ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

E-BANKING

ΤΟΥ ΤΑΧΥΔΡΟΜΙΚΟΥ ΤΑΜΙΕΥΤΗΡΙΟΥ ΕΛΛΑΔΟΣ

2007-2012

ΥΠΟ

Πάκας Ευαγγελίας

Φοιτήτριας του τμήματος Λογιστικής ΑΦΜ:288/07

Επιβλέπων: Καθ. Γ.Β. Παπαδιοδώρου

Θεσσαλονίκη, Σεπτέμβριος 2012

ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

E-BANKING

ΤΟΥ ΤΑΧΥΔΡΟΜΙΚΟΥ ΤΑΜΙΕΥΤΗΡΙΟΥ ΕΛΛΑΔΟΣ

2007-2012

ΥΠΟ

Πάκας Ευαγγελίας

Φοιτήτριας του τμήματος Λογιστικής ΑΦΜ:288/07

Επιβλέπων: Καθ. Γ.Β.Παπαδιοδώρου

Θεσσαλονίκη, Σεπτέμβριος 2012

Στον σύντροφό μου και

στην οικογένειά μου

ΠΕΡΙΕΧΟΜΕΝΑ:

ΜΕΡΟΣ 1

ΚΕΦΑΛΑΙΟ 4

4.1. ΑΣΦΑΛΕΙΑ

4.1.1. Ο ΡΟΛΟΣ ΤΗΣ ΤΡΑΠΕΖΑΣ

4.1.2.Ο ΡΟΛΟΣ ΤΟΥ ΧΡΗΣΤΗ

4.2. ΑΠΕΙΛΕΣ-ΚΙΝΔΥΝΟΙ

4.3. ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΕΙΛΩΝ-ΚΙΝΔΥΝΩΝ

4.4. ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΦΑΛΕΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΚΕΦΑΛΑΙΟ 5

5. ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ

ΜΕΡΟΣ 2

- ΓΝΩΡΙΜΙΑ ΜΕ ΤΟ ΤΑΧΥΔΡΟΜΙΚΟ ΤΑΜΙΕΥΤΗΡΙΟ
- ΠΟΤΕ ΕΜΦΑΝΙΣΤΗΚΕ ΤΟ E-BANKING ΣΤΟ ΤΤ
- ΤΙ ΑΣΦΑΛΕΙΑ ΧΡΗΣΙΜΟΠΟΙΕΙ ΤΟ ΤΤ
- ΤΟ ΤΤ ΕΝΗΜΕΡΩΝΕΙ ΤΟΥΣ ΧΡΗΣΤΕΣ ΓΙΑ ΤΟ E-BANKING

ΜΕΡΟΣ 3

- ΣΥΜΠΕΡΑΣΜΑΤΑ
- ΙΣΤΟΓΡΑΦΙΑ
- ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ
- ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

ΠΕΡΙΛΗΨΗ

Αντικείμενο της εργασίας αυτής αποτελεί το e-banking στην Ελλάδα από το 2007-2012. Στο πρώτο μέρος, δίνεται μία σύντομη ιστορική αναδρομή και η εξέλιξη του e-banking. Στην συνέχεια δίνονται συγκεκριμένες έννοιες για την κατανόηση του θέματος , οι δυνατότητες που παρέχει η υπηρεσία αυτή και σε ποια είδη χωρίζεται. Έπειτα, αναφέρεται πως έγινε η διείσδυση της υπηρεσίας αυτής στην χώρα μας και πως αντέδρασαν οι Έλληνες. Δίνονται στοιχεία για το πόσοι άνθρωποι στην Ελλάδα πραγματοποιούν συναλλαγές μέσω e-banking , πόσοι το εμπιστεύονται και γίνεται σύγκριση με την εμπιστοσύνη που έχουν οι άνθρωποι του εξωτερικού στις συναλλαγές μέσω internet ενώ στο επόμενο κεφάλαιο δίνονται τα πλεονεκτήματα και τα μειονεκτήματα που έχει η χρήση του e-banking. Επίσης, αναφέρονται οι κίνδυνοι που εγκυμονεί η χρήση του e-banking και οι τρόποι αντιμετώπισής τους. Στο τελευταίο κεφάλαιο του πρώτου μέρους, δίνονται στατιστικά στοιχεία για μια ολοκληρωμένη εικόνα για την κατάσταση που επικρατεί στη χώρα μας σχετικά με το internet e-banking . Πιο συγκεκριμένα , δίνεται η διαχρονική εξέλιξη για το σύνολο των χρηστών και απαντιούνται τα ερωτήματα του τύπου :Ποιοι χρησιμοποιούν τις υπηρεσίες e-banking και ποιες τραπεζικές υπηρεσίες χρησιμοποιούν οι χρήστες .

Στο δεύτερο μέρος της εργασίας γίνεται αναφορά στο e-banking του ταχυδρομικού ταμιευτηρίου. Γίνεται μία σύντομη ιστορική διαδρομή της συγκεκριμένης τράπεζας και στη συνέχεια θα διαπιστωθεί αν το ταχυδρομικό ταμιευτήριο παρέχει τη δυνατότητα του e-banking , πόσο καλά την παρέχει και αν έχει απήχηση. Επίσης, θα γίνει αναφορά για το ποια ασφάλεια έχει επιλέξει το ταχυδρομικό ταμιευτήριο από αυτές που προαναφέρθηκαν και κατά πόσο ενημερώνει το κοινό για τους κινδύνους που προκαλούν οι ηλεκτρονικές συναλλαγές.

ABSTRACT

The object of this essay is the e-banking in Greece from 2007-2012. The first part is a brief historical overview of the evolution of e-banking. Then given specific concepts for the understanding of the issue, the possibilities offered by the service, and what kinds of splits. Then was mentioned that the penetration of this service to our country and how the Greeks responded. Given of how many people in Greece transacting through e-banking, how many people trust and are compared with the confidence that people have in foreign trade through internet while in the next chapter are the advantages and disadvantages of the use of e - banking. Also mentions the dangers posed by the use of e-banking and ways to overcome them. The last chapter of the first part, given statistics for a complete picture of the situation in our country on the internet e-banking. More specifically, given the evolution for all users and answered the questions like: Who uses the e-banking services and banking services which utilize users.

In the second part of the project is reported in e-banking in the postal savings bank. A brief history of the bank and will then determine whether the postal savings enables the e-banking, how well they provide resonates. We will also refer to what security has selected TT than those mentioned above and how to inform the public about the risks posed by electronic transactions.

ΜΕΡΟΣ ΠΡΩΤΟ

ΚΕΦΑΛΑΙΟ 1

1.1 E-BANKING

Στα τέλη της δεκαετίας του ’90, στην Αμερική, επικρατούσε ένα παραλήρημα σχετικά με τις νέες τεχνολογίες.Όπως τελικά αποδείχτηκε, ο ενθουσιασμός αυτός οδήγησε σε μη ρεαλιστικές προσδοκίες και προβλέψεις για τη διείσδυση των νέων τεχνολογιών, οι οποίες μιλούσαν για ιδιαίτερα βραχυπρόθεσμη αποδοχή τους από το ευρύ κοινό. Ήταν συνεπώς εύκολο να παρασυρθεί και η αγορά του Internet banking που το 1999 προέβλεπε ότι το 25% των Ελλήνων θα κάνει χρήση του διαδικτύου για τη διεκπεραίωση των τραπεζικών του συναλλαγών. Είναι λογικό να μην έχουν επιβεβαιωθεί αυτές οι προβλέψεις. Είναι τόσο μεγάλος ο αριθμός των νέων δεδομένων που καλείται να αφομοιώσει ο μέσος άνθρωπος στη σύγχρονη κοινωνία της πληροφορίας που διανύουμε , που θα ήταν αδύνατο για αυτόν να ανταπεξέλθει πλήρως.

Όμως, αξιοσημείωτο είναι το γεγογός ότι η διείσδυση των νέων τεχνολογιών στην ελληνική αγορά, και κυρίως αυτή του internet e-banking , ακολουθεί συνεχώς αυξανόμενη πορεία δίχως να εμφανίζει κάποια καμπή. Άρα κρίνοντας από το αποτέλεσμα , μπορούμε να αναφέρουμε ότι όλο και περισσότεροι Έλληνες εγγράφονται κάθε μήνα στις υπηρεσίες e-banking. Γίνεται απόλυτα σαφές λοιπόν ότι η ηλεκτρονική τράπεζα μπήκε στη ζωή μας και σηματοδοτεί μία νέα εποχή στις τραπεζικές συναλλαγές μας. Βάζει τέλος στις ουρές των ταμείων και στην αναμονή των πελατών, αφού αρκεί μια συσκευή σταθερού ή κινητού τηλεφώνου, ή ένας υπολογιστής εγκατεστημένος στο σπίτι ή στο γραφείο, για να κάνουμε τις συναλλαγές με απόλυτη ασφάλεια, όλο το 24ωρο.

Δεν πρέπει να ξεχνάμε όμως ότι θα απαιτηθεί χρόνος έως ότου η ηλεκτρονική τραπεζική λάβει απολύτως μαζικό χαρακτήρα, ωστόσο όσοι από τους τραπεζικούς ομίλους έχουν ενταχθεί στο χώρο αυτό διατηρούν συγκριτικό πλεονέκτημα. Η χρήση είναι αρκετά απλή και η μεγάλη επιτυχία της κινητής τηλεφωνίας στην χώρα μας αποτελεί προάγγελο της επιτυχίας που θα έχει στην Ελλάδα η ηλεκτρονική τραπεζική. Ωστόσο, τα φυσικά δίκτυα των τραπεζών δεν αναμένεται να καταργηθούν αλλά να αλλάξουν μορφή. Θα έχουμε μικρότερα καταστήματα τα οποία θα χρησιμοποιούν τεχνολογία αιχμής. Ας μη ξεχνάμε τέλος ότι η ηλεκτρονική τραπεζική εξυπηρέτηση δεν καλύπτει όλες τις συναλλαγές.

Οι τράπεζες, μέσω της ηλεκτρονικής τραπεζικής, θέτουν στην υπηρεσία του πελάτη το ηλεκτρονικό τους κατάστημα για άμεση εξυπηρέτηση 24 ώρες το 24ωρο, 7 μέρες την εβδομάδα. Ο πελάτης δύναται να πραγματοποιεί τις αναγκαίες του συναλλαγές με απόλυτη ασφάλεια και φυσικά διατηρώντας το απόρρητό του. Οι νέες τεχνολογίες των υπολογιστών και ειδικότερα το internet , έχουν φέρει επανάσταση στον τρόπο των συναλλαγών και γενικότερα του τραπεζικού συστήματος. Το e-banking μεταφέρει την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών , παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών.

Όταν οι πιστωτικές κάρτες έκαναν την εμφάνισή τους, όλοι μιλούσαν για επανάσταση στο ηλεκτρονικό εμπόριο. Σήμερα, το e-banking υπόσχεται την επανάσταση στις συναλλαγές μας με τις τράπεζες, καθώς μεταφέρει την ίδια την τράπεζα στην οθόνη του υπολογιστή μας , μειώνοντας έτσι δραστικά το κόστος και για τις δύο πλευρές, ενώ οι καταναλωτές κερδίζουν και πολύτιμο χρόνο. Μέσω internet μπορεί κάποιος πλέον να συνδεθεί με όποια τράπεζα συνεργάζεται, να ρωτήσει για το υπόλοιπο του λογαριασμού του, να πληρώσει την πιστωτική του κάρτα και να υπολογίσει τους τόκους καταθέσεων. Αυτές είναι μόνο ορισμένες από τις συναλλαγές που μπορεί να πραγματοποιηθούν από το σπίτι. Αρκετές τράπεζες προσφέρουν και άλλες υπηρεσίες , ακόμα και εκτέλεση εντολών για το χρηματιστήριο. Αυτό, καθώς φαίνεται είναι μόνο η αρχή. Την πρόσβαση στο internet διεκδικούν και άλλες συσκευές εκτός από τον ηλεκτρονικό υπολογιστή, όπως είναι τα μικρά ηλεκτρονικά organizers, ακόμα και τα κινητά τηλέφωνα. Έτσι, η πρόσβαση στις τραπεζικές συναλλαγές γίνονται πλέον εύκολα, γρήγορα και από παντού.

Με την εφαρμογή της ηλεκτρονικής τραπεζικής συναλλαγής, μία τράπεζα μπορεί να πετύχει διεύρυνση της παρουσίας της και να προσελκύσει νέους πελάτες, καθώς υποψήφιοι πελάτες της δεν είναι μόνο οι γείτονες του νέου καταστήματος, αλλά ολόκληρος ο κόσμος. Η εξοικονόμηση χρόνου είναι ένας από τους βασικότερους λόγους πάνω στην οποία θεμελιώνεται η αναγκαιότητα της χρήσης του e-banking , καθώς οι ηλεκτρονικές συναλλαγές γίνονται απλά μέσω του ηλεκτρονικού υπολογιστή, χωρίς ανάγκη μετακίνησης και με αποφυγή της γραφειοκρατίας και της ουράς.

Το διαδίκτυο προσφέρει πολλαπλές δυνατότητες εμπορικής ανάπτυξης των ηλεκτρονικών συναλλαγών. Με το ηλεκτρονικό χρήμα να αποτελεί , εδώ και πολύ καιρό, μια καθημερινή συνήθεια ο δρόμος για ριζοσπαστικές αλλαγές έχει ανοίξει. Υπάρχει βεβαίως , το κρίσιμο θέμα της ασφάλειας των συναλλαγών. Η πρόοδος είναι σημαντική και ραγδαία. Χρειάζεται όμως περισσότερη δουλειά για να πεισθούν όσοι δεν έχουν εμπειρία των ηλεκτρονικών συναλλαγών. Παράλληλα η καλύτερη παρακολούθηση και η συνεχής εξέλιξη των ηλεκτρονικών συστημάτων υποστηρίζει την εμπέδωση σχέσεων εμπιστοσύνης με τους πελάτες. **(Γούναρη Αναστασία2009)**

1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΚΑΙ

ΕΞΕΛΙΞΗ ΤΟΥ E-BANKING

Για να υπάρξει το e-banking απαραίτητο συστατικό στοιχείο είναι η δυνατότητα πρόσβασης στο διαδίκτυο. Όλα ξεκίνησαν στα τέλη της δεκαετίας του ’60 , όταν ο οργανισμός ARPA (Advanced Research Projects Agency) στις ΗΠΑ , προσανατολισμένος σε ερευνητικά προγράμματα υψηλής τεχνολογίας, ξεκίνησε μια ερευνητική δραστηριότητα σχετικά με τα δίκτυα, δημιουργώντας το ARPAnet το οποίο αποτέλεσε πρόδρομο του internet. Το 1971, μόνον τέσσερις υπερυπολογιστές ήταν συνδεδεμένοι στο δίκτυο. (**Αγγέλης Β., 2005)**

Σταθμός στην ιστορία του e-banking ήταν και τα τέλη της δεκαετίας του ’80 όταν οι μεγαλύτερες τράπεζες των Ηνωμένων Πολιτειών εισήγαγαν την έννοια του Home Banking . Με το Home Banking οι τράπεζες έδιναν τη δυνατότητα στους πελάτες τους να πραγματοποιούν τις βασικές τραπεζικές τους συναλλαγές από το σπίτι μέσω του ηλεκτρονικού υπολογιστή. Οι τράπεζες έχοντας αναπτύξει τα κατάλληλα δίκτυα και παρέχοντας στους πελάτες τους δωρεάν λογισμικό, στόχευαν να εξαπλωθεί η καινούργια αυτή υπηρεσία στους πλέον απαιτητικούς και εύπορους πελάτες. Ο κύκλος ζωής του Home Banking ήταν σύντομος καθώς στα μέσα της δεκαετίας του ’90 επικράτησε το internet e-banking και γενικότερα το e-banking.

Το σημαντικότερο πλεονέκτημα που προσέφερε το e-banking σε σχέση με τον προκάτοχο του ήταν το γεγονός ότι οι τράπεζες δεν απαιτούνταν πλέον να συντηρούν ιδιωτικά δίκτυα τα οποία συνεπάγονταν υψηλό κόστος. Επιπλέον , ούτε οι πελάτες χρειάζονταν να εφοδιάζονται με κάποιο ιδιαίτερο λογισμικό ώστε να έχουν πρόσβαση στο σύστημα της τράπεζας. Το internet ως ανοιχτό σύστημα αποτέλεσε πρόκληση για τις τράπεζες οι οποίες διέκριναν την ευκαιρία να διευρύνουν μέσω αυτού την πελατειακή τους βάση. Σταθμός στην ιστορία του διαδικτύου αποτελεί το έτος 1993 οπότε και κατασκευάστηκε ο παγκόσμιος ιστός (World Wide Web) στο CERN της Ελβετίας. Ο παγκόσμιος ιστός συνέβαλε στη δημιουργία μιας ευρύτερης και πιο εύκολα προσβάσιμης δικτυακής υποδομής . Το 1994 αναπτύχθηκε ο Netscape Navigator , ο πρώτος περιηγητής του διαδικτύου που καθιστούσε πλέον δυνατή την περιήγηση στο internet οποιουδήποτε διέθετε έναν ηλεκτρονικό υπολογιστή και ένα modem. Τον Οκτώβριο του 1995 εγκαινιάστηκε στην Αμερική η πρώτη ηλεκτρονική τράπεζα , η Security First Network Bank , η οποία χωρίς να διαθέτει δίκτυο καταστημάτων εξυπηρετούσε την πελατεία της μόνο μέσα από το διαδίκτυο.**(Guttmann Robert, Palgrave Macmillan,2003)**

Στην Ελλάδα η πρώτη εφαρμογή e-banking παρουσιάστηκε τον Φεβρουάριο του 1998. Την καινοτομία αυτή εισήγαγε στην Ελλάδα , που αριθμούσε τότε λίγο περισσότερους από 100.000 συνδρομητές internet , η Εγνατία Τράπεζα παρουσιάζοντας την ολοκληρωμένη υπηρεσία Web Teller μέσω της οποίας οι αταναλωτές είχαν τη δυνατότητα να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω του internet. **(Περιοδικό Ram ,Ιούνιος 2000)**

Η τάση αυτή συνεχίστηκε και στο μέλλον. Τα αναμφισβήτητα πλεονεκτήματα των νέων τραπεζών φάνηκε ότι είχαν υπερκτιμηθεί. Ο εντυπωσιακός ρυθμός ανάπτυξης της πελατείας των νέων τραπεζών , επισκιάστηκε από το γεγονός ότι οι πελάτες των ηλεκτρονικών τραπεζών έπρεπε τελικά να καταφύγουν και πάλι τις παραδοσιακές τράπεζες, στα καταστήματα, για να καλύψουν αυτά που από τη φύση τους οι ηλεκτρονικές τράπεζες δε θα μπορούσαν να εξυπηρετήσουν. (πηγή: Περιοδικό RAM «Οι τράπεζες στο χορό του internet», Ιούνιος 2000).

Παράλληλα οι παραδοσιακές τράπεζες, οι οποίες μέσα από τα καταστήματα προωθούσαν προϊόντα και υπηρεσίες και εξυπηρετούσαν τις συναλλαγές των πελατών τους, ένιωσαν απειλή, καθώς διαπίστωσαν ότι τα τμήματα πελατών τους άρχιζαν να στρέφονται προς τις τράπεζες νέας μορφής. Οι τράπεζες αυτές έπρεπε κάτι να κάνουν κι έτσι με γρήγορα βήματα άρχισαν να αναπτύσσουν εναλλακτικά , ως προς τα καταστήματα , δίκτυα εξυπηρέτησης , στα πρότυπα των ηλεκτρονικών τραπεζών. Σε αρκετές περιπτώσεις αναγκάστηκαν να προβούν σε ριζική αναθεώρηση των πληροφοριακών συστημάτων και ορισμένων επιχειρησιακών λειτουργιών τους , για να ανταποκρίνονται στα αιτήματα των πελατών που τους διαβιβάζονταν ηλεκτρονικά.

Τελικά οι παραδοσιακές και οι ηλεκτρονικές τράπεζες άρχισαν να συγκλίνουν προς ένα τρόπο λειτουργίας που δικαίως δίνει περισσότερη έμφαση στη συνέργεια ανάμεσα στα φυσικά και ηλεκτρονικά δίκτυα, καθώς αναγνωρίστηκε η διπλωματικότητα τους. Τα ηλεκτρονικά δίκτυα μπορούν άριστα να εξυπηρετήσουν επαναλαμβανόμενες τραπεζικές – χρηματοοικονομικές εργασίες, να πληροφορήσουν να ειδοποιήσουν τον πελάτη, να τον διευκολύνουν στην προσωπική του χρηματοοικονομική διαχείριση , ενώ το δίκτυο καταστημάτων παραμένει αναντικατάστατο στην προσέγγιση του πελάτη για την ανάλυση των αναγκών του, την επεξήγηση πολύπλοκων προϊόντων, την εκπαίδευση της πελατείας σε νέα προϊόντα και δίκτυα και τέλος στην εξυπηρέτηση όσων συναλλαγών απαιτούν ακόμη τη φυσική παρουσία του πελάτη στο κατάστημα.

Αποτελώντας την εξαίρεση που δεν αναιρεί αλλά επιβεβαιώνει τον κανόνα, λειτουργούν και σήμερα αποκλειστικά ηλεκτρονικές τράπεζες, απευθυνόμενες κυρίως σε συγκεκριμένα τμήματα πελατείας και παραμένουν επιτυχείς στους τομείς που έχουν επιλέξει να δραστηριοποιούνται. Το σημερινό πρότυπο λειτουργίας των δικτύων διανομής των τραπεζικών προϊόντων και υπηρεσιών, προσομοιάζει προς την εικόνα μιας ζυγαριάς. Σαφώς το βάρος με την έννοια της δημιουργίας κερδοφορίας βρίσκεται προς το μέρος

του δικτύου καταστημάτων, αλλά με την πάροδο του χρόνου αρχίζει να αποκτά ειδικό βάρος και κρίσιμη μάζα, η πλευρά της ηλεκτρονικής τραπεζικής ως εναλλακτικού δικτύου πώλησης και εξυπηρέτησης της πελατείας.

Οποιαδήποτε προσπάθεια να προβλεφθεί η χρονική στιγμή κατά την οποία η ζυγαριά θα γείρει προς την πλευρά της ηλεκτρονικής τραπεζικής με παράλληλη ουσιαστική συρρίκνωση του ρόλου των καταστημάτων , είναι παρακινδυνευμένη. Βέβαια το σημερινό τραπεζικό σύστημα έχει αρκετές διαφορές από προηγούμενες δεκαετίες. Σίγουρα δε μένει αμέτοχο στην εξέλιξη της ηλεκτρονικής τραπεζικής, καθώς πέρα από το e-banking , φιλοξενεί όλο και περισσότερα ηλεκτρονικά δίκτυα , συνήθως σε κάποιο προθάλαμο αυτό-εξυπηρέτησης, με συσκευές όπως ATM , η τηλεφωνική συσκευή για απευθείας σύνδεση με την Υπηρεσία Τηλεφωνικής Εξυπηρέτησης και οι ειδικές μονάδες για πληρωμή λογαριασμών με μετρητά. Ακόμα, το προσωπικό του καταστήματος έχει προσανατολιστεί στο νέο του ρόλο, την πώληση προιόντων και εξυπηρέτηση πελατείας με τη χρήση των νέων τεχνολογιών, τόσο κατά την διάρκεια της συνομιλίας με τον πελάτη, όσο και κατά την διεκπεραίωση εργασιών εντός του ίδιου του καταστήματος.

(Hilmon Richard , Wong Kane,2000)

Συμπερασματικά μπορούμε να αναφέρουμε τα εξής:

- Οι αμιγώς ηλεκτρονικές τράπεζες αποτέλεσαν μια αφετηρία που αποδείχθηκε στην πράξη και προορισμός, αφού η μετέπειτα πορεία τους και η περαιτέρω ανάπτυξή τους, περνά σχεδόν υποχρεωτικά από τη συνεργασία τους με ένα δίκτυο καταστημάτων.

- Η ηλεκτρονική τραπεζική εξυπηρέτηση παραμένει ένας τελικός προορισμός και η ταχύτητα επίτευξης της εξαρτάται σε μεγάλο βαθμό από το ρυθμό διείσδυσης των νέων τεχνολογιών στην καθημερινή ζωή. Παράλληλα όμως, αποτελεί και την αφετηρία για βελτιστοποίηση των επιχειρησιακών λειτουργιών στις παραδοσιακές τράπεζες , οι οποίες αναγκαστικά πλέον προσδένονται στο άρμα της ηλεκτρονικής τραπεζικής και πρέπει να αποκτήσουν εσωτερική αποτελεσματικότητα. Αποτελεσματικότητα που να τους επιτρέπει να εκτελούν εσωτερικές εργασίες με ταχύτητα και αμεσότητα αντίστοιχη εκείνης, με την οποία ο πελάτης συνεργάζεται με την τράπεζα μέσα από τα ηλεκτρονικά δίκτυα. Καθώς ο ανταγωνισμός βρίσκεται τόσο μακριά όσο το πάτημα ενός κουμπιού στον υπολογιστή ή στην τηλεφωνική συσκευή, η σύγχρονη πρόκληση για τις τράπεζες παραμένει η οργάνωσή τους, έτσι ώστε να ανταποκρίνονται άμεσα στη δημιουργία νέων δικτύων, νέων προϊόντων και υπηρεσιών. **(Δελτίο Ελληνικής Ένωσης , Ιούλιος-Σεπτέμβριος 2003)**

ΤΙ ΕΙΝΑΙ ΤΟ E-BANKING

Η ηλεκτρονική τραπεζική e-banking είναι ένα αναπόσπαστο κομμάτι του ηλεκτρονικού εμπορίου το οποίο περικλείει όλες τις συναλλαγές που γίνονται μέσω ηλεκτρονικών δικτύων. Τα ηλεκτρονικά κανάλια χρησιμοποιούνται τόσο για συναλλαγές μεταξύ επιχειρήσεων (business to business) αλλά και μεταξύ επιχειρήσεων και καταναλωτών (business to costumer), όπως η αγορά και η πληρωμή αγαθών. Το e-banking είναι μέρος του e-commerce διότι οι τράπεζες συμμετέχουν σε επιχειρηματικές συναλλαγές μέσω ηλεκτρονικών μέσων. Με άλλα λόγια το e-banking δεν είναι απλώς ένα τραπεζικό προϊόν , αλλά η ηλεκτρονική διεκπεραίωση των τραπεζικών συναλλαγών και η ηλεκτρονική διεπαφή μεταξύ των τραπεζών και των πελατών τους. **(Deutsche Bundesbank, December 2000)**

1.3 ΟΡΙΣΜΟΣ

Οι τράπεζες ήταν εδώ και αρκετά χρόνια από τους πρωτοπόρους οργανισμούς που χρησιμοποίησαν ηλεκτρονικά κανάλια για την επικοινωνία και τις συναλλαγές εγχώριων και διασυνοριακών πελατών τους. Με την ανάπτυξη του internet και του περιεχομένου του παγκόσμιου ιστού (world wide web) κατά το δεύτερο μισό της δεκαετίας του ’90 , οι τράπεζες αξιοποίησαν τις δυνατότητες της τεχνολογίας και άρχισαν να προσφέρουν αρκετά από τα προϊόντα και τις υπηρεσίες τους μέσω internet . Ο τρόπος αυτός παροχής των τραπεζικών υπηρεσιών είναι γνωστός με την ονομασία ηλεκτρονική τραπεζική και περιλαμβάνει την παροχή προϊόντων και υπηρεσιών λιανικής τραπέζης , τραπεζικών προϊόντων και υπηρεσιών σε μεγάλους πελάτες και επιχειρήσεις καθώς και υπηρεσίες ηλεκτρονικών πληρωμών με την χρήση ηλεκτρονικών καναλιών διανομής. **(Ramirez Carl, Diane publishing co.,1998)**

Ο διεθνής όρος internet e-banking αποδίδεται στην ελληνική ως διαδικτυακή τράπεζα, όμως πιο συχνά χρησιμοποιείται ισοδύναμα ο όρος Ηλεκτρονική Τράπεζα ή e-banking. Παρά το γεγονός ότι συχνά δε γίνεται διάκριση μεταξύ των όρων internet e-banking και e-banking , ο ένας αποτελεί ειδικότερη κατηγορία του άλλου.

