουμε τα εμπλεκόμενα τμήματα που λαμβάνουν μέρος προκειμένου μια συναλλαγή να διεκπεραιωθεί. Τέλος, έρευνα που απευθύνθηκε ηλεκτρονικά στα πλαίσια της διπλωματικής με σκοπό τη διερεύνηση της χρήσης των συστημάτων ηλεκτρονικής τραπεζικής και κατά πόσο ένας χρήστης είναι ενημερωμένος με τη νέα τεχνολογία, παρουσιάζεται στο τελευταίο μέρος.

1. Τραπεζική Πληροφορική

Ο τραπεζικός κλάδος την τελευταία εικοσαετία με την εισαγωγή και την χρήση της πληροφορικής άλλαξε ουσιαστικά τον τρόπο λειτουργίας του. Παραδοσιακά, η άσκηση των τραπεζικών δραστηριοτήτων γίνονταν με τη χρήση του "χαρτιού" σε όλες τις δυνατές μορφές του (έντυπα, επιστολές, συμβάσεις, τίτλοι αξίας κλπ). Μετά την εμφάνιση της Μηχανογράφησης, η παραδοσιακή χρήση του "χαρτιού" ως βασικής παραμέτρου για την άσκηση των τραπεζικών δραστηριοτήτων περιορίζεται συνεχώς και τείνει να εξαφανισθεί

Η διεξαγωγή των τραπεζικών εργασιών και δραστηριοτήτων, η οποία σήμερα στηρίζεται καθοριστικά στην Πληροφορική Τεχνολογία (**Information Technology - "I.T."**) και την ευρύτατη χρήση των ηλεκτρονικών υπολογιστών (Η/Υ.), αναφέρεται συνήθως με τον ξενόγλωσσο όρο "**electronic banking**". Το "electronic banking" επεκτείνεται ταχύτατα στη σύγχρονη λειτουργία των τραπεζών, με την αξιοποίηση των δυνατοτήτων που προσφέρονται από τη ραγδαία εξελισσόμενη τεχνολογία της πληροφορικής [1].

Έχοντας οι τράπεζες ως έρεισμα την τεχνολογία, παρέχουν τη δυνατότητα πρόσβασης των πελατών τους σ' ένα ευρύ φάσμα χρηματοοικονομικών υπηρεσιών, προσφορά που προτιμά όλο και μεγαλύτερο μερίδιο της αγοράς και ιδιαίτερα τα νεαρά άτομα της ηλικίας. Η νέα εποχή του **self service banking** προϋποθέτει ένα μέρος των συναλλαγών να το υλοποιεί από μόνος του ο πελάτης [3].

Οι συνήθεις μορφές που λαμβάνει το electronic banking είναι οι ακόλουθες :

- Τα A.T.M. **(**Automated teller machine), ό**π**υ ο πελάτης έχει τη δυνατότητα να κάνει ανάληψη/καταθεση μετρητών όπως επίσης να εκτελέσει τραπεζικές υπηρεσίες που περιλαμβάνουν πληρωμές λογαριασμών και μεταφορές χρημάτων.
- τα EFT/POS, συσκευές ηλεκτρονικών πληρωμών στα σημεία πωλήσεων

- το remote banking, η εξ αποστάσεως διενέργεια συναλλαγών
- το home banking, οι συναλλαγές μέσω προσωπικών οικιακών υπολογιστών.
- το phone banking, οι συναλλαγές με επικοινωνία μέσω τηλεφωνικών συσκευών από τους πελάτες χρησιμοποιώντας κατάλληλους κωδικούς
- Internet Banking, οι συναλλαγές με τη χρήση υπολογιστή μέσω διαδικτύου
- Mobile Banking, οι συναλλαγές με τη χρήση κινητών συσκευών μέσω Internet

1.1. Κίνητρα της τραπεζικής πληροφορικής

Βασικά κίνητρα για την εισαγωγή της πληροφορικής στις τράπεζες ήταν τα ακόλουθα :

- η μείωση του χρόνου διεκπεραίωσης των εργασιών
- η καλύτερη οργάνωση και η πιο αξιόπιστη τήρηση των στοιχείων
- η καλύτερη εξυπηρέτηση των πελατών και πληροφόρηση της διοίκησης
- η πίεση του ανταγωνισμού από τις άλλες τράπεζες.

Κατά την περίοδο που οι πρώτες τράπεζες ξεκινούσαν τη μηχανογράφηση τους, η χρήση της τεχνολογίας χρησιμοποιούνταν προκειμένου να διευκολύνει το προσωπικό από τις χρονοβόρες εργασίες που είχαν σχέση με την επεξεργασία τεράστιων όγκων παραστατικών. Το πρόβλημα με την πάροδο των ετών, διογκωνόταν αφού ο όγκος των συναλλαγών αυξανόταν με μεγάλο ρυθμό άρα χρειαζόταν περισσότερο προσωπικό για την επεξεργασία παραστατικών με πολλά ανθρώπινα λάθη κατά την επεξεργασία. Με την εισαγωγή της νέας τεχνολογίας, τα προβλήματα αυτά ξεπεράστηκαν γρήγορα, ενώ μειώθηκαν σημαντικά οι πιθανότητες ύπαρξης λάθους στα αποτελέσματα των επεξεργασιών. Εκτός από την καλύτερη πληροφόρηση και αποτελεσματικότητα, σημαντικό ρόλο στις αποφάσεις της διοίκησης των τραπεζών έπαιξε και ο βαθμός εξυπηρέτησης που πρόσφερε στην πελατεία της. Έτσι, βλέποντας και οι άλλες τράπεζες τα οφέλη που πρόσφερε ο τομέας της πληροφορικής στην γρήγορη, αξιόπιστη και σύγχρονη εξυπηρέτηση των πελατών, προχώρησαν με τη σειρά τους στην υιοθέτηση της πληροφορικής για τη βελτίωση της

λειτουργικότητάς τους και αποδοτικότητάς τους. Με τον τρόπο αυτό, τα μερίδια της αγοράς τους αυξήθηκαν και τα οικονομικά τους μεγέθη βελτιώθηκαν με συνέπεια τη βελτίωση της ανταγωνιστικότητας τους.

Στις μέρες μας καμιά τράπεζα δεν μπορεί να ξεκινήσει τη λειτουργία της χωρίς την ύπαρξη ενός ισχυρού τομέα πληροφορικής, που θεωρείται θεμελιώδης προϋπόθεση για την αποτελεσματική, αξιόπιστη και επικερδή λειτουργία της.

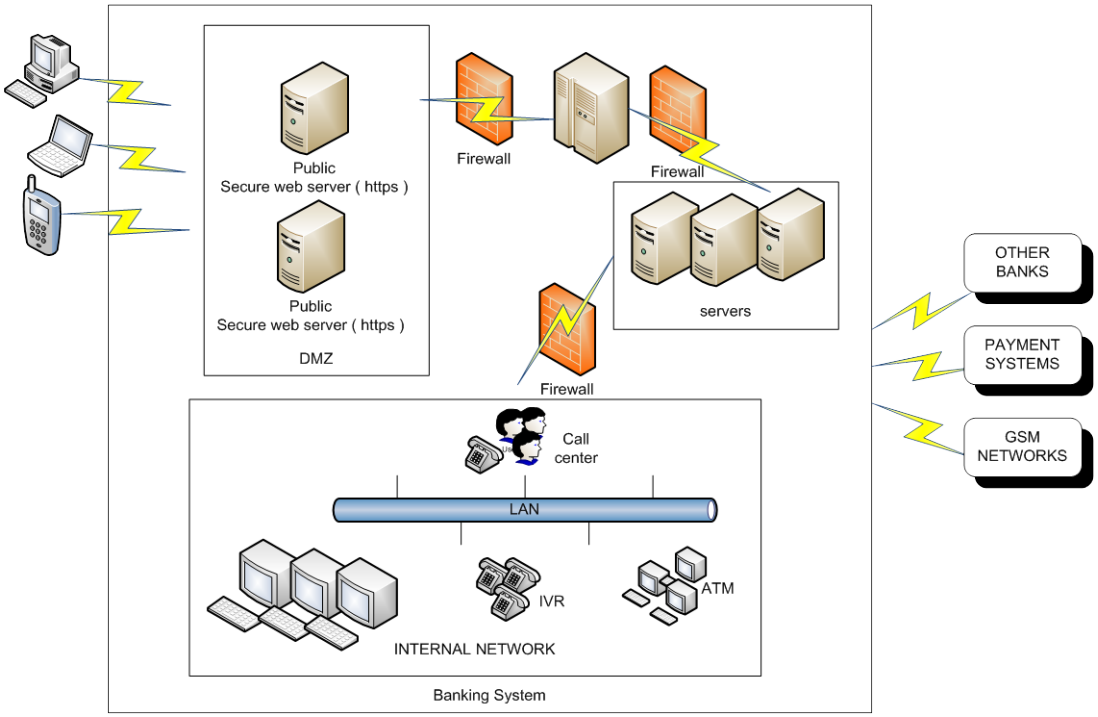
1.1.1 Ηλεκτρονικά συστήματα που εμπλέκονται στην Τραπεζική πληροφορική

Η πληροφορική σε ένα χρηματοπιστωτικό ίδρυμα, χρησιμοποιείται σε όλες τις δραστηριότητές της. Με τη χρήση νέων τεχνολογιών, οι τράπεζες είναι σε θέση να παρέχουν μεγάλο μέρος από τα προϊόντα του με πολύ χαμηλότερο κόστος συγκριτικά με το παραδοσιακό τραπεζικό σύστημα.

Μια τυπική δομή μιας τράπεζας δε διαφέρει συγκριτικά με συστήματα μεγάλων επιχειρήσεων. Η διαφορά μεταξύ αυτών των δύο είναι ότι τα συστήματα των τραπεζών ελέγχονται ανά τακτά χρονικά διαστήματα ώστε να διασφαλίζουν συνεχή ροή πληροφοριών παρέχοντας ασφάλεια δεδομένων. Ενδεικτικά μπορούμε να απεικονίσουμε ένα τυπικό τραπεζικό σύστημα το οποίο περιλαμβάνει τα τμήματα της τράπεζας όπως και τις διασυνδέσεις μεταξύ των συστημάτων. Ένα τραπεζικό σύστημα περιλαμβάνει κεντρικές βάσεις δεδομένων προκειμένου να αντλούν πληροφορίες. Οι διασυνδέσεις ανάλογα με την χρήση διαφοροποιούνται. Έτσι, λ.χ. όταν πρόκειται για εφαρμογές που είναι εκτεθειμένες προς το κοινό μέσω διαδικτύου, η πληροφόρηση είναι περιορισμένη και μόνο για τις ανάγκες των εφαρμογών. Για λόγους ασφαλείας, το εσωτερικό δίκτυο της τράπεζας, από τέτοιου είδους εφαρμογές αποκόπτεται και επιτρέπονται μόνο λειτουργίες πρόσβασης στα δεδομένα αυτά. Για το λόγο αυτό οι πολλοί οργανισμοί χρησιμοποιούν «ζώνες πρόσβασης» το λεγόμενο DMZ [11] (Demilitarized Zone in Computer Networking). Το DMZ στην ασφάλεια των υπολογιστικών συστημάτων, είναι ένα φυσικό ή λογικό μέσο δικτύου, το οποίο διασυνδέεται με το υπάρχον δίκτυο μιας επιχείρησης αλλά και με δίκτυα που είναι εκτεθειμένα σε κίνδυνο (συνήθως διαδίκτυο). Η χρήση ενός DMZ είναι

χρειάζεται προκειμένου να προστεθεί ένα επιπλέον επίπεδο δικτύου για την αύξηση της ασφάλειας πρόσβασης σε δεδομένα κυρίως εμπιστευτικά. Βέβαια, η περιγραφή στη συγκεκριμένη διπλωματική είναι μόνο καθαρά για πληροφόρηση, στην πράξη ένας οργανισμός θα μπορούσε να διαθέτει πληθώρα τέτοιων δικτύων ώστε να διασφαλίζει την ασφάλεια των δεδομένων. Στο σχηματικό διάγραμμα που ακολουθεί, διακρίνουμε τη σύνδεση των διαφόρων τμημάτων με τα σχετικά συστήματα ώστε να παρέχουν υπηρεσίες υποστήριξης και εξυπηρέτησης προς τους πελάτες της επιχείρησης. Τέτοιες υπηρεσίες είναι είτε ηλεκτρονικές είτε με απευθείας επικοινωνία με το ανθρώπινο δυναμικό της επιχείρησης (στην προκειμένη περίπτωση μια Τράπεζα). Οι ηλεκτρονικές υπηρεσίες μπορεί να διαχωρίζονται σε :

- Υποστήριξη προς τους πελάτες π.χ. με τη χρήση του τηλεφωνικού κέντρου όπου ο πελάτης εισάγει τα στοιχεία του, γίνεται αναγνώριση ηλεκτρονική και μπορεί να κάνει περιορισμένες ενέργειες.
- Υποστήριξη προς άλλα συστήματα. Τέτοια συστήματα μπορεί να είναι :
    - Η σύνδεση με συστήματα πληρωμών για την αποστολή και παραλαβή εμβασμάτων ή άλλων πληρωμών.
    - Η σύνδεση με συστήματα αποστολής ειδοποιήσεων
    - Η σύνδεση με συστήματα online όπως παρακολούθηση της συνεδρίασης του χρηματιστηρίου σε πραγματικό χρόνο.
    - Σύνδεση με συστήματα άλλων τραπεζών (π.χ. σύνδεση με θυγατρικές τράπεζες του ίδιου ομίλου μέσω εσωτερικού δικτύου).



Σχήμα 1.1 Τυπικό σύστημα ενός τραπεζικού φορέα

1.1.2 EFT/POS

Μια σχετικά διαδεδομένη εφαρμογή στο χώρο της εμπορίας προϊόντων μαζικής κατανάλωσης (μεγάλα καταστήματα, σουπερ μάρκετ κτλ), είναι τα συστήματα σημείου πώλησης. Η έμφαση στα σημεία αυτά δίνεται στις λιανικές πωλήσεις οι οποίες καταχωρούνται στον υπολογιστή στο σημείο όπου πραγματοποιείται η πώληση. Ειδικά τερματικά (POS terminals), που δεν είναι τίποτα άλλο από εξελιγμένες ταμειακές μηχανές, επιτρέπουν την αυτόματη εκτέλεση των παρακάτω εργασιών:

- Αναζήτηση τιμής πώλησης
- Υπολογίσμοί (τιμή Χ ποσότητα, αθροίσματα αξιών, εκπτώσεων, φόρων)
- Επεξεργασία πιστώσεων και επιστροφών
- Καταγραφή δοσοληψιών.

Πολλά συστήματα POS είναι εφοδιασμένα ή αντικαθίστανται από συσκευές εισαγωγής δεδομένων οι οποίες χρησιμεύουν ως τερματικά που δέχονται δεδομένα με τον έναν από τους δυο τρόπους :

- Πληκτρολόγηση
- Ανάγνωση γραμμωτού κώδικα (barcode)

Από την άλλη οπτική γωνία, τα EFT/POS είναι συστήματα που δημιουργούν χρηματοοικονομικές ροές στον εμπορικό κόσμο και εξασφαλίζουν μεγαλύτερη ασφάλεια. Οι σημερινοί στόχοι των τραπεζών μέσω της υλοποίησης τέτοιων συστημάτων είναι :

- Πληρωμές χωρίς μετρητά και χρήση φυσικού χαρτιου·
- Μείωση των κρουσμάτων απάτης και εξασφάλιση μεγαλύτερης ασφάλειας στις συναλλαγές
- Διοικητικά οφέλη στον επιχειρηματικό κόσμο
- Εξασφάλιση μεγαλύτερου παραγωγικού χρόνου για τους πελάτες και τους επιχειρηματίες.

Οι υπηρεσίες που προσφέρονται μέσω των EFT/POS είναι δυνατό να καλύπτουν ένα μεγάλο μέρος εύρος συναλλαγών. Για μερικές ευρωπαϊκές τράπεζες τα συστήματα αυτά θεωρούνται ως μέσο μεταφοράς ποσών μεταξύ τρεχούμενων λογαριασμών-από τον πελάτη στον πωλητή τη στιγμή της πώλησης (Real time), αν και σήμερα η μεταφορά αυτή μπορεί να έχει συμφωνηθεί να εκτελεστεί κατά το τέλος της ημέρας ή ακόμη και κατά τις επόμενες ημέρες.

Τα οφέλη που αποκομίζουν με τη χρήση των EFT/POS ανά κατηγορία συναλλασσομένων είναι :

Για τους λιανοπωλητές-εμπόρους (retailers) :

- Αύξηση της ταχύτητας συναλλαγής στα σημεία ελέγχου και πώλησης
- Εγγυημένη είσπραξη των οφειλών
- Ταχεία είσπραξη των οφειλών-αύξηση της ρευστότητας
- Μεγαλύτερη ασφάλεια στις συναλλαγές από τη μη χρήση των μετρητών
- Μείωση του όγκου του χαρτιού όπως αντίστοιχα και του χρόνου επεξεργασίας των συναλλαγών
- Μείωση των εξόδων – προμηθειών προς τις Τράπεζες
- Διαθεσιμότητα πληροφοριών για τον καλύτερο προγραμματισμό, έλεγχο και διοίκηση-διαχείρηση της επιχείρησης.

Για τις Τράπεζες :

- Περιορισμός της ουράς μέσα στις τράπεζες, του χρόνου αναμονής των πελατών στα ταμεία για αναλήψεις
- Περιορισμός της απάτης

- Μείωση του όγκου του χαρτιού
- Μείωση των λειτουργικών δαπανών της τράπεζας
- Δυνατότητα διάθεσης νέων προϊόντων και υπηρεσιών
- Διεύρυνση της καταναλωτικής βάσης

Για τους καταναλωτές

- Η ευκολία στις συναλλαγές τους
- Η ευελιξία και η ταχύτητα στις συναλλαγές τους.

1.1.3 Α.Τ.Μ. Αυτόματες Ταμειολογιστικές Μηχανές (Automated Teller Machines)

Προσφέρουν βασικές τραπεζικές υπηρεσίες στους πελάτες των τραπεζών στα σημεία όπου είναι εγκατεστημένα, κατά τη διάρκεια όλου του 24ώρου. Τα Α.Τ.Μ. έχουν γίνει πλήρως αποδεκτά και χρησιμοποιούνται ευρύτατα. Μηχανές που έδιναν μετρητά είχαν τοποθετηθεί και χρησιμοποιηθεί στην Αμερική από τα μέσα της δεκαετίας του 1960. Στη Μεγάλη Βρετανία (cash dispensers) έγιναν ευρύτατα γνωστές στις αρχές της δεκαετίας του 1970. Όπως συμβαίνει και για τις μηχανές ηλεκτρονικής μεταφοράς κεφαλαίων (Electronic Funds Transfer – EFT) , αλλά και οι περισσότερες πηγές βιβλιογραφίας ορίζουν το ATM ως τη μηχανή που δίνει μετρητά (cash dispenser) και παρέχει μερικές συμπληρωματικές υπηρεσίες.

Οι προσφερόμενες υπηρεσίες από τα ATMs διαφέρουν κατά πολύ. Σε γενικές γραμμές ένα ATM μπορεί να προσφέρει τις παρακάτω υπηρεσίες:

- Ανάληψη μετρητών και ενημέρωση λογαριασμών
- Κατάθεση μετρητών και επιταγών
- Μεταφορά χρημάτων μεταξύ λογαριασμών
- Αναλυτική κίνηση λογαριασμών
- Ενημέρωση υπολοίπου λογαριασμού
- Εκτύπωση υπολοίπου
- Πληρωμή λογαριασμών με αυτόματη χρέωση λογαριασμού

Η λίστα αυτή είναι ενδεικτική και δεν έχει στόχο να καταγράψει όλες τις συναλλαγές που πραγματοποιούνται μέσω των ATM. Τα σύγχρονα ATM στις περισσότερες περιπτώσεις είναι πολύ «έξυπνα» μηχανήματα και λειτουργούν

τόσο σε on-line όσο και σε off-line. Τελευταία διαθέτουν υπολογιστές ώστε σε περίπτωση βλάβης τους να μπορούν απομακρυσμένα να διορθώνονται όταν είναι εφικτό από το κατάλληλο προσωπικό.

1.1.4 Home banking

Η λειτουργία του home banking με την ανάπτυξη του διαδικτύου αφορά την εξυπηρέτηση πελατών (κυρίως εταιριών) μέσω ενός κατάλληλου λογισμικού ώστε η κάθε επιχείρηση που έχει εγκαταστήσει το λογισμικό, να συνδέεται απ' ευθείας με τις υπηρεσίες των τραπεζών. Το λογισμικό, έπρεπε να καλύπτει μια μεγάλη ποικιλία υπολογιστών (hardware) και λειτουργικών συστημάτων, αντίστοιχη με τις πλατφόρμες που προϋπήρχαν.

Το home banking (ή αλλιώς PC-banking), δίνει στους πελάτες να πραγματοποιούν διάφορες συναλλαγές, όπως το να πληρώνουν τους λογαριασμούς, να ενημερώνονται για τα υπόλοιπα των λογαριασμών, την πώληση και αγοράς ομολόγων και αμοιβαίων κεφαλαίων και χρεογράφων.

Οι υπηρεσίες home banking ξεκίνησαν στις αρχές του 1980 και εκ' τότε έχουν αυξηθεί παράλληλα με την αύξηση της χρήσης των υπολογιστών που με τον καιρό έγιναν πιο εύχρηστοι και προσιτοί στους πελάτες των τραπεζών. Η δυνατότητα συναλλαγών με την τράπεζα από το σπίτι οποιαδήποτε στιγμή της ημέρας είχε κάνει το home banking μια ελκυστική εναλλακτική μέθοδο των χρηματοοικονομικών υπηρεσιών. Το 1990, τα χρηματοπιστωτικά ιδρύματα, διεύρυναν τις υπηρεσίες home banking δίνοντας στους πελάτες τους απευθείας πρόσβαση σε υπηρεσίες τραπεζικές μέσω διαδικτύου επιτρέποντας σε πολλούς να κάνουν συναλλαγές τους από οπουδήποτε.

1.1.5 Phone banking (IVR – Interactive Voice Response)

Κατά τη διάρκεια της τελευταίας δεκαετίας, η εξέλιξη της πληροφορικής οδήγησε σε μια πρόοδο και στον τομέα της διαχείρισης φωνητικών ή μη εντολών μέσω τηλεφώνου. Το IVR αποτελεί ένα σύστημα που επιτρέπει την άμεση αλληλεπίδραση του καλούντα με το πληροφοριακό υλικό που είναι αποθηκευμένο στη βάση δεδομένων ή δημιουργείται δυναμικά με τη χρήση της τεχνολογίας TTS (Text to Speech). Η αλληλεπίδραση αυτή είναι εφικτή με δύο τρόπους, τα

συστήματα DTMF (Dual Tone Multi Frequency) και την αναγνώριση της φωνής του καλούντα.

Η πρώτη λύση χρησιμοποιεί το τονικό σύστημα για την εισαγωγή εντολών μέσω του πληκτρολογίου του τηλεφώνου. Ο χρήστης με την κλήση σε έναν αριθμό DNIS (Dialed Number Information Service) και μετά από ένα ηχογραφημένο ή δυναμικά δημιουργημένο μήνυμα, ακολουθεί τις οδηγίες και με τα πλήκτρα του τηλεφώνου επιλέγει τις επιλογές από το αντίστοιχο μενού.

Τα σήματα DTMF, χρησιμοποιούνται για τη μετάδοση των τηλεφωνικών εντολών μέσα από τις γραμμές του δικτύου φωνής σε ένα κέντρο που δρομολογεί όλες τις εισερχόμενες ροές.

Η δεύτερη λύση είναι παρόμοια με τα σήματα DTMF με τη διαφορά ότι επιτρέπει στον καλούντα να προηγηθεί στο μενού των διαθέσιμων επιλογών απλά με τη φωνή του, χρησιμοποιώντας προκαθορισμένες λέξεις ή φράσεις.

Το IVR Banking αρχικοποιείται με την πραγματοποίηση κλήσεων του πελάτη των εναλλακτικών δικτύων σε έναν προκαθορισμένο αριθμό και , μέσω τηλεπικοινωνιακού φορέα, η σύνδεση του με τον εξυπηρετητή της Τράπεζας. Οι διαθέσιμες επιλογές για την διεκπεραίωση των συναλλαγών μέσω τηλεφώνου είναι είτε με τη σύνδεση του call center της τράπεζας και συνομιλία με κάποιον τηλεφωνικό αντιπρόσωπο (παραδοσιακό phone banking) είτε με τη χρήση του συστήματος επιλογών μέσω πλήκτρων είτε με την αξιοποίηση του συστήματος αναγνώρισης φωνής.

Μία από τις πιο συνηθισμένες συναλλαγές μιας Τράπεζας, είναι η μεταφορά ποσών από λογαριασμό σε λογαριασμό του ίδιου πελάτη, Με τη χρήση του IVR, ο πελάτης επικοινωνεί με το τηλεφωνικό κέντρο της Τράπεζας μέσω του σταθερού ή κινητού του τηλεφώνου και ακολουθώντας τις οδηγίες θα πρέπει να δηλώσει το χρηματικό ποσό που επιθυμεί να μεταφέρει, όπως και τους λογαριασμούς που θα εμπλακούν στη συναλλαγή. Αυτή η διαδικασία συνήθως γίνεται με τη βοήθεια του πληκτρολογίου και έχει σαν αποτέλεσμα την ανταλλαγή μη φωνητικών εντολών με την πύλη φωνής (voice gateway). Η πύλη, αφού μετατρέψει τις τονικές επιλογές του χρήστη σε δεδομένα κατανοητά από το λειτουργικό σύστημα της Τράπεζας και ελέγξει τα στοιχεία του πελάτη (ταυτοποίηση), αποστέλλει τα δεδομένα στον εξυπηρετητή της Τράπεζας.

1.1.6 electronic banking

Οι καθημερινές χρηματοοικονομικές συναλλαγές μεταξύ πελατών – επιχειρηματιών και μη και τραπεζών αποτελούν τον κύριο όγκο των τραπεζικών λειτουργιών. Αυτές είναι επίσης και κύρια πηγή κόστους, αλλά και πιθανών λαθών.

Οι σύγχρονες τεχνολογίες πληροφορικής μπορούν να αυξήσουν την αποδοτικότητα των καθημερινών λειτουργιών και να επιτρέψουν την ευρεία διανομή των υπηρεσιών.

Στις μέρες μας το ανθρώπινο δυναμικό των τραπεζών κοστίζει περισσότερο από τις μηχανές. Η τεχνολογία δεν πρέπει να περιορίζεται μόνο στους υπαλλήλους για την καλύτερη εξυπηρέτηση των πελατών αλλά και για την μείωση των εξόδων, αλλά θα πρέπει να χαράσσεται μια πολιτική που να οδηγεί έναν μεγάλο αριθμό συναλλαγών μέσω των **συστημάτων αυτοεξυπηρέτησης** (self-service).

Με τον προσανατολισμό προς την αυτοεξυπηρέτηση, ο ίδιος ο πελάτης δημιουργεί τη συναλλαγή. Τα δεδομένα μεταφέρονται μέσω ηλεκτρονικών δικτύων επικοινωνίας και δημιουργούν τις κατάλληλες χρεώσεις, πιστώσεις και ελέγχους. Με αυτόν τον τρόπο αρκετές συναλλαγές δεν χρειάζονται προσωπικό διεκπεραίωσης.

Με το electronic banking περιορίζεται ο αριθμός των συναλλασσομένων στα γκισέ των τραπεζών. Λόγω του e-banking οι τράπεζες δεν έχουν ανάγκη να χρησιμοποιούν έγγραφα ως μηχανισμό μεταφοράς στοιχείων και αποθήκευσης δεδομένων για αναλήψεις και απλές τραπεζικές συναλλαγές. Παραμένει όμως η ανάγκη των πελατών είτε να επισκέπτονται το τραπεζικό κατάστημα, όπου συνεργάζονται για σύνθετες τραπεζικές εργασίες και διαπραγμάτευση των όρων συνεργασίας τους, είτε να χρησιμοποιούν σε πολλές περιπτώσεις τραπεζικά έγγραφα που επιβάλλονται από τα συναλλακτικά ήθη και τις διοικητικές ρυθμίσεις (συναλλαγματικές, χρεόγραφα, τίτλους, φορτωτικές, αποδείξεις, και έντυπα που αποδεικνύουν τη γνησιότητα τους από υπογραφές).

1.1.7 Internet Banking

Είναι γεγονός ότι τα τελευταία χρόνια έχουν συσταθεί και λειτουργούν τράπεζες που παρέχουν σε παγκόσμια κλίμακα τις υπηρεσίες τους αποκλειστικά και μόνο μέσω Διαδικτύου, χωρίς να έχουν φυσική παρουσία στην επικράτεια ενός ή περισσοτέρων κρατών μέσω ίδρυσης καταστημάτων. Πρόκειται για τις εικονικές

τράπεζες ή Internet only banks. Η απλούστατη και πιο διαδεδομένη μορφή παρουσίας συνίσταται στη διαμόρφωση της **απλής ηλεκτρονικής σελίδας**, μέσα από την οποία τόσο οι πελάτες της τράπεζας όσο και το επενδυτικό και αποταμιευτικό κοινό αντλούν πληροφορίες σχετικά με τη λειτουργία και τις υπηρεσίες του τραπεζικού οργανισμού.

Λόγω ότι μελέτη του Internet Banking αποτελεί μελέτη της υπάρχουσας διπλωματικής, θα αναφερθούμε εκτενέστερα στη συνέχεια της εργασίας.

1.1.8 Mobile Banking

Με την εξέλιξη της τεχνολογίας και την ενσωμάτωση των υπηρεσιών του διαδικτύου ως υπηρεσίας που διατίθεται από τους πάροχους στις συσκευές κινητής τηλεφωνίας, οι τράπεζες έχουν προχωρήσει και αναπτύξει εκείνα τα εργαλεία που παρέχουν συνοπτική πληροφόρηση στους πελάτες που κάνουν χρήση των υπηρεσιών (κινητής τηλεφωνίας).

Οι τράπεζες πάντα ήθελαν να προσφέρουν στους πελάτες τους τη δυνατότητα συναλλαγών εκτός γκισέ και το phone banking ήταν από τις πρώτες υπηρεσίες που προσφέρθηκαν προτού καν αναπτυχθεί και το Internet Banking [18].

Οι πρώτες προσπάθειες για παροχή υπηρεσιών τραπεζικής σε κινητά χαμηλής ανάλυσης (τα πρώτα κινητά δηλαδή που είχαν πρόσβαση στο διαδίκτυο), ήταν η χρήση του πρωτοκόλλου WAP (wireless application protocol). Σύντομα εγκαταλείφτηκε η συγκεκριμένη ιδέα λόγω ότι οι συγκεκριμένες υπηρεσίες ήταν δύσχρηστες.

Βλέποντας οι εταιρίες κινητής τηλεφωνίας την ανάγκη χρήσης του διαδικτύου περισσότερο, προχώρησαν σε δίκτυα $2^{ης}$ γενιάς (2G) όπου η μετάδοση της πληροφορίας πέρασε από το αναλογικό σήμα σε ψηφιακό σήμα [22]. Πολλές εταιρίες κινητής τηλεφωνίας, κατασκεύασαν συσκευές που υποστήριζαν το συγκεκριμένο δίκτυο και ένα νέο πρωτόκολλο μετάδοσης πληροφορίας GPRS (General Packet Radio Service) χρησιμοποιήθηκε μέσω αυτού του δικτύου με ταχύτητες από 56 kbit/δευτερόλεπτο 115 kbit/δευτερόλεπτο.

Η επόμενη γενιά δικτύων 3G (3^{rd} generation) αποτέλεσε ίσως το μεγαλύτερο άλμα στη διάδοση φωνής, διαδικτύου, τηλεόρασης μέσω κινητών τηλεφώνων. Με ταχύτητες που φθάνουν μέχρι τα 14.4 Mbits/δευτερόλεπτο, είναι ταχύτητες ικανοποιητικές για τη μετάδοση μεγαλύτερης πληροφορίας. Έτσι με τα

τελευταίου είδους «έξυπνα κινητά» ο χρήστης μπορεί να εκμεταλλευτεί μέσα από το κινητό του υπηρεσίες όπως :

- Υψηλές ταχύτητες
- Εμπλουτισμένες υπηρεσίες ήχου και εικόνας
- Τηλεδιάσκεψη
- Υψηλές ταχύτητες διαδικτύου και WAP
- IPTV (Τηλεόραση μέσω διαδικτύου)

Με τη χρήση του δικτύου 3G εκμεταλλευόμενοι και τις δυνατότητες των «έξυπνων τηλεφώνων», πολλές τράπεζες προχώρησαν στη διάθεση προγραμμάτων κατάλληλων για τη χρήση των κινητών προσφέροντας υπηρεσίες τραπεζικής κατάλληλες για τη χρήση των κινητών.

