ΑΤΕΙ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΟΙ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΣΤΟ ΗΛΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΗΣ ΣΠΟΥΔΑΣΤΡΙΑΣ:

ΓΙΑΝΝΑΚΟΠΟΥΛΟΥ ΑΡΙΣΤΕΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:ΠΑΠΑΔΟΠΟΥΛΟΣ ΔΗΜΗΤΡΙΟΣ

ΠΑΤΡΑ 2012

1.ΠΕΡΙΛΗΨΗ

Η ραγδαία **ε**ξέλιξη του διαδικτύου την τελευταία δεκαετία και η χρήση του για εμπορικούς σκοπούς δημιούργησε νέες ανάγκες στον χώρο των επιχειρήσεων. Οι επιχειρήσεις προκειμένου να συμβαδίσουν με αυτές τις νέες τεχνολογικές αλλαγές και να παραμείνουν ανταγωνιστικές στον ολοένα και μεταβαλλόμενο επιχειρηματικό κόσμο καλούνται να δημιουργήσουν τις υποδομές εκείνες που θα επιτρέψουν στους καταναλωτές την αγορά προϊόντων και υπηρεσιών μέσω του διαδικτύου.

Αρχικά στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι ηλεκτρονικές συναλλαγές γίνονταν δίχως την χρήση διαδικτύου. όμως αυτός ο τρόπος ήταν χρονοβόρος και πολλές φόρες και αναξιόπιστος σε σχέση με τον σημερινό τρόπο διεκπεραίωσης διαδικτυακών συναλλαγών. Έτσι άρχισε σίγα σίγα να αναπτύσσεται μια σειρά από ηλεκτρονικά συστήματα πληρωμών. Αυτά τα ηλεκτρονικά συστήματα πληρωμών έδωσαν στο καταναλωτικό κοινό την δυνατότητα χρήσης μιας γκάμας καινοτομιών όπως την χρήση πιστωτικής κάρτας μέσω του internet για την αγορά προϊόντων και την εξόφληση λογαριασμών κ.α.

Σκοπός της παρούσας πτυχιακής εργασίας πτυχιακής εργασίας είναι να αναδεχθεί το θέμα που αφορά την κρυπτογραφία και πως βρίσκει εφαρμογή στο ηλεκτρονικό εμπόριο και την ηλεκτρονική τραπεζική. Η εργασία θα ξεκινήσει με μια μικρή αναφορά γενικά στο internet, και θα ακολουθούσουν κάποια στατιστικά στοιχειά σχετικά με την χρήση του στην Ελλάδα. Έπειτα θα αναφερθώ στο ηλεκτρονικό εμπόριο και τις ηλεκτρονικές πληρωμές και κατ' επέκταση στο e-banking. Στην συνέχεια στους κινδύνους που απειλούν τις ηλεκτρονικές συναλλαγές και ποιες μεθόδους ασφάλειας χρησιμοποιούν οι επιχειρήσεις και οι τράπεζες προκειμένου ν προστατέψουν τα προϊόντα τους και τους πελάτες τους.

1.ABSTRACT

The rapid development of the Internet over the last decade and its use for commercial purposes created new needs in the area of operations. Businesses in order to keep pace with these new technological changes and to remain competitive in an increasingly changing business world are invited to create the infrastructure that will enable consumers to purchase products and services via the Internet.

Originally in the early stages of development of electronic commerce transactions were without the use of Internet. but this was time-consuming and many times and unreliable compared with the current way of handling online transactions. Thus began to developed a series of electronic payment systems. These electronic payment systems have in common the ability to use consumer a range of innovations such as using a credit card over the internet to buy products and payment accounts etc.

The purpose of this thesis is to take over the issue concerning Cryptography and that finds application in e-commerce and online banking. The task will start with a small general reference on the internet, and some statistical data follow on use in Greece. Then refer to the e-commerce and electronic payments and e-' extension to banking. Then the dangers which threaten electronic transactions and what security methods used by companies and banks in order n protect products and their customers.

