Αλεξάνδρειο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Θεσσαλονίκης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: Mobile Banking: Η χρήση της υπηρεσίας στην Ελλάδα, πλεονεκτήματα και μειονεκτήματα

Επιμέλεια: Γάτος Εμμανουήλ

Υπεύθυνος Καθηγητής: Καργίδης Θεόδωρος

Ιανουάριος 2009
Θεσσαλονίκη

Περίληψη

Στα πλαίσια της συγγραφής αυτής της πτυχιακής εργασίας, πραγματοποιήθηκε η παρακάτω έρευνα. Αφορά μια εκτίμηση της υπηρεσίας Mobile Banking (m-banking) των τραπεζών. Είναι σχετικά μια νέα υπηρεσία των τραπεζών που έχει ως σκοπό τη διευκόλυνση των πελατών τους.

Η οικονομία σε παγκόσμιο επίπεδο αλλάζει αλματωδώς καθώς είναι συνυφασμένη με την ανάπτυξη της τεχνολογίας και ιδιαίτερα της πληροφορικής. Οι νέες τεχνολογίες που παρέχει στις επιχειρήσεις, η ανάπτυξη της πληροφορικής και ιδιαίτερα ο κλάδος των τηλεπικοινωνιών, έχουν εξαλείψει πλέον τις αποστάσεις και μέσω του ηλεκτρονικού επιχειρείν (e-business) οι εταιρείες έχουν εύκολη και γρήγορη πρόσβαση σε παγκόσμια κλίμακα.

Επειδή, στη σημερινή εποχή σημαντικό ρόλο παίζει η ταχύτητα διακίνησης της πληροφορίας, οι τράπεζες χρησιμοποιούν τα μέσα που τους παρέχει η τεχνολογία (π.χ. Internet, κινητή τηλεφωνία, κτλ.) με σκοπό την επιβίωση τους σε μια ανταγωνιστική και πελατοκεντρική αγορά. Το m-banking αποτελεί αποτέλεσμα της προσπάθειας των τραπεζών να εγκλιματιστούν σε αυτήν την εποχή.

Στην πτυχιακή αυτή εργασία, αναφέρεται η ευρύτερη έννοια της ηλεκτρονικής τραπεζικής (e-banking) και το νομοθετικό πλαίσιο που περιβάλλει αυτό το νέο είδος παροχής τραπεζικών υπηρεσιών, ενώ γίνεται προσπάθεια ανάλυσης της χρησιμότητας της υπηρεσίας m-banking, της ασφάλειας των τραπεζικών συναλλαγών μέσω χρήσης αυτής της εναλλακτικής υπηρεσίας, καθώς και των πλεονεκτημάτων και μειονεκτημάτων της. Ασφαλώς, γίνεται αναφορά της χρήσης του m-banking στην Ευρώπη αλλά και στην Ελλάδα. Δηλαδή, κατά πόσο οι τράπεζες παρέχον ηλεκτρονικές υπηρεσίες αλλά και κατά πόσο οι Έλληνες πελάτες είναι εξοικειωμένοι με τη χρήση της υπηρεσίας m-banking για τη διεκπαιρέωση των τραπεζικών τους συναλλαγών.

Πρόλογος

Η σημερινή εποχή προστάζει ακόμη και τις τράπεζες στην προσφυγή της χρήσης νέων τεχνολογιών για την αναβάθμιση των υπηρεσιών που παρέχουν, έτσι ώστε να επιβιώσουν σε ένα έντονα ανταγωνιστικό περιβάλλον. Η χρήση του Internet εισήγαγε μια νέα μορφή διεκπαιρέωσης των τραπεζικών συναλλαγών, το e-banking, το οποίο σε συνδυασμό με την κινητή τηλεφωνία κατάφερε να εισάγει ένα από τα είδη της ηλεκτρονικής τραπεζικής το m-banking. Με αυτόν τον τρόπο οι τράπεζες παρέχουν γρήγορα και εύκολα υπηρεσίες στους πελάτες-χρήστες τους αυξάνοντας το ανταγωνιστικό πλεονέκτημά τους.

Από την άλλη, αυτές οι καινοτόμες, εναλλακτικές τραπεζικές υπηρεσίες επέφεραν και νέου είδους κινδύνους που καλούνται να αντιμετωπίσουν τράπεζες και πελάτες, έτσι ώστε να διατηρήσουν την ασφάλεια των τραπεζικών συναλλαγών.

Στον ελλαδικό χώρο, η υπηρεσία m-banking βρίσκεται σε στάδιο ανάπτυξης. Αν και οι περισσότερες τράπεζες παρέχουν τις υπηρεσίες τους ηλεκτρονικά, το m-banking είναι ένα από τα είδη του e-banking που προσφέρεται από λίγες τράπεζες.

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να εκφράσω τις ευχαριστίες μου σε όσους με βοήθησαν για να διεκπεραιώσω την εργασία αυτή. Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του καθηγητή κ. Καργίδη Θεόδωρου, τον οποίο ευχαριστώ θερμά για τη συμπαράσταση και την καθοδήγηση καθ' όλη τη διάρκεια της εκπόνησης της παρούσας εργασίας. Θα ήθελα επίσης να ευχαριστήσω θερμά τον κ. Χατζηπουλίδη Άρη για όλο το χρονικό διάστημα της συγγραφής αυτής της εργασίας, που αφιέρωσε πολύτιμο χρόνο, με τις πολύτιμες οδηγίες, επισημάνσεις και διορθώσεις του για να με βοηθήσει να την φέρω εις πέρας καθώς και για το πολύτιμο βιβλιογραφικό υλικό που μου προσέφερε.

2**ΠΕΡΙΕΧΟΜΕΝΑ**

ΚΕΦΑΛΑΙΟ Ι: ΕΙΣΑΓΩΓΗ

i. Σπουδαιότητα του προβλήματος

Οι τράπεζες στην προσπάθειά τους να ανταποκριθούν στις απαιτήσεις του διεθνούς επιχειρηματικού περιβάλλοντος, εκτός από τις ακολουθούμενες στρατηγικές ενοποίησης (εξαγορές, συγχωνεύσεις, στρατηγικές συμμαχίες) εντός του κλάδου, αναπτύσσουν το εύρος των προσφερόμενων υπηρεσιών τους και γίνονται περισσότερο πελατοκεντρικές. Επίσης, συνεχώς βελτιώνουν την ποιότητα των προσφερόμενων τραπεζικών προϊόντων, υπηρεσιών τους και βελτιώνουν την παραγωγικότητά τους, αφού ολοένα και περισσότερο επενδύουν στη νέα τεχνολογία και στο ανθρώπινο δυναμικό.

Με την αξιοποίηση των λύσεων που προσφέρει η σύγχρονη τεχνολογία, επιταχύνονται οι καθημερινές διαδικασίες, μειώνεται ο χρόνος διεκπεραίωσης των συναλλαγών και δημιουργούνται ευέλικτες βάσεις δεδομένων που βοηθούν πολύπλευρα στην αποδοτικότητα της τράπεζας (π.χ. βοηθούν τα τμήματα μάρκετινγκ στην επίτευξη πωλήσεων). Στην ουσία, με την επίδραση της τεχνολογίας ολόκληρος ο τραπεζικός κλάδος μετασχηματίζεται, εφόσον δημιουργούνται νέα προϊόντα, διευκολύνεται η πρόσβαση σε νέες αγορές (με την εξάλειψη των γεωγραφικών ορίων), διακινείται λιγότερο χαρτί, υπάρχει καλύτερη διαχείριση των πληροφοριών κ.ο.κ. Ειδικότερα, η μεγάλη ανάπτυξη του διαδικτύου (internet) έχει επιπτώσεις, και στον τραπεζικό χώρο. Το χαμηλό κόστος και η εύκολη πρόσβαση που προσφέρει το διαδίκτυο στον κάθε χρήστη, έχει ήδη προκαλέσει ένταση του ανταγωνισμού στον συγκεκριμένο κλάδο και καθιέρωση εναλλακτικών δικτύων (τραπεζική μέσω διαδικτύου, τραπεζική μέσω σταθερού τηλεφώνου, τραπεζική μέσω κινητού τηλεφώνου) στην καθημερινή λειτουργία των τραπεζών αλλά και στη συνείδηση των πελατών.

Η ανάπτυξη των υπηρεσιών ηλεκτρονικής τραπεζικής (e-banking) τα τελευταία χρόνια υπήρξε μεγάλη και όλο και περισσότεροι πελάτες τραπεζών, εμπιστεύονται τις ηλεκτρονικές υπηρεσίες, απολαμβάνοντας

πλήθος ευκολιών και εξοικονομώντας πολύτιμο χρόνο. Στην Ελλάδα, η ηλεκτρονική τραπεζική είναι ένα σχετικά νέο εναλλακτικό κανάλι, που συναγωνίζεται αντίστοιχες προσφερόμενες υπηρεσίες του εξωτερικού.

Με την παρούσα εργασία θα μπορέσουμε να κατανοήσουμε τη νέα αυτή διάσταση που παίρνουν οι τραπεζικές εργασίες με τη χρήση της τεχνολογίας internet αλλά και κινητού τηλεφώνου.

ii. Στόχοι της εργασίας

Στόχος της παρούσας εργασίας αποτελεί η ανάλυση και η βαθύτερη κατανόηση του όρου m-banking αλλά και γενικότερα του μηχανισμού της ηλεκτρονικής τραπεζικής (e-banking). Επίσης, θα μπορέσουμε να κατανοήσουμε το μηχανισμό λειτουργίας της νέας αυτής υπηρεσίας των τραπεζών και θα εξάγουμε συμπεράσματα σχετικά με το πόσο ωφέλιμη υπηρεσία είναι για τους πελάτες των τραπεζών που την υποστηρίζουν, αλλά και να ξεχωρίσουμε τις αδυναμίες της. Τέλος, στόχος της εργασίας αυτής αποτελεί και η πληροφόρηση σχετικά με το στάδιο ανάπτυξης της υπηρεσίας m-banking από τις ελληνικές τράπεζες.

iii. Ορολογία

ATM	Αυτόματες Ταμειακές Μηχανές
BA	Bearer Adapter
e-banking	Electronic Banking
e–Code	Electronic Code
e-commerce	Electronic Commerce
e-mail	Electronic Mail
DES	Data Description Standard
IVR	Interactive Voice Response
m-banking	Mobile Banking
PDA	Personal Digital Assistant
SET	Secure Electronic Transaction
SMAC	Standalone Mobile Application Clients
SMS	Short Messaging Service
SSL	Secure Sockets Layer

PKI	Public Key Infrastructure
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WSP	Wireless Session Protocol
WTP	Wireless Transport Protocol
WTLS	Wireless Transport Layer Security

iv. Διάρθρωση της εργασίας

Στο δεύτερο κεφάλαιο, αναφέρεται η ετυμολογία του όρου e-banking, καθώς και τα είδη της ηλεκτρονικής τραπεζικής (internet, phone και mobile-banking). Γίνεται επίσης αναφορά της λειτουργίας του στην Ελλάδα, της ασφάλεια που το διέπει και της νομοθεσίας που το περιβάλλει. Τέλος, θα παρουσιάσουμε τα πλεονεκτήματα και τα μειονεκτήματα από τη χρήση του.

Στο τρίτο κεφάλαιο, αναλύονται, το m-banking ως προς τον ορισμό, τις εφαρμογές και τις βασικές του έννοιες, οι απαιτήσεις ασφάλειας και οι τρόποι υλοποίησης αυτών και φυσικά πώς επιτυγχάνεται η ασφάλεια των συναλλαγών από την πλευρά των τραπεζών, καθώς και όλα τα πλεονεκτήματα και μειονεκτήματα από την εφαρμογή του.

Στο τέταρτο κεφάλαιο, παρατίθενται οι κίνδυνοι και οι τρόποι ασφάλειας από τη χρήση της υπηρεσίας m-banking,το ηλεκτρονικό έγκλημα και οι δικτυακές απάτες και κανόνες για ασφαλείς συναλλαγές που προτείνουν οι ενώσεις Γερμανικών και Ελληνικών Τραπεζών στους πελάτες-χρήστες της υπηρεσίας αυτής.

Στο πέμπτο κεφάλαιο, περιγράφεται το m-banking στην Ευρώπη και στην Ελλάδα, πώς προσφέρεται η υπηρεσία από την Εθνική Τράπεζα της Ελλάδος (Ε.Τ.Ε) και την Τράπεζα Πειραιώς, την ασφάλεια που παρέχουν και τέλος ηλεκτρονικές διευθύνσεις των τραπεζών στην Ελλάδα που προσφέρουν την υπηρεσία m-banking.

Τέλος στο έκτο κεφάλαιο, ακολουθούν τα συνολικά συμπεράσματα της εργασίας.

ΚΕΦΑΛΑΙΟ ΙΙ: E-BANKING

Για να μπορέσουμε να αναλύσουμε και να κατανοήσουμε την υπηρεσία mobile banking, θα πρέπει να αναφερθούμε στην ευρύτερη έννοια της ηλεκτρονικής τραπεζικής, μιας και το m-banking αποτελεί ένα από τα είδη της. Σε αυτό το κεφάλαιο γίνεται επίσης αναφορά και του νομοθετικού πλαισίου που περιβάλλει το e-banking, το οποίο καθιερώνει τις τραπεζικές συναλλαγές μέσω διαδικτύου ασφαλείς.

i. Ορισμός του e-banking

E-banking ορίζεται ως η αυτοματοποιημένη παράδοση των νέων και των παραδοσιακών τραπεζικών προϊόντων και υπηρεσιών απευθείας στους πελάτες μέσω ηλεκτρονικών, διαδραστικών καναλιών επικοινωνίας. Το e-Banking περιλαμβάνει συστήματα που επιτρέπουν στο χρηματοπιστωτικό ίδρυμα, στους πελάτες, ιδιώτες ή στις επιχειρήσεις, να έχουν πρόσβαση σε λογαριασμούς, να συναλλάσσονται ή να λαμβάνουν πληροφορίες για τα χρηματοοικονομικά προϊόντα και υπηρεσίες μέσω δημόσιων ή ιδιωτικών δικτύων, συμπεριλαμβανομένου του Internet. Οι πελάτες μπορούν να έχουν πρόσβαση στην ηλεκτρονική τραπεζική υπηρεσία, χρησιμοποιώντας μια έξυπνη ηλεκτρονική συσκευή, όπως έναν προσωπικό υπολογιστή (PC), Personal Digital Assistant (PDA), αυτόματες ταμειακές μηχανές (ATM), περίπτερο, ή Touch Tone τηλέφωνο (**www.go-online.gr**).

ii. Χρήση

Οι πελάτες (ιδιώτες και επιχειρήσεις) ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking, καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με την τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις ΜΜΕ το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το

κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος.

Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής. Συχνό είναι και το φαινόμενο των προσφορών ή της εφαρμογής ευνοϊκότερων όρων στην παροχή προϊόντων μέσω Internet, γεγονός που από μόνο του είναι ικανό να προσελκύσει σημαντική μερίδα καταναλωτών που αναζητούν προσφορές.

Οι βασικότερες υπηρεσίες που παρέχουν μέσω Internet οι ελληνικές τράπεζες είναι οι εξής:

- Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς.
- Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος.
- Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών.
- Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων λογαριασμών.
- Παραγγελία μπλοκ επιταγών.
- Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκ επιταγών.
- Εντολές αγοραπωλησίας μετοχών.
- Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων.
- Δυνατότητα υποβολής αιτήσεων εμβασμάτων.
- Αλλαγή του απορρήτου κωδικού PIN.
- Προσωπικά μηνύματα.

Σε πολλές ευρωπαϊκές χώρες, όπου τα συστήματα πληρωμών είναι περισσότερο ανεπτυγμένα και τυποποιημένα, ο προσανατολισμός των τραπεζών στρέφεται σταδιακά στην παροχή πρόσθετων υπηρεσιών προς τις επιχειρήσεις (corporate sites), πεδίο στο οποίο η γκάμα των επιλογών είναι ιδιαίτερα διευρυμένη (**www.go-online.gr**).

iii. Είδη της ηλεκτρονικής τραπεζικής (e-banking)

Η ηλεκτρονική τραπεζική (electronic banking ή e-banking) χωρίζεται κυρίως στα εξής τρία είδη, σύμφωνα με το μέσο ή κανάλι, μέσω του οποίου πραγματοποιούνται οι τραπεζικές συναλλαγές (Αγγέλης, 2005):

1) Internet Banking (Τραπεζικές υπηρεσίες μέσω διαδικτύου)

Το "internet banking" που αποτελεί το σημαντικότερο κομμάτι του e-banking, πραγματοποιείται κατά κύριο λόγο μέσω του διαδικτύου, αλλά και μέσω άλλων δικτύων όπως εσωτερικών ή εξωτερικών (Intranets ή Extranets). Για να μπορέσει ένας χρήστης να χρησιμοποιήσει τις υπηρεσίες του χρειάζεται απαραίτητα να διαθέτει έναν ηλεκτρονικό υπολογιστή και μια σύνδεση στο διαδίκτυο. Στην πλειονότητα των περιπτώσεων, τα παραπάνω αρκούν για την πρόσβαση στις ηλεκτρονικές υπηρεσίες, ωστόσο για λόγους μεγαλύτερης ασφάλειας πολλές φορές απαιτούνται και ορισμένες συσκευές ασφάλειας, όπως οι έξυπνοι αναγνώστες ή ειδικό λογισμικό ασφάλειας (software) τα οποία τα παρέχουν οι τράπεζες στους πελάτες τους.

Μέσω του "internet banking" ο πελάτης έχει τη δυνατότητα να επιλέξει ανάμεσα σε μια μεγάλη ποικιλία τραπεζικών υπηρεσιών, στις οποίες θα αναφερθούμε αναλυτικά σε επόμενη ενότητα. Αξίζει να αναφέρουμε ότι τα χρηματοπιστωτικά ιδρύματα έχουν την τεχνογνωσία να προσωποποιούν τις προσφερόμενες ηλεκτρονικές υπηρεσίες τους, ανάλογα με την κατηγορία των πελατών που αυτές προορίζονται. Για παράδειγμα, σε εταιρικούς πελάτες, δηλαδή επιχειρήσεις, προσφέρονται περισσότερες δυνατότητες ηλεκτρονικών συναλλαγών, οι οποίες είναι ειδικά προσαρμοσμένες.

Θα πρέπει να τονίσουμε ότι η ασφάλεια στο internet banking είναι πολύ σημαντική και συνεχώς γίνονται προσπάθειες από την μεριά των τραπεζών, για την ασφαλή διεκπεραίωση των ηλεκτρονικών τραπεζικών συναλλαγών, αλλά και την δημιουργία εμπιστοσύνης στους πελάτες που χρησιμοποιούν

το "internet banking". Θα αναφερθούμε αναλυτικά σε θέματα ασφάλειας των ηλεκτρονικών συναλλαγών και προστασίας του καταναλωτή, σε επόμενο κεφάλαιο.

2) Phone Banking (Τραπεζικές υπηρεσίες μέσω σταθερού τηλεφώνου)

Οι υπηρεσίες που προσφέρει το "phone banking" χωρίζονται σε δύο κατηγορίες: α) Αυτές που διεκπεραιώνονται από πράκτορες τηλεφωνικών κέντρων (call center agents) και β) Αυτές που διεκπεραιώνονται αυτόματα μέσω ειδικών συστημάτων αναγνώρισης της φωνής (IVRs).

Και στις δύο περιπτώσεις το μόνο που απαιτείται από την πλευρά του πελάτη, είναι η ύπαρξη μιας τηλεφωνικής συσκευής και σύνδεσης. Στις τραπεζικές συναλλαγές με πράκτορες τηλεφωνικών κέντρων, ο υπάλληλος της τράπεζας αρχικά ζητά από τον πελάτη κάποια στοιχεία ταυτοποίησης και επαλήθευσης, όπως ένας προσωπικός κωδικός αριθμός (Pin). Αφού ο πελάτης δώσει σωστά αυτόν τον προσωπικό κωδικό, ο οποίος χρησιμοποιείται μόνο για τις συναλλαγές μέσω "phone banking" και όχι για άλλες συναλλαγές (π.χ. internet banking, ATMs), στη συνέχεια ο υπάλληλος του τηλεφωνικού κέντρου διεκπεραιώνει τις συναλλαγές που θα του υποδείξει ο πελάτης. Αντίστοιχη είναι και η δεύτερη κατηγορία του phone banking, με τη μόνη διαφορά ότι στην άλλη άκρη της τηλεφωνικής γραμμής δεν είναι ένας υπάλληλος της τράπεζας, αλλά ένας υπολογιστής ή καλύτερα ένα αυτοματοποιημένο σύστημα αναγνώρισης της φωνής IVR (Interactive Voice Response). Έτσι, η συγκεκριμένη διαδικασία είναι πλήρως αυτοματοποιημένη και ο πελάτης απαντά στα φωνητικά μηνύματα που ακούει.