1.2 Συστήματα πληρωμών

Στην ηλεκτρονική Τραπεζική και γενικά σε κάθε τραπεζικό σύστημα, η διακίνηση χρημάτων γίνονται μέσα από διασυνδεμένα ηλεκτρονικά συστήματα μεταξύ Τραπεζικών Ιδρυμάτων. Τα συστήματα αυτά ελέγχονται από κεντρικούς οργανισμούς υπηρεσίες και ακολουθούν δικούς τους κανόνες (π.χ. SWIFT, SEPA).

Κάθε σύστημα πληρωμών που είναι διαθέσιμο στο Ελληνικό Τραπεζικό σύστημα μπορεί να χρησιμοποιηθεί και στα συστήματα e-banking. Μέσω των συστημάτων αυτών, ένας πελάτης μπορεί να στείλει κάποιο έμβασμα σε οποιοδήποτε λογαριασμό που μπορεί να βρίσκεται είτε εντός Ελλάδας (μέσω τραπεζικών συστημάτων ΔΙΑΣ), εντός Ευρωπαϊκής Ένωσης (μέσω του συστήματος SEPA), εκτός Ευρωπαϊκής Ένωσης ή εκτός Ζώνης τους Ευρώ μέσω του συστήματος SWIFT (Society for Worldwide Interbank Financial Telecommunication).

1.2.1 S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication)

Ο οργανισμός SWIFT χειρίζεται ένα παγκόσμιο σύστημα ανταλλαγής μηνυμάτων μεταξύ τραπεζών και άλλων χρηματοοικονομικών ιδρυμάτων. Ο

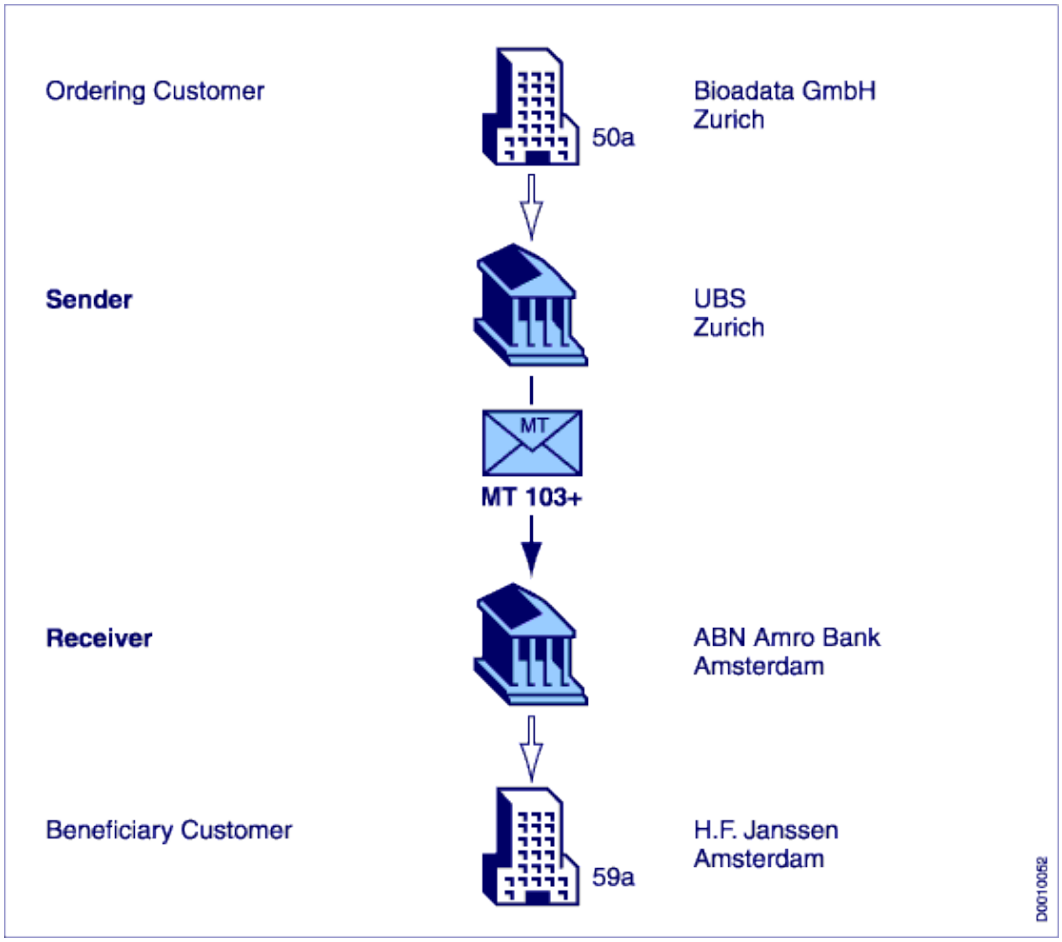
οργανισμός SWIFT επίσης χειρίζεται το λογισμικό και τις υπηρεσίες με τα χρηματοοικονομικά ιδρύματα μέσω του δικτύου SWIFTNet. Κάθε Τράπεζα αποκτά ή χρηματοοικονομικός οργανισμός αποκτά ένα αναγνωριστικό κωδικό, τον λεγόμενο BIC (business identifier code) σύμφωνα με ISO 9362:2009, γνωστός και ως «SWIFT CODE».[4] Αυτοί οι κωδικοί χρησιμοποιούνται για να την αποστολή μέσω δύο Τραπεζών (ή χρηματοοικονομικών οργανισμών), χρημάτων. Η αποστολή γίνεται με την ανταλλαγή κατάλληλου τύπου μηνύματος (SWIFT message) το οποίο περιέχει μία γραμμογράφηση ανάλογα με τον τύπο του μηνύματος, καθορισμένη από τον οργανισμό SWIFT. Έτσι, π.χ. όταν κάποιος θέλει να στείλει ένα έμβασμα σε μια τράπεζα στο εξωτερικό, θα πρέπει να γνωρίζει εκτός από τον λογαριασμό που θέλει να μεταφερθούν, αλλά και το αναγνωριστικό της Τράπεζας που θα σταλούν τα χρήματα. Από την πλευρά της εντολοδόχου τράπεζας, θα σχηματιστεί ένα μια γραμμογράφηση η οποία θα περιέχει όλα τα στοιχεία της αποστολής του εμβάσματος και θα αποσταλεί μέσω του δικτύου SWIFTNet. Το μήνυμα στη συνέχεια θα επεξεργαστεί από την παραλήπτρια τράπεζα και θα αποστείλει ένα απαντητικό μήνυμα έτσι ώστε να γίνει η αντίστοιχη χρέωση του ποσού στον αποστολέα ή η απόρριψη του μηνύματος.

Το σύστημα SWIFTNet, χειρίζεται μέχρι στιγμής δέκα κατηγορίες μηνυμάτων βασιζόμενοι στα SWIFT Standards τα οποία προσαρμόζονται κάθε χρόνο σύμφωνα με τις νέες ανάγκες των χρηματοπιστωτικών ιδρυμάτων.

Message Type	***Description***
MT0xx	**System Messages**
MT1xx	**Customer Payments and Cheques**
MT2xx	**Financial Institution Transfers**
MT3xx	**Treasury Markets**
MT4xx	**Collection and Cash Letters**
MT5xx	**Securities Markets**
MT6xx	**Treasury Markets - Metals and Syndications**
MT7xx	**Documentary Credits and Guarantees**
MT8xx	**Travellers Cheques**
MT9xx	**Cash Management and Customer Status**

Σχήμα 1.2 Κατηγορίες μηνυμάτων SWIFT

Κάθε μήνυμα που αποστέλλεται, ανήκει σε μία από τις δέκα κατηγορίες, έτσι π.χ. όταν στέλνει μια τράπεζα μια εντολή μεταφοράς χρημάτων, αποστέλλεται ένα μήνυμα τύπου MT103. Το μήνυμα αυτό θα ελεγχθεί για την ορθότητα του και θα αποσταλεί όπως προαναφέραμε στο δίκτυο SWIFTNet ακολουθώντας σχηματικά την πορεία που βλέπουμε στο παρακάτω σχήμα [6]:



Σχήμα 1.3 Απεικόνιση αποστολής μηνύματος SWIFT

Ο Οργανισμός SWIFT, εξυπηρετεί μέχρι στιγμής πάνω από 9700 τραπεζικούς οργανισμούς, χρηματοπιστωτικά ιδρύματα και εταιρικούς πελάτες σε 209 χώρες διακινώντας καθημερινά εκατομμύρια «οικονομικά μηνύματα»[7].

Ο οργανισμός SWIFT επιτρέπει στους «πελάτες» της την αυτοματοποίηση και προτυποποίηση των χρηματοοικονομικών τους συναλλαγών με χαμηλό κόστος μειώνοντας τον λειτουργικό κίνδυνο.

1.2.2 Ενιαίος Χώρος Πληρωμών σε Ευρώ (Single Euro Payments Area – SEPA).

Με την εισαγωγή του Ευρώ σε φυσική μορφή στις χώρες του Ευρώ το 2002, δημιουργήθηκε η ανάγκη για ενιαίο σύστημα πληρωμών και μεταφοράς χρημάτων εντός της Ευρωζώνης. Έτσι, η ευρωπαϊκή τραπεζική κοινότητα δημιούργησε το Ευρωπαϊκό Συμβούλιο πληρωμών και ξεκίνησε το έργο που καλείται SEPA. Ο SEPA είναι ένας χώρος στον οποίο οι καταναλωτές, οι εταιρίες και οι λοιποί οικονομικοί παράγοντες θα είναι σε θέση να διενεργούν και να δέχονται εγχώριες και διασυνοριακές πληρωμές σε ευρώ με τους ίδιους βασικούς όρους και τα ίδια δικαιώματα και υποχρεώσεις ανεξάρτητα από τη γεωγραφική τους θέση. Σκοπός του SEPA είναι η δημιουργία μιας ενοποιημένης, ανταγωνιστικής και καινοτόμου αγοράς πληρωμών μικρής αξίας στον ευρωπαϊκό χώρο, όπου οι πληρωμές σε ευρώ χωρίς μετρητά θα διενεργούνται με τη χρήση ενός μόνο τραπεζικού λογαριασμού και μιας ενιαίας δέσμης μέσων πληρωμών [8].

Η λειτουργία των μηνυμάτων μέσω του SEPA στηρίζεται στη δημιουργία κανόνων με χρήση xml[1] μηνύματα βασίζοντας στο πρότυπο ISO 20022. [9]

1.2.3 Διατραπεζικά συστήματα ΔΙΑΣ

Η εταιρεία ΔΙΑΤΡΑΠΕΖΙΚΑ ΣΥΣΤΗΜΑΤΑ (ΔΙΑΣ) Α.Ε. [9] ιδρύθηκε στις 28 Ιουνίου 1989, με πρωτοβουλία της Ελληνικής Ένωσης Τραπεζών.

Η ΔΙΑΣ έχει αναπτύξει και λειτουργεί το σύστημα πληρωμών ΔΙΑΣ μέσω του οποίου διακινούνται και εκκαθαρίζονται ηλεκτρονικά διατραπεζικές πληρωμές τόσο εντός της χώρας όσο και διασυνοριακά.

Το σύστημα πληρωμών ΔΙΑΣ ταξινομείται στα συστήματα πληρωμών μικρής αξίας με εξέχουσα σημασία (Prominently Important Retail Payment Systems - PIRPS) σύμφωνα με τα πρότυπα επίβλεψης της Ευρωπαϊκής Κεντρικής Τράπεζας και βρίσκεται υπό την επίβλεψη της Τράπεζας της Ελλάδος.

[1] XML (Extensible Markup Language) είναι μια γλώσσα σήμανσης που περιέχει ένα σύνολο κανόνων για την ηλεκτρονική κωδικοποίηση κειμένων.

Αποτελείται από ένα σύνολο εργαλείων πληρωμών ως ακολούθως:

- μεταφορές πίστωσης,
- άμεσες χρεώσεις,
- επιταγές,
- συναλλαγές σε ATM,
- πληρωμές με κάρτες.

Στο σύστημα πληρωμών ΔΙΑΣ συμμετέχουν εμπορικές τράπεζες και η Τράπεζα της Ελλάδος όπως προβλέπεται στον κανονισμό λειτουργίας του συστήματος.

1.2.4 Γενικά περί συστημάτων πληρωμών

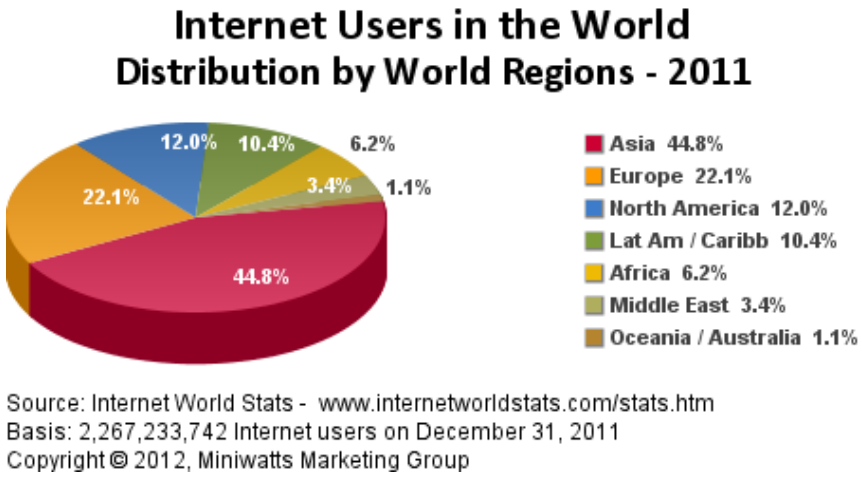
Τα συστήματα πληρωμών έχουν ως σκοπό την αυτοματοποίηση της κάθε συναλλαγής ενός χρηματοπιστωτικού τομέα. Ανάλογα με τον τύπο της πληρωμής, οι φορείς και κυρίως οι τράπεζες, διοχετεύουν τις αντίστοιχες εντολές πληρωμής προς τα κατάλληλα κανάλια επικοινωνίας. Έτσι π.χ. αν κάποιος πελάτης θέλει να στείλει κάποια χρήματα προς μια άλλη τράπεζα του εξωτερικού, η τράπεζα αφού λάβει την εντολή είτε μέσω διαδικτύου π.χ. e-banking, είτε μέσω ενός συνδεδεμένου συστήματος σε κάποιο κατάστημα ή εξουσιοδοτημένο εκπρόσωπο, θα δημιουργήσει κατάλληλο μήνυμα, δηλαδή μια γραμμογράφηση που θα περιλαμβάνει όλα τα στοιχεία του παραλήπτη αλλά και του αποστολέα και θα το στείλει στο δίκτυο SWIFT. Μόλις το δίκτυο παραλάβει το μήνυμα και στείλει την αντίστοιχη εντολή πληρωμής στον προορισμό με σκοπό να πιστωθεί ο αντίστοιχος λογαριασμός, επιστρέφει ανάλογο μήνυμα ότι παραλήφθηκε είτε απορρίφθηκε ώστε να αντιλογιστεί ο λογαριασμός του καταθέτη. Άλλο ένα παράδειγμα, με το νέο σύστημα πληρωμών SEPA, ο πελάτης θα επιλέξει να στείλει χρήματα ή να πληρώσει λογαριασμό παροχής υπηρεσιών (π.χ. αντίστοιχος λογαριασμός τηλεπικοινωνιών) σε άλλη χώρα εντός Ευρωζώνης. Η διαδικασία που ακολούθησε στο πρώτο παράδειγμα, είναι ακριβώς η ίδια και σε αυτή την περίπτωση, δηλαδή θα καταχωρήσει τα στοιχεία πληρωμής και τον προορισμό και αυτόματα η εντολή θα επεξεργαστεί από τα συστήματα της Τράπεζας, θα δημιουργηθεί το κατάλληλο μήνυμα στη νέα του μορφή (xml)

που δέχεται το σύστημα πληρωμών SEPA και θα διαβιβάσει το μήνυμα στον αντίστοιχο δίκτυο.

Γενικά παρατηρούμε ότι η διαδικασία για μια μεταφορά χρημάτων από την πλευρά του πελάτη έχει γίνεται όσο το δυνατόν πιο απλή ώστε να μπορεί να στείλει άμεσα τις συγκεκριμένες εντολές. Οι κάθε φορείς που διαχειρίζονται τις αντίστοιχες εντολές, διαθέτουν κατάλληλο προσωπικό και μέσα ώστε να μπορούν να κατανοήσουν κάθε φορά τις υποδομές και τους κανόνες που θέτουν τα συστήματα πληρωμών.

2. e-banking Ηλεκτρονική Τραπεζική με τη χρήση του Ίντερνετ

Η ραγδαία εξέλιξη του διαδικτύου έφερε την επανάσταση στο τρόπο λειτουργίας των συναλλαγών σε παγκόσμιο επίπεδο. Έρευνα δείχνει ότι το Δεκέμβριο του 2011 οι χρήστες διαδικτύου ανέρχονται παγκοσμίως τα 2.267 εκατομμύρια χρήστες (πηγή www.internetworldstats.com) με αύξηση μέσα σε μια δεκαετία σε ποσοστό 528,1% με στο σύνολο των χρηστών που χρησιμοποιούν διαδίκτυο που αναλογεί στο 32.7% του πληθυσμού. Στην ίδια έρευνα παρατηρούμε ότι στην Ελλάδα, το ποσοστό χρήσης του διαδικτύου φτάνει στο 46,9% ανάμεσα σε 10.760.136 εγγεγραμμένους κατοίκους. Η συγκεκριμένη έρευνα δείχνει ότι το διαδίκτυο ως μέσο επικοινωνίας και αποτελεί πλέον ένα από τα σημαντικότερα κανάλια επικοινωνίας σύμφωνα με το οποίο, η χρήση του αυξάνεται καθημερινά και γίνεται αποδεκτό από περισσότερο κόσμο.



Σχήμα 2.1 Χρήστες διαδικτύου

WORLD INTERNET USAGE AND POPULATION STATISTICS December 31, 2011						
World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	139,875,242	13.5 %	2,988.4 %	6.2 %
Asia	3,879,740,877	114,304,000	1,016,799,076	26.2 %	789.6 %	44.8 %
Europe	816,426,346	105,096,093	500,723,686	61.3 %	376.4 %	22.1 %
Middle East	216,258,843	3,284,800	77,020,995	35.6 %	2,244.8 %	3.4 %
North America	347,394,870	108,096,800	273,067,546	78.6 %	152.6 %	12.0 %
Latin America / Carib.	597,283,165	18,068,919	235,819,740	39.5 %	1,205.1 %	10.4 %
Oceania / Australia	35,426,995	7,620,480	23,927,457	67.5 %	214.0 %	1.1 %
WORLD TOTAL	6,930,055,154	360,985,492	2,267,233,742	32.7 %	528.1 %	100.0 %

Σχήμα 2.2 Χρήστες διαδικτύου

Internet and Facebook Usage in Europe					
EUROPE	Population (2011 Est.)	Internet Users, 31-Dec-11	Penetration (% Population)	Users % in Europe	Facebook 31-Mar-12
Albania	2,994,667	1,441,928	48.1 %	0.3 %	1,060,760
Andorra	84,825	68,740	81.0 %	0.0 %	36,760
Austria	8,217,280	6,143,600	74.8 %	1.3 %	2,766,540
Belarus	9,577,552	4,436,800	46.3 %	0.9 %	409,120
Belgium	10,431,477	8,489,901	81.4 %	1.7 %	4,634,220
Bosnia-Herzegovina	4,622,163	1,955,277	42.3 %	0.4 %	1,268,560
Bulgaria	7,093,635	3,464,287	48.8 %	0.7 %	2,386,800
Croatia	4,483,804	2,656,089	59.2 %	0.5 %	1,452,300
Cyprus	1,120,489	584,863	52.2%	0.1 %	553,860
Czech Republic	10,190,213	7,220,732	70.9 %	1.4 %	3,502,420
Denmark	5,529,888	4,923,824	89.0 %	1.0 %	2,835,120
Estonia	1,282,963	993,785	77.5 %	0.2 %	447,620
Faroe Islands	49,267	37,500	76.1 %	0.0 %	29,880
Finland	5,259,250	4,661,265	88.6 %	0.9 %	2,078,880
France	65,102,719	50,290,226	77.2 %	10.0 %	23,544,460
Germany	81,471,834	67,364,898	82.7 %	13.5 %	22,123,660
Gibraltar	28,956	20,200	69.8 %	0.0 %	18,800
Greece	10,760,136	5,043,550	46.9 %	1.0 %	3,562,120
Guernsey & Alderney	65,068	48,300	74.2 %	0.0 %	440
Hungary	9,976,062	6,516,627	65.3 %	1.3 %	3,751,300
Iceland	311,058	304,129	97.8 %	0.1 %	210,220
Ireland	4,670,976	3,122,358	66.8 %	0.6 %	2,093,960
Italy	61,016,804	35,800,000	58.7 %	7.1 %	20,889,260
Jersey	94,161	45,800	48.6 %	0.0 %	820
Kosovo	1,825,632	377,000	20.7 %	0.1 %	n/a
Latvia	2,204,708	1,540,859	69.9 %	0.3 %	319,300
Liechtenstein	35,236	28,826	81.8 %	0.0 %	11,880
Lithuania	3,535,547	2,103,471	59.5 %	0.4 %	983,440
Luxembourg	503,302	459,833	91.4 %	0.1 %	190,020
F.Y.R.O.M.	2,077,328	1,069,432	51.5 %	0.2 %	879,540
Malta	408,333	262,404	64.3 %	0.1 %	191,940
Man, Isle of	84,655	35,600	42.1 %	0.0 %	30,660
Moldova	4,314,377	1,429,154	33.1 %	0.3 %	221,220
Monaco	30,539	23,000	75.3 %	0.0 %	36,800
Montenegro	661,807	328,375	49.6 %	0.1 %	292,700
Netherlands	16,847,007	15,071,191	89.5 %	3.0 %	5,759,840
Norway	4,691,849	4,560,572	97.2 %	0.9 %	2,561,820
Poland	38,441,588	23,852,486	62.0 %	4.8 %	7,524,220
Portugal	10,760,305	5,455,217	50.7 %	1.1 %	4,174,000
Romania	21,904,551	8,578,484	39.2 %	1.7 %	4,161,340
Russia	138,739,892	61,472,011	44.3 %	12.3 %	5,237,420
San Marino	31,817	17,000	53.4 %	0.0 %	8,240
Serbia	7,310,555	4,107,000	56.2 %	0.8 %	3,173,440
Slovakia	5,477,038	4,337,868	79.2 %	0.9 %	1,889,160
Slovenia	2,000,092	1,420,776	71.0 %	0.3 %	670,660
Spain	46,754,784	30,654,678	65.6 %	6.1 %	15,682,800
Svalbard & Jan Mayen	2,019	n/a	n/a	n/a	n/a
Sweden	9,088,728	8,441,718	92.9 %	1.7 %	4,519,780
Switzerland	7,639,961	6,430,363	84.2 %	1.3 %	2,727,600
Turkey	78,785,548	35,000,000	44.4 %	7.3 %	30,963,100
Ukraine	45,134,707	15,300,000	33.9 %	3.1 %	1,686,500
United Kingdom	62,698,362	52,731,209	84.1 %	10.5 %	30,470,400
Vatican City State	832	480	57.7 %	0.0 %	20
TOTAL Europe	816,426,346	500,723,686	61.3 %	100.0 %	235,525,280

Σχήμα 2.3 Χρήστες διαδικτύου στην Ευρώπη

Από την παραπάνω έρευνα παρατηρο ψιε ό **τ** με την αύξηση χρήσης το υ διαδικτύου, αυξήθηκε και η ζήτηση για περισσότερες υπηρεσίες μέσω διαδικτύου. Παρατηρούμε ότι οι υπηρεσίες με τον καιρό έχουν γίνει πιο φιλικές και προσιτές σε όλες τις κατηγορίες των χρηστών. Πολλές εταιρίες ανάμεσα σε αυτές και οι Τραπεζικοί οργανισμοί, επενδύουν τεράστια ποσά στην προσέλκυση πελατών και για αναβαθμίσεις συστημάτων που παρέχουν τέτοιου είδους υπηρεσίες όπως είναι και το e-banking.

Το «e-Banking» ως όρος, αναφέρεται στην ικανότητα ενός συνδρομητή του διαδικτύου να έχει πρόσβαση σε ένα τραπεζικό σύστημα και να μπορεί να χρησιμοποιεί της υπηρεσίες τους μέσω διαδικτύου από το σπίτι του, υπηρεσίες που παλαιότερα χρειαζόταν τη φυσική παρουσία του χρήστη σε κάποιο κατάστημα της Τράπεζας.

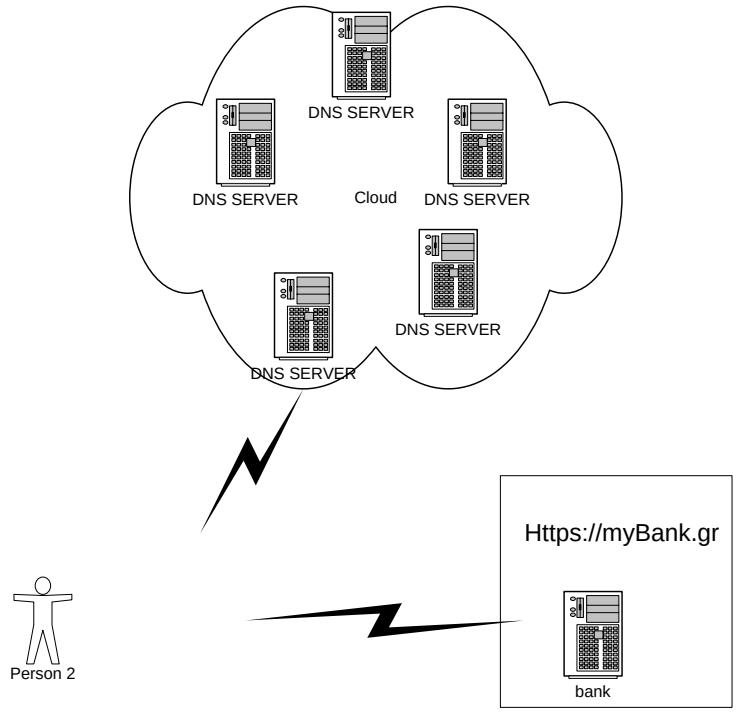
Για να αντιληφθούμε πώς λειτουργεί ένα σύστημα e-banking θα αναλύσουμε στη συνέχεια με απλά λόγια, τον τρόπο που ένα σύστημα χρησιμοποιείται από τους χρήστες, τα τμήματα που συνεργάζονται προκειμένου να συντηρούν την εφαρμογή όπως και ένα παράδειγμα πώς λειτουργεί εσωτερικά η διαδικασία υλοποίησης ενός προϊόντος διαθέσιμο στο e-banking.

2.1 Τι είναι το “e-Banking”

Για να κατανοήσουμε τι εννοούμε με την έννοια e-Banking θα πρέπει να δούμε από τι αποτελείται ένα σύστημα e-Banking. Ας αρχίσουμε λοιπόν με τον τρόπο χρήσης μιας απλής μορφής ιστοσελίδας στο διαδικτύου ώστε να κατανοήσουμε και τον τρόπο λειτουργίας του συγκεκριμένου καναλιού (e-banking). Οι περισσότεροι χρήστες που ασχολούνται με το διαδίκτυο γνωρίζουν τη χρήση ενός φυλομετρητή ή αλλιώς browser (π.χ. Internet Explorer, Firefox κλπ). Τη στιγμή που θέλουν να προσπελάσουν μια ιστοσελίδα, επιλέγουν την κατάλληλη εφαρμογή δηλαδή ένα φυλομετρητή (browser), πληκτρολογούν την επιθυμητή διεύθυνση και έπειτα από αναμονή μερικών δευτερολέπτων, εμφανίζεται η ιστοσελίδα. Αυτό είναι το θεμιτό και επιθυμητό αποτέλεσμα. Τεχνικά όμως, η διαδικασία μεταφοράς της ιστοσελίδας στον υπολογιστή είναι ένας από τους ρόλους του διαδικτύου. Πώς μεταφράζεται αυτό δηλαδή; Όταν ο χρήστης πληκτρολογήσει μια διεύθυνση π.χ. http://www.myAddress.com, λόγω ότι είναι δύσκολο να θυμάται αριθμούς, αυτόματα η http://www.myAddress.com

μεταφράζεται σε διεύθυνση από τέσσερις τριψήφιους αριθμούς XXX.YYY.ZZZ.WWW (π.χ. 192.168.1.1) όπου ένας διακομιστής (DNS server) κάνει αυτή τη μετάφρασή, δηλαδή ανακτά τον αριθμό με βάση μια λίστα με διευθύνσεις και αριθμούς που διαθέτει για το διαδίκτυο. Σε περίπτωση υπαρκτής διεύθυνσης, θα επιστρέψει την αντιστοιχία των αριθμών πίσω στον φυλομετρητή και ο «φυλομετρητής» θα συνδεθεί στον συγκεκριμένο server ειδάλλως θα προσπαθήσει από ανακτήσει τη διεύθυνση από αντίστοιχους διακομιστές (servers) όταν πρόκειται για διεύθυνση που αντιστοιχεί σε κόμβο εξωτερικού. Αν όλα αποτύχουν, θα επιστραφεί ένα μήνυμα λάθους στο χρήστη ότι θα πρέπει να ελέγξει τη διεύθυνση που έχει πληκτρολογήσει. Σε περίπτωση που εντοπιστεί η διεύθυνση, τότε η φυλομετρητής «ρωτάει» τον διακομιστή (server) αν υπάρχει η συγκεκριμένη ιστοσελίδα και επιστρέφει η απάντηση στο χρήστη, δηλαδή επιστρέφουν οδηγίες στον φυλομετρητή ώστε να σχεδιάσει στον χρήστη τη σελίδα με τα αντίστοιχα χρώματα και εικόνες.

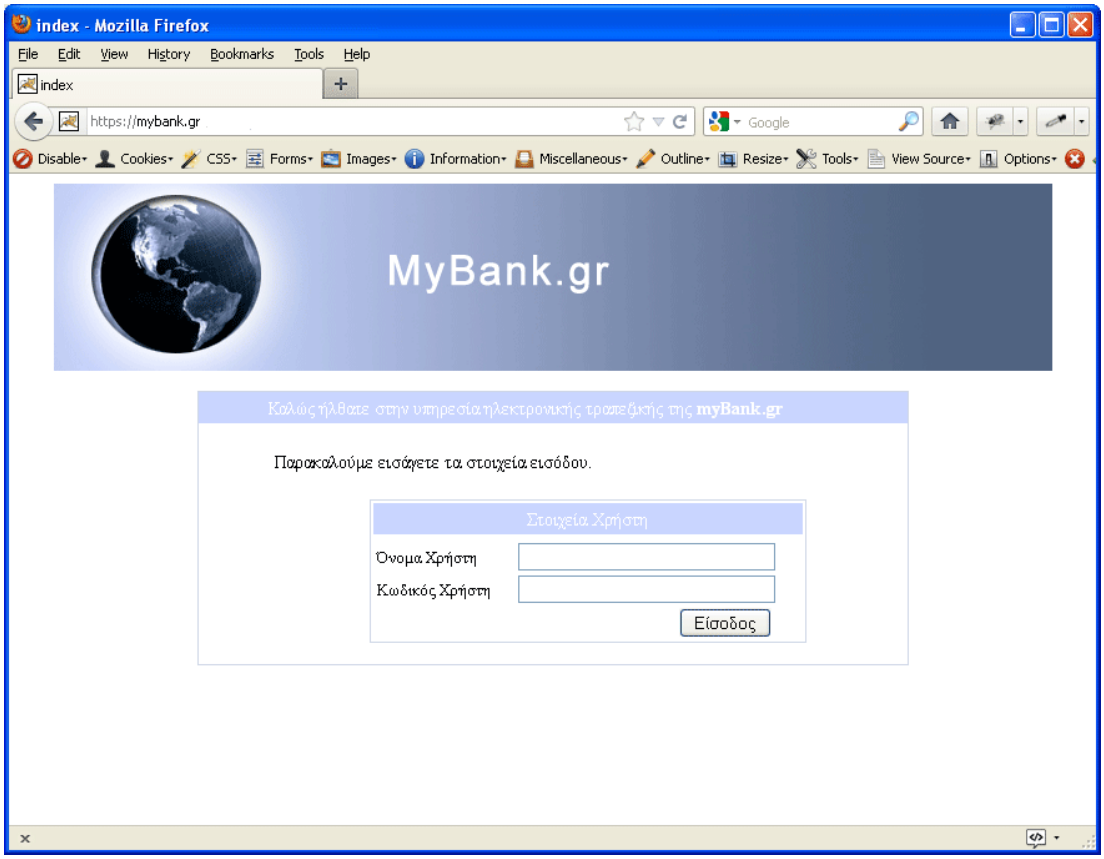
Οι «οδηγίες» προς το φυλομετρητή στην ουσία είναι ένας κώδικας κατανοητός από τον browser βασιζόμενος σε πρότυπα που έχει δημιουργήσει ο οργανισμός w3c (World wide web consortium – www.w3.org) που ονομάζεται html (Hypertext Markup Language) όπου σύμφωνα με αυτή τη γλώσσα έχει χτιστεί η δομή των ιστοσελίδων του διαδικτύου. Η μεταφορά του κώδικα στον φυλομετρητή από τον διακομιστή (server) γίνεται μέσω κάποιων οδηγιών το λεγόμενο πρωτόκολλο http (Hypertext Transfer Protocol) ενώ για τις ασφαλείς συνδέσεις χρησιμοποιείται το πρωτόκολλο https (Hypertext Transfer Protocol Secure).