Πιο συγκεκριμένα με τον όρο Ηλεκτρονική τραπεζική εννοούμε όλες εκείνες τις υπηρεσίες που παρέχουν οι τράπεζες χωρίς τη φυσική παρουσία του πελάτη στο υποκατάστημα τους. Εναλλακτικά θα μπορούσαμε να ορίσουμε την ηλεκτρονική τράπεζα ως την αυτοματοποιημένη παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών χρηματοοικονομικής φύσης , απευθείας στους πελάτες μέσω ηλεκτρονικών, αλληλεπιδραστικών καναλιών επικοινωνίας.

Βασικότερες υπηρεσίες e-banking:

- Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς
- Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ίδιου 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 αγοροπωλησίας μετοχών
- Ενημέρωση για τη κίνηση των προσωπικών αμοιβαίων κεφαλαίων
- Δυνατότητα υποβολής αιτήσεων εμβασμάτων
- Αλλαγή του απόρρητου κωδικού Pin
- Προσωπικά μηνύματα
- Υπόλοιπα πιστωτικών καρτών
- Κινήσεις και πληρωμές δανείων
- Μεταφορά χρημάτων μεταξύ προσωπικών λογαριασμών

1.4 ΕΙΔΗ E-BANKING

Τα είδη του e-banking με κριτήριο το μέσω που χρησιμοποιείται για τη διενέργεια των τραπεζικών συναλλαγών είναι:

A.INTERNET BANKING

Το Internet banking, το οποίο συχνά ονομάζεται και online banking, χρησιμοποιεί το Internet ως μέσο διεξαγωγής τραπεζικών δραστηριοτήτων. Για να μπορέσει ένας χρήστης να χρησιμοποιήσει τις υπηρεσίες e- banking πρέπει να διαθέτει ηλεκτρονικό υπολογιστή και να έχει σύνδεση στο διαδίκτυο. Ωστόσο σε ορισμένες περιπτώσεις απαιτούνται περισσότερες συσκευές ασφαλείας όπως εγκατάσταση ειδικού λογισμικού ασφαλείας ή ψηφιακό πιστοποιητικό. Ο πελάτης μιας τράπεζας, μέσω του Internet banking, έχει τη δυνατότητα να εκτελεί, σχεδόν όλες τις τραπεζικές συναλλαγές και να λαμβάνει την πληροφόρησης που επιθυμεί .Μεγάλη επένδυση γίνεται και στο θέμα της ασφάλειας που είναι ιδιαίτερα κρίσιμο για την αξιοπιστία των ηλεκτρονικών τραπεζικών συστημάτων και που θα αναλυθεί παρακάτω.

Β.PHONE BANKING

Μέσω του Phone Banking, η Τράπεζα, γίνεται πλέον προσιτή από το σπίτι, το γραφείο, το αυτοκίνητο, ενώ ταυτόχρονα διατηρείται ως ένα βαθμό και η παραδοσιακή τραπεζική σχέση μεταξύ υπαλλήλου και πελάτη. Συσκευές όπως τα κινητά τηλέφωνα ή τα PDAs που είναι εφοδιασμένες με την τεχνολογία WAP και μπορούν να συνδεθούν στο Internet μπορούν να παρέχουν στους χρήστες τους τη δυνατότητα διεξαγωγής τραπεζικών συναλλαγών.

Οι υπηρεσίες που προσφέρονται μέσω phone banking χωρίζονται σε δύο κατηγορίες:

- αυτές που διεκπεραιώνονται από πράκτορες (agents) τηλεφωνικού κέντρου
- αυτές που διεκπεραιώνονται αυτόματα μέσω συστημάτων αναγνώρισης φωνής

Το phone banking, δίνει τη δυνατότητα στον πελάτη μίας τράπεζας, να έχει στη διάθεση του, σχεδόν όλες τις συναλλαγές που έχει και μέσω Internet banking.

Γ. MOBILE BANKING

Πολλές φορητές συσκευές όπως τα κινητά τηλέφωνα, οι φορητές ατζέντες (PDAs) και οι υπολογιστές παλάμης (Hand-held PC's) πρόσβαση στο Internet μέσω της τεχνολογίας WAP. Έτσι οι χρήστες μπορούν να εκτελέσουν Internet Banking και από άλλες συσκευές εκτός του PC. Αυτού του είδους οι συναλλαγές περιγράφονται με τον όρο mobile Banking.

Το Mobile banking παρά τα πλεονεκτήματα, τις ευκολίες και την ευχρηστία του, δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό και συνεπώς δεν έχει εδραιωθεί ακόμα σε σχέση με το internet και το phone banking. Αν λάβουμε υπόψη όμως την ανάπτυξη της κινητής τηλεφωνίας στην εγχώρια αγορά, τότε το Mobile banking έχει όλες τις προοπτικές να αποτελέσει στο άμεσο μέλλον ένα ευρέως χρησιμοποιούμενο κανάλι πραγματοποίησης ηλεκτρονικών συναλλαγών.

Μεγάλη σημασία δίνεται επίσης σε ότι αφορά το Mobile banking στην ασφάλεια των συναλλαγών και στην πιστοποίηση του χρήστη .**(Β.Αγγελής,2005)**

1.5 ΔΥΝΑΤΟΤΗΤΕΣ E-BANKING

Οι υπηρεσίες που προσφέρει το e-banking χωρίζονται σε τέσσερις μεγάλες διακριτές κατηγορίες:

- Οικονομικές συναλλαγές
- Πληροφοριακές συναλλαγές
- Αιτήσεις
- Άλλες υπηρεσίες

ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Οι οικονομικές συναλλαγές καλύπτουν όλη την γκάμα των συναλλαγών που μπορεί να κάνει ο συναλλασσόμενος και σε ταμείο της τράπεζας. Οι συναλλαγές αυτές αφορούν ενδοτραπεζικές συναλλαγές όπως μεταφορές κεφαλαίων , πληρωμή καρτών και δανείων, συναλλαγές που υλοποιούνται ύστερα από διμερείς συμφωνίες της τράπεζας με τρίτο οργανισμό , όπως πληρωμές λογαριασμών εταιριών σταθερής και κινητής τηλεφωνίας και συναλλαγές που υλοποιούνται στα πλαίσια διατραπεζικών συστημάτων κυρίως της ΔΙΑΣ ΑΕ , αλλά και άλλων όπως το σύστημα ΕΡΜΗΣ.

Μεταφορές εντός τράπεζας :

Οι μεταφορές εντός τράπεζας διακρίνονται σε μεταφορές σε **λογαριασμό ιδίου** και σε μεταφορές **λογαριασμό τρίτου.**

Μεταφορές σε λογαριασμό ιδίου: Στις περισσότερες των περιπτώσεων οι μεταφορές εντός τράπεζας εκτελούνται on line. Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό πίστωσης. Στις μεταφορές μεταξύ των λογαριασμών ιδίου, ο χρήστης δε χρειάζεται να πληκτρολογεί τους αριθμούς λογαριασμών. Πολλές τράπεζες πέραν των αριθμών λογαριασμών που εμφανίζουν στα σύνθετα πεδία εμφανίζουν και το τρέχον διαθέσιμο υπόλοιπο , διευκολύνοντας τον χρήστη να γνωρίζει ανα πάσα στιγμή το υπόλοιπο αυτών.

Ακολούθως, πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Όταν η ημερομηνία είναι η τρέχουσα, η συναλλαγή εκτελείται άμεσα. Ο χρήστης έχει την πολυτέλεια και μεταχρονολογημένων μεταφορών , γεγονός που τον διευκολύνει να προγραμματίζει τις πληρωμές του. Οι forward εντολές είναι ένα σημαντικό πλεονέκτημα του e-banking . Το τελευταίο που καταχωρεί ο χρήστης είναι ένας κωδικός επιβεβαίωσης της συναλλαγής που προκύπτει είτε από κάποιο token είτε από λίστα tan είτε από extra pin. Στη συνέχεια επιλέγει το button << εκτέλεση>>. Στην οθόνη εμφανίζονται όλα τα στοιχεία που καταχώρησε ο πελάτης. Εφόσον ο πελάτης επιβεβαιώσει τα στοιχεία, εκτελείται η συναλλαγή. Μετά το πέραν της συναλλαγής, ο χρήστης μπορεί να εκτυπώσει την εντολή μεταφοράς, η οποία υπέχει θέση παραστατικού της συναλλαγής. **(Αγγέλης, 2005).**

Μεταφορές σε λογαριασμό τρίτου: Και οι μεταφορές σε λογαριασμό τρίτου, εντός τράπεζας εκτελούνται on line. Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης. Στις μεταφορές από λογαριασμό του , ο χρήστης δε χρειάζεται να πληκτρολογεί τον αριθμό λογαριασμό του. Στη συνέχεια, ο χρήστης καλείται να πληκτρολογήσει τον αριθμό λογαριασμό πίστωσης. Οι τράπεζες προκειμένου να διασφαλίσουν όσο περισσότερο μπορούν τον πελάτη διενεργούν έλεγχο ψηφίου ελέγχου (check digit). Ο έλεγχος αυτός, εξασφαλίζει ότι ο αριθμός λογαριασμού που πληκτρολογήθηκε είναι έγκυρος. Ακολούθως, πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Ο χρήστης έχει την πολυτέλεια και μεταχρονολογημένων μεταφορών, γεγονός που τον διευκολύνει να προγραμματίζει τις πληρωμές του. Οι forward εντολές είναι πολύ σημαντικό πλεονέκτημα του e-banking.

Εμβάσματα εσωτερικού: Η πλειοψηφία των εμβασμάτων εσωτερικού σε νόμισμα ευρώ διεκπεραιώνεται μέσω του διατραπεζικού συστήματος DIASTRANSFER. Στο σύστημα αυτό συμμετέχουν όλες σχεδόν οι εγχώριες τράπεζες. Για την αποστολή εμβάσματος, ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης. Στη συνέχεια επιλέγει την τράπεζα δικαιούχου από ένα σύνθετο πεδίο που περιέχει όλες τις τράπεζες του εσωτερικού. Έπειτα, ο πελάτης καλείται να πληκτρολογήσει τον αριθμό του λογαριασμού δικαιούχου. Οι τράπεζες προκειμένου να διασφαλίσουν όσο περισσότερο μπορούν τον πελάτη , διενεργούν έλεγχο ψηφίο ελέγχου (CHECK DIGIT). Ο έλεγχος αυτός, εξασφαλίζει ότι ο αριθμός του λογαριασμού που πληκτρολογήθηκε είναι έγκυρος. Επόμενο στοιχείο που καταχωρείται είναι η επωνυμία του δικαιούχου. Ακολούθως ο πελάτης πληκτρολογεί το ποσό που θέλει να μεταφέρει , την αιτιολογία και επιλέγει τον υπόχρεο εξόδων από ένα σύνθετο πεδίο. Τέλος πληκτρολογεί την ημερομηνία που επιθυμεί να γίνει η πληρωμή και καταχωρεί ένα κωδικό επιβεβαίωσης της συναλλαγής.

Πληρωμές δανείων: Η πληρωμή δανείου είναι ουσιαστικά συναλλαγή μεταφοράς εντός τράπεζας και όπως στις λοιπές των περιπτώσεων μεταφορών εντός τράπεζας εκτελείται On line. Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και το λογαριασμό δανείου. Ακολούθως, πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Το τελευταίο που καταχωρεί ο

χρήστης είναι ένας κωδικός επιβεβαίωσης της συναλλαγής που προκύπτει είτε από κάποιο token είτε από λίστα tan είτε από extra pin .

Πληρωμές πιστωτικών καρτών: Οι πληρωμές πιστωτικών καρτών διακρίνονται σε τρεις κατηγορίες.

- Πληρωμή πιστωτικής κάρτας ιδίου
- Πληρωμή πιστωτικής κάρτας τρίτου
- Πληρωμή πιστωτικής κάρτας άλλης τράπεζας

Οι πληρωμές πιστωτικών καρτών ιδίου γίνονται αυθημερόν. Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και τον αριθμό της πιστωτικής κάρτας που επιθυμεί να πληρώσει. Στις πληρωμές καρτών ιδίου , ο χρήστης δε χρειάζεται να πληκτρολογεί τους αριθμούς λογαριασμών και καρτών. Ακολούθως, πληκτρολογεί το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Το τελευταίο που καταχωρεί ο χρήστης είναι ένας κωδικός επιβεβαίωσης της συναλλαγής που προκύπτει είτε από κάποιο token είτε από λίστα tan είτε από extra pin. Ομοίως εκτελούνται και οι πληρωμές πιστωτικής κάρτας τρίτου. Όσον αφορά την πληρωμή πιστωτικής κάρτας άλλης τράπεζας αυτή διεκπεραιώνεται μέσω του διατραπεζικού συστήματος Dias transfer. Η εκτέλεσή της γίνεται παρόμοια με την πληρωμή πιστωτικής κάρτας ιδίου με τη διαφορά ότι ο χρήστης πρέπει να επιλέξει την τράπεζα δικαιούχου.

Πληρωμές δημοσίου: Πολλές υποχρεώσεις ενός πελάτη έναντι του δημοσίου μπορούν να ολοκληρώνονται μέσω του e-banking. Οι περισσότερες εξ αυτών διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIAS DEBIT. Οι πληρωμές δημοσίου έχουν συμπληρώσει το πακέτο των ηλεκτρονικών πληρωμών καθιστώντας το ελκυστικό για αρκετές ομάδες επαγγελματιών στη χώρα μας.

ΦΠΑ: Η πληρωμή του φόρου προστιθέμενης αξίας γίνεται αποκλειστικά μέσω τραπεζών. Ο υπόχρεος πρέπει πρώτα να έχει κάνει την περιοδική δήλωση φπα μέσω του ιστότοπου www.taxisnet.gr του υπουργείου Οικονομικών και στη συνέχεια να τελέσει την αντίστοιχη πληρωμή στην τράπεζα. Σε περίπτωση που δεν έχει γίνει δήλωση στο taxis net η πληρωμή φπα επιστρέφεται στον οφειλέτη.

Για την πληρωμή φπα , ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης. Στη συνέχεια, πληκτρολογεί τον αριθμό του φορολογικού μητρώου (ΑΦΜ) του υπόχρεου. Οι τράπεζες προκειμένου να διασφαλίσουν όσο περισσότερο μπορούν τον πελάτη διενεργούν έλεγχο ψηφίο ελέγχου. Ο έλεγχος αυτός εξασφαλίζει ότι ο ΑΦΜ που πληκτρολογήθηκε είναι έγκυρος. Έπειτα, ο πελάτης καλείται να πληκτρολογήσει την αιτιολογία της πληρωμής (π.χ. ΦΠΑ μηνός Ιανουαρίου). Ακολούθως, πληκτρολογεί το

ποσό που θέλει να πληρώσει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Το τελευταίο που καταχωρεί ο χρήστης είναι ένας κωδικός επιβεβαίωσης της συναλλαγής και έπειτα επιλέγει «ΕΚΤΕΛΕΣΗ».

Καθώς έχει αποδειχθεί και από έρευνες , στο e-banking η πληρωμή ΦΠΑ όπως και αυτή του ΙΚΑ είναι από τις πλέον δημοφιλείς. Για το λόγο αυτό και προκειμένου αν διευκολύνουν τους πελάτες τους , αρκετές τράπεζες πρόσθεσαν επιπλέον λειτουργικότητα και κατέστησαν το προιόν τους περισσότερο ελκυστικό. Ομοίως με την πληρωμή ΦΠΑ εκτελούνται και οι εργοδοτικές εισφορές ΙΚΑ , ΤΕΒΕ κ.α.

Πληρωμές λογαριασμών ΔΕΚΟ: Σχεδόν όλες οι μονάδες ηλεκτρονικής τραπεζικής της χώρας παρέχουν στους πελάτες τους ολοκληρωμένο πακέτο πληρωμών λογαριασμών ΔΕΚΟ.

ΟΤΕ: Η πληρωμή ΟΤΕ εκτελείται πάντα την ημερομηνία που επιθυμεί ο χρήστης. Η εξόφληση λογαριασμών ΟΤΕ διεκπεραιώνεται μέσω του διατραπεζικού συστήματος DIAS DEBIT . Για την πληρωμή ΟΤΕ ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης. Στη συνέχεια, πληκτρολογεί τον κωδικό λογαριασμού που αναγράφεται στο λογαριασμό τηλεπικοινωνιακών τελών που λαμβάνει από τον Οργανισμό. Οι τράπεζες προκειμένου να διασφαλίσουν όσο περισσότερο μπορούν τον πελάτη διενεργούν έλεγχο ψηφίο ελέγχου. Ο έλεγχος αυτός εξασφαλίζει ότι ο κωδικός λογαριασμού που πληκτρολογήθηκε είναι έγκυρος. Ακολούθως, πληκτρολογεί το ποσό που θέλει να πληρώσει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Το τελευταίο που καταχωρεί ο χρήστης είναι ένας κωδικός επιβεβαίωσης της συναλλαγής και έπειτα επιλέγει «εκτέλεση».

Ειδικά για τον ΟΤΕ υπάρχει και εντολή πληρωμής λογαριασμών μεγάλων πελατών. Η συγκεκριμένη συναλλαγή διατίθεται από λίγα e-banking sites. Η μόνη διαφορά έγκειται στο ότι η συναλλαγή απευθύνεται σε περιορισμένο αριθμό εταιριών που έχουν χαρακτηριστεί ως μεγάλοι πελάτες από τον Οργανισμό τηλεπικοινωνιών και οι οποίες λαμβάνουν λογαριασμό τηλεπικοινωνιακών υπηρεσιών.

Πληρωμές σταθερής και κινητής τηλεφωνίας: Κάποιες από τις πληρωμές σταθερής και κινητής τηλεφωνίας διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIAS DEBIT ενώ άλλες αποτελούν προϊόν διμερούς συμφωνίας μεταξύ τραπεζών και εταιριών. Κατά τα άλλα οι πληρωμές σταθερής και κινητής τηλεφωνίας εκτελούνται με παρόμοιο τρόπο με τις πληρωμές λογαριασμών ΔΕΚΟ.

ΚΑΤΑΣΤΑΣΗ ΕΝΤΟΛΩΝ

Ένα internet banking που σέβεται τον εαυτό του απαιτείται να δίνει στον πελάτη του εύκολη ενημέρωση για το status των εντολών οικονομικής φύσης. Μια εντολή που καταχωρείται μέσω του internet μπορεί να περάσει από διάφορες καταστάσεις μέχρι να καταλήξει στην οριστική. Για το λόγο αυτό, ο χρήστης του e-banking καλό είναι να ενημερώνεται και να παρακολουθεί συχνά το status των συναλλαγών του ώστε να γνωρίζει ανά πάσα στιγμή ποιες εντολές του δεν εκτελέστηκαν.

Οι καταστάσεις εντολών είναι οι εξής:

- Προς επεξεργασία
- Ακυρωμένη από χρήστη
- Ακυρωμένη από τράπεζα
- Ακυρωμένη από οργανισμό
- Επιβεβαιωμένη από τράπεζα
- Εκτελεσμένη
- Μερικώς εκτελεσμένη

Ο χρήστης επιλέγει αν επιθυμεί να δει όλες του τις εντολές ή εντολές ενός συγκεκριμένου χρονικού διαστήματος. Προαιρετικά , μπορεί να επιλέξει και άλλα κριτήρια όπως κατάσταση εντολής , είδος εντολής και τύπος εντολής.

Προμήθειες συναλλαγών: Προτού ένας χρήστης ξεκινήσει να κάνει κάποια οικονομική συναλλαγή μέσω e-banking πρέπει να ενημερώνεται για τις προμήθειες των συναλλαγών. Οι τράπεζες οφείλουν να έχουν σε δημόσια θέα το τιμολόγιό τους. Λόγω μεγάλου ανταγωνισμού ενδέχεται οι τράπεζες να προβαίνουν συχνά σε αναπροσαρμογές των τιμολογίων τους. Ένα βασικό πλεονέκτημα των ηλεκτρονικών συναλλαγών είναι οι μειωμένες τους προμήθειες.

Σήμερα, όλες οι τράπεζες δε χρεώνουν προμήθεια στις μεμονωμένες μεταφορές κεφαλαίων εντός τράπεζας. Συνήθως δε χρεώνεται προμήθεια και στις πληρωμές δημοσίου από τις περισσότερες τράπεζες. Από εκεί και πέρα υπάρχουν μικρές προμήθειες για την εξόφληση λογαριασμών οργανισμών που ξεκινούν από λίγα λεπτά (0,30 Ε) και μπορούν να φτάσουν μέχρι και ένα ευρώ , προμήθεια ανά συναλλαγή για μαζικές πληρωμές και μισθοδοσίες αλλά και για πάγιες εντολές. Η μεγαλύτερη προμήθεια παρακρατείται στα εμβάσματα εσωτερικού και εξωτερικού. Η προμήθεια μπορεί να ξεκινά από 1,50 ευρώ και να φτάσει σε ορισμένες περιπτώσεις μέχρι και 20 ευρώ. Η τιμολογιακή πολιτική για τα εμβάσματα είναι στη πλειονότητα των περιπτώσεων κλιμακωτή ανάλογα με το ποσό μεταφοράς και εξαρτάται από το αν οι τράπεζες περιλαμβάνουν σε αυτήν και τα έξοδα του εμβάσματος ή επιβαρύνουν με αυτά τον πελάτη τους.

ΠΛΗΡΟΦΟΡΙΑΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Ιδιαίτερα σημαντικό είναι το κομμάτι των πληροφοριακών συναλλαγών που καλύπτει το e-banking. Ο χρήστης μπορεί να πάρει πληροφορίες για όλα τα προϊόντα που διαθέτει η τράπεζα. Οι συναλλαγές αυτές διακρίνονται σε τέσσερις κατηγορίες:

- Πληροφορίες λογαριασμών
- Πληροφορίες πιστωτικών καρτών
- Πληροφορίες επιταγών
- Πληροφορίες δανείων

Πληροφορίες λογαριασμών: Ο χρήστης μπορεί να δει όλες τις πληροφορίες που σχετίζονται με τον τραπεζικό του λογαριασμό on line. Στην πλειοψηφία των e-banking συστημάτων ο αριθμός λογαριασμού εμφανίζεται με τη διεθνή IBAN μορφή του. Ο χρήστης βλέπει την επωνυμία του δικαιούχου, το είδος του τραπεζικού λογαριασμού , το κατάστημα διαχείρισης , το επιτόκιο του και το νόμισμά του. Εμφανίζονται πληροφορίες για το υπόλοιπο του λογαριασμού σε όλες του τις μορφές. Ο χρήστης γνωρίζει το διαθέσιμο υπόλοιπο, το λογιστικό υπόλοιπο , το τοκιζόμενο υπόλοιπο και τυχόν δεσμεύσεις που υπάρχουν στο λογαριασμό του. Τέλος, άλλη μια σημαντική υπηρεσία που αφορά πληροφορίες λογαριασμών είναι η παροχή των κινήσεων λογαριασμού. Ο χρήστης διαθέτει επιλογές όπως να δει κινήσεις ενός χρονικού διαστήματος , να δει στις τελευταίες κινήσεις του λογαριασμού ορίζοντας αυτός το πλήθος τους , να παρακολουθήσει mini statement του λογαριασμού του, δηλαδή τις δέκα τελευταίες χρεοπιστώσεις . Αντίστοιχες είναι και οι πληροφορίες που το σύστημα e-banking παρέχει για τις πιστωτικές κάρτες , τα δάνεια και τις επιταγές του πελάτη.

ΑΙΤΗΣΕΙΣ

Οι τράπεζες προκειμένου να διευκολύνουν τους πελάτες τους ενσωμάτωσαν στο e-banking ηλεκτρονικές αιτήσεις για τα περισσότερα των προϊόντων τους. Χαρακτηριστικά παραδείγματα ηλεκτρονικών αιτήσεων είναι η αίτηση ανοίγματος λογαριασμού , η αίτηση για δάνειο καθώς και η αίτηση για παραγγελία συναλλάγματος ή μπλοκ επιταγών.

ΠΡΟΣΘΕΤΕΣ ΥΠΗΡΕΣΙΕΣ

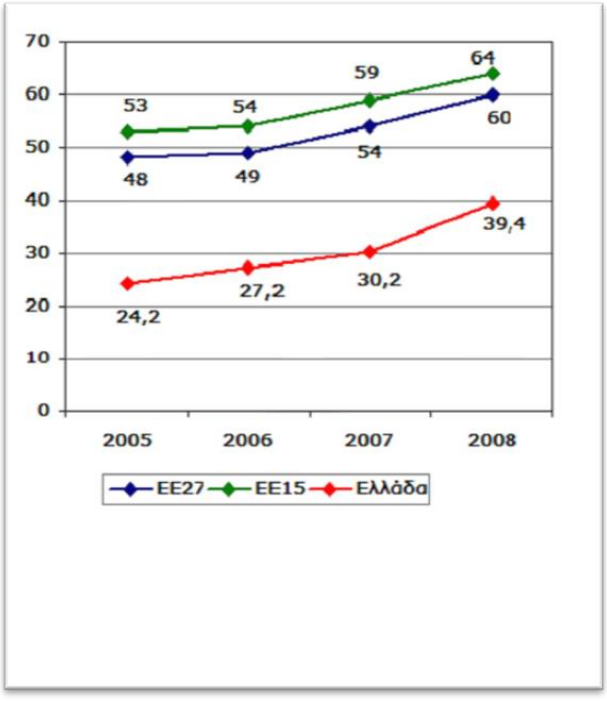
Πέραν των υπηρεσιών που αναφέρθηκαν , το e-banking δεν περιορίζεται μόνο σε αυτές. Υπάρχει πλήθος προϊόντων που συμπληρώνουν το e-banking και καλύπτουν τις ανάγκες και του πλέον απαιτητικού χρήστη και περιλαμβάνουν ηλεκτρονικές επενδυτικές υπηρεσίες , ηλεκτρονικό εμπόριο και πληρωμές , on line εισαγωγές και εξαγωγές και πολλές ακόμα. Χαρακτηριστικό παράδειγμα αποτελεί το e- investment το οποίο περιλαμβάνει κυρίως χρηματιστηριακές συναλλαγές καθώς και συναλλαγές αμοιβαίων κεφαλαίων και αμοιβαίων λογαριασμών. Η πλέον συνηθισμένη συναλλαγή μέσω e-banking είναι η αποστολή εμβάσματος (55% των συναλλαγών πραγματοποιείται μέσω διαδικτύου) και ακολουθούν οι χρηματιστηριακές συναλλαγές (το 22% πραγματοποιείται μέσω διαδικτύου) , οι πληρωμές ΦΠΑ,ΙΚΑ,ΤΕΒΕ (είναι χαρακτηριστικό ότι το 70% των συγκεκριμένων συναλλαγών πραγματοποιείται μέσω e-banking) καθώς και οι μεταφορές σε λογαριασμούς τρίτων.

Τέλος, αρκετές τράπεζες με διεθνείς δραστηριότητες παρέχουν επίσης προϊόντα και υπηρεσίες ηλεκτρονικής τραπεζικής σε διάφορες χώρες μέσω των web sites των θυγατρικών τους , οι οποίες έχουν την άδεια να δραστηριοποιούνται στη κάθε χώρα. Οι υπηρεσίες ηλεκτρονικής τραπεζικής που παρέχονται με τον τρόπο αυτό είναι απλά μια επέκταση των διεθνών δραστηριοτήτων των τραπεζών, αλλά υπόκεινται στους κανονισμούς του τραπεζικού περιβάλλοντος της κάθε χώρας. Έχουν αναπτυχθεί μοντέλα διασυνοριακής ηλεκτρονικής τραπεζικής από τραπεζικά ιδρύματα που είναι εγκατεστημένα σε μία χώρα , σε πελάτες άλλων χωρών , στις οποίες δεν διαθέτουν άδεια λειτουργίας και κατά συνέπεια δεν έχουν φυσική παρουσία.