Μέσω του "phone banking", ο χρήστης του, δηλαδή ο πελάτης μιας τράπεζας έχει στη διάθεσή του πάρα πολλές τραπεζικές υπηρεσίες είτε σε επίπεδο πληροφόρησης, είτε σε επίπεδο οικονομικών συναλλαγών. Έτσι, για παράδειγμα μπορεί να ενημερωθεί για το υπόλοιπο των λογαριασμών του, τις πρόσφατες κινήσεις των λογαριασμών του, και την αποτίμηση του χαρτοφυλακίου του σε επίπεδο πληροφόρησης. Ακόμη, έχει τη δυνατότητα να πραγματοποιήσει οικονομικές συναλλαγές όπως: μεταφορές κεφαλαίων

σε άλλους λογαριασμούς (στην ίδια ή σε άλλη τράπεζα και στην Ελλάδα ή στο εξωτερικό), πληρωμή λογαριασμών και πιστωτικών καρτών, πραγματοποίηση πάγιων εντολών για αγορά ή πώληση μετοχών και αμοιβαίων κεφαλαίων κ.ά.

3) Mobile Banking (Τραπεζικές υπηρεσίες μέσω κινητού τηλεφώνου)

Το τρίτο είδος της ηλεκτρονικής τραπεζικής, δηλαδή οι τραπεζικές υπηρεσίες που προσφέρονται μέσω κινητών τηλεφώνων (mobile banking), είναι στη φάση ανάπτυξης του ακόμα. Με αυτόν, τον εξελισσόμενο τομέα της ηλεκτρονικής τραπεζικής, είναι δυνατή η επικοινωνία μέσω κινητού τηλεφώνου με τη μορφή γραπτών μηνυμάτων και με την τεχνολογία "WAP", του πελάτη με την τράπεζα.

Οι υπηρεσίες που προσφέρονται με το "mobile banking" είναι περίπου οι ίδιες με τα υπόλοιπα δύο είδη της ηλεκτρονικής τραπεζικής. Πιο συγκεκριμένα, ο χρήστης έχει τη δυνατότητα να παρακολουθεί τα υπόλοιπα των λογαριασμών του καθώς και το χαρτοφυλάκιό του, να μεταφέρει χρήματα, να δίνει πάγιες εντολές για πληρωμές λογαριασμών και πιστωτικών καρτών κ.ά.

Οι τεχνολογίες που χρησιμοποιούνται σε αυτό το σύγχρονο είδος της ηλεκτρονικής τραπεζικής διαφέρουν πολλές φορές από αυτές που χρησιμοποιούνται στο "internet banking". Τα τελευταία χρόνια, μια εταιρεία κινητής τηλεφωνίας στη χώρα μας χρησιμοποιεί την τεχνολογία "i-mode", η οποία γνωρίζει μεγάλη ανάπτυξη στο εξωτερικό (και ιδιαίτερα στην Ιαπωνία) και πολλά είναι τα χρηματοπιστωτικά ιδρύματα που φιλοδοξούν να την εκμεταλλευτούν.

Θα πρέπει να αναφέρουμε ότι τραπεζικές υπηρεσίες μέσω κινητών τηλεφώνων (mobile banking), δεν προσφέρουν όλες οι τράπεζες στην Ελλάδα, σε αντίθεση με τα άλλα δύο είδη της ηλεκτρονικής τραπεζικής (internet banking, phone banking), τα οποία προσφέρονται από την πλειοψηφία των χρηματοπιστωτικών ιδρυμάτων.

iv. Το e-banking στην Ελλάδα

Έντονη ανάπτυξη παρουσιάζει η προσφορά τραπεζικών και χρηματιστηριακών συναλλαγών μέσω διαδικτύου από τις ελληνικές τράπεζες. Τράπεζες και επιχειρήσεις προχωρούν σε υψηλές επενδύσεις για την ανάπτυξη αυτού του τομέα, χωρίς να έχει απαντηθεί ακόμη το ερώτημα κατά πόσον έχουν αποδώσει τα κεφάλαια που δαπάνησαν.

Οι χρήστες του Internet στη χώρα μας υπολογίζονται σε 700 χιλιάδες περίπου και η συντριπτική πλειοψηφία τους είναι σε ηλικία κάτω από τα 20 έτη, με αποτέλεσμα να μην είναι οικονομικά ενεργοί. Αντιθέτως, μικρή είναι η εξοικείωση όσων έχουν οικονομική δραστηριότητα, ενώ έντονη είναι και η αμφισβήτηση για την ασφάλεια των ηλεκτρονικών συναλλαγών.

Έτσι η παροχή τραπεζικών υπηρεσιών μέσω Internet (e-banking) και πολύ συχνά και υπηρεσιών σχετικών με το Χρηματιστήριο βρίσκεται ακόμη σε πρώιμο στάδιο ανάπτυξης. Επίσης, οι ηλεκτρονικές συναλλαγές που γίνονται μέσω κινητού τηλεφώνου, το mobile banking, μια δυνατότητα που παρέχουν οι νέες γενιές τηλεφώνου, είναι πιο εξελιγμένη τεχνολογικά αλλά με μικρότερη ακόμη διείσδυση στην αγορά.

Θα πρέπει να τονιστεί ότι το e-banking αφορά συναλλαγές του πελάτη ως ιδιώτη με την τράπεζα, ενώ για τις εταιρείες διαμορφώνεται διαφορετικός τρόπος ηλεκτρονικής επικοινωνίας. Διαφέρει πάντως από το e-commerce το ηλεκτρονικό εμπόριο, που περνά από τα τραπεζικά κανάλια μόνο αναφορικά με την εκκαθάριση των συναλλαγών που πραγματοποιούνται.

Οι έρευνες στην ελληνική αγορά έχουν δείξει ότι οι χρήστες που επιλέγουν να επικοινωνήσουν "ηλεκτρονικά" με την τράπεζά τους περιορίζονται μόνο στην ενημέρωση για τους λογαριασμούς τους ή τα χαρτοφυλάκια μετοχών και αποφεύγουν άλλου είδους συναλλαγές. Ο λόγος είναι απλός: η επιφύλαξη για τη διατήρηση ενός "ασφαλούς" περιβάλλοντος στο διαδίκτυο. Οι τράπεζες πάντως εφαρμόζουν την τελευταία λέξη της τεχνολογίας σε επίπεδο ασφαλείας και έχουν επενδύσει πολλά στα πιο εξελιγμένα πρωτόκολλα ασφαλείας. Αξίζει να σημειωθεί ότι ανάλογη δυσπιστία είχε προκαλέσει και η εμφάνιση των ATMs, στα οποία πολλοί αποφεύγουν να κάνουν καταθέσεις υπό το "φόβο των Ιουδαίων".

Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω διαδικτύου. Τα αποτελέσματα της Εθνικής Έρευνας για τις Νέες Τεχνολογίες και την Κοινωνία της Πληροφορίας δείχνουν ότι το 2001 περίπου 150.000 πελάτες (1%-1,5% του πληθυσμού) πραγματοποίησαν τραπεζικές συναλλαγές ηλεκτρονικά. Το 2002 ο αριθμός αυτός ξεπέρασε τους 250.000 (2,5% του συνολικού πληθυσμού). Σύμφωνα με εκτιμήσεις τραπεζών, το 2001 ο τζίρος από online τραπεζικές συναλλαγές έφθασε τα 2 δισ. ευρώ. Το 2002 το ποσό αυτό εκτιμάται ότι αυξήθηκε σε 10 δισ. ευρώ, ενώ για φέτος αναμένεται να υπερβεί τα 12 δισεκατομμύρια.

Σύμφωνα με στοιχεία της Τράπεζας Πειραιώς, οι συναλλαγές μέσω Winbank Internet παρουσιάζουν ραγδαία ανάπτυξη: το 2003 οι εγχρήματες συναλλαγές αυξάνονται με ρυθμό της τάξεως του 150% έναντι του 2002. Επίσης, το 50% όλων των πληρωμών ΙΚΑ πραγματοποιείται on-line, ενώ οι ηλεκτρονικές χρηματιστηριακές συναλλαγές υπερβαίνουν το 15% επί του συνόλου.

Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο. Ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών. Ενδεικτικά, στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7% (**www.go-online.gr**).

v. Η ασφάλεια των συναλλαγών

Η ασφάλεια των συναλλαγών και των προσωπικών δεδομένων των χρηστών της ηλεκτρονικής τραπεζικής μέσω διαδικτύου (internet banking), είναι μείζονος σημασίας. Εκτός από τα συστήματα ασφάλειας των τραπεζών και των μέτρων προστασίας από την πλευρά του χρήστη υπάρχει ένα συγκεκριμένο νομοθετικό πλαίσιο σε σχέση με την ηλεκτρονική τραπεζική, το οποίο κατοχυρώνει ακόμη περισσότερο τον καταναλωτή(Αγγέλης, 2005).

Συγκεκριμένα, η πραγματοποίηση ηλεκτρονικών τραπεζικών συναλλαγών στο διαδίκτυο διέπεται από την ελληνική και την κοινοτική τραπεζική νομοθεσία. Το ρυθμιστικό πλαίσιο της ηλεκτρονικής τραπεζικής μέσω

διαδικτύου αφορά τη διασυνοριακή παροχή τραπεζικών και χρηματοοικονομικών υπηρεσιών. Οι κύριοι τομείς που θα αναλύσουμε στη συνέχεια και που διέπουν την ηλεκτρονική τραπεζική μέσω διαδικτύου είναι:

- ✓ Η νομοθεσία για τη διεξαγωγή τραπεζικών και χρηματοοικονομικών συναλλαγών – Τραπεζική εποπτεία.
- ✓ Η νομοθεσία για την προστασία του καταναλωτή.
- ✓ Η νομοθεσία για την προστασία των προσωπικών δεδομένων.
- ✓ Το ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική.

1. Γενική τραπεζική νομοθεσία

Η ηλεκτρονική τραπεζική (e-banking) υπάγεται ως τραπεζική εργασία, στην εποπτεία της Κεντρικής Τράπεζας και στις οδηγίες της Ευρωπαϊκής Ένωσης περί πιστωτικών ιδρυμάτων. Συνεπώς, ορισμένες διατάξεις που αφορούν τον περιορισμό του σκοπού και των ποσοστών συμμετοχής φυσικών ή νομικών προσώπων για τα πιστωτικά ιδρύματα, ισχύουν και στην περίπτωση της ηλεκτρονικής τραπεζικής. Τέλος, εφαρμόζονται οι ειδικές διατάξεις σχετικά με τη δημοσιοποίηση οικονομικών αποτελεσμάτων (π.χ. λογιστικές καταστάσεις).

Η εποπτεία από την κεντρική τράπεζα περιλαμβάνει τον ορισμό των ιδίων κεφαλαίων των πιστωτικών ιδρυμάτων (*ΠΔ/ΤΕ 2053/1992*), τον έλεγχο φερεγγυότητας (*ΠΔ/ΤΕ 2054/1992*), τον έλεγχο ρευστότητας, τον έλεγχο κεφαλαιακής επάρκειας (*ΠΔ/ΤΕ 2397/1996*), τον έλεγχο συγκέντρωσης κινδύνων (*ΠΔ/ΤΕ 2246/1993*) και του συστήματος εσωτερικού ελέγχου των τελευταίων (*ΠΔ/ΤΕ 2438/1998*). Επίσης, η οδηγία 2000/31 που αφορά το ηλεκτρονικό εμπόριο (ενσωματώθηκε στο ελληνικό δίκαιο με το *προεδρικό διάταγμα 131/2003*) ρυθμίζει τις υπηρεσίες ηλεκτρονικής τραπεζικής (Μαρούδη, 2005). Ειδικότερα η εν λόγω οδηγία εισάγει την αρχή του "κράτους προέλευσης" και αναφέρει ότι: " *ο τόπος εγκατάστασης εταιρείας που παρέχει υπηρεσίες μέσω διεύθυνσης (site) του διαδικτύου, δεν βρίσκεται εκεί που είναι η τεχνολογία που υποστηρίζει την εν λόγω διεύθυνση, ούτε εκεί που παρέχεται πρόσβαση στην εν λόγω διεύθυνση, αλλά εκεί που ασκεί την οικονομική της δραστηριότητα".*

Θα πρέπει να αναφέρουμε ότι και για την ηλεκτρονική τραπεζική εφαρμόζεται ο *νόμος 2076/1992* που αφορά τα χρηματοπιστωτικά ιδρύματα και ο *νόμος 2396/1996* που αφορά τις χρηματοοικονομικές υπηρεσίες. Φυσικά, όπως σε όλες τις περιπτώσεις, έτσι και στην περίπτωση της ηλεκτρονικής τραπεζικής, εφαρμόζονται οι διάφορες νομοθετικές ρυθμίσεις που εκδίδονται κατά καιρούς, είτε από τον Διοικητή της Τράπεζας της Ελλάδος, είτε από την επιτροπή κεφαλαιαγοράς.

Ακόμη, για την εξ' αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές είναι σε ισχύ η *οδηγία* της Ευρωπαϊκής Ένωσης *2002/65/ΕΚ*. Η τελευταία η οποία υπάγεται στο κοινοτικό δίκαιο, όταν ενσωματωθεί στο ελληνικό δίκαιο, θα παρέχει μια ολοκληρωμένη προστασία στον καταναλωτή σχετικά με τις χρηματοοικονομικές υπηρεσίες.

Τέλος, πρέπει να επισημάνουμε ότι η τράπεζα της Ελλάδος είναι αρμόδια για την εφαρμογή σε όλα τα πιστωτικά ιδρύματα, των διατάξεων του *νόμου 2331/95*, ο οποίος αφορά την πρόληψη και την καταστολή της νομιμοποίησης των εσόδων από εγκληματικές πράξεις. Επίσης, με τον *νόμο 2655/98* η Ελλάδα έχει επικυρώσει την Ευρωπαϊκή σύμβαση για το ξέπλυμα, την έρευνα, την κατάσχεση και τη δήμευση των προϊόντων, τα οποία προέρχονται από εγκληματικές πράξεις (G. Adams: 2003).

2. Νομοθεσία σχετικά με τις ηλεκτρονικές πληρωμές μέσω διαδικτύου

Οι ηλεκτρονικές πληρωμές, δηλαδή οι συναλλαγές που πραγματοποιούνται ηλεκτρονικά και ανεξάρτητα από τα μέσα που χρησιμοποιούνται, χωρίζονται στις εξής κατηγορίες: 1)Πληρωμές μέσω πιστωτικών καρτών (με χρέωση της κάρτας του πελάτη), 2)Απευθείας πίστωση ενός λογαριασμού με ταυτόχρονη μεταφορά σε άλλους λογαριασμούς (π.χ. πάγιες εντολές εξόφλησης λογαριασμών), 3)Απευθείας χρέωση του λογαριασμού του χρήστη, με χρήση αριθμού ή χρεωστικής κάρτας, 4)Πληρωμές μέσω προπληρωμένων καρτών και 5)Πληρωμές μέσω ειδικών πυλών πληρωμών.

Όσον αφορά το νομικό πλαίσιο αυτών των ηλεκτρονικών πληρωμών στην ηλεκτρονική τραπεζικής μέσω διαδικτύου (internet banking), εφαρμόζεται ο *νόμος 2789/2000*, ο οποίος έχει ενσωματώσει την κοινοτική *οδηγία 98/26*. Επίσης, το θεσμικό πλαίσιο για τις διασυνοριακές πληρωμές, το ρυθμίζει το *προεδρικό διάταγμα 33/2000*, το οποίο ακολουθεί την *οδηγία 97/5* για τις διασυνοριακές πληρωμές μέχρι 50.000 ευρώ. Το παραπάνω θεσμικό πλαίσιο ολοκληρώνεται με τον *κανονισμό 2560/2001*, ο οποίος διασφαλίζει τη διαφάνεια των εξόδων που επιβάλλονται αλλά και την ευθυγράμμιση του ύψους των συναλλαγών εντός της Ευρωπαϊκής Ένωσης.

Τέλος, ως προς την διεκπεραίωση οικονομικών συναλλαγών με ιδρύματα ηλεκτρονικού χρήματος, είναι σε ισχύ ο *νόμος 3148/2003*, ο οποίος έχει ενσωματώσει τις κοινοτικές *οδηγίες 2000/46 και 2000/28* που αφορούν το ηλεκτρονικό χρήμα.

3. Η νομοθεσία για την προστασία του καταναλωτή

Για την προστασία των καταναλωτών στην παροχή τραπεζικών υπηρεσιών και από φυσικά αλλά και από εναλλακτικά δίκτυα (internet banking), εφαρμόζεται ο *νόμος 2251/94*. Ειδικότερα στην περίπτωση της ηλεκτρονικής τραπεζικής, πρέπει τα χρηματοπιστωτικά ιδρύματα να συμμορφώνονται με τις διατάξεις για τις καταχρηστικές ρήτρες συμβάσεων με τους πελάτες τους, αλλά και με τις διατάξεις για την παραπλανητική διαφήμιση.

Ειδικά για τις προσφερόμενες υπηρεσίες ηλεκτρονικής τραπεζικής μέσω διαδικτύου (internet banking), κατευθυντήριες γραμμές δίνει το άρθρο 4 του προαναφερθέντος νόμου, το οποίο ενσωματώνει την κοινοτική *οδηγία 97/7* σχετικά με τις εξ' αποστάσεως συμβάσεις (διαδικτυακές συναλλαγές). Οι ηλεκτρονικές συμβάσεις που καταρτίζονται στο διαδίκτυο είναι είτε συμβάσεις προσχωρήσεως είτε συμβάσεις με γενικούς όρους συναλλαγών (Γ.Ο.Σ.), οι οποίοι έχουν διατυπωθεί εκ των προτέρων. Αυτοί οι όροι θα πρέπει να εμφανίζονται σε εμφανές μέρος του εγγράφου της σύμβασης, να είναι ευανάγνωστοι και να είναι διατυπωμένοι στην Ελληνική αλλά και στην Αγγλική γλώσσα.

Τέλος, όσον αφορά τη διαφήμιση στο διαδίκτυο και στο ηλεκτρονικό εμπόριο, εφαρμόζεται ο *νόμος 2251/1994* ο οποίος απαγορεύει κάθε αθέμιτη και παραπλανητική διαφήμιση.

4. Η νομοθεσία για την προστασία των προσωπικών δεδομένων

Το ζήτημα της προστασίας των προσωπικών δεδομένων των καταναλωτών είναι ιδιαίτερα σημαντικό για την προστασία των θεμελιωδών δικαιωμάτων τους, ελευθεριών τους αλλά και της ίδιας τους της ιδιωτικής ζωής. Το νομικό πλαίσιο που θωρακίζει τα προσωπικά δεδομένα των καταναλωτών, διέπεται από τον Ελληνικό *νόμο 2472/1997* αλλά και από διεθνείς συμβάσεις, όπως την "Οικουμενική διακήρυξη των Δικαιωμάτων του ανθρώπου" του ΟΗΕ (1948), το "Διεθνές Σύμφωνο Ατομικών και Πολιτικών Δικαιωμάτων" και τη "Σύμβαση της Ρώμης" για την προάσπιση των δικαιωμάτων και των θεμελιωδών ελευθεριών του ατόμου (1950).

Ακόμη, οι οδηγίες της Ευρωπαϊκής Ένωσης που ολοκληρώνουν το νομοθετικό πλαίσιο της προστασίας των προσωπικών δεδομένων του καταναλωτή είναι οι εξής:

1. Η κοινοτική *οδηγία 95/46/ΕΚ* αποτελεί τη βάση για την προστασία των καταναλωτών και την ελεύθερη κυκλοφορία των δεδομένων αυτών (ο προαναφερθέντας *νόμος 2472/1997* ενσωμάτωσε αυτή την οδηγία).
2. Η κοινοτική *οδηγία 97/66/ΕΚ* αποσκοπεί στην εναρμόνιση όλων των κρατών μελών, με στόχο να επιτευχθεί ένα ίδιο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων των πολιτών τους και ειδικότερα στον τομέα των τηλεπικοινωνιών (στην Ελλάδα ενσωματώθηκε στο νόμο 2774/99).
3. Η κοινοτική *οδηγία 2002/58/ΕΚ* είναι η πιο πρόσφατη, και αφορά την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Στην περίπτωση της ηλεκτρονικής τραπεζικής μέσω διαδικτύου, αποκτά ιδιαίτερη σημασία η απαγόρευση να διαβιβάζονται δεδομένα σε τρίτες

χώρες (εκτός Ε.Ε.), οι οποίες δεν παρέχουν "ικανοποιητικό επίπεδο προστασίας" (άρθρο 9 του *νόμου 2472/97*). Η απαγόρευση μπορεί να αρθεί στην περίπτωση που η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, κρίνει ότι το επίπεδο της παρεχόμενης προστασίας στην Τρίτη χώρα, είναι ικανοποιητικό.