DNS SERVER
DNS SERVER
Cloud
DNS SERVER
DNS SERVER
DNS SERVER
Https://myBank.gr
Person 2
bank

οποίος παραβιάσει ενδιάμεσα κάποια επικοινωνία, η πληροφορία που θα υποκλαπεί δεν είναι ευανάγνωστη δηλαδή άχρηστη και δεν μπορεί να κάνει κάποια ενέργεια εις βάρος του χρήστη.

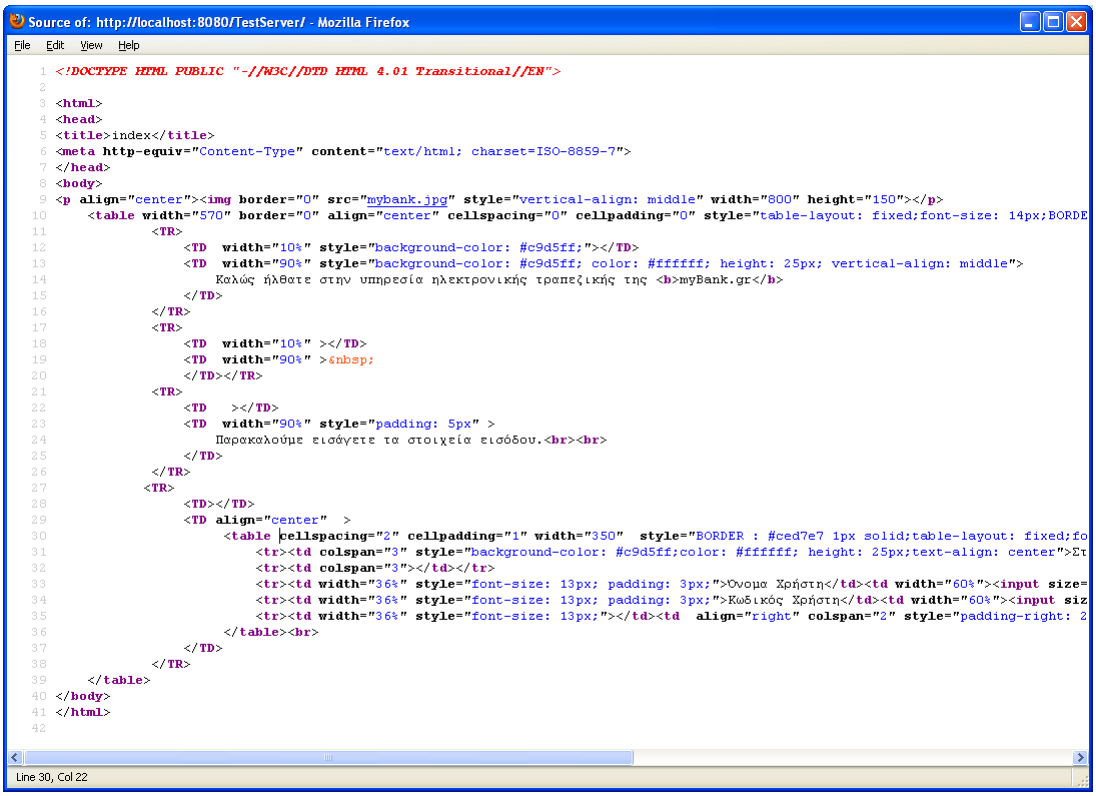
Ένα τραπεζικό σύστημα e-banking δε διαφέρει σε τίποτα από τα παραπάνω, ακολουθεί τον τρόπο κατασκευής των ιστοσελίδων σε μορφή html λόγω ότι οι φυλομετρητές αναγνωρίζουν μόνο αυτού του είδους μορφή γλώσσας. Σε πολλά συστήματα τραπεζών όμως (servers) οι ιστοσελίδες τους που σχεδιάζονται μπορεί να δημιουργούνται σε διάφορων τύπου γλώσσες προγραμματισμού, ωστόσο, το παραγόμενο αποτέλεσμα πρέπει να είναι κατάλληλο για να το αναγνωρίζει ο browser.

Ένα παράδειγμα για να το κατανοήσουμε καλύτερα, ένας χρήστης πληκτρολογεί τη διεύθυνση της τράπεζας σε έναν φυλομετρητή. Για να δούμε πιο αναλυτικά πληκτρολογεί για παράδειγμα https://www.myBank.gr. Στο σχήμα 2.5 εμφανίζεται η οθόνη εισόδου στο χρήστη προκειμένου να καταχωρήσει τα στοιχεία εισόδου.



Σχήμα 2.5 Σελίδα εισόδου mybank.gr

Αν δούμε τον κώδικα html που δημιουργήθηκε (δεξί κλικ πάνω στην οθόνη και επιλέγουμε «προβολή κώδικα»), θα παρατηρήσουμε κάτι ανάλογο όπως φαίνεται παρακάτω στο σχήμα 2.6. Εδώ πρέπει να αναφερθούμε ότι η τράπεζα mybank.gr είναι εικονική και έχει σχεδιαστεί μόνο για το παράδειγμά μας.



Σχήμα 2.6 Σελίδα εισόδου mybank.gr σε μορφή html

Από τα παραπάνω προκύπτει ότι ο σχεδιασμός ενός e-banking συστήματος δε διαφέρει από τον τρόπο σχεδιασμού οποιασδήποτε σελίδας αλλά διαφέρουν τα συστήματα τα οποία προβάλλουν αυτού του είδους τις σελίδες, συστήματα τα οποία περιέχουν μεθόδους ασφαλείας και τρόποι καταγραφή και εντοπισμού χρηστών που έχουν στόχο την οποιαδήποτε ζημιά στα συστήματα αυτά όπως και την επιχειρηματική λογική των συναλλαγών και διασύνδεσης με όλα τα απαιτούμενα συστήματα της Τράπεζας.

2.2 Εμπλεκόμενα Τμήματα

Προκειμένου να δημιουργηθεί μια συναλλαγή διαθέσιμη στα «κανάλια» του διαδικτύου όπως είναι και το e-banking, επιμέρους τμήματα συνεργάζονται ώστε το τελικό αποτέλεσμα να είναι διαθέσιμο στους πελάτες της τράπεζας.

Ενδεικτικά τμήματα που εμπλέκονται στην υλοποίηση μιας συναλλαγής είναι τα εξής :

- Τμήμα Εναλλακτικών Δικτύων
- Διεύθυνση Επικοινωνίας
- Διεύθυνση Marketing
- Διεύθυνση Πληροφορικής
- Διεύθυνση Ασφαλείας

Τα παραπάνω τμήματα αφορούν ένα γενικό μοντέλο μιας Τράπεζας που λειτουργεί στον Ελλαδικό χώρο για το σκοπό αυτό αναφερόμαστε πιο αναλυτικά στο πέμπτο κεφάλαιο της διατριβής.

2.3 Τρόπος και διαδικασία υλοποίησης συναλλαγής

Ένα νέο προϊόν ή μια συναλλαγή στο e-banking μπορεί δημιουργηθεί είτε από ένα αίτημα της διεύθυνσης των εναλλακτικών δικτύων, είτε από ένα αίτημα της διεύθυνσης marketing. Στη διαδικασία αυτή οι δύο διευθύνσεις, θα συνεργαστούν από κοινού ώστε να αποφασίσουν το τελικό αποτέλεσμα. Αφού αποφασίσουν το προϊόν που πρόκειται να δημιουργηθεί και να διατεθεί στα διαθέσιμα κανάλια, θα ζητηθεί από τη διεύθυνση πληροφορικής την εκτίμηση το σχετικού έργου ώστε να αποφασιστεί αν μπορεί να υλοποιηθεί είτε να δοθεί σε εξωτερικούς συνεργάτες το έργο και να δώσουν προσφορά. Μετά τη σχετική εκτίμηση, σε περίπτωση που κάποιο έργο υπερβαίνει την αρχική εκτίμηση, εγκρίνεται από τη διοίκηση της Τράπεζας. Μετά τη σχετική έγκριση και αφού γίνει η συλλογή των απαραίτητων μέσων (ανθρώπινο δυναμικό, κατάλληλο λογισμικό ή μέσο που θα χρησιμοποιηθεί), ξεκινάει η υλοποίηση από το τμήμα της πληροφορικής είτε γίνεται ανάθεση σε εξωτερικούς συνεργάτες βάση των οδηγιών που δίνονται από το τμήμα πληροφορικής. Για την υλοποίηση, συντάσσονται αναλυτικές προδιαγραφές από το τμήμα που έχει ζητήσει το σχετικό έργο που στις περισσότερες περιπτώσεις ανήκει στη διεύθυνση των εναλλακτικών δικτύων. Στην υλοποίηση χρησιμοποιούνται πολλές φορές διάφορα συστήματα που αφορούν το είδος της συναλλαγής. Έτσι, λ.χ, αν η υλοποίηση αφορά μια νέα πληρωμή μέσου του καναλιού e-banking διαμέσου του διατραπεζικού συστήματος ΔΙΑΣ, θα πρέπει να υλοποιηθεί και η διασύνδεση του συστήματος με το αντίστοιχο τμήμα πληρωμών. Στην υλοποίηση της

συναλλαγής, λαμβάνονται υπ' όψιν και οι οδηγίες που δίνονται από το τμήμα ασφαλείας προκειμένου η συναλλαγή που υλοποιείται να πληροί τους κανονισμούς ασφαλείας της Τράπεζας. Μετά το πέρας της υλοποίησης, ανατίθεται για έλεγχο όλης της εφαρμογής ή τμήμα της, σε $2^{ο}$ επίπεδο ελέγχου, όπου γίνεται έλεγχος της εφαρμογής βάση των προδιαγραφών που έχουν δοθεί. Αν όλα πάνε καλά και ο σχετικός έλεγχος έχει επιτευχθεί από τη διεύθυνση ποιότητας ελέγχου, τότε δίνεται η έγκριση για να προχωρήσει από το δοκιμαστικό περιβάλλον σε περιβάλλον παραγωγής. Το τμήμα πληροφορικής μέσω των αρμόδιων αναλυτών προετοιμάζουν εκείνα τα μέρη του κώδικα και της βάσης δεδομένων που έχουν τροποποιηθεί είτε δημιουργηθεί, με σκοπό να προχωρήσουν και να διαθέσουν άμεσα στους πελάτες της Τράπεζας το παραγόμενο προϊόν ή υπηρεσίας. Αφού γίνει έλεγχος Αρχιτεκτονικά του υλικού από το αρμόδιο τμήμα , δίνεται εντολή να προχωρήσει η διαδικασία, λαμβάνοντας ταυτόχρονα τις εγκρίσεις των τμημάτων και προχωράει στην τελική διαδικασία. Μετά την ολοκλήρωση της συναλλαγής και την επιτυχή διάθεσή της, αναλαμβάνει το τμήμα επικοινωνίας στη συνέχεια προκειμένου το παραγόμενο υλικό να «επικοινωνικοποιηθεί» προς το κοινό. Το τμήμα επικοινωνίας εξετάζει το μέγεθος του έργου αλλά και το «διαθέσιμο διαφημιστικό ποσό» (budget) που διαθέτει ώστε να προχωρήσει σε συνεργασία με το τμήμα marketing, μια διαφημιστική καμπάνια προώθησης του προϊόντος ή της πιο πάνω υπηρεσίας μέσα από ζώνες διαφήμισης (περιοδικά, τηλεοπτικά και ακουστικά μέσα). Τέλος, προκειμένου να διαπιστωθεί αν η σχετική υπηρεσία ή συναλλαγή που δημιουργήθηκε, έχει ανταπόκριση από το κοινό, το τμήμα ερευνών διεξάγει έρευνα προς τους πελάτες της ώστε να αποσπάσει τη γνώμη τους προκειμένου να βελτιώσει τις παραγόμενες υπηρεσίες.

2.4 Συμπέρασμα

Το e-banking είναι ίσως το σημαντικότερο κανάλι σε έναν τραπεζικό οργανισμό με σκοπό την παροχή υπηρεσιών προς το κοινό. Ένα σύστημα e-banking δε διαφέρει από τα συστήματα τα οποία προσφέρουν πληροφορίες μέσω ιστοσελίδων, αλλά προσφέρουν εξειδικευμένες υπηρεσίες όχι μόνο για πληροφόρηση αλλά και για εκτέλεση συναλλαγών όπως πληρωμές και μεταφορές χρημάτων. Για την υλοποίηση των υπηρεσιών και νέων συναλλαγών,

συνεργάζονται διαφορετικά τμήματα με στόχο την υποστήριξη τους τα οποία έχουν ως σκοπό τη βελτίωση των υπηρεσιών προς τους πελάτες με αποτέλεσμα την αύξηση της κερδοφορίας.

3. Mobile Banking - Ηλεκτρονική Τραπεζική μέσω κινητών

Οι ευρείες οικονομικές εξελίξεις της προηγούμενης δεκαετίας (π.χ. προσπάθεια συνένωσης της παγκόσμιας οικονομίας), έχουν αυξήσει τις μετακινήσεις πληθυσμών σε διάφορες αγορές εργασίας. Ταυτόχρονα, οι τεχνολογικές εξελίξεις, ειδικά στον τομέα των τηλεπικοινωνιών, δημιούργησαν εφικτή την προσφορά καινοτομίας, παρέχοντας ευαίσθητες υπηρεσίες βασιζόμενες στον "μετακινούμενο πελάτη" [11]

Επιχειρήσεις που παρέχουν τέτοιου είδους υπηρεσίες γνωστές και ως «mobile commerce» σε μια πιο απλουστευμένη μορφή μπορεί να θεωρηθεί και ως μια επέκταση του ηλεκτρονικού εμπορίου με τη χρήση ασύρματων μέσων. Υπηρεσίες παρεχόμενες μέσω κινητής στον χρηματοπιστωτικό τομέα είναι γνωστές σε γενικές γραμμές και ως «χρηματοπιστωτικές υπηρεσίες μέσω κινητής τηλεφωνίας (MFS – mobile financial services). Οι υπηρεσίες αυτές διαχωρίζονται σε δύο επίπεδα εφαρμογών, στην πληρωμή μέσω κινητής (mobile payment) αλλά και στην ηλεκτρονική τραπεζική μέσω κινητής τηλεφωνίας (mobile-banking).

Το mobile-banking [25] παρουσιάζει μια μεγάλη αποδοχή τα τελευταία χρόνια στο κοινό που ασχολείται με νέες τεχνολογίες, ειδικά μετά την «ανάρρωση» από το «σοκ» των εικονικών εταιρειών τύπου ".com" που είχαν εμφανιστεί στο τέλος της δεκαετίας του 90. Διάφορες μελέτες Rajnish Tiwari and Stephan Buse [2006], Meridea [2003], Suoranta [2003] and Buse [2002] έχουν διαπιστωθεί ότι στην Δυτική Ευρώπη υπάρχει μια αξιοσημείωτη ζήτηση για υπηρεσίες χρηματοοικονομικές μέσω κινητών τηλεφώνων. Ειδικά οι Tiwari and Buse [2006] δείχνουν ότι ο «πραγματικός ρυθμός απόρριψης» των υπηρεσιών μέσω κινητής τηλεφωνίας είναι 8%, πολύ χαμηλότερο από ότι πιστεύεται συχνά. Επιπλέον, πολλοί πελάτες των τραπεζών με βάση τη μελέτη, είναι πρόθυμοι για το επιπλέον χρηματικό κόστος για την αξιοποίηση των υπηρεσιών αυτών. Παρόμοιες εξελίξεις έχουν αναφερθεί και σε άλλα μέρη του κόσμου όπως παράδειγμα στην Νότια Κορέα όπου ο αριθμός των συναλλαγών μέσω κινητής τηλεφωνίας αυξήθηκε σε ημερήσιο μέσο όρο σε 287.000 συναλλαγές το 2005 και ποσοστό 104%, ενώ ο αριθμός των εγγεγραμμένων χρηστών αυξήθηκε κατά 108% συγκριτικά με το 2004 [Korea Times,2006].

Οι παραπάνω εξελίξεις δείχνουν μια θετική αντίληψη για της χρηματοοικονομικές υπηρεσίες μέσω κινητών τηλεφώνων. Αυτή η θετική μεταστροφή στις αντιλήψεις μπορεί να εντοπιστεί στους εξής παράγοντες [Tiwari et al, 2006] :

- Το ποσοστό της διείσδυσης της κινητής τηλεφωνίας στην κοινωνία είναι από τα υψηλότερα.
- Η ενοποίηση της παγκόσμιας οικονομίας οδηγεί σε μια διαρκής κινητικότητα και έτσι πλέον οι υπηρεσίες που παρέχονται μέσω κινητών τηλεφώνων δεν είναι απλά πολυτέλεια αλλά αναγκαίες.
- Οι νεότερες γενιές της κοινωνίας φαίνεται να γοητεύονται περισσότερο από σύγχρονα δεδομένα και τηλεπικοινωνιακές υπηρεσίες.
- Οι φορητές συσκευές έχουν γίνει πιο ισχυρές και η ταχύτητα μετάδοσης των δεδομένων έχει αυξηθεί αρκετά.

Βλέποντας τις παραπάνω εξελίξεις πολλές τράπεζες προσανατολίζονται εδώ και πολλά χρόνια και στην επέκταση των υπηρεσιών τους διαμέσου της κινητής τηλεφωνίας. Οι υπηρεσίες που μέχρι στιγμής προσφέρονται με τη χρήση κινητού είναι οι ακόλουθες :

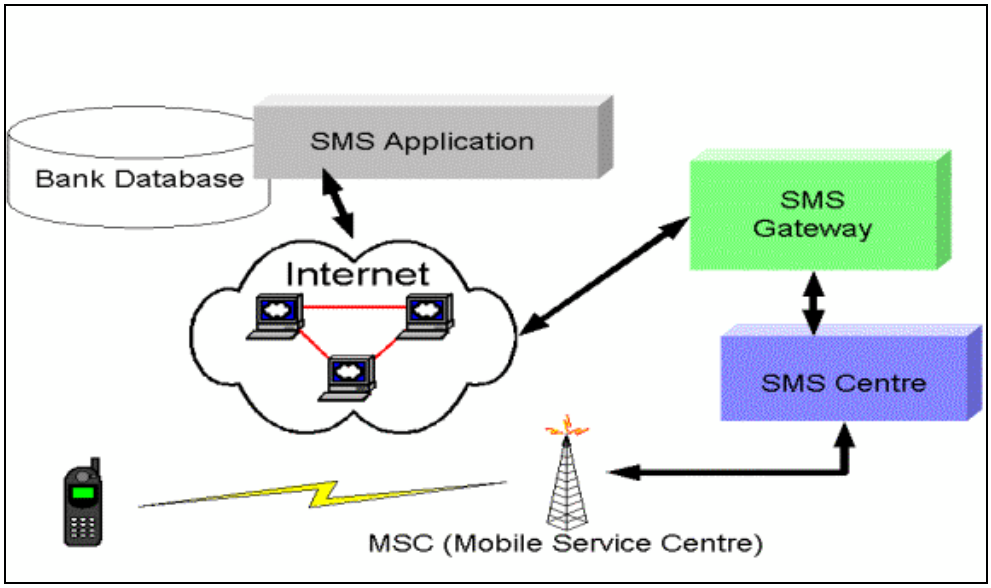
- ✓ Μέσω SMS (Short Message Service)
- ✓ WAP (Wireless Application Protocol)
- ✓ IVR (Interactive Voice Response)
- ✓ SMAC (Standalone Mobile Application Client)
- ✓ Mobile-Web Application
- ✓ M-banking for Smartphones

3.1 SMS Banking

Η υπηρεσία των γραπτών μηνυμάτων Short Message Service, γνωστή παγκοσμίως απλά ως SMS, είναι μία ασύρματη υπηρεσία που δίνει την δυνατότητα ανταλλαγής μηνυμάτων, με περιεχόμενο αλφαριθμητικά και σύμβολα έως 160 χαρακτήρες, μεταξύ χρηστών κινητής τηλεφωνίας ανεξαρτήτου δικτύου κάλυψης. Μετά την εμφάνισή της το 1991 στην Ευρώπη σαν πρότυπο του συστήματος GSM έγινε ταχύτατα παγκοσμίως αποδεκτή, αφού υποστηρίζεται από όλες τις συσκευές κινητών τηλεφώνων.

Η υπηρεσία SMS χρησιμοποιεί ένα κέντρο, το Short Message Service Center (SMSC), που έχει τον ρόλο ενός συστήματος τύπου store-and-forward. Το ασύρματο δίκτυο μεταφέρει τα γραπτά μηνύματα μεταξύ του κέντρου και των ασύρματων τερματικών προσφέροντας εγγυημένη παράδοση των δεδομένων ανιχνεύοντας οποιοδήποτε πρόβλημα προκύψει και αποθηκεύοντας το μήνυμα έως ότου αυτό το πρόβλημα ρυθμιστεί. Το κυριότερο χαρακτηριστικό της υπηρεσίας είναι ότι ένα κινητό μπορεί να λάβει ή να στείλει μηνύματα οποιαδήποτε ώρα (υπό την προϋπόθεση ότι είναι ενεργό) ανεξάρτητα αν εκείνη τη στιγμή βρίσκεται σε εξέλιξη κλήση για φωνή ή δεδομένα. Ένα ακόμη χαρακτηριστικό είναι η μη επιβάρυνση του δικτύου αφού απαιτεί μικρό εύρος ζώνης. Επίσης, η υπηρεσία χρησιμοποιείται πολλές φορές και από το ίδιο το σύστημα για ανταλλαγή σημάτων ελέγχου χωρίς ο χρήστης να αντιλαμβάνεται κάτι.

Το SMS Banking αρχικοποιείται με την αποστολή ενός δομημένου SMS (Structured SMS) από έναν πιστοποιημένο πελάτη στην Τράπεζα για τις υπηρεσίες pull ή με την απευθείας αποστολή ενός κοινού SMS από την Τράπεζα στον πελάτη για τις υπηρεσίες push. Το SSMS θα πρέπει να περιέχει μια αναγνωριστική λέξη της αιτούμενης τραπεζικής υπηρεσίας, η οποία προκαθορίζεται από την Τράπεζα και βρίσκεται πάντα στην αρχή του μηνύματος, έτσι ώστε πύλη SMS να προωθήσει το μήνυμα στη σωστή εφαρμογή. Η αρχιτεκτονική και τα δομικά στοιχεία της υπηρεσίας φαίνονται στο παρακάτω σχήμα:

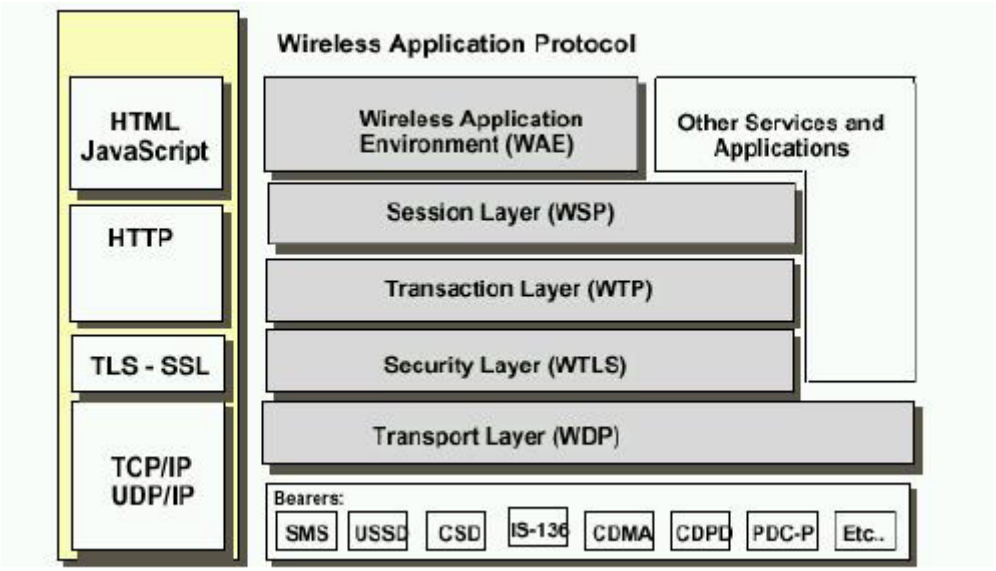


Σχήμα 3.1. SMS Banking Structure

3.2 WAP BANKING

Το WAP (Wireless Application Protocol) είναι ένα ανοιχτό διεθνές πρότυπο για την μεταφορά και παρουσίαση δεδομένων σε ψηφιακά κινητά τηλέφωνα, PDAs και άλλα ασύρματα τερματικά. Το πρωτόκολλο αυτό αναπτύχθηκε το 1997 από τον οργανισμό WAP Forum, με πρωτοστατούσες εταιρίες τις Nokia, Ericsson, Motorola και Unwired Planet , για την εξασφάλιση κοινά αποδεκτών τεχνικών προδιαγραφών που θα εξυπηρετούν την ανάπτυξη εφαρμογών και υπηρεσιών στα ασύρματα τηλεπικοινωνιακά δίκτυα και τη δυνατότητα πρόσβασης σε υπηρεσίες του Internet από ασύρματες συσκευές. Είναι προφανές λοιπόν ότι το WAP συνδέεται άμεσα με τις τεχνολογίες του Internet και αποτελεί τον συνδετικό κρίκο μεταξύ αυτών των τεχνολογιών και της ασύρματης μετάδοσης της πληροφορίας. Μάλιστα, δεν είναι λίγοι εκείνοι που ταυτίζουν το WAP με το Internet του κινητού τηλεφώνου.

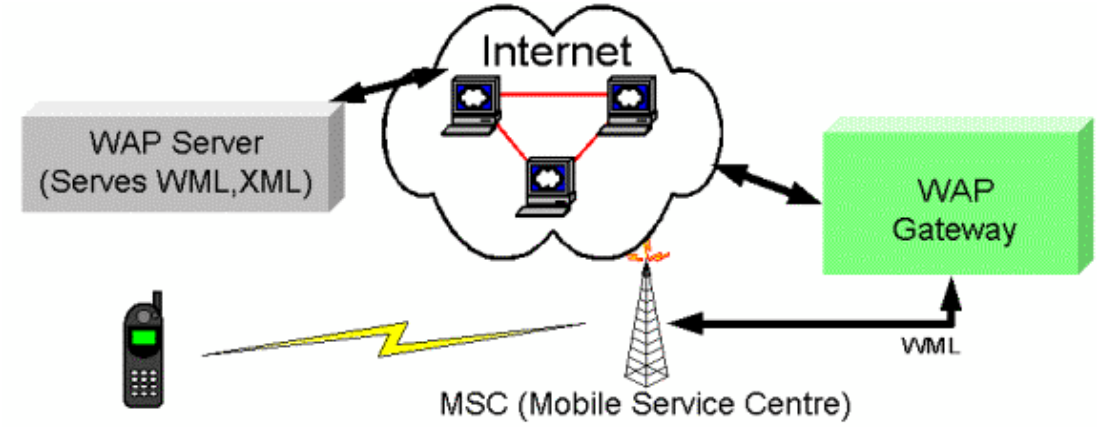
Το μοντέλο μετάδοσης δεδομένων του WAP έχει επιρροές από το Διαδίκτυο, γεγονός αναμενόμενο λόγω του αυτοσκοπού του, και στηρίζεται στην ανταλλαγή μηνυμάτων εξυπηρετούμενου και εξυπηρετητή (Client - Server). Στη βασική εκδοχή του μοντέλου, ο εξυπηρετούμενος κάνει μια αίτηση προς τον εξυπηρετητή που με τη σειρά του απαντά με το περιεχόμενο. Για την επικοινωνία, όμως, των δύο μελών είναι απαραίτητη η ύπαρξη μιας πύλης WAP, ή αλλιώς WAP Proxy, η οποία παίζει το ρόλο του ενδιάμεσου-μεταφραστή μεταξύ της κινητής συσκευής και του εξυπηρετητή. Έτσι, η επικοινωνία της πύλης με τον κινητό σταθμό γίνεται με βάση τα πρωτόκολλα του WAP ενώ με τον εξυπηρετητή με βάση τα πρωτόκολλα του Internet. Τα πέντε πρωτόκολλα του WAP αντιστοιχούν στα πέντε στρώματα της αρχιτεκτονικής του προτύπου και παρουσιάζονται στο παρακάτω σχήμα σε αντιπαραβολή με τα πρωτόκολλα του Διαδικτύου.



Σχήμα 3.2. Τα πρωτόκολλα του WAPSMS Banking Structure

Οι χρήστες των εφαρμογών ασύρματου περιβάλλοντος μέσω ενός ενσωματωμένου φυλλομετρητή τους είναι σε θέση να επισκέπτονται ιστοσελίδες σχεδιασμένες σε WML (Wireless Mark-up Language), οι οποίες είτε είναι αποθηκευμένες στον εξυπηρετητή είτε δημιουργούνται δυναμικά με την αποστολή της αίτησης. Επιπλέον, ο browser της ασύρματης συσκευής είναι υπεύθυνος για τον έλεγχο της διεπαφής με το χρήστη.

Το WAP Banking αρχικοποιείται με την είσοδο του πελάτη στον φυλλομετρητή του κινητού του και, μέσω του παρόχου, τη σύνδεση με το WAP site της Τράπεζας. Καθώς, ο WAP browser παρέχει τις βασικές υπηρεσίες ενός WEB browser εξαιτίας των περιορισμών λειτουργικότητας μιας ασύρματης συσκευής, ο χρήστης έχει την αίσθηση πρόσβασης διαδικτυακών ιστοσελίδων σε μικρογραφία, όπου μπορεί να πλοηγηθεί εύκολα με την χρήση του πληκτρολογίου. Το περιβάλλον εργασίας μιας «κινητής» ιστοσελίδας Τράπεζας είναι όσο το δυνατόν εύχρηστο, παρά καλαίσθητο, χωρίς, παράλληλα, να στερείται διαθέσιμων τραπεζικών υπηρεσιών σε σχέση με το αντίστοιχο web portal. Όσον αφορά στις τραπεζικές εφαρμογές, αυτές βρίσκονται στον εξυπηρετητή της Τράπεζας, ελεγχόμενες και ασφαλείς από κακόβουλους χρήστες, όπως άλλωστε συμβαίνει και με το e-banking. Το παρακάτω σχήμα παρουσιάζει την θέση του WAP στο μοντέλο Client – Server:



Σχήμα 3.3. WAP στο μοντέλο Client – Server

3.3. IVR Banking

Στο IVR αναφερθήκαμε στην ενότητα 1.1.5 και θα αναφερθούμε συνοπτικά αφού ανήκει στην κατηγορία της τραπεζικής πληροφορικής με χρήση τηλεφωνίας.

Το IVR αποτελεί ένα σύστημα που επιτρέπει την άμεση αλληλεπίδραση του καλούντα με το πληροφοριακό υλικό που είναι αποθηκευμένο στη βάση δεδομένων ή δημιουργείται δυναμικά με τη χρήση της τεχνολογίας TTS (Text to Speech). Η αλληλεπίδραση αυτή είναι εφικτή με δύο τρόπους, τα συστήματα DTMF (Dual Tone Multi Frequency) και την αναγνώριση της φωνής του καλούντα.