ΠΕΡΙΕΧΟΜΕΝΑ

2.ΓΕΝΙΚΑ ΓΙΑ ΤΟ INTERNET

Για πρώτη φορά στην ανθρωπινή ιστορία όλος ο κόσμος βρίσκεται πραγματικά στα δάκτυλα μας .Η αστείρευτη πηγή που λέγεται internet κρύβει κάποια μυστικά που όσο πιο καλά τα γνωρίζει κάποιος τόσο πιο εύκολα υλοποιεί το σκοπό του. Το διαδίκτυο είναι ένα μέσο μαζικής επικοινωνίας .Είναι ένα πλέγμα από εκατομμύρια διασυνδεδεμένους υπολογιστές που εκτείνεται σε κάθε γωνία του πλανήτη και παρέχει τις υπηρεσίες του σε εκατομμύρια χρηστές .Αποτελεί ένα παγκόσμιο ηλεκτρονικό χωριό οι κάτοικοι του οποίου ανεξάρτητα από υπηκοότητα, ηλικία, θρήσκευμα και χρώμα μοιράζονται πληροφορίες και ανταλλάσουν απόψεις, μορφώνονται, διασκεδάζουν περά από γεωγραφικά και κοινωνικά σύνορα. Σύμφωνα με εκτιμήσεις αυτός ο παγκόσμιος ιστός υπολογιστών και χρηστών αριθμεί σήμερα δισεκατομμύρια χρηστές ενώ επεκτείνεται διαρκώς σε εκθετικούς αριθμούς. Το διαδίκτυο αλλά και η ψηφιακή τεχνολογία γενικότερα έχουν τη ικανότητα να δημιουργούν εικονικούς χώρους, εικονικές κοινότητες όπου παύουν να υφίστανται οι κοινωνικές και πολιτιστικές διαχωριστικές γραμμές

που υπάρχουν στο πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεραστούν εύκολα.

Η επικοινωνία μέσω του διαδικτύου γίνεται άμεση και αμφίδρομη.
Δίνεται η δυνατότητα σε κάθε χρήστη ηλεκτρονικού υπολογιστή συνδεδεμένου στο διαδίκτυο να πληροφορηθεί ανταλλάσοντας απόψεις μέσω ενός συμετοχικότερου και λιγότερο ελεγχόμενου διαύλου επικοινωνίας. Οι χρήστες αποτελούν ολοένα και περισσότερο την ιδιότητα του παγκόσμιου πολίτη. Υπάρχει ήδη από την αρχή της εμφάνισης του διαδικτύου να θεωρείται ως άκρως δημοκρατικό μέσο επικοινωνίας το οποίο αποδιαμεσολαβεί την επικοινωνία και καθιστά ισχυρότερο τον μέσο άνθρωπο καθώς δίνει στον τελευταίο την δυνατότητα πρόσβασης σε μεγάλο όγκο πληροφοριών συγκεντρωμένων σε ένα χώρο και την δυνατότητα της προσωπικής επιλογής των πληροφοριών αυτών.

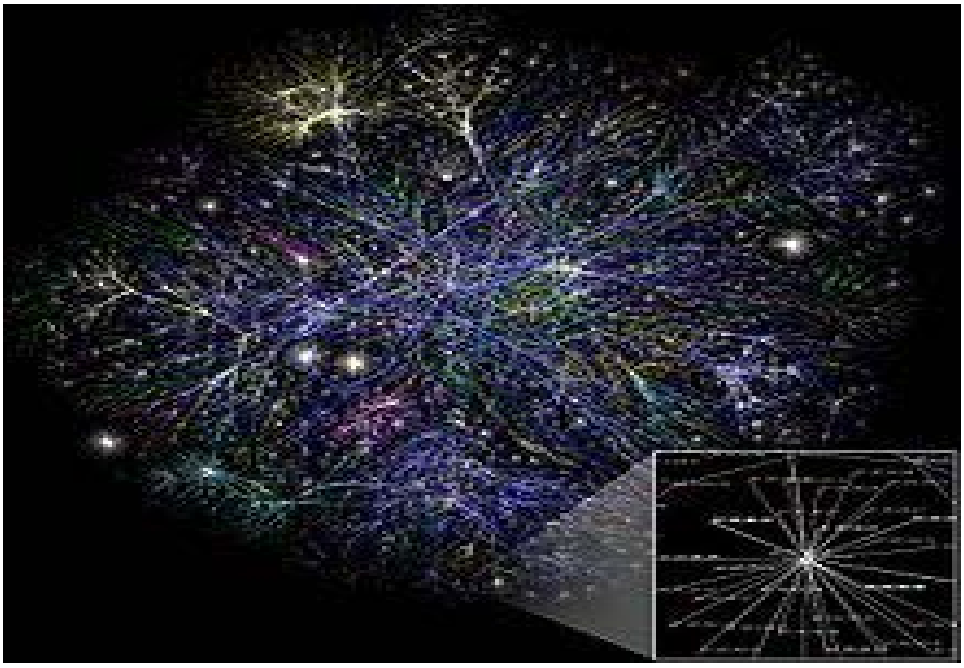
2.1 ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ INTERNET