5. Το Ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική

Το ρυθμιστικό πλαίσιο για την ηλεκτρονική τραπεζική στο Ευρωπαϊκό κοινοτικό δίκαιο έχει τους εξής στόχους:

- ✓ Να δημιουργήσει ένα συνεκτικό κανονιστικό πλαίσιο που θα εξασφαλίσει την άρτια παροχή ηλεκτρονικών τραπεζικών υπηρεσιών, αποφεύγοντας τις εθνικές νομοθετικές αποκλίσεις.
- ✓ Να διασφαλίσει τη συνοχή μεταξύ της νομοθεσίας για τα χρηματοπιστωτικά ιδρύματα και της οδηγίας για το ηλεκτρονικό εμπόριο.

Το Ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική, αποτελείται από αρκετές οδηγίες, οι οποίες είναι ταξινομημένες σε 3 θεματικές ενότητες:

1. Σε αυτήν την ενότητα εντάσσονται οι οδηγίες που αφορούν την ανάληψη και άσκηση δραστηριοτήτων ηλεκτρονικής τραπεζικής από τα κοινοτικά χρηματοπιστωτικά ιδρύματα. Ειδικότερα υπάρχουν οι εξής οδηγίες:

- Η βασική τραπεζική οδηγία *2000/12/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ανάληψη και άσκηση δραστηριότητας πιστωτικών ιδρυμάτων.

- Η *οδηγία 2000/28/ΕΚ* η οποία τροποποιεί την προηγούμενη.

- Η *οδηγία 2000/46/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την ανάληψη, την άσκηση και την προληπτική εποπτεία των δραστηριοτήτων των ιδρυμάτων ηλεκτρονικού χρήματος.

2. Σε αυτήν την ενότητα εντάσσονται οι οδηγίες που αφορούν την κοινωνία της πληροφορίας και την εξ' αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών. Ειδικότερα υπάρχουν οι εξής οδηγίες:

- Η *οδηγία πλαίσιο 2000/31/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για κάποιες νομικές πτυχές των υπηρεσιών της κοινωνίας της κυκλοφορίας και ιδιαίτερα του ηλεκτρονικού εμπορίου.

- Η *οδηγία 2002/65/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εξ' αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς τους καταναλωτές.

- Η *οδηγία 1999/93/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σε σχέση με τις ηλεκτρονικές υπογραφές.

- Η *οδηγία 98/48/ΕΚ* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, που τροποποιεί την *οδηγία 98/34/ΕΚ* και αφορά την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των προτύπων και των προδιαγραφών.

3. Σε αυτήν την ενότητα εντάσσονται κοινοτικές πράξεις που αφορούν την διενέργεια πληρωμών στο ηλεκτρονικό εμπόριο, και συνοπτικά είναι οι παρακάτω:

- Η σύσταση 97/489/ΕΚ της Ευρωπαϊκής Επιτροπής σχετικά με τις συναλλαγές που πραγματοποιούνται με μέσα ηλεκτρονικών πληρωμών.

- Ο κανονισμός 2560/2001/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο οποίος αφορά τις διασυνοριακές πληρωμές (σε Ευρώ).

- Η απόφαση-πλαίσιο 2001/413/ΔΕΥ του Ευρωπαϊκού Συμβουλίου για την καταπολέμηση της απάτης και της πλαστογραφίας. (Σινανιώτη-Μαρούδη, Φαρσαρώτας: 2005).

6. Οι ηλεκτρονικές υπογραφές στο Ελληνικό και Ευρωπαϊκό δίκαιο

Όπως αναφέραμε σε προηγούμενο κεφάλαιο, οι ηλεκτρονικές (ή ψηφιακές) υπογραφές αποσκοπούν στην δήλωση και εξασφάλιση της ταυτότητας του χρήστη (ή αντισυμβαλλομένου) σε ένα ανοικτό δίκτυο, όπως το διαδίκτυο ή με απλά λόγια είναι μια μέθοδος απόδειξης της γνησιότητας. Εδώ θα πρέπει να διευκρινίσουμε ότι η ηλεκτρονική υπογραφή έχει ποικίλες μορφές, όπως τη βιομετρική υπογραφή ή την ψηφιακή υπογραφή. Με άλλα λόγια, η ψηφιακή υπογραφή είναι μία μέθοδος ηλεκτρονικών υπογραφών και μάλιστα θεωρείται η πιο προηγμένη και ασφαλής μεταξύ των μεθόδων αναγνώρισης της γνησιότητας ενός εκδότη ηλεκτρονικού εγγράφου. Για να διασφαλιστεί λοιπόν, η ασφάλεια των χρηστών σε μια ηλεκτρονική σύμβαση όταν χρησιμοποιούν ηλεκτρονικές υπογραφές, έχει θεσπιστεί ένα ολόκληρο νομικό πλαίσιο.

Πιο συγκεκριμένα, η *οδηγία 1999/93/ΕΚ* έθεσε τις βάσεις για τη δημιουργία ενός ολοκληρωμένου ρυθμιστικού πλαισίου σχετικά με τις ηλεκτρονικές υπογραφές στα κράτη της Ευρωπαϊκής Ένωσης. Η σημαντικότερη συνεισφορά της, συνίσταται στη νομική αναγνώριση των ηλεκτρονικών υπογραφών ως αντιστοίχων με τις ιδιόχειρες, εκεί που απαιτείται από τον νόμο. Στο *άρθρο 5.1*. της συγκεκριμένης οδηγίας απαριθμούνται οι προϋποθέσεις που είναι απαραίτητες για τη δημιουργία ενός ενιαίου επιπέδου ηλεκτρονικών υπογραφών μεταξύ των κρατών μελών. Στην Ελλάδα, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι υπεύθυνη να παρακολουθεί και να ρυθμίζει εκτός των άλλων, τις υπάρχουσες ηλεκτρονικές υπογραφές.

Η προσαρμογή της προηγούμενης οδηγίας στα ελληνικά δεδομένα, πραγματοποιήθηκε με την ενσωμάτωσή της στο *προεδρικό διάταγμα 150/2000* για τις ηλεκτρονικές υπογραφές. Το εν λόγω διάταγμα αναγνωρίζει στην Ελλάδα, τους ακόλουθους τύπους ηλεκτρονικών υπογραφών:

1. Τις απλές ηλεκτρονικές υπογραφές (π.χ. με ένα ψηφιακό αποτύπωμα μιας χειρόγραφης υπογραφής).

2. Τις προηγμένες ηλεκτρονικές υπογραφές οι οποίες διέπονται από τις εξής αυστηρές προϋποθέσεις: α) Η μονοσήμαντη σύνδεση της υπογραφής με τον υπογράφοντα, β) Η ικανότητά της να προσδιορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντα, γ) Η δημιουργία της με μέσα του αποκλειστικού ελέγχου του υπογράφοντα και δ) Η εύκολη διαπίστωση ενδεχόμενης αλλοίωσης στα δεδομένα της εκάστοτε ψηφιακής υπογραφής.
3. Τις προηγμένες ηλεκτρονικές υπογραφές οι οποίες έχουν αναγνωρισμένο πιστοποιητικό (Clarke, Roger, 1996).

7. Εφαρμοστέο δίκαιο - Συμπεράσματα

Στον Ευρωπαϊκό χώρο ισχύει ο *Κανονισμός ΕΚ/44/2001* και θα πρέπει να τονίσουμε ότι καθοριστική σημασία για την ηλεκτρονική τραπεζική μέσω διαδικτύου (Internet banking), διαδραματίζει η κατοικία του εναγόμενου, ανεξάρτητα από την τοποθεσία που βρίσκεται εγκατεστημένος ο υπολογιστής. Στα *άρθρα 5.1., 5.3. και* 16 του συγκεκριμένου κανονισμού αναφέρονται 3 εξαιρέσεις από τον παραπάνω κανόνα:

1. Όταν υπάρχουν διαφορές εκ συμβάσεως, αρμόδιο είναι το δικαστήριο του τόπου εκπλήρωσης της παροχής.
2. Όταν εμφανιστεί περίπτωση αδικοπραξίας, αρμόδιο είναι το δικαστήριο του τόπου όπου έλαβε χώρα το ζημιογόνο γεγονός. Φυσικά, για τις περιπτώσεις του διαδικτύου τα πράγματα είναι ιδιαίτερα δύσκολα, καθώς είναι δυνατόν να θεωρηθεί ότι κάποιο γεγονός αδικοπραξίας (π.χ. διασπορά ιού υπολογιστών από κάποια ιστοσελίδα τράπεζας) έλαβε χώρα σε όλα τα κράτη μέλη!
3. Η πιο σημαντική εξαίρεση αφορά τις συμβάσεις των καταναλωτών, αφού σύμφωνα με το άρθρο 16 ο κάθε καταναλωτής έχει τη δυνατότητα να ασκήσει αγωγή είτε στον τόπο κατοικίας του είτε στον τόπο κατοικίας του αντισυμβαλλομένου του.

Συμπερασματικά, θα μπορούσαμε να πούμε ότι για την περίπτωση της ηλεκτρονικής τραπεζικής μέσω διαδικτύου (internet banking), μπορεί η εν δυνάμει πελατειακή βάση να είναι παγκόσμια, εντούτοις δεν είναι εφικτό τα

χρηματοπιστωτικά ιδρύματα να πληρούν και να συμμορφώνονται με το σύνολο των νόμων της κάθε χώρας.

Οι Ελληνικές τράπεζες οφείλουν να συμμορφώνονται με τους ελληνικούς νόμους στους 3 τομείς που αναφέραμε σε προηγούμενες ενότητες (τραπεζική νομοθεσία, προστασία καταναλωτή και προστασία προσωπικών δεδομένων) και να προσπαθούν να συμμορφώνονται με τις νομικές απαιτήσεις των χωρών προς τις οποίες απευθύνουν τα προϊόντα/υπηρεσίες τους στο εξωτερικό (E. Banks: 2001).

vi. Τα πλεονεκτήματα και τα μειονεκτήματα από τη χρήση του e-banking

Τι προσφέρει το e-banking; Πλεονεκτήματα που έχουν να κάνουν με το κόστος και το χρόνο. Οι ηλεκτρονικές συναλλαγές γίνονται απλά μέσω του ηλεκτρονικού υπολογιστή, χωρίς ανάγκη μετακίνησης, με αποφυγή της γραφειοκρατίας και της "ουράς". Οι πιο συχνές υπηρεσίες που προσφέρονται διαδικτυακά είναι η ενημέρωση για την κίνηση λογαριασμών, η μεταφορά χρημάτων μεταξύ λογαριασμών, η πληρωμή λογαριασμών και πιστωτικών καρτών. Επίσης έχουμε μείωση του λειτουργικού κόστους των τραπεζών, άμεση επέκταση της γεωγραφικής παρουσίας της, δυνατότητα ανάπτυξης νέων επιχειρηματικών δραστηριοτήτων και πλήρη διαφάνεια των όρων των συναλλαγών από πλευράς τιμής και κόστους. Πρόσφατα δόθηκε η δυνατότητα καταβολής ΦΠΑ μόνο όμως σε όσους υποβάλλουν με τον ίδιο τρόπο φορολογική δήλωση. Με το e-banking οι τραπεζικές συναλλαγές προσφέρονται ανά πάσα στιγμή με ευκολία και ταχύτητα. Πρέπει να σημειωθεί ότι σε πολλές τραπεζικές εργασίες απαιτείται η "φυσική" υπογραφή του πελάτη, όπως για παράδειγμα στα δάνεια, ώστε να μην είναι δυνατή η διάθεσή τους μέσω Internet. Φυσικά η κατηγορία αυτή απαιτεί πελάτες ανώτερου μορφωτικού επιπέδου και αφήνουν μεγαλύτερο κέρδος στην τράπεζα από τον μέσο πελάτη.

Παρόλα αυτά όμως υπάρχουν και μερικά μειονεκτήματα από τη χρήση του e-banking, όπως η έλλειψη απόδειξης και υπογραφής κατά την πραγματοποίηση των τραπεζικών συναλλαγών, γι' αυτό εμφανίζεται ιδιαίτερη δυσπιστία κατά τη χρήση του. Τέλος άλλο ένα μειονέκτημα

αποτελεί η συγκέντρωση πληροφοριών από ένα τρίτο μη εξουσιοδοτημένο πρόσωπο γύρω από τη οικονομική, ιδιωτική ζωή των πολιτών (**www.naftemporiki.gr**).

ΚΕΦΑΛΑΙΟ ΙΙΙ: MOBILE BANKING

Σε αυτό το κεφάλαιο ορίζεται η έννοια του mobile banking, αναφέρεται η χρήση αυτής της υπηρεσίας και τα κανάλια διανομής της. Επίσης γίνεται αναφορά στις απαιτήσεις ασφάλειας της υπηρεσίας αυτής αλλά και στον τρόπο υλοποίησης αυτών των απαιτήσεων από τις τράπεζες. Τέλος, παρατίθενται τα πλεονεκτήματα και τα μειονεκτήματα από τη χρήση του m-banking και δίδεται η χρήση της υπηρεσίας αυτής στον ελλαδικό χώρο αλλά και στην Ευρώπη.

i. Ορισμός του m-banking

Το m-banking, σύντμηση του mobile banking, επιτρέπει τη διαχείριση των τραπεζικών λογαριασμών από το κινητό τηλέφωνο. Πρόκειται για μια υπηρεσία που διαθέτει τα χαρακτηριστικά ενός σύνθετου τρόπου πληρωμής, ο οποίος μπορεί να χρησιμοποιηθεί ως εναλλακτική λύση έναντι των μετρητών, της επιταγής, του online-banking και τις πιστωτικής κάρτας (Κελτσόπουλου, Συρμακέζη, 1997).

Το ηλεκτρονικό εμπόριο μέσω κινητού τηλεφώνου βρίσκει εφαρμογή σε ένα ευρύ πεδίο δραστηριοτήτων, πυρήνα των οποίων αποτελεί ο κύκλος των εμπορικών συναλλαγών. Κατά συνέπεια μιλάμε για την ηλεκτρονική εμπορευματοποίηση των φυσικών αγαθών και υπηρεσιών, τη διαφήμιση και προώθηση αυτών, την διευκόλυνση της επικοινωνίας μεταξύ των εμπόρων, την υποστήριξη πελάτη(πριν και μετά την πώληση, την εξαγγελία προμήθειας και την υποστήριξη κοινών επιχειρηματικών διαδικασιών).

Οι βασικές υπηρεσίες που μπορούν να γίνουν μέσω m-banking είναι:

- ✓ Πληροφορίες για την κίνηση του λογαριασμού και για το περιεχόμενο της τελευταίας κατάστασης του λογαριασμού
- ✓ Πληροφορίες για τραπεζικές εντολές
- ✓ Πληροφορίες για κάρτες
- ✓ Αλλαγή ταχυδρομικής διεύθυνσης
- ✓ Πάγιες εντολές εξόφλησης λογαριασμών ΟΤΕ, ΔΕΗ κλπ και ανακλήσεις αυτών

- ✓ Αλλαγή σε τραπεζική εντολή
- ✓ Επανέκδοση κατάστασης λογαριασμού ή καρνέ επιταγών
- ✓ Μεταφορά κεφαλαίων μεταξύ λογαριασμών του ίδιου του πελάτη ή μεταξύ λογαριασμών αυτού και λογαριασμών τρίτων στην τράπεζα ή σε άλλο πιστωτικό ίδρυμα
- ✓ Μεταφορά κεφαλαίων για πληρωμή πιστωτικής κάρτας του πελάτη ή για πληρωμή δανείου
- ✓ Διαβίβαση χρηματιστηριακών εντολών
- ✓ Ακύρωση πιστωτικής κάρτας
- ✓ Επανέκδοση PIN ή κάρτας
- ✓ Αίτηση για χορήγηση δανείου ή κάρτας
- ✓ Συναλλαγματικές ισοτιμίες
- ✓ Λήψη πληροφοριών και διαφημιστικών μηνυμάτων για υπηρεσίες

ii. Εφαρμογές του m-banking

Η ανάπτυξη του m-banking υπόσχεται μία επανάσταση στις τραπεζικές συναλλαγές. Συγκεκριμένα καθιστά δυνατή τη διαχείριση τραπεζικών λογαριασμών από κινητές συσκευές καθώς και την άμεση διενέργεια συναλλαγών, χωρίς ο πελάτης να δεσμεύεται από παράγοντες όπως ο χρόνος ή ο τόπος. Οι ευκολίες που προσφέρει και η ευχρηστία του σε συνδυασμό με την εκτεταμένη χρήση κινητών τηλεφώνων το έχουν κάνει ιδιαίτερα δημοφιλή στο καταναλωτικό κοινό σε ολόκληρο τον κόσμο.

Οι υπηρεσίες που προσφέρονται στους χρήστες κινητών συσκευών μέσω του mobile banking αναλυτικά είναι (**www.eurobank.gr**):

Ενημέρωση

Τραπεζικές Υπηρεσίες

- Συνολική Εικόνα Πελάτη (λογαριασμοί, κάρτες, δάνεια, μετοχές, Α/Κ)
- Πληροφορίες Λογαριασμών (δικαιούχοι, δεσμευμένο/ λογιστικό υπόλοιπο, πιστωτικοί/ χρεωστικοί τόκοι, κατάστημα διαχείρισης, κλπ.)
- Υπόλοιπα Λογαριασμών

- Κινήσεις Λογαριασμών
- Υπόλοιπα Πιστωτικών Καρτών
- Κινήσεις Πιστωτικών Καρτών
- Πληροφορίες Δανείων (συνδεδεμένοι λογ/σμοί, όρια, δεσμεύσεις, κτλ.)
- Υπόλοιπα Δανείων
- Κινήσεις Δανείων
- Τηλεειδοποιήσεις μέσω sms & e-mail για ημερήσιες κινήσεις λογαριασμών και πιστωτικών καρτών
- Πληροφορίες κατάθεσης πολλαπλών επιταγών
- Πληροφορίες/ Κατάσταση μεμονωμένων επιταγών (και σε ενέχυρο)
- Ενημέρωση για Εγγυητικές επιστολές
- Ιστορικότητα Συναλλαγών (μεταφορών, πληρωμών, εμβασμάτων)
- Πληροφορίες Συναλλαγής (ημ/νία, λογ. Χρέωσης/ πίστωσης, αιτιολογία, κτλ)

Χρηματιστηριακές Υπηρεσίες

- Παρακολούθηση της συνεδρίασης του ΧΑΑ
- Οικονομικές Αναλύσεις, on-line νέα της αγοράς, ημερήσιο σχόλιο
- Παρουσίαση Online ενδοσυνεδριακών δεδομένων & Ticker ΧΑΑ
- Κινήσεις Παραγώγων
- Εταιρικά Νέα & Εταιρικές Πράξεις των τραπεζών
- Συγκριτικά Γραφήματα επενδυτικών προϊόντων
- Ισολογισμοί & Αριθμοδείκτες Εισηγμένων Εταιριών
- Δημόσιες Εγγραφές
- Ημερήσιο Κλείσιμο Μετοχών, Παραγώγων, Αμοιβαίων Κεφαλαίων
- Ημερήσιο Δελτίο Τιμών Ομολόγων Ελληνικού Δημοσίου
- Δελτίο Τιμών Εμπορευμάτων
- Διεθνείς Δείκτες
- Κατάσταση Ημερήσιων Εντολών Μετοχών και Α/Κ

Συναλλαγές

Μεταφορές (on-line, προγραμματισμένες & περιοδικές)

- Μεταφορά Χρημάτων μεταξύ Προσωπικών Λογαριασμών

- Μεταφορά Χρημάτων σε Λογαριασμούς Τρίτων
- Μεταφορά Χρημάτων σε Λογαριασμούς Εσωτερικού εκτός τράπεζας
- Μεταφορά Χρημάτων σε Λογαριασμούς Εξωτερικού (λογαριασμούς του ιδίου, φοιτητικό έμβασμα, συνδρομή εφημερίδων και περιοδικών)
- Ομαδική Μεταφορά
- Διαχείριση εντολής προγραμματισμένης-περιοδικής μεταφοράς

Πληρωμές (on-line & προγραμματισμένες)

- Πληρωμή Δόσης Δανείου
- Πληρωμή Πιστωτικής Κάρτας
- Χρέωση Πιστωτικού Ορίου
- Πληρωμή Πιστωτικής Κάρτας άλλης Τράπεζας
- Φόρτιση/ Επαναφόρτιση Προπληρωμένης Κάρτας
- Πληρωμές Δημοσίου (ΦΠΑ, ΙΚΑ, ΟΑΕΕ, ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ, Φόρου Εισοδήματος, Εθνικό Κτηματολόγιο 401, Εθνικό Κτηματολόγιο 402, ΔΕΥΑ Ρόδου, Ενιαίου Φόρου Ακινήτων Φυσικών Προσώπων)
- Πληρωμές Τηλεφωνίας (Vodafone, WIND, Tellas, Columbia Telecom, Lannet, Forthnet, Vivodi, CYTA Hellas)
- Πληρωμές Ασφαλειών και λογαριασμών
- Διαχείριση εντολής προγραμματισμένης πληρωμής