3.4 m-banking μέσω SMAC (Standalone Mobile Application Client)

Οι αυτόνομες κινητές εφαρμογές πελάτη SMAC (Standalone Mobile Application Clients) είναι ένα σύνολο προγραμμάτων που αναπτύσσονται στις ασύρματες συσκευές των χρηστών του τηλεπικοινωνιακού δικτύου και παρέχουν τη δυνατότητα συνεχούς σύνδεσης με πάροχους υπηρεσιών όπως οι Τράπεζες. Η άμεση πρόσβαση είναι αποτέλεσμα της εγκατάστασης των προγραμμάτων αυτών τοπικά, καταλαμβάνοντας χώρο στη μνήμη του τηλεφώνου ή στη SIM Card. Το μεγάλο τους πλεονέκτημα σε σχέση με τα υπόλοιπα κανάλια διανομής υπηρεσιών είναι η ευχρηστία που παρουσιάζουν, καθώς είναι εφικτή η μορφοποίηση τους με βάση το προφίλ του χρήστη. Στην κατηγορία των SMAC ανήκουν οι εφαρμογές SIM Application Toolkit (SAT) και J2ME (JAVA 2 Micro Edition).

Αν και η αρχιτεκτονική του SMS ήταν πολύ επιτυχής, η ανάγκη υποστήριξης της νέας γενιάς υπηρεσιών προστιθέμενης αξίας, όπως οι τραπεζικές υπηρεσίες,

οδήγησε σε επέκταση του προτύπου και της λειτουργικότητας των SIM Card των κινητών τηλεφώνων.

3.5 Web Mobile Banking

Η υπηρεσία του mobile banking μέσω web είναι όμοια με τη υπηρεσία e-banking την υπηρεσία δηλαδή υπηρεσία που χρησιμοποιεί κάποιος μέσω ενός προσωπικού υπολογιστή με τη χρήση ενός φυλλομετρητή (browser) με τη διαφορά ότι χρησιμοποιείται ο αντίστοιχος browser ενός κινητού. Στην ουσία πρόκειται για ιστοσελίδες κατάλληλα διαμορφωμένες για τις συσκευές κινητής τηλεφωνίας με σκοπό να έχουν πρόσβαση στις υπηρεσίες της τράπεζας. Η χρήση της υπηρεσίας αυτής είναι σχετικά απλή. Στις περισσότερες τράπεζες που παρέχουν αυτού του είδους την υπηρεσία, οι σελίδες που προβάλλονται διαμορφώνονται κατάλληλα στο μέγεθος της συσκευής.

Η υπηρεσία web-mobile banking ακολουθεί τα πρότυπα ασφάλειας του κανονικού e-banking που μπορεί κάποιος να δει από τον υπολογιστή όπως και τεχνολογικά ακολουθεί τον ίδιο τρόπο λειτουργίας. Δηλαδή, ένας χρήστης που κάνει χρήση του web-mobile μιας τράπεζας, θα πρέπει να πληκτρολογήσει τη διεύθυνση της ιστοσελίδας που προσφέρεται για χρήση του κινητού και αφού ταυτοποιηθεί ως χρήστης, να προχωρήσει στην καταχώρηση των εντολών αν πρόκειται για πληρωμές ή μεταφορές ή να δει τα στοιχεία του χαρτοφυλακίου του όπως στοιχεία λογαριασμών, δανείων, υπόλοιπο πιστωτικής, χαρτοφυλάκιο μετοχών κλπ.

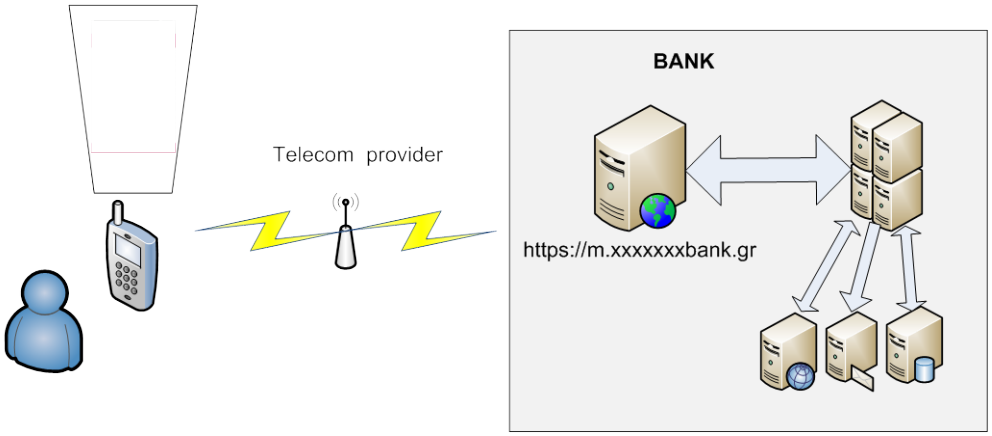
Παραθέτουμε ένα παράδειγμα web - mobile banking της Millennium bank που δραστηριοποιείται στην Ελλάδα. Όπως βλέπουμε στο παρακάτω σχήμα, ένας χρήστης πληκτρολογεί τη διεύθυνση της σελίδας στον browser του κινητού του και μετά από κάποια δευτερόλεπτα, εμφανίζεται η επιθυμητή σελίδα. Στην πραγματικότητα, η σύνδεση του αποτελέσματος της σελίδας, περιλαμβάνει μια αλληλουχία από επικοινωνίες προς και από άλλους διακομιστές (servers). Ενδεικτικά αναφέρουμε ότι οι servers μπορεί να είναι :

1. Ένα διακομιστής ιστού (web-server), ο οποίος είναι υπεύθυνος για να στείλει πίσω στο κινητό την ιστοσελίδα.
2. Διακομιστής περιεχομένου (CMS-content management server), ο οποίος είναι υπεύθυνος για το περιεχόμενο που θα στείλει πίσω το οποίο δεν αφορά δεδομένα δυναμικά αλλά στατικό περιεχόμενο (π.χ. πληροφοριακά μηνύματα ή μηνύματα για διαφημιστικούς σκοπούς).

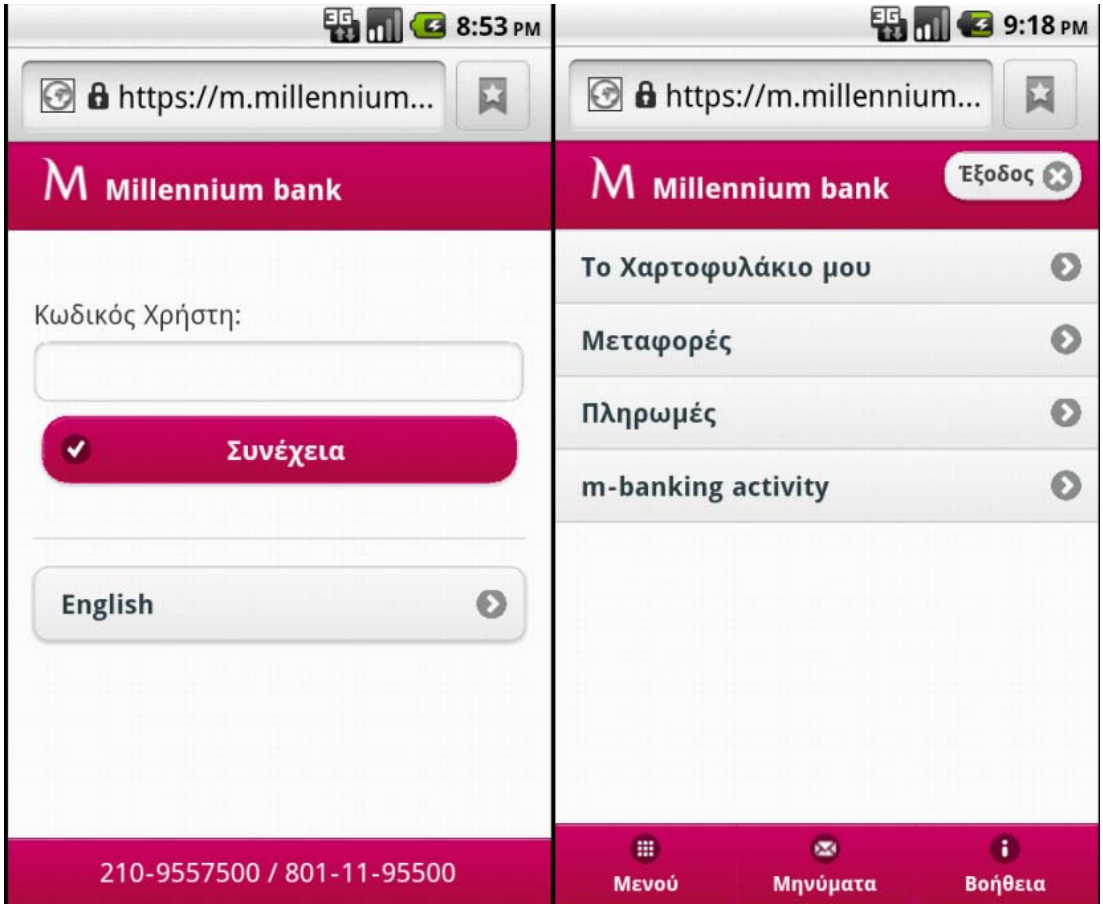
3. Διακομιστής βάσης δεδομένων (database server), όπου είναι υπεύθυνος για τη διαχείριση των πληροφοριών ανά πελάτη και αποθήκευσης πληροφοριών.
4. Διακομιστής εφαρμογών (application server), όπου εκτελούνται οι εφαρμογές για τη διαχείριση των μηνυμάτων.

Για να κατανοήσουμε τα πιο πάνω θα δώσουμε ένα παράδειγμα :

Αν ένας πελάτης χρειαστεί να μεταφέρει ποσά από έναν λογαριασμό σε έναν άλλο λογαριασμό, ο πελάτης μέσα από το κινητό θα κάνει τις απαιτούμενες ενέργειες, δηλαδή, θα επιλέξει τη συναλλαγή, θα καταχωρήσει το ποσό και τους λογαριασμούς και θα πατήσει το πλήκτρο της επιβεβαίωσης. Στην ουσία όμως οι ενέργειες που πρόκειται να γίνουν είναι οι εξής : Ο διακομιστής ιστού θα μεταφέρει το μήνυμα προς τον διακομιστή εφαρμογών (π.χ. στείλε αυτά τα χρήματα στον XXX λογ/σμό). Θα κληθεί από μια εφαρμογή με βάση την εντολή που θα λάβει, θα δώσει με τη σειρά της εντολή στον διακομιστή της βάσης δεδομένων ώστε να χρεώσει τον έναν λογαριασμό και να πιστώσει τον επόμενο. Παράλληλα αφού γίνει έλεγχος ότι μεταφέρθηκαν σωστά, θα συνθέσει μια νέα σελίδα με πληροφορίες από τον διακομιστή περιεχομένου η οποία μπορεί να περιλαμβάνει διάφορες πληροφορίες όπως για τις χρεώσεις του πελάτη, και θα στείλει πίσω στον διακομιστή ιστού το αποτέλεσμα της εντολής. Αν έχει εκτελεστεί, θα αποστείλει μήνυμα επιτυχίας, σε κάθε άλλη περίπτωση, θα στείλει μήνυμα αποτυχίας και θα αποστείλει σχετικό email (προεραιτικά) για τους λόγους αποτυχίας. Τέλος, ο διακομιστής ιστού, θα στείλει όλο το περιεχόμενο στον πάροχο τηλεπικοινωνιών και θα εμφανιστεί στη συσκευή του κινητού το αποτέλεσμα της συναλλαγής.



Σχήμα 3.4. Διάγραμμα απεικόνισης της επικοινωνίας web-mobile banking



Σχήμα 3.5. Εφαρμογή web-mobile banking της Millennium bank

Όσο απλή κι αν την έχουμε παρουσιάσει τη σχετική επικοινωνία του κινητού με την τράπεζα, παρουσιάζονται όμως πολλοί κίνδυνοι που μπορεί κάποιος να αντιμετωπίσει με τη χρήση των εφαρμογών web τους οποίους θα αναφέρουμε στην επόμενη ενότητα όπως επίσης και ενδεικτικά τρόπους προφύλαξης. Πρέπει να τονίσουμε ότι τα «έξυπνα τηλέφωνα» διατρέχουν τον ίδιο κίνδυνο έκθεσης στο διαδίκτυο όπως και κάθε υπολογιστής αφού η τεχνολογία τους δε διαφέρει από εκείνη των υπολογιστών που διαθέτουμε στο σπίτι.

Στην παγκόσμια αγορά οι χρήστες των «έξυπνων τηλεφώνων» (smartphones) ολοένα και αυξάνονται λόγω της ιδιαιτερότητας που έχουν τα συγκεκριμένα κινητά να μπορούν να προσφέρουν πολλές επιλογές στο χρήστη σε ότι αφορά εικόνα, ήχο, υπηρεσίες διαδικτύου, φωτογράφιση κλπ, κάθε κινητό είναι άμεσα εκτεθειμένο σε «επιθέσεις» όπως και την «μεταφορά και χρήση» κακόβουλου λογισμικού που έχει αποτέλεσμα και στόχο τις διάφορες υποκλοπές προσωπικών δεδομένων. Πολλοί κατασκευαστές, επιδιώκουν να εγκαταστήσουν το δικό τους λειτουργικό στις

συσκευές τους ώστε να διασφαλίζουν με τον τρόπο αυτό τη μέγιστη ασφάλεια στους κατόχους των συσκευών, όμως είναι αδύνατο να ενημερώνονται συνεχώς με νέες αναβαθμίσεις λογισμικού και ρυθμίσεις ασφαλείας λόγω ότι πολλοί χρήστες δε διαθέτουν τις κατάλληλες γνώσεις πέραν από τη χρήση των κινητών. Έτσι πιστεύουμε ότι οι χρήστες των κινητών είναι πιο ευάλωτοι μέχρι στιγμής σε κινδύνους από το διαδίκτυο από ότι οι χρήστες που χρησιμοποιούν τον υπολογιστή τους λόγω της πολυμορφίας (διάφοροι κατασκευαστές με διαφορετικά λειτουργικά συστήματα) που δεν κυκλοφορούν πολλά προγράμματα προστασίας κατά των κακόβουλων λογισμικών σε σχέση με τους ηλεκτρονικούς υπολογιστές. Ωστόσο, είναι ένα εργαλείο το οποίο μπορεί κάποιος να κερδίσει σημαντικό προσωπικό χρόνο διεκπεραιώνοντας τις συναλλαγές του από οποιοδήποτε σημείο βρίσκεται και οποιαδήποτε ώρα.

Παραθέτουμε ορισμένα από τα πλεονεκτήματα και μειονεκτήματα που εμφανίζονται στη χρήση των υπηρεσιών web mobile banking :

Πλεονεκτήματα :

- ✓ Δεν είναι απαραίτητη η εγκατάσταση του λογισμικού αφού μπορεί να χρησιμοποιηθεί από τον browser του κινητού και να χρησιμοποιήσει άμεσα την υπηρεσία.
- ✓ Οι οθόνες είναι απλά σχεδιασμένες χωρίς ιδιαίτερα γραφικά, ώστε οι σελίδες να αναδύονται γρήγορα και το να μην καταναλώνει χρόνο και δεδομένα περιττά πράγμα που αυξάνει το κόστος της υπηρεσίας από πλευράς παρόχου υπηρεσίας διαδικτύου.
- ✓ Μπορείτε να εκτελέσετε τις περισσότερες συναλλαγές που διατίθενται στο e-banking όπως πληρωμές λογαριασμών και πιστωτικής κάρτας, μεταφορές χρημάτων, εμφάνιση υπολοίπων κλπ.

Μειονεκτήματα :

- Δεν μπορεί να γίνει εκμετάλλευση των δυνατοτήτων της συσκευής όπως
  - τη μετάδοση ήχου και εικόνας μέσα από την εφαρμογή
  - τη χρήση στοιχείων της συσκευής όπως GPS και κάμερα

3.6 Mobile Appls for Smartphone

Οι εφαρμογές m-banking για νέου τύπου κινητά τα λεγόμενα «έξυπνα κινητά» ή αλλιώς «smartphones», πρόκειται για εφαρμογές που είναι κατασκευασμένες αποκλειστικά για τον τύπο του κινητού.

Τα «έξυπνα» κινητά είναι κινητά τα οποία στηρίζονται στην τεχνολογία των ηλεκτρονικών υπολογιστών απλά με μικρότερες δυνατότητες από ότι ένας υπολογιστής. Μέσω των συγκεκριμένων συσκευών παρέχεται η δυνατότητα κλήσης τηλεφώνων αλλά παράλληλα περιέχουν εφαρμογές και λειτουργίες που μόνο σε υπολογιστές παλαιότερα μπορούσαμε να τις βρούμε. Έτσι παρατηρούμε ότι σε μια τέτοιου είδους συσκευή τα βασικά εξαρτήματα είναι συνήθως συσκευές ήχου, χαμηλής ανάλυσης ψηφιακή μηχανή, GPS (Global Point System), ασύρματο δίκτυο (wi-fi), ενσωματωμένο browser για να γίνεται περιήγηση στο Internet.

Για να καταλάβουμε το τι είναι τα «έξυπνα κινητά» στην πραγματικότητα θα πρέπει να δούμε ιστορικά την μέχρι τώρα εξέλιξη της τεχνολογίας των κινητών μέχρι να φθάσουμε στη σημερινή κατάσταση. Στην αρχική τους μορφή οι συσκευές ήταν απλές και μπορούσαν να χρησιμοποιηθούν μόνο για κλήσεις και αποθήκευση επαφών και τηλεφώνων στην κάρτα μνήμης. Παράλληλα έκαναν την εμφάνιση τους και τα PDA (personal digital assistant) ή αλλιώς palmtop computer (υπολογιστής παλάμης) με σκοπό την οργάνωση καθημερινών εργασιών, επαφών και συγχρονισμό με τον υπολογιστή [26]. Στη συνέχεια τα PDA ενσωμάτωσαν τη δυνατότητα ασύρματης επικοινωνίας και είχαν τη δυνατότητα να λαμβάνουν και να δέχονται ηλεκτρονική αλληλογραφία (e-mail). Στη συνέχεια, τα PDA ενσωμάτωσαν και λειτουργίες των κινητών όπως και η τεχνολογία των κινητών ενσωμάτωσαν περισσότερο λειτουργίες των PDA. Το αποτέλεσμα εξελίχθηκε στη δημιουργία των «έξυπνων συσκευών» ή αλλιώς smartphones.

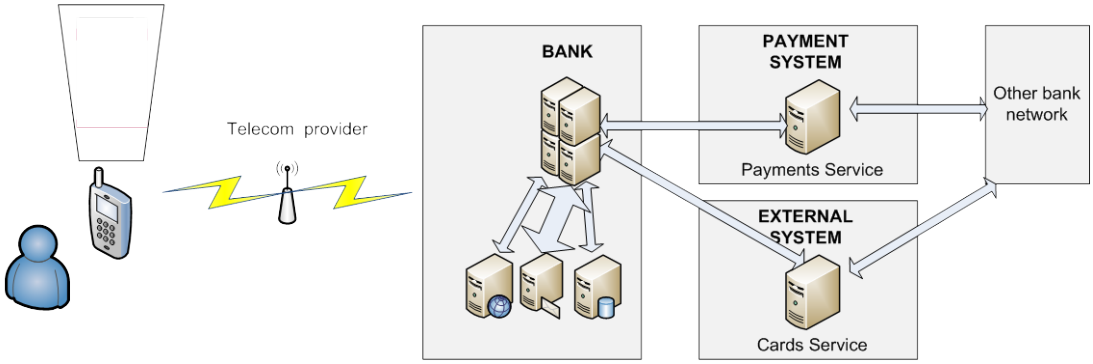
Οι τράπεζες, βλέποντας τις δυνατότητες που προσφέρουν οι έξυπνες συσκευές, έσπευσαν να εκμεταλλευτούν αυτού του τύπου κανάλι επικοινωνίας, δημιουργώντας παράλληλα εφαρμογές που εκμεταλλεύονται τις δυνατότητες των κινητών και παράλληλα έχουν πρόσβαση στις τραπεζικές υπηρεσίες.

Πώς όμως επιτυγχάνεται από μια συσκευή που εγκαθίσταται ένα λογισμικό από την τράπεζα που ένας πελάτης έχει συνεργασία, να μπορεί να επικοινωνήσει και να κάνει συναλλαγές ;

Ένας πελάτης, γνωρίζοντας ότι η τράπεζα που συνεργάζεται, διαθέτει κατάλληλο λογισμικό για τη συσκευή του, εγκαθιστά σύμφωνα με τις οδηγίες την αντίστοιχη εφαρμογή. Οι εφαρμογές που χρησιμοποιούνται στις συσκευές κινητών αντίστοιχα, έχουν δημιουργηθεί από το προσωπικό της τράπεζας ή συνεργαζόμενης εταιρείας με σκοπό την μέγιστη αξιοποίηση των δυνατοτήτων της συσκευής. Τέτοιου είδους εφαρμογές διαθέτουν πέραν από την πρόσβαση στο Τραπεζικό χαρτοφυλάκιο του πελάτη, δυνατότητες ώστε να εκμεταλλευτούν και τις «συσκευές» που διαθέτει το κινητό.

Για να καταλάβουμε πως λειτουργεί μια εφαρμογή, θα θέσουμε ένα παράδειγμα για πώς μπορεί κάποιος να επικοινωνήσει με την Τράπεζα μέσω μιας εφαρμογής κατάλληλης για το κινητό. Αν για παράδειγμα ένας χρήστης διαθέτει συσκευή i-phone από την εταιρεία Apple, η εγκατάσταση της εφαρμογής γίνεται μέσα από το ίδιο το κινητό και μέσω της επιλογής που συνδέεται με το ηλεκτρονικό κατάστημα της εταιρίας Apple (Appstore). Αφού επιλέξει ο χρήστης (μέσω αναζήτησης) την εφαρμογή και την εγκαταστήσει, η εφαρμογή είναι άμεσα διαθέσιμη προκειμένου να γίνουν οι συναλλαγές με την Τράπεζα. Έστω ότι ο πελάτης επιλέγει να κάνει μια συναλλαγή για παράδειγμα ότι θέλει να δει το υπόλοιπο της πιστωτικής του κάρτας. Τα βήματα που θα ακολουθήσει είναι τα εξής :

1. θα επιλέξει την εφαρμογή πλέον που είναι ήδη εγκατεστημένη
2. Θα εισάγει τα προσωπικά του στοιχεία όπως κωδικός πελάτη και κωδικός εισόδου.
3. Θα επιλέξει την επιλογή πληροφορίες καρτών
4. Μετά την εκτέλεση της συναλλαγής, θα αποσυνδεθεί από την εφαρμογή.



Στο παραπάνω σχήμα παρατηρούμε τη λειτουργία ενός mobile banking συστήματος τον τρόπο που γίνεται η επικοινωνία προκειμένου να δει ένας πελάτης μια πληροφορία όπως για παράδειγμα τις κινήσεις μιας πιστωτικής κάρτας ή λογαριασμού ή να κάνει μια πληρωμή σε άλλη τράπεζα. Στο συγκεκριμένο παράδειγμα η εφαρμογή «καλεί» απευθείας με τα web-services της τράπεζας μέσω ασφαλούς σύνδεση SSL **(Secure Sockets Layer)** πρωτοκόλλου. Ένα web-service είναι μια μέθοδος επικοινωνίας δύο υπολογιστών μέσω του διαδικτύου. Έχει μια «διαπροσωπεία» ή αλλιώς ένα interface το οποίο περιγράφεται μέσω ενός αρχείου που περιλαμβάνει τον τρόπο κλήσης των υπηρεσιών (Web Services Description Language ή wsdl). Ο τρόπος κλήσης των web-services είναι κοινός για όλους τους κατασκευαστές συστημάτων. Συνεχίζοντας το παράδειγμα, αποστέλλεται ένα μήνυμα (web-service) από το κινητό (χρησιμοποιώντας το διαδίκτυο) με τα στοιχεία που έχει καταχωρήσει ο χρήστης κρυπτογραφημένα. Μόλις ληφθούν τα στοιχεία από την τράπεζα και ταυτοποιηθεί ο χρήστης, τότε αποστέλλονται πίσω στην εφαρμογή στοιχεία με τις ενεργές επιλογές που επιτρέπεται στον χρήστη να χρησιμοποιήσει. Επιλέγοντας για παράδειγμα την εμφάνιση πληροφοριών για τις συναλλαγές μιας πιστωτικής κάρτας, ένα μήνυμα αποστέλλεται σε ένα εξωτερικό σύστημα (εντός δικτύου της τράπεζας) και τα αποτελέσματα επιστρέφουν στο κινητό το οποίο τα εμφανίζει στην οθόνη του χρήστη. Αντίστοιχα μηνύματα αποστέλλονται και σε περίπτωση που κάποιος επιλέξει την πληρωμή ενός λογαριασμού, τότε ένα μήνυμα αποστέλλεται σε ένα σύστημα πληρωμών και εκτελεί την χρεοπίστωση είτε αποστέλλει την πληρωμή σε άλλο διατραπεζικό δίκτυο. Η λογική και στις εφαρμογές των κινητών, ακολουθούν τη δομή όπως την παρουσιάσαμε στο web-mobile banking με τη μόνη διαφορά ότι οι οθόνες που παρεμβάλλονται στο κινητό του χρήστη είναι ήδη εγκατεστημένες ως εφαρμογή ενώ στο web-mobile banking οι οθόνες είναι σελίδες ιστού τύπου html και η διαχείριση και συντήρησή τους γίνεται αποκλειστικά στα συστήματα της τράπεζας.

Οι ιδιαιτερότητες που παρουσιάζουν οι εφαρμογές των smartphones είναι ότι γράφονται κατάλληλα για τη λειτουργία του κινητού και έτσι μπορούν να εκμεταλλευτούν πλήρως της δυνατότητες της συσκευής. Όπως για παράδειγμα, ένας χρήστης χρησιμοποιώντας μια αντίστοιχη εφαρμογή, έχει τη δυνατότητα :

- Να εισέλθει στο m-banking της τράπεζας και να πραγματοποιήσει τις τραπεζικές συναλλαγές όπως πληρωμές και μεταφορές.

- Μέσω του GPS της συσκευής, να εντοπίσει το πιο κοντινότερο ATM ή κατάστημα.
- Μπορεί να πληρώσει λογαριασμούς χρησιμοποιώντας την ψηφιακή κάμερα του κινητού προκειμένου να σαρώσει την γραμμογράφηση barcode των λογαριασμών είτε το νέα γραμμογράφηση barcode το λεγόμενο qrcode[2].
- Μπορεί να χρησιμοποιήσει διάφορα εργαλεία όπως Ισοτιμία, μετατροπή συναλλάγματος, υπολογισμό IBAN, υπολογισμό Δανείου
- Μπορεί να χρησιμοποιήσει την υπηρεσία τηλεφωνικής υποστήριξης όπου μπορεί να εισάγει τον αριθμό του κινητού και ένας διαθέσιμος εκπρόσωπος της τράπεζας επικοινωνεί μαζί του.

Το βασικό μειονέκτημα είναι ότι για μια αναβάθμιση μιας υπηρεσίας (π.χ. προσθήκη μιας νέας πληρωμής), θα πρέπει να ενημερωθούν όλες οι εφαρμογές των κινητών που έχουν δημιουργηθεί από την εταιρεία και να γίνει ταυτόχρονη ενημέρωση στα κινητά, πράγμα που είναι αρκετά δύσχρηστο για την Τράπεζα και για τον πελάτη στη συνέχεια.

3.7 Συμπεράσματα

Το m-banking μπορούμε να πούμε ότι ήρθε για να μείνει. Πλέον πολλές εταιρίες όπως και οι Τράπεζες, σχεδιάζουν κατάλληλα λογισμικά προκειμένου να έχουν μέρος της αγοράς με αποτέλεσμα ολοένα να μπορεί κάποιος να απολαμβάνει τις υπηρεσίες τους με απώτερο σκοπό το κέρδος κάθε οργανισμού. Ωστόσο, πολλές τράπεζες, διατηρούν και συντηρούν και εφαρμογές web κατάλληλες για κινητά ώστε να καλύψουν όσο το δυνατόν περισσότερες συσκευές κινητής τηλεφωνίας. Ο πελάτης μιας τράπεζας, μπορεί από το κινητό του που το έχει τις περισσότερες φορές κοντά του, να εκτελέσει τις πληρωμές είτε να στείλει χρήματα είτε να δώσει εντολές χρηματιστηριακές κλπ. Δηλαδή μπορούμε να πούμε ότι έχει «μια τράπεζα δίπλα του».

4. Ασφάλεια Δεδομένων και συστημάτων από επιθέσεις μέσω διαδικτύου

Κάθε χρηματοπιστωτικό ίδρυμα προσπαθεί να προστατεύσει σε μέγιστο βαθμό τα συστήματα που έχει εκτεθειμένα στο διαδίκτυο ώστε να διασφαλίσουν την ασφάλεια μεταξύ των πελατών αλλά και των συστημάτων τους. Στο Internet ο βαθμός επικινδυνότητας επιθέσεων σε μια υπηρεσία διεξαγωγής on-line συναλλαγών είναι μεγάλος και προβληματίζει τους συναλλασσόμενους έντονα γι αυτό. Οι επιθέσεις που χρησιμοποιούν κακόβουλοι είναι διαφορετικού τύπου κάθε φορά προκειμένου να διεισδύσουν με κάθε τρόπο στο τραπεζικό σύστημα και αντίστοιχα στους λογαριασμούς πελατών με σκοπό την μεταφορά χρηματικών ποσών είτε την καταστροφή των συστημάτων. Οι πλειονότητα των επιθέσεων συνήθως γίνονται μέσω του διαδικτύου. Παρακάτω αναλύουμε ορισμένες επιθέσεις που υφίστανται τα συστήματα των τραπεζών καθώς και τρόποι που αναλαμβάνουν οι τράπεζες για τη διαφύλαξή τους.

4.1 Μέθοδοι επιθέσεων στα συστήματα Τραπεζών

Προκειμένου να διεισδύσουν μέσω διαδικτύου στα κεντρικά συστήματα των τραπεζών με σκοπό να υποκλέψουν δεδομένα είτε να κάνουν ζημιά στα συστήματα και να τα καταστήσουν άχρηστα, οι «ηλεκτρονικοί διαρρήκτες» χρησιμοποιούν διάφορες τεχνικές για να πετύχουν το στόχο τους. Ορισμένες από αυτές παρουσιάζουμε στην παρούσα ενότητα.

4.1.1 SQL Injection

Για να εξηγήσουμε αυτού του είδους της επίθεσης που δέχονται τα συστήματα, θα πρέπει πρώτα να εξηγήσουμε το τί είναι ένα απλό πεδίο εισαγωγής δεδομένων σε μια φόρμα (input field). Κάθε σελίδα με πεδία που εισάγουμε δεδομένα όπως όνομα χρήστη, κωδικός, σχόλια κλπ, είναι πεδίο εισαγωγής δεδομένων. Από τη στιγμή που πατηθεί το «κουμπί καταχώρησης» (button submit), όλα τα δεδομένα που έχουν καταχωρηθεί, αποστέλλονται στην εφαρμογή. Η εφαρμογή, αποστέλλει συγκρίνει, αποθηκεύει τα δεδομένα σε μια βάση δεδομένων και επιστρέφει το αποτέλεσμα πίσω στο χρήστη. Πριν την αποστολή η εφαρμογή, ελέγχει την ορθότητα των δεδομένων προς καταχώρηση. Παράδειγμα ελέγχου που μπορεί να δημιουργηθεί είναι αν σε ένα πεδίο που περιμένει δεδομένα ημερομηνίας να καταχωρηθεί ένα όνομα.

4.1.2 cross-site scripting (XSS)

Όταν ένας χρήστης εισάγεται σε ένα σύστημα, η εφαρμογή χρησιμοποιεί ένα "cookie"[1] προκειμένου να αποθηκεύσει τις ανακτημένες πληροφορίες από το σύστημα στο περιβάλλον του Χρήστη. Σε περίπτωση «κλοπής» του συγκεκριμένου cookie, μπορεί ένας επιτιθέμενος να «ξεγελάσει» το σύστημα με την ταυτοποίηση του χρήστη.