ΚΕΦΑΛΑΙΟ 2

2.1.ΔΙΕΙΣΔΥΣΗ ΤΟΥ E-BANKING ΣΤΗΝ ΕΛΛΑΔΑ

Στον χώρο της ηλεκτρονικής τραπεζικής δραστηριοποιούνται με επιτυχία εδώ και αρκετά χρόνια οι περισσότερες ελληνικές και πολυεθνικές τράπεζες που λειτουργούν στην ελληνική επικράτεια. Παρόλα αυτά παρατηρείται σχετικά χαμηλή διείσδυση του e-banking στην Ελλάδα σε σχέση με τις υπόλοιπες ευρωπαϊκές χώρες. Το γεγονός αυτό οφείλεται στα γενικότερα χαμηλά ποσοστά εξοικείωσης του ελληνικού κοινού με τις νέες τεχνολογίες και το internet , το οποίο έχει ως αποτέλεσμα ο κόσμος να αντιμετωπίζει την ηλεκτρονική τραπεζική με σχετική δυσπιστία ακόμη και σήμερα. Ένας ακόμη παράγοντας που σχετίζεται με την μικρή σχετικά εξάπλωση του e-banking είναι και τα σχετικά χαμηλά ποσοστά ευρυζωνικότητας, δηλαδή της γρήγορης σύνδεσης στο διαδίκτυο, στους Έλληνες χρήστες κάτι που σχετίζεται και με το κόστος σύνδεσης. Εντούτοις, σύμφωνα με τραπεζικούς κύκλους , τα τελευταία χρόνια ο αριθμός των χρηστών τέτοιου είδους υπηρεσιών αυξάνεται με γρήγορους ρυθμούς. Όσον αφορά τους χρήστες του διαδικτύου , στο σχεδιάγραμμα που ακολουθεί διαγράφεται αυτή η θετική πορεία που παρουσιάζει η διείσδυση του internet στην Ελλάδα τα τελευταία χρόνια , σε αντιδιαστολή με τα κράτη της Ευρωπαϊκής Ένωσης.



Πιο συγκεκριμένα, στα τέλη του 2006 οι χρήστες υπηρεσιών ηλεκτρονικής τραπεζικής ξεπέρασαν τους 500.000 , γεγονός ιδιαίτερα αισιόδοξο για το μέλλον αν αναλογιστεί κανείς ότι το αντίστοιχο νούμερο το 2001 δεν ξεπερνούσε τους 150.000 χρήστες. Το Παρατηρητήριο για την κοινωνία της πληροφορίας εκτίμησε το 2007 από την πλευρά του ότι οι χρήστες των on line τραπεζικών υπηρεσιών στην Ελλάδα ανερχόταν στο 15% του συνόλου των χρηστών του internet στη χώρα, ενώ ένα ποσοστό 7% χρησιμοποιούσε το διαδίκτυο και για χρηματιστηριακές συναλλαγές. Εκτιμάται επιπλέον ότι οι on line υπηρεσίες των ελληνικών τραπεζών δεν υστερούν σε τίποτα από τις αντίστοιχες των τραπεζών του εξωτερικού , εξασφαλίζοντας αμεσότητα , ικανοποιητική εξυπηρέτηση και ασφάλεια στους χρήστες. Τα παραπάνω νούμερα και ποσοστά αναμένεται στο άμεσο μέλλον να αυξηθούν καθώς ο ανταγωνισμός τόσο

μεταξύ των παρόχων ευρυζωνικού internet, όσο και μεταξύ των τραπεζών έχει ενταθεί, πράγμα που οδηγεί στην αυξανόμενη διείσδυση του internet και των υπηρεσιών ηλεκτρονικής τραπεζικής στα ελληνικά νοικοκυριά. **(εφημερίδα ημερησία ,12/12/2006)**

Τα πιστωτικά ιδρύματα στη χώρα μας ανέπτυξαν το e-Banking με αργά βήματα και μακρύ διάστημα σε πιλοτικά συστήματα , αφού τα στελέχη της πληροφορικής κλήθηκαν να εκπονήσουν προγράμματα για το νέο σύστημα, χωρίς να υπάρχει προηγούμενη εμπειρία στον τομέα αυτό. Με το e-banking υπάρχει η ανάγκη υποστήριξης του χρήστη (monitoring, help desk) που να διευκολύνει τη διόρθωση τυχόν λαθών κατά τις συναλλαγές του μέσω internet. Για τη στελέχωση των ανωτέρω τμημάτων απαιτείται εξειδικευμένο προσωπικό. Οι τράπεζες χρειάστηκαν αρκετό διάστημα σε σχετικά πιλοτικά συστήματα για τη διερεύνηση του θέματος, πριν οριστικοποιήσουν το νέο τους οργανόγραμμα. Για να προσφέρουν την απαραίτητη βοήθεια στο πελάτη τα πιστωτικά ιδρύματα προέβησαν σε διοικητική αναδιοργάνωση και δημιουργήθηκαν νέες υπηρεσίες για την παρακολούθηση, υποστήριξη του χρήστη, έλεγχο και διαχείριση τόσο του συστήματος όσο και του κινδύνου που συνεπάγονται οι τραπεζικές συναλλαγές μέσω διαδικτύου. Οι χρηματοπιστωτικοί οργανισμοί έπρεπε να αξιολογήσουν τις εναλλακτικές δυνατότητες και κατόπιν να λάβουν αποφάσεις σχετικά με τη πολιτική που θα ακολουθούσαν στο συγκεκριμένο θέμα. Τόσο στη περίπτωση εύρεσης προσωπικού μέσω νέων προσλήψεων όσο και με την εκπαίδευση του ήδη υπάρχοντος πέρασε αρκετό χρονικό διάστημα μέχρι να ολοκληρωθούν οι σχετικές διαδικασίες. **(Χατζηκωνσταντής Λ. 2003).**

Η ένταξη της Ελλάδας στην Οικονομική Νομισματική Ένωση (ΟΝΕ) έδωσε την ευκαιρία στις ελληνικές τράπεζες να εκσυγχρονιστούν και να εναρμονίσουν τη λειτουργία τους με βάση τα ευρωπαϊκά πρότυπα. Επίσης , η εισαγωγή του ευρώ σε φυσική μορφή έφερε σημαντικές μεταβολές στις χρηματοπιστωτικές δραστηριότητες του ελληνικού τραπεζικού συστήματος . Τα πιστωτικά ιδρύματα στο νέο περιβάλλον του κοινού νομίσματος για να διατηρήσουν τη πελατεία τους και να αυξήσουν τα έσοδά τους πρέπει να προσφέρουν και νέα προϊόντα σε συνδυασμό με την παροχή υψηλής ποιότητας υπηρεσιών. Σε αυτό συμβάλλει το e-banking επειδή έχοντας παγκόσμια εμβέλεια , τους δίνει τη δυνατότητα να βελτιώσουν την ανταγωνιστικότητα και την παραγωγικότητα τους , να αυξήσουν το μερίδιό τους στη διεθνή αγορά , γεγονός ιδιαίτερα σημαντικό για τις ελληνικές τράπεζες λόγω του μεγάλου αριθμού των ελλήνων της διασποράς. **(Κεφαλάς Χ.,2001).**

2.2 Η ΤΕΛΕΥΤΑΙΑ ΠΕΝΤΑΕΤΙΑ

2.2.1 ΟΙ 15 ΤΡΑΠΕΖΕΣ ΤΙΣ ΕΛΛΑΔΑΣ

2007:Στον παρακάτω πίνακα 1 παρουσιάζεται μία επισκόπηση τω ν ελληνικών τραπεζών και πιο συγκεκριμένα, τα δεδομένα είναι από τις 15 μεγαλύτερες τράπεζες. Η ανάλυση χωρίζεται σε τρεις ομάδες των πέντε τραπεζών η κάθε μία. Οι τράπεζες κατηγοριοποιούνται σύμφωνα με την Παγκόσμια κατάταξη (με βάση τις επίσημες εκθέσεις που έχουν δημοσιευθεί στη Bank scope.) Έτσι, η πρώτη ομάδα έχει πέντε μεγάλες τράπεζες (Εθνική τράπεζα Ελλάδος, Euro bank, Alpha bank, Τράπεζα Πειραιώς, Εμπορική τράπεζα). Η δεύτερη ομάδα αποτελείται από την Αγροτική τράπεζα, Marfin bank, Post bank ,Γενική τράπεζα, Τράπεζα Αττικής. Ενώ στη τελευταία ομάδα περιέχει τις πέντε υπόλοιπες τράπεζες:Aspis bank, Probank, Proton bank, Πανελλήνια τράπεζα, Millennium bank.

ΠΙΝΑΚΑΣ 1

BANK	ΠΑΓΚΟΣΜΙΑ ΚΑΤΑΤΑΞΗ	ΙΔΡΥΣΗ	ΣΥΝΟΛΟ ΕΝΕΡΓΗΤΙΚΟΥ 2007	WEBSITE
GROUP 1				
National bank of Greece	169	1841	90386	www.nbg.gr
Eurobank	215	1997	68389	www.eurobank.gr
Alpha bank	256	1879	54684	www.alphabank.gr
Piraeus bank	287	1916	46427	www.pireausbank.gr
Emporiki bank	439	1907	27324	www.emporiki.gr
GROUP 2				
ATE bank	488	1929	24273	www.atebank.gr
Marfin bank	741	1991	13715	www.marfinbank.gr
Post bank	762	1900	13182	www.ttbank.gr
General bank	1552	1937	4335	www.geniki.gr
Attica bank	1653	1925	3916	www.bankofattica.gr
GROUP 3				
Aspis bank	1927	1992	2944	www.aspisbank.gr
Probank	2037	2001	2862	www.probank.gr
Proton bank	2185	2001	2365	www.proton.gr
Panellinia bank		2001	626	www.panelliniabank.gr
Millennium bank		2006	3825	www.milleniumbank.gr

ΠΗΓΗ: Bank scope 2008

Οι κορυφαίες τράπεζες παρουσιάζουν σταθερή απόδοση με τη πάροδο του χρόνου (δηλαδή οι χρήστες του internet και οι πελάτες, επισκέπτονται τους ιστόχωρους τους τακτικά). Με άλλα λόγια ο παράγοντας εμπιστοσύνης μεταξύ των τρεχόντων χρηστών είναι αρκετά υψηλός. Εντούτοις, το γεγονός ότι οι στατιστικές για τις ελληνικές τράπεζες είναι χαμηλές (έναντι άλλων ανεπτυγμένων χωρών) σημαίνει ότι οι ελληνικές τράπεζες πρέπει να επενδύσουν περισσότερο για να βελτιώσουν τη ποιότητα των ιστοχώρων τους. Αυτό θα αυξήσει την αξιοπιστία των πελατών και θα προσελκύσει περισσότερους πελάτες ηλεκτρονικής τραπεζικής.

Έκπληξη προκαλεί ότι από το 2009 οι περισσότεροι καταναλωτές προτιμούν το e-banking για τις συναλλαγές τους, παρά τις παραδοσιακές μεθόδους.

Τα στατιστικά στην Ελλάδα:

Σε πρόσφατη έρευνα του παρατηρητηρίου για την κοινωνία της πληροφορίας διαπιστώθηκε: **Αν και εξοικειωμένοι με το διαδίκτυο, οι Έλληνες διστάζουν να πραγματοποιήσουν ηλεκτρονικές συναλλαγές.** Η σχέση των Ελλήνων με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο βελτιώνεται αισθητά χρόνο με το χρόνο, ωστόσο το 'ψηφιακό τοπίο' μεταβάλλεται αρκετά όταν πρόκειται για διαδικτυακές δραστηριότητες που εμπεριέχουν οικονομικές συναλλαγές. Ενδεικτικά, η ανάλυση των πιο πρόσφατων διαθέσιμων στοιχείων καταδεικνύει τα εξής:

- 1 στους 10 Έλληνες έχει χρησιμοποιήσει το διαδίκτυο για να παραγγείλει ή να αγοράσει αγαθά ή υπηρεσίες, ενώ ένα ελαφρώς μικρότερο ποσοστό (8%) προχώρησε σε ανάλογη ενέργεια κατά το τελευταίο τρίμηνο του 2009. Τα αντίστοιχα ποσοστά για τον μέσο Ευρωπαίο πολίτη κινούνται σε επίπεδα 3,5 φορές υψηλότερα.
- 1 στους 20 Έλληνες χρησιμοποιεί συστήματα ηλεκτρονικής τραπεζικής, με το αντίστοιχο χάσμα έναντι της ευρωπαϊκής ένωσης να εκτοξεύεται στις 27 ποσοστιαίες μονάδες το 2009 (5% έναντι 32%).
- Μόλις 1 στους 100 Έλληνες έχει χρησιμοποιήσει το διαδίκτυο για πώληση αγαθών ή υπηρεσιών, π.χ. μέσω ηλεκτρονικών πλειστηριασμών. Το αντίστοιχο ευρωπαϊκό ποσοστό αγγίζει το 10%.

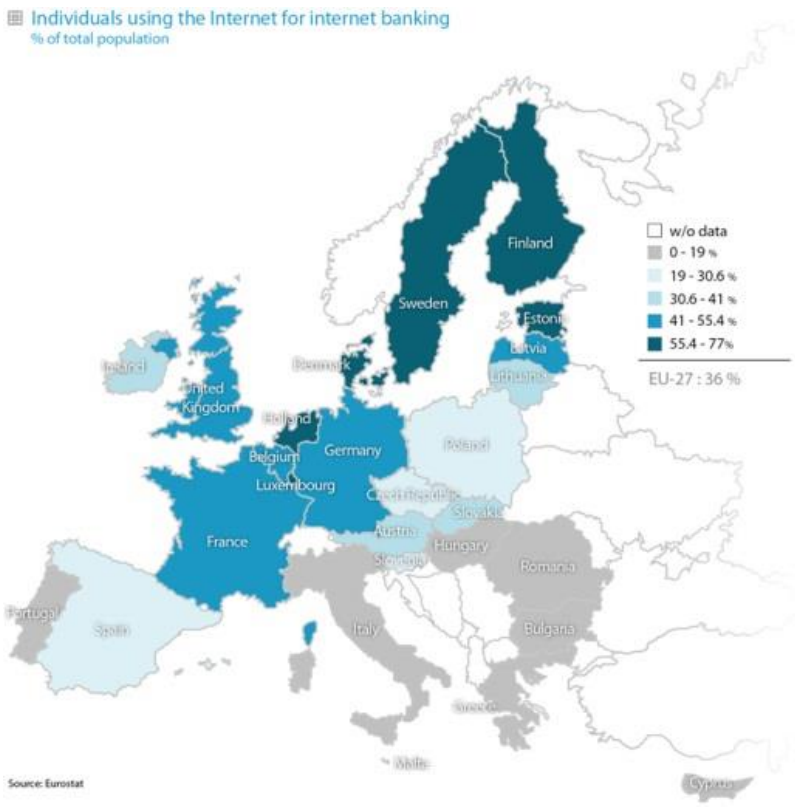
Οι κύριες αιτίες για αυτό είναι ότι στη χώρα μας υπάρχουν πολλά νοικοκυριά χωρίς Η/Υ ή πρόσβαση στο internet. Επίσης ,το μεγαλύτερο ποσοστό που κάνει χρήση του internet είναι από ηλικίες 15 έως 25 που δεν είναι οικονομικά ενεργοί πολίτες. Όμως χρόνο με το χρόνο το e-banking φαίνεται να κερδίζει έδαφος και από τους οικονομικά ενεργούς στις μεγαλύτερες ηλικίες (30 με 55).

Επίσης ,σχετικά με τους δείκτες καταναλωτικής πίστης προκύπτει δυσπιστία των καταναλωτών ως προς την αποτελεσματικότητα των ανεξάρτητων αρχών για την προστασία του καταναλωτή καθώς:

- Οι καταναλωτές στην Ελλάδα, παρουσιάζουν από τα μεγαλύτερα ποσοστά δυσπιστίας ως προς την αποτελεσματικότητα των ανεξάρτητων αρχών για την προστασία του καταναλωτή, καθώς μόνο 4 στους 10 δηλώνουν ικανοποιημένοι.
- Πάνω από το 50% των Ελλήνων καταναλωτών φέρονται να μην εμπιστεύονται ούτε τις δημόσιες αρχές για τον ίδιο λόγο.
- Μόλις 3 στους 10 Έλληνες αισθάνονται ασφάλεια με τα ισχύοντα μέτρα για την προστασία του καταναλωτή, ενώ παρόμοιο ποσοστό «Διαφωνεί απόλυτα» με έναν τέτοιο ισχυρισμό. **(www.in.gr ,31/08/2010)**

2.2.3 Η ΘΕΣΗ ΤΗΣ ΕΛΛΑΔΑΣ ΣΤΗΝ ΕΥΡΩΠΗ ΜΕ ΒΑΣΗ ΤΗ ΧΡΗΣΗ ΤΟΥ E-BANKING

Στην ΕΕ, ο αριθμός των ατόμων που χρησιμοποιούν το Διαδίκτυο για τραπεζικές υπηρεσίες μέσω Διαδικτύου αυξήθηκε κατά 4 ποσοστιαίες μονάδες κατά το τελευταίο έτος, από 32% το 2009 σε 36% το 2010, γεγονός που επιβεβαιώνει την ανοδική τάση σε αυτή τη χρήση του Διαδικτύου. Μια πιο λεπτομερής ανάλυση αποκαλύπτει ότι, εντός της ΕΕ-27, χώρες της Βόρειας Ευρώπης καταγράφουν τα υψηλότερα ποσοστά. Οι Κάτω Χώρες, τη Φινλανδία και τη Σουηδία, η οποία σκόραρε 40 πόντους τιμές πάνω από τον ευρωπαϊκό μέσο όρο, είναι οι χώρες με τα υψηλότερα ποσοστά. Αντιθέτως, η Βουλγαρία, η Ρουμανία και η Ελλάδα είναι πολύ κάτω από το μέσο κοινό.



2007-2012(πηγή:Eurostat)

2.2.4 Η ΕΛΛΑΔΑ ΩΣ ΑΝΕΞΑΡΤΗΤΟ ΚΟΜΜΑΤΙ ΤΗΣ ΕΥΡΩΠΗΣ

Ολοένα και μεγαλύτερος αριθμός πελατών των τραπεζών χρησιμοποιεί τα εναλλακτικά δίκτυα διανομής τραπεζικών προϊόντων και υπηρεσιών, κερδίζοντας έτσι χρόνο αλλά σε ορισμένες περιπτώσεις και χρήμα, από ενδεχόμενες επιβαρύνσεις που επιβάλλονται εάν η συναλλαγή πραγματοποιηθεί από τραπεζικό υποκατάστημα. Ειδικότερα σύμφωνα με στοιχεία που περιλαμβάνονται στην μελέτη της Ελληνικής Ένωσης Τραπεζών (ΕΕΤ) με θέμα "το ελληνικό τραπεζικό σύστημα το 2010" εντυπωσιακή υπήρξε η συνεχιζόμενη αύξηση των εγγεγραμμένων χρηστών στις υπηρεσίες ηλεκτρονικής τραπεζικής που έχουν αναπτύξει οι ελληνικές τράπεζες.

Στο πρώτο εξάμηνο του 2010, περισσότερα από 1.929.800 (2009: 1.719.800) φυσικά και νομικά πρόσωπα ήταν εγγεγραμμένοι χρήστες σε υπηρεσίες ηλεκτρονικής τραπεζικής, σημειώνοντας ετήσια αύξηση 12%. Η αξία των εγχρήματων συναλλαγών, συμπεριλαμβανομένων των ενδοτραπεζικών, διατραπεζικών και χρηματιστηριακών συναλλαγών, παρουσίασε ετήσια αύξηση 8% (ήτοι περίπου 19,7 δισ. ευρώ το πρώτο εξάμηνο του 2010 έναντι 18,3 δισ. ευρώ στο τέλος Ιουνίου 2009).

Οι Έλληνες φαίνεται να έχουν ξεπεράσει τους συνήθεις δυσπιστία των συναλλαγών που δεν είναι πρόσωπο με πρόσωπο, προτιμώντας να κερδίσει χρόνο και σε ορισμένες περιπτώσεις τα χρήματα, πάρα πολύ, καθώς απαλλάσσονται από πρόσθετες επιβαρύνσεις που επιβάλλονται κατά τη συναλλαγή διεξάγονται στο μετρητή. **(εφημερίδα έθνος, 08/07/2011)**

Ένα ιδιαίτερα ενθαρρυντικό στοιχείο είναι ότι η διείσδυση των νέων τεχνολογιών στην ελληνική αγορά και δη του Internet Banking, ακολουθεί συνεχώς αυξανόμενη πορεία. Δεν υπάρχει κάποια καμπή. Αυτό οφείλεται και στο γεγονός ότι παρατηρούμε μια ταχέως αυξητική πορεία στη χώρα μας όσον αφορά τη χρήση του Internet. Εκ’ του αποτελέσματος, όλο και περισσότεροι Έλληνες εγγράφονται κάθε μήνα στις υπηρεσίες e-Banking. ένα ιδιαίτερα ενθαρρυντικό στοιχείο είναι ότι η διείσδυση των νέων τεχνολογιών στην ελληνική αγορά και δη του Internet Banking, ακολουθεί συνεχώς αυξανόμενη πορεία. Δεν υπάρχει κάποια καμπή. Αυτό οφείλεται και στο γεγονός ότι παρατηρούμε μια ταχέως αυξητική πορεία στη χώρα μας όσον αφορά τη χρήση του Internet. Εκ’ του αποτελέσματος, όλο και περισσότεροι Έλληνες εγγράφονται κάθε μήνα στις υπηρεσίες e-Banking.

Γίνεται απόλυτα σαφές λοιπόν ότι η ηλεκτρονική τραπεζική μπήκε στη ζωή μας και σηματοδοτεί μία νέα εποχή στις τραπεζικές συναλλαγές μας. Βάζει τέλος στις ουρές των ταμείων και στην αναμονή των πελατών, αφού αρκεί μία συσκευή σταθερού ή κινητού τηλεφώνου, ή ένας υπολογιστής εγκατεστημένος στο σπίτι ή στο γραφείο, για να κάνουμε τις συναλλαγές μας με απόλυτη ασφάλεια, όλο το 24ωρο. Δεν

πρέπει να ξεχνάμε όμως ότι θα απαιτηθεί χρόνος έως ότου η ηλεκτρονική τραπεζική λάβει απολύτως μαζικό χαρακτήρα, ωστόσο όσοι από τους τραπεζικούς ομίλους έχουν ενταχθεί στον χώρο αυτόν διατηρούν συγκριτικό πλεονέκτημα. Η χρήση είναι αρκετά απλή και η μεγάλη επιτυχία της κινητής τηλεφωνίας στην χώρα μας αποτελεί προάγγελο της επιτυχίας που θα έχει στην Ελλάδα η ηλεκτρονική τραπεζική.

Ωστόσο, τα φυσικά δίκτυα των τραπεζών δεν αναμένεται να καταργηθούν αλλά να αλλάξουν μορφή. Θα έχουμε μικρότερα καταστήματα τα οποία θα χρησιμοποιούν τεχνολογία αιχμής. Ας μην ξεχνάμε τέλος ότι η ηλεκτρονική τραπεζική εξυπηρέτηση δεν καλύπτει όλες τις συναλλαγές. Οι τράπεζες, μέσω της ηλεκτρονικής τραπεζικής, θέτουν στην υπηρεσία του πελάτη το ηλεκτρονικό τους κατάστημα για άμεση εξυπηρέτηση 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Ο πελάτης δύναται να πραγματοποιεί τις αναγκαίες του συναλλαγές με απόλυτη ασφάλεια και φυσικά διατηρώντας το απόρρητό του. Σύμφωνα με έρευνες, όλο και περισσότεροι ιδιώτες αλλά και επιχειρήσεις στην Ελλάδα προτιμούν να διεκπεραιώνουν τις τραπεζικές τους συναλλαγές μέσω διαδικτύου.

ΚΕΦΑΛΑΙΟ 3

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ Ε BANKING

3.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΓΙΑ ΤΟΝ ΙΔΙΩΤΗ ΠΕΛΑΤΗ

Εξυπηρέτηση :Η διαθεσιμότητα των υπηρεσιών είναι 24 ώρες το 24ωρο και 7 ημέρες την εβδομάδα , δίνοντας τη δυνατότητα στον εκάστοτε πελάτη να εξυπηρετηθεί οποιαδήποτε στιγμή αυτός επιθυμεί.

Αποφυγή ουράς εξυπηρέτησης: Η ανάγκη φυσικής παρουσίας στην τράπεζα πλέον εξαλείφεται και η επιθυμητή από τον πελάτη συναλλαγή μπορεί να εκτελεστεί εύκολα και άμεσα χωρίς να χρειάζεται ο ίδιος να περιμένει στην ουρά εξυπηρέτησης ή σε κάποιο ταμείο της τράπεζας.

Εξοικονόμηση χρόνου: Η πραγματοποίηση των συναλλαγών χωρίς πλέον την ανάγκη μετάβασης σε κάποιο από τα καταστήματα της τράπεζας είναι προφανές πως συμβάλλει στην εξοικονόμηση χρόνου.

On line παρακολούθηση τραπεζικών προϊόντων: Η on line πρόσβαση του πελάτη στα τραπεζικά του προϊόντα έχει ως αποτέλεσμα την εύκολη και γρήγορη ενημέρωσή του για οτιδήποτε αφορά αυτά.

On line μεταφορές κεφαλαίων: Ο χρήστης της ηλεκτρονικής τραπεζικής μέσα από εξαιρετικά συνοπτικές διαδικασίες έχει τη δυνατότητα να μεταφέρει κεφάλαια τόσο εντός της τράπεζας του , όσο και σε άλλες τράπεζες έχοντας σε πλήρη έλεγχο τόσο τις οφειλές όσο και τις υποχρεώσεις του.

Εύκολη πρόσβαση από οποιοδήποτε σημείο του κόσμου: Με μόνη προϋπόθεση ο πελάτης να έχει πρόσβαση στο διαδίκτυο , του παρέχεται η δυνατότητα ανά πάσα στιγμή και από οποιοδήποτε μέρος του κόσμου να έχει πρόσβαση στο τραπεζικό του χαρτοφυλάκιο και να εκτελεί τις συναλλαγές του.

Μεγάλη γκάμα εξόφλησης λογαριασμών Οργανισμών και Επιχειρήσεων: Μια συνεχώς αυξανόμενη γκάμα οργανισμών και επιχειρήσεων παρέχεται στους πελάτες οι οποίοι έχουν τη δυνατότητα να εξοφλήσουν τις οφειλές τους προς αυτές. Με αυτό τον τρόπο μπορούν να έχουν μια συγκεντρωτική ενημέρωση αλλά και να κάνουν καλύτερο προγραμματισμό των υποχρεώσεών τους.

Δυνατότητα επενδυτικών συναλλαγών (π.χ χρηματιστήριο): Μέσω της ηλεκτρονικής τραπεζικής οι χρήστες έχουν τη δυνατότητα εκτέλεσης επενδυτικών συναλλαγών. Ακόμη μπορούν οι ίδιοι να ελέγχουν τις εντολές τους, τα χαρτοφυλάκια τους και την αποτίμηση αυτών.

Μικρότερο κόστος συναλλαγών: Είναι γεγονός πως για τους πελάτες του e-banking όλο το εύρος των τραπεζικών συναλλαγών παρέχεται με μικρότερο κόστος. Ακόμη , πολλές είναι οι συναλλαγές που παρέχονται εντελώς δωρεάν ενώ σε περίπτωση πραγματοποίησης τους σε κάποιο υποκατάστημα της τράπεζας χρεώνεται κανονικά.