Πληρωμή Μέσω Πάγιας Εντολής

- Λογαριασμών Δημοσίου (ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ, ΟΑΕΕ)
- Λογαριασμών Τηλεφωνίας
- Λογαριασμών Ασφάλειας
- Άλλων Λογαριασμών
- Απενεργοποίηση Πάγιων Εντολών

Χρηματιστήριο

- Αγορά και Πώληση Μετοχών
- Ακύρωση εντολής Αγοράς, Πώλησης Μετοχών
- Intraday Εντολές Μετοχών
- Συμμετοχή στην τράπεζα με δυνατότητα Εξαγοράς, Μεταφοράς

- Ακύρωση Εντολών Eurobank A/K
- Συμμετοχή σε Δημόσιες Εγγραφές
- Ακύρωση Αίτησης Συμμετοχής σε Δημόσιες Εγγραφές
- Δημιουργία, Διαχείριση & Αποτίμηση Εικ. Χαρτοφυλακίων Μετοχών & A/K

Αιτήσεις

- Αίτηση Έκδοσης Μπλοκ Επιταγών
- Αίτηση Αλλαγής Κύριας Διεύθυνσης
- Αίτηση εγγραφής στο Mobile Banking
- Αίτηση προσωποποίησης πιστωτικής κάρτας

Άλλες Υπηρεσίες

- Αποστολή, παραλαβή κρυπτογραφημένων προσωπικών μηνυμάτων
- Δυνατότητα διενέργειας δωρεάς σε Κοινωφελείς Οργανισμούς

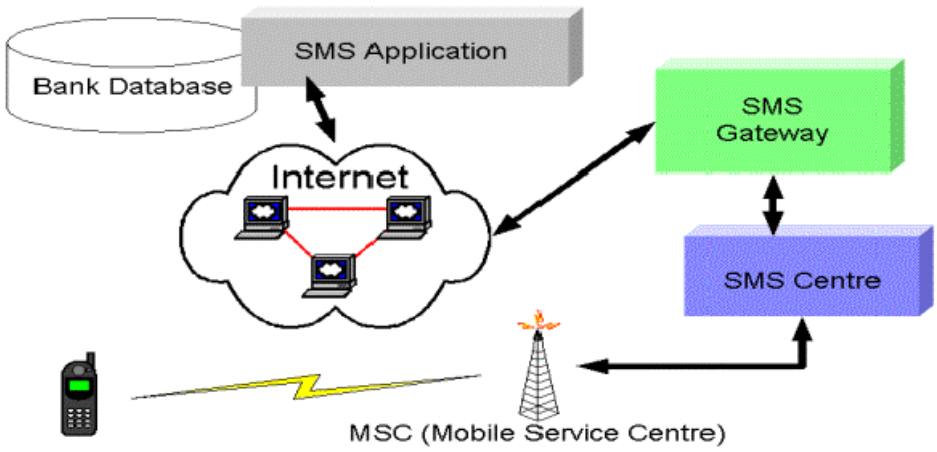
Εργαλεία

- Αλλαγή Κωδικού Εισόδου (Password)
- Αλλαγή Κωδικού Πιστοποιητικού (Certificate)
- Ονομασία προϊόντων (λογ/σμοι, κάρτες, δάνεια)
- Ευρετήριο λογ/σμών
- Ευρετήριο Πιστωτικών Καρτών
- Διαχείριση Ψηφιακών Πιστοποιητικών

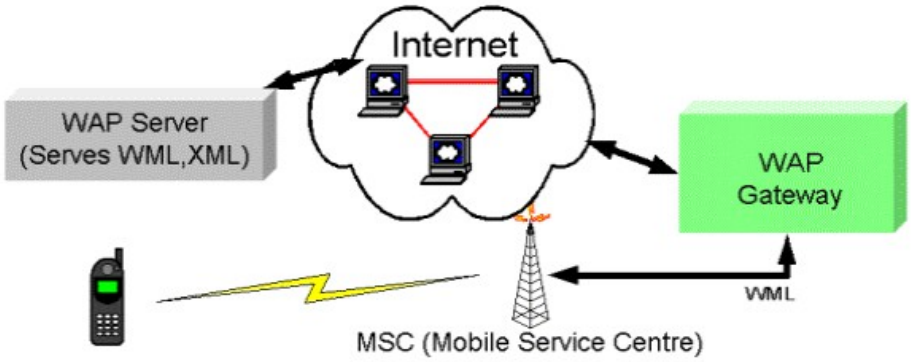
iii. Βασικές έννοιες του m-banking

Κανάλια διανομής (www.hba.gr):

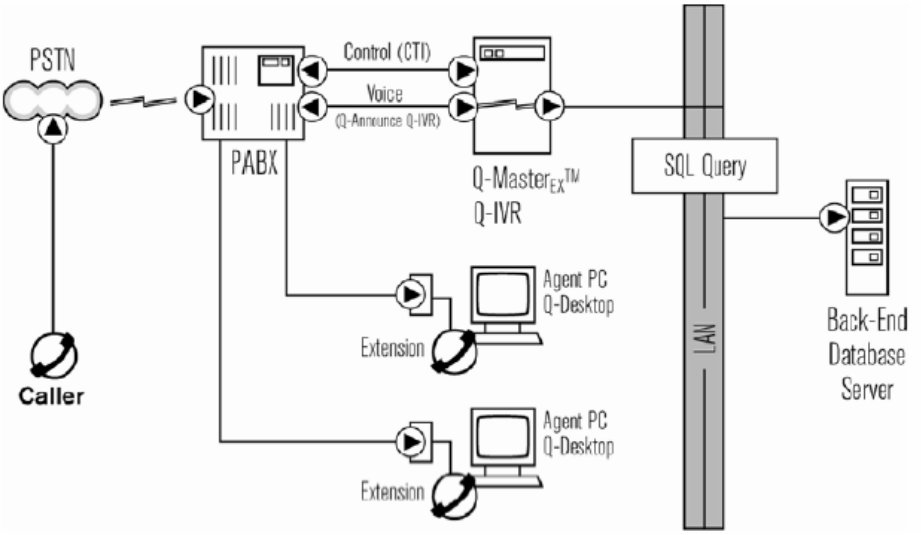
8. SMS(Short Messaging Service)



9. WAP(Wireless Application Protocol)



10. IVR(Interactive Voice Response)



11. SMAC(Standalone Mobile Application Clients)

iv. Απαιτήσεις ασφάλειας m-banking

Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή του κινητού εμπορίου είναι η Εμπιστευτικότητα (Cofidentiality) η Ακεραιότητα (Intergity) και ο Έλεγχος Αυθεντικότητας (Authentication), ενώ ο έλεγχος προσπέλασης (Access Control), η εξουσιοδότηση (Authorization), η μη αποποίηση ευθύνης (Non- Repudiation), η επίβλεψη (Auditing) και η υπευθυνότητα (Accountability) είναι μερικές ακόμη απαιτήσεις που εξασφαλίζουν την ασφάλεια των τραπεζικών συναλλαγών μέσω κινητού τηλεφώνου.

1. Εμπιστευτικότητα (Confidentiality). Η εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας των μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσω κρυπτογράφησης. Σε ένα ηλεκτρονικό περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.
2. Ακεραιότητα (Integrity). Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσω ψηφιακής υπογραφής. Τα

δεδομένα που ανταλλάσσονται ως μέρος της συναλλαγής πρέπει να είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς και αποθήκευσης τους στο δίκτυο.

3. Έλεγχος Προσπέλασης (Access Control) και Εξουσιοδότηση (Authorization). Η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στον λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.
4. Αυθεντικότητα (Authentication). Η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά τη μεταφορά, οριοθετούν την έννοια του ελέγχου αυθεντικότητας. Σύμφωνα με τον παραπάνω ορισμό, η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη, ώστε κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσω ψηφιακής υπογραφής.
5. Μη αποποίηση ευθύνης (Non- Repudiation). Κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή.
6. Επίβλεψη (Auditing) και Υπευθυνότητα (Accountability). Η εμπιστοσύνη, ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται. Για παράδειγμα, μια από τις απαιτήσεις του πελάτη είναι η βεβαιότητα ότι ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος (Μπερνίτσα, 1985:8).

v. Υλοποίηση βασικών απαιτήσεων

Η μεγάλη ασφάλεια μπορεί να συνοδεύεται από μεγάλη πολυπλοκότητα επίτευξής της. Κάθε βήμα που πραγματοποιείται πρέπει να είναι όσο το δυνατόν πιο κατανοητό και απλό για όλους μέσα σε μια εταιρεία. Όσο

περισσότερα δυσνόητα σημεία περιέχουν οι οδηγίες και οι διαδικασίες, τόσο αυξάνονται οι πιθανότητες παρερμηνείας και κακής εφαρμογής.

Η ασφάλεια και η ευκολία χρήσης των συστημάτων είναι συχνά παράγοντες αντιστρόφως ανάλογοι. Δεν υπάρχει «πλήρης ασφάλεια» σε ένα εύχρηστο σύστημα. Κατά συνέπεια, είναι σημαντικό να προσπαθεί κανείς να μειώσει ένα κίνδυνο, χωρίς όμως να σπαταλά πόρους, προσπαθώντας να τον εξαλείψει πλήρως. Μια τέτοια πραγματική αντίληψη εξασφαλίζει μια καλή ευκαιρία να επιτευχθεί ένα επαρκές επίπεδο ασφαλείας, χωρίς να επηρεάζεται η παραγωγικότητα.

Είναι προτιμότερο να υπάρχει ένας επαρκής και ικανοποιητικός βαθμός ασφαλείας σήμερα, παρά να επιδιώκεται η απόλυτη ασφάλεια.

Μια λανθασμένη αίσθηση ασφαλείας είναι χειρότερη από μια ρεαλιστική αίσθηση ανασφάλειας. Γνωρίζοντας τις αδυναμίες της εταιρείας όσον αφορά την ασφάλεια αποκτούμε ένα πλαίσιο για περαιτέρω ενέργειες. Μια λανθασμένη αίσθηση ασφαλείας δεν παρέχει κίνητρα για βελτίωση.

Είναι καλύτερα να επικεντρωνόμαστε σε γνωστές, πιθανές απειλές. Υπάρχουν κατά φαντασία απειλές, πραγματικές και πιθανές απειλές. Επίσης, υπάρχουν γνωστές και άγνωστες απειλές. Πιο ρεαλιστικό είναι να μας ενδιαφέρουν οι πραγματικές και πιθανές απειλές και στη συνέχεια το σύνολο των γνωστών απειλών(Μάγιογλου, 2005).

1) **Σχεδιασμός και Υλοποίηση Συστήματος Ασφάλειας**

Όταν τα παραπάνω για να γίνουν κοινός τόπος για όλους τους εμπλεκόμενους ενός συστήματος ασφαλείας, θα πρέπει να ακολουθήσουν τα παρακάτω βήματα για την ανάλυση, το σχεδιασμό και την υλοποίηση ενός τέτοιου συστήματος.

Φάση 1: Ανάλυση επικινδυνότητας υπαρχόντων συστημάτων (Risk Analysis). Στη φάση αυτή πρέπει να καταγραφεί η ανάλυση των κινδύνων και η αξιολόγηση των απειλών. Περιλαμβάνονται ο προσδιορισμός και η αξιολόγηση των πλεονεκτημάτων, ανάδειξη και ανάλυση των απειλών,

αξιολόγηση των τρωτών σημείων, εκτίμηση των υφιστάμενων αντιμέτρων, καθώς και ανάλυση του λόγου κόστους.

Φάση 2: Καθορισμός βασικής πολιτικής ασφάλειας (Security Policy) και σύνταξη εγχειριδίων ασφάλειας (Security Manual). Μπορεί πλέον να αναπτυχθεί η βασική πολιτική ασφάλειας. Με τη βασική πολιτική ασφάλειας αντιμετωπίζεται ο τρόπος με τον οποίο ένας οργανισμός χειρίζεται τις πληροφορίες και καθορίζονται πώς και ποιοί θα έχουν πρόσβαση στις πληροφορίες αυτές. Επίσης, προσδιορίζονται οι τρόποι ελέγχου που εφαρμόζονται. Η βασική πολιτική ασφαλείας περιλαμβάνει συνήθως τα εξής:

- Γενική παρουσίαση βασικής πολιτικής.
- Κατευθυντήριες γραμμές αρχιτεκτονικής ασφάλειας.
- Διαδικασίες ανταπόκρισης σε συμβατά–εισβολές.
- Πολιτικές αποδεκτής χρήσης.
- Διαδικασίες διαχείρισης συστήματος.
- Άλλες διαδικασίες διαχείρισης.

Φάση 3: Σχεδιασμός λύσεων ασφαλείας. Αφού οι απαιτήσεις είναι πλέον καλά προδιαγεγραμμένες από το Security Manual, είναι εύκολο για τους υπεύθυνους συμβούλους ασφαλείας να παρουσιάσουν τις εναλλακτικές αρχιτεκτονικές συστημάτων και να αξιολογήσουν ποιες από αυτές ικανοποιούν την πλειονότητα των απαιτήσεων και σε ποιο βαθμό, έτσι ώστε να γίνει βέλτιστη με οικονομο–τεχνικά κριτήρια.

Φάση 4: Υλοποίηση λύσεων ασφαλείας. Στην υλοποίηση πλέον των λύσεων γίνεται η εφαρμογή όλου του Security Policy του οργανισμού. Ο έλεγχος του συστήματος είναι το πιο σημαντικό στάδιο αυτής της φάσης γιατί θα πρέπει να προσομοιωθούν όλοι οι δυνατοί συνδυασμοί που μπορεί να προκύψουν κατά τη λειτουργία του συστήματος, όπως επίσης πρέπει να ελεγχθούν η συμπεριφορά και η αντίδραση του συστήματος μετά την αναγνώριση κακοήθους συμβάντος, ανάλογα με το βαθμό σοβαρότητάς του. Θα πρέπει επίσης να ελεγχθεί το πώς συμπεριφέρεται σε πραγματικό χρόνο και να διαπιστωθεί ο βαθμός της πιθανής επιβάρυνσης στο συνολικό πληροφοριακό σύστημα.

Φάση 5: Σχεδιασμός και υλοποίηση συνεχούς αξιολόγησης του συστήματος ασφαλείας (Security Auditing). Δεδομένης της δυναμικής του χώρου της πληροφορικής και των νέων αναγκών που καθημερινά προκύπτουν, θα πρέπει να σχεδιαστούν διαδικασίες τακτικής αξιολόγησης της ασφαλείας του συνολικού συστήματος., όπως και οι διαδικασίες βελτίωσης της συνολικής πολιτικής ασφάλειας της επιχείρησης. Οι διαδικασίες αυτές μπορεί να εφαρμόζονται τόσο σε επίπεδο ελέγχου πρόσβασης όσο και σε επίπεδο εφαρμογών.

Φάση 6: Δοκιμές εισβολής. (Penetration Testing). Δεδομένου ότι η εμπειρία των επίδοξων εισβολέων συνεχώς αυξάνεται, είναι θεμιτό να πραγματοποιούνται δοκιμές εισβολής σε ένα σύστημα ασφαλείας. Πολλές εταιρείες πληροφορικής διατηρούν τα λεγόμενα τμήματα «ethical hackers», οι οποίοι προσπαθούν να εισβάλουν στα συστήματα των πελατών τους με μοναδικό σκοπό να σπάσουν την ασφάλεια με όποιο καινούριο μέσο υπάρχει στην αγορά, χωρίς όμως να προκαλέσουν μεγαλύτερη βλάβη (Clarke, Roger, 1996: 24-27).

vi. Ασφάλεια

Η ασφάλεια των συναλλαγών είναι το μεγαλύτερο πρόβλημα των υπευθύνων μηχανογράφησης και των αρμοδίων στελεχών των τραπεζών. Δεν είναι το ίδιο να μπορεί κανείς να έχει πρόσβαση σε μία πιστωτική κάρτα και σε όλους του λογαριασμούς της τράπεζας. Η πιστωτική κάρτα έχει περιορισμένη χρήση μόνο για αγορές και για περιορισμένο πιστωτικό όριο. Αντίθετα η πρόσβαση στο λογαριασμό μπορεί να έχει πολλαπλά αποτελέσματα, καθώς θεωρητικά είναι σε θέση κανείς να εκτελέσει διάφορες συναλλαγές, να πιστώσει και να χρεώσει άλλους λογαριασμούς.

Το αίτημα για μία ασφαλής διαδικασία τραπεζικών συναλλαγών είναι επιτακτικό. Παρακάτω αναφέρονται οι εξής μέθοδοι ασφάλειας όσον αφορά τη διεκπεραίωση των τραπεζικών συναλλαγών μέσω κινητού τηλεφώνου:

1) Ασφάλεια με ψηφιακές υπογραφές (WIM)

Μια καινούργια μέθοδος ασφάλειας είναι οι ψηφιακές υπογραφές (WIM), που προσφέρουν αρκετά μεγάλη ασφάλεια για το m-banking.

Συγκεκριμένα οι ψηφιακές υπογραφές προσφέρουν στους χρήστες την εγγύηση τριών πραγμάτων:

1. Αυθεντικότητα (authenticity), ότι δηλαδή ο αποστολέας εγγράφων είναι όντως αυτός που ισχυρίζεται ότι είναι.
2. Ακεραιότητα (integrity), ότι δηλαδή τα αρχεία που στέλνονται φτάνουν στον παραλήπτη όπως ακριβώς στέλνονται.
3. Εμπιστευτικότητα (confidentiality), ότι δηλαδή το περιεχόμενο των αρχείων δεν θα φανερωθεί σε άλλα άτομα εκτός των αρμοδίων.

Τα τελευταία χρόνια οι μέθοδοι υπογραφών βασίζονται σε συστήματα PKI (public key infrastructure) τα οποία χρησιμοποιούνται για αυτές τις διαδικασίες. Τα συστήματα αυτά βασίζονται στην ύπαρξη ενός ζεύγους κλειδιών, ενός δημοσίου κλειδιού (public key) που είναι αποθηκευμένο στον server της τράπεζας και ένα μυστικό ιδιωτικό κλειδί (secret private key) που είναι μόνιμα αποθηκευμένο στην συσκευή του χρήστη. Ο χρήστης χρησιμοποιεί το ιδιωτικό κλειδί σε συνδυασμό με τον προσωπικό κωδικό ασφαλείας (PIN public key infrastructure) που ο ίδιος έχει ο ίδιος δημιουργήσει, για να πιστοποιήσει την αυθεντικότητα και να εξουσιοδοτήσει οποιεσδήποτε τραπεζικές συναλλαγές (Jossey-Bass, D. Chaffey: 2002).

2) Ασφάλεια με i mode

Το i-mode είναι ένα ιδιόκτητο πρωτόκολλο της ιαπωνικής εταιρίας (NTT DoCoMo) το οποίο παρέχει τις υπηρεσίες του διαδικτύου χρησιμοποιώντας τα χαρακτηριστικά (PDC - Ψηφιακό κυψελοειδή-πακέτο) και ένα υποσύνολο της HTML 3.0. Επιτρέπει εφαρμογές που δίνουν τη δυνατότητα στα κινητά τηλέφωνα να χρησιμοποιούν τεχνολογία java (applets) και επιτρέπει επίσης στους χρήστες να κατεβάσουν αυτές τις εφαρμογές. Χρησιμοποιεί packetwitched τεχνολογία για ασύρματη σύνδεση, ενώ για καλωδιακή σύνδεση η επικοινωνία γίνεται με το πρωτόκολλο TCP/ IP (συστήματα εναλλακτικής μετάδοσης πακέτου πληροφοριών). Τα συστήματα αυτά στέλνουν και λαμβάνουν πληροφορίες με τη διαίρεση των μηνυμάτων σε μικρότερα πακέτα, με την προσθήκη των επιγραφών που περιέχουν τη διεύθυνση και με τον έλεγχο πληροφορίας σε κάθε πακέτο.

Αυτό επιτρέπει να γίνονται πολλαπλάσιες επικοινωνίες σε ένα κοινό κανάλι, ενώ επιτρέπει επίσης την αποδοτική χρήση καναλιών με το χαμηλότερο δυνατό κόστος.