Οι επιθέσεις αυτού του είδους, διακρίνονται σε :

- Self reflecting XSS, ένας επιτιθέμενος μπορεί να στείλει ένα κρυπτογραφημένο link το οποίο να περιλαμβάνει έναν επιπλέον κώδικα με τέτοια μορφή που ο χρήστης δεν αντιλαμβάνεται. Ο χρήστης αφού κάνει κλικ, αποστέλλει τις αποθηκευμένες πληροφορίες σε κάποιου είδους ιστοσελίδας.
- Cross reflecting XSS, χρησιμοποιεί την ίδια αρχή. Σε αυτή την περίπτωση, ο επιτιθέμενος χρησιμοποιεί ιστοσελίδες που είναι διαθέσιμες προς όλους, και εμφανίζει μηνύματα που παρακινούν τους χρήστες να απαντήσουν (π.χ. ένα μήνυμα απάντησης με πληροφορία NAI/OXI). Αυτού του είδους μηνύματα, περιλαμβάνουν επιπλέον κώδικα ο οποίος ενεργοποιεί και αποστέλλει τις πληροφορίες που είναι αποθηκευμένες στο περιβάλλον του Χρήστη.

4.1.3 cross-site request forgery (CSRF)

Ενώ φαίνεται ότι είναι ίδιο με το Cross Site Scripting (XSS), παρόλαυτα είναι πιο ύπουλο από αυτό. Σε μια επίθεση Cross Site Scripting, ένας επιτιθέμενος χρειάζεται να έχει ένα παρόμοιο λογαριασμό εισόδου ώστε να καταλάβει ακριβώς πώς λειτουργεί μια εφαρμογή. Το CSRF είναι μια επίθεση που αναγκάζει έναν τελικό χρήστη να εκτελέσει τις ανεπιθύμητες ενέργειες σε μια διαδικτυακή εφαρμογή στην οποία αυτός / αυτή έχει εισέλθει. Μια επιτυχημένη εκμεταλλεύονται CSRF μπορεί να θέσει σε κίνδυνο τα δεδομένα του τελικού χρήστη και τη λειτουργία σε περίπτωση κανονικής χρήσης. Αν ο τελικός χρήστης στόχο είναι ο λογαριασμός διαχειριστή, αυτό μπορεί να θέσει σε κίνδυνο ολόκληρη την web εφαρμογή. [14]

Cookie ή αλλιώς **web cookie ή browser cookie**, χρησιμοποιείται από έναν Ιστοχώρο για να στείλει στατικές πληροφορίες σε έναν φυλομετρητή ενός χρήστη (browser) και για τον ιστόχώρο, να ανακτήσει τις στατικές πληροφορίες από τον φυλλομετρητή του χρήστη.

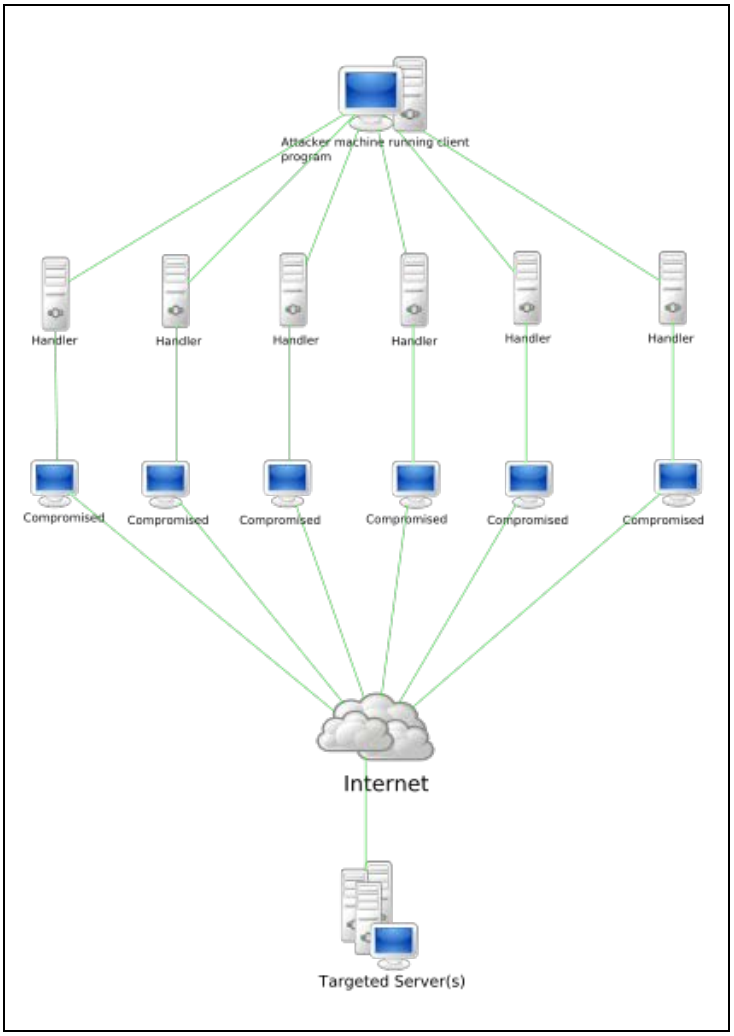
4.1.4 Denial-of-service attack (DoS)

Η επίθεση αυτή (γράφεται και ως DoS attach) [17], έχει ως κύριο στόχο το να μπορέσει ένα υπολογιστικό σύστημα ή μια δικτυακή υποδομή να μην είναι διαθέσιμη στο κοινό. Αυτό σημαίνει ότι μοτίβα και στόχοι μιας επίθεσης DoS ποικίλουν, σε γενικές γραμμές αποτελείται από τις συντονισμένες προσπάθειες ενός ατόμου ή πολλών ατόμων προκειμένου μια ιστοσελίδα να μη λειτουργήσει σωστά ή να σταματήσει να λειτουργεί. Η διείσδυση των επιθέσεων DoS γίνεται συνήθως σε συστήματα που έχουν υψηλού προφίλ όπως είναι οι τράπεζες, εταιρίες πληρωμών μέσω πιστωτικών καρτών.

Μια κοινή μέθοδο επιθέσεων περιλαμβάνει τον κορεσμό του συστήματος στόχος μέσω εξωτερικών αιτήσεων για εξυπηρέτηση. Λόγω της ταυτόχρονης ζήτησης εξυπηρέτησης μιας ιστοσελίδας, ο ιστότοπος εξυπηρετεί πολύ αργά είτε δεν ανταποκρίνεται λόγω της υπερφόρτωσης του. Σε γενικές γραμμές οι επιθέσεις DoS εξαναγκάζουν το σύστημα «θύμα» σε επανεκκίνηση ή καταναλώνουν τους διαθέσιμους πόρους για να μην μπορεί να παρέχει τις υπηρεσίες ή διακόπτουν τις επικοινωνίες μεταξύ των χρηστών και του θύματος.

Η επίθεση DoS θεωρείται παραβίαση της ορθής χρήσης του συμβουλίου αρχιτεκτονικής του διαδικτύου (IAB-Internet Architecture Board) και επίσης παραβιάζουν τους όρους χρήσης των πάροχων υπηρεσιών διαδικτύου.

Στο σχηματικό διάγραμμα φαίνεται ο τρόπος με τον οποίο μια επίθεση μπορεί να επιτευχθεί. Παρατηρούμε λοιπόν τα συστήματα που επιτίθενται σε ένα κεντρικό σύστημα με σκοπό την κατάρρευση του. Τα συστήματα που επιτίθενται στις περισσότερες φορές μπορεί και να είναι και υπολογιστές προσωπικούς, όπου οι χειριστές τους αγνοούν ότι ο υπολογιστής τους χρησιμοποιείται για επίθεση επειδή έχει «παγιδευτεί» από κακόβουλο λογισμικό που εν αγνοία του έχει εκτελέσει είτε μπαίνοντας σε κάποια ιστοσελίδα που «κρυφά» μαζί με τα στοιχεία που έχει δει ο χρήστης, να έχει εγκαταστήσει στον υπολογιστή και εφαρμογές.



Σχήμα 4.1 Επίθεση σε σύστημα με σκοπό DoS

4.2 Μέθοδοι Υποκλοπών κωδικών εισόδου.

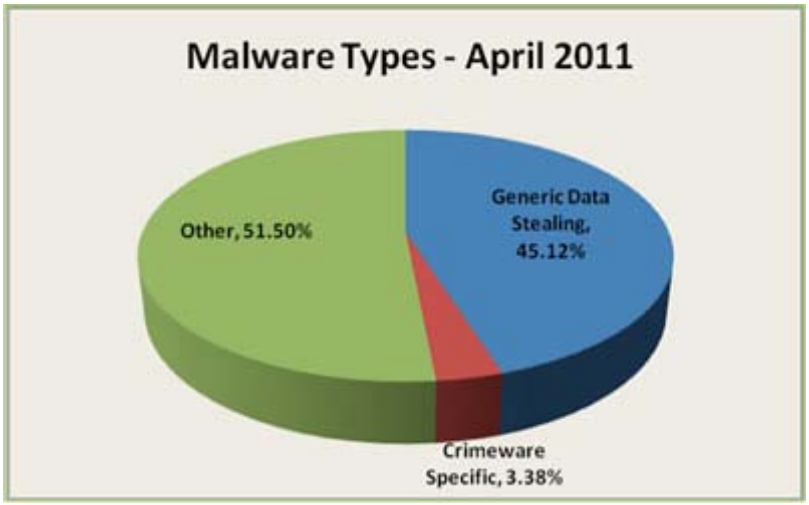
Πολλοί «ηλεκτρονικοί εγκληματίες» επιδιώκουν χρησιμοποιώντας τις νέες τεχνολογίες, εκμεταλλευόμενοι την άγνοια των χρηστών, να παραπλανήσουν, να εξαπατήσουν και να υποκλέψουν κωδικούς πρόσβασης στους λογαριασμούς των χρηστών έτσι ώστε είτε να αποσπάσουν χρηματικά ποσά είτε να κάνουν ζημιά στο αντίστοιχο τραπεζικό σύστημα.

4.2.2 Phishing attach

Phishing ή το λεγόμενο «ψάρεμα» είναι ένας τρόπος προσπάθειας να αποσπάσουν πληροφορίες από τους χρήστες (και πολλές φορές έμμεσα χρήματα), όπως κωδικοί χρήστη, κωδικοί εισόδου, αριθμούς καρτών συμπεριφερόμενο ως ασφαλής τοποθεσία στην ηλεκτρονική επικοινωνία. Η προσπάθεια αυτή στέλλεται μέσα από δημοφιλείς ιστοσελίδες όπως κοινωνικής δικτύωσης, ιστοσελίδες δημοπρασιών,

σελίδες άμεσων πληρωμών είτε διευθύνσεις πληροφορικής σελίδες οι οποίες δεν υποκινούν την υποψία των χρηστών. Τυπικά το «ψάρεμα» στέλλεται μέσω ηλεκτρονικού ταχυδρομείου και τις περισσότερες φορές κατευθύνουν τους χρήστες σε ιστοσελίδες σχεδιασμένες ίδιες με τις πραγματικές σελίδες ώστε ο χρήστης να μην υποψιάζεται αν βρίσκεται στη σελίδα π.χ. της Τράπεζας ή σε ψεύτικη ιστοσελίδα. Αφού καταχωρήσει τα στοιχεία που του ζητούνται στην ψεύτικη σελίδα, κατευθύνονται είτε στην πραγματική σελίδα, είτε βγάζει κάποιο μήνυμα λάθους φιλικό προς τον χρήστη.

Σύμφωνα με έρευνα που εμφανίζεται στο σχήμα 4.2 από τον οργανισμό www.antiphishing.org [12] παρατηρείται ότι η μέθοδος Phishing τον Απρίλιο του 2011 με σκοπό την υποκλοπή δεδομένων μέσω κακόβουλων λογισμικών, έχει φτάσει στο ποσοστό 45,12 % στο 1^{ο} τετράμηνο του 2011, αρκετά υψηλό σε σχέση με τους άλλους τρόπους επιθέσεων.



Σχήμα 4.2 Έρευνα Phishing

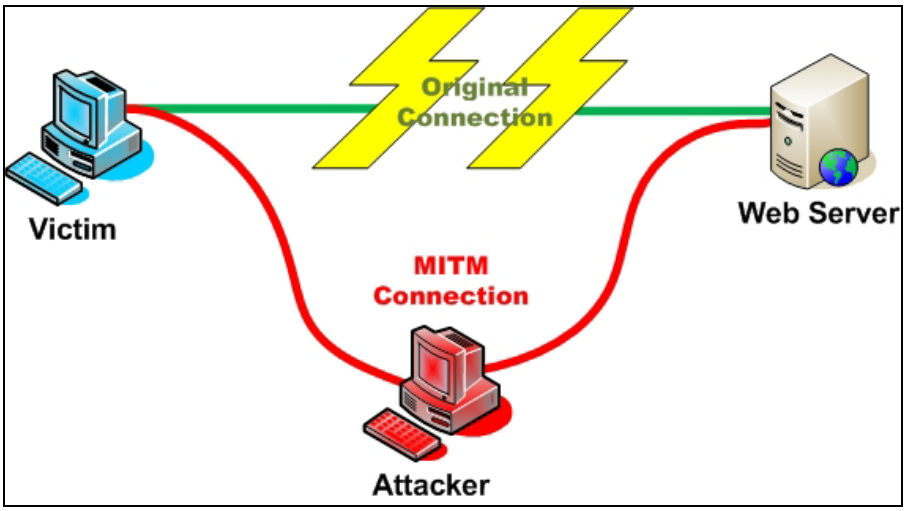
4.2.3 Pharming

Η επίθεση Pharming [15] είναι μια επίθεση ανακατεύθυνσης μιας ιστοσελίδας σε μια άλλη ψεύτικη σελίδα που οπτικά είναι ίδια με την αρχική. Το pharming μπορεί να επιτευχθεί, είτε με την αλλαγή του αρχείου host στον υπολογιστή του θύματος είτε με την αλλαγή της διεύθυνσης σε επίπεδο DNS διακομιστή. Οι διακομιστές DNS είναι υπολογιστικά συστήματα υπεύθυνα στην «μετάφραση» των ονομάτων του Internet σε πραγματικές διευθύνσεις. Π.χ. όταν θέλουμε να προσπελάσουμε έναν

ιστοχώρο, αντί να πληκτρολογήσουμε την εξής διεύθυνση http://10.0.2.35 πληκτρολογούμε http://www.myaddress.gr . Αυτόματα, ο διακομιστής DNS μας μεταφέρει στη διεύθυνση 192.168.1.35 που είναι μια φυσική διεύθυνση ενός συστήματος στο διαδίκτυο. Σε μια τέτοιου είδους επίθεση, η διεύθυνση που θα μεταφερθεί θα είναι παραδείγματος η 192.100.3.55 αντί της 192.168.1.35, ενώ ο χρήστης θα βλέπει κανονικά τη διεύθυνση http://www.myaddress.gr. (οι διευθύνσεις I.P. και διευθύνσεις ονομάτων είναι εντελώς τυχαίες στο παράδειγμά μας και δεν ανταποκρίνονται στην πραγματικότητα).

4.2.4 Man in the middle

Οι επιθέσεις **man in the middle** [16] παρακολουθούν μια επικοινωνία μεταξύ δύο συστημάτων. Παράδειγμα, σε μια συναλλαγή ο στόχος είναι η σύνδεση μεταξύ των δύο συστημάτων μεταξύ πελάτη και διακομιστή (π.χ. πελάτη και μιας τράπεζας). Χρησιμοποιώντας διάφορες τεχνικές, ο εισβολέας, «χωρίζει» σε δύο νέες συνδέσεις μία μεταξύ πελάτη και τον επιτιθέμενο και άλλη μια μεταξύ του επιτιθέμενου και του διακομιστή όπως φαίνεται στο σχήμα. Μόλις η σύνδεση πραγματοποιηθεί, ο επιτιθέμενος λειτουργεί ως ενδιάμεσος και τροποποιεί τα δεδομένα της επικοινωνίας.



Σχήμα 4.3 Man in the middle

4.2.5 Προβλέψιμοι κωδικοί εισόδου (Weak passwords)

Συχνά πολλοί χρήστες χρησιμοποιούν κοινούς κωδικούς προκειμένου να τους θυμούνται ευκολότερα. Κωδικοί εύκολα προβλέψιμοι μπορεί να είναι ένα όνομα από

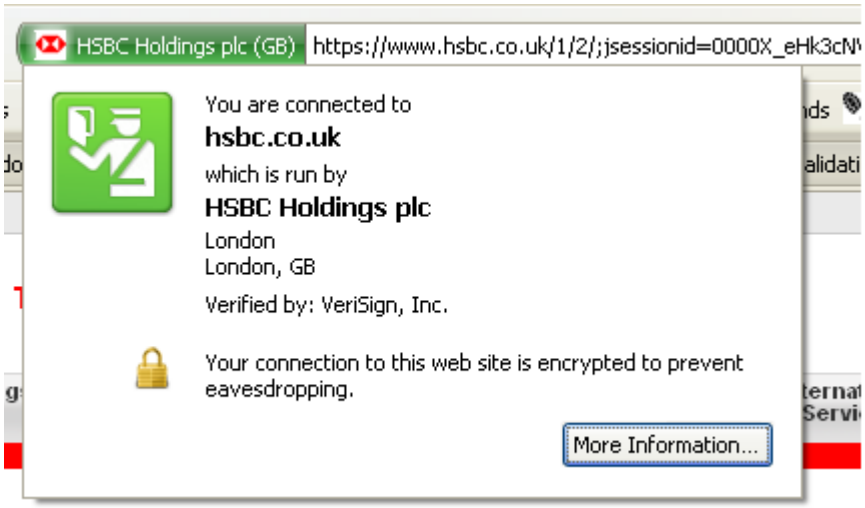
κατοικίδιο, μια ημερομηνία γέννησης, κωδικοί απλοί (π.χ. 12345). Ένας «ηλεκτρονικός διαρρήκτης» προσπαθεί με κάποιο τρόπο να βρει μεθόδους να διεισδύσει σε ένα σύστημα. Συνήθως τέτοιου είδους επιθέσεις γίνονται από γνωστούς ή από το οικείο περιβάλλον. Ένα παράδειγμα που θα μπορούσε κάποιος να πέσει σε παγίδα τέτοιου τύπου είναι οι σελίδες κοινωνικής δικτύωσης. Μέσα από αυτές τις σελίδες πολύ συχνά κάποιος βάζει προσωπικά στοιχεία. Αυτά τα στοιχεία είναι αρκετά προκειμένου να εισέλθει κάποιος σε μια σελίδα συναλλαγών και να αποσπάσει χρηματικό ποσό.

4.3 Μέθοδοι Προστασίας

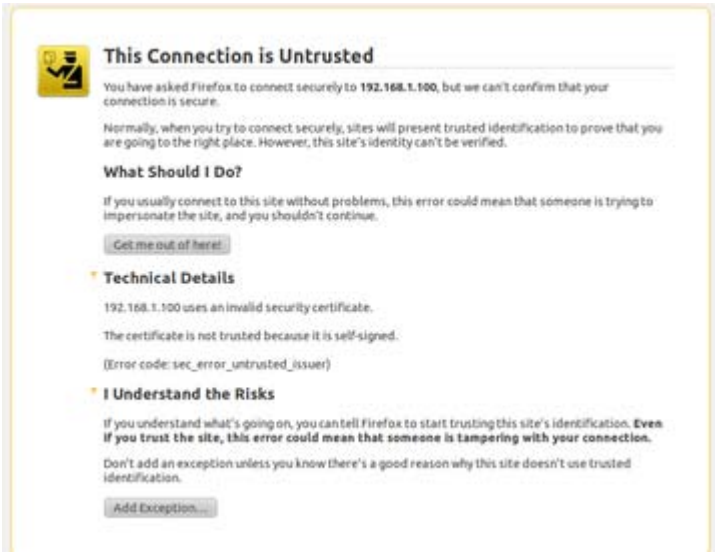
Οι τράπεζες προκειμένου να διασφαλίσουν την ακεραιότητα των δεδομένων στις ηλεκτρονικές συναλλαγές με τους πελάτες αλλάζουν πολύ συχνά τον τρόπο εισόδου στα συστήματα ενισχύοντας την ασφάλεια στων συστημάτων τους. Ενδεικτικά μέτρα που αναλαμβάνει μια τράπεζα προκειμένου να προστατεύσει τις ηλεκτρονικές της συναλλαγές είναι :

4.3.1 Ταυτοποίηση Τράπεζας

Η ιστοσελίδα που πελάτης καταχωρεί τους προσωπικούς κωδικούς εισόδου είναι πιστοποιημένη από εταιρεία ως πάροχο πιστοποίησης της ταυτότητας στο διαδίκτυο. Οι ασφαλείς ιστοσελίδες (παρατηρούμε ότι ξεκινούν με https:// αντί http://) βασίζονται στο πρωτόκολλο https (hypertext transfer protocol secure) που είναι ένας συνδυασμός του πρωτόκολλου http μαζί με ssl. Με άλλα λόγια, παρέχει μια κρυπτογραφημένη επικοινωνία μεταξύ της τράπεζας και του χρήστη μέσω από ασφαλή αναγνώριση. Στις ασφαλείς σελίδες εμφανίζεται συχνά ένα μικρό «λουκετάκι», επίσης πολλοί φυλομετρητές (browsers) αναγνωρίζουν αν η σελίδα που έχει ασφάλεια, έχει και έγκυρο πιστοποιητικό με το να εμφανίζουν έναν εικονικό «τροχονόμο» με χρώμα πράσινο ή μπλε ενώ αν δεν είναι ασφαλείς να εμφανίζουν μήνυμα προειδοποιητικό ότι υπάρχει πρόβλημα στην ιστοσελίδα που έχει εισέλθει ο χρήστης.



Σχήμα 4.4 Μήνυμα έγκυρου πιστοποιητικού ασφαλείας



Σχήμα 4.5 Μήνυμα μη έγκυρου πιστοποιητικού ασφαλείας

4.3.2 Ταυτοποίηση Χρήστη

Για την ταυτοποίηση των χρηστών e-Banking, οι τράπεζες χρησιμοποιούν έναν προσωπικό κωδικό εισόδου (password) μοναδικό για κάθε χρήστη της υπηρεσίας σε συνδυασμό με ένα Usern ame πο υ έχει δηλώσει ο χρήστης κάτα την πρώτη το υ είσοδο στην υπηρεσία.

Ο συνδυασμός αυτών των δύο επιτρέπει στον χρήστη την πρόσβαση του στις ενημερωτικές υπηρεσίες του e-Banking αλλά και τη διενέργεια συναλλαγών στις οποίες είτε είναι ο ίδιος δικαιούχος του λογαριασμού στον οποίο μεταφέρονται τα χρήματα είτε η μεταφορά αφορά σε πληρωμή οφειλών του π.χ. ΔΕΗ, δόση δανείου κ.λπ.

Για τη διενέργεια συναλλαγών στις οποίες ο παραλήπτης δεν είναι γνωστός και συνεπώς εμπεριέχουν ρίσκο (πχ. μεταφορές σε τρίτους, εμβάσματα),
ορισμένες Τράπεζες δεν αρκείται σε αυτό το επίπεδο ταυτοποίησης του χρήστη αλλά απαιτούν μια επιπλέον δικλείδα ασφαλείας,
την ψηφιακή πιστοποίηση. Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί το μέσο που παρέχει τη δυνατότητα στον κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-Banking. Το πιστοποιητικό, όταν εγκατασταθεί σε κάποιον υπολογιστή, προσφέρει τη δυνατότητα ταυτοποίησης του χρήστη και επιτρέπει συναλλαγές και μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο χρήστη.
Το ψηφιακό πιστοποιητικό είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο και εκδίδεται από τον Πάροχο Ψηφιακής Πιστοποίησης. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο πάροχος εκδίδει.
Πέραν των ψηφιακών πιστοποιητικών, στο e-Banking, δίνεται και η δυνατότητα ολοκλήρωσης των συναλλαγών προς τρίτους με Κωδικούς μιας Χρήσης οι οποίοι στέλνονται στο κινητό τηλέφωνο του χρήστη. Οι Κωδικοί μιας Χρήσης προσφέρουν ευελιξία και αυξημένη ασφάλεια καθότι έχουν σύντομη διάρκεια ζωής και μπορούν να χρησιμοποιηθούν για μια και μόνο συναλλαγή.
Επιπλέον ασφάλεια παρέχεται από ορισμένες τράπεζες με τη χρησιμοποίηση συσκευών που παράγουν για σύντομο χρονικό περιθώριο (συνήθως 5 λεπτά), μοναδικούς κωδικούς συναλλαγών.

4.3.2 Εξασφάλιση της μεταφοράς δεδομένων

Μια επιπρόσθετη δικλείδα ασφαλείας, με την οποία εξασφαλίζεται το απόρρητο κατά τη μεταφορά των δεδομένων, είναι η κρυπτογράφηση τους. Η Τράπεζες χρησιμοποιούν το πρωτόκολλο επικοινωνίας SSL (Secure Sockets Layer) μαζί με την κρυπτογράφηση στα 128bit το οποίο εξασφαλίζει την ασφάλεια των συναλλαγών μέσω διαδικτύου. Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2128 πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από τον browser (Internet Explorer) στον server της τράπεζας. Για αυτόν τον λόγο, η κρυπτογράφηση στα 128bit θεωρείται πρακτικά αδύνατο να παραβιαστεί. Μπορεί να αναγνωρίστεί εάν η σελίδα η οποία βρίσκεται είναι ασφαλής, καθώς το πρωτόκολλο

που εμφανίζεται με την διεύθυνση της τράπεζας μετατρέπεται από «http» σε «https» και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας.

4.3.3 Ελεγχόμενη πρόσβαση στα συστήματα της τράπεζας

Η πρόσβαση στα συστήματα της Τράπεζας προστατεύεται από τελευταία τεχνολογία "Τοίχο προστασίας" (Firewall), η οποία επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών απαγορεύοντας, παράλληλα, την πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Τράπεζας σε μη αναγνωρισμένους χρήστες.

4.3.4 Αυτόματη Αποσύνδεση Χρήστη

Μια επιπλέον δικλείδα ασφαλείας αποτελεί η αυτόματη αποσύνδεση χρήστη. Η ολοκλήρωση μιας συναλλαγής επιτρέπεται μέσα σε ένα συγκεκριμένο χρονικό όριο (δεκαπέντε λεπτά) μετά τη λήξη του οποίου το σύστημα αποσυνδέει τον χρήστη αυτόματα.

4.3.4 Υποχρεωτική Αλλαγή Κωδικών

Με την πρώτη εισαγωγή του νέου χρήστη στο e-Banking, το σύστημα τον υποχρεώνει στην άμεση αλλαγή του προσωπικού του κωδικού με κάποιον της επιλογής του, ο οποίος να είναι και πιο εύκολα μνημονεύσημος.

4.3.5 Μπλοκάρισμα Κωδικών

Οι προσωπικοί κωδικοί χρήστη μπλοκάρονται μετά από 3 συνεχόμενες λανθασμένες προσπάθειες εισαγωγής στο σύστημα ή σε συνολικά 9 λανθασμένες μέσα σε μια εβδομάδα, καθώς οι συνεχείς λανθασμένες προσπάθειες θεωρούνται ύποπτες.

4.3.6 Μπλοκάρισμα Πρόσβασης και μείωση ορίου συναλλαγών

Παράλληλα με το μπλοκάρισμα των κωδικών, μέσα από το e-Banking δίνεται η δυνατότητα στο χρήστη είτε να μπλοκάρει την πρόβασή του όποτε το επιθυμεί είτε να μειώσει το όριο που έχει για τις συναλλαγές του μέσω της υπηρεσίας.

4.3.7 Εισαγωγή Στοιχείων Εισόδου

Καθώς παρατηρήθηκε η εμφάνιση ιών, οι οποίοι είχαν τη δυνατότητα να καταγράφουν πληκτρολογήσεις χρηστών, υιοθετήθηκε η προαιρετική χρήση εικονικού πληκτρολογίου για την καταχώρηση του ενός από τα δύο στοιχεία ταυτοποίησης. Έτσι, ακόμα κι αν μπορούσε να υπεκλαπεί ο ένας από τους δύο κωδικούς ταυτοποίησης, δεν θα είχε καμία ισχύ η μεμονωμένη χρήση του και ο χρήστης θα παρέμενε ασφαλής.

4.4 Τι πρέπει να κάνουν οι Χρήστες των συστημάτων

Κάποιες ενδεικτικές οδηγίες κοινοποιούν οι Τράπεζες προκειμένου ο χρήστης να μπορεί να αισθάνεται πιο ασφαλής όταν κάνει ηλεκτρονικές συναλλαγές με την Τράπεζα. Ο κάθε πελάτης που κάνει χρήση των ηλεκτρονικών υπηρεσιών μιας τράπεζας, θα πρέπει να ακολουθεί τις παρακάτω οδηγίες :

- **Προσωπικά e-mails,** των οποίων ως αποστολέας εμφαίνεται παραπλανητικά η εκάστοτε τράπεζα, και είτε ζητούν την επιβεβαίωση των στοιχείων του χρήστη (κωδικούς e-Banking, στοιχεία λογαριασμών και καρτών, κτλ) είτε περιέχουν συνδέσμους (links) οι οποίοι οδηγούν σε ψεύτικες οθόνες καταχώρησης στοιχείων μη προερχόμενες από την τράπεζα. Επίσης, έχουν παρατηρηθεί και emails τα οποία μέσω συνδέσμων εγκαθιστούν ιούς στους υπολογιστές των χρηστών. Οι ιοί αυτοί έχουν τη δυνατότητα να καταγράφουν και να αποθηκεύουν οποιαδήποτε στοιχεία καταχωρεί ο χρήστης μέσω του πληκτρολογίου του, όπως κωδικοί πρόσβασης σε ηλεκτρονικές υπηρεσίες.
- **Οθόνες καταχώρισης στοιχείων**, οι οποίες μπορεί να εμφανιστούν ξαφνικά στην οθόνη μολυσμένου από σχετικό ιό υπολογιστή, ακόμα και αν ο χρήστης πλοηγείται σε αυθεντικές ιστοσελίδες τραπεζικού site. Οι οθόνες καταχώρισης στοιχείων συνήθως μοιάζουν με τις ιστοσελίδες της εκάστοτε τράπεζας, αλλά δεν ανήκουν σε αυτήν και ζητούν από τον χρήστη να καταχωρίσει προσωπικά του στοιχεία.
- **Τηλεφωνήματα**, στα οποία ο ομιλών, υποστηρίζοντας πως είναι εκπρόσωπος της τράπεζας, προσπαθεί να αποσπάσει προσωπικά στοιχεία του πελάτη.

Σε περιπτώσεις που παρατηρηθεί οποιαδήποτε απάτη προς τους ίδιους, καλό είναι να επικοινωνεί με την Τράπεζα άμεσα και να ακολουθεί τις οδηγίες τους.

Ο χρήστης θα πρέπει να εκτελεί πάντα τις εξής διαδικασίες εισόδου :

- Να πληκτρολογεί ο ίδιος τη διεύθυνση της Τράπεζας και όχι από κάποιο link.
- Να κάνει κλίκ στο «λουκέτο» πάνω στη διεύθυνση ώστε να βρίσκεται στην αυθεντική διεύθυνση της Τράπεζας.
- Να εγκαθιστά προγράμματα προστασίας από ιούς. Η εμφάνιση νέων και εξελιγμένων ιών καθιστά τη συχνή ανανέωση των προγραμμάτων που τους καταπολεμούν απαραίτητη.

Ο χρήστης **δεν** θα πρέπει να εκτελεί πάντα τις εξής διαδικασίες εισόδου :

- Να μη μοιράζεται με οποιονδήποτε τρίτο τα προσωπικά στοιχεία του, ακόμα και αν κάποιος ισχυρίζεται ότι εκπροσωπεί την Τράπεζά μας ή ότι ζητά τα στοιχεία σας για λόγους ασφάλειας.
- Να μην κάνει login στην ιστοσελίδα της Τράπεζας χωρίς να υπάρχει το κίτρινο λουκέτο μέσω του οποίου μπορεί να πιστοποιήσει την ταυτότητα της.
- Να μην εγκαθιστά προγράμματα στον υπολογιστή τουτην ταυτότητα των οποίων δεν είναι σίγουρος ότι γνωρίζει.

5 Εμπειρική Έρευνα

Στην παρούσα ενότητα, έχουμε καταγράψει την εμπειρία μας στον τραπεζικό κλάδο σε γενικές γραμμές όπως επίσης παραθέτουμε και έρευνα σύμφωνα με την οποία απευθύνουμε ερωτήσεις στο κοινό ώστε να διεξάγουμε συμπεράσματα κατά πόσο είναι εξοικειωμένος ο χρήστης με τις νέες τεχνολογίες.