Γνωριμία με νέες τεχνολογίες: Μέσω της ηλεκτρονικής τραπεζικής ο πελάτης της τράπεζας έρχεται αντιμέτωπος με νέες τεχνολογίες. Έτσι πέρα από τα πλεονεκτήματα που αυτός επωφελείται από τη χρήση του e-banking ταυτόχρονα γνωρίζει και νέες τεχνολογίες.

Εύκολες συναλλαγές για άτομα με ειδικές ανάγκες: Άτομα με κινητικά κυρίως προβλήματα αλλά και άλλες ομάδες ατόμων για τα οποία η μετακίνηση αποτελεί φραγμό , μέσω του e-banking βρίσκουν τη λύση για την πραγματοποίηση των συναλλαγών τους. Έτσι οι συναλλαγές τους μπορούν να γίνουν εύκολα και γρήγορα χωρίς να χρειάζεται κάποια μετακίνηση σε υποκατάστημα της τράπεζας τους.

3.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΕΤΑΙΡΙΑ-ΠΕΛΑΤΗ

Τα οφέλη για τον ιδιώτη ισχύουν και για μια εταιρία , αρκετές όμως τραπεζικές υπηρεσίες του e-banking απευθύνονται αποκλειστικά σε επιχειρήσεις .

Ολοκληρωμένα πακέτα υπηρεσιών πληρωμών για επιχειρήσεις: Παρέχεται ένα ολοκληρωμένο περιβάλλον πληρωμών για τις εταιρίες τόσο των οφειλών τους στο Δημόσιο , όσο και των οφειλών τους σε οργανισμούς και ΔΕΚΟ.

Εύκολη ενημέρωση των μηχανογραφικών συστημάτων της εταιρίας: Τα μηχανογραφικά και τα λογιστικά συστήματα των επιχειρήσεων μπορούν να ενημερωθούν εύκολα και άμεσα με τις κινήσεις των λογαριασμών της εταιρίας μέσω της ευκολίας του downloading που προσφέρουν οι υπηρεσίες μέσω e-banking.

Εκτέλεση μισθοδοσίας προσωπικού ή μαζικών πληρωμών προμηθευτών: Η εκτέλεση της μισθοδοσίας του προσωπικού μιας επιχείρησης , η πληρωμή των προμηθευτών της και η on line παρακολούθηση της κατάστασης των πληρωμών της μπορούν πλέον να εκτελεστούν με πολύ συνοπτικές διαδικασίες από την ίδια.

Διαφορετικά δικαιώματα χρήσης και πρόσβασης: Παρέχεται η δυνατότητα στην εταιρία να επιλέξει ποιο υπάλληλοι της θα μπορούν να χρησιμοποιούν ηλεκτρονικές τραπεζικές υπηρεσίες καθώς και τι δικαιώματα θα έχουν , τόσο σε επίπεδο πρόσβασης σε λογαριασμούς και κάρτες , όσο και σε επίπεδο τέλεσης συναλλαγών. Ακόμη δίνεται η δυνατότητα της έγκρισης συναλλαγών , δηλαδή άλλος χρήστης να καταχωρεί τις εντολές και διαφορετικός χρήστης να δίνει την έγκριση για την εκτέλεση τους.

Δημιουργία εναλλακτικού δικτύου εξόφλησης λογαριασμών: Πολλές είναι οι εταιρίες που μπορούν να εκμεταλλευτούν το e-banking σαν ένα επιπλέον δίκτυο είσπραξης των υποχρεώσεων των πελατών τους. Ήδη αρκετές είναι οι εταιρίες που χρησιμοποιούν το διατραπεζικό σύστημα DIASDEBIT σε συνεργασία με τραπεζικά ιδρύματα του εσωτερικού για την εξόφληση των λογαριασμών τους.

Δημιουργία εναλλακτικού δικτύου πώλησης προϊόντων και υπηρεσιών : Οι συνεργασίες στο χώρο του E-COMMERCE και των E-PAYMENTS δίνουν τη δυνατότητα στις εταιρίες να προσφέρουν στους πελάτες τους ένα εναλλακτικό, ασφαλή και εξ αποστάσεως τρόπο αγορών αλλά και πληρωμής των οφειλών τους.

3.3 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΓΙΑ ΤΟΝ ΙΔΙΩΤΗ/ΕΤΑΙΡΙΑ

Χρονοβόρα εγγραφή πελατών: Η διαδικασία εγγραφής κάποιου πελάτη στο on line πρόγραμμα της τράπεζας του, είναι αρκετά χρονοβόρα καθώς απαιτεί από τον πελάτη να δώσει τα στοιχεία της ταυτότητας του και να υπογράψει τα αντίστοιχα έντυπα της τράπεζας , ενώ αν πρόκειται για μια αποκλειστικά ηλεκτρονική τράπεζα , τα έντυπα θα αποσταλούν ταχυδρομικώς έτσι ώστε να συμπληρωθούν και να αποσταλούν και πάλι στην τράπεζα.

Δυσκολία στο χειρισμό: Πελάτες οι οποίοι δεν είναι εξοικειωμένοι με το διαδίκτυο είναι πολύ πιθανόν να αντιμετωπίσουν προβλήματα στο χειρισμό των τραπεζικών δικτυακών τόπων. Ακόμη, η έλλειψη γνώσεων πάνω σε θέματα νέων τεχνολογιών μπορεί να ενισχύσει τους ενδοιασμούς ορισμένων πελατών σχετικά με τη χρησιμοποίηση του internet banking.

3.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΤΡΑΠΕΖΑ

Εναλλακτικά δίκτυα: Μέσω του e-banking παρέχεται πλέον στους πελάτες της εκάστοτε τράπεζας η δυνατότητα να διεκπεραιώσουν τις συναλλαγές τους μέσω νέων καναλιών που πριν από μερικά χρόνια δεν υπήρχαν, όπως το internet ,το τηλέφωνο και το κινητό.

Καινοτομικές υπηρεσίες :Οι τράπεζες αναγνωρίζοντας τα προνόμια που προσφέρει η τεχνολογία ,τη χρησιμοποιούν για τη δημιουργία καινοτόμων και πρωτοποριακών υπηρεσιών , οι οποίες σε διαφορετική περίπτωση δεν θα μπορούσαν να υλοποιηθούν.

Μείωση λειτουργικού κόστους: Αν δούμε συγκριτικά τα κόστη που έχει η τράπεζα για τη διεκπεραίωση συναλλαγών μέσω ταμείου και τα αντίστοιχα κόστη από τις συναλλαγές μέσω εναλλακτικών δικτύων θα δούμε πως η εξοικονόμηση που κάνει η τράπεζα μέσω της ηλεκτρονικής τραπεζικής είναι πολύ σημαντική.

Αύξηση ποιότητας εξυπηρέτησης: Η ποιότητα εξυπηρέτησης των πελατών όχι μόνο αυξάνεται, αλλά μέσω της πιστοποίησης από εξουσιοδοτημένους φορείς , προσθέτει κύρος στις μονάδες ηλεκτρονικής τραπεζικής.

Αύξηση πελατειακής βάσης: Η χρησιμοποίηση φιλικών προς το χρήστη πλατφορμών , οι οποίες παρέχουν ολοκληρωμένα πακέτα υπηρεσιών και συναλλαγών , έχουν μεγάλη συμβολή στην αύξηση της πελατειακής βάσης της τράπεζας και στην προσέλκυση νέων πελατών.

Ενίσχυση της αφοσίωσης των πελατών: Πολλοί είναι οι τραπεζικοί αναλυτές οι οποίοι υποστηρίζουν ότι μέσω των υπηρεσιών της ηλεκτρονικής τραπεζικής , η αφοσίωση των πελατών ενισχύεται αφού η σχέση μεταξύ τράπεζας και πελάτη τίθεται σε νέα βάση. Οι πελάτες επομένως που έχουν εξοικειωθεί με τις ηλεκτρονικές υπηρεσίες που προσφέρονται από μια τράπεζα θεωρούνται περισσότερο πιστοί και το ενδεχόμενο να αλλάξουν τράπεζα είναι πολύ μικρότερο σε σχέση με τους υπόλοιπους πελάτες.

Καλή φήμη: Η ηλεκτρονική τραπεζική αποτέλεσε και συνεχίζει να αποτελεί ένα είδος βιτρίνας για τους τραπεζικούς οργανισμούς. Πολλά είναι τα παραδείγματα μικρών τραπεζών που στηρίζουν ένα μέρος της καλής τους εικόνας στο e-banking τους.

3.5 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΓΙΑ ΤΗΝ ΤΡΑΠΕΖΑ

Υψηλό αρχικό κόστος εγκατάστασης: Η αγορά του απαιτούμενου εξοπλισμού αλλά και η εκπαίδευση του προσωπικού της τράπεζας πάνω στα θέματα των νέων τεχνολογιών , απαιτούν από τη μεριά της τράπεζας μεγάλη επένδυση η οποία είναι σαφές πως πρέπει να γίνει με προσοχή καθώς και να είναι συμβατή με την επιχειρηματική στρατηγική της.

Ασφάλεια: θέματα όπως η ασφάλεια των συναλλαγών και η προστασία των συναλλασσόμενων είναι υψίστης σημασίας για τις τράπεζες. Κανένα υπολογιστικό σύστημα δε μπορεί να θεωρηθεί ασφαλές 100% και πολλές είναι οι περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στα τραπεζικά ηλεκτρονικά συστήματα. Συνεπώς, αποτελεί ένα θέμα το οποίο οι τράπεζες πρέπει να φροντίζουν διαρκώς για την ομαλή λειτουργία του συστήματος και την εξασφάλιση τόσο των πελατών όσο και των ίδιων των τραπεζών.

ΚΕΦΑΛΑΙΟ 4

4.1.ΑΣΦΑΛΕΙΑ

Η διασφάλιση του απορρήτου των ηλεκτρονικών συναλλαγών αποτελεί πρωταρχικό στόχο για κάθε τράπεζα και οι επενδύσεις σε αυτό το τομέα υπήρξαν και συνεχίζουν να είναι πολύ σημαντικές. Η ασφαλής διαδικασία συναλλαγών είναι αρκετά πολύπλοκο θέμα και προϋποθέτει την ύπαρξη ασφαλών γραμμών , ψηφιακών πιστωτικών και πιστοποιημένων διακομιστών. Ωστόσο, παράλληλα παρατηρείται μια διστακτικότητα από πλευράς κοινής γνώμης στη χρήση των ηλεκτρονικών υπηρεσιών , με κύρια αιτία την άγνοια σε θέματα ασφαλείας. Το σίγουρο είναι πως για να επιτευχθεί ο στόχος και να αντιμετωπιστούν οποιεσδήποτε πιθανές απειλές, η συνεργασία τραπεζών και χρηστών είναι απαραίτητη.

Η ασφάλεια είναι σημαντικό θέμα για τις τράπεζες επειδή μέσω internet e-banking εκτελούνται χρηματικές συναλλαγές που συχνά γίνονται στόχος για απάτη. Επίσης, τα πιστωτικά ιδρύματα φροντίζουν να μην υπάρχει αμφιβολία για την ασφάλεια του συστήματος, ώστε το κοινό να το εμπιστευθεί και να υιοθετήσει αυτό το εναλλακτικό κανάλι τραπεζικών υπηρεσιών. Συνήθη ερωτήματα που διατυπώνουν οι πελάτες γύρω από την ασφάλεια του e-banking είναι :

Πως αποδεικνύεται ότι είναι αυθεντική η ιστοσελίδα της συγκεκριμένης τράπεζας (διεύθυνση IP) και δε θα παραπλανηθεί ο χρήστης από κάποια ψεύτικη;

- Μπορεί κάποιος κακόβουλος να αποσπάσει το user ID ή password κατά τη διάρκεια της επικοινωνίας με την τράπεζα;

- Είναι δυνατόν να διαρρεύσουν προσωπικά δεδομένα όπως ονόματα , τηλέφωνα, αριθμοί λογαριασμών και να χρησιμοποιηθούν σε βάρος τους;

Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα που στέλνει να μη μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι'αυτό άτομα. (ΕΜΠΙΣΤΕΥΤΙΚΌΤΗΤΑ). Τα δεδομένα δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά τη μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει. (ΑΚΕΡΑΙΟΤΗΤΑ). Επιπλέον, σε μια τέτοια συναλλαγή είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (ΑΥΘΕΝΤΙΚΟΤΗΤΑ). Δηλαδή να γνωρίσει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ. είναι όντως από αυτό τον κύριο και όχι από κάποιον που τον παριστάνει. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή. (ΜΗ ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ).

Οι παραπάνω ιδιότητες (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση ευθύνης) στον ηλεκτρονικό κόσμο αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί , τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

4.1.1. Ο ΡΟΛΟΣ ΤΗΣ ΤΡΑΠΕΖΑΣ

Το internet δεν είναι ούτε ένα σύστημα , ούτε είναι ιδιοκτησία ενός προσώπου , ούτε ελέγχεται από ένα άτομο , ούτε είναι αντικείμενο νομοθεσίας μιας χώρας , ούτε βρίσκεται σε ένα χώρο μόνο. Το e-banking είναι ανοιχτό σύστημα, επομένως, οποιοσδήποτε μπορεί να υποκλέψει , τροποποιήσει ή αμφισβητήσει κάποια μετάδοση . Συνεπώς η ασφάλεια που χρειάζεται είναι διαφορετική από αυτή που απαιτείται στα παραδοσιακά εσωτερικά δίκτυα. Τα πιστωτικά ιδρύματα οφείλουν να προστατεύουν τον εαυτό τους αναπτύσσοντας μια δομή που να εξασφαλίζει τη μέγιστη δυνατή ασφάλεια για το πληροφοριακό σύστημα και τους πελάτες τους. Η προστασία τους, απαιτείται για λόγους ανταγωνιστικότητας , υπευθυνότητας και διασφάλισης των περιουσιακών τους στοιχείων.

Οι τράπεζες λοιπόν, επικεντρώνουν τις προσπάθειές τους στη διασφάλιση της συναλλαγής με τον τελικό χρήστη , σε όλα τα στάδια που περιλαμβάνονται μέχρι την επιτυχή ολοκλήρωσή της . Απαραίτητη είναι η ταυτοποίηση της ίδιας της τράπεζας, του τελικού χρήστη, αλλά και η διασφάλιση του απόρρητου της «συνομιλίας» τους. Επίσης, υπάρχουν και κάποιες επιπρόσθετες δικλείδες ασφαλείας , που ενισχύουν περαιτέρω τις προσπάθειες των τραπεζών στην αντιμετώπιση εξωτερικών απειλών.

ΤΑΥΤΟΠΟΙΗΣΗ ΤΡΑΠΕΖΑΣ

Κάθε τράπεζα επιλέγει έναν αναγνωρισμένο παροχέα (Trusted Third Party) , ο οποίος να είναι σε θέση να πιστοποιήσει την ταυτότητά της στο διαδίκτυο. Ένα παράδειγμα παροχέα τέτοιου είδους πιστοποίησης , ιδιαίτερα φνωστό στο ευρύ κοινό , είναι η εταιρία Verisign . Για τον τελικό χρήστη αυτό μπορεί εύκολα να αναγνωριστεί από την εμφάνιση ενός μικρού εικονιδίου με μορφή λουκέτου στο κάτω μέρος των συγκεκριμένων σελίδων , μέσω του οποίου ο χρήστης μπορεί να επιβεβαιώσει ότι βρίσκεται στο σωστό προορισμό.

ΤΑΥΤΟΠΟΙΗΣΗ ΧΡΗΣΤΗ

Όπως ακριβώς το ATM επιτρέπει μια συναλλαγή μέσω της κάρτας και ενός κωδικού, έτσι και το e-banking απαιτεί την ταυτοποίηση του χρήστη, προτού του επιτρέψει την πρόσβαση στους λογαριασμούς του. Για την ταυτοποίηση των χρηστών e-banking οι τράπεζες ακολουθούν μια κοινή πρακτική , χρησιμοποιώντας το προσωπικό κωδικό χρήστη (username) που αποτελείται από 10 ψηφία σε συνδυασμό με ένα επίσης προσωπικό κωδικό (password) που αποτελείται από 4-6 χαρακτήρες. Ο χρήστης πρέπει να παραλαμβάνει τους δύο προσωπικούς του κωδικούς ξεχωριστά. Με τον τρόπο αυτό διασφαλίζεται ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο ή στα περιεχόμενα των web servers των τραπεζών. Κοινή πρακτική αποτελεί επίσης οι προσωπικοί κωδικοί να μπλοκάρονται μετά από κάποιες λανθασμένες προσπάθειες εισαγωγής του χρήστη , καθώς οι συνεχείς λανθασμένες προσπάθειες θεωρούνται ύποπτες.

Για την περαιτέρω διασφάλιση των χρηστών , ορισμένες τράπεζες έχουν προχωρήσει σε ένα επιπλέον επίπεδο ασφάλειας, με πρόσθετους κωδικούς , αριθμούς εξουσιοδότησης συναλλαγής (TAN) και ψηφιακά πιστοποιητικά. Οι αριθμοί TAN (Transaction Authorization Number) είναι αριθμοί που απαιτούνται για την πραγματοποίηση μιας συναλλαγής , δημιουργούνται από την τράπεζα , δένονται με τον κωδικό του χρήστη και εισάγονται κατά τη διαδικασία της συναλλαγής. ΤΑ PINS και TANS παίζουν το ρόλο της ηλεκτρονικής υπογραφής ενώ σε νεώτερες τεχνολογίες η ανάγνωση της ταυτότητας του πελάτη γίνεται από τις smart cards που εισάγονται σε ειδική συσκευή του υπολογιστή.

Το token είναι συσκευή που χρησιμοποιεί διαδικασία πιστοποίησης δύο επιπέδων , συμπληρωμένη από έναν κωδικό χρήσης ως πρώτο επίπεδο. Τα tokens που παράγουν κωδικούς προσφέρουν μια αποτελεσματική άμυνα απέναντι στην ανίχνευση κωδικών καθώς παράγουν ένα νέο password σε καθορισμένα χρονικά διαστήματα (one time password) ή παρέχουν ένα μοναδικό κωδικό χρήσης σε απάντηση ενός μηνύματος απόκρισης από την τράπεζα (Challenge –Response) . Τα tokens είναι εύκολα στη χρήση ενώ αποτελούν και μια σχετικά φθηνή λύση. Τα One time password tokens χρησιμοποιούνται από μεγάλο αριθμό τραπεζικών οργανισμών για την πιστοποίηση κυρίως εταιρικών πελατών.

Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί το μέσο που παρέχει τη δυνατότητα στο κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-banking . Το πιστοποιητικό, όταν εγκατασταθεί σε κάποιον υπολογιστή, προσφέρει τη δυνατότητα ταυτοποίησης του χρήστη και επιτρέπει συναλλαγές και μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από τον συγκεκριμένο χρήστη. Τα επιπλέον επίπεδα ασφάλειας απαιτούνται συνήθως σε συναλλαγές που περιλαμβάνουν μεταφορές χρηματικών ποσών και όχι για συναλλαγές ενημερωτικού χαρακτήρα. Η

φιλοσοφία είναι παρόμοια με αυτή που ακολουθείται στα γκισέ των τραπεζών , όπου ο υπάλληλος απαιτεί από τον πελάτη την επίδειξη της ταυτότητας του, όταν αυτός ζητήσει την μεταφορά χρημάτων.

ΕΞΑΣΦΑΛΙΣΗ ΤΗΣ ΜΕΤΑΦΟΡΑΣ ΔΕΔΟΜΕΝΩ

Μια επιπρόσθετη δικλείδα ασφάλειας , με την οποία εξασφαλίζεται το απόρρητο κατά τη μεταφορά των δεδομένων, είναι η κρυπτογράφησή τους. Το πρωτόκολλο επικοινωνίας SSL(Secure Sockets Layer) μαζί με την κρυπτογράφηση στα 128bit εξασφαλίζει την ασφάλεια των συναλλαγών μέσω διαδικτύου. Η ανάγκη για εμπιστευτικότητα λοιπόν στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιοδήποτε τρίτο. Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό μέχρι να αποκρυπτογραφηθεί.

Η κρυπτογράφηση με 128bit σημαίνει ότι υπάρχουν 2^{128} πιθανά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων από το Internet explorer στον server της τράπεζας. Γι αυτό το λόγο η κρυπτογράφηση στα 128Bit θεωρείται πρακτικά αδύνατο να παραβιαστεί. Με αυτό τον τρόπο ελέγχεται συνεχώς η αυθεντικότητα της επικοινωνίας μεταξύ του ηλεκτρονικού υπολογιστή του χρήστη και του κεντρικού συστήματος. Σε οποιαδήποτε διαταραχή ή παρεμβολή στην επικοινωνία η συναλλαγή διακόπτεται αμέσως και η επικοινωνία ηλεκτρονικού υπολογιστή και κεντρικού συστήματος πρέπει να αποκατασταθεί από την αρχή.

Ο χρήστης μπορεί να αναγνωρίσει εάν η σελίδα στην οποία βρίσκεται είναι ασφαλής , καθώς το πρωτόκολλο που εμφανίζεται με τη διεύθυνση της τράπεζας μετατρέπεται από http σε https και εμφανίζεται παράλληλα και το χαρακτηριστικό εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας.

Για την ακεραιότητα των μεταδιδόμενων δεδομένων χρησιμοποιείται η ψηφιακή υπογραφή. Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία του δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (δημόσιο-ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της.

Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτως του μεγέθους του παράγεται η «σύνοψή» του , η οποία είναι μια σειρά από bits συγκεκριμένου μεγέθους. Η σύνοψη του

μηνύματος είναι μια ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από τη σύνοψη που δημιουργεί είναι υπολογιστικά αδύνατο κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά τη μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή η ψηφιακή υπογραφή είναι διαφορετική για κάθε μήνυμα , σε αντίθεση με την ιδιόχειρη υπογραφή. Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στη πλήρη κατοχή του , τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στο παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.

Μια ψηφιακή υπογραφή μπορεί να «πλαστογραφηθεί» εάν ο κάτοχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχο του (π.χ. αν χάσει το μέσο στο οποίο έχει αποθηκεύσει το ιδιωτικό κλειδί). Η ψηφιακή υπογραφή επιβεβαιώνει την ταυτότητα του αποστολέα εγγράφου σε ηλεκτρονική μορφή και εξασφαλίζει ότι δεν έχει τροποποιηθεί από τη στιγμή που υπογράφτηκε. Αυτή έχει την τεχνική διάσταση και το ρυθμιστικό κανονιστικό πλαίσιο. Νομικά η προσέγγιση του θέματος σε διεθνές επίπεδο πριν το 1999 μπορούσε να χαρακτηριστεί σαν χάος. Η Ευρωπαϊκή Ένωση όμως με την οδηγία 99/93ΕΚ όρισε το κανονιστικό πλαίσιο για τις ηλεκτρονικές υπογραφές. Όσον αφορά την Ελλάδα , η εναρμόνιση της νομοθεσίας σε αυτό το τομέα έγινε με το ΠΔ 150/2001. Οι νομοθετικές αυτές ρυθμίσεις αναγνωρίζουν τις ηλεκτρονικές υπογραφές σε ένα ευρύ φάσμα εφαρμογών αλλά είναι τεχνολογικά ουδέτερες. Οι νομοθεσίες θεωρούνται ουδέτερες από τεχνολογική άποψη εφόσον δεν υιοθετούν άμεσα ή έμμεσα καμία τεχνολογία σαν αναφορά. Δίνουν δηλαδή ιδιαίτερη βαρύτητα στις νομικές συνέπειες και τον καταμερισμό ευθυνών που προκύπτουν από τη χρήση των ηλεκτρονικών υπογραφών.

ΕΛΕΓΧΟΜΕΝΗ ΠΡΟΣΒΑΣΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΤΗΣ ΤΡΑΠΕΖΑΣ

Η πρόσβαση στα συστήματα των περισσότερων τραπεζών (servers) προστατεύεται από τελευταία τεχνολογία Firewall και IDS (Intrusion Detection Systems) , η οποία επιτρέπει τη χρήση συγκεκριμένων υπηρεσιών , απαγορεύοντας παράλληλα την πρόσβαση σε συστήματα και βάσεις δεδομένων με απόρρητα στοιχεία και πληροφορίες της τράπεζας σε μη αναγνωρισμένους χρήστες. Το firewall είναι ουσιαστικά ένας σύνδεσμος software και hardware που παρεμβάλλεται μεταξύ του internet και της τράπεζας και φιλτράρει τα δεδομένα που κυκλοφορούν σύμφωνα με τις συνθήκες που καθορίζει η τράπεζα.

ΕΠΙΠΛΕΟΝ ΔΙΚΛΕΙΔΕΣ ΑΣΦΑΛΕΙΑΣ

Εισαγωγή στοιχείων εισόδου :Καθώς παρατηρήθηκε η εμφάνιση ιών, οι οποίοι είχαν τη δυνατότητα να καταγράφουν πληκτρολογήσεις χρηστών , ορισμένες τράπεζες υιοθέτησαν τη χρήση εικονικού πληκτρολογίου για την καταχώρηση των στοιχείων χρήστη ή επιλεκτικά την καταχώρηση ορισμένων από τα στοιχεία αυτά. Έτσι ακόμα και αν μπορούσε να υποκλαπεί ο ένας από τους δύο κωδικούς ταυτοποίησης , δεν θα είχε καμία ισχύ η αποκλειστική του χρήση και ο χρήστης θα παρέμενε ασφαλής.

Αυτόματη αποσύνδεση χρήστη: Στις περισσότερες εφαρμογές e-banking , η ολοκλήρωση μιας συναλλαγής επιτρέπεται μέσα σε ένα συγκεκριμένο χρονικό όριο (συνήθως πέντε με δεκαπέντε δευτερόλεπτα) , μετά τη λήξη του οποίου το σύστημα αποσυνδέει το χρήστη αυτόματα.

Υποχρεωτική αλλαγή κωδικών: Η πλειονότητα των τραπεζών υποχρεώνει τους χρήστες e-banking στην άμεση αλλαγή των προσωπικών τους κωδικών με κάποιους της επιλογής τους, οι οποίοι να εντυπώνονται και πιο εύκολα στη μνήμη. Συνήθης πρακτική αποτελεί επίσης η αυτόματη απενεργοποίηση των κωδικών μετά από ένα συγκεκριμένο χρονικό διάστημα , στο οποίο ο χρήστης δεν έχει προχωρήσει σε κάποια συναλλαγή.

Ειδικά για τους εταιρικούς χρήστες προβλέπονται επιπλέον δικαιώματα χρήσης όπως:

- Διπλή υπογραφή ανά συναλλαγή
- Διαφορετικά χρηματικά όρια ανά συναλλαγή
- Διαφορετικά εγκριτικά επίπεδα ή επίπεδα πρόσβασης
- Καθορισμός διαχειριστή ο οποίος ελέγχει και παρακολουθεί τις κινήσεις που διενεργούνται από τους άλλους χρήστες της εταιρίας

ΔΙΑΔΙΚΑΣΙΕΣ

Παράλληλα με την απαραίτητη τεχνολογική υποδομή , η διασφάλιση των ηλεκτρονικών συναλλαγών απαιτεί και την υιοθέτηση αυστηρών διαδικασιών από την τράπεζα, όσον αφορά την ανάπτυξη, διαχείριση και προσφορά της υπηρεσίας e-banking . Είναι κοινή τραπεζική πρακτική , που ακολουθείται και στις υπηρεσίες e-banking , να προστατεύονται τα προγράμματα και τα συστήματα από διαδικασίες που απαιτούν συνδυασμένες ενέργειες δύο ή περισσότερων ανθρώπων από διαφορετικά τμήματα. Παράλληλα όλες οι νέες εφαρμογές σχεδιάζονται και υλοποιούνται κάτω από ιδιαίτερα αυστηρές διαδικασίες ελέγχου προτού παραδοθούν. Τέλος , πολλές τράπεζες επιλέγουν τη συνεργασία με ανεξάρτητους εξωτερικούς φορείς για τον έλεγχο της λειτουργίας των διαδικασιών που ακολουθούν.