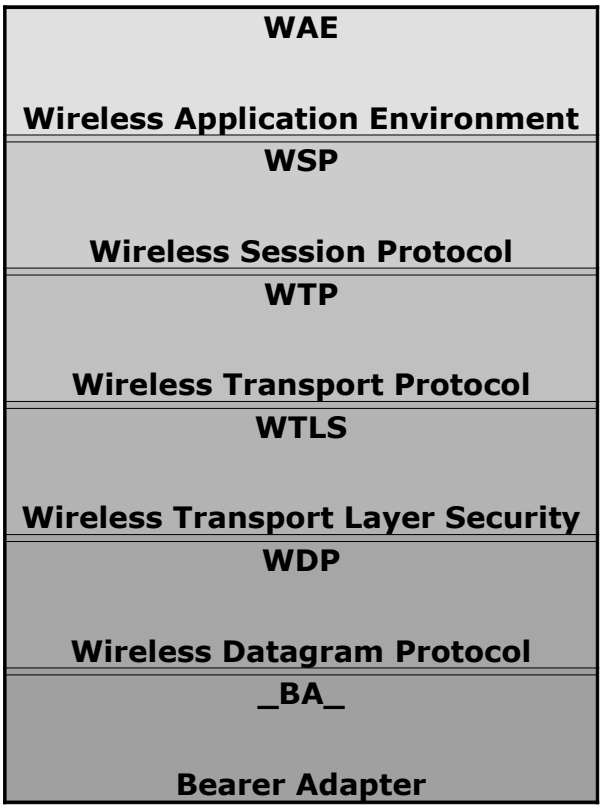
Το πρωτόκολλο i-mode είναι βασισμένο στα άλλα πρωτόκολλα του διαδυκτίου, όπως το HTTP και τα SSL/TLS που χρησιμοποιούν end-to-end μηχανισμούς ασφάλειας. Το i-mode ξεκίνησε να δημιουργείται το Μάρτιο του 2001, τη στιγμή που χαμηλότερων επιπέδων πρωτόκολλα, είχαν ήδη κατασκευαστεί από την (NTT DoCoMo). Η ιαπωνική βιομηχανία βασισμένη σε μια συμβουλευτική εταιρία (Eurotechnology) πήρε πληροφορίες από έναν κατάλογο με συχνά ερωτώμενους (FAQ) για την ασφάλεια στο i-mode. Σε αυτό τον κατάλογο, προσδιορίστηκαν τα πέντε πιο σημαντικά ζητήματα ασφαλείας στο i-mode, με την προϋπόθεση ότι αυτά έπρεπε να αντιμετωπιστούν χωριστά:

1. Ασφάλεια της ράδιο σύνδεσης μεταξύ i-mode μικροτηλεφώνου και του κυψελοειδούς σταθμού της βάσης.
2. Ασφάλεια στη μεταφορά δεδομένων του κοινού διαδυκτίου στη σύνδεση μεταξύ των περιοχών i-mode και μικροτηλεφώνου, στο στρώμα HTML
3. Ασφάλεια των ιδιωτικών δικτύων σε i-mode.
4. Ασφάλεια των ιδιωτικών συνδέσεων δικτύων μεταξύ του κέντρου i-mode και ειδικών υπηρεσιών όπως είναι οι τράπεζες (MOBILE BANKING)
5. Ασφάλεια κωδικού πρόσβασης

Συνεπώς κατορθώθηκε να φτιαχτεί ένα πρωτόκολλο (i-mode) που να παρέχει end-to-end ασφάλεια σε ολόκληρο το κινητό δίκτυο (ασφάλεια μέσα σε ένα κινητό δίκτυο και ασφάλεια στη μεταφορά τοπικών δικτύων). Οι υπηρεσίες ασφαλείας όπως ο προσδιορισμός των χρηστών, η επικύρωση κ.τ.λ μπορούν πλέον να εξασφαλισθούν, άρα να χρησιμοποιηθούν και από τα συναλλασσόμενα μέρη (Ashley, Hinton, Vandenwauver, 2001).

3) Ασφάλεια με WAP

Οι ασύρματοι μεταφορείς είναι γνωστοί για το χαμηλό εύρος ζώνης, την υψηλή λανθάνουσα κατάσταση και την απρόβλεπτη αξιοπιστία τους. Οι ασύρματες συσκευές αντιπροσωπεύουν την περιορισμένη δύναμη επεξεργασίας, τη μνήμη και το απλό ενδιάμεσο με το χρήστη. Όλοι αυτοί οι περιορισμοί εξετάζονται από το WAP, κάνοντας το την καταλληλότερη πλατφόρμα για την υποστήριξη της τηλεφωνίας και των υπηρεσιών πληροφοριών στις φορητές συσκευές. Τα σημαντικότερα μέρη της λίστας πρωτοκόλλου WAP περιγράφονται παρακάτω:



Σχήμα 1 : Τα στρώματα του Πρωτοκόλλου WAP(πηγή HTTP://www.ercim.org/publication/ercim_news/enw41/index.html)

Το στρώμα ασφάλειας στο WAP είναι το WTLS (ασύρματη ασφάλεια στρώματος μεταφορών). Αυτό το πρωτόκολλο είναι βασισμένο στο πρωτόκολλο TLS, το οποίο καθιστά την πιστοποίηση ταυτότητας πελατών εξυπηρετητών πιθανή και εκτελεί τις κρυπτογραφικές διαδικασίες. Επιπλέον, η ασφάλεια επιπέδων εφαρμογής μπορεί να προσεγγιστεί χρησιμοποιώντας το WMLScript (ασύρματο γλωσσικό χειρόγραφο

σήμανσης). Εντούτοις, προκειμένου να εξεταστούν οι περισσότερες από τις απαιτήσεις ασφαλείας των πελατών, μερικές από τις λειτουργίες ασφαλείας πρέπει να εκτελεσθούν σε μια ανθεκτική συσκευή. Για αυτόν το λόγο το WAP χρησιμοποιεί το WIM (ενότητα ταυτότητας WAP), που εφαρμόζεται συνήθως από μια έξυπνη κάρτα, ενδεχομένως μαζί με την (ενότητα ταυτότητας συνδρομητών) κάρτα SIM.

Σύμφωνα με το WAP, όχι μόνο ένας κινητός χρήστης είναι σε θέση να έχει πρόσβαση στις υπηρεσίες, αλλά και η πλευρά κεντρικών υπολογιστών δεν είναι πλέον εντοπισμένη. Στην περίπτωση των εφαρμογών έξυπνων καρτών, μια νέα τεχνολογία στις εφαρμογές είναι η smartX που καθορίζει ένα πλήρες πλαίσιο για την ανάπτυξη έξυπνων καρτών. Με το χωρισμό της διαδικασίας εφαρμογής (η λογική της εφαρμογής) από το πρωτόκολλο εφαρμογής (κάρτα- συγκεκριμένο στρώμα), η smartX καθιστά πιθανή τη γρήγορη και αποδοτική μετανάστευση σε μια νέα έξυπνη κάρτα.

Το smartX στηρίζεται σε SML (γλώσσα σήμανσης smartX στοιχείων και των διαδικασιών εφαρμογής), μια γλώσσα περιγραφής των έξυπνων καρτών και στην τεχνολογία δυνάμεων XML για την παραγωγή των έξυπνων καρτών.

Οι δραστηριότητές μας στο εγγύς μέλλον θα περιλάβουν την περιγραφή των λειτουργιών του mobile banking, δεδομένου ότι το HTML διαδίκτυο κινείται προς την τεχνολογία XML. Η περιγραφή του mobile banking σε XML συμπεριλαμβανομένων των επιχειρηματικών στοιχείων συμπεριφοράς, των συναλλαγών των στοιχείων και των ροών προϊόντων είναι μια νέα προσέγγιση που θα καταστήσει πολύ ευκολότερη την οικοδόμηση της σύνδεσης μεταξύ του περιεχομένου και των καναλιών επικοινωνίας. Με το συνδυασμό της τεχνολογίας WAP και smartX λαμβάνουμε μια πολύ εύκαμπτη, ασφαλή κινητή αρχιτεκτονική που μαζί με το mobile banking, αντιπροσωπευόμενο σε XML, θα παράσχει ένα ασφαλές περιβάλλον επιχειρησιακής επικοινωνίας (Ashley, Hinton, Vandenwauver, 2001).

vii. Πλεονεκτήματα και μειονεκτήματα από την εφαρμογή του m-banking

Οι σημερινές επιχειρήσεις λειτουργούν σε ένα όλο και περισσότερο κινητό περιβάλλον (mobile commerce) όπου όρος ‘’κινητικότητα’’ μπορεί να οριστεί ως η πρόσβαση στο επιχειρηματικό δίκτυο οποτεδήποτε και οπουδήποτε. Η τάση για ένα όλο και περισσότερο κινητό περιβάλλον ,έχει ως συνέπεια την αύξηση του πλήθους των φορητών συσκευών που χρησιμοποιούν συνεργάτες και πελάτες για να αυξήσουν την παραγωγικότητα. Αυτός ο πολλαπλασιασμός των ασύρματων συσκευών παγκοσμίως, παρακινεί τις επιχειρήσεις να επιτύχουν τα οφέλη που απορρέουν από την ελεύθερη μετακίνηση, αλλά ταυτόχρονα να διατηρήσουν τον έλεγχο του επιχειρηματικού δικτύου. Οι κινητές συσκευές (κυρίως κινητά τηλέφωνα) μπορούν να χρησιμοποιηθούν σήμερα για περισσότερους λόγους εκτός από τις κλήσεις. Οι πρόσθετες λειτουργίες όπως η κινητή περιοδεία στο Διαδίκτυο, ATMs για τις τραπεζικές συναλλαγές, κ.τ.λ θα είναι διαθέσιμες για καθημερινή χρήση και οι τράπεζες είναι οι πρώτες υποψήφιες για να χρησιμοποιήσουν αυτούς τους νέους τύπους λειτουργιών εκτενώς. Σήμερα, το κινητό εμπόριο αντιπροσωπεύει με τον καλύτερο τρόπο τις προσπάθειες της σύγκλισης και της παγκοσμιοποίησης. Από μια άποψη πληροφοριών, το μέλλον του mobile banking κινείται στην ίδια κατεύθυνση.

Μέσω της υπηρεσίας mobile banking, οι πελάτες της τράπεζας έχουν τη δυνατότητα να εκτελούν τις προσφιλέστερες τραπεζικές τους συναλλαγές, να αναζητούν καταστήματα και ATM και να ενημερώνονται για χρήσιμα νέα της τράπεζας, μέσω των ιδιαίτερα απλών και φιλικών στη χρήση υπηρεσιών i-mode, από το κινητό τους τηλέφωνο. Το i-mode ,μια υπηρεσία για όλους, ιδιαίτερα απλή και φιλική στη χρήση, αποτελεί το internet της κινητής τηλεφωνίας καθώς μεταφέρει πιο εύκολα και γρήγορα από ποτέ τη φιλοσοφία του Διαδικτύου στο κινητό τηλέφωνο. Με λίγα λόγια το i-mode προσφέρει ευκολία και απλότητα στη χρήση, υψηλές ταχύτητες, αξιοπιστία, εξαιρετικά διευρυμένο φάσμα υπηρεσιών και περιεχομένου, νέες εξελιγμένες και ελκυστικές συσκευές αλλά και προηγμένο και απλό στη χρήση e-mail. Φυσικά υπάρχουν και άλλα πρωτόκολλα έχει καθοριστεί για τον ασύρματο κόσμο, αποκαλούμενο WAP (ασύρματο πρωτόκολλο εφαρμογής), το οποίο κάνει αξιόπιστη και γρήγορη την πρόσβαση των στοιχείων και των πιθανών υπηρεσιών(Frank, 2001).

Το mobile banking είναι το λιγότερο διαδεδομένο κανάλι ηλεκτρονικής τραπεζικής, κυρίως διότι η τεχνολογία που χρησιμοποιείται δεν καλύπτει τις αυξημένες απαιτήσεις ταχύτητας και ασφάλειας. Αρκετές είναι οι ελληνικές τράπεζες που έχουν αρχίσει να παρέχουν υπηρεσίες mobile banking τόσο με ανταλλαγή γραπτών μηνυμάτων όσο και μέσω WAP. Ο πελάτης της τράπεζας χρησιμοποιώντας το κινητό του τηλέφωνο και τους προσωπικούς κωδικούς χρήσης των υπηρεσιών, μπορεί, από οπουδήποτε και αν βρίσκεται να παρακολουθεί τις κινήσεις των λογαριασμών του, να ενημερώνεται για τα υπόλοιπα τους και να πραγματοποιεί , μεταξύ των λογαριασμών του, μεταφορές ποσών. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι υπηρεσίες ειδοποίησης του πελάτη με γραπτό μήνυμα για διάφορα τραπεζικά θέματα (π.χ. αυξομείωση υπολοίπου λογαριασμού, εκτέλεση χρηματιστηριακών εντολών). Η εξέλιξη της τεχνολογίας στους τομείς της κινητής τηλεφωνίας και των πληρωμών μέσω κινητών τηλεφώνων αναμένεται να δώσει μεγάλη ώθηση στις υπηρεσίες mobile banking τα επόμενα χρόνια. Επίσης πολλές είναι οι –προς το παρόν- προσπάθειες, ώστε το κινητό τηλέφωνο να υποκαταστήσει την πιστωτική- χρεωστική κάρτα για τις πληρωμές στο φυσικό κόσμο. Αυτές οι προσπάθειες συνίσταται στην άμεση επικοινωνία του κινητού τηλεφώνου με το τερματικό POS (π.χ μέσω υπέρυθρων ακτινών ή με το πρωτόκολλο Bluetooth). Στη συνέχεια ο κάτοχος του τηλεφώνου επικοινωνεί απευθείας με την τράπεζά του και επιβεβαιώνει τη συναλλαγή. Η επικοινωνία γίνεται είτε με φωνή (ο πελάτης δέχεται κλήση στο κινητό του από το τηλεφωνικό κέντρο της τράπεζας και εισάγει τον κωδικό του στο σύστημα IVR) είτε με γραπτό μήνυμα (ο πελάτης στέλνει τον κωδικό του στο κέντρο SMS της τράπεζας). (www.m-comm.internet.com).

Οι εξελίξεις στην κινητή τηλεφωνία, όσον αφορά το περιεχόμενο, μοιάζουν να ακολουθούν την πορεία που έχει χαράξει το Internet. Υπάρχουν όμως ουσιώδεις διαφορές που πηγάζουν από τη φύση του μέσου, τις ισορροπίες των φορέων- εταιριών που συμμετέχουν και τις προσδοκίες των χρηστών. Η περίοδος που διανύουμε είναι μεταβατική και θα διαμορφώσει τον τρόπο με τον οποίο το περιεχόμενο θα φτάσει στο κινητό των χρηστών. Αντίστοιχα το ηλεκτρονικό εμπόριο μέσω κινητών τηλεφώνων αποτελεί την

επέκταση της σχέσης του Internet με το ηλεκτρονικό εμπόριο, πέρα από τον ηλεκτρονικό υπολογιστή και την τηλεόραση.

ΚΕΦΑΛΑΙΟ IV: Κίνδυνοι και ασφάλεια από τη χρήση της υπηρεσίας m-banking

Στο κεφάλαιο αυτό θα αναφερθούμε αναλυτικά στους κινδύνους που διατρέχουν οι τραπεζικές συναλλαγές μέσω internet. Θα ορίσουμε την έννοια του ηλεκτρονικού εγκλήματος, θα δούμε μορφές απειλών και νέες ορολογίες, όπως το spoofing και το phising. Τέλος θα δούμε τους τρόπους αντιμετώπισης των κινδύνων αυτών και τί συμβουλεύουν οι τράπεζες τους πελάτες τους, όσον αφορά τα μέτρα ασφαλείας.

i. Ηλεκτρονικό έγκλημα και δικτυακές απάτες

Ο όρος ηλεκτρονικό έγκλημα ή ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. Ηλεκτρονικό έγκλημα αποτελούν πράξεις όπως η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά (Ταβλαρίδης, 2000).

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο, οι συχνότητα τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on-line υπηρεσίες. Η αύξηση είναι τεράστια και αποτελεί ένα ανησυχητικό φαινόμενο, αφού πολλοί θεωρούν τις οικονομικές πληροφορίες που τους αφορούν άκρως απόρρητες και διατηρούν μια επιφυλακτική στάση απέναντι σε διαδικασίες που τις καθιστούν ευάλωτες στο ευρύ κοινό, όπως είναι το m-banking.

Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους να επιτύχουν τους σκοπούς τους. Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για on-line banking, οι μεγαλύτεροι κίνδυνοι προέρχονται από τον ανθρώπινο παράγοντα. Στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς έχουν την εκούσια ή ακούσια βοήθεια και κάποιου που εργάζεται στην τράπεζα. Και χωρίς την βοήθεια εκ των έσω, οι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το κινητό τους τηλέφωνο, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι άνθρωποι αυτοί αποτελούν τους

πιο προκλητικούς στόχους, μια και δεν έχουν συνείδηση του μεγέθους της ζημιάς που μπορούν να κάνουν ανοίγοντας απλά μια επισύναψη στο ηλεκτρονικό τους ταχυδρομείο ή ακολουθώντας ένα link. Οι απλοί χρήστες πέφτουν πολύ εύκολα θύματα προγραμμάτων που υποτίθεται ότι κάνουν κάτι χρήσιμο για αυτούς, αλλά στη πραγματικότητα επιτρέπουν την πρόσβαση σε hackers.

Οι κλεμμένες πληροφορίες αποτελούν την πρώτη φάση μιας αρκετά επίμονης διαδικασίας, η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες, έτσι ώστε ο hacker να υποδυθεί κάποιον άλλον στο διαδίκτυο. Η διαδικασία αυτή διευκολύνεται συνεχώς με καινούργια προγράμματα που κυκλοφορούν στην αγορά.

Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως, αλλά σε μια από τις εταιρείες που συνεργάζονται με αυτήν προκειμένου να διαχειριστούν τις πληρωμές των λογαριασμών και τις συναλλαγές με τους πελάτες της. Σε πολλές περιπτώσεις οι τράπεζες επιτρέπουν στις εταιρείες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτήν την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρείες επεξεργάζονται τις πληρωμές και μεταφέρουν τα χρήματα. Μόλις βρεθεί μια αδυναμία κάνουν την κίνησή τους.

Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες, χρησιμοποιώντας ευάλωτα σε εισβολείς συστήματα.

Η ταχεία εξάπλωση των επιθέσεων τύπου phishing αποτελεί μια ιδιαίτερη σοβαρή απειλή για τράπεζες και χρηματοοικονομικούς οργανισμούς (Κατσουλάκος, 2001:201).

Τι είναι το phishing;

Το phishing είναι ένας τύπος εξαπάτησης που έχει σχεδιαστεί για την υποκλοπή στοιχείων της ταυτότητάς του πελάτη. Σε μια περίπτωση απάτης phishing, κάποιο κακόβουλο άτομο παροτρύνει τον πελάτη να δώσει

πληροφορίες, όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης, στοιχεία λογαριασμών ή άλλα προσωπικά στοιχεία, πείθοντάς τον με ψεύτικα προσχήματα. Οι απάτες phishing φτάνουν στον πελάτη συνήθως μέσω ανεπιθύμητης αλληλογραφίας ή αναδυόμενων παραθύρων (www.panelliniabank.gr).

Πώς λειτουργεί το phishing;

Ο κακόβουλος χρήστης στέλνει εκατομμύρια πλαστά μηνύματα που εμφανίζονται σαν να προέρχονται από γνωστές διαδικτυακές τοποθεσίες ή από τοποθεσίες εμπιστοσύνης, όπως της τράπεζας ή του οργανισμού της πιστωτικής κάρτας. Τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι διαδικτυακές τοποθεσίες στις οποίες παραπέμπουν, μοιάζουν αρκετά επίσημα και εξαπατούν πολύ κόσμο στο να πιστέψει ότι είναι νόμιμα. Πιστεύοντας ότι τα μηνύματα αυτά είναι νόμιμα, οι ανυποψίαστοι χρήστες απαντούν συχνά στο αίτημα των ηλεκτρονικών μηνυμάτων για τους αριθμούς των πιστωτικών καρτών, τους κωδικούς πρόσβασης, τις πληροφορίες του λογαριασμού ή άλλα προσωπικά δεδομένα. Για να κάνει αυτά τα μηνύματα ακόμη πιο πιστευτά, ο εισβολέας ίσως τοποθετήσει μέσα στο πλαστό μήνυμα έναν σύνδεσμο προς κάποια νόμιμη διαδικτυακή τοποθεσία, αλλά στην πραγματικότητα οδηγεί τον πελάτη σε μια ψεύτικη τοποθεσία ή σε κάποιο αναδυόμενο παράθυρο που είναι ακριβώς ίδιο με την επίσημη τοποθεσία. Αυτά τα αντίγραφα ονομάζονται «πλαστές διαδικτυακές τοποθεσίες». Μόλις βρεθεί κανείς σε κάποια από αυτές τις πλαστές διαδικτυακές τοποθεσίες, ίσως ξεγελαστεί και εισάγει περισσότερα προσωπικά δεδομένα, τα οποία θα μεταδοθούν άμεσα στο άτομο που δημιούργησε την τοποθεσία και ο οποίος μπορεί έπειτα να χρησιμοποιήσει τα δεδομένα αυτά για αγορές, για μια αίτηση νέας πιστωτικής κάρτας, ή για την κλοπή της ταυτότητάς σας (www.panelliniabank.gr).

Προστασία από το phishing

Όπως συμβαίνει και στον πραγματικό κόσμο, οι «επαγγελματίες» απατεώνες θα συνεχίσουν να αναπτύσσουν ακόμη πιο δόλιους τρόπους για να ξεγελάσουν τους χρήστες στο διαδίκτυο.