Προκειμένου να γίνει αντιληπτός ο τρόπος υλοποίησης μιας υπηρεσίας e-banking ή και m-banking, διάφορα τμήματα της τράπεζας συνεργάζονται για να συνθέσουν αυτού του είδους τις υπηρεσίες. Στο κεφάλαιο αυτό αναλύουμε μια οργανωτική δομή του e-banking στις Ελληνικές Τράπεζες αναλύοντας τα τμήματα που συνεργάζονται προκειμένου να υλοποιηθεί η σχετική υπηρεσία. Στη συνέχεια αναφέρουμε τη χρήση της υπηρεσίας m-banking ανά Τράπεζα όπως εφαρμόζεται το m-banking στις Ελληνικές Τράπεζες. Τέλος, έχουμε θέσει στο κοινό ερωτήματα σχετικά με τις υπηρεσίες της ηλεκτρονικής Τραπεζικής και παρουσιάζουμε τα αποτελέσματα της έρευνας.

5.1.1. Η οργανωτική δομή του e-banking στις Ελληνικές Τράπεζες

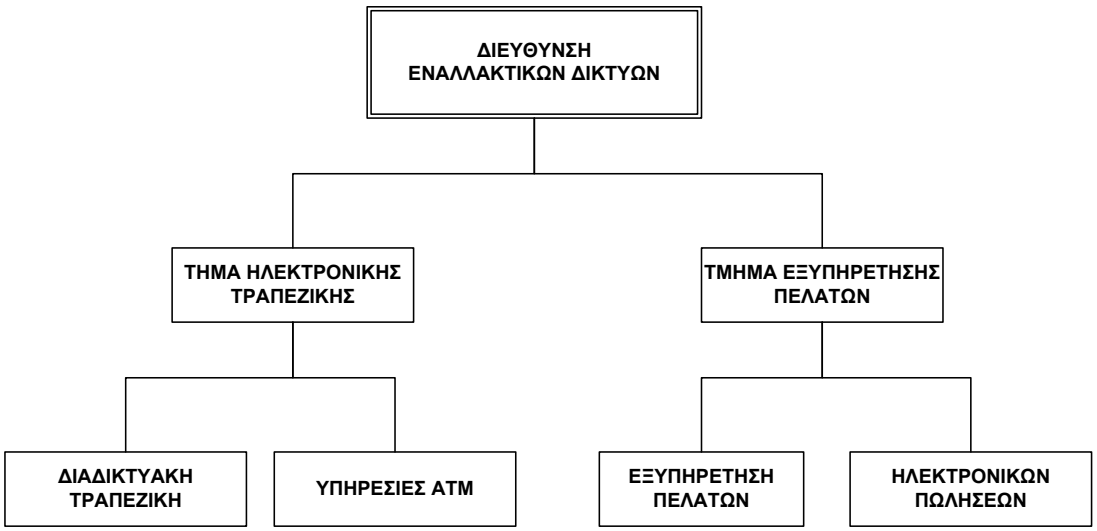
Για να δημιουργηθεί μια συναλλαγή διαθέσιμη στα «κανάλια» του διαδικτύου όπως είναι και το e-banking, επιμέρους τμήματα συνεργάζονται ώστε το τελικό αποτέλεσμα να είναι διαθέσιμο στους πελάτες της τράπεζας. Τα τμήματα που θα αναφέρουμε είναι ενδεικτικά αλλά άμεσα εμπλεκόμενα όταν πρόκειται να υλοποιηθεί μια συναλλαγή στο διαδίκτυο. Ενδεικτικά τμήματα είναι :

- Τμήμα Εναλλακτικών Δικτύων
- Διεύθυνση Επικοινωνίας
- Διεύθυνση Marketing
- Διεύθυνση Πληροφορικής
- Διεύθυνση Ασφαλείας

5.1.2 Εναλλακτικά Δίκτυα (Remote Channels)

Η διεύθυνση των εναλλακτικών δικτύων είναι το τμήμα εκείνο της Τράπεζας το οποίο είναι υπεύθυνο για τις προσφερόμενες υπηρεσίες μέσω του διαδικτύου. Ο ρόλος του είναι να παρακολουθεί τον ανταγωνισμό και να προάγει νέες υπηρεσίες προς τους πελάτες της Τράπεζας σε συνεργασία με τα υπάρχοντα τμήματα της Τράπεζας. Το τμήμα των εναλλακτικών δικτύων είναι υπεύθυνο

πέρα από τις υπηρεσίες του διαδικτύου και για διάφορα τμήματα της Τράπεζας όπως οι υπηρεσίες εξυπηρέτησης πελατών (contact center), το τμήμα παρακολούθησης και εξυπηρέτησης των Α.Τ.Μ., τηλεφωνικές πωλήσεις κλπ. Ένα σχετικό οργανόγραμμα της Διεύθυνσης μπορείτε να δείτε στο σχήμα 2.7



Σχήμα 2.7 Οργανόγραμμα Διεύθυνσης Εναλλακτικών δικτύων

Μια μικρή αναφορά στα επιμέρους τμήματα του τμήματος εναλλακτικών δικτύων είναι :

5.1.2.1 Τμήμα Εξυπηρέτησης Πελατών

Το τμήμα εξυπηρέτησης Πελατών είναι ένα τμήμα που εξυπηρετεί τους πελάτες της Τράπεζας μέσω του phone banking. Το τμήμα αυτό εξειδικεύεται στην παροχή κατάλληλων πληροφοριών στους πελάτες της Τράπεζας από εξειδικευμένο προσωπικό είτε εκτελούν συναλλαγές για λογαριασμό πελατών. Κάθε υπάλληλος τηλεφωνικής εξυπηρέτησης (agent) παρέχει συγκεκριμένες πληροφορήσεις στους πελάτες ύστερα από κατάλληλη αναγνώριση. Για λόγους που πολλές φορές μπορεί να υπάρχουν αμφιβολίες από πελάτες για εκτέλεση συναλλαγών, κάθε κλήση καταγράφεται και έτσι αποτρέπονται διάφοροι «κακόβουλοι» χειρισμοί από τους εμπλεκόμενους.

Ορισμένες από τις υπηρεσίες που παρέχει το τμήμα εξυπηρέτησης είναι :

- Πληροφορίες για λογαριασμούς κάρτες και δάνεια
- Πληροφορίες για συναλλαγές Λογ/σμών
- Μεταφορές ποσών μεταξύ λογαριασμών

- Αποστολή χρημάτων στις τράπεζες εσωτερικού και εξωτερικού
- Απεμπλοκή κωδικών Internet Banking
- Αγοραπωλησία Χρηματιστηριακών μετοχών
- Πληρωμή λογαριασμών συμβεβλημένων με την Τράπεζα (ΔΕΗ,ΕΥΔΑΠ,ΟΤΕ κλπ).

Το τμήμα εξυπηρέτησης πελατών μπορεί να διαχωριστεί σε δύο επιμέρους τμήματα που περιλαμβάνουν κατά κύριο όγκο, υπηρεσίες εξυπηρέτησης μέσω του τηλεφωνικού κέντρου και διαχωρίζεται στο τμήμα εξυπηρέτησης πελατών, που αφορά πελάτες που έχουν καλέσει την τράπεζα και έχουμε αναφερθεί πιο πάνω αλλά και στο τμήμα πωλήσεων που αφορά κλήσεις προς πελάτες της τράπεζας για πληροφόρηση είτε για πώληση προϊόντων και υπηρεσιών ανάλογα με την κατηγοριοποίηση του πελάτη.

5.1.2.2 Τμήμα Ηλεκτρονικής Τραπεζικής

Το τμήμα αυτό μπορεί να διαχωριστεί σε δύο επιμέρους τμήματα όπως είναι το τμήμα διαδικτυακής τραπεζικής και την υπηρεσία ATM.

Το τμήμα διαδικτυακής τραπεζικής ασχολείται με τις υπηρεσίες του διαδικτύου και διαθέτει πολλές επιμέρους αρμοδιότητες. Μία από τις αρμοδιότητες του είναι να δέχεται τα αιτήματα από το τμήμα εξυπηρέτησης πελατών τα οποία δεν μπορούν να απαντηθούν από το προσωπικό του τηλεφωνικού κέντρου και χρειάζονται περεταίρω διερεύνηση όπως για παράδειγμα, αν κάποιος πελάτης της τράπεζας διαμαρτυρηθεί για κάποια επιβάρυνση η οποία δε θα έπρεπε να υφίσταται στο λογαριασμό του που ενημερώθηκε. Στην προκειμένη περίπτωση, ο αρμόδιος υπάλληλος θα κάνει διερεύνηση στο σύστημα με σκοπό να εντοπίσει τυχόν σφάλμα στα δεδομένα. Σε περίπτωση που εντοπίσει τη λύση του προβλήματος, θα ενημερώσει τον πελάτη ανάλογα με το αίτημα του (ηλεκτρονικά ή τηλεφωνικά). Σε περίπτωση που δεν μπορεί να εντοπίσει άμεσα το πρόβλημα, τότε προωθεί το αίτημα εσωτερικά προς περεταίρω διερεύνηση (π.χ. συνεργασία με το τμήμα πληροφορικής) ώστε ενημερωθεί ο πελάτης για το αίτημα του.

Μια επιπλέον αρμοδιότητα του συγκεκριμένου τμήματος είναι να δημιουργήσει τις προδιαγραφές για νέες συναλλαγές και για οποιοδήποτε υλικό θα αναρτηθεί στο διαδίκτυο (e-banking, m-banking, bank's site κλπ) .

Η υπηρεσία Α.Τ.Μ. ασχολείται αποκλειστικά με την εξυπηρέτηση των πελατών μέσω των ΑΤΜ μηχανών. Παραλαμβάνει οποιοδήποτε υλικό που αφορά στην ανάρτηση διαφημίσεων είτε την προσθήκη συναλλαγών στα ATMs όπως επίσης αναλαμβάνει οποιαδήποτε επικοινωνία που αφορά με ερωτήσεις ή παράπονα πελατών συντονίζοντας τα αρμόδια τμήματα για επιπλέον διερεύνηση.

5.1.3 Διεύθυνση Επικοινωνίας

Η διεύθυνση επικοινωνίας και Διαφήμισης είναι υπεύθυνη για την επικοινωνιακή πολιτική της Τράπεζας. Η συγκεκριμένη διεύθυνση συνεργάζεται με διάφορα τμήματα της τράπεζας, μεταξύ αυτών και της διεύθυνσης των εναλλακτικών δικτύων προκειμένου να προωθηθεί μια διαφημιστική καμπάνια. Ακολουθώντας την εξέλιξη της τεχνολογίας, η Τράπεζα επικοινωνεί τα προϊόντα, τις υπηρεσίες και τα πακέτα προσφορών που διαθέτει (TV & Radio spots, νέα προϊόντα, αλλαγή σε υφιστάμενα, Δελτία Τύπου, διαφημιστικό υλικό) στο καταναλωτικό κοινό και μέσω του Διαδικτύου. Για την δημιουργία των τελικών προϊόντων διαφήμισης, συνεργάζεται με εξωτερικούς συνεργάτες και τους κατευθύνει ή εγκρίνει το τελικό παραγόμενο προϊόν διαφήμισης.

5.1.4 Διεύθυνση Marketing

Η διεύθυνση marketing, είναι υπεύθυνη για τη διαμόρφωση των κατάλληλων προϊόντων στην αγορά με σκοπό την προσέλκυση νέων πελατών είτε να επεκτείνουν την σχέση της Τράπεζας τους με υφιστάμενους πελάτες. Υπάρχουν διάφορα τμήματα της υπηρεσίας marketing όπως τμήμα που ασχολείται με την προώθηση διαφημιστικής καμπάνιας μέσω των τηλεοπτικών και ραδιοφωνικών καναλιών και διαδικτύου. Η διεύθυνση marketing είναι ανεξάρτητο τμήμα και αναφέρεται στην διοίκηση ώστε οι αποφάσεις που λαμβάνονται από το συγκεκριμένο τμήμα, να εγκρίνονται και να προωθούνται άμεσα με σκοπό την ταχύτερη προώθηση των υπηρεσιών. Ο στόχος του συγκεκριμένου τμήματος επιγραμματικά είναι :

Αύξηση της κερδοφορίας του κάθε τμήματος

- Αύξηση των ενεργών πελατών
- Αύξηση των διαθέσιμων προϊόντων και υπολοίπων (καταθέσεων)
- Βελτίωση κερδών

- Αύξηση της εμπιστοσύνης προς την Τράπεζα και μείωση της τυχόν κακής φήμης

Καλύτερη κατανόηση των αναγκών των καταναλωτών

- Διαφοροποίηση του επιπέδου των υπηρεσιών , των προϊόντων, των τιμών
- Ικανοποίηση των αναγκών των πελατών με ταυτόχρονη επίτευξη των προτεραιοτήτων της Τράπεζας.

Η στρατηγική του τμήματος marketing είναι σε γενικές γραμμές

Νέοι πελάτες μέσω νέων προϊόντων :

- Νέα αμοιβαία κεφάλαια
- Απόκτηση Πιστωτικών καρτών
- Αμοιβαία κεφάλαια με υψηλές αποδόσεις

Διατήρηση υπαρχόντων πελατών

- Ενεργοποίηση αδρανείς και ανενεργούς πελάτες
- Αμυντικό μηχανισμό για τους νέους πελάτες στα δάνεια και στις καταθέσεις των.
- Δημιουργία καινοτόμων προτάσεων και προσφορών

Γνωρίζοντας τους Πελάτες καλύτερα με επικέντρωση σε διασταυρωμένες πωλήσεις .

5.1.5 Διεύθυνση Πληροφορικής

Η Διεύθυνση Πληροφορικής είναι υπεύθυνη να εκπονεί και να υλοποιεί την κατάλληλη στρατηγική ανάπτυξης συστημάτων και εφαρμογών που συνάδουν με τους στόχους της τράπεζας. Προς τούτο προετοιμάζει εγκαίρως και εισηγείται προς έγκριση τους αναγκαίους οικονομικούς προϋπολογισμούς (τόσο βραχυπρόθεσμα αλλά και μεσοπρόθεσμα), και λαμβάνει όλα εκείνα τα απαραίτητα οργανωτικά μέτρα που απαιτούνται για την εξασφάλιση των πόρων (ανθρωπίνων και μη) ώστε να μπορέσει να υλοποιήσει στο μέλλον αυτή την στρατηγική της τράπεζας επί όλων των θεμάτων πληροφορικής πριν μπορέσει να προχωρήσει σε κάποια ανάθεση ή υλοποίηση έργου.

Η Διεύθυνση Πληροφορικής εξυπηρετεί τους εξής τρεις βασικούς σκοπούς:

1. Την Υλοποίηση, Διαχείριση, και Συντήρηση των Πληροφοριακών και Δικτυακών συστημάτων της Τράπεζας. Πληροφοριακά συστήματα θεωρείται ο εξοπλισμός εκείνος (υλικό και λογισμικό) που υποστηρίζει την εκτέλεση των συναλλαγών και την διακίνηση των πληροφοριών ενός πελάτη, ενώ Δικτυακά συστήματα είναι ο εξοπλισμός εκείνος (υλικό και λογισμικό) που επιτρέπει την εξυπηρέτηση του πελάτη από πολλά διαφορετικά και ίσως ανόμοια σημεία ανά τον κόσμο. Τέτοια σημεία μπορεί να είναι τα Καταστήματα, τα ATM, το Διαδίκτυο, το Τηλέφωνο, τα Σημεία Πώλησης (Εμπορικά καταστήματα).
2. Την Επιλογή και Εφαρμογή της Τεχνολογίας βάσει συγκεκριμένης στρατηγικής ώστε να δημιουργηθούν νέες υπηρεσίες, να μειωθεί το λειτουργικό κόστος και να βελτιωθεί η ποιότητα εξυπηρέτησης των πελατών.
3. Την Μέριμνα για Ασφάλεια των εκτελούμενων συναλλαγών και της διακίνησης των δεδομένων του πελάτη από άκρο σε άκρο, συμμορφούμενη με τις εκάστοτε πολιτικές ασφάλειας όπως αυτές διαμορφώνονται στο τραπεζικό περιβάλλον, και κοινοποιούνται υπό την μορφή οδηγιών και υποχρεώσεων από την Τράπεζα της Ελλάδος ή άλλες ρυθμιστικές και κανονιστικές αρχές.

5.1.6 Διεύθυνση Ασφάλειας

Η διεύθυνση Ασφάλειας είναι υπεύθυνη για την Ασφάλεια των συστημάτων της Τράπεζας σε όλους τους τομείς πρόσβασης σε αυτή. Στα διαδικτυακά συστήματα, επιβάλει τους κανόνες πρόσβασης σε αυτά και ενημερώνει τους αρμόδιους αναλυτές ή δίκτυο σε περίπτωση που διαπιστωθεί κάποια

5.2.1 Η εφαρμογή του m-banking στις Ελληνικές Τράπεζες – Εφαρμογή ανά Τράπεζα

Οι Ελληνικές Τράπεζες παρουσιάζουν λύσεις mobile banking είτε μέσω web όπως και εφαρμογές.

5.2.1.1 Alpha mobile banking

Η Alpha προσφέρει την εφαρμογή Alpha Mobile Banking για i-Phone. Οι υπηρεσίες που προσφέρονται είναι :

- υπηρεσίες για τα υπόλοιπα και τις κινήσεις των καρτών και λογαριασμών
- ενημέρωση για bonus πόντους των καρτών
- πληρωμές λογαριασμών Δημοσίου, Ταμείων , Τηλεφωνίας κ.α.
- πληρωμές πιστωτικών καρτών/δανείων
- μεταφορές ποσών σε λογαριασμούς
- εντοπισμός ATM και καταστημάτων σε χάρτες

5.2.1.2 CITI MOBILE (CITIBANK)

Η Citibank είναι από τις τράπεζες που προσφέρουν εφαρμογές για τις δημοφιλέστερες πλατφόρμες (iOS, Android και Blackberry).

Με την εφαρμογή city-mobile μπορείτε :

- να βλέπετε υπόλοιπα και κινήσεις των τραπεζικών λογαριασμών (ιστορικά τριών μηνών)
- υπόλοιπα και τις πρόσφατες κινήσεις των πιστωτικών καρτών σας
- να μεταφέρετε χρήματα μεταξύ των λογαριασμών σας αλλά και σε τράπεζες στην Ελλάδα ή στο εξωτερικό.
- Πληρωμές πιστωτικών καρτών
- Πληρωμές λογ/σμών
- Αναζήτηση καταστημάτων

Επιπλέον, μέσα από την εφαρμογή, δίνεται η δυνατότητα επικοινωνίας με την υπηρεσία Cityphone 24/7 όπως και αποσύνδεση του χρήστη μετά την πάροδο ανενεργής χρήσης μετά από πέντε λεπτά.

QR Code (**Quick Response Code**) είναι σήμα κατατεθέν ενός τύπου (matrix) barcode που αρχικά σχεδιάστηκε για την αυτοκινητοβιομηχανία. Πρόσφατα, έγινε δημοφιλής λόγω ότι μπορεί να αναγνωστεί πιο γρήγορα από τις συσκευές αλλά και να αποθηκεύσει περισσότερη πληροφορία από τα κοινά barcodes τύπου UPC

- αναζήτηση ATM και καταστημάτων
- πληροφόρηση για επιτόκια, τιμές αμοιβαίων, δελτίο συναλλάγματος

Επίσης μπορείτε από την εφαρμογή να συνδεθείτε με εκπρόσωπο της τράπεζας για συναλλαγές και τηλεφωνική εξυπηρέτηση.

5.2.1.3 ΕΘΝΙΚΗ MOBILE BANKING

Η Εθνική Τράπεζα διαθέτει εφαρμογή για συσκευές i-phone, Symbian, windows phone και Blackberry.

Σε ότι αφορά την εφαρμογή για i-Phone, προσφέρει βασικές υπηρεσίες, όπως :

- ενημέρωση για τους λογαριασμούς και τις πιστωτικές κάρτες
- μεταφορές χρημάτων σε λογαριασμούς της ίδιας τράπεζας
- εξόφληση λογαριασμών ΔΕΗ, ΟΤΕ, Cosmote, Vodafone
- πληρωμή πιστωτικής κάρτας
- εντοπισμός των πλησιέστερων καταστημάτων ή ATM
- επικοινωνία με εκπρόσωπο της τράπεζας

5.2.1.4 ΕΜΠΟΡΙΚΗ MOBILE BANKING

Η Εμπορική Τράπεζα διαθέτει τη δική της εφαρμογή για i-Phone, χωρίς να υποστηρίζονται άλλες πλατφόρμες κινητών. Η εφαρμογή δίνει τη δυνατότητα να ενημερωθείτε για τα υπόλοιπα και τις κινήσεις των λογαριασμών των καρτών και δανείων όπως και αναλυτικές πληροφορίες για τα προϊόντα. Με την εφαρμογή μπορούν οι χρήστες να πληρώσουν πιστωτικές κάρτες της Εμπορικής Τράπεζας , λογαριασμούς δημοσίων φορέων και ταμείων αλλά και λογαριασμών ενέργειας, ύδρευσης, τηλεφωνίας και διαφόρων εταιριών. Τέλος, μπορείτε να αναζητήσετε ή εντοπίσετε πλησιέστερο κατάστημα ή ATM μέσω GPS και να επικοινωνήσετε με το κέντρο εξυπηρέτησης πελατών.

5.2.1.5 EUROBANK M-BANKING

Η Eurobank έχει διάφορες λύσεις για όλες τις φορητές πλατφόρμες. Με την εφαρμογή m-banking μπορείτε να ενημερωθείτε για τους λογαριασμούς, τις κάρτες, τα δάνεια και τις επενδύσεις. Επίσης, μπορείτε να μεταφέρετε χρήματα

μεταξύ λογαριασμών σας και σε λογαριασμούς τρίτων Eurobank και άλλων τραπεζών εντός Ελλάδας. Επιπλέον μέσα από το m-banking, μπορούν να γίνει εξόφληση της κάρτας, κάρτες τρίτων και άλλων Τραπεζών, πληρωμή δανείου καθώς και λογαριασμών όπως ΔΕΗ,ΟΤΕ,ΕΥΔΑΠ,Vodafone, ΦΠΑ, ΟΑΕΕ). Άλλες παροχές που μπορούν να γίνουν μέσα από το κινητό είναι η εύρεση του κοντινότερου ATM ή κατάστημα Eurobank και η τηλεφωνική εξυπηρέτηση από εκπρόσωπο της τράπεζας.

5.2.1.6 MARFIN MOBILE BANKING & DIRECT

Η Marfin Egnatia Bank προσφέρει δύο ειδών υπηρεσίες mobile banking. Η πρώτη απευθύνεται σε χρήστες Smartphones ανεξαρτήτως πλατφόρμας με σύνδεση στο Internet. Η χρήση της γίνεται μέσω του browser του κινητού. Το Mobile Banking της Marfin Egnatia Bank προσφέρει τη δυνατότητα παρακολούθησης υπολοίπων και κινήσεων λογαριασμών και πιστωτικών καρτών, πραγματοποίηση πληρωμών λογαριασμών και μεταφορών κεφαλαίων, ενημέρωση για τις τιμές μετοχών και δεικτών καθώς και τιμές συναλλάγματος και, τέλος, εύκολη αναζήτηση των καταστημάτων και των ATM της Marfin Egnatia Bank, μέσα από την οθόνη του κινητού τηλεφώνου. Για χρήστες iOS και Android υπάρχει η υπηρεσία MarfinDirect όπως και υποστηρίζει συσκευές iPhone, iPod Touch, iPad και συσκευές κινητής τηλεφωνίας και tablets που λειτουργούν σε λειτουργικό σύστημα android. Επιπλέον μπορείτε να στείλετε ειδοποίηση απώλειας κάρτας προκειμένου να επικοινωνήσει άμεσα ένας εξουσιοδοτημένος εκπρόσωπος της Τράπεζας. Επιπλέον παροχές είναι ότι μπορείτε να αναζητηθούν διευθύνσεις των καταστημάτων και των ATM της Marfin Egnatia Bank και να εντοπίσετε την τοποθεσία τους στο χάρτη.

5.2.1.7 MILLENNIUM BANK M-BANKING

Η Millennium bank δε διαθέτει ακόμα κάποια εξειδικευμένη εφαρμογή για «έξυπνα κινητά» αλλά ένα ειδικά σχεδιασμένο web-site για την πρόσβαση από το κινητό και το tablet pc. Έχει το πλεονέκτημα ότι δε χρειάζεται εγκατάσταση πρόσθετης εφαρμογής αλλά και ότι υποστηρίζονται όλες οι φορητές πλατφόρμες. Το μόνο που απαιτείται είναι ένας mobile browser.

Με την υπηρεσία m-banking μπορείτε να προβάλλετε τη λίστα των τρεχούμενων, καταθετικών και δανειακών λογαριασμών, να προβάλλετε τις

κινήσεις των πιστωτικών καρτών, να μεταφέρετε ποσά μεταξύ των λογαριασμών της Millennium bank, την πληρωμή της κάρτας όπως και πληρωμή πολλών οργανισμών (ΔΕΗ,ΕΥΔΑΠ,Cosmote, e-PASS κλπ) με τη δυνατότητα ο ίδιος ο χρήστης μέσα από το e-banking να επιλέγει τις συναλλαγές που θα εμφανίζονται στο κινητό.

5.2.1.8 WINBANK MOBILE APPS

Η Τράπεζα Πειραιώς, έχει τρείς διαφορετικές εφαρμογές ηλεκτρονικής τραπεζικής : Winbank Mobile, Winbank EasyPay και Winbank Λεφτά στο λεπτό. Και οι τρείς είναι διαθέσιμες για κινητά με λειτουργικό σύστημα iOS όπως και Android.

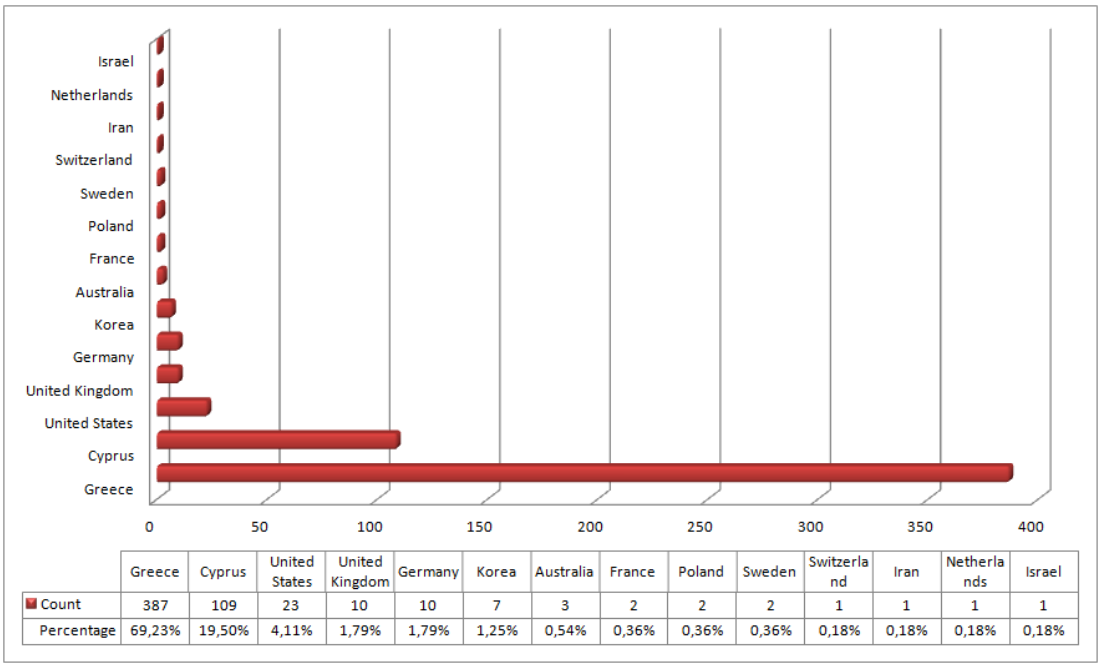
Το winbank mobile είναι η βασική εφαρμογή της Τράπεζας Πειραιώς. Οι δυνατότητες που σας παρέχει είναι η ενημέρωση για τα υπόλοιπα και τις κινήσεις των λογαριασμών και καρτών, πληροφόρηση δανείων, μεταφορές ποσών σε λογαριασμούς, εμβάσματα σε άλλες Ελληνικές ή Ευρωπαϊκές Τράπεζες, πληρωμές πιστωτικών καρτών, πληρωμές Δημοσίου, ταμείων, τηλεφωνίας κλπ., χρηματιστήριο, εντοπισμός ATM και καταστημάτων σε χάρτες καθώς και άμεση επικοινωνία με e-mail ή τηλέφωνο με την Τράπεζα.

Η εφαρμογή «Λεφτά στο Λεπτό» σας δίνει τη δυνατότητα να κάνετε ανάληψη μετρητών από οποιοδήποτε ATM της Τράπεζας χωρίς τη χρήση της κάρτας και να στέλνετε χρήματα σε όποιον επιθυμείτε, να βρείτε το πλησιέστερο σημείο υπηρεσιών της Τράπεζας (ATM, κατάστημα, μηχανήματα EasyPay κλπ).

Με την εφαρμογή Winbank Easypay μπορείτε να πληρώνετε τους λογαριασμούς με σάρωση των barcodes του λογαριασμού, φωτογραφίζοντας το λογαριασμό ή πληκτρολογώντας τα απαραίτητα στοιχεία. Υποστηρίζονται οι λογαριασμοί ΔΕΗ, ΕΥΔΑΠ,ΟΤΕ, Cosmote, Vodafone και Wind, ενώ η πληρωμή γίνεται με οποιαδήποτε πιστωτική ή χρεωστική κάρτα (Visa ή Mastercard).

5.3 Πρωτογενή έρευνα με ερωτήματα σε καταναλωτές

Σκοπός της έρευνας ήταν να αντλήσουμε πληροφορίες με το πόσο οι χρήστες είναι εξοικειωμένοι με τις νέες τεχνολογίες και κατά πόσο γίνεται χρήση της Ηλεκτρονικής Τραπεζικής. Η Έρευνα διεξήχθη ηλεκτρονικά μέσω της ιστοσελίδας http://www.freequeston.com από το διάστημα 25/2/2012 έως 17/3/2012. Προκειμένου να μπορέσουμε να έχουμε όσο το δυνατόν μεγαλύτερη απόκριση στην έρευνα, το ερωτηματολόγιο, στάλθηκε μέσω ηλεκτρονικής αλληλογραφίας σε πάνω από 4000 άτομα όπως επίσης κοινοποιήθηκε και στην ιστοσελίδα κοινωνικής δικτύωσης “facebook”.



	Greece	Cyprus	United States	United Kingdom	Germany	Korea	Australia	France	Poland	Sweden	Switzerland	Iran	Netherlands	Israel
Count	387	109	23	10	10	7	3	2	2	2	1	1	1	1
Percentage	69,23%	19,50%	4,11%	1,79%	1,79%	1,25%	0,54%	0,36%	0,36%	0,36%	0,18%	0,18%	0,18%	0,18%

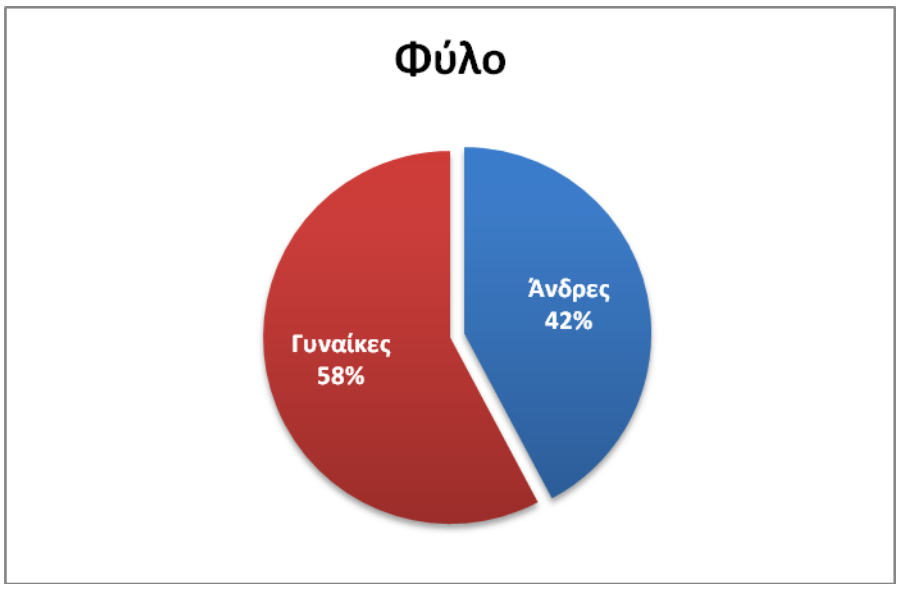
Σχήμα 5.1 Πλειονότητα ερωτηθέντων

Από τους Ερωτηθέντες, οι πλειονότητα που απαντήσανε το ερωτηματολόγιο (Σχήμα 5.1) ήταν από Ελλάδα με ποσοστό 69,23% (387 άτομα), ενώ από Κύπρο απάντησαν αντίστοιχα ποσοστό 19,5% (109 άτομα). Οι ερωτήσεις που τέθηκαν είχαν τη δομή δυναμικών απαντήσεων ανάλογα με εισαγωγή της ερώτησης. Έτσι οι επόμενες ερωτήσεις διαμορφώθηκαν ανάλογα με τις απαντήσεις των χρηστών.