4.1.2 Ο ΡΟΛΟΣ ΤΟΥ ΧΡΗΣΤΗ

Οι τράπεζες από μόνες τους δεν είναι σε θέση να εξασφαλίσουν απόλυτα την ασφάλεια των συναλλαγών, είτε ηλεκτρονικών είτε φυσικών. Η προσοχή και η ανάληψη προληπτικών μέτρων από τη μεριά του χρήστη σε συνδυασμό με τις απαραίτητες παροχές από την τράπεζα , μπορούν να εξασφαλίσουν την επιτυχία της συναλλαγής. Ιδιαίτερη προσοχή πρέπει να δίνεται σε περίπτωση που ο υπολογιστής που χρησιμοποιείται δεν ανήκει στο χρήστη (αεροδρόμια, internet cafeé κτλ) κυρίως στο τι επιλέγει να αποθηκεύσει σε αυτόν. Είναι απαραίτητη η εγκατάσταση στον υπολογιστή προγράμματος που να τον προστατεύει από την απειλή ιών. Καθώς παρατηρείται συνεχώς η εμφάνιση καινούργιας μορφής ιών, η συχνή ανανέωση των σχετικών προγραμμάτων είναι επίσης απαραίτητη. Επίσης, οι πελάτες πρέπει να γνωρίζουν ότι οι τράπεζες ούτε ζητούν , ούτε στέλνουν εμπιστευτικά προσωπικά δεδομένα μέσω ηλεκτρονικού ταχυδρομείου (email).

Τέλος, καλό θα ήταν ο χρήστης να αποστηθίζει τους κωδικούς του και να μην τους έχει σε γραπτή μορφή , καθώς υπάρχει ο κίνδυνος να κλαπούν, και να τους αλλάζει τακτικά. Επίσης καλό είναι να μην χρησιμοποιούνται οι κωδικοί που έχουν επιλεχθεί για είσοδο στο e-banking και σε άλλα , μη ασφαλές site . Είναι απαραίτητος ο έλεγχος της διεύθυνσης της ιστοσελίδας, στην οποία θα εισάγει τα στοιχεία του , καθώς μπορεί να αποτελεί αντιγραφή κάποιου τραπεζικού site , με σκοπό την παραπλάνηση και την απόκτηση των προσωπικών του στοιχείων. Στην περίπτωση που η ηλεκτρονική διεύθυνση δεν είναι εμφανής, ένας ακόμη τρόπος επιβεβαίωσης της ταυτότητας της ιστοσελίδας είναι μέσω του εικονιδίου (λουκέτο) , το οποίο εμφανίζεται στις ασφαλείς τραπεζικές σελίδες.

4.2.ΑΠΕΙΛΕΣ-ΚΙΝΔΥΝΟΙ

Αν και οι ηλεκτρονικές επιθέσεις δεν αποτελούν νέο φαινόμενο , η συχνότητα τους τα τελευταία χρόνια αυξάνεται μια και όλο και περισσότερες τράπεζες παρέχουν στους πελάτες τους on line υπηρεσίες. Η αύξηση αυτή δεν είναι τεράστια , εντούτοις όμως αποτελεί ένα ανησυχητικό φαινόμενο μια και 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 e-banking .

Οι επίδοξοι εισβολείς έχουν πολλούς τρόπους πάντως να επιτύχουν τους σκοπούς τους. Παρά τις οποιεσδήποτε τεχνικές αδυναμίες των συστημάτων για on line banking , οι μεγαλύτεροι κίνδυνοι προέρχονται από τον ανθρώπινο παράγοντα. Έρευνες που έχουν γίνει από ειδικούς σε θέματα ασφάλειας αποδεικνύουν ότι στις περισσότερες περιπτώσεις επιθέσεων, οι εισβολείς είχαν την εκούσια ή ακούσια βοήθεια και κάποιου που εργαζόταν στη τράπεζα.

Και χωρίς τη βοήθεια εκ των έσω , πάντως, οι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους , 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 γι' αυτούς, αλλά στη πραγματικότητα ανοίγουν τρύπες ασφάλειας στο σύστημα επιτρέποντας σε χάκερς , να έχουν πρόσβαση σε αυτό.

Οι κλεμμένες πληροφορίες αποτελούν τη πρώτη φάση μιας αρκετά επίπονης διαδικασίας η οποία μπορεί να διαρκέσει μέχρι και εβδομάδες , έτσι ώστε ο χάκερ να υποδυθεί κάποιον άλλο στο διαδίκτυο. Η οποία όμως διευκολύνεται συνεχώς με καινούργια προγράμματα που κυκλοφορούν στην αγορά. Η εποχή που πολλές επιθέσεις θα γίνονται με αυτοματοποιημένο τρόπο δεν απέχει πολύ , σύμφωνα με ειδικούς.

Μια άλλη μέθοδος που τις περισσότερες φορές έχει αποτελέσματα δεν επικεντρώνεται στην τράπεζα ευθέως , αλλά σε μια από τις εταιρίες 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 εταιρίες αυτές να διαχειρίζονται ολόκληρο το δίκτυό τους. Σε αυτή την περίπτωση, ο εισβολέας θα πρέπει να μελετήσει τον τρόπο με τον οποίο οι εταιρίες 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 στο τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες. Δυστυχώς όμως, λόγω αυτής της βιασύνης , οι τράπεζες αφήνουν πολλές τρύπες στα συστήματά τους , κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα.

ΕΙΔΗ ΑΠΕΙΛΩΝ

SNIFFERS : Ένας sniffer είναι ένα πρόγραμμα ή μια συσκευή που παρακολουθεί κρυφά την κίνηση ενός δικτύου με σκοπό να αρπάξει πληροφορία που ταξιδεύει σε αυτό. Ουσιαστικά οι sniffers είναι τεχνολογία υποκλοπής δεδομένων. Λειτουργούν επειδή Ethernet κατασκευάστηκε γύρω από την αρχή του sharing. Η πλειοψηφία των δικτύων χρησιμοποιεί τεχνολογία εκπομπής όπου τα μηνύματα από έναν υπολογιστή μπορούν να διαβαστούν από άλλο υπολογιστή σε αυτό το δίκτυο. Πρακτικά, όλοι οι υπόλοιποι υπολογιστές του δικτύου αγνοούν το μήνυμα πλην αυτού που είναι ο παραλήπτης του. Ωστόσο υπολογιστές μπορούν να διαμορφωθούν ώστε να δέχονται μηνύματα ακόμα και αν δεν είναι γι' αυτούς. Αυτό γίνεται με τη χρήση ενός sniffer.

Key loggers: Το key logger (καταγραφή πληκτρολογήσεων) συμβαίνει όταν καταγράφονται οι πληκτρολογήσεις του χρήστη χωρίς ο ίδιος να το ξέρει ή να το επιτρέπει. Χρησιμοποιείται από επιτήδειους για την κλοπή στοιχείων πιστωτικής κάρτας, τραπεζικών συναλλαγών και προσωπικών κωδικών και αποτελεί σοβαρή απειλή για τη διαρροή προσωπικών/εταιρικών στοιχείων. Η καταγραφή και αποθήκευση των πληκτρολογήσεων γίνεται από ειδικό υλικό το οποίο είναι εύκολο να εγκατασταθεί και ταυτόχρονα δύσκολο να εντοπιστεί. Τα key loggers καταγράφουν και αποθηκεύουν τις πληκτρολογήσεις και τα κλικ του ποντικιού σε το οποίο και αποστέλλουν μέσω internet σε αυτόν που κατασκοπεύει το χρήστη.

Κοινωνική μηχανική: Η κοινωνική μηχανική ορίζεται ως ένα μη τεχνικό είδος παράνομης εισβολής που βασίζεται κυρίως στην ανθρώπινη επικοινωνία και συχνά περιλαμβάνει κόλπα τα οποία ωθούν τους ανθρώπους να καταργήσουν τις οριζόμενες διαδικασίες ασφάλειας. Σενάρια κοινωνικής μηχανικής μπορούν να περιλαμβάνουν για παράδειγμα τηλεφωνική επικοινωνία του κοινωνικού μηχανικού με το χρήστη όπου ο πρώτος προσποιείται ότι είναι μέλος της ομάδας IT που χρειάζεται τους κωδικούς πρόσβασής του χρήστη και άλλες πληροφορίες. **(Αγγέλης, 2005)**

Δούρειοι ίπποι: Ένας δούρειος ίππος (Trojan horse) είναι ένα φαινομενικά χρήσιμο πρόγραμμα για τον υπολογιστή που περιέχει καμουφλαρισμένες εντολές οι οποίες όταν εκτελεστούν δημιουργούν αθέμιτες ή βλαπτικές δράσεις. Παραδείγματα τέτοιων δράσεων αποτελούν η καταστροφή αρχείων , η υποκλοπή δεδομένων, η εγκατάσταση ιών ή άλλων δούρειων ίππων. Γενικά οι δούρειοι ίπποι μπορούν να κάνουν οτιδήποτε μπορεί να κάνει ο χρήστης που τους εγκατέστησε.

Phishing: Το phishing είναι η αποστολή email σε χρήστη προσποιούμενο ότι προέρχεται από νόμιμη επιχείρηση κυρίως τράπεζα με σκοπό να εξαπατήσει το χρήστη και να πάρει ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για κλοπή της ταυτότητας του. Το email προτρέπει το χρήστη να επισκεφτεί ένα website όπου του ζητείται να ενημερώσει τις προσωπικές του πληροφορίες όπως κωδικούς και αριθμούς πιστωτικών καρτών. Το website όμως είναι πλαστό και έχει δημιουργηθεί με σκοπό να κλέψει τη ζητούμενη πληροφορία.

Pharming: Καθώς οι χρήστες και οι οργανισμοί είναι πλέον περισσότερο προσεκτικοί στις επιθέσεις phishing , οι απατεώνες προχώρησαν ένα βήμα παραπάνω. Η νέα τάση στην ηλεκτρονική υποκλοπή κωδικών ονομάζεται pharming .

Οι βασικές διαφορές του pharming απέναντι στο phishing είναι δύο:

- Η επίθεση μπορεί να γίνει μαζικά σε πολλούς χρήστες και όχι μεμονωμένα σε κάθε χρήστη.
- Η μετακίνηση σε pharming site γίνονται χωρίς την παρεμβολή του χρήστη.

Fake banks: Τέλος, ιδιαίτερα διαδεδομένη είναι η χρήση ψευδών τραπεζικών sites (fake banks). Στη περίπτωση αυτή οι εισβολείς δημιουργούν sites που υποτίθεται ότι είναι ηλεκτρονικές τράπεζες. Αρκετοί είναι οι χρήστες που εξαπατώνται και διενεργούν εικονικές συναλλαγές χωρίς καμία υπόσταση δίνοντας έτσι κωδικούς , αριθμούς λογαριασμών και καρτών εν αγνοία τους.

4.3 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Για την αντιμετώπιση των ανωτέρω απαιτούνται σύγχρονα συστήματα διακίνησης πληροφοριών που να παρέχουν υπηρεσίες πιστοποίησης ταυτότητας του αποστολέα , κρυπτογράφησης , αποκρυπτογράφησης, ανίχνευσης αλλοιώσεων , τήρησης του απορρήτου των δεδομένων και μη αποποίηση ευθύνης. Συνεπώς, για ασφαλή επικοινωνία μέσω e-banking πρέπει να τηρείται το απόρρητο κατά την πρόσβαση στους servers και τα μηνύματα να μη διαβάζονται από τρίτους. Η εξασφάλιση της μυστικότητας και του απορρήτου των ηλεκτρονικών μηνυμάτων ή δεδομένων επιτυγχάνεται με διάφορες μεθόδους

κρυπτογράφησης. Η ακεραιότητα σημαίνει ότι τα μηνύματα δεν έχουν τροποποιηθεί και προστατεύονται με την ψηφιακή υπογραφή. Όσον αφορά την πιστοποίηση ταυτότητας , ότι δηλαδή τα μηνύματα προέρχονται από τον συγκεκριμένο αποστολέα , αυτή βεβαιώνεται με πιστοποιητικά από έμπιστη τρίτη οντότητα. **(Αγγέλης, 2005)**

Οι περισσότερες ελληνικές τράπεζες ακολουθούν το πρωτόκολλο SET (Secure Electronic Transaction), που υποστηρίζεται από τους δύο σημαντικότερους χρηματοπιστωτικούς οργανισμούς , τη Master card και τη Visa , καθώς και από εταιρίες όπως Microsoft και Netscape . Το πρωτόκολλο Set βασίζεται στη κρυπτογραφία.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

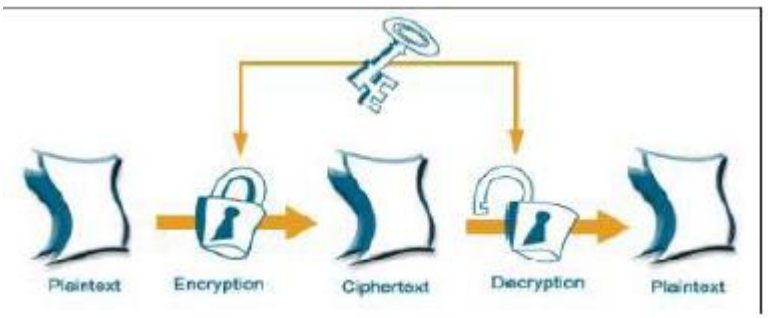
Δύο είναι οι κύριες μέθοδοι κρυπτογράφησης , η συμμετρική και η ασύμμετρη. Στη συμμετρική η κρυπτογράφηση υλοποιείται με τη χρήση του ίδιου κλειδιού , τόσο στη κωδικοποίηση όσο και στην αποκωδικοποίηση. Πράγμα το οποίο σημαίνει ότι ο αποστολέας και ο παραλήπτης του μηνύματος μοιράζονται το ίδιο κλειδί. 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.

Πλεονεκτήματα κρυπτογράφησης

- Είναι ασφαλές
- Είναι γρήγορο
- Έχει ευρύτατη χρήση και διάδοση

Μειονεκτήματα κρυπτογράφησης

- Η διαχείριση του μυστικού κλειδιού είναι πολύπλοκη , απαιτώντας και από τα δύο μέρη να διατηρούν τον απόλυτο έλεγχο στην ανταλλαγή κλειδιών
- Δεν περιλαμβάνει ξεχωριστό μηχανισμό αυθεντικότητας
- Δεν έχει non repudiation (αδιάσειστη απόδειξη συμμετοχής και του αποστολέα και του παραλήπτη



Η ασύμμετρη είναι επίσης γνωστή και ως κρυπτογράφηση με δημόσιο/ιδιωτικό κλειδί και περιλαμβάνει δύο κλειδιά. Ο αποστολέας για να σφαλίσει την πληροφορία , κάνει την κρυπτογράφηση χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Ωστόσο ο παραλήπτης μπορεί να διαβάσει την πληροφορία μόνο με τη χρήση του ιδιωτικού του κλειδιού. Μια διαδεδομένη τεχνική δημοσίου κλειδιού είναι η RSA και η κύρια χρήση της είναι για πιστοποίηση και ασφαλή ανταλλαγή κλειδιών κρυπτογράφησης και των ψηφιακών υπογραφών. Το μήκος του κλειδιού ποικίλει από 40 έως 1.024bits.

Ένα από τα πλεονεκτήματα της κρυπτογράφησης με δημόσιο / ιδιωτικό κλειδί είναι ότι απλοποιεί τη διαχείριση των κλειδιών. Ενώ το κυριότερο μειονέκτημα είναι ότι η κρυπτογράφηση με δημόσιο κλειδί είναι πολύ πιο αργή από την κρυπτογράφηση με ιδιωτικό κλειδί. Για το λόγο αυτό χρησιμοποιείται κυρίως για την πιστοποίηση τμημάτων μηνυμάτων , παρά για την κρυπτογράφηση ενός ολόκληρου μηνύματος.

Πρακτικά τώρα μιλώντας για την κρυπτογράφηση το επιθυμητό αποτέλεσμα από μεριάς τραπεζών είναι να διασφαλίζεται το μήνυμα και να πιστοποιείται ο αποστολέας του. Η ορθή προσέγγιση είναι να χρησιμοποιούνται άρρηκτα συνδεδεμένες οι συμμετρικές και ασύμμετρες τεχνολογίες κρυπτογράφησης, της συμμετρικής για κρυπτογράφηση μεγάλων όγκων πληροφορίας (λόγω της ταχύτητας της) και της ασύμμετρης για πιστοποίηση. Στην πράξη αυτό σημαίνει πως εάν μια τράπεζα θέλει να στείλει ένα ασφαλές μήνυμα πρέπει να κάνει δύο πράγματα. Πρώτα να διασφαλίσει ότι το μήνυμα είναι ασφαλές χρησιμοποιώντας DES ή triple-DES για να κρυπτογραφήσει το μήνυμα και στη συνέχεια να πιστοποιήσει τον εαυτό της. Αυτό το κάνει χρησιμοποιώντας μια hash συνάρτηση (μια μαθηματική συνάρτηση που προκύπτει από το μήνυμα) , ώστε να δημιουργήσει μια ανασκόπηση του μηνύματος από το κείμενο. Στη συνέχεια με RSA η τράπεζα κρυπτογραφεί την ανασκόπηση του μηνύματος, χρησιμοποιώντας μόνο το δημόσιο κλειδί της τράπεζας.

Με αυτόν τον τρόπο , οι παραλήπτες γνωρίζουν ότι το μήνυμα προέρχεται από την τράπεζα. Οι παραλήπτες από τη μεριά τους, χρησιμοποιούν το δημόσιο κλειδί της τράπεζας για την αποκρυπτογράφηση της ανασκόπησης του μηνύματος. Έτσι εγκρίνοντας το αποκρυπτογραφημένο hash σύνολο με αυτό που υπολόγισαν ανεξάρτητα από το μήνυμα μπορούν να έχουν ένα υψηλό επίπεδο ασφάλειας ότι το μήνυμα προέρχεται από την τράπεζα και δεν έχει αλλοιωθεί τίποτα κατά τη διάρκεια της μετάδοσης.

PKI

Η τεχνολογία PKI (public key infrastructure) είναι πολύ γνωστή . Μπορεί να χρησιμοποιηθεί για να αναγνωρίσει οντότητες , να κρυπτογραφήσει πληροφορία και να υπογράψει ηλεκτρονικά έγγραφα. Επίσης, αναγνωρίζει και διαχειρίζεται σχέσεις μεταξύ των μελών μιας ηλεκτρονικής ανταλλαγής δεδομένων, εξυπηρετεί ένα μεγάλο εύρος αναγκών ασφαλείας , συμπεριλαμβανομένων ελέγχου πρόσβασης, εμπιστευτικότητα , ακεραιότητα, πιστοποίηση και μη αποποίηση ευθύνης. Η PKI χρησιμοποιεί επίσης μοναδικά ψηφιακά πιστοποιητικά για να ασφαλίσει το e-banking και το e-commerce , το e-mail , την ανταλλαγή δεδομένων. Η τεχνολογία αυτή τέλος, χρησιμοποιείται για να πιστοποιήσει την ταυτότητα και τα δεδομένα του κάθε χρήστη. Επιπρόσθετα, η αρχή πιστοποίησης, που είναι αυτή που εγγυάται την PKI τεχνολογία παρέχει ένα ολοκληρωμένο πακέτο διαχείρισης των δημοσίων κλειδιών και πιστοποιητικών , που περιλαμβάνει την έκδοση , την πιστοποίηση, την αποθήκευση , την πρόσβαση, το backup, την ενημέρωση και την ανανέωση. Όλοι οι χρήστες της PKI πρέπει να έχουν μία εγκεκριμένη ταυτότητα , η οποία είναι αποθηκευμένη σε ένα ψηφιακό πιστοποιητικό που εκδίδει η αρχή πιστοποίησης. Αυτό λειτουργεί ως ο σύνδεσμος της εμπιστοσύνης στο PKI. Απομακρυσμένοι χρήστες και δικτυακοί τόποι που χρησιμοποιούν δημόσια και ιδιωτικά κλειδιά και πιστοποιητικά δημοσίων κλειδιών μπορούν να πιστοποιηθούν με υψηλό βαθμό εμπιστοσύνης. Η πιστοποίηση αυτή, εξαρτάται από τρεις συνθήκες:

- Πρέπει να κατοχυρώνεται ότι το δημόσιο κλειδί που κατέχει το κάθε μέρος , δεν έχει κλαπεί ή αντιγραφεί από τον ιδιοκτήτη του
- Το πιστοποιητικό πρέπει να εκδίδεται στον ιδιοκτήτη σε αρμονία με την καταγεγραμμένη πολιτική του εκδότη πιστοποιητικών
- Οι πολιτικές του εκδότη πιστοποιητικών πρέπει να ικανοποιούν τα εμπλεκόμενα μέρη , όσον αφορά την πιστοποίηση της ταυτότητας
- Από την στιγμή που ικανοποιούνται αυτές οι τρείς συνθήκες , τότε υπάρχει η σωστή βάση για την εξασφάλιση της ασφάλειας.

Δημόσια και ιδιωτικά κλειδιά: Η PKI χρησιμοποιεί ένα σύστημα ζευγαριών κλειδιών, που είναι ασύμμετρα , συνδέονται μαθηματικά μεταξύ τους και εκτελούν αντίθετες ενέργειες , δηλαδή ότι κλειδώνει το ένα κλειδί , μόνο το άλλο μπορεί να ξεκλειδώσει.

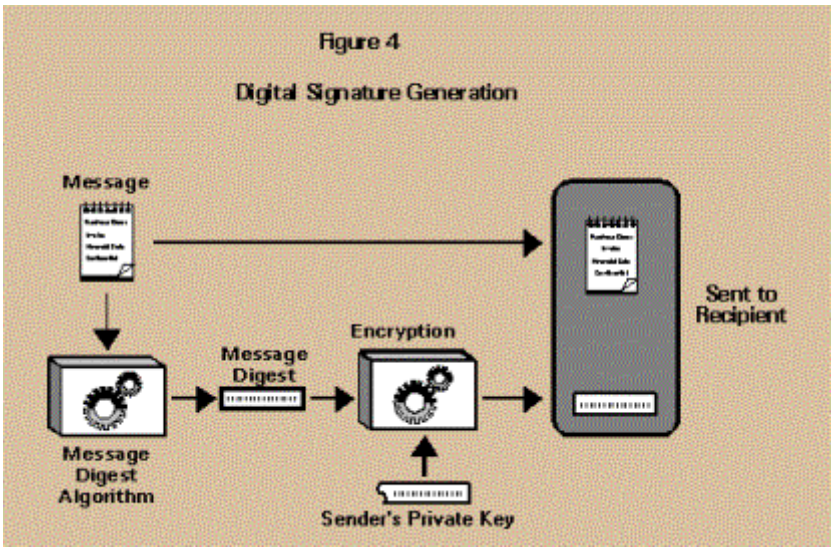
Τα δημόσια και ιδιωτικά κλειδιά είναι μοναδικά για κάθε χρήστη σε PKI σύστημα. Το ιδιωτικό κλειδί δημιουργείται πρώτα. Μια μαθηματική συνάρτηση εφαρμόζεται στο ιδιωτικό κλειδί για τη δημιουργία του δημόσιου κλειδιού. Είναι πρακτικά αδύνατο να ανιχνευτεί το ιδιωτικό κλειδί κάποιου από το δημόσιο κλειδί του. Τα ιδιωτικά κλειδιά πρέπει να προστατεύονται από υποκλοπές και συνήθως

αποθηκεύονται σε φυσικές συσκευές όπως είναι οι έξυπνες κάρτες ή τα tokens . Τα δημόσια κλειδιά από την άλλη πλευρά , είναι διαθέσιμα σε όλους. Οποιοσδήποτε επιθυμεί να κάνει ασφαλείς συναλλαγές χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη ως μέρος της διαδικασίας κρυπτογράφησης . Κρυπτογραφώντας κάτι με το δημόσιο κλειδί κάποιου άλλου , εξασφαλίζεται ότι μόνο αυτός μπορεί να το αποκωδικοποιήσει. Αν για οποιοδήποτε λόγο το μήνυμα αποστολής μιας κρυπτογραφημένης συναλλαγής παραβιαστεί , είναι απίθανο αυτό το μήνυμα να αποκωδικοποιηθεί και εκτελεστεί.

Ψηφιακές υπογραφές: όταν παραλαμβάνεται ένα κρυπτογραφημένο μήνυμα ή συναλλαγή , είναι σημαντικό να υπάρχει η δυνατότητα πιστοποίησης ότι ο αποστολέας του, είναι όντως αυτός που ισχυρίζεται. Αυτό επιτυγχάνεται μέσω της ψηφιακής υπογραφής. Μιας μοναδικής διαδικασίας υπογραφής μηνύματος που αποκαλύπτει την ταυτότητα του αποστολέα και πιστοποιεί την ακεραιότητα του μηνύματος. Οι ψηφιακές υπογραφές είναι αδιάψευστες , μοναδικές για κάθε συναλλαγή και είναι σχεδόν απίθανο να αντιγραφούν ή να μεταφερθούν. Αλλιώς μπορούν να οριστούν σαν ένα σύστημα μέσω του οποίου η μια πλευρά μπορεί να στέλνει ένα υπογεγραμμένο μήνυμα στην άλλη πλευρά με τέτοιο τρόπο ώστε:

- Ο παραλήπτης μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο αποστολέας
- Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος
- Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του

Η υπογραφή είναι μια μαθηματική συνάρτηση που περιλαμβάνει το πρωτότυπο μήνυμα και το ιδιωτικό κλειδί του αποστολέα. Το πρώτο βήμα στη διαδικασία υπογραφής περιλαμβάνει την εκτέλεση ενός μαθηματικού αλγορίθμου , γνωστός ως hash. Ο hash παίρνει το πρωτότυπο μήνυμα και το μειώνει σε ένα καθορισμένο μέγεθος 160bit χαρακτήρων, την ανασκόπηση μηνύματος. Η ανασκόπηση είναι η μαθηματική αναπαράσταση του πρωτότυπου μηνύματος. Με αλλαγή ενός μόνο χαρακτήρα αλλάζει και η ανασκόπηση. Στη συνέχεια, η ανασκόπηση κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα και το αποτέλεσμα της κρυπτογράφησης είναι γνωστό ως ψηφιακή υπογραφή. Το επόμενο στάδιο της PKI διαδικασίας είναι η ασφάλιση του μηνύματος και της υπογραφής. Αυτό γίνεται κρυπτογραφώντας το μήνυμα και την υπογραφή. Η κρυπτογράφηση περιλαμβάνει μια μοναδική μαθηματική συνάρτηση που μετασχηματίζει τα δεδομένα σε μια κωδικοποιημένη μορφή που απαιτεί ένα κλειδί κρυπτογράφησης για να ξεκλειδωθεί. Η ισχύς του κλειδιού εξαρτάται από τον αριθμό των bits που έχει.



Από τη στιγμή που θα κρυπτογραφηθεί το μήνυμα και η υπογραφή , το επόμενο στάδιο είναι η ασφαλής μεταφορά του κλειδιού που απαιτείται για την αποκρυπτογράφηση. Ο τύπος του κλειδιού που χρησιμοποιείται σε κρυπτογράφηση μηνύματος είναι γνωστό ως συμμετρικό κλειδί. Ένα συμμετρικό κλειδί είναι μοναδικό κλειδί που δημιουργείται για χρήση μιας φοράς και είναι ικανό τόσο να κλειδώσει όσο και να ξεκλειδώσει το μήνυμα. Αποστολέας και παραλήπτης χρειάζονται το ίδιο κλειδί για την κωδικοποίηση και αποκωδικοποίηση του μηνύματος. Η PKI προσθέτει ένα επιπλέον επίπεδο ασφαλείας κρυπτογραφώντας το συμμετρικό κλειδί μιας χρήσης με το δημόσιο κλειδί του παραλήπτη , ώστε μόνο αυτός να μπορεί να το αποκωδικοποιήσει με το ιδιωτικό του κλειδί. Το κρυπτογραφημένο συμμετρικό κλειδί μιας χρήσης επισυνάπτεται στο κρυπτογραφημένο μήνυμα και το μήνυμα είναι έτοιμο να σταλεί.