Ακολουθώντας όμως αυτά τα πέντε εύκολα βήματα θα μπορέσει κάποιος να προστατεύσει τον εαυτό του και τα δεδομένα του.

Βήμα 1: Ποτέ δεν πρέπει να απαντά σε αιτήσεις προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου.

Οι τράπεζες και όλες οι νόμιμες επιχειρήσεις δεν θα ζητήσουν ποτέ με μήνυμα ηλεκτρονικού ταχυδρομείου κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή άλλα προσωπικά δεδομένα. Εάν λάβει ο πελάτης κάποιο μήνυμα που ζητά τέτοιου είδους πληροφορίες, δεν πρέπει να απαντήσει. Εάν θεωρεί πως το μήνυμα είναι νόμιμο, επικοινωνεί τηλεφωνικά με την εταιρεία ή μέσω της διαδικτυακής τοποθεσίας για να επιβεβαιώσει το αίτημα. Μπορεί να ανατρέξει στο βήμα 2 για τους καλύτερους τρόπους μετάβασης σε μια διαδικτυακή τοποθεσία, εάν πιστεύει πως έχει πέσει θύμα πλαστού μηνύματος.

Βήμα 2: Επίσκεψη σε διαδικτυακές τοποθεσίες πληκτρολογώντας την διεύθυνση URL στη γραμμή διεύθυνσης. Εάν πιστεύει πως κάποιο ηλεκτρονικό μήνυμα από την εταιρεία της πιστωτικής του κάρτας, από την τράπεζα, από την ηλεκτρονική υπηρεσία πληρωμών ή από κάποια άλλη διαδικτυακή τοποθεσία με την οποία συνεργάζεται δεν είναι νόμιμο, να μην χρησιμοποιεί τους συνδέσμους προς τη διαδικτυακή τοποθεσία που υπάρχουν στο μήνυμα ηλεκτρονικού ταχυδρομείου. Ο σύνδεσμος αυτός ενδεχομένως να οδηγήσει σε κάποια πλαστή τοποθεσία που πιθανόν να στείλει όλες τις πληροφορίες που θα εισάγει στον δημιουργό αυτής της τοποθεσίας.

Ακόμη και στην περίπτωση που στη γραμμή διεύθυνσης εμφανίζεται η σωστή διεύθυνση, οι hackers έχουν πολλούς τρόπους στη διάθεσή τους για να εμφανίσουν μια ψεύτικη διεύθυνση URL στη γραμμή διεύθυνσης του προγράμματος περιήγησης. Οι νεότερες εκδόσεις του Internet Explorer καθιστούν την πλαστογράφηση της γραμμής διεύθυνσης ακόμη πιο δύσκολη, έτσι καλό θα ήταν να επισκέπτεται ο πελάτης την τοποθεσία Windows Update τακτικά και να ενημερώνει το λογισμικό του. Εάν πιστεύει πως δεν πρόκειται να το θυμάται ή επιθυμεί οι εγκαταστάσεις

ενημερωμένων εκδόσεων να γίνονται χωρίς την δική του μεσολάβηση, ίσως να μπορεί να ρυθμίζει τον υπολογιστή του για αυτόματη ενημέρωση.

Βήμα 3: Εξακρίβωση ότι η διαδικτυακή τοποθεσία χρησιμοποιεί κρυπτογράφηση. Εάν δεν μπορεί να εμπιστευθεί κάποια διαδικτυακή τοποθεσία από το περιεχόμενο της γραμμής διεύθυνσης, πώς μπορεί να ξέρει ότι είναι ασφαλής; Υπάρχουν μερικοί τρόποι. Πρώτον, προτού εισάγει τυχόν προσωπικά δεδομένα, να βεβαιωθεί ότι η διαδικτυακή τοποθεσία χρησιμοποιεί κρυπτογράφηση για την αποστολή των προσωπικών του δεδομένων. Στον Internet Explorer υποδεικνύεται με την εμφάνιση ενός εικονιδίου κίτρινου λουκέτου στη γραμμή κατάστασης. Το σύμβολο αυτό υποδεικνύει ότι η τοποθεσία χρησιμοποιεί κρυπτογράφηση για την προστασία ευαίσθητων προσωπικών δεδομένων, όπως αριθμοί πιστωτικών καρτών, αριθμός λογαριασμού, στοιχεία πληρωμής, που εισάγει κανείς.

Βήμα 4: Τακτικός έλεγχος της πιστωτικής κάρτας και του τραπεζικού λογαριασμού. Ακόμη κι αν ακολουθήσει τα τρία βήματα παραπάνω, ίσως και πάλι να πέσει θύμα κλοπής ταυτότητας. Εάν ελέγχει τον τραπεζικό λογαριασμό και το λογαριασμό της πιστωτικής κάρτας τουλάχιστον κάθε μήνα, μπορεί να εντοπίσει κάποιον απατεώνα και να τον εμποδίσει να προκαλέσει σημαντική ζημιά.

Βήμα 5: Καταγγελία για ύποπτες καταχρήσεις των προσωπικών του δεδομένων στις κατάλληλες αρχές (www.panelliniabank.gr)**.**

ii. Ασφαλείς Τραπεζικές Συναλλαγές μέσω κινητού τηλεφώνου

Η ασφάλεια και το απόρρητο των τραπεζιών συναλλαγών μέσω κινητού τηλεφώνου (όπως άλλωστε και των συναλλαγών που εκτελούνται με τις παραδοσιακές μεθόδους) είναι εξαιρετικής σημασίας για τις τράπεζες. Οι τράπεζες έχουν λάβει όλες τις απαραίτητες προφυλάξεις και χρησιμοποιούν τις πιο σύγχρονες και αυστηρές μεθόδους ασφάλειας τόσο από άποψη τεχνολογιών, όσο και διαδικασιών και οργάνωσης. Επιπλέον δεσμεύονται το απόρρητο όλων των προσωπικών πληροφοριών από τη χρήση της υπηρεσίας m-banking.

Οι περισσότερες τράπεζες ακολουθούν το πρωτόκολλο SET (Secure Electronic Transaction), που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς, τη MasterCard και τη Visa, καθώς και από εταιρίες όπως η IBM, η Microsoft και η Netscape. Η ασφαλής διαδικασία των συναλλαγών είναι αρκετά πολύπλοκο θέμα και προϋποθέτει την ύπαρξη ασφαλών γραμμών, ψηφιακών πιστοποιητικών και πιστοποιημένων διακομιστών. Το πρωτόκολλο SET βασίζεται στην κρυπτογραφία, μια μέθοδος που χρησιμοποιείται εδώ και πολλά χρόνια για να προστατεύσει τη μετάδοση ευαίσθητων πληροφοριών από τη μια τοποθεσία στην άλλη. Σε ένα κρυπτογραφικό σύστημα οι πληροφορίες μεταδίδονται σε μορφή μηνυμάτων τα οποία κωδικοποιούνται χρησιμοποιώντας ένα κλειδί. Το κωδικοποιημένο μήνυμα μεταφέρεται στον παραλήπτη όπου αποκρυπτογραφείται, χρησιμοποιώντας ένα αντίστοιχο κλειδί, για να εμφανιστεί η αρχική του μορφή.

Δύο είναι οι κύριες μέθοδοι κρυπτογράφησης: η συμμετρική και η ασύμμετρη. Στη συμμετρική, η κρυπτογράφηση υλοποιείται με τη χρήση του ίδιου "κλειδιού", τόσο στην κωδικοποίηση όσο και στην αποκωδικοποίηση. Πράγμα το οποίο σημαίνει ότι ο αποστολέας και ο παραλήπτης του μηνύματος μοιράζονται το ίδιο κλειδί. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Ένας από τους πιο γνωστούς αλγόριθμους που χρησιμοποιούν αυτή τη μέθοδο είναι το DES (Data Description Standard), που χρησιμοποιείται από τραπεζικούς οργανισμούς για τη δημιουργία των αριθμών PIN.

Η ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο κλειδιά: το ένα (κοινό κλειδί) για να κωδικοποιήσει το μήνυμα και ένα άλλο (ιδιωτικό κλειδί) για να το αποκωδικοποιήσει. Ένα μήνυμα που θα κωδικοποιηθεί με το ένα κλειδί θα μπορέσει να αποκωδικοποιηθεί μόνο με το άλλο. Τα δύο κλειδιά έχουν μαθηματική σχέση μεταξύ τους, έτσι ώστε ένα μήνυμα που θα κωδικοποιηθεί με το ένα κλειδί θα μπορέσει να αποκωδικοποιηθεί μόνο με το άλλο. Ο παροχέας περιεχομένου, στην προκειμένη περίπτωση η

τράπεζα, μπορεί να διανείμει το κοινό κλειδί, κρατώντας το ιδιωτικό κλειδί για την αποκωδικοποίηση. Για να εξασφαλιστεί η σιγουριά στη μέθοδο κρυπτογράφησης, η τράπεζα έχει την ευθύνη να δημιουργήσει και να αποθηκεύσει τα δύο ζευγάρια κλειδιών. Ένας από τους πιο γνωστούς αλγορίθμους που χρησιμοποιούν αυτή τη μέθοδο είναι ο RSA.

Όσον αφορά στις τραπεζικές συναλλαγές, κάθε τράπεζα ακολουθεί τη δική της λύση, όπως είναι οι αριθμοί PIN, τα ψηφιακά πιστοποιητικά και οι αριθμοί TAN, που ακολουθούν κάθε συναλλαγή.

Υπάρχουν αρκετές εταιρίες που μπορεί να χρησιμοποιήσει ένας οργανισμός για να πετύχει ασφαλή πρόσβαση. Μία από αυτές είναι η VeriSign, το λογισμικό της οποίας χρησιμοποιείται στις τραπεζικές όσο και σε άλλου τύπου διαδικτυακές συναλλαγές.

Η πιστοποίηση της ταυτότητας του χρήστη και κάθε συναλλαγή του εξασφαλίζονται με τη βοήθεια ενός μοναδικού ψηφιακού πιστοποιητικού (digital certificate). Αυτό το πιστοποιητικό αναγνωρίζει τον υπολογιστή του χρήστη και επιτρέπει τις συναλλαγές και τις μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο υπολογιστή. Τα πιστοποιητικά αυτά εξασφαλίζονται εγκαθιστώντας ένα πρόγραμμα από την αντίστοιχη εταιρία πιστοποίησης.(www.lawnet.gr).

iii. Κανόνες για ασφαλείς τραπεζικές συναλλαγές

Η ασφάλεια των τραπεζικών συναλλαγών μέσω κινητού τηλεφώνου πρέπει να εξασφαλίζεται από τις τράπεζες που παρέχουν αυτήν την υπηρεσία(m-banking). Από τη μεριά τους οι πελάτες καλό θα ήταν να εφιστήσουν την προσοχή τους σε μερικούς κανόνες ασφαλείας, οι οποίοι θα βοηθήσουν στην ασφάλεια των προσωπικών τους συναλλαγών, καθιστώντας τους λιγότερο ευάλωτους σε κινδύνους που συνοδεύουν μια τραπεζική συναλλαγή μέσω κινητού τηλεφώνου και κατ' επέκταση μέσω internet.

Παρακάτω αναφέρονται κάποιοι κανόνες ασφαλείας των τραπεζικών συναλλαγών που προτείνουν, η ένωση των γερμανικών τραπεζών αλλά και η αντίστοιχη ένωση των ελληνικών τραπεζών και απευθύνονται στους πελάτες.

1) Ένωση Γερμανικών Τραπεζών

Η Ένωση Γερμανικών Τραπεζών προτείνει 10 κανόνες που περιγράφονται στη συνέχεια, οι οποίοι μπορούν να ενισχύσουν σημαντικά την ασφάλεια του κινητού που χρησιμοποιείται για τραπεζικές συναλλαγές στο διαδίκτυο και έτσι να περιοριστούν οι κίνδυνοι στο ελάχιστο.

Κανόνας 1ος: Προστατεύστε τα ευαίσθητα δεδομένα που στέλνετε μέσω ανοικτών δικτύων.

Κάθε μη ασφαλής μεταβίβαση δεδομένων μέσω του διαδικτύου μπορεί να υποκλαπεί από μη εξουσιοδοτημένα τρίτα πρόσωπα ή να προβληθεί στα συστήματά τους. Συνεπώς δεν θα πρέπει ποτέ να στέλνετε ευαίσθητα δεδομένα μέσω ανοικτών δικτύων, εκτός αν είναι κρυπτογραφημένα. Προστατεύετε την εμπιστευτική σας αλληλογραφία χρησιμοποιώντας ασφαλείς μεθόδους κρυπτογράφησης.

Οι τράπεζες έχουν λάβει μέτρα για να διασφαλίσουν πως όσα δεδομένα αποστέλλονται κατά τη διενέργεια τραπεζικών συναλλαγών στο διαδύκτιο, μεταβιβάζονται με τη χρήση ασφαλούς τεχνολογίας κρυπτογράφησης. Εισάγεται το PIN και τον μοναδικό κωδικό μιας χρήσης μόνο αν βρίσκεστε στις ασφαλείς σελίδες της τράπεζάς σας και η σύνδεση είναι κρυπτογραφημένη. Μία μέθοδος επαλήθευσης είναι να ελέγξετε ότι το URL της τράπεζάς σας ξεκινά με το πρόθεμα <**https://**>.

Τι σημαίνει το URL

Πρόκειται για τα αρχικά των λέξεων Uniform Resource Locator και είναι η τεχνική ορολογία για την ηλεκτρονική διεύθυνση μιας εταιρείας ή ενός προσώπου στο διαδύκτιο.

Μην ξεχνάτε πως όσα δεδομένα μεταβιβάζονται κατά τη διάρκεια τραπεζικών συναλλαγών στο διαδύκτιο δεν κρυπτογραφούνται αυτομάτως όταν αποθηκεύονται στον υπολογιστή σας, άρα θα πρέπει να προστατεύονται από πρόσθετα μέτρα ασφάλειας.

Κανόνας 2ος: Βεβαιωθείτε με ποιόν έχετε να κάνετε.

Στο διαδίκτυο δεν δηλώνουν όλοι την πραγματική τους ταυτότητα. Είναι σχετικά εύκολο για έναν ειδικό να πλαστογραφήσει μια διεύθυνση e-mail ή ακόμα να παραχαράξει ολόκληρη ιστοσελίδα, ενδεχομένως την ιστοσελίδα κάποιας τράπεζας που θέλετε να επισκεφθείτε.

Ελέγξτε το URL στη γραμμή διευθύνσεων του προγράμματος πλοήγησης και βεβαιωθείτε ότι η διεύθυνση της τράπεζας σας στο διαδίκτυο είναι σωστά γραμμένη. Η παραμικρή παρέκκλιση μπορεί να αποτελεί ένδειξη ότι η ιστοσελίδα είναι ψεύτικη.

Ελέγξτε επίσης τις πληροφορίες ασφαλείας που παρέχει το σύστημα πλοήγησης, όπως τα αποτελέσματα επαλήθευσης πιστοποιητικού. Μεταξύ άλλων, έτσι είναι δυνατή η εξακρίβωση από μια ανεξάρτητη αρχή των διαπιστευτηρίων του διακομιστή με τον οποίο συνδέεστε.

Είναι απαραίτητο η ιστοσελίδα στην οποία καταχωρείτε τους προσωπικούς σας κωδικούς εισόδου να είναι πιστοποιημένη από ένα ανεξάρτητο παροχέα πιστοποίησης (Trusted Third Party). Αυτό μπορεί εύκολα να αναγνωριστεί από την εμφάνιση ενός μικρού εικονιδίου με μορφή λουκέτου στο κάτω μέρος των σελίδων m-banking, μέσω του οποίου μπορείτε να επιβεβαιώσετε ότι βρίσκεστε στο σωστό προορισμό.

Δεν θα πρέπει να εμπιστευτείτε κάποια διεύθυνση, αν ο φερόμενος ως κάτοχός της είναι και εκδότης του πιστοποιητικού. Αν έχετε αμφιβολίες μπορείτε να λάβετε από την τράπεζα σας πληροφορίες σχετικά με αξιόπιστες αρχές πιστοποίησης.

Μην γνωστοποιείτε προσωπικά δεδομένα αν δεν είστε βέβαιοι ποιος τα λαμβάνει και ποια θα είναι η τύχη τους. Να είστε καχύποπτοι απέναντι σε κάθε παρέκκλιση από τα συνηθισμένα, όπως λόγου χάρη αιτήματα να εισάγετε το PIN σας σε κάποια στιγμή που δεν το περιμένετε.

Κανόνας 3ος: Προσοχή με ευαίσθητα δεδομένα και μέσα πρόσβασης

Προστατέψτε τους κωδικούς και τα μέσα πρόσβασής σας (PIN, μοναδικούς κωδικούς μιας χρήσης ή έξυπνες κάρτες) από κάθε μη εξουσιοδοτημένη χρήση. Ποτέ μην αποθηκεύετε ευαίσθητα δεδομένα (κωδικούς πρόσβασης,

PIN, μοναδικούς κωδικούς μιας χρήσης και αριθμούς πιστωτικών καρτών) στη μνήμη του κινητού σας.

Επιπλέον, μπορεί κάποια ειδικά προγράμματα που έχουν κατορθώσει τρίτοι να παρεισφρήσουν στο κινητό σας τηλέφωνο, να είναι σε θέση να υποκλέψουν τα δεδομένα σας και να τα μεταβιβάσουν, λόγω χάρη, μέσω e-mail. Αν χρησιμοποιείται εξοπλισμό ασφαλείας, όπως κατασκευή ανάγνωσης «έξυπνων» καρτών με πληκτρολόγιο εισαγωγής PIN, βεβαιωθείτε ότι εισάγεται τους μυστικούς κωδικούς μόνο όταν σας το ζητά η συσκευή.

Το πιο σημαντικό είναι να μην αποθηκεύεται τον κωδικό σύνδεσής σας με το διαδίκτυο. Έτσι θα είναι πιο εύκολο να προστατευθείτε από ανεπιθύμητες συνδέσεις.

Κανόνας 4ος: Επιλέξτε ασφαλή κωδικό πρόσβασης

Αν θέλετε να χρησιμοποιείτε το κινητό σας τηλέφωνο για να ξεκινήσετε μια εφαρμογή όπως το on-line banking, συνήθως αρχίζετε με την εισαγωγή ενός κωδικού πρόσβασης. Πρόκειται για ένα προσωπικό εμπιστευτικό στοιχείο, το οποίο βοηθά να αποδείξετε την ταυτότητά σας και δείχνει ότι είστε εξουσιοδοτημένοι να εργαστείτε σε ένα συγκεκριμένο κινητό τηλέφωνο ή σε μια συγκεκριμένη εφαρμογή. Συνεπώς, είναι ζήτημα ζωτικής σημασίας να μην αποκαλύπτετε σε κανέναν το συγκεκριμένο αυτό στοιχείο. Επίσης δεν πρέπει να γράφετε πουθενά τον κωδικό πρόσβασης, ο οποίος θα πρέπει να είναι μοναδικός και να μαντεύεται δύσκολα.

Ο καλός κωδικό πρόσβασης περιλαμβάνει από 6 ως 8 χαρακτήρες και ένα συνδυασμό πεζών και κεφαλαίων γραμμάτων, αριθμών και ειδικών συμβόλων. Καλό θα ήταν να αποφεύγονται κύρια ονόματα, γνωστοί όροι της καθομιλουμένης, επαναλήψεις ενός χαρακτήρα (π.χ. ΑΑΑ-ΑΑΑ) ή ακολουθίες γραμμάτων του πληκτρολογίου (π.χ. qwerty). Υπάρχουν διάφορες μέθοδοι επιλογής κωδικών πρόσβασης που δύσκολα μαντεύονται: μια απλή μέθοδος είναι να φτιάξετε ένα κωδικό από τα πρώτα γράμματα ενός γνωμικού ή ποιήματος. Η προσθήκη ειδικών συμβόλων ή αριθμών μπορεί να περιπλέξει ακόμα περισσότερο τα πράγματα. Αλλάξτε τον

κωδικό πρόσβασης αν υποψιάζεστε ότι κάποιος μπορεί να τον έχει ανακαλύψει.

Κανόνας 5ος: Χρησιμοποιείτε προγράμματα μόνο από αξιόπιστες πηγές

Μην κατεβάζετε στη μνήμη του κινητού σας τηλεφώνου προγράμματα από το διαδύκτιο, εκτός αν είστε βέβαιοι ότι η πηγή είναι αξιόπιστη. Εξακριβώστε την ταυτότητα του προμηθευτή. Με τη φόρτωση προγραμμάτων ή το άνοιγμα συνημμένων αρχείων e-mail μπορούν να εισχωρήσουν στο κινητό σας τηλέφωνο ιοί ή Trojan. Μην ανοίγετε συνημμένα αρχεία αν δεν γνωρίζετε τον αποστολέα τους ή το περιεχόμενό τους.