Παρά τις τεχνικές δυσκολίες που διεξήχθησαν στην ηλεκτρονική πλατφόρμα των ερωτήσεων, θεωρούμε το δείγμα επαρκές για να βγάλουμε καθοριστικό συμπέρασμα.

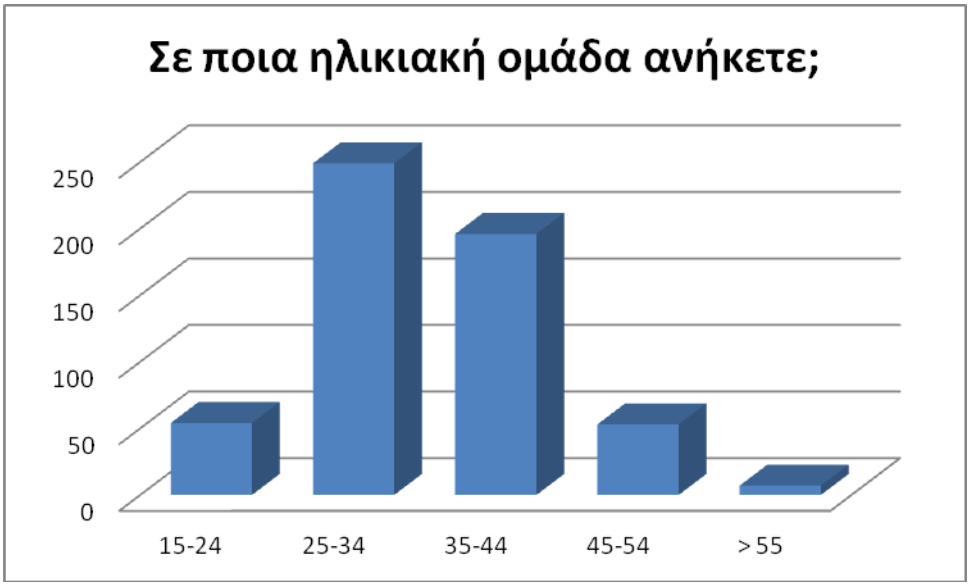
5.3.1 Χαρακτηριστικά δείγματος

Οι έγκυρες απαντήσεις του ερωτηματολογίου ανήλθαν στις 559 εκ των οποίων απαντήσανε 323 Γυναίκες και 236 άνδρες με αντίστοιχο ποσοστό 58% και 42%.



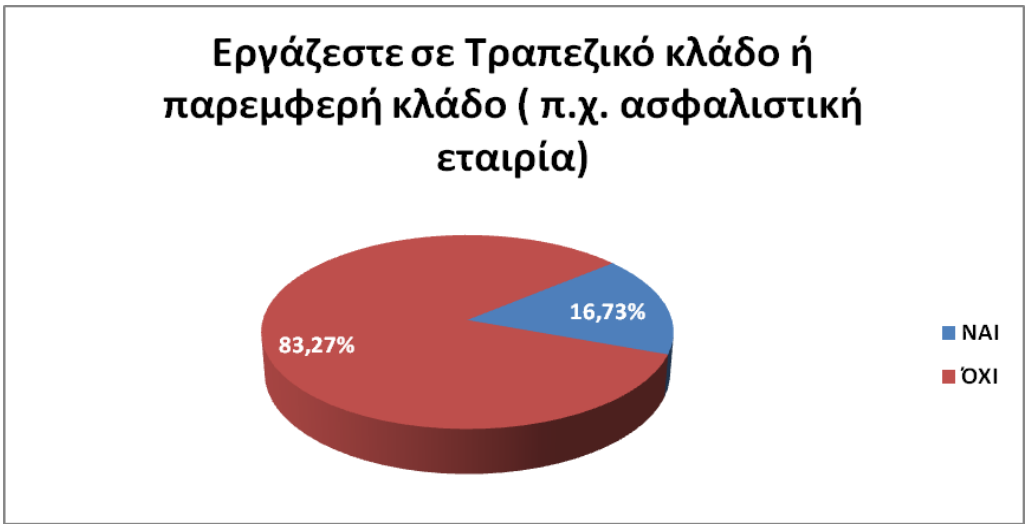
Σχήμα 5.1 Ποσοστό απάντησης στο ερωτηματολόγιο

Στη συγκεκριμένη έρευνα το μεγαλύτερο ποσοστό που συμμετείχε ήταν ηλικιακά 25-34 ετών με ποσοστό 44,54% και 35-44 ετών με ποσοστό 35,06% ενώ βλέπουμε ότι οι ηλικίες 15-24, 45-54 και >54 αντίστοιχα απαντήσανε σε ποσοστά 9,66%, 9,48% και 1,25%



Σχήμα 5.2 Ηλικιακή ομάδα

Στην έρευνα συμμετείχαν 83,27% χρήστες που δεν έχουν σχέση με τραπεζικό κλάδο σε αντίθεση με το 16,73 % που εργάζεται σε αντίστοιχο τραπεζικό ή ασφαλιστικό κλάδο.



Σχήμα 5.3 Εργασία σε Τράπεζες ή παρεμφερή κλάδο

5.3.2 Συσχέτιση Θεωρίας με τις Ερωτήσεις

Προκειμένου να έχουμε μια γενική εικόνα σε ότι αφορά τη συσχέτιση της θεωρίας με τις ερωτήσεις που έχουμε υποβάλει στο κοινό, παρακάτω έχουμε δημιουργήσει σχετικό πινακάκι συσχέτισης της Θεωρίας με τις Ερωτήσεις.

	Ερώτηση
Γενική Ερώτηση	5.3.4 Διαθέτετε λογαριασμό σε οποιαδήποτε Τράπεζα στην Ελλάδα ή στο εξωτερικό;
Γενική Ερώτηση	5.3.5 Ποιες είναι οι πιο συχνές συναλλαγές που χρησιμοποιείτε;
Ebanking m-banking	5.3.6 Πόσο εξοικειωμένος με τη χρήση νέων τεχνολογιών και τη χρήση του Διαδικτύου
Ebanking m-banking	5.3.7 Με τι συχνότητα κάνετε χρήση του Διαδικτύου
Ebanking m-banking	5.3.8 Γνωρίζετε ότι μπορείτε να κάνετε τις Τραπεζικές σας συναλλαγές από το σπίτι σας ή το γραφείο χωρίς να χρειαστεί η παρουσία σας σε κάποιο κατάστημα μέσω των υπηρεσιών e-banking ή mobile banking
Ebanking m-banking	5.3.9 Είστε χρήστης των υπηρεσιών e-banking ή mobile-banking
Ebanking m-banking	5.3.10 Ποια υπηρεσία ηλεκτρονικής Τραπεζικής χρησιμοποιείτε πιο συχνά;
Ebanking m-banking	5.3.11 Ποιες είναι οι πιο συχνές συναλλαγές που χρησιμοποιείτε από το σύνολο των υπηρεσιών e-banking ή m-banking;
Ασφάλεια Δεδομένων	5.3.12 Θεωρείτε ότι οι τράπεζες παρέχουν κατάλληλη ασφάλεια για τις ηλεκτρονικές σας συναλλαγές
Ασφάλεια Δεδομένων	5.3.13 Ποια ή ποιες είναι οι μέθοδοι που χρησιμοποιούν οι τράπεζες προκειμένου να αισθάνεστε πιο ασφαλής χρησιμοποιώντας το e-banking μιας τράπεζας;
Ασφάλεια Δεδομένων	5.3.14 Θεωρείτε ότι ο υπολογιστής που χρησιμοποιείτε είναι κατάλληλος για συναλλαγές μέσω διαδικτύου (internet) σύμφωνα με τις προϋποθέσεις που προτείνει η τράπεζα για ασφαλείς συναλλαγές μεταξύ σας ;
Ασφάλεια Δεδομένων	5.3.15 Τι είδους ασφάλεια χρησιμοποιείτε για να προστατέψετε τον υπολογιστή σας από κακόβουλο λογισμικό (επικίνδυνο ιο)*;
Ebanking m-banking	5.3.16 Για ποιους λόγους δεν χρησιμοποιείτε τις υπηρεσίες e-banking και mobile banking ;

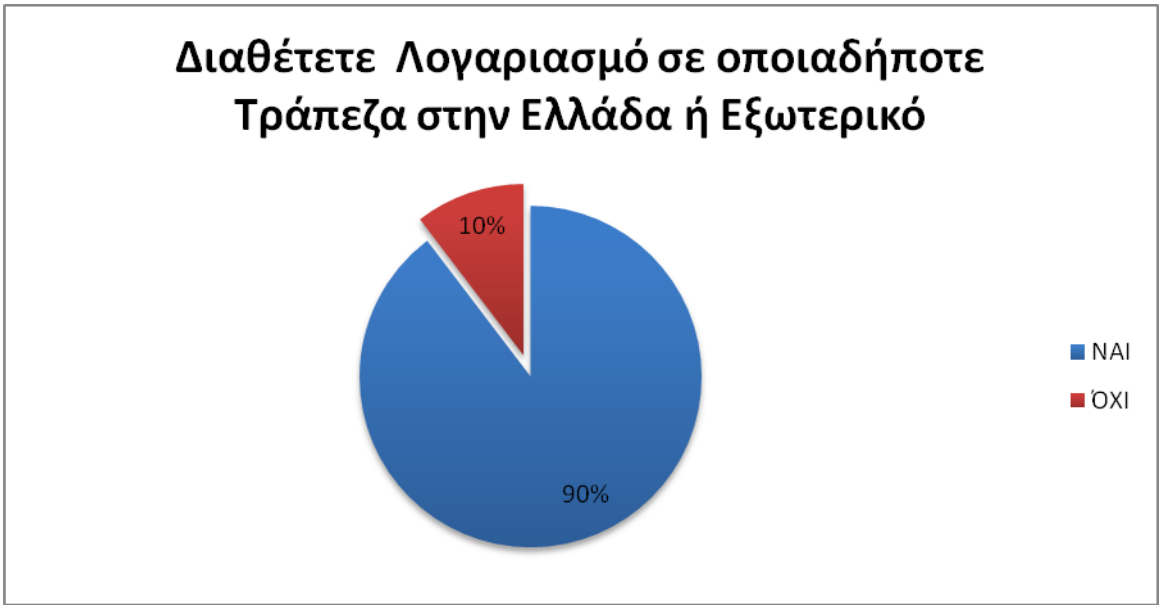
Οι δύο πρώτες ερωτήσεις (5.3.4 και 5.3.5) είναι γενικού περιεχομένου και τέθηκαν ώστε να απομονώσουμε τους χρήστες που δεν χρησιμοποιούν το διαδίκτυο ως μέσο τραπεζικών συναλλαγών. Οι επόμενες τρείς ερωτήσεις (5.3.6 – 5.3.9) τέθηκαν προκειμένου να διαπιστώσουμε το κοινό γνωρίζει για την ύπαρξη της τραπεζικής πληροφορικής και τη χρησιμότητά της. Οι ερωτήσεις 5.3.9 -5.3.11 αφορούν τη χρησιμοποίηση των χρηστών της ηλεκτρονικής Τραπεζικής μέσω των υπηρεσιών e-banking και m-banking. Τέλος, οι ερωτήσεις 5.3.12 – 5.3.15 αφορούν την ασφάλεια δεδομένων των υπηρεσιών e-banking και m-banking, κατά πόσο ο χρήστης είναι εξοικειωμένος με τη χρήση των υπηρεσιών αυτών.

Η τελευταία ερώτηση τέθηκε στους χρήστες που δεν χρησιμοποιούν υπηρεσίες e-banking και m-banking προκειμένου να εντοπίσουμε τους λόφους που δεν κάνουν χρήση.

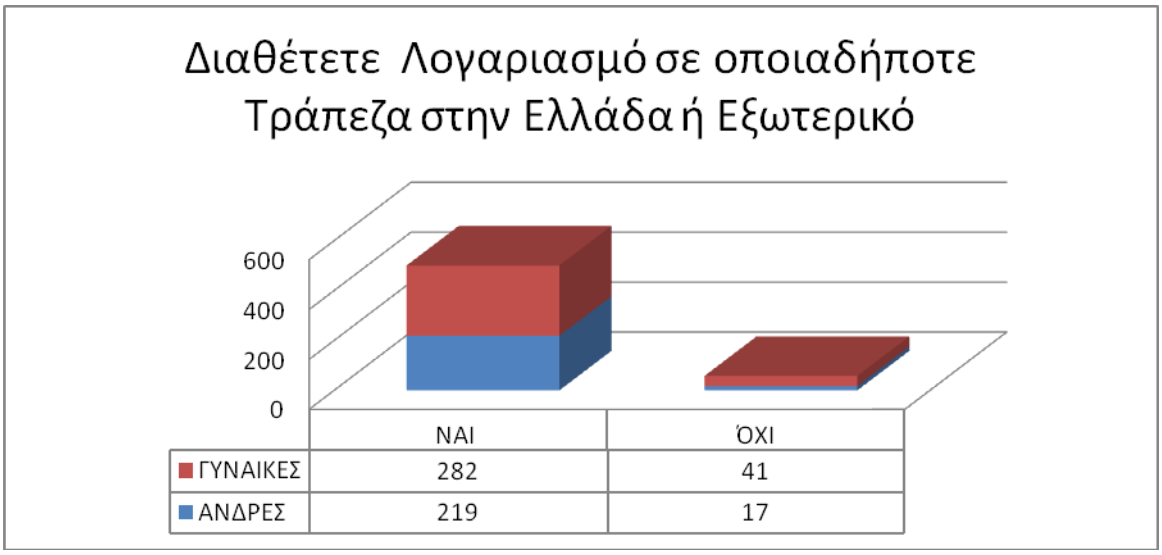
5.3.3 Ερώτηση : Διαθέτετε λογαριασμό σε οποιαδήποτε Τράπεζα στην Ελλάδα ή στο εξωτερικό;

Βασική Ερώτηση που τέθηκε ήταν αν ο Ερωτώμενος διαθέτει κάποιο τραπεζικό Λογαριασμό σε Ελληνική ή Ξένη Τράπεζα που είναι λογικό ώστε τα άτομα τα οποία δεν διαθέτουν λογαριασμό να μη χρειάζεται να προχωρήσουν στην έρευνα, Παρατηρούμε ότι σε ποσοστό 10% (58 απαντήσεις), δεν έχουν κάποιο λογαριασμό σε τράπεζα σε αντιθέσει με το 90% των συμμετεχόντων (501 απαντήσεις) που διαθέτουν.

ΑΠΑΝΤΗΣΕΙΣ	ΝΑΙ	ΟΧΙ
ΑΝΔΡΕΣ	219	17
ΓΥΝΑΙΚΕΣ	282	41
	501	58



Σχήμα 5.5 Ποσοστό διάθεσης λογαριασμού Τραπεζικού



Σχήμα 5.6 Αναλογία διάθεσης λογαριασμού μεταξύ φύλων

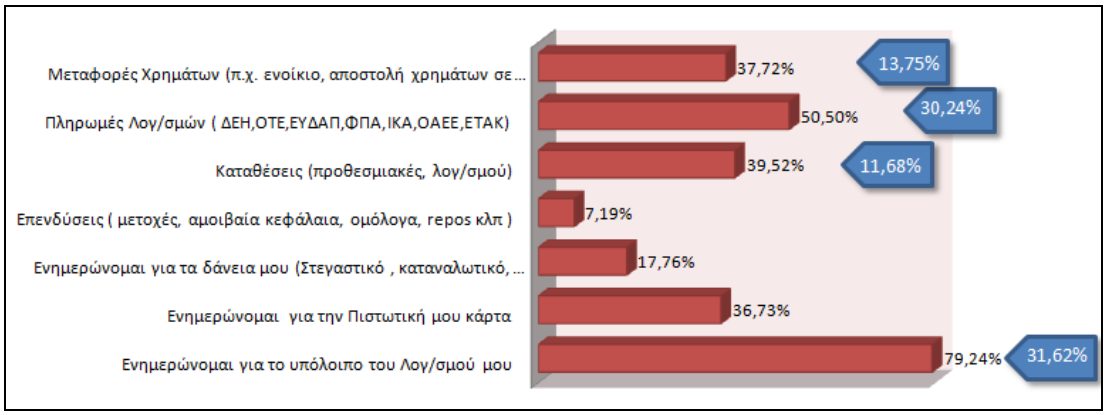
Στην ερώτηση πολλαπλών επιλογών «Με ποιο τρόπο συναλλάσσεστε πιο συχνά με την Τράπεζα σας» παρατηρούμε ότι η χρήση των Α.Τ.Μ. γίνεται πιο συχνή με ποσοστό 82,24% μέσα από δείγμα 501 απαντήσεων. Εναλλακτικά χρησιμοποιείται το διαδίκτυο σε ποσοστό 55,89% ενώ παραδοσιακά ο χρήστης επισκέπτεται κάποιο κατάστημα. Οι περιπτώσεις που ο χρήστης συναλλάσσεται μέσω email είτε με τη χρήση τηλεφωνίας (σταθερής ή κινητής) είναι πολύ μικρές με ποσοστά 1,80% και 5,39% αντίστοιχα. Από τους ερωτηθέντες σημαντικότερη είναι η χρήση του διαδικτύου και του e-banking με ποσοστό 46,48% ενώ η χρήση των ATM θεωρείτε

εξίσου σημαντική κατά 39,08%. Μικρός όμως αριθμός ερωτηθέντων θεωρεί σημαντικότερο το να επισκέπτεται το κατάστημα και σε ποσοστό 13,73%.

Σχήμα 5.7 Τρόποι Συναλλαγής σε μια Τράπεζα

5.3.4 Ερώτηση : Ποιες είναι οι πιο συχνές συναλλαγές που χρησιμοποιείτε;

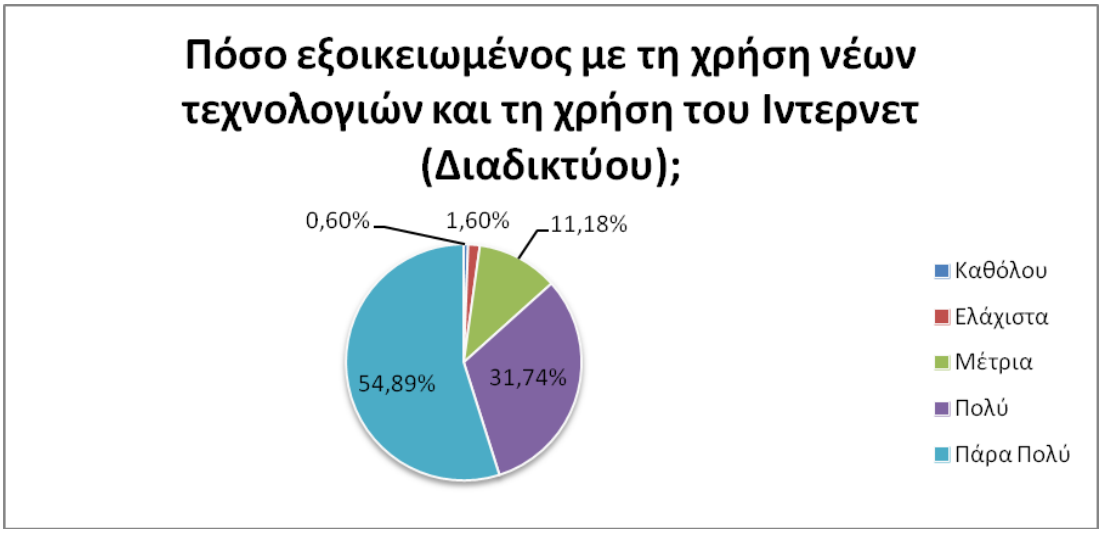
Στη συγκεκριμένη ερώτηση ποιες οι πιο συχνές συναλλαγές που χρησιμοποιούν οι ερωτηθέντες, από το δείγμα 501 ατόμων, παρατηρούμε ότι η τραπεζική τους σχέση είναι περισσότερο η ενημέρωση για το υπόλοιπο του λογαριασμού τους με ποσοστό 79,24%. Ένα μεγάλο ποσοστό χρησιμοποιεί τα εναλλακτικά δίκτυα για τις πληρωμές λογαριασμών σε ποσοστό 50,50%, ενώ στα ίδια περίπου επίπεδα οι χρήστες χρησιμοποιούν την τραπεζική τους σχέση για καταθέσεις χρημάτων, μεταφορές χρημάτων όπως και ενημέρωση της πιστωτικής κάρτας με ποσοστά αντίστοιχα 39,52%, 37,72% και 36,73%. Από τους ερωτώμενους πιο σημαντική είναι η ενημέρωση των λογαριασμών τους και οι πληρωμές λογαριασμών.



Σχήμα 5.8 Πιο συχνά χρησιμοποιούμενες συναλλαγές

5.3.5 Ερώτηση : Πόσο εξοικειωμένος με τη χρήση νέων τεχνολογιών και τη χρήση του Διαδικτύου;

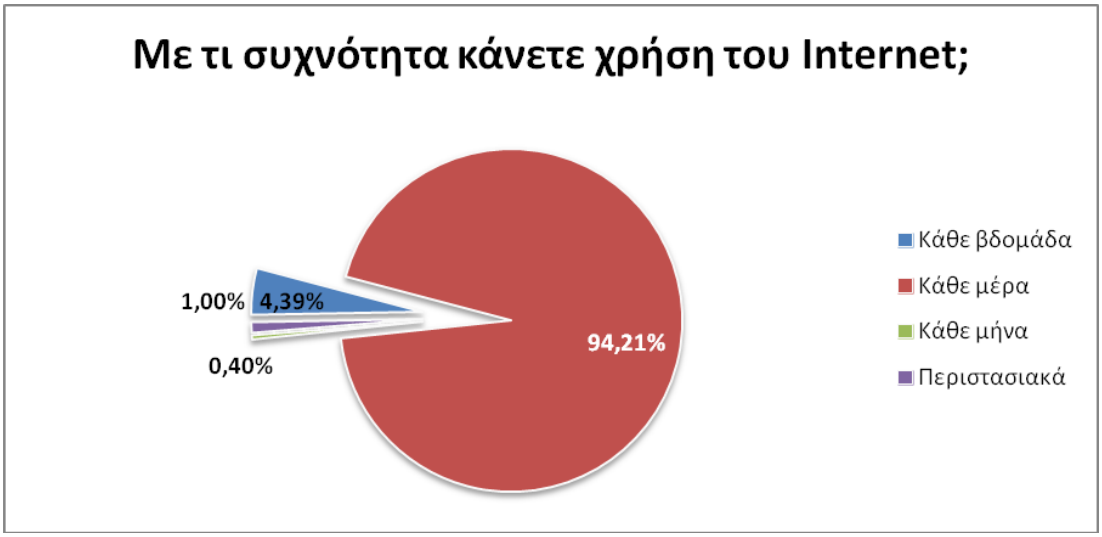
Σε δείγμα ερωτηθέντων για τη εξοικείωση στη χρήση των νέων τεχνολογιών προκειμένου να αντιληφθούμε το επίπεδο των χρηστών που χρησιμοποιούν τα ηλεκτρονικά μέσα συναλλαγής με την Τράπεζα, παρατηρούμε ότι το μεγαλύτερο ποσοστό έχουν καλή έχω πολύ καλή γνώση με ποσοστά 31,74% και 54,89%, ενώ ελάχιστο είναι το ποσοστό που χρησιμοποιεί τραπεζικές συναλλαγές μέσω διαδικτύου και δεν έχει εξοικείωση με τις νέες τεχνολογίες (13,38% συνολικά).



Σχήμα 5.9 Εξοικείωση με νέες τεχνολογίες στο διαδίκτυο

5.3.6 Ερώτηση : Με τι συχνότητα κάνετε χρήση του Διαδικτύου;

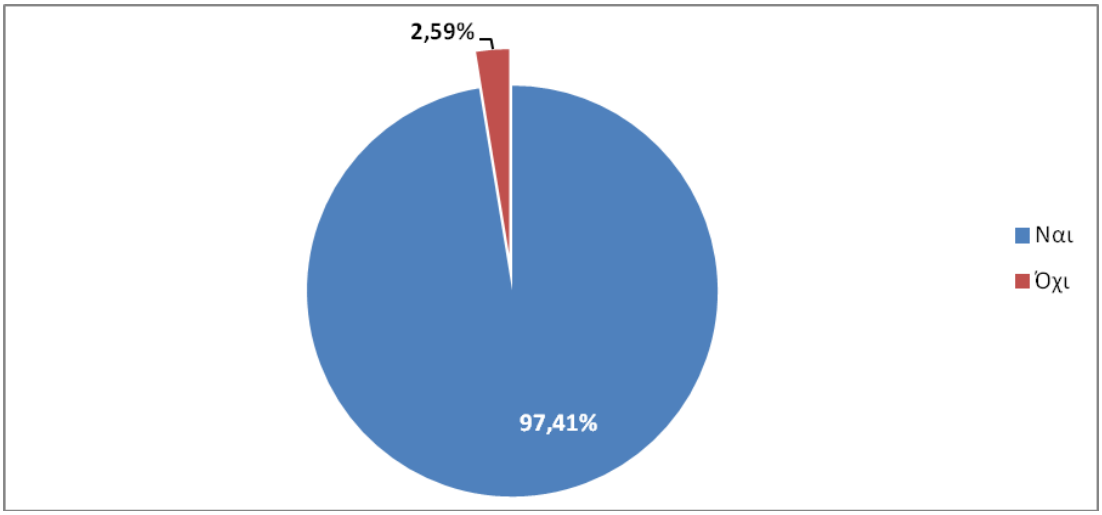
Στη συγκεκριμένη ερώτηση παρατηρούμε οι ερωτηθέντες κάνουν καθημερινή του διαδικτύου σε ποσοστό 94,21%.



Σχήμα 5.10 Συχνότητα Χρήσης του Διαδικτύου

5.3.7 Ερώτηση : Γνωρίζετε ότι μπορείτε να κάνετε τις Τραπεζικές σας συναλλαγές από το σπίτι σας ή το γραφείο χωρίς να χρειαστεί η παρουσία σας σε κάποιο κατάστημα μέσω των υπηρεσιών e-banking ή mobile banking;

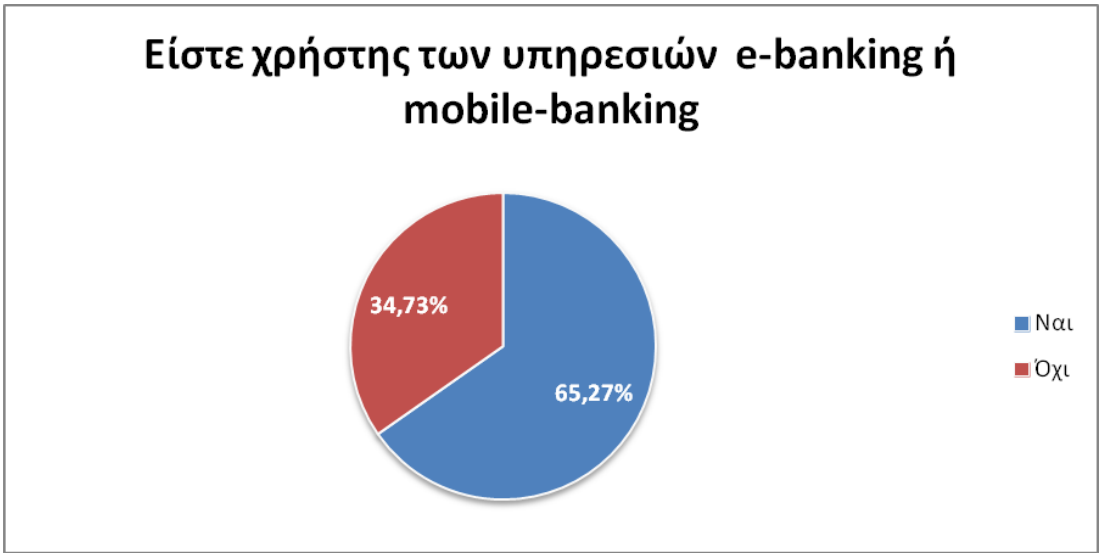
Στην ερώτηση αν γνωρίζουν οι χρήστες ότι το διαδίκτυο μέσω των υπηρεσιών e-banking και mobile banking προσφέρεται για τη συναλλαγή τους με την τράπεζα, καταφατικά απάντησαν το 97,41% σε αντίθεση με το 2,59% που απάντησε αρνητικά. Παρατηρούμε ότι οι χρήστες είναι εξοικειωμένοι με τη χρήση των τραπεζικών υπηρεσιών μέσω του διαδικτύου σε μεγάλο ποσοστό.



Σχήμα 5.11 Γνώση συναλλαγών μέσω e-banking

5.3.8 Ερώτηση: Είστε χρήστης των υπηρεσιών e-banking ή mobile-banking;

Σε σύνολο 501 ατόμων, ποσοστό 65,27% (327 άτομα) χρησιμοποιεί τις υπηρεσίες e-banking και mobile banking σε αντιθέσει με ποσοστό 34,73% (174 άτομα) που δεν χρησιμοποιούν τις αντίστοιχες υπηρεσίες.



Σχήμα 5.12 Χρήστες υπηρεσιών e-banking ή m-banking

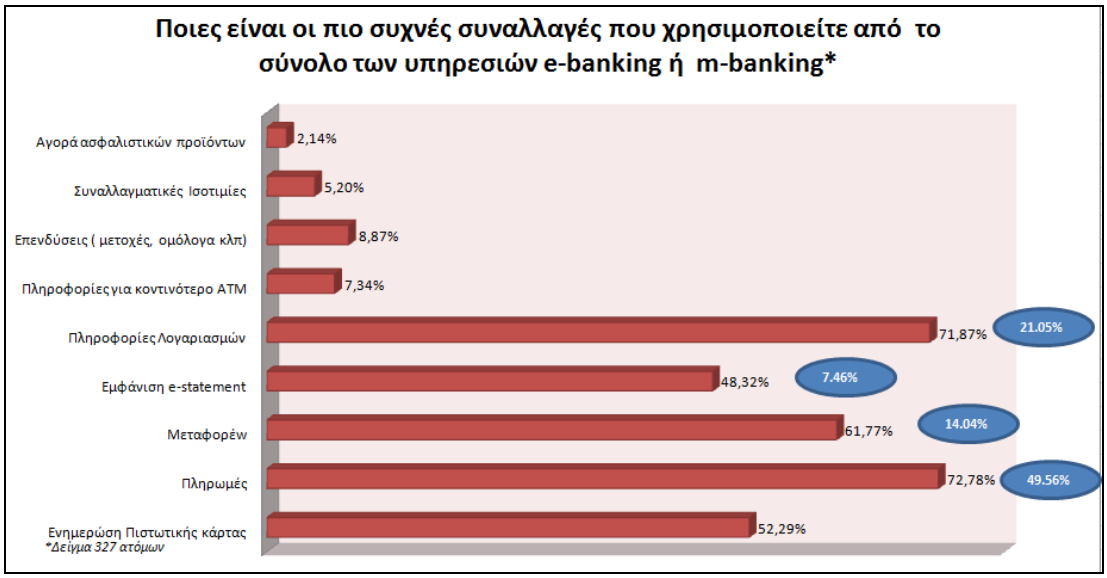
5.3.9 Ερώτηση : Ποια υπηρεσία ηλεκτρονικής Τραπεζικής χρησιμοποιείτε πιο συχνά;

Στην ερώτηση για ποια είναι η χρήση των υπηρεσιών e-banking και mobile banking, επικρατέστερη με ποσοστό 83,49% είναι η χρήση των υπηρεσιών e-banking σε αντίθεση με το 15,90% που κάνει χρήση της κινητής συσκευής για τις συναλλαγές.