Ψηφιακά πιστοποιητικά: Τα ψηφιακά πιστοποιητικά ή πιστοποιητικά δημόσιου κλειδιού είναι ηλεκτρονικές φόρμες ταυτοποίησης που μπορούν να επικυρωθούν από μια αναγνωρισμένη αρχή. Όλοι οι PKI χρήστες πρέπει να έχουν αυτή τη μορφή ταυτοποίησης. Τα πιστοποιητικά μπορούν να περιέχουν μια ποικιλία πληροφοριών, συμπεριλαμβανομένων της επωνυμίας του κατόχου , του δημοσίου κλειδιού , της ημερομηνίας λήξης του πιστοποιητικού , των λειτουργιών που μπορεί να εκτελέσει το δημόσιο κλειδί , της ψηφιακής υπογραφής του εκδότη , του σειριακού του αριθμού και της μεθόδου κρυπτογράφησης. Τα ψηφιακά πιστοποιητική χρησιμοποιούνται για να πιστοποιήσουν ή να επαληθεύσουν ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.

Αρχές πιστοποίησης: Ο κύριος σκοπός μιας αρχής πιστοποίησης είναι η έκδοση ψηφιακών πιστοποιητικών και η επιβεβαίωση του ατόμου που συνδέεται με το πιστοποιητικό. Η αρχή πιστοποίησης προσθέτει ένα επιπλέον επίπεδο εμπιστοσύνης στις συναλλαγές που βασίζονται στην PKI.

- Ο συνδρομητής (αποστολέας) αιτείται στην αρχή πιστοποίησης ένα ψηφιακό πιστοποιητικό .
- Η αρχή πιστοποίησης επαληθεύει τον συνδρομητή και εκδίδει το ψηφιακό πιστοποιητικό.
- Η αρχή πιστοποίησης δημοσιεύει το πιστοποιητικό , σε ένα on line repository
- Ο συνδρομητής υπογράφει το μήνυμα του με ένα ιδιωτικό κλειδί και τα στέλνει στους παραλήπτες.

- Ο παραλήπτης επαληθεύει την ψηφιακή υπογραφή με χρήση του δημόσιου κλειδιού του αποστολέα και αιτείται επαλήθευση του ψηφιακού πιστοποιητικού του αποστολέα από το δημόσιο repository. Το repository αναφέρει status του ψηφιακού πιστοποιητικού του αποστολέα.

Αφού το υπογεγραμμένο και κρυπτογραφημένο μήνυμα παραληφθεί , το μήνυμα αποκρυπτογραφείται και επαληθεύεται η ακεραιότητα του περιεχομένου του. Το συμμετρικό κλειδί μιας χρήσης που χρησιμοποιήθηκε για την κωδικοποίηση του μηνύματος, αποκρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί του παραλήπτη. Στη συνέχεια, χρησιμοποιείται για την αποκωδικοποίηση του κρυπτογραφημένου μηνύματος και της υπογραφής.

ΠΙΣΤΟΠΟΙΗΣΗ ΔΥΟ ΠΑΡΑΓΟΝΤΩΝ

Οι περισσότεροι ειδικοί του IT συμφωνούν ότι η πιστοποίηση δύο παραγόντων είναι ζωτική για την αποτελεσματική ασφάλεια δικτύων. Οι δύο παράγοντες μεταφράζονται ως κάτι που γνωρίζει ο χρήστης (π.χ. password) και κάτι που έχει στην κατοχή του και είναι αποκλειστικά δικό του (π.χ. token, κινητό τηλέφωνο, ψηφιακό πιστοποιητικό κ.α.). Το επίπεδο ασφαλείας αυξάνεται σε κάθε περίπτωση χρήσης extraPIN (μέσο κινητού τηλεφώνου ή και συσκευής παραγωγής κωδικών μιας χρήσης). Ωστόσο κάθε οργανισμός πρέπει να επιλέξει ποια από όλες τις παρεχόμενες λύσεις πιστοποίησης δύο παραγόντων είναι κατάλληλη για τις ανάγκες του. Υπάρχουν τρείς εναλλακτικές λύσεις:

- Challenge-Response
- Event-Synchronous
- Time-Synchronous

Παρακάτω παρατίθενται οι διαφορές μεταξύ τριών λύσεων:

- Challenge-Response

1. Ο χρήστης εισάγει username και password
2. Ο server στέλνει ένα challenge
3. Ο χρήστης εισάγει το challenge
4. Ένα response εμφανίζεται στην οθόνη του token
5. Ο χρήστης εισάγει το response και γίνεται το validation

- Event-Synchronous

1. Ο χρήστης ενεργοποιεί τον επόμενο κωδικό του token πατώντας ένα κουμπί σε αυτό.
2. Ο χρήστης εισάγει username και passcode.
3. Ο server πιστοποιεί τον χρήστη ταιριάζοντας το passcode του χρήστη passcode του server.

- Time-synchronous

1. Ο χρήστης εισάγει username και passcode
2. Ο server και το token υπολογίζουν τον κωδικό του token συνδυάζοντας το seed και την τρέχουσα ώρα Greenwich. Ο server πιστοποιεί τον χρήστη ταιριάζοντας τον passcode του χρήστη με το passcode του server.

Η πιστοποίηση με Time-synchronous ταυτοποίηση θεωρείται πιο αποτελεσματική από τις άλλες δύο για τους εξής λόγους:

- Ενίσχυση ασφάλειας: Η time-synchronous προσέγγιση της ταυτοποίησης δύο παραγόντων είναι πολύ πιο ασφαλείς από τις λοιπές. Η τεχνολογία αυτή βασίζεται στο μυστικό seed του token , που ουσιαστικά δεν μπορεί να σπάσει. Οι άλλες προσεγγίσεις είναι λιγότερο τεχνικά εξελιγμένες και ευάλωτες.
- Ευκολία χρήσης: Είναι διαδικασία δύο βημάτων μόνο, σε αντίθεση με τις άλλες δύο που είναι πέντε και τριών αντίστοιχα. Άρα και πιο ευάλωτες σε λάθη χρηστών.
- Μικρότερο διαχειριστικό κόστος: Επειδή απαιτούνται λίγα μόνο πατήματα πλήκτρων, υπάρχουν μικρότερες πιθανότητες να κλειδωθεί ο χρήστης και άρα να πρέπει ο διαχειριστής να τον ξεκλειδώσει.
- Φορητότητα: Τα time-synchronous tokens είναι εντελώς φορητά, επειδή σε καμία περίπτωση δεν εγκαθίσταται μόνιμα στον υπολογιστή του χρήστη. **(ΑΓΓΕΛΗΣ,2005)**

ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Πολλά είναι τα παραδείγματα των έξυπνων καρτών που χρησιμοποιούνται στη καθημερινή ζωή με την κάρτα SIM του κινητού μας τηλεφώνου να αποτελεί ένα από τα πιο χαρακτηριστικά. Οι έξυπνες κάρτες μπορούν να αποθηκεύσουν μεγάλη ποσότητα δεδομένων και παρέχουν δυνατότητες κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια των περιεχομένων τους. Διαθέτουν ενσωματωμένο μικροεπεξεργαστή και παρέχουν ισχυρή αυθεντικοποίηση μέσω κωδικού pin αλλά και της φυσικής κατοχής.

Η τεχνολογία των έξυπνων καρτών μπορεί να χρησιμοποιηθεί για να δημιουργήσει κάρτες που παρέχουν ισχυρή ταυτοποίηση κάτι που επιτυγχάνεται με την ενσωμάτωση ηλεκτρονικών κλειδιών στη κάρτα. Ένα μεγάλο ζήτημα σχετικά με τις έξυπνες κάρτες είναι η χρήση τους για πιστοποίηση. Στην πραγματικότητα οι έξυπνες κάρτες μπορούν να παρέχουν προσωπικές πληροφορίες του κατόχου , κλειδιά για ψηφιακή υπογραφή κ.α. Φυσικά, για να αποφευχθεί το γεγονός οι πληροφορίες που προσφέρει μία κάρτα , να καταντήσουν περιορισμός και όχι πλεονέκτημα για τις ηλεκτρονικές υπηρεσίες , οι τελευταίες πρέπει να σχεδιάζονται χωρίς να λαμβάνουν υπόψη τις έξυπνες κάρτες που υπάρχουν. Αυτό συμβαίνει γιατί αρκετοί πελάτες δεν θα έχουν στην κατοχή τους για μεγάλο χρονικό διάστημα τέτοιου είδους κάρτες.

ΠΙΣΤΟΠΟΙΗΣΗ ΔΥΟ ΠΑΡΑΓΟΝΤΩΝ ΚΑΙ PKI

Για περισσότερη ασφάλεια, ένας τραπεζικός οργανισμός μπορεί να απαιτεί το ψηφιακό πιστοποιητικό του πελάτη να αποθηκεύεται στο token ή σε μια έξυπνη κάρτα. Οι έξυπνες κάρτες και άλλες συσκευές για τον καταναλωτή που περιέχουν ηλεκτρονικά τσιπς είναι πιο ακριβές λύσεις από λύσεις λογισμικού. Έχουν όμως το πλεονέκτημα , αποθηκεύοντας ιδιωτικά κλειδιά σε tokens αντί στο σκληρό δίσκο του υπολογιστή να αποτρέπουν την πρόσβαση μη εγκεκριμένων χρηστών στον υπολογιστή του πελάτη με σκοπό την περιγραφή των κρυπτογραφημένων κλειδιών χωρίς να έχει γνώση ο χρήστης.

USB TOKENS

Μια δυνατή λύση είναι τα USB tokens. Τα USB όταν συνδυάζονται με την PKI τεχνολογία παρέχουν ισχυρή πιστοποίηση δύο παραγόντων. Τα πλεονεκτήματα που απορρέουν είναι τα ακόλουθα:

Υψηλή ασφάλεια: Οι συσκευές δε μπορούν να αντιγραφούν, ενώ το PIN τους αποθηκεύεται κρυπτογραφημένο , έτσι προστατεύεται το PKI ψηφιακό ID του χρήστη από κλοπή.

Πολλές δυνατότητες: Το PKI ψηφιακό ID του χρήστη μπορεί να χρησιμοποιηθεί για πολλές λειτουργίες όπως πιστοποίηση , ψηφιακή υπογραφή ,κρυπτογράφηση κ.α. Επίσης , το ψηφιακό ID μπορεί να χρησιμοποιηθεί για ασφάλεια του χρήστη σε περισσότερες από μία εφαρμογές.

Ευκολία χρήσης: Τα USB tokens μπορούν να μεταφέρονται εύκολα. Συνδέονται εύκολα με τον υπολογιστή μέσω USB θύρας και δεν απαιτούν επιπρόσθετο εξοπλισμό. Βοηθούν το χρήστη να μη χρειάζεται να απομνημονεύει πολλούς κωδικούς , αφού τα αναγνωριστικά του αποθηκεύονται με ασφάλεια στο token.

SINGLE SIGN ON (SSO)

Καθώς τα IT συστήματα πολλαπλασιάζονται για να υποστηρίξουν τις επιχειρηματικές διαδικασίες , οι χρήστες και οι διαχειριστές τους αντιμετωπίζουν ένα αυξανόμενο πολύπλοκο περιβάλλον για να ολοκληρώσουν τις εργασίες τους. Προβλήματα αντιμετωπίζουν και οι administrators των συστημάτων που πρέπει να διαχειρίζονται λογαριασμούς χρηστών μέσα σε κάθε σύστημα και να διασφαλίζουν την ακεραιότητα επιβολής της πολιτικής ασφάλειας.

Η παραδοσιακή λύση για την πρόσβαση σε πολλαπλά συστήματα είναι η παροχή διαφορετικών κωδικών για είσοδο σε όλα τα domains , primary και secondary. Συνεπώς , ο χρήστης που έχει καταχωρήσει τα αναγνωριστικά στο primary domain , δε μπορεί να αιτηθεί υπηρεσίες από τα secondary παρά μόνο εισάγοντας κωδικούς χρήσης για την πρόσβαση σε αυτά. Η συγκεκριμένη προσέγγιση , τόσο από άποψη χρηστικότητας , όσο και από άποψη ασφάλειας , δίνει αφορμή για την ανάγκη συντονισμού και ενοποίησης, όπου αυτό είναι δυνατό, των λειτουργιών εισόδων των χρηστών και των λειτουργιών διαχείρισης των λογαριασμών των χρηστών , ώστε αυτές να βρίσκονται σε ένα ενιαίο περιβάλλον μέσα στον οργανισμό.

Μια υπηρεσία που παρέχει τέτοιο συντονισμό και ενοποίηση , δίνει πολλά πλεονεκτήματα. Όπως:

- Μείωση του χρόνου που καταναλώνουν οι χρήστες για είσοδο σε διαφορετικές υπηρεσίες.
- Μείωση της πιθανότητας λαθών στις διαδικασίες sign on.
- Βελτίωση της ασφάλειας εξαιτίας του γεγονότος ότι ο χρήστης δε χρειάζεται να διατηρεί και να θυμάται πολλά sets κωδικών.
- Μείωση του χρόνου διαχείρισης λογαριασμών χρηστών για τους administrators.
- Βελτίωση της ασφάλειας μέσω της ενσωματωμένης δυνατότητας για τους administrators να συντηρούν την ακεραιότητα της δομής διαχείρισης χρηστών.

Τέτοιου είδους υπηρεσία καλείται single sign on. Το σύστημα συλλέγει όλη την πληροφορία του sign on στο primary domain , που περιλαμβάνει όλα τα αναγνωριστικά που απαιτούνται για secondary domain. Η πληροφορία αυτή που δίνει ο χρήστης χρησιμοποιείται από την sso υπηρεσία ώστε να πιστοποιεί το χρήστη κάθε φορά που αυτός αλληλεπιδρά με άλλα domains. Δηλαδή, το πρόσωπο επικυρώνει μια μόνο φορά την ταυτότητα του για την έναρξη μιας συνόδου εργασίας , ανεξάρτητα από το που βρίσκονται οι πληροφορίες όπου θέλει να γίνει η πρόσβαση. Με τη διαδικασία αυτή, επιτυγχάνεται τόσο ενισχυμένη ασφάλεια όσο και συγχρονισμός των κωδικών πρόσβασης.

Από άποψη διαχείρισης το μοντέλο SSO , προσφέρει ένα περιβάλλον διαχείρισης μοναδικών λογαριασμών χρηστών , μέσω του οποίου όλα τα domains διαχειρίζονται και συντονίζονται με ένα συγκεκριμένο τρόπο.

Σημαντικά θέματα ασφαλείας σχετικά με την SSO είναι:

Το secondary domain πρέπει να εμπιστεύεται το primary domain ώστε να βεβαιώνουν ορθά την ταυτότητα και αναγνωριστικά πιστοποίησης του χρήστη και να προστατεύουν τα αναγνωριστικά πιστοποίησης που χρησιμοποιούνται για την επαλήθευση της ταυτότητας του χρήστη στο secondary domain από μη εγκεκριμένη χρήση.

Τα αναγνωριστικά πιστοποίησης πρέπει να προστατεύονται όταν μεταδίδονται μεταξύ primary και secondary domain απέναντι σε απειλές υποκλοπής που μπορούν να οδηγήσουν σε καλά καλυμμένες επιθέσεις.

FIREWALLS

Φράγμα ασφαλείας ονομάζεται ένα σύστημα που αποτελείται από δικτυακά στοιχεία τα οποία τοποθετούνται μεταξύ δύο δικτύων και το οποίο έχει τα ακόλουθα χαρακτηριστικά:

- Όλη η δικτυακή κίνηση από και προς το εσωτερικό δίκτυο πρέπει να περάσει μέσα από το σύστημα.
- Η διέλευση επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες, όπως αυτή καθορίζεται από την πολιτική ασφαλείας.
- Είναι αδιαπέραστο σε απόπειρες διείσδυσης.

Ένα firewall είναι μια μέθοδος προστασίας που υλοποιείται σε επίπεδο υλικού ή και λογισμικού και χρησιμοποιείται για να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Πρόκειται για μια ειδική εφαρμογή που απομονώνει το σύστημά μας από το διαδίκτυο και στην ουσία το καθιστά μη ορατό για τον έξω κόσμο, ακόμα και αν είναι on line. Επιπλέον, με βάση κάποιους συγκεκριμένους κανόνες ελέγχει και κατά συνέπεια επιτρέπει ή εμποδίζει να εισέλθουν στο σύστημα ή να εξέλθουν από αυτό τα πακέτα δεδομένων του διαδικτύου. Αναγκάζει όλη την κίνηση δεδομένων να κατευθυνθεί ή να δρομολογηθεί προς αυτό , όπου μπορεί να εξεταστεί και να αποφασιστεί αν θα επιτραπεί η διέλευσή της. Δηλαδή, προσπαθεί να αποτρέψει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία από και προς το ενδοεπιχειρησιακό δίκτυο καθώς και να επιτρέψει στον οργανισμό να επιβάλει μια πολιτική ασφαλείας σχετικά με τη ροή των δεδομένων μεταξύ του ιδιόκτητου δικτύου και του διαδικτυακού. **(Πομπόρτσης, Παπαδημητρίου 2003)**

Ακόμη, το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο ενώ επίσης προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού. Επίσης, υπάρχει η δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης. Ωστόσο, το firewall δε μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών που προέρχονται από το εσωτερικό του οργανισμού ή από συνδέσεις οι οποίες δε προέρχονται από αυτό.

ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΑΣΦΑΛΕΙΑΣ SERVERS (SSL certificates)

Το SSL (Secure Sockets Layer) είναι ευέλικτο, γενικού σκοπού σύστημα κρυπτογράφησης για την προστασία της επικοινωνίας μέσω του Παγκόσμιου ιστού , το οποίο είναι ενσωματωμένο και στα προγράμματα πλοήγησης της Netscape και της Microsoft. Το πρωτόκολλο SSL παρέχει κρυπτογράφηση δεδομένων , πιστοποίηση εξυπηρέτη, ακεραιότητα μηνυμάτων και προαιρετική πιστοποίηση του πελάτη. Έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων , από τα οποία το ένα λειτουργεί ως πελάτης και το άλλο σαν εξυπηρέτης. Αποτελείται δε από δύο μέρη: το SSL Handshake Protocol (SSLHP), και το SSL Record Protocol (SSLRP).

Το απόρρητο της επικοινωνίας εξασφαλίζεται με την κρυπτογράφηση της μεταδιδόμενης πληροφορίας. Παρέχει επιπλέον , υποχρεωτική πιστοποίηση της ταυτότητας του εξυπηρέτη και προαιρετικά της ταυτότητας του πελάτη μέσω έγκυρων πιστοποιητικών που έχουν εκδοθεί από έμπιστες Αρχές Πιστοποίησης. Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για την αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων , εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs) , ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός.

Αντικαθιστώντας ένα 128-bit SSL πιστοποιητικό ασφαλείας server από μια αναγνωρισμένη αρχή πιστοποίησης στο sites της, μια Τράπεζα ασφαλίζει τις υπηρεσίες και δημιουργεί αίσθημα σιγουριάς στον πελάτη, κρυπτογραφώντας όλες τις on line συναλλαγές. Με το SSL πιστοποιητικό ασφαλείας server οι πελάτες γνωρίζουν ότι ο δικτυακός τόπος είναι ασφαλής.

Τα ασφαλή πιστοποιητικά ασφαλείας προσφέρουν σε μια Τράπεζα , υψηλή ασφάλεια και έχουν πολλαπλή χρησιμότητα , για τους ακόλουθους λόγους:

- Είναι πλήρως αναγνωρισμένα
- Έχουν 128-bit κρυπτογράφηση
- Διαρκούν από 1 έως 3 χρόνια
- Προσφέρουν 99% αναγνώριση browser
- Έχουν αυστηρή πιστοποίηση
- Υποστηρίζονται από την αρχή πιστοποίησης

Το ασφαλές SSL πιστοποιητικό server είναι ένα ψηφιακό πιστοποιητικό που πιστοποιεί την ταυτότητα του διαδικτυακού τόπου στους browsers που χρησιμοποιούνται για την πρόσβαση σε αυτόν και κρυπτογραφεί την πληροφορία για τον server μέσω SSL τεχνολογίας.

Αξίζει να σημειωθεί ότι οι περισσότερες Ελβετικές τράπεζες που προσφέρουν τις υπηρεσίες τους διαμέσου του internet έχουν αναπτύξει την ασφάλεια των εφαρμογών ηλεκτρονικής τραπεζικής με βάση το πρωτόκολλο SSL. Αυτή η απόφαση είναι στην ίδια κατεύθυνση με τη στρατηγική της Ευρωπαικής Επιτροπής για Τραπεζικά Πρότυπα (European Committee for Banking Standards-ECBS).

- Το SSL πιστοποιητικό περιέχει την ακόλουθη πληροφόρηση:
- Το όνομα του κατόχου του πιστοποιητικού
- Τον σειριακό αριθμό του πιστοποιητικού και την ημερομηνία λήξης του
- Αντίγραφο ου δημοσίου κλειδιού του κατόχου του
- Την ψηφιακή υπογραφή της αρχής πιστοποίησης που έκδωσε το πιστοποιητικό

Η διαδικασία SSL πιστοποίησης server λειτουργεί ως εξής:

1. Όταν ο χρήστης επισκέπτεται ένα SSL ασφαλές site , ο browser του χρήστη ζητά ένα ασφαλές session από το web server
2. Ο server απαντά, αποστέλλοντας στον browser του χρήστη το πιστοποιητικό του
3. Ο browser πιστοποιεί την εγκυρότητα του πιστοποιητικού, πιστοποιεί ότι χρησιμοποιείται από το site για το οποίο έχει εκδοθεί και ότι έχει εκδοθεί από αρχή πιστοποίησης που είναι αναγνωρισμένη
4. Αν το πιστοποιητικό είναι εγκεκριμένο , ο browser δημιουργεί ένα κλειδί μιας φοράς και το κρυπτογραφεί με το δημόσιο κλειδί του server\
5. Ο browser στέλνει το κρυπτογραφημένο κλειδί στον server ώστε να έχουν και οι δύο από ένα αντίγραφο
6. Ο server αποκρυπτογραφεί το κλειδί χρησιμοποιώντας το ιδιωτικό κλειδί του
7. Η διαδικασία SSL πιστοποίησης server έχει ολοκληρωθεί και έχει εγκατασταθεί μια ασφαλής σύνδεση
8. Ένα εικονίδιο κλειδαριάς εμφανίζεται στην γραμμή κατάστασης του browser, υποδηλώνοντας ότι το site είναι ασφαλές.

ΛΙΣΤΕΣ TAN (Transaction Authorization Numbers),Extra PINs

Μια κοινή μέθοδος αντιμετώπισης ζητημάτων ασφαλείας είναι η χρήση PINs για πιστοποίηση και αριθμών TAN για την έγκριση on line συναλλαγών. Οι αριθμοί TAN υπάρχουν τυπωμένοι σε ένα φύλλο χαρτιού , το οποίο δίδεται στον πελάτη του internet banking. Κάθε φορά που ο χρήστης πραγματοποιεί συναλλαγή , εισάγει ως κωδικό έγκρισης έναν τέτοιο αριθμό. Κάθε αριθμός που χρησιμοποιείται δεν μπορεί να χρησιμοποιηθεί εκ νέου. Για κάθε αριθμό TAN υπάρχει και το ζευγάρι του. Ο δεύτερος αυτός αριθμός επιστρέφεται στην οθόνη του χρήστη μετά από κάθε συναλλαγή , ώστε να επιβεβαιώνεται η ορθή χρήση του TAN . Ο χρήστης αντιπαραβάλει τον αριθμό αυτό με τον αντίστοιχο τυπωμένο στην λίστα του και εφόσον συμφωνούν είναι βέβαιος για την επιτυχή έκβαση της συναλλαγής του. Κάθε φορά που εξαντλούνται οι αριθμοί TAN ο πελάτης παραγγέλνει καινούργια λίστα.

Ωστόσο, υπάρχουν αρκετά σημεία που φέρουν κινδύνους ασφαλείας και δυσχρηστίας. Πρώτα από όλα οι αριθμοί είναι δύσκολο να απομνημονευτούν από τον χρήστη και για το λόγο αυτό, ο χρήστης πρέπει να έχει πάντα μαζί του τη λίστα. Δεύτερον, η εγκυρότητα τους έχει απεριόριστη διάρκεια, γεγονός που είναι αντίθετο με τα standards ασφαλείας. Τρίτον, ο χρήστης πρέπει να σημειώνει ποιους αριθμούς έχει χρησιμοποιήσει , διαφορετικά η χρήση των ίδιων αριθμών τον οδηγεί σε κλείδωμα της λίστας, ανάλογα του ορίου που θέτει η τράπεζα.

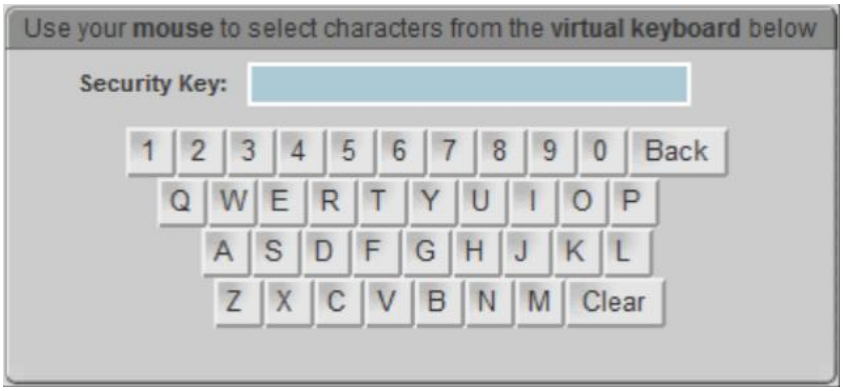
Εναλλακτική μέθοδος για την ασφάλεια των ηλεκτρονικών συναλλαγών, αποτελούν τα λεγόμενα extra pins. Ο χρήστης δηλώνει τον αριθμό κινητού τηλεφώνου στον οποίο επιθυμεί να λαμβάνει τα extra pins. Στην συνέχεια κάθε φορά που πραγματοποιεί on line συναλλαγή, αιτείται με sms νέο extra pin , το οποίο και εισάγει ως κωδικό έγκρισης συναλλαγής. Όπως και με τη λίστα TAN έτσι και με τα extra pins υπάρχουν κάποια προβλήματα δυσχρηστίας. Η λύση απαιτεί την ύπαρξη κινητού για τον χρήστη και την εξοικείωσή του με αυτό. Ο χρόνος ισχύος του extra pin είναι περιορισμένος και συνεπώς ένας χρήστης που εκτελεί συναλλαγές καθ'όλη την διάρκεια της ημέρας, πρέπει να αποστέλλει sms για τη λήψη νέων pins.

Για την αντιμετώπιση των παραπάνω δυσκολιών οι τράπεζες έχουν προχωρήσει ένα βήμα παραπάνω με τη δημιουργία συσκευής extraPIN generator. Η συσκευή αυτή είναι μια γεννήτρια τυχαίων κωδικών μιας χρήσης (one time passwords) και έχει πρόσθετη λειτουργικότητα μέσω των ενσωματωμένων USB connector (σύνδεση στη USB θύρα του υπολογιστή) και smartchip διαθέτει (δυνατότητα που θα εξυπηρετήσει μελλοντικά στην αποθήκευση των ψηφιακών πιστοποιητικών.). Η ευκολία που αποκτά κάποιος από τη χρήση τέτοιων συσκευών είναι σημαντική καθώς μπορεί ανα πάσα στιγμή , όπου και αν βρίσκεται να έχει πρόσβαση στους λογαριασμούς.