Κανόνος 6ος: Χρησιμοποιήστε ενημερωμένες εκδόσεις προγραμμάτων

Να χρησιμοποιείτε μόνο την ενημερωμένη έκδοση του προγράμματος πλοήγησης διαδυκτίου. Μόνο οι πιο πρόσφατες εκδοχές δημοφιλούς διαδικτυακού λογισμικού εγγυώνται την εξάλειψη κάθε γνωστής διαρροής ασφαλείας.

Οι παραγωγοί λογισμικού αναπτύσσουν, επίσης μικρά προγράμματα γνωστά ως διορθώσεις σφαλμάτων (bug fixes) ή διορθωτικές εκδόσεις (patches), για την επίλυση προβλημάτων ασφαλείας που έχουν ανακαλύψει. Πρέπει να εγκαταστήσετε το συντομότερο δυνατό αυτές τις διορθώσεις ασφαλείας ή διορθωτικές εκδόσεις για να προστατεύσετε το κινητό σας τηλέφωνο από γνωστές αδυναμίες ασφαλείας. Μείνετε συντονισμένοι με τις πιο πρόσφατες εξελίξεις: οι περισσότεροι κατασκευαστές και οι τράπεζες διατηρούν για το σκοπό αυτό υπηρεσίες ενημέρωσης.

Κανόνας 7ος: Εκτελέστε έλεγχο ασφαλείας στο κινητό σας τηλέφωνο

Πριν χρησιμοποιήσετε το κινητό σας τηλέφωνο για τραπεζικές συναλλαγές στο διαδύκτιο, αφιερώστε μερικά λεπτά για να εκτελέσετε έναν προσωπικό έλεγχο ασφαλείας. Ενεργοποιείστε τα χαρακτηριστικά ασφαλείας που

προστατεύουν το κινητό σας τηλέφωνο από μη εξουσιοδοτημένη πρόσβαση. Σε αυτά περιλαμβάνονται, λόγου χάρη, ο κωδικός πρόσβασης (PIN) κατά το άνοιγμα του κινητού σας τηλεφώνου.

Να έχετε κατά νου ότι εάν δεν είστε ο μοναδικός χρήστης ενός υπολογιστή, όπως, λόγου χάρη, συμβαίνει στα internet cafe, δεν μπορείτε ποτέ να γνωρίζετε ακριβώς τι είδους προγράμματα εκτελούνται. Είναι δυνατόν ακόμα και να έχει γίνει παρέμβαση στο πληκτρολόγιο. Σε ένα τέτοιο περιβάλλον είναι αδύνατον να περιμένει ότι η ασφάλεια θα είναι απόλυτη. Αν είστε υποχρεωμένος να χρησιμοποιήσετε κάποιο internet cafe για τη διενέργεια τραπεζικών συναλλαγών στο διαδύκτιο, να καθαρίζετε πάντα στη συνέχεια την προσωπική μνήμη (cache) του προγράμματος πλοήγησης, έτσι ώστε οι επόμενοι χρήστες να μην μπορούν να ανακαλέσουν σελίδες που επισκεφθήκατε και να δουν κωδικούς πρόσβασης που έχετε τυχόν εισάγει.

Κανόνας 8ος: Ενεργοποιήστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησης

Ενεργοποιήστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησής σας στο διαδύκτιο. Μπορείτε να ενισχύσετε σημαντικά την ασφάλειά σας στο διαδύκτιο με την έξυπνη χρήση των επιλογών ασφαλείας του προγράμματος πλοήγησής σας και μόνο. Πρέπει οπωσδήποτε να μπλοκάρετε τα Active Controls και να επιτρέπει την εκτέλεση προγραμμάτων Java Applet μόνο κατόπιν επιβεβαίωσης. Πρόκειται για μικρά, ανεξάρτητα προγράμματα ενεργού περιεχομένου, τα οποία εκτελούνται στο κινητό σας τηλέφωνο και μπορούν σε συγκεκριμένες περιπτώσεις να ενεργοποιήσουν ανεπιθύμητες λειτουργίες (όπως την αποστολή του κωδικού πρόσβασής σας σε κάποιον τρίτο, μέσω e-mail).

Μη χρησιμοποιείτε τη λειτουργία αυτόματης καταχώρησης του προγράμματος πλοήγησης, η οποία αποθηκεύει τα ονόματα χρήστη και τους κωδικούς πρόσβασης που εισάγετε και προτείνει αντιστοιχίσεις.

Κανόνας 9ος : Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο λογισμικό ασφαλείας

Ένα σημαντικό πρόσθετο εργαλείο είναι κάθε αποδοτικό πρόγραμμα ανίχνευσης ιών, το οποίο ενημερώνεται συνεχώς, άρα είναι σε θέση να εντοπίζει νέους ιούς. Σχεδόν κάθε μέρα ανακαλύπτονται νέοι ιοί και είναι πάρα πολύ πιθανό να προσβληθείτε ενώ «σερφάρετε» στο δίκτυο. Μην ξεχνάτε πώς, όσο βρίσκεστε στο διαδύκτιο, διάφοροι τρίτοι μπορούν να σχηματίσουν εικόνα του είδους των πληροφοριών που βρίσκονται στο κινητό σας τηλέφωνο, επειδή έχει τη δική του διεύθυνση στον ιστό, άρα μπορεί να δεχτεί εξωτερικές παρεμβάσεις.

Αν δεν έχετε εγκαταστήσει επαρκή μέτρα ασφαλείας, αντιμετωπίζετε τον κίνδυνο να αποκτήσουν κάποια μη εξουσιοδοτημένα πρόσωπα πρόσβαση στα δεδομένα του κινητού σας τηλεφώνου. Επίσης, υπάρχει η πιθανότητα να ανοίξουν οι hackers back door στο κινητό σας τηλέφωνο και να τη χρησιμοποιούν κάθε φορά που βρίσκεστε στο διαδίκτυο, για να στέλνουν, λόγου χάρη, εν αγνοία σας ανεπιθύμητα e-mail(spam). Η ύπαρξη προσωπικού τείχους ασφαλείας (firewall) μπορεί να σας προστατεύσει από τέτοιου είδους υποθέσεις.

Κανόνας 10ος : Να δημιουργείτε τακτικά αντίγραφα ασφαλείας

Η διατήρηση αντιγράφων ασφαλείας των αρχείων σας είναι ένας από τους χρυσούς κανόνες είτε διενεργείτε τραπεζικές συναλλαγές στο διαδίκτυο είτε όχι. Συνήθως είναι εξαιρετικά περίπλοκο, αν όχι αδύνατο, να διασώσετε δεδομένα μετά τη διαγραφή ή την καταστροφή τους. Ένας βολικός τρόπος δημιουργίας αντιγράφων ασφαλείας είναι η χρήση κινητών μονάδων σκληρού δίσκου, συσκευών εγγραφής cd ή dvd ή μονάδων μαγνητοταινίας κατόπιν μεταφοράς των δεδομένων σε έναν ηλεκτρονικό υπολογιστή.

Όποια μέθοδο και αν επιλέξετε, μη ξεχνάτε να δημιουργείτε σε τακτική βάση αντίγραφα ασφαλείας των νέων ή τροποποιημένων αρχείων. Επίσης, φυλάξτε τα αντίγραφα ασφαλείας σε ασφαλές μέρος, δηλαδή ξεχωριστά από τον υπολογιστή σας και προστατευμένα από κάθε μη εξουσιοδοτημένη πρόσβαση (http://sicherheit-im-internet.de).

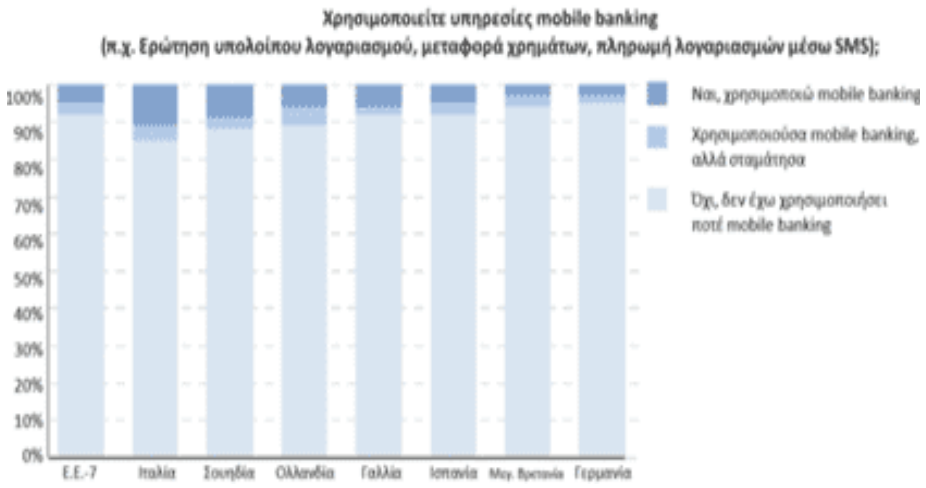
2) Ελληνική Ένωση Τραπεζών

Η Ελληνική Ένωση Τραπεζών και οι τράπεζες μέλη της, παράλληλα με τα μέτρα ασφαλείας που οι ίδιες οι τράπεζες λαμβάνουν, υπενθυμίζουν και συνιστούν προς όλους τους χρήστες της Ηλεκτρονικής Τραπεζικής τα εξής (www.hba.gr):

- Μην αποκαλύπτετε ποτέ και σε κανέναν τους προσωπικούς σας κωδικούς.
  Σε περίπτωση που υποπτεύεστε διαρροή του κωδικού πρόσβασής σας επικοινωνήστε άμεσα με την Τράπεζά σας.
- Αγνοείστε «ύποπτα» e-mail με τα οποία σας ζητούνται προσωπικά σας στοιχεία (αριθμός λογαριασμού, μυστικοί προσωπικοί κωδικοί, ονοματεπώνυμο κ.α.) ή περιέχουν συνδέσμους (links) σε «άγνωστες» ιστοσελίδες. Οι Τράπεζες δεν πρόκειται για κανένα λόγο να σας ζητήσουν τα προσωπικά σας στοιχεία μέσω e-mail ή τηλεφώνου. Για το λόγο αυτό να διαγράφετε τα e-mail αυτά ως πλαστά και να αγνοείτε αντίστοιχες πιθανές τηλεφωνικές κλήσεις.
- Βεβαιωθείτε ότι βρίσκεστε στη σωστή διεύθυνση της τράπεζάς σας.
  Μην συνδεθείτε ποτέ με την ιστοσελίδα της τράπεζάς σας μέσω εξωτερικού συνδέσμου (link) που σας παρέχει κάποιος τρίτος και ιδιαίτερα μέσω e-mail. Βεβαιωθείτε ότι στην ιστοσελίδα Ηλεκτρονικής Τραπεζικής της Τράπεζάς σας εμφανίζεται το εικονίδιο με το «λουκέτο» μέσω του οποίου μπορείτε ανοίγοντας το με διπλό κλικ, να επιβεβαιώσετε ότι βρίσκεστε στο ασφαλές περιβάλλον της Τράπεζάς σας.
- Ρυθμίστε το λειτουργικό σύστημα του υπολογιστή σας και το πρόγραμμα antivirus που χρησιμοποιείτε, ώστε να ενημερώνονται αυτόματα.
  Αν δε γνωρίζετε πως να το κάνετε συμβουλευτείτε τον προμηθευτή του υπολογιστή σας.

ΚΕΦΑΛΑΙΟ IV: Το m-banking στην Ευρώπη και στην Ελλάδα

Πρόκληση για τις τράπεζες και τα τηλεπικοινωνιακά δίκτυα αποτελούν οι υπηρεσίες mobile banking. Από τη στιγμή που οι τραπεζικές υπηρεσίες μέσω κινητού τηλεφώνου είναι διαθέσιμες από τις περισσότερες μεγάλες τράπεζες της Ευρώπης, από τα τέλη της δεκαετίας του '90, θα ήταν επόμενο η διείσδυση αυτών των υπηρεσιών να κυμαίνεται σε υψηλά ποσοστά. Η έρευνα όμως της **Forrester Research**(2007) δείχνει το αντίθετο καθώς είναι λίγοι οι Ευρωπαίοι -περίπου το 5% των πελατών των τραπεζών- που χρησιμοποιούν τις υπηρεσίες mobile banking που βασίζονται κατά κύριο λόγο στην τεχνολογία των γραπτών μηνυμάτων (SMS) (Διάγραμμα 1).



Διάγραμμα 1. Καταναλωτές που χρησιμοποιούν υπηρεσίες mobile banking στην Ευρώπη, Βάση: 7.160 χρήστες, Πηγή: Forrester Research, 2007

Οι χρήστες είναι κυρίως νέοι ηλικίας μεταξύ 25 - 35 ετών, που χρησιμοποιούν επίσης τις on-line τραπεζικές εργασίες. Ανήκουν στην κατηγορία των υψηλών εισοδημάτων, είναι τεχνολογικά ενημερωμένοι και χρησιμοποιούν το Διαδίκτυο καθημερινά. Το 57% των χρηστών υπηρεσιών mobile banking προτιμούν συνήθως τις απλές εφαρμογές και η πιο συνηθισμένη είναι ο έλεγχος του τραπεζικού λογαριασμού. Εξίσου δημοφιλείς είναι οι ειδοποιήσεις μέσω SMS ενώ ένα ποσοστό γύρω στο 27% των χρηστών κάνουν έλεγχο των τραπεζικών τους συναλλαγών μέσω

του κινητού τους τηλεφώνου. Πιο σύνθετες συναλλαγές, όπως η μεταφορά χρημάτων ή η αλλαγή τραπεζικού κωδικού, είναι λιγότερο συνηθισμένες μέσω του mobile banking (Διάγραμμα 2).

Διάγραμμα 2. Χρήση υπηρεσιών mobile banking στην Ευρώπη ανά ηλικία, Βάση: 374 χρήστες, Πηγή: Forrester Research, 2007

Το ερώτημα όμως που απασχολεί την τραπεζική αγορά αλλά και τους αναλυτές του τεχνολογικού κλάδου είναι γιατί το mobile banking έχει τόσο χαμηλά ποσοστά διείσδυσης στο κοινό.

Σύμφωνα με τη Forrester Research(2007) οι καταναλωτές δεν αντιλαμβάνονται τα οφέλη των υπηρεσιών mobile banking γι' αυτό και δεν τις χρησιμοποιούν. Προτιμούν τη χρήση των ATM ή των παραδοσιακών μεθόδων συναλλαγής με την τράπεζα. Αυτό αποτελεί μία από τις βασικές αιτίες της χαμηλής διείσδυσης του mobile banking στην ευρωπαϊκή αγορά. Η πλειονότητα επίσης δε γνωρίζει ότι υπάρχουν οι συγκεκριμένες υπηρεσίες, ενώ παράλληλα νιώθουν ανασφαλείς κατά τη χρήση τους.

Επίσης, ένα σημαντικό ποσοστό αναρωτιέται για το κόστος αυτών των υπηρεσιών και υποστηρίζει πως δεν κατέχει την τεχνολογικά προηγμένη συσκευή κινητής τηλεφωνίας για τέτοιου είδους εφαρμογές.

Σύμφωνα με την έρευνα, οι υπηρεσίες mobile banking είναι μια "καυτή" πολλά υποσχόμενη αγορά για την ευρωπαϊκή λιανική τραπεζική αλλά και τα

τηλεπικοινωνιακά δίκτυα. Πολλές τράπεζες έχουν επενδύσει στο συγκεκριμένο τομέα θεωρώντας πως θα αποτελέσουν ένα ακόμα κανάλι αυτό-εξυπηρέτησης των καταναλωτών.

Όπως τονίζουν οι αναλυτές, οι τράπεζες που προσφέρουν υπηρεσίες mobile banking πρέπει να καταστήσουν σαφές στους πελάτες τους την απλότητα και την εγκυρότητα αυτών των υπηρεσιών και να γίνει συνείδηση των καταναλωτών ότι αυτές οι υπηρεσίες προσφέρονται οπουδήποτε και οποιαδήποτε στιγμή.

Η Forrester Research(2007) επισημαίνει πως οι επικεφαλής των τμημάτων πληροφορικής των τραπεζών μπορούν να κάνουν πολλά για να αλλάξουν τα δεδομένα.

Δουλεύοντας από κοινού μαζί με τα τμήματα μάρκετινγκ των τραπεζών μπορούν να πείσουν τους πελάτες τους για τη χρησιμότητα και την απλή λειτουργία των υπηρεσιών mobile banking. Μπορούν να αποδείξουν με συγκεκριμένα παραδείγματα για την υπεραξία αυτών των υπηρεσιών. Μπορούν επίσης να εστιάσουν σε συγκεκριμένες κατηγορίες πελατών όπως είναι οι νέοι σε ηλικία και τεχνολογικά εγγράμματοι χρήστες και να τους προσφέρουν ποικιλία υπηρεσιών mobile banking, προωθώντας έγκυρες και χωρίς χρονικούς και τοπικούς περιορισμούς υπηρεσίες.

Παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, το m-banking δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό. Αυτό οφείλεται ενδεχομένως στη χρήση του κινητού ως κατεξοχήν μέσου επικοινωνίας, συνεπώς η αποδοχή της αξιοπιστίας του ως μέσου διεξαγωγής χρηματοοικονομικών συναλλαγών δεν είναι εύκολη. Οι Έλληνες χρήστες και οι επιχειρήσεις δείχνουν να εμπιστεύονται περισσότερο το Internet, γεγονός που εξηγεί τα μεγαλύτερα ποσοστά διείσδυσης του e-banking έναντι του m-banking.

Ωστόσο, με αργούς αλλά σταθερούς ρυθμούς τα πράγματα αλλάζουν. Οι επιχειρήσεις, και ειδικότερα οι μικρομεσαίες, αλλά και οι ιδιώτες έχουν αρχίσει να αντιλαμβάνονται ότι οι υπηρεσίες mobile banking αποφέρουν κέρδος σε πολύτιμο χρόνο και, κατά συνέπεια, χρήμα.

Από έρευνες που έχουν πραγματοποιηθεί για λογαριασμό τραπεζών υπολογίζεται ότι το 7% των πελατών τους κάνει σήμερα χρήση του τηλεφώνου για τραπεζικές συναλλαγές. Τα τελευταία στοιχεία που έχουν στη διάθεσή τους οι τράπεζες δείχνουν ότι το 2001 πραγματοποιήθηκαν 100.000 εγχρήματες συναλλαγές μέσω κινητού τηλεφώνου, ενώ ο τζίρος ανήλθε σε 4 δισ. ευρώ. Φέτος οι συναλλαγές αναμένεται να αυξηθούν σε 120.000 και ο τζίρος σε 10 δισ. ευρώ.

i. Η υπηρεσία m-banking της Εθνικής Τράπεζας της Ελλάδας(Ε.Τ.Ε.)

1) Προσφερόμενες υπηρεσίες

Με το Mobile Banking υπάρχει 24ωρη πρόσβαση στις περισσότερες από τις παρεχόμενες συναλλαγές του Internet Banking, σε οποιοδήποτε γεωγραφικό σημείο στην Ελλάδα ή στο εξωτερικό:

- Πληροφόρηση (υπόλοιπα & κινήσεις συνδεδεμένων λογαριασμών)
- Μεταφορά ποσών σε λογαριασμό Εθνικής Τράπεζας ή τράπεζας εσωτερικού
- Εξόφληση οφειλών σε συμβεβλημένες εταιρείες, καθώς και πιστωτικές κάρτες Εθνικής και άλλων τραπεζών
- Πληρωμή Φόρου Εισοδήματος, αγοραπωλησία μετοχών και ενημέρωση μετοχικού χαρτοφυλακίου κ.ά.

Στο πλαίσιο της παρεχόμενης πληροφόρησης μέσω της συσκευής i-mode® ο πελάτης μπορεί επίσης:

- να ενημερώνεται για τα επενδυτικά, στεγαστικά, καταναλωτικά και επαγγελματικά προϊόντα της Τράπεζας,
- να εντοπίζει τα σημεία που υπάρχουν ATMs και
- να βρίσκει τις ταχυδρομικές διευθύνσεις, τα τηλέφωνα και τους κωδικούς των καταστημάτων της τράπεζας.

Επιλέγοντας οι πελάτες την πραγματοποίηση των συναλλαγών σας μέσω του Mobile Banking εξοικονομούν χρόνο και έξοδα, καθώς οι κινήσεις

λογαριασμών και οι περισσότερες συναλλαγές είναι δωρεάν (π.χ. πληρωμές λογαριασμών, μεταφορές σε λογαριασμούς Εθνικής Τράπεζας), ενώ το κόστος αποστολής εμβασμάτων και χρηματιστηριακών συναλλαγών είναι σημαντικά μειωμένο.