Σχήμα 5.13 Συχνά χρησιμοποιούμενες υπηρεσίες

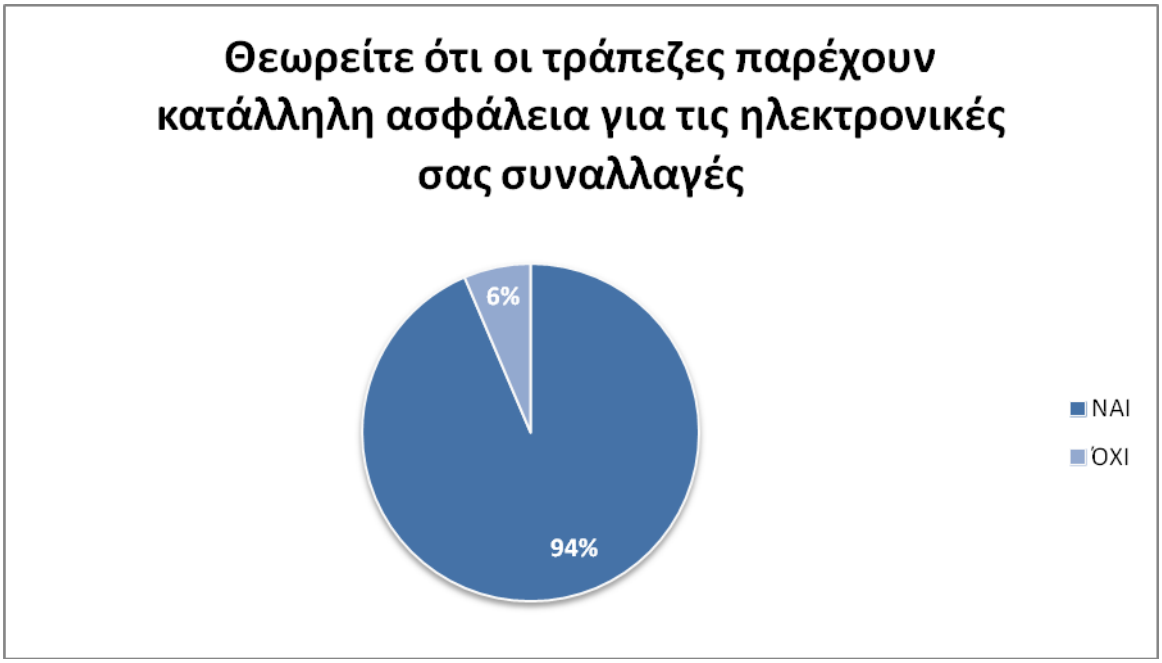
5.3.10 Ερώτηση : Ποιες είναι οι πιο συχνές συναλλαγές που χρησιμοποιείτε από το σύνολο των υπηρεσιών e-banking ή m-banking;

Στην ερώτηση ποιες συναλλαγές χρησιμοποιούν από την υπηρεσία e-banking, από το σύνολο των 327 χρηστών απάντησαν ότι με ποσοστό 72,78% επιλέγουν το e-banking ως μέσο πληρωμών. Εν συνεχεία, με ποσοστό 71,57 % χρησιμοποιούν για την πληροφόρηση λογαριασμών, αντίστοιχα με ποσοστά 61,77%, 52,29% και 48,32% εμφανίζονται οι χρήσεις των υπηρεσιών «μεταφορές χρημάτων», «ενημέρωση πιστωτικής κάρτας», και εμφάνιση e-statement. Από την έρευνα σε αυτή στη συγκεκριμένη ερώτηση χαμηλά ποσοστά εμφανίζονται στις ερωτήσεις που αφορούν «ασφαλιστικά προϊόντα» (2,14%), «συναλλαγματικές ισοτιμίες» (5,20%), «πληροφορίες για κοντινότερο Α.Τ.Μ. (7,34%) και «επενδύσεις» (8,87%)



Σχήμα 5.14 Συχνά χρησιμοποιούμενες συναλλαγές

5.3.11 Ερώτηση : Θεωρείτε ότι οι τράπεζες παρέχουν κατάλληλη ασφάλεια για τις ηλεκτρονικές σας συναλλαγές



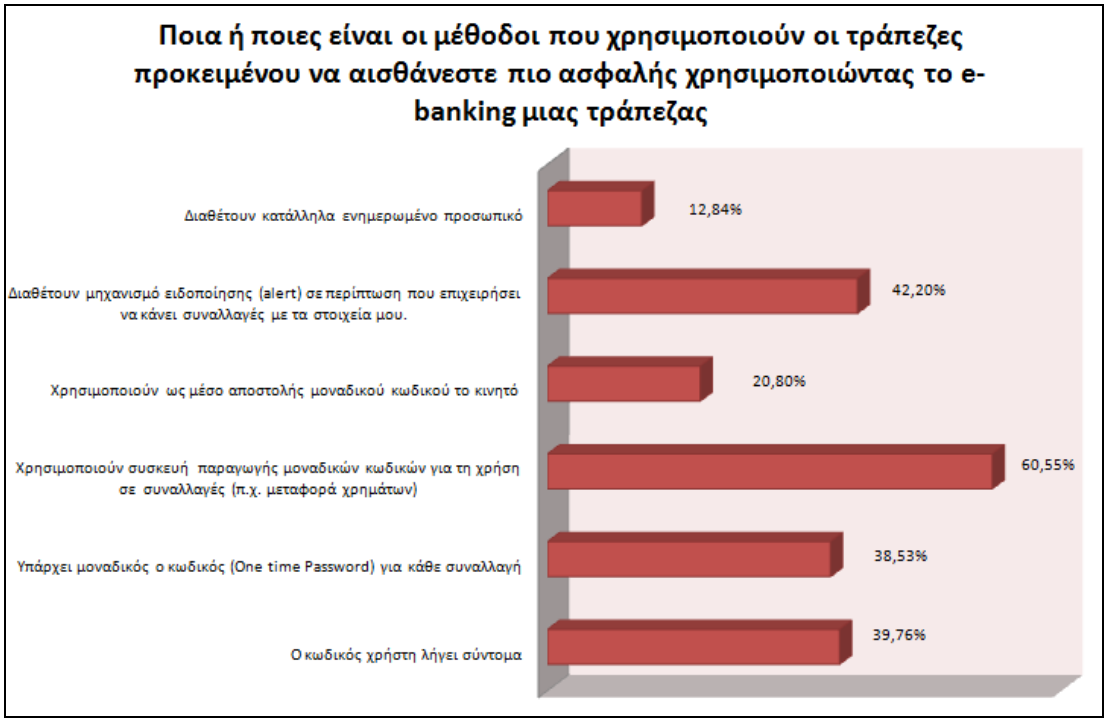
Σχήμα 5.15 Ασφάλεια συναλλαγών

Στην ερώτηση αν θεωρείτε ότι οι τράπεζες παρέχουν κατάλληλη ασφάλεια στις ηλεκτρονικές συναλλαγές, από δείγμα των 327 ατόμων το 94% θεωρεί ότι είναι ασφαλείς οι συναλλαγές τους μέσω διαδικτύου εν αντιθέσει με το 6% που δε θεωρεί κατάλληλη την ασφάλεια που παρέχουν οι τράπεζες στις συναλλαγές τους. Εδώ θα

πρέπει να τονίσουμε ότι το δείγμα των 327 ατόμων είναι εκείνο το οποίο χρησιμοποιεί υπηρεσίες e-banking.

5.3.12 Ερώτηση : Ποια ή ποιες είναι οι μέθοδοι που χρησιμοποιούν οι τράπεζες προκειμένου να αισθάνεστε πιο ασφαλής χρησιμοποιώντας το e-banking μιας τράπεζας

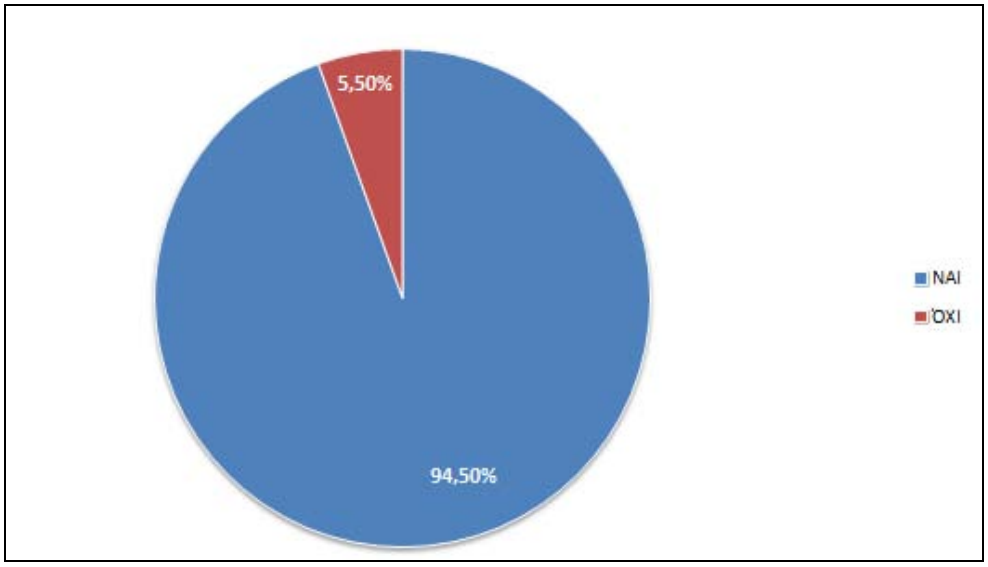
Στην ερώτηση για τις μέθοδοι που χρησιμοποιούν οι τράπεζες ώστε το αίσθημα ασφάλειας να είναι ικανοποιητικό, φαίνεται ότι η χρησιμοποίηση της συσκευής που παράγει μοναδικούς κωδικούς είναι η επικρατέστερη με ποσοστό 60,55%, ενώ ποσοστό 42,20% θεωρούν οι ερωτηθέντες ότι πιο ασφαλές είναι η αποστολή ενημερωτικού SMS (alert) σε κάθε κίνηση για τους λογαριασμούς που διαθέτει ένας πελάτης με την τράπεζα. Ωστόσο σημαντικά ποσοστά φαίνονται ότι επικρατούν στο ότι «ο κωδικός λήγει σύντομα» και «υπάρχει μοναδικός κωδικός (one time password) με ποσοστά 39,76% και 38,53% αντίστοιχα. Τέλος τα μικρότερα ποσοστά φαίνονται στις επιλογές «χρησιμοποίηση ως μέσου αποστολής μοναδικού κωδικού την συσκευή κινητής τηλεφωνίας» όπως και τη «διάθεση κατάλληλου ενημερωμένου προσωπικού» με ποσοστά αντίστοιχα 20,80% και 12,84%.



Σχήμα 5.16 Μέθοδοι ασφάλειας συναλλαγών

5.3.13 Ερώτηση : Θεωρείτε ότι ο υπολογιστής που χρησιμοποιείτε είναι κατάλληλος για συναλλαγές μέσω διαδικτύου (internet) σύμφωνα με τις προϋποθέσεις που προτείνει η τράπεζα για ασφαλείς συναλλαγές μεταξύ σας

Στην ερώτηση αν οι χρήστες διαθέτουν κατάλληλο υπολογιστή προκειμένου να διενεργήσουν τραπεζικές συναλλαγές μέσω διαδικτύου, το ποσοστό αυτό φαίνεται ότι οι χρήστες θεωρούν ότι διαθέτουν κατάλληλο εξοπλισμό για τις συναλλαγές τους με ποσοστό 94,5% σε αντίθεση με 5,5% που θεωρούν ότι ο υπολογιστής τους δεν είναι κατάλληλος για τη χρήση τους σε συναλλαγές μέσω διαδικτύου.

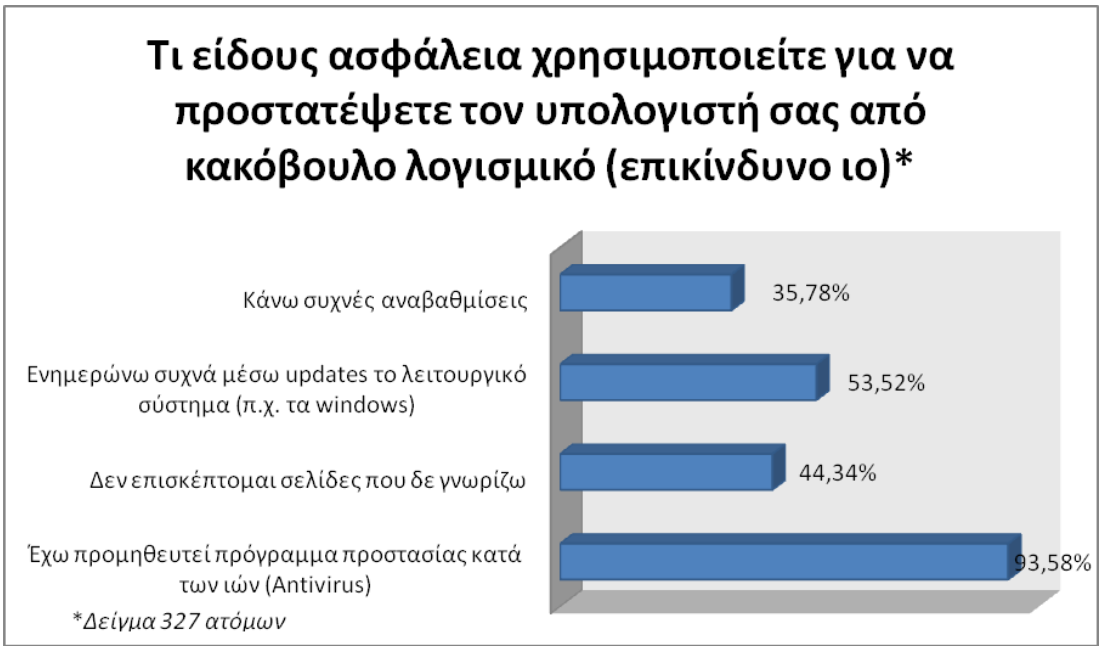


Σχήμα 5.17 Καταλληλότητα συστημάτων πρόσβασης διαδικτύου

5.3.14 Ερώτηση : Τι είδους ασφάλεια χρησιμοποιείτε για να προστατέψετε τον υπολογιστή σας από κακόβουλο λογισμικό (επικίνδυνο ιο)*

Η ερώτηση αυτή θα μπορούσε να τεθεί σε όλο το σύνολο των ερωτηθέντων, όμως θα θέλαμε να διεξάγουμε το συμπέρασμα αν όσοι χρησιμοποιούν τις υπηρεσίες e-banking και mobile banking είναι εξοικειωμένοι με την ασφάλεια του υπολογιστή τους. Πολλές φορές παρατηρούνται παράπονα στις υπηρεσίες των τραπεζών ότι παρουσιάζονται διάφορα προβλήματα υποκλοπών τα οποία οφείλονται σε έλλειψη ασφάλειας των υπολογιστών. Έτσι, από τους 327 ερωτηθέντες, το 93,58% χρησιμοποιεί λογισμικό για την προστασία κατά των ιών (Antivirus). Από τα αποτελέσματα βλέπουμε ότι σε ποσοστό 53,52% κάνει συχνές ενημερώσεις στο

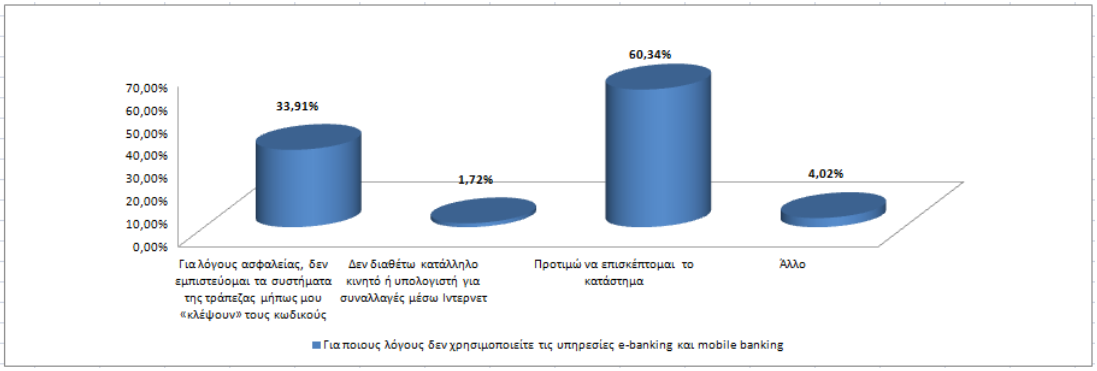
λειτουργικό σύστημα. Ποσοστό 44,34 % δεν επισκέπτεται σελίδες που δε γνωρίζει ενώ το 35,78% κάνει αναβαθμίσεις συχνές στον υπολογιστή του.



Σχήμα 5.18 Μέθοδοι ασφαλείας που χρησιμοποιούνται από τους Χρήστες Διαδικτύου

5.3.15 Ερώτηση : Για ποιους λόγους δεν χρησιμοποιείτε τις υπηρεσίες e-banking και mobile banking

Στην ερώτηση αυτή απαντήσανε οι 174 ερωτηθέντες της ερώτησης 7.2.6 προκειμένου να ερευνήσουμε τους λόγους που δεν χρησιμοποιούν την υπηρεσία e-banking και mobile-banking. Σε ποσοστό 60,34% των ερωτηθέντων προτιμά να επισκέπτεται το κατάστημα, ενώ σε ποσοστό 33,91% των ερωτηθέντων δεν εμπιστεύεται τα συστήματα με το φόβο ότι θα γίνει κάποια υποκλοπή των κωδικών τους. Ένα ποσοστό 1,72 % δε διαθέτει κατάλληλο κινητό ή υπολογιστή προκειμένου να κάνει συναλλαγές στο διαδίκτυο ενώ σε ποσοστό 4,02 των ερωτηθέντων για διάφορους λόγους δε χρησιμοποιεί τις υπηρεσίες αυτές.



Σχήμα 5.19 Λόγοι μη χρησιμοποίησης υπηρεσιών e-banking και m-banking

Συμπέρασμα

Από τα αποτελέσματα της έρευνας προκύπτουν τα εξής συμπεράσματα:

Ήδη από την 1^{η} ερώτηση συμπεράνουμε ότι από τους ερωτώμενους άνδρες εκείνοι που συναλλάσσονται με τράπεζες σε ποσοστό 92,8% σε αντίθεση με ποσοστό 87,31% των γυναικών. Ωστόσο οι χρησιμότητα των τραπεζικών συναλλαγών γίνονται συχνότερα με τη χρήση των εναλλακτικών δικτύων με κύριο όγκο χρήσης η χρήση των ATM και στη συνέχεια με τη χρήση των καναλιών του διαδικτύου. Ωστόσο υπάρχει ένα μεγάλο ποσοστό πελατών που συνηθίζει να κάνει τις συναλλαγές παραδοσιακά μέσω τραπεζικού καταστήματος. Από τους συναλλάσσοντας παρατηρείτε ότι οι χρήση του διαδικτύου προτιμάται ως η πιο σημαντική από τα μέσα των εναλλακτικών δικτύων. Οι πιο συχνοί πελάτες των συναλλαγών είναι χρήστες ηλικίας 25-44 γεγονός ότι οι χρήστες αυτοί έχουν μεγαλύτερη ευχέρεια και εξοικείωση με τις νέες τεχνολογίες ενώ αρκετά υψηλό είναι το ποσοστό για τις ηλικίες 35-44. Από τους συγκεκριμένους χρήστες ο μεγαλύτερος πληθυσμός προτιμά να χρησιμοποιεί τις υπηρεσίες διαδικτύου για να βλέπει τα υπόλοιπα των λογαριασμών τους και να κάνει πληρωμές. Επιπλέον παρατηρούμε ότι οι περισσότεροι χρήστες είναι εξοικειωμένοι κατά μεγάλο ποσοστό με το διαδίκτυο και ως πελάτες των τραπεζικών υπηρεσιών διαδικτύου, το μεγαλύτερο ποσοστό προτιμά το e-banking και εμπιστεύονται την ασφάλεια της τράπεζας.

6 Γενικά Συμπεράσματα

Οι συνεχής χρήση των νέων τεχνολογιών και ιδιαίτερα μέσω του διαδικτύου, η ηλεκτρονική τραπεζική τείνει να υπερκεράσει την παραδοσιακή χρήση της τραπεζικής. Βλέπουμε συνεχώς ότι ο τραπεζικός κλάδος, αντιλαμβάνεται ότι η χρήση του διαδικτύου κερδίζει συνεχώς έδαφος στην κερδοφορία της και έτσι προσανατολίζεται συνέχεια στη δημιουργία νέων μεθοδολογιών ώστε να παρέχει έναντι κατάλληλων προμηθειών, συνεχείς υπηρεσίες προς τους πελάτες τους κερδίζοντας όσο το δυνατόν μεγαλύτερο μέρος από την «πίτα της αγοράς».

Στην προσπάθεια τους οι τράπεζες να γίνουν όσο το δυνατόν περισσότερο ανταγωνιστικές, αυξάνουν τις προσφερόμενες υπηρεσίες προς τους πελάτες τους δημιουργώντας τα εργαλεία εκείνα που θα αυξήσουν την κερδοφορία τους, «ανοίγοντας» διαρκώς νέα κανάλια επικοινωνίας και ιδιαίτερα μέσω διαδικτύου. Αυτά τα «ανοίγματα» όμως, δημιουργούν πέραν από κέρδη, και αλλεπάλληλα προβλήματα που συσχετίζονται με την έκθεση των «καναλιών επικοινωνίας» σε συνεχή κίνδυνο. Έτσι, προκειμένου να έχουν θέση στο διαδίκτυο, οι τράπεζες, επενδύουν συνεχώς σε νέες μεθόδους προστασίας από τους συνεχής κινδύνους που τους περιβάλλουν, κίνδυνοι που μπορούν να προκαλέσουν αποσταθεροποίηση στις δομές των τραπεζών (συστημικοί κίνδυνοι). Ένα τέτοιο σύστημα ηλεκτρονικής τραπεζικής στην ουσία για τους χρήστες είναι ένα απλό σύστημα συναλλαγών, μια ιστοσελίδα η οποία επιτρέπει τη διεξαγωγή συναλλαγών με την Τράπεζα και είναι προ σπελάσιμο από το σύνολο των υπολογιστών. Σε γενικές γραμμές το αποτέλεσμα που βλέπει ένας πελάτης της Τράπεζας είναι απλό και ο τρόπος εκτέλεσης των συναλλαγών γίνεται με απλό τρόπο. Πίσω όμως από τα συστήματα, η λειτουργία δεν είναι τόσο απλή όπως φαίνεται στο χρήστη. Για κάθε κίνηση που γίνεται από το χρήστη εκτελείται μια σύνθετη λογική με ελέγχους προκειμένου να ολοκληρωθούν οι συναλλαγές.

Για την ολοκλήρωση των συναλλαγών, διάφορα συστήματα πληρωμών (μέσω εσωτερικού δικτύου των τραπεζών) συνεργάζονται ώστε οι συναλλαγές αυτές να διεκπεραιωθούν. Ανάλογα με τον τύπο της πληρωμής, οι κινήσεις διοχετεύονται με αντίστοιχες εντολές πληρωμής προς τα κατάλληλα κανάλια επικοινωνίας. Έτσι μια πληρωμή μπορεί να σταλθεί μέσω των συστημάτων SWIFT, SEPA, ΔΙΑΣ ή άλλων συστημάτων πληρωμών που έχουν συμφωνήσει οι Τραπεζικοί οργανισμοί με διμερείς συμφωνίες μεταξύ τους.

Ένας πελάτης της τράπεζας έχει σήμερα τη δυνατότητα να εκτελέσει με δύο δημοφιλής τρόπους τις συναλλαγές του, είτε από ηλεκτρονικό υπολογιστή (χρήση του κλασικού e-banking) είτε μέσω του κινητού του τηλεφώνου χρησιμοποιώντας τον browser (φυλομετρητή) του κινητού ή εφαρμογή κατάλληλη με την προϋπόθεση να έχουν σύνδεσης στο διαδίκτυο. Για τη σύνδεση και τη διεκπεραίωση μιας συναλλαγής σε ένα από τα διαθέσιμα κανάλια (e-banking ή mobile banking), συνεργάζονται διάφορα τμήματα ώστε να παραχθεί το τελικό αποτέλεσμα.

Πλέον, παρατηρείται στις μέρες μας ότι οι πελάτες των τραπεζών, έχουν εξοικειωθεί περισσότερο με τη χρήση του διαδικτύου συγκριτικά με τις αρχές της δεκαετίας που η ανάπτυξη του διαδικτύου ήταν ακόμη στα σπάργανα. Σύμφωνα με την έρευνα που έχουμε διεξάγει, παρατηρούμε ότι οι ηλικίες 25-44 είναι οι κύριοι χρήστες της ηλεκτρονικής τραπεζικής οι οποίοι είναι εξοικειωμένοι με τη χρήση του διαδικτύου κυρίως σε καθημερινή βάση. Οι συγκεκριμένοι χρήστες, χρησιμοποιούν τις τραπεζικές υπηρεσίες κυρίως για να ενημερωθούν για τις μεταβολές στους τραπεζικούς λογαριασμούς όπως και για διάφορες πληρωμές εταιριών κερδίζοντας με τον τρόπο αυτό χρόνο διεκπεραίωσης τους που θα καταναλώνονταν από τη φυσική τους παρουσία σε κάποιο κατάστημα. Οι χρήστες αυτοί είναι εξοικειωμένοι με τη χρήση των υπολογιστών και μπορούν να λαμβάνουν τα κατάλληλα μέτρα για την προστασία από διάφορες «ασθένειες των υπολογιστών» όπως ιοί και κακόβουλα λογισμικά. Ωστόσο, υπάρχουν και χρήστες που δεν χρησιμοποιούν τις υπηρεσίες e-banking και mobile banking σε ποσοστό 35% των ερωτηθέντων που διαθέτουν τραπεζικό λογαριασμό που είναι σχετικά σημαντικό ότι προτιμούν να συναλλάσσονται με τον παραδοσιακό τρόπο με τις τράπεζες δηλαδή να επισκέπτονται ένα κατάστημα από ότι να χρησιμοποιούν την τεχνολογία για τις συναλλαγές τους. Πιστεύουμε ότι με την πάροδο του χρόνου και την αύξηση και εξοικείωση περισσότερου πληθυσμού συγκριτικά με το διαδίκτυο, ο αριθμός των υπηρεσιών e-banking και m-banking πλέον θα είναι πολύ μεγαλύτερος από ότι οποιαδήποτε συναλλαγή θα χρειάζεται τη φυσική παρουσία σε κάποιο κατάστημα της Τράπεζας.

7 Περιορισμοί της Έρευνας

Πρέπει να επισημανθεί ότι η παρούσα μελέτη δεν φιλοδοξεί την ολόπλευρη και εξαντλητική προσέγγιση όλων των πτυχών του θέματος στο οποίο εστιάζει.

Η συλλογή των στοιχείων έγινε με κατασκευασμένο ηλεκτρονικό ερωτηματολόγιο πράγμα που περιορίζεται σε ανθρώπους που έχουν κάποιου είδους εξοικείωση με ηλεκτρονικό υπολογιστή και δεν καλύπτει το γενικό σύνολο των ατόμων ακόμη και αν δεν διαθέτουν ηλεκτρονικό υπολογιστή αλλά διαθέτουν κατάλληλη συσκευή τηλεφώνου για τις ανάγκες της έρευνας. Τα αποτελέσματα της έρευνας εξήχθησαν με την καταμέτρηση των αποτελεσμάτων με προγραμματιστικό τρόπο που λόγω απειρίας, θα μπορούσε να εξάγει λανθασμένα συμπεράσματα. Άλλος περιοριστικός παράγοντας ήταν το γεγονός ότι η πλειονότητα των ερωτηθέντων απάντησαν στην Ελληνική γλώσσα, λόγω ότι τα χρονικά περιθώρια ήταν περιορισμένα και δεν κοινοποιήθηκε αντίστοιχα σε συνδέσμους του εξωτερικού γεγονός που περιορίζει την έρευνα στη χρήση τραπεζικών συναλλαγών στην Ελληνική (69,23%) και Κυπριακή περιφέρεια (19,50%).

Παρά τους περιορισμούς αυτούς, θεωρείται ότι η μέθοδος που ακολουθήθηκε, η μελέτη κατέληξε σε σωστά και ενδεικτικά συμπεράσματα για τη χρήση των τραπεζικών διαδικτυακών υπηρεσιών καθώς τα αποτελέσματα διασταυρώθηκαν με το στατιστικό εργαλείο SPSS και το αποτέλεσμα κρίνεται ορθό.

8 Προτάσεις για περεταίρω Έρευνα

Τα ηλεκτρονικά συστήματα e-banking και mobile banking είναι δημιουργία των τραπεζών και καθένα είναι προσαρμοσμένο στο εκάστοτε σύστημα της Τράπεζας. Όμως η τάση της αγοράς σε μια ενιαία οικονομία, δίνει και το έναυσμα σε ένα γεγονός ώστε οι τράπεζες και τα συστήματα τους θα πρέπει να προσαρμοστούν στην παγκόσμια οικονομία και να μην βλέπουν μόνο την τοπική αγορά. Δηλαδή θα πρέπει να δημιουργηθούν εκείνα τα συστήματα που θα επιτρέπουν συναλλαγές για λογαριασμό άλλων τραπεζών από ένα μόνο σημείο αναφοράς. Έτσι π.χ. αν ένας πελάτης που παράλληλα διατηρεί λογαριασμό σε δύο διαφορετικές τράπεζες είτε εσωτερικού είτε εξωτερικού, θα μπορούσε να τα διαχειριστεί ομοιόμορφα από ένα κεντρικό σύστημα e-banking (ή mobile banking) ταυτόχρονα και τους δύο λογαριασμούς χωρίς να έχει την ανάγκη να εισέρχεται διαδοχικά στα αντίστοιχα συστήματα των τραπεζών. Επιπλέον, λόγω του πιο πάνω περιορισμού της έρευνας στον Ελλαδικό και Κυπριακό χώρο, θα μπορούσε η έρευνα να απευθυνθεί και σε άλλες χώρες εμπλουτίζοντας την έρευνα με μετάφραση των αντίστοιχων κειμένων στη γλώσσα της χώρας που θέλουμε να εξάγουμε αποτελέσματα.

9 Αναφορές

[1]. http://www.eline.gr/servicedet.asp?p=&type=1&id=206

[2]. http://internetworldstats.com/stats.htm

[3]. Τραπεζική Πληροφορική (Ε.Α.Π.) Δ. Μυρτίδης

[4]. http://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

[5]. http://www.bankofgreece.gr/Pages/el/PaymentsSystems/SEPA/default.aspx

[6]. http://www.10588.com/pub_web/swift/books/us1m/doc/alah.htm

[7]. http://www.swift.com/about_swift/company_information/index.page?

[8]. http://www.bankofgreece.gr/Pages/el/PaymentsSystems/SEPA/default.aspx

[9]. http://www.bankofgreece.gr/BoGDocuments/Ο_Ενιαίος_Χώρος_Πληρωμών_σε_Ευρώ(SEPA).pdf

[10] www.dias.com.gr/

[11] http://en.wikipedia.org/wiki/DMZ_(computing)

[12] http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf

[13] Security Testing Handbook for Banking Applications

[14] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

[15] http://en.wikipedia.org/wiki/Pharming

[16] https://www.owasp.org/index.php/Man-in-the-middle_attack

[17] http://en.wikipedia.org/wiki/Denial-of-service_attack

[18] Computer για όλους τεύχος Απριλίου 2012

[19] http://en.wikipedia.org/wiki/Wireless_Application_Protocol

[20] http://en.wikipedia.org/wiki/General_Packet_Radio_Service

[21] Μπιζανίδης Γεώργιος (2007), Διπλωματική εργασία «mobile banking»

[22] http://en.wikipedia.org/wiki/2G

[23] http://www.webopedia.com/TERM/G/GPRS.html

[24] http://www.answers.com/topic/online-banking

[25] http://www.tu-harburg.de/tim/downloads/arbeitspapiere/Working_Paper_48.pdf

[26] http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm

[27] http://en.wikipedia.org/wiki/Phishing

[28] http://en.wikipedia.org/wiki/HTTP_Secure