Ο κωδικός που παράγεται από το extrapin generator , εμφανίζεται στην οθόνη LCD της συσκευής. Ο κωδικός αυτός θα πρέπει να καταχωρείται μέσα σε 60 δευτερόλεπτα καθώς μετά παύει να ισχύς του. Η διάρκεια ζωής του κωδικού αποτυπώνεται στο αριστερό μέρος της οθόνης με τη μορφή μπάρας γραμμών. Κάθε γραμμή της μπάρας αντιστοιχεί σε 10 δευτερόλεπτα. Από τη στιγμή που θα καταχωρηθεί ο κωδικός μια φορά, παύει να ισχύει. Οι χρήστες έχουν τη δυνατότητα καταχώρησης του κωδικού είτε κατά την είσοδο τους στην υπηρεσία είτε σε δεύτερο στάδιο και ενώ έχουν ήδη συνδεθεί με αυτή. Σε περίπτωση που ο πελάτης διαπιστώσει ότι έχει χάσει την ειδική συσκευή ακόμα και στην περίπτωση που δε λειτουργεί, θα πρέπει να επικοινωνήσει με το κέντρο εξυπηρέτησης πελατών της τράπεζας.

ΕΙΚΟΝΙΚΑ ΠΛΗΚΤΡΟΛΟΓΙΑ

Τα εικονικά πληκτρολόγια αποτελούν μια καλή λύση στο πρόβλημα του key logging. Τα εικονικά πληκτρολόγια είναι στην ουσία μια επιπλέον προσθήκη στο λογισμικό της πλατφόρμας του e-banking.



Συνήθως έχουν τη μορφή pop up παραθύρου. Περιλαμβάνουν όλη τη λειτουργικότητα του φυσικού πληκτρολογίου. Ο χρήστης μπορεί κάνοντας χρήση μόνο του ποντικιού του να εισάγει τους κωδικούς πρόσβασης στο internet banking. Με τον τρόπο αυτό, αποφεύγεται ο κίνδυνος υποκλοπής των πλήκτρων που πατάει ο χρήστης. Λόγω της δυσχρηστίας τους όμως, συνήθως δίνονται ως προαιρετική επιλογή στον χρήστη.

4.4.ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΑΣΦΑΛΕΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Βασικές οδηγίες

1. Οι χρήστες θα πρέπει να προτιμούν τον προσωπικό υπολογιστή τους ή κάποιον με εγγυημένο επίπεδο ασφαλείας , ενώ οι οικονομικές συναλλαγές από internet café , δημόσιες βιβλιοθήκες και άλλους χώρους , όπου πολλοί χρήστες έχουν πρόσβαση , θα πρέπει να αποφεύγονται.
2. Όσον αφορά τους κωδικούς πρόσβασης που χρησιμοποιούνται για τις διαδικτυακές συναλλαγές :

- ✓ Θα πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα και ιδιαίτερα στην περίπτωση που υπάρχει υποψία ότι έχουν εκτεθεί.
- ✓ Χρήσιμο θα ήταν οι κωδικοί πρόσβασης να μην έχουν σχέση με τα προσωπικά στοιχεία των πελατών , όπως αριθμός τηλεφώνου, ημερομηνία γέννησης ή οτιδήποτε άλλο μπορεί να βρεθεί από άλλα έγγραφα.
- ✓ Οι προσωπικοί κωδικοί θα πρέπει να τοποθετούνται σε ασφαλή μέρη, πορτοφόλια, τσάντες, ατζέντες κλπ. Καλύτερα να αποφεύγονται.
- ✓ Ακόμη θα πρέπει να αποφεύγεται η χρησιμοποίηση του ίδιου κωδικού πρόσβασης σε περισσότερες από μία κάρτες.
- ✓ Είναι σαφές πως οι κωδικοί πρόσβασης δε πρέπει να παραχωρούνται σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Οι χρήστες θα πρέπει να είναι πολλοί επιφυλακτικοί , ιδιαίτερα σε τηλεφωνήματα και e-mail που έχουν ασυνήθιστο χαρακτήρα.

3.Οι χρήστες θα πρέπει να επικοινωνούν άμεσα με την τράπεζα τους αν πιστεύουν ότι κάποιος γνωρίζει τον κωδικό πρόσβασης τους για την υπηρεσία internet banking.

4.Χρήσιμο θα ήταν η λειτουργία << Αυτόματης Καταχώρησης>> του προγράμματος περιήγησης να απενεργοποιηθεί . Η αποθήκευση των κωδικών στον υπολογιστή τους καθιστά έκθετους.

5.Για τις αγορές μέσω διαδικτύου χρήσιμο θα ήταν οι χρήστες να εμπιστεύονται κατά κύριο λόγο γνωστές εταιρίες , οι οποίες παρέχουν εγγυήσεις ασφαλείας. Ακόμη , μια σωστή πρακτική θα ήταν η χρησιμοποίηση μιας κάρτας αποκλειστικά για αυτό το σκοπό. Έτσι, σε περίπτωση απάτης ο πελάτης θα έχει καλύτερο έλεγχο της κατάστασης.

6.Το επίπεδο ασφαλείας του υπολογιστή είναι ανάγκη να διατηρεί σε υψηλό επίπεδο:

- ✓ Η λήψη των ενημερωμένων εκδόσεων των προγραμμάτων που χρησιμοποιούνται και κυρίως των επιδιορθώσεων ασφαλείας πρέπει να γίνονται σε τακτά χρονικά διαστήματα. Πρόκειται για προγράμματα που εκδίδουν οι εταιρίες οι οποίες έχουν παράγει το λογισμικό και καλύπτουν τυχόν κενά ασφαλείας που έχουν διαπιστωθεί μετά την έκδοσή του.
- ✓ Η εγκατάσταση προγράμματος προστασίας από τους ιούς (antivirus) και ενός firewall και η τακτική λήψη των ενημερωμένων εκδόσεών τους θα πρέπει να παίζει πρωταρχικό ρόλο. Το firewall προφυλάσσει σε μεγάλο βαθμό από τις πιθανές εισβολές που πιθανόν θα δεχτεί ο χρήστης κατά την περιήγηση του στο διαδίκτυο.
- ✓ Για την αποφυγή πρόσβασης στον υπολογιστή του χρήστη μη εξουσιοδοτημένων χρηστών, εύλογη θα ήταν η χρήση κωδικού πρόσβασης.

7.Για τους χρήστες ηλεκτρονικού ταχυδρομείου (email):

- ✓ Ηλεκτρονικά μηνύματα , η προέλευση ή ο αποστολέας των οποίων δεν είναι βέβαιη δεν πρέπει να ανοίγονται. Ιδιαίτερη σημασία πρέπει να δίνεται στα μηνύματα άγνωστης προέλευσης που περιέχουν και συνημμένα αρχεία με κατάληξη .exe,pif ή vbs. Επειδή ορισμένοι ιοί στέλνουν αντίγραφά τους σε όλες τις επαφές του βιβλίου διευθύνσεων του υπολογιστή , το μήνυμα μπορεί να φαίνεται ότι έχει σταλεί από κάποιον γνωστό.
- ✓ Ηλεκτρονικά μηνύματα μέσω των οποίων ζητούνται προσωπικά στοιχεία του κατόχου δεν θα πρέπει να απαντώνται. Ακόμη , προσωπικά στοιχεία του πελάτη ή στοιχεία των συναλλαγών δεν θα πρέπει να αποστέλλονται μέσω μιας κοινής διεύθυνσης ηλεκτρονικού ταχυδρομείου (webmail) , αφού είναι εύκολη η υποκλοπή τους από τρίτα μη εξουσιοδοτημένα άτομα.

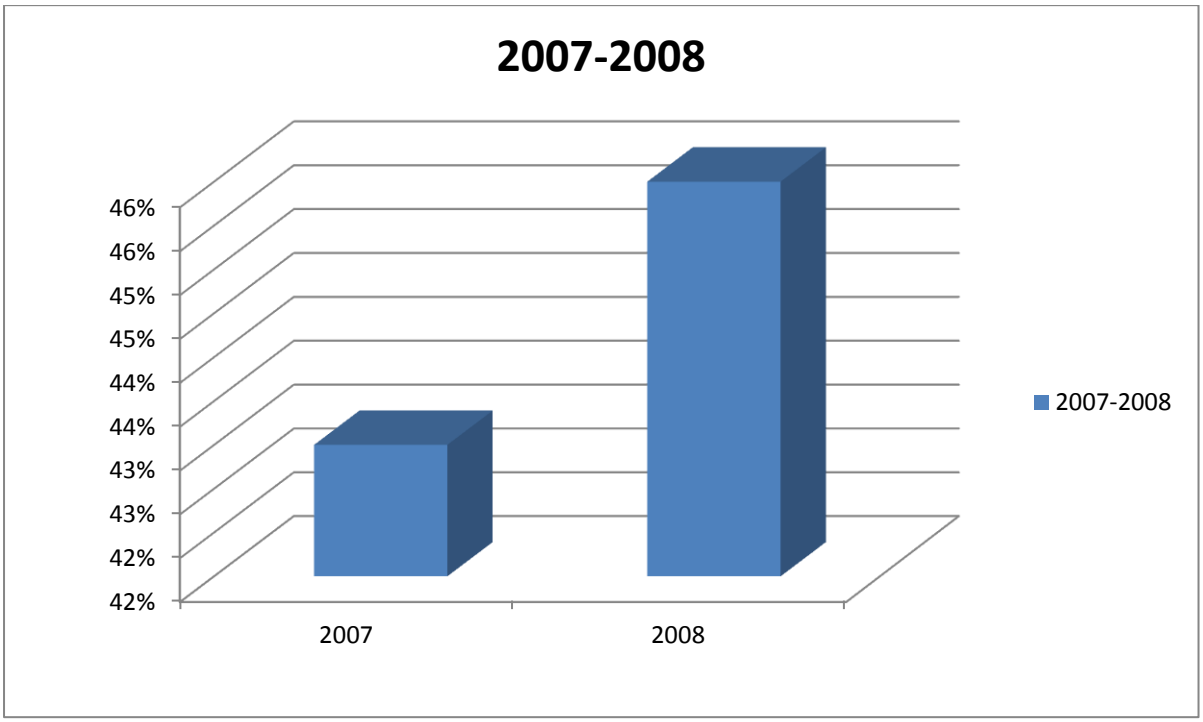
8.Κάθε χρήστης θα πρέπει να ενημερώνεται για τους λογαριασμούς του και να φροντίζει για την ασφάλεια των προσωπικών του στοιχείων και εγγράφων. Ειδικότερα θα πρέπει να ελέγχει τακτικά τους τραπεζικούς του λογαριασμούς και τους λογαριασμούς των πιστωτικών του καρτών για ασυνήθιστες συναλλαγές ή αναλήψεις . Και σε περίπτωση που διαπιστώσει οτιδήποτε , να επικοινωνήσει αμέσως με την τράπεζα.

ΚΕΦΑΛΑΙΟ 5

ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ

Για να δοθεί μια ολοκληρωμένη εικόνα για την κατάσταση που επικρατεί στη χώρα μας σχετικά με το internet e-banking δίνονται τα παρακάτω στοιχεία. Τα στοιχεία προέρχονται από έρευνα της e-metrics για τη χρήση διαδικτύου για το 2008.

Α) Διαχρονική εξέλιξη για το σύνολο των χρηστών

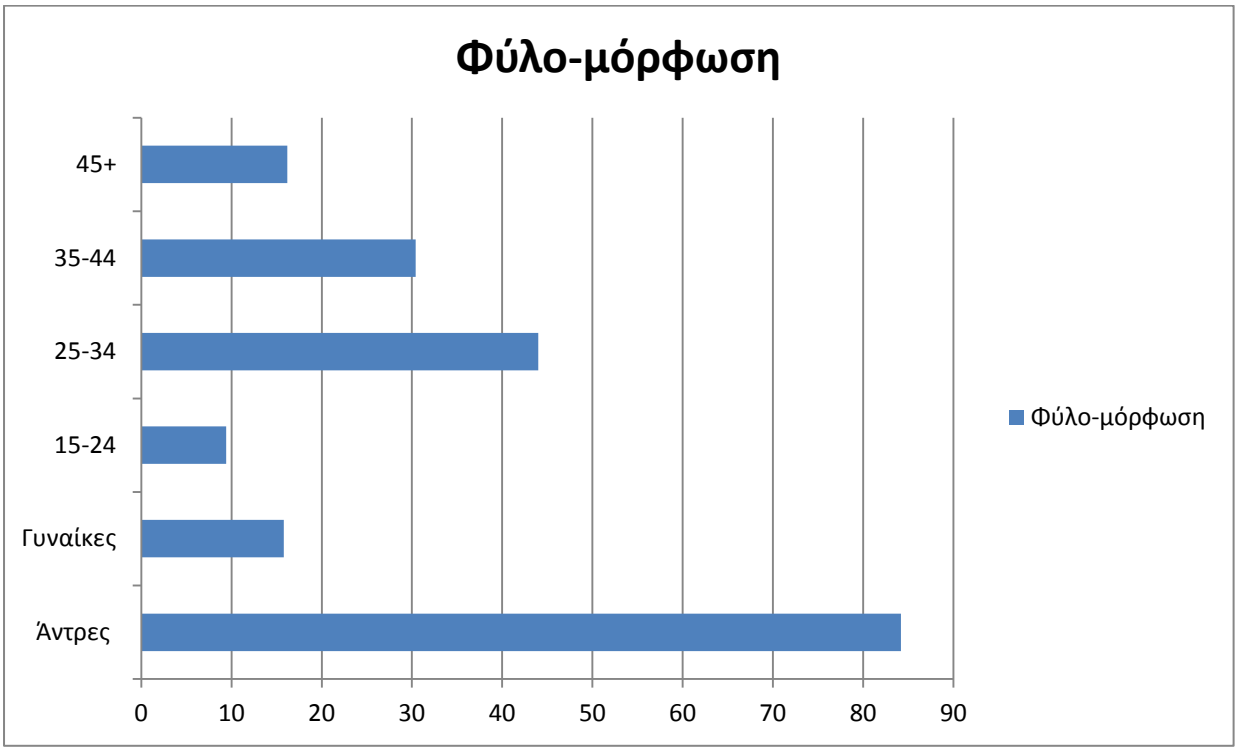


Βάση : Όσοι συμμετείχαν στην metrics

Πηγή: Έρευνα e metrics , AGB Nielsen Media Research 2008

Το 2008 εμφανίζεται μία μικρή αύξηση του ποσοστού των χρηστών που χρησιμοποιούν το internet για διεκπεραίωση τραπεζικών συναλλαγών. Από το 43% το 2007, το ποσοστό ανεβαίνει το 2008 στα 46%.

Β) Προφίλ χρηστών που χρησιμοποιούν τις υπηρεσίες e-banking

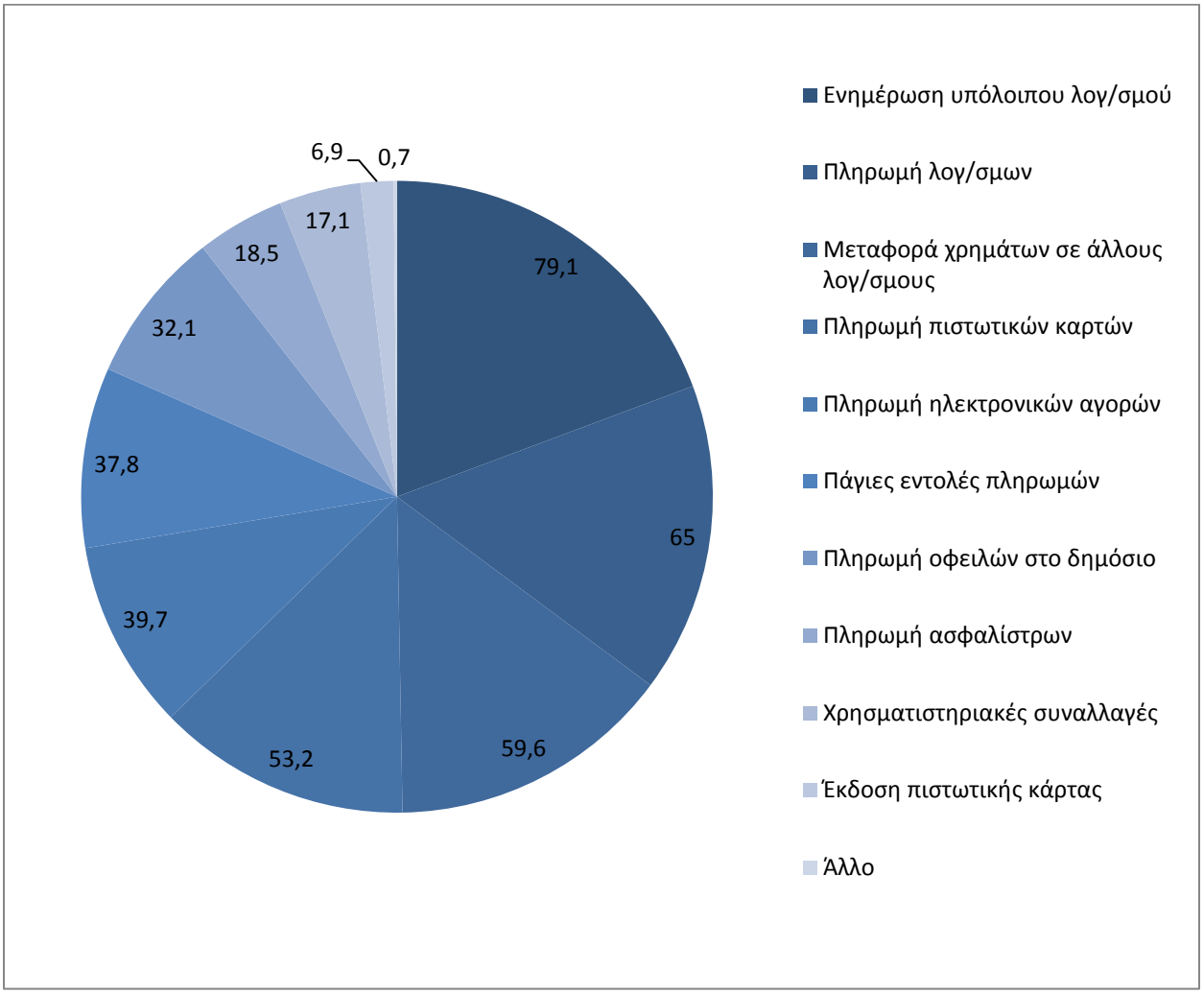


Βάση : Όσοι συμμετείχαν στην metrics

Πηγή: Έρευνα e metrics , AGB Nielsen Media Research 2008

Το 84,2 του συνόλου των χρηστών που συμμετείχαν στην έρευνα και χρησιμοποιούν το internet για διεκπεραίωση τραπεζικών συναλλαγών είναι άντρες. Το 44% των χρηστών που χρησιμοποιούν το internet e-banking ανήκουν στην ηλιακή ομάδα 25-34 , το 30,4 % είναι ηλικίας 35-44 , το 16,2% είναι χρήστες ηλικίας άνω των 45 και το μικρότερο ποσοστό 9,4% σε χρήστες ηλικίας από 15 έως 24 ετών.

Γ) Τραπεζικές υπηρεσίες που χρησιμοποιούν

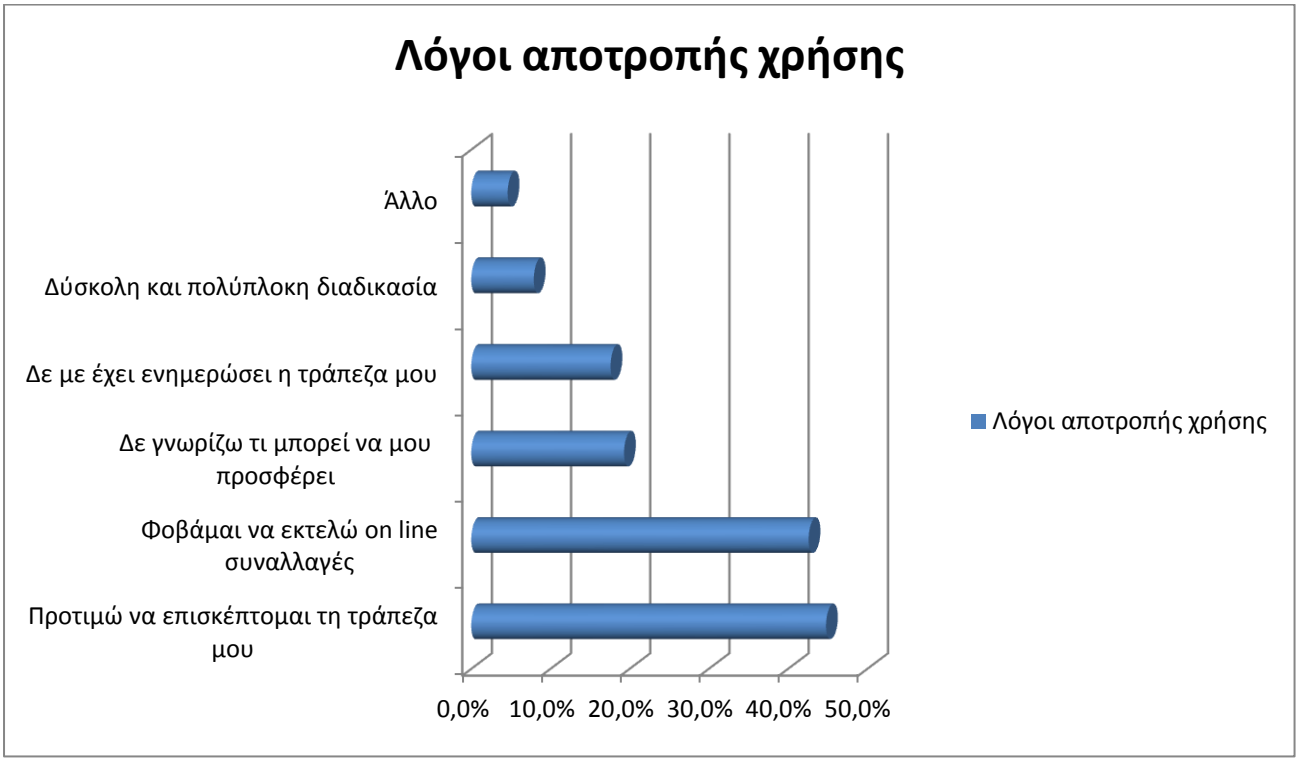


Βάση : Όσοι συμμετείχαν στην metrics

Πηγή: Έρευνα e metrics , AGB Nielsen Media Research 2008

Το 79,1% των χρηστών e-banking , χρησιμοποιούν την υπηρεσία αυτή για να ενημερώνονται για το υπόλοιπο του λογαριασμού τους , ενώ δεύτερη πιο συχνή ηλεκτρονική τραπεζική υπηρεσία με 65% είναι η πληρωμή διαφόρων λογαριασμών (ΔΕΗ, ΟΤΕ κ,α,) , το 59,6% χρησιμοποιεί τις υπηρεσίες του e-banking για μεταφορά χρημάτων σε άλλους λογαριασμούς και το 53,2% για να πληρώνουν την πιστωτική τους κάρτα. Το 39,7% πληρώνει τις ηλεκτρονικές αγορές ενώ η πληρωμή λογαριασμών ενοικίου είναι μια ηλεκτρονική τραπεζική υπηρεσία που χρησιμοποιείται από το 37,8%. Η διεκπεραίωση χρηματιστηριακών συναλλαγών μέσω web banking αφορά το 17,1% του συνόλου των χρηστών που χρησιμοποιούν τις υπηρεσίες e-banking ενώ σε μικρά ποσοστά είναι η χρήση των υπηρεσιών αυτών για πληρωμή ασφαλίστρων και έκδοσης πιστωτικής κάρτας.

Δ) Λόγοι αποτροπής χρήσης του e-banking



Βάση : Όσοι συμμετείχαν στην metrics

Πηγή: Έρευνα e metrics , AGB Nielsen Media Research 2008

Οι λόγοι που αποτρέπου τους χρήστες που συμμετείχαν στην έρευνα , να χρησιμοποιούν τις υπηρεσίες e-banking , είναι το ότι το 44,8% προτιμάει να επισκέπτεται το υποκατάστημα της τράπεζας του προκειμένου να πραγματοποιήσει τις τραπεζικές του συναλλαγές ενώ παράλληλα το 42,6 % φοβάται να εκτελεί τραπεζικές συναλλαγές μέσω internet. Το 19,3% αναφέρει ότι δε γνωρίζει τι μπορεί να του προσφέρει η υπηρεσία αυτή, το 17,6% δεν έχει ικανή ενημέρωση από την τράπεζα ενώ τέλος, το 7,9% θεωρεί ότι το e-banking είναι μία δύσκολη και πολύπλοκη διαδικασία.

ΜΕΡΟΣ 2

ΤΟ E-BANKING ΤΟΥ ΤΑΧΥΔΡΟΜΙΚΟΥ ΤΑΜΙΕΥΤΗΡΙΟΥ 2007-2012

ΕΙΣΑΓΩΓΗ

Το Ταχυδρομικό Ταμιευτήριο ιδρύθηκε το 1900 αποτελώντας την πρώτη ολοκληρωμένη μορφή Ταμιευτηρίου στη χώρα μας. Το 2006 και μετά την παραχώρηση της σχετικής άδειας το ΤΤ ξεκίνησε να λειτουργεί ως πιστωτικό ίδρυμα ενώ ταυτόχρονα εισήχθη στο Χρηματιστήριο Αθηνών. Με την ίδρυση θυγατρικών έχει επεκτείνει τις δραστηριότητες του σε τομείς όπως η διαχείριση αμοιβαίων κεφαλαίων και το Leasing αποτελώντας πλέον έναν ολοκληρωμένο όμιλο. Σήμερα το συνολικό ενεργητικό της τράπεζας ξεπερνάει τα 16 δις ευρώ ενώ διαθέτει ένα δίκτυο 146 καταστημάτων σε όλη την ελληνική επικράτεια , εκ των οποίων 57 καταστήματα στην Αττική, 18 καταστήματα στην Θεσσαλονίκη, 15 καταστήματα στην Περιφερειακή Διεύθυνση Κρήτης και λοιπών νησιών, 15 καταστήματα στην Περιφερειακή Διεύθυνση Πελοποννήσου και 40 καταστήματα στη λοιπή Ελλάδα. Η έδρα της τράπεζας είναι ο δήμος Αθηνών. Το δίκτυο καταστημάτων της τράπεζας είναι ευρέως εξαπλωμένο και καλύπτει σχεδόν όλες τις πρωτεύουσες των νομών της Ελλάδας. Σχεδόν όλα τα καταστήματα της τράπεζας παρέχουν στους πελάτες πρόσβαση σε όλο το φάσμα των χρηματοοικονομικών προϊόντων και υπηρεσιών της. Στο δίκτυο αυτό προστίθενται τα καταστήματα ΕΛΤΑ .