Επιπλέον :

- Η χρήση του Internet /Mobile Banking, συμπεριλαμβανομένης και της παράδοσης ή αντικατάστασης της συσκευής e–Code, είναι δωρεάν για τους φοιτητές.
- Η χρήση του Internet/Mobile Banking, συμπεριλαμβανομένης και της παράδοσης ή αντικατάστασης της συσκευής e–Code έχει μειωμένη προμήθεια για τους δικαιούχους λογαριασμών Μισθοδοτικού Plus, Επαγγελματικού Plus ή Αγροτικού Plus (www.nbg.gr).

2) Ασφάλεια

Η διενέργεια τραπεζικών συναλλαγών μέσω κινητού τηλεφώνου (i-mode) της Cosmote διασφαλίζεται με το ίδιο επίπεδο και τα μέτρα ασφάλειας που παρέχονται και στο Internet Banking, δεδομένου ότι η τεχνολογία i-mode επιτρέπει την μεταφορά δεδομένων μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL (Secure Sockets Layer).

Οι συνδρομητές του Internet Banking μπορούν να εισέλθουν στην εφαρμογή μέσω του κινητού τους τηλεφώνου με τον Κωδικό Χρήστη (UserID) και το Μυστικό (Password). Κάθε φορά που θέλουν να πραγματοποιούν συναλλαγές μέσω του κινητού τηλεφώνου, θα πρέπει να ακολουθούν τα ίδια βήματα που περιγράφονται για το Internet Banking. Για πρόσθετη ασφάλεια στις εγχρήματες συναλλαγές απαιτείται η εισαγωγή πρόσθετου κωδικού μίας χρήσης, που παράγεται από τη συσκευή e-Code (www.nbg.gr).

ii. Η υπηρεσία m-banking της Τράπεζας Πειραιώς

1) Προσφερόμενες υπηρεσίες

Διαχείριση Λογαριασμών

Ο πελάτης μπορεί να ενημερωθεί για τη συνολική εικόνα του χαρτοφυλακίου του στην Τράπεζα Πειραιώς με την τρέχουσα αξία του και να δει αναλυτικές πληροφορίες όλων των λογαριασμών του, το υπόλοιπο τους και τις συναλλαγές του.

- Υπόλοιπα Λογαριασμών και Ανάλυση: Ενημέρωση για το λογιστικό και το διαθέσιμο υπόλοιπο των λογαριασμών, πιθανές δεσμεύσεις που έχουν γίνει καθώς και πιστώσεις με μελλοντική ημερομηνία αξίας.
- Κινήσεις Λογαριασμών: Πληροφόρηση για τις χρεώσεις και τις πιστώσεις που έγιναν στους λογαριασμούς του πελάτη, αναζητώντας με τα πλήκτρα πλοήγησης την ημερομηνία που του ενδιαφέρει.
- Αναλυτικά Στοιχεία Λογαριασμού: Πληροφόρηση για το κατάστημα στο οποίο τηρούνται λογαριασμοί, τους συνδικαιούχους και άλλα χαρακτηριστικά των λογαριασμών.
- Παραγγελία Βιβλιαρίου Επιταγών.
- Ανάκληση Βιβλιαρίου Επιταγών ή Επιταγής.

Διαχείριση Καρτών

Διαχείριση των πιστωτικών καρτών και παρακολούθηση των κινήσεων και των στοιχείων, συγκεκριμένα:

- Υπόλοιπα και Κινήσεις Πιστωτικών Καρτών.
- Αναλυτικά Στοιχεία Πιστωτικών Καρτών.
- Πληρωμή Δόσης.

Διαχείριση Δανείων

Μέσω της υπηρεσίας winbank mobile, είναι άμεσα διαθέσιμες όλες οι πληροφορίες σχετικά με τα δάνεια που έχει ο πελάτης στην Τράπεζα Πειραιώς:

- Συνολική Απεικόνιση όλων των Δανειακών Προϊόντων.
- Αναλυτικά Στοιχεία Δανείων, όπως την Κατάστασή τους, το Διαθέσιμο, Ληξιπρόθεσμο και Ανεξόφλητο Ποσό, την Ημέρα Πληρωμής, κ.ά.
- Ιστορικό όλων των Πληρωμών Δόσεων Δανείων.

Πληρωμές – Μεταφορές

Υπάρχει η δυνατότητα καταχώρησης εντολών για πληρωμές, εμβάσματα και μεταφορές και διαχείρισης των οφειλών. Συγκεκριμένα, μπορεί ο πελάτης να εκτελέσει:

Μεταφορές

- Σε Λογαριασμούς.
- Σε Λογαριασμούς Τρίτων στην Τράπεζα Πειραιώς.

Μεμονωμένες Εντολές Πληρωμών

- Πιστωτικών Καρτών της Τράπεζας Πειραιώς.
- ΔΕΚΟ (ΟΤΕ, ΔΕΗ).
- Ασφαλιστικών ταμείων (ΙΚΑ, ΦΠΑ, ΤΕΒΕ).

Εμβάσματα

- Σε Ελλάδα.
- Σε Τράπεζες του Εξωτερικού.

Επιπλέον, ανά πάσα στιγμή ο πελάτης μπορεί να διαχειριστεί τις εντολές που έχει καταχωρήσει. Συγκεκριμένα :

- Διαγραφή ή απενεργοποίησή τους.
- τροποποίηση των λεπτομερειών εκτέλεσης τους.
- καταχώρηση νέας όμοιας εντολής
- Ιστορικό των συναλλαγών

Χρηματιστήριο

Αγοραπωλησία μετοχών, real-time παρακολούθηση του χαρτοφυλακίου και των τιμών των μετοχών.

- Εντολές Αγοράς Μετοχών με Χρέωση Λογαριασμού.
- Εντολές Πώλησης Μετοχών με Πίστωση Λογαριασμού.
- Ενημέρωση για την Εκτέλεση των Εντολών (Πινακίδια).
- Εμφάνιση Κατάστασης Εντολών Ημέρας.
- Συμμετοχή σε Δημόσιες Εγγραφές.

Οδηγίες Πρόσβασης

Πρόσβαση στην υπηρεσία m-banking της τράπεζας γίνεται μέσω φορητής συσκευής στην ιστοσελίδα της winbank, χωρίς επιπλέον ρυθμίσεις:

- Απευθείας, στην ηλεκτρονική διεύθυνση, mobile.winbank.gr (χρησιμοποιώντας οποιαδήποτε εταιρία κινητής τηλεφωνίας που παρέχει σύνδεση στο internet)
- Μέσω του i-mode, το internet της κινητής τηλεφωνίας από την COSMOTE (ισχύει μόνο για πελάτες της Cosmote).

Μοναδική προϋπόθεση για την πρόσβαση στην ιστοσελίδα της winbank, είναι ο πελάτης να έχει κωδικούς πρόσβασης στην υπηρεσία winbank mobile και να ενεργοποιήσει τη σύνδεση του στο internet (π.χ. wap / gprs) από τις ασύρματες συσκευές του.

Το συνολικό κόστος της χρήσης της υπηρεσίας εξαρτάται είτε από τις χρεώσεις της εκάστοτε εταιρία κινητής τηλεφωνίας (3G, gprs, wap) στην οποία είναι συνδρομητής ο πελάτης είτε από τους φορείς ασύρματης επικοινωνίας (wi-fi) (**www.piraeusbank.gr**).

2) Ασφάλεια

Η winbank εξασφαλίζει τη μέγιστη δυνατή ασφάλεια των ηλεκτρονικών συναλλαγών με τις πιο σύγχρονες και προηγμένες μεθόδους:

Αναγνώριση Πελάτη

Οι κωδικοί που χρησιμοποιούνται για την αναγνώρισή του πελάτη είναι δύο: ο Κωδικός Εισόδου (UserID) και ο Προσωπικός Κωδικός Ασφαλείας (PIN), τους οποίους καταχωρεί κάθε φορά ο πελάτης που χρησιμοποιεί την υπηρεσία mobile.

Η winbank δίνει τη δυνατότητα μεταβολής των κωδικών όσο συχνά επιθυμεί ο πελάτης, ώστε να διασφαλίζεται ακόμα περισσότερο η ασφάλεια των συναλλαγών. Οι προσωπικοί κωδικοί μπορούν να αλλαχθούν μέσω της υπηρεσίας internet banking ή μέσω της υπηρεσίας mobile.

Εξασφάλιση του Απορρήτου της Μεταφοράς των Δεδομένων

Για την εξασφάλιση του απορρήτου της μεταφοράς των δεδομένων, χρησιμοποιείται το πρωτόκολλο κρυπτογράφησης SSL/128 bit.

Κλείδωμα Κωδικών

Σε περίπτωση εισαγωγής του Προσωπικού Κωδικού Ασφαλείας (PIN) τρεις φορές λανθασμένα, το σύστημα κλειδώνει τους κωδικούς. Για την επαναλειτουργία τους πρέπει ο πελάτης να καλέσει το κέντρο εξυπηρέτησης πελατών της Τράπεζας Πειραιώς και αφού γίνει πιστοποίηση των στοιχείων του, κάποιος από τους τραπεζικούς αντιπροσώπους της τράπεζας θα ενεργοποιήσει τον Προσωπικό Κωδικό Ασφαλείας (PIN).

Αυτόματη Αποσύνδεση

Εάν δεν υπάρξει καμία δραστηριότητα για επτά λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία winbank mobile.

Ελεγχόμενη Πρόσβαση (firewall)

Η πρόσβαση στα συστήματα της Τράπεζας (servers) ελέγχεται από firewall, το οποίο επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών από τους πελάτες/ επισκέπτες απαγορεύοντας, παράλληλα, την πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της Τράπεζας. (**www.piraeusbank.gr**).

iii. Οι ηλεκτρονικές διευθύνσεις των τραπεζών στην Ελλάδα που προσφέρουν την υπηρεσία m-banking

Παρακάτω αναφέρονται μερικές ηλεκτρονικές διευθύνσεις των τραπεζών στην Ελλάδα που προσφέρουν την υπηρεσία m-banking:

ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.
http://www.nbg.gr

ALPHA BANK S.A.
http://www.alpha.gr

ΤΡΑΠΕΖΑ EFG EUROBANK ERGASIAS Α.Ε.
http://www.eurobank.gr

ΕΜΠΟΡΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.
http://www.emporiki.gr

ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ Α.Ε.
http://www.piraeusbank.gr

ΤΡΑΠΕΖΑ ΚΥΠΡΟΥ
http://www.bankofcyprus.gr

CITIBANK INTERNATIONAL

http://www.citibank.gr

ΓΕΝΙΚΗ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.

http://www.geniki.gr

MARFIN EGNATIA BANK A.E.

http://www.marfinegnatiabank.gr

ΚΕΦΑΛΑΙΟ V: Συμπεράσματα

Με το πέρας της πτυχιακής εργασίας προκύπτουν κάποια συμπεράσματα τα οποία είναι χρήσιμο να παρατεθούν και να τονιστεί η σημασία τους.

Τα τελευταία χρόνια οι τράπεζες χρησιμοποιούν τα μέσα που τους παρέχει η τεχνολογία για τη διεκπαιρέωση των τραπεζικών συναλλαγών. Η χρήση του διαδικτύου εισήγαγε την ηλεκτρονική τραπεζική φέρνοντας σε πλεονασματική θέση τις τράπεζες έναντι στον ανταγωνισμό και στις ολοένα αυξανόμενες απαιτήσεις των πελατών, αλλά παράλληλα διευκόλυνε τις τραπεζικές συναλλαγές. Ένα από τα προσφερόμενα είδη της ηλεκτρονικής τραπεζικής είναι το mobile banking, συνδυάζοντας κινητό τηλέφωνο και Internet για την πραγματοποίηση τραπεζικών συναλλαγών. Το m-banking δίνει τη δυνατότητα στους πελάτες να φέρουν εις πέρας τραπεζικές συναλλαγές (όπως πληροφορίες για την κίνηση του λογαριασμού, ακύρωση πιστωτικής κάρτας, αίτηση για χορήγηση δανείου ή κάρτας, κτλ) γρηγορότερα και ευκολότερα από τις συμβατικές μορφές διεκπαιρέωσης των τραπεζικών αυτών συναλλαγών.

Παρόλα αυτά, η ηλεκτρονική τραπεζική στην Ελλάδα δεν προσελκύει όσους πελάτες θα επιθυμούσαν οι τράπεζες υιοθετώντας την. Αυτό πιθανόν να οφείλεται στην ελλιπή εξοικείωση των χρηστών με την τεχνολογία, στους φόβους όσον αφορά σε θέματα ασφάλειας, αλλά και στη μη ολοκληρωμένη ενημέρωση των υποψηφίων πελατών για τις πιθανές απολαβές από τη χρήση του m-banking. Χρειάζεται ακόμα αρκετός χρόνος ωρίμανσης προκειμένου να εισέλθει η χώρα μας σε ένα στάδιο άνθισης της ηλεκτρονικής τραπεζικής. Για το λόγο αυτό, θα πρέπει οι τράπεζες να φροντίσουν να χρησιμοποιούν φιλικά συστήματα για τον χρήστη-πελάτη και να τους παρέχουν συνεχή ενημέρωση, καθοδήγηση και υποστήριξη για την καλύτερη χρήση των συστημάτων της ηλεκτρονικής τραπεζικής και κατ’ επέκταση της υπηρεσίας m-banking.

Ένα άλλο σημαντικό συμπέρασμα είναι η καθιέρωση της διαφάνειας και της ασφάλειας της υπηρεσίας m-banking. Η χρήση του Internet απαιτεί από τις τράπεζες να εφαρμόζουν όλα τα απαραίτητα μέτρα ασφάλειας, έτσι ώστε

να εξασφαλίζεται η σωστή διεκπαιρέωση των τραπεζικών συναλλαγών και η διατήρηση του απορρήτου των προσωπικών δεδομένων των πελατών που απαιτούν τέτοιου είδους συναλλαγές βάση του νομικού πλαισίου και των όρων σύμβασης παροχής υπηρεσιών μέσω διαδικτύου. Στόχος των τραπεζών είναι η εξάλειψη των προβλημάτων που ενδέχεται να παρουσιάσει η πραγματοποίηση των συναλλαγών μέσω διαδικτύου, έτσι ώστε οι πελάτες να εμπιστευτούν περισσότερο την υπηρεσία m-banking.

Η ασφάλεια όμως των τραπεζικών συναλλαγών δεν εξαρτάται μόνο από τον φορέα παροχής τους αλλά και από τον χρήστη. Για το λόγο αυτό οι τράπεζες εντείνουν την προσοχή στους πελάτες τους για τη σωστή χρήση του Internet και της υπηρεσίας m-banking, έτσι ώστε να αποφευχθεί ενδεχόμενη εισβολή hacker και κατ' επέκταση υποκλοπή προσωπικών δεδομένων των πελατών και κατάχρηση των λογαριασμών τους.

Επίσης, η υπηρεσία m-banking παρέχεται σχετικά από λίγες τράπεζες στην Ελλάδα, ακόμη και από τράπεζες που έχουν αναπτύξει το e-banking. Ο ανταγωνισμός όμως μεταξύ των τραπεζών, τις οδήγησε στην ανάπτυξη πελατοκεντρικών στρατηγικών που με τη χρήση των νέων τεχνολογιών (κινητού τηλεφώνου και Internet) μπόρεσαν να δημιουργήσουν ποιοτικές, γρήγορες και ασφαλείς υπηρεσίες δημιουργώντας σχέσεις προστιθέμενης αξίας με τον πελάτη. Έτσι, η ανάπτυξη όλων των ειδών της ηλεκτρονικής τραπεζικής είναι απαραίτητη για την επιβίωση τους και γι' αυτό το λόγο ολοένα και περισσότερες τράπεζες αναπτύσσουν το m-banking, δημιουργώντας εύκολη και γρήγορη διεκπαιρέωση των τραπεζικών συναλλαγών.

Τέλος, συνοπτικά το m-banking είναι ένα από τα είδη της ηλεκτρονικής τραπεζικής που καταφέρνει να διευκολύνει τις τραπεζικές συναλλαγές. Επειδή, είναι μια νέα σχετικά υπηρεσία, οι αρμόδιοι φορείς πρέπει να εφιστήσουν την προσοχή τους στη διατήρηση της ασφάλειας των τραπεζικών συναλλαγών όταν χρησιμοποιείται το διαδίκτυο και το κινητό τηλέφωνο. Το μέλλον της ηλεκτρονικής τραπεζικής στην Ελλάδα για τα επόμενα χρόνια, διαγράφεται θετικό και ελπιδοφόρο.

Βιβλιογραφία

Ελληνική βιβλιογραφία

1. Χ. Θεοφιλίδης (2002). *'Ή Συγγραφή Επιστημονικής Εργασίας"*. Αθήνα: Γ. Δαρδάνος.
2. Β. Αγγελής (2005). *'Ή βίβλος του E-Banking"*. Αθήνα: Τεχνογνωσία.
3. Α. Σινανιώτη-Μαρούδη, Ι. Φαρσαρώτας (1957). *'Ήλεκτρονική Τραπεζική"*. Αθήνα : Α. Ν. Σάκκουλας, 2005.
4. Τ. Μάγιογλου (2005). *'Ήλεκτρονική Τραπεζική (E-Banking): Η Ελληνική Πραγματικότητα"*. Αδημοσίευτη διπλωματική εργασία.
5. Φ. Τζιμκίδου (2006). *''Το E-Banking: Οι κίνδυνοι και η ασφάλεια των συναλλαγών'"*. Αδημοσίευτη διπλωματική εργασία.
6. Γ. Κατσουλακός (2001). *'Ήνέα Οικονομία, Διαδίκτυο και Ηλεκτρονικό Εμπόριο"*. Αθήνα: Κέρκυρα.
7. Β. Κελτσόπουλου, Σ. Συρμακέζη (1997*). 'Ίδιαδικτυακή Τραπεζική (Web-banking)"*. Δελτίο Ένωσης Ελληνικών Τραπεζών.
8. Π. Μπερνίτσα (1985). *'Ίσκέψεις και προβληματισμοί για τις ηλεκτρονικές συναλλαγές"*. Αθήνα: Δελτίο Ένωσης Ελληνικών Τραπεζών.
9. Κ. Ταβλαρίδης (2000). *'Ή προστασία των καταναλωτών στην ηλεκτρονική τραπεζική".* Αθήνα: Δελτίο Ένωσης Ελληνικών Τραπεζών.
10. F. Frank (2001). *'Ί E-Marketing: επιχειρηματικές εφαρμογές του μαρκετινγκ στο διαδίκτυο"*. Αθήνα: Γκιούρδας.
11. Α. Αρχοντάκης (1999). *'Τραπεζικές υπηρεσίες και προϊόντα μέσω Internet"*. Παγκόσμια πλατφόρμα ενεργητικής επικοινωνίας & ηλεκτρονικού εμπορίου.

Ξένη βιβλιογραφία

1. Mosad Zineldin (1995). *'Bank - company interactions and relationships: some empirical evidence"*. International Journal of Bank Marketing.
2. Zona Research Incorporation (2000). *'Second Generation of Electronic Commerce"*. International Journal of Bank Marketing.

3. E. Banks (2001). *''E-Finance: The Electronic Revolution''*. Financial Times Management.
4. Clarke, Roger (1996). *''Message Transmission Security (or Cryptography in Plain Text)''*. Privacy Law & Policy Reporter.
5. P. Ashley, H. Hinton, M. Vandenwauver (2001). *''Wired Versus Wireless Security: The Internet, WAP and iMode for E-Commerce''*. Tivoli:IBM Software Group.
6. Jossey-Bass, D. Chaffey (2002). *''E-Business and E-Commerce Management: Strategy Implementation and Practise''*. Financial Times Management.
7. G. Adams (2003). *''E-Business Revolution & The New Economy: Economics After the Dot-Com Crash''*. South-Western Educational Publishing.

Ιστοσελίδες

- **www.nbg.gr** (Εθνική Τράπεζα της Ελλάδος)
- **www.piraeusbank.gr** (Τράπεζα Πειραιώς)
- **www.m-comm.internet.com**
- **www.hba.gr** (Ένωση Ελληνικών Τραπεζών)
- **www.panelliniabank.gr** (Πανελλήνια Τράπεζα)
- **www.setco.org**
- **http://sicherheit-im-internet.de** (Ένωση Γερμανικών Τραπεζών)
- **http://en.wikipedia.org** (Ηλεκτρονική Εγκυκλοπαίδεια)
- **www.go-online.gr** (Εκπαιδευτική Στήριξη του Προγράμματος "Δικτυωθείτε")
- **www.naftemporiki.gr** (Ναυτεμπορική)
- **www.eurobank.gr** (Eurobank)
- **www.ercim.org/publication/Ercim_News/enw41/index.html** (Ercim News)
- **www.alpha.gr** (Alpha Bank)
- **www.geniki.gr** (Γενική Τράπεζα)
- **www.citibank.gr** (Citibank)
- **www.marfinegnatiabank.gr** (Marfin Egnatia Bank)
- **www.bankofcyprus.gr** (Τράπεζα Κύπρου)

- **www.emporiki.gr** (Εμπορική Τράπεζα)
- **www.bankofgreece.gr** (Τράπεζα της Ελλάδος)