ΔΕΙΚΤΗΣ ΚΕΦΑΛΑΙΑΚΗΣ ΕΠΑΡΚΕΙΑΣ

Η έκθεση της Citigroup σχετικά με τα «κεφάλαια» των ευρωπαϊκών τραπεζών , κατατάσσει το ταχυδρομικό ταμιευτήριο στην τρίτη θέση πανευρωπαϊκά και στην πρώτη πανελλαδικά από πλευράς κεφαλαιακής επάρκειας (δείκτης 1-14%) , σύμφωνα με τις εκτιμήσεις για το 2009. Η κατάταξη αυτή του ταχυδρομικού ταμιευτηρίου, παίζει σημαντικό ρόλο και αποκτά υψηλή σημασία , αφού μεγάλες τράπεζες έχουν δείκτη κεφαλαιακής επάρκειας κάτω από το μέσο όρο (σύμφωνα πάντα με την ίδια έκθεση). **(Περιοδικό «Ταχυδρομικό Ταμιευτήριο 2009)**

Το πρώτο τρίμηνο 2011 το ταχυδρομικό ταμιευτήριο παρουσίασε κέρδη μετά από φόρους ύψους 22 εκατ. ευρώ . Παράλληλα, η οργανική κερδοφορία του Τ.Τ. αυξήθηκε κατά 94%, στα 49,4 εκατ. ευρώ, από 25,5 εκατ. ευρώ την αντίστοιχη περίοδο του 2010. Τα καθαρά έσοδα από τόκους, αυξήθηκαν κατά 30%, στα 102,2 εκατ. ευρώ από 78,8 εκατ. ευρώ την αντίστοιχη περίοδο του 2010. Τα λειτουργικά έξοδα συγκρατήθηκαν στα ίδια επίπεδα με αυτά της προηγούμενης συγκριτικής περιόδου του 2010, στα 52 εκατ. ευρώ. Ο δείκτης κεφαλαιακής επάρκειας ανήλθε σε 18,99%, ενώ χωρίς το συνυπολογισμό των προνομιούχων μετοχών, ο δείκτης θα ανερχόταν σε 15,54%. Ο δείκτης καθυστερούμενων δανείων , σε σχέση με το ευρύτερο τραπεζικό σύστημα, διαμορφώθηκε σε 4,16%. **(πανελλήνιος σύλλογος διαμετακομιστών ΕΛΤΑ, 30 Μαΐου 2011)**

ΕΙΣΑΓΩΓΗ ΤΟΥ E-BANKING

Συμφωνία συνεργασίας στον τομέα της ηλεκτρονικής τραπεζικής (e-banking) και της καταναλωτικής πίστης, μέσω και έκδοσης χρεωστικών καρτών, υπέγραψαν στις 29/06/2009 στη Θεσσαλονίκη, ο Πρόεδρος του ΤΤ Hellenic Postbank κ. 'Άγγελος Φιλιππίδης και ο Πρόεδρος του Συμβουλίου Απόδημου Ελληνισμού (ΣΑΕ) και της ΔΕΣΜΟΣ ΑΜΚΕ κ. Στέφανος Ταμβάκης, παρουσία των Μελών του Προεδρείου του ΣΑΕ.

Ο πρόεδρος του Ταχυδρομικού ταμιευτηρίου , κ. Άγγελος Φιλιππίδης τόνισε ότι είναι μία ιστορική μέρα για το Ταχυδρομικό Ταμιευτήριο, που έμπρακτα αγκαλιάζει τους απανταχού Έλληνες. Με την πλατφόρμα ηλεκτρονικής τραπεζικής (e-banking) ο κάθε ομογενής θα μπορεί να ανοίξει λογαριασμό, μέσω του οποίου θα είναι σε θέση να κάνει όλες τις συναλλαγές», , προσθέτοντας ότι από τα χρήματα που εξασφαλίζονται από τις συναλλαγές αυτές, θα επιδοτούνται και δράσεις του απόδημου Ελληνισμού. Επίσης, θεωρώ ότι η υπογραφή της συμφωνίας με το Ταχυδρομικό Ταμιευτήριο αποτελεί ένα σταθμό, καθώς μέσω αυτής το ΣΑΕ πλέον αποκτά μερική οικονομική αυτοδυναμία, που συζητείται από χρόνια και τώρα σταδιακά υλοποιείται. **(εφημερίδα εξπρές 29/06/2009)**

Το e-banking site του Ταχυδρομικού Ταμιευτηρίου είναι σε XML με βάση και αναπτύχθηκε σύμφωνα με τα παγκόσμια πρότυπα της οικονομικής ανταλλαγής πληροφοριών. Το E-postbank. δίνει τη δυνατότητα να εκτελούν όλα τα είδη πληρωμών, που υποστηρίζονται από το βουλγαρικό τραπεζικό σύστημα, συμπεριλαμβανομένης της μεταφοράς συναλλάγματος. Το εξαιρετικά υψηλό επίπεδο ασφάλειας είναι εγγυημένη από τα ψηφιακά πιστοποιητικά που προσδιορίζουν τον πελάτη από έναν προσωπικό αριθμό πελάτη. Υπάρχει μια ευκαιρία να κάνει μια on line αίτηση για το άνοιγμα τραπεζικού λογαριασμού. Αφού ο πελάτης λαμβάνει τα απαραίτητα έγγραφα σε χαρτί και ανοίγει λογαριασμό και με την Τράπεζα, λαμβάνει διπλό προστατευόμενο ψηφιακό έγγραφα με ένα μοναδικό κωδικό, που διατίθεται μόνο στον πελάτη.

Το e-banking θα δίνει τη δυνατότητα σε κάθε ομογενή να κάνει ολοκληρωμένη χρηματοοικονομική διαχείριση των οικονομικών υποχρεώσεων του με την Ελλάδα (π.χ. εμβάσματα σε συγγενείς και άλλα φυσικά πρόσωπα, πληρωμές προς κρατικούς φορείς (φορολογία, κτηματολόγιο, κτλ)., τιμολογίων ΔΕΚΟ (ΔΕΗ, ΟΤΕ, κτλ). προς άλλους δημόσιους οργανισμούς (παράβολα, κτλ), αλλά και μεταφορές χρημάτων σε άλλες ελληνικές τράπεζες, όπως και πληρωμές υποχρεώσεων σε επιχειρήσεις του ιδιωτικού τομέα - ασφάλειες, ξενοδοχεία, κινητή τηλεφωνία, κτλ). **(Εφημερίδα Ελληνική γνώμη, Ιούλιος 2009)**

Σταδιακά, το πρόγραμμα κατά την εξέλιξή του, θα παρέχει πολλές επιπλέον δυνατότητες, όπως για παράδειγμα συνεργασία με άλλους ομογενείς στο εξωτερικό, παροχή πληροφοριών για την αγορά ακινήτων.

Όμως , το ταχυδρομικό Ταμιευτήριο δε σταματά εδώ. Συνεχίζει να βελτιώνει την ηλεκτρονική τραπεζική. Στις 24/01/2012 στο site www.banknews.gr δημοσιεύτηκε ότι δυναμική είσοδο στην ηλεκτρονική τραπεζική αποκτά το Ταχυδρομικό Ταμιευτήριο, εγκαινιάζοντας μια σειρά από καινοτομίες στον τομέα του e-banking.

Όπως αναφέρεται σε σχετική ανακοίνωση, τη στιγμή που όλο και περισσότεροι καταναλωτές -ήδη υπερβαίνουν τις 10.000- δίνουν ψήφο εμπιστοσύνης στο e-bank του το ΤΤ, η Τράπεζα καινοτομεί, δίνοντας στους πελάτες τη δυνατότητα να σερφάρουν στους λογαριασμούς τους ακόμη πιο εύκολα, γρήγορα, οικονομικά, με μεγαλύτερη ασφάλεια και αξιοπιστία, όπου και αν βρίσκονται, όποια στιγμή επιθυμούν.

«Πάντα σε επαφή» με τις ανάγκες του καταναλωτή, η Τράπεζα εισάγει μια καινοτόμα υπηρεσία, που εγγυάται υψηλό επίπεδο ασφάλειας, με την αποστολή κωδικού μιας χρήσης στο κινητό (SMS TAN) για την εκτέλεση εγχρήματων εντολών.

Παράλληλα, το e-banking του ΤΤ συνεχίζει να παρέχει όλη την γκάμα των προηγμένων υπηρεσιών ηλεκτρονικής τραπεζικής, όπως η ενημέρωση, με δωρεάν μήνυμα στα κινητό (sms alerts) για την ολοκλήρωση εγχρήματων συναλλαγών.

Το e-bank παρέχει διαχείριση, ενημέρωση υπολοίπων και κινήσεων λογαριασμών, δανείων, επιταγών, μεταφορά χρημάτων στην Ελλάδα και το εξωτερικό (σε ευρώ και σε συνάλλαγμα), πληρωμές λογαριασμών και συνδρομών (ΔΕΗ, ΟΤΕ, ΕΥΔΑΠ, κινητής τηλεφωνίας κ.ά.), πληρωμές ασφαλιστικών εισφορών, ΦΠΑ, Φόρου Εισοδήματος, πληρωμές πιστωτικών καρτών.

Μέσω του e-banking μπορεί ο χρήστης να παρακολουθεί ή να λαμβάνει δεδομένα σε πραγματικό χρόνο σχετικά με:

- Συναλλαγματικές ισοτιμίες
- Υπόλοιπο όλων των λογαριασμών σας στην Τράπεζα
- Diffrent είδη των εκθέσεων
- Λάθη
- Μεταφορές έλαβε
- SWIFT αντίγραφα σε πραγματικό χρόνο
- Ιστορία των συναλλαγών
- Πιστωτικοί λογαριασμοί, τα προγράμματα εξόφλησης
- Οι άμεσες χρεώσεις
- Εξαγωγή σε μορφή XLS
- Εξαγωγή σε μορφή PDF
- Μορφή εύκολης εκτύπωσης

Επίσης , μπορεί να κάνει ή να παραγγείλει :

- Άμεσες πληρωμές
- Πληρωμές του προϋπολογισμού
- Συλλογές
- Μαζικές πληρωμές
- Πληρωμές νομίσματος
- Παρακολούθηση και ακύρωση της συναλλαγής
- Μοτίβα
- Αίτηση για την απόσυρση του ταμείου

ΑΣΦΑΛΕΙΑ

Όσον αφορά την ασφάλεια που έχει επιλέξει το ταχυδρομικό ταμιευτήριο, στην είσοδο ζητούνται τα στοιχεία εισαγωγής πελάτη στο on line banking.Για επιπλέον ασφάλεια , από όσα όλα έχουν προαναφερθεί η τράπεζα χρησιμοποιεί το VIP-token το οποίο γνωρίζουμε ότι είναι πρόσθετος κωδικός ασφαλείας συναλλαγών.

VIP-token:
Ηλεκτρονική συσκευή πρόσθετου κωδικού ασφαλείας συναλλαγών

Αξιοποιώντας την τεχνολογία του σήμερα και λαμβάνοντας υπόψη τις σύγχρονες απαιτήσεις για ασφαλείς και παράλληλα απλές συναλλαγές μέσω διαδικτύου (e Banking) υιοθετείτε η χρήση της συσκευής VIP-token.

Περιγραφή & χρήση της συσκευής

Η συσκευή VIP-token, είναι φορητή, μικρού μεγέθους και η διάρκεια της μπαταρίας της μπορεί να φτάσει τα 3 χρόνια μετά τα οποία, η συσκευή αντικαθίσταται. Η συσκευή παράγει με κρυπτογραφημένο αλγόριθμο ένα εξαψήφιο αριθμό μίας χρήσεως ο οποίος έχει διάρκεια ζωής περίπου 30 δευτερόλεπτα και ο οποίος σε συνδυασμό με τον κωδικό πελάτη (User ID), πιστοποιεί ότι η συναλλαγή προέρχεται από το συγκεκριμένο χρήστη.

Η συσκευή αυτή χρησιμοποιείται:
Σε συνδυασμό με τον κωδικό και τη συνθηματική λέξη για τη πραγματοποίηση εγχρήματων συναλλαγών στην υπηρεσία e Banking όπως:

- Μεταφορές ποσών μεταξύ λογαριασμών ιδίου ή
- σε λογαριασμούς τρίτων της πρώην Τ Bank,
- Εμβάσματα σε άλλη τράπεζα εσωτερικού,
- Πληρωμές λογαριασμών (π.χ. ΑΕΗ, ΟΤΕ κ.λπ.)

ΠΡΟΣΟΧΗ

Η σύνδεση στην υπηρεσία e Banking χωρίς τη χρήση της συσκευής VIP-token ,είναι εφικτή μόνο για πληροφόρηση (π.χ. ενημέρωση για υπόλοιπα ή κινήσεις λογαριασμών ή πιστωτικών καρτών κλπ).
Οι πελάτες που έχουν ήδη παραλάβει (με αίτησή τους) συσκευή VIP-token, μπορούν να ζητούν την άμεση ενεργοποίησή της.

Λειτουργία

Η συσκευή VIP-token διαθέτει ένα μόνο πλήκτρο, το πάτημα του οποίου παράγει με βάση κρυπτογραφημένο αλγόριθμο, ένα εξαψήφιο αριθμό, τον οποίο εμφανίζει στην οθόνη της για 30 δευτερόλεπτα. Ο αριθμός αυτός είναι μοναδικός και εισάγεται από τον χρήστη στο σύστημα όταν και όπου αυτό απαιτείται για την ολοκλήρωση μίας συγκεκριμένης συναλλαγής. Για να χρησιμοποιηθεί εκ νέου η συσκευή (σε επόμενη συναλλαγή), θα πρέπει να παρέλθουν τα 30 δευτερόλεπτα για να παραχθεί νέος κωδικός.

Πλεονεκτήματα

• Ευκολία στη χρήση
• Εύκολη μεταφορά, λόγω μικρού όγκου.
• Εξαιρετικά υψηλό επίπεδο ασφάλειας.
• Δεν μπορεί να χρησιμοποιηθεί από τρίτους, διότι συνδέεται υποχρεωτικά με
τον κωδικό του πελάτη.

ΕΝΗΜΕΡΩΣΕΙΣ ΑΠΟ ΤΗΝ ΤΡΑΠΕΖΑ

Επίσης, στην είσοδο η τράπεζα επειδή θέλει να προστατεύσει τους χρήστες της δίνει ορισμένες πληροφορίες σχετικά με την αποφυγή παγίδων. Έχει μία επιλογή ως ασφάλεια. Αν τη πατήσει ο χρήστης θα βρει το παρακάτω προστατευτικό μήνυμα:

Προβείτε σε έλεγχο ασφαλείας του φυλλομετρητή σας

Οδηγίες για την ασφάλεια σας

«Το ταχυδρομικό ταμιευτήριο θα ήθελε να επιστήσει την προσοχή σας σε πρόσφατα περιστατικά υποκλοπής προσωπικών δεδομένων από πελάτες γνωστών οικονομικών οργανισμών στο διεθνή χώρο , με γνώμονα την ενημέρωσή σας και πρόληψη από τυχόν παρόμοια περιστατικά.

Συγκεκριμένα, άγνωστοι στέλνουν email σε τυχαίες λίστες κατόχων email προσποιούμενοι κατόχους τραπεζών (email scams) . Με το email αυτό , ζητούν από τους πελάτες είτε την αποκάλυψη εμπιστευτικών στοιχείων όπως κωδικούς πρόσβασης και pin είτε προτρέπουν τη μετάβαση σε ιστοσελίδα (hyperlink) που μοιάζει με την αυθεντική ιστοσελίδα της τράπεζας , ώστε να εισάγουν τους προσωπικούς κωδικούς ή άλλα εμπιστευτικά τους στοιχεία σε ένα ψεύτικο σύστημα για να μπορούν να τα υποκλέψουν.»

Ση συνέχεια παροτρύνουν τους χρήστες να ενημερωθούν σχετικά με το θέμα στο Anti-Phishing Working Group.

Επίσης τονίζουν ότι πρέπει να υπάρχει ιδιαίτερη προσοχή στην παραλαβή ηλεκτρονικών μηνυμάτων ή εμφάνιση pop-up παραθύρων , banners κτλ. Όπου ζητούνται:

- ✓ Η αποκάλυψη προσωπικών κωδικών
- ✓ Η μετάβαση σε ιστοσελίδα που μοιάζει με την ιστοσελίδα της τράπεζας

Τέλος, δίνει κάποιες διευκρινήσεις:

« Το ταχυδρομικό ταμιευτήριο δεν σας ζητά ποτέ την αποκάλυψη του προσωπικού σας κωδικού πρόσβασης με οποιοδήποτε τρόπο , σε ότι αφορά στην πρόσβασή σας στην υπηρεσία του e-banking.

Για μεγαλύτερη ασφάλεια , συνδεθείτε στην υπηρεσία T-BANKING πληκτρολογώντας πάντα εκ νέου τη διεύθυνση https://ebanking.tbank.com.gr

Επιπλέον , όταν συνδέεστε στην υπηρεσία t-e banking ελέγχετε πάντα ότι όλες οι σελίδες της ξεκινούν με https://ebanking.tbank.com.gr και ότι βρίσκεται σε ασφαλές περιβάλλον. Αυτό διαπιστώνεται εύκολα από την εμφάνιση του λουκέτου στη Γραμμή κατάστασης (συνήθως στη κάτω δεξιά πλευρά της οθόνης σας) καθώς και από τη διεύθυνση https://ebanking.tbank.com.gr που περιέχει το “s” στο πρωτόκολλο http.

Επίσης, ελέγχετε πάντα το ψηφιακό πιστοποιητικό , που πιστοποιεί την αυθεντικότητα της σελίδας του ταχυδρομικού ταμιευτηρίου και της υπηρεσίας T E-BANKING , κάνοντας διπλό κλικ στο λουκέτο στη γραμμή κατάστασης. Το ' ebanking.tbank.com.gr ' επιβεβαιώνει ότι είστε συνδεδεμένος στον επίσημο server του Ταχυδρομικού Ταμιευτηρίου.

ΜΕΡΟΣ 3

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σήμερα, όλες οι τράπεζες στη χώρα μας, προσφέρουν στους πελάτες τους τη δυνατότητα να μπορούν να πραγματοποιούν τις συναλλαγές τους μέσω της ηλεκτρονικής τραπεζικής , χωρίς να χρειάζεται η φυσική τους παρουσία στο κατάστημα της τράπεζας. Οι ελληνικές τράπεζες, παρά το ρίσκο που αντιμετωπίζουν υιοθετώντας μία υπηρεσία που δεν είναι ακόμα ευρέως διαδεδομένη, δεν έχουν να ζηλέψουν σε τίποτα τις τράπεζες του εξωτερικού, σε ότι έχει να κάνει με το e-banking.

Η υιοθέτηση της συγκεκριμένης υπηρεσίας σε μία χώρα όπως η Ελλάδα, η οποία δεν είναι ακόμα πλήρως εξοικειωμένη με την ταχύτατη ανάπτυξη της τεχνολογίας μπορεί να χαρακτηριστεί ως ριψοκίνδυνη. Οι περισσότερες ελληνικές τράπεζες που προσφέρουν υπηρεσίες e-banking , χρησιμοποιούν internet banking , ενώ με την πάροδο των ετών όλο και περισσότερες είναι οι τράπεζες που δίνουν τη δυνατότητα στους πελάτες τους να διαχειρίζονται τους λογαριασμούς του μέσω σταθερού ή κινητού τηλεφώνου.

Οι υπηρεσίες που προσφέρουν καλύπτουν σχεδόν όλες τις ανάγκες των καταναλωτών χωρίς ο πελάτης να χρειάζεται να σπαταλά το χρόνο του περιμένοντας στο γκισέ κάποιας τράπεζας. Τα οφέλη τα οποία έχουν αποκομίσει οι τράπεζες, είναι πολλά και αρκετά προσοδοφόρα, αφού με τη χρήση της ηλεκτρονικής τραπεζικής , καταφέρνουν να μειώσουν τα λειτουργικά έξοδα της τράπεζας, αυξάνοντας ταυτόχρονα τον αριθμό των πελατών της. Παρά τα οφέλη τα οποία έχουν οι τράπεζες από την παροχή της συγκεκριμένης υπηρεσίας, πολλά συνεχίζουν να είναι και τα εμπόδια τα οποία αντιμετωπίζουν σχετικά με την υιοθέτηση της , όπως το υψηλό κόστος και ο μικρός αριθμός των χρηστών στην χώρα μας.

Το κοινό στόχος (target group) στο οποίο απευθύνονται οι περισσότερες τράπεζες στη χώρα μας αφορά άτομα νεαρής ηλικίας με υψηλό μορφωτικό και οικονομικό επίπεδο, καθώς επίσης και ελεύθερους επαγγελματίες και επιχειρήσεις όλων των μεγεθών. Το επίπεδο ασφαλείας που προσφέρουν οι ελληνικές τράπεζες στους χρήστες της ηλεκτρονικής τραπεζικής, μπορούμε να πούμε ότι βρίσκεται σε ικανοποιητικό επίπεδο όμως τα περιθώρια βελτίωσης του είναι ακόμα μεγάλα αν κρίνουμε και από την συνεχή εμφάνιση νέων κινδύνων-απειλών στις ηλεκτρονικές συναλλαγές.

Πιο συγκεκριμένα, στο σύνολο τους οι ελληνικές τράπεζες γνωρίζουν όλους τους κινδύνους και τις απειλές που μπορούν να προκύψουν κατά τη χρήση καθώς επίσης, είναι ενημερωμένες και παρέχουν τους περισσότερους με τους οποίους μπορούν να αντιμετωπιστούν οι κίνδυνοι αυτοί.

Σαν τελικό συμπέρασμα θα μπορούσαμε να πούμε ότι για να είναι επιτυχημένες οι τράπεζες στο μέλλον, θα πρέπει να έχουν διαμορφώσει στρατηγικές προσαρμοσμένες στις εξελίξεις της αγοράς και του σύγχρονου οικονομικού περιβάλλοντος καθώς και οργανωτικές δομές, που θα αποσκοπούν στην καλύτερη δυνατή διαχείριση πελατών και όχι προϊόντων.

Όσον αφορά τους χρήστες της ηλεκτρονικής τραπεζικής , μπορούμε να πούμε ότι στην πλειοψηφία τους είναι νεαρά άτομα, ηλικίας 25-35 ετών, με υψηλό μορφωτικό επίπεδο και υψηλό εισόδημα. Άτομα δηλαδή εξοικειωμένα με την τεχνολογική ανάπτυξη, τα οποία δε διστάζουν να ρισκάρουν χρησιμοποιώντας μία νέα υπηρεσία , η οποία όμως είναι ικανή να απλουστεύσει πολλά προβλήματα της καθημερινής τους ζωής. Οι Έλληνες καταναλωτές έχουν δείξει ότι δύσκολα εμπιστεύονται κάτι άγνωστο σε αυτούς, πόσο μάλλον όταν αυτό έχει να κάνει με την διαχείριση των χρημάτων τους. Έτσι, το ποσοστό χρήσης e-banking στη χώρα μας βρίσκεται ακόμα σε χαμηλά επίπεδα.

Τα οφέλη που αποκομίζουν οι χρήστες της ηλεκτρονικής τραπεζικής από τη χρήση της, είναι πολλά. Τα σημαντικότερα από αυτά είναι ότι δεν χρειάζεται πια να περιμένουν με τις ώρες στις ουρές των τραπεζών για να πραγματοποιήσουν τις συναλλαγές τους, αφού μπορούν να το κάνουν καθισμένοι στον καναπέ του σπιτιού τους ή στην καρέκλα του γραφείου τους. Επίσης, γνωρίζουν ότι η τράπεζα τους δεν κλείνει ποτέ αφού το e-banking τους δίνει τη δυνατότητα να πραγματοποιούν όποια συναλλαγή επιθυμούν οποιαδήποτε ημέρα της εβδομάδας καθώς και να ενημερώνονται για τα υπόλοιπα τους όποτε αυτοί επιθυμούν.

Το επίπεδο γνώσης των χρηστών της ηλεκτρονικής τραπεζικής σε θέματα σχετικά με την ασφάλεια των ηλεκτρονικών τους συναλλαγών , τους κινδύνους και τις απειλές που πιθανόν να αντιμετωπίσουν καθώς και τους τρόπους με τους οποίους μπορούν να προστατευθούν , δεν είναι ακόμα αρκετά υψηλό στη χώρα μας. Γενικά , θα μπορούσαμε να πούμε , ότι στο μεγαλύτερο ποσοστό τους , οι χρήστες έχουν θετική άποψη για το internet e-banking , θεωρούν ότι είναι εύκολο στη χρήση του και γρήγορο στην εκτέλεση συναλλαγών. Θεωρούν ότι υπάρχει οργάνωση από τις τράπεζες σε ότι αφορά τη διεξαγωγή ηλεκτρονικών συναλλαγών και θα προέτρεπαν και άλλους να χρησιμοποιήσουν τις on line υπηρεσίες. Είναι αρκετά ευχαριστημένοι και από το επίπεδο ασφαλείας το οποίο προσφέρουν οι ελληνικές τράπεζες στις ηλεκτρονικές συναλλαγές. Χρόνο με το χρόνο το ποσοστό των χρηστών της ηλεκτρονικής τραπεζικής στη χώρα μας αυξάνεται σημαντικά και προβλέπεται ότι σε μερικά χρόνια η ηλεκτρονική τραπεζική θα έχει γίνει αναπόσπαστο κομμάτι της καθημερινότητας.

Προτεραιότητα τους θα πρέπει να είναι η βελτίωση της συνεργασίας μεταξύ καταστημάτων, διαδικτύου και κέντρων επικοινωνίας. Οι επόμενες σημαντικότερες βελτιώσεις θα πρέπει να αφορούν την αύξηση της λειτουργικότητας των πωλήσεων μέσω online banking , τη μετακίνηση περισσότερων πελατειακών συναλλαγών μακριά από τα ταμεία των καταστημάτων και τη βελτίωση των υπηρεσιών mobile internet banking.

Τέλος , αν οι τράπεζες ενδιαφέρονται για την προώθηση των εναλλακτικών αυτών καναλιών θα πρέπει αφενός να επενδύσουν σε τεχνολογίες που θα διασφαλίζουν υψηλότερο επίπεδο ασφάλειας, για το οποίο θα μπορούν να πείσουν όμως τους καταναλωτές, αφετέρου να ενημερώσουν τους πελάτες τους διεξοδικά για τις δυνατότητες που προσφέρουν οι μορφές αυτές , αλλά και να τους παρέχουν τη δυνατότητα δοκιμαστικής χρήσης σε όλες τις περιπτώσεις. Οι καταναλωτές , στην πλειοψηφία τους , φαίνονται θετικοί έναντι των καναλιών αυτών και αν αρθούν τα εμπόδια που εμποδίζουν την υιοθέτηση τους είναι ζήτημα χρόνου να φτάσουν στη χρήση.

ΙΣΤΟΓΡΑΦΙΑ

- www.in.gr :Δημοσίευση 31/08/2010
- www.digilib.lib : «Ηλεκτρονική τραπεζική», Ψηφιακή βιβλιοθήκη Πανεπιστημίου Πειραιά
- www.tbank.com
- www.banknew.gr
- www.diametakomistes-elta.blogspot.gr: Κέρδη 22 εκατ. ευρώ στο πρώτο τρίμηνο

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Εφημερίδα: Ελληνική γνώμη , Ιούλιος 2009
- Αγγέλης Βασίλειος :«Η βίβλος του e-banking»,εκδόσεις νέων τεχνολιγιών,2005
- Εφημερίδα ημερησία: «500.000 Έλληνες χρησιμοποιούν την ηλεκτρονική τραπεζική»,12/12/06
- Εφημερίδα Έθνος: 08/07/2011
- Χατζηκωνσταντής Λ. : «Τάσεις και προκλήσεις για την αγορά της ηλεκτρονικής τραπεζικής», e-banking forum,2003
- Κεφαλάς Χ. : «Η λειτουργία των Ελληνικών τραπεζών στο περιβάλλον της ONE»,ΕΕΤ,2001
- Κράπης Βασίλειος: «Διαδικτυακές εφαρμογές στον τραπεζικό χώρο»,2008
- Περιοδικό RAM: web teller , Εγνατία Τράπεζα, Ιούνιος 2000
- Περιοδικό RAM : Οι τράπεζες στο χορό του internet , Ιούνιος 2000
- Δελτίο Ελληνικής Ένωσης Τραπεζών: Αφιέρωμα στο e-banking, Ιούλιος – Σεπτέμβριος 2003
- Εφημερίδα εξπρές : 29/06/2009

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- ✓ **Ramirez Carl, electronic banking, Diane publishing Co., 1998**
- ✓ **Hilmon Richard, Wong Kate, electronic banking, Diane publishing Co., 2000**
- ✓ **Guttmann Robert cyber cash: The coming era of electronic money, Palgrave Macmillan,2003**
- ✓ **Deutsch Bundesbank, Electronic banking from a prudential supervisory perspective**