Ένα βασικό χαρακτηριστικό του internet είναι ότι μπορεί να συνδέσει υπολογιστές διαφορετικού τύπου, δηλαδή υπολογιστές που μπορεί να διαφέρουν όσον αφορά την αρχιτεκτονική του υλικού(hardware), το λειτουργικό σύστημα που χρησιμοποιούν και το πρωτόκολλο δικτύωσης που εφαρμόζεται στο τοπικό τους δίκτυο. Ακριβώς εξαιτίας αυτής της ευελιξίας του εξαπλώθηκε σε ολόκληρο τον πλανήτη κατά την διάρκεια των τελευταίων δεκαετιών. Ένα άλλο χαρακτηριστικό του internet είναι ότι είναι αποκεντρωμένο κα αυτοδιαχειριζόμενο. Δεν υπάρχει δηλαδή κάποιος κεντρικός οργανισμός που να το διευθύνει και να παίρνει συνολικά αποφάσεις ,σχετικά με το είδος των πληροφοριών που διακινούνται, τις υπηρεσίες που παρέχονται από τους διάφορους υπολογιστές ή την διαχείρησή του. Καθένα από τα μικρότερα δίκτυα που το αποτελούν διατηρεί την ανωνυμία και είναι το ίδιο υπεύθυνο για το είδος των πληροφοριών που διακινεί, τις υπηρεσίες που προσφέρουν οι υπολογιστές και την διαχείρισή του.

2.2 Η ΤΕΧΝΟΛΟΓΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Η τεχνολογία του είναι κυρίως βασισμένη στην διασύνδεση επιμέρους δικτύων ανά τον κόσμο και πολυάριθμα τεχνολογικά πρωτόκολλα με κύριο το TCP/IP.Μερικά από τα ποιο γνωστά διαδικτυακά πρωτόκολλα είναι το IP,TCP.UDP,DNS,PPS,SLIP,ICMP,POP3,IMAP,SMTP,HTTPS,HTTP,SSH,TELNET,FTP,LDAP,SSL
Μερικές από τις πιο γνωστές διαδικτυακές υπηρεσίες που χρησιμοποιούν αυτά τα πρωτόκολλα είναι .
-Το ηλεκτρονικό ταχυδρομείο(e-mail)
- Οι ομάδες συζητήσεων (newsgroups)
-Η διαμοίραση αρχείων (file sharing)
-Η επιφόρτιση αρχείων (file transfer)
-Ο παγκόσμιος ιστός (world wide web)
Από αυτές το ηλεκτρονικό ταχυδρομείο και ο παγκόσμιος ιστός είναι οι πιο ευρέως χρησιμοποιούμενες, ενώ πολλές άλλες υπηρεσίες έχουν βασιστεί πάνω σε αυτές, όπως οι ταχυδρομικές λίστες (mailing lists) και τα αρχεία καταγραφής ιστού (blogs) .Το διαδίκτυο καθιστά δυνατή την διάθεση υπηρεσιών σε πραγματικό χρόνο, υπηρεσίες όπως το ραδιόφωνο μέσω ιστού και οι προβλέψεις μέσω ιστού, που είναι προσπελάσιμες από οπουδήποτε στον κόσμο. [1]

[1] Πηγή:http://www.freshweb.gr



Οπτικοποιημένη αναπαράσταση διαφόρων διαδρομών (routes) διαμέσου ενός τμήματος του Ίντερνετ

2.3 ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το Ίντερνετ, σε συνδυασμό με την ολοένα αναπτυσσόμενη ψηφιακή τεχνολογία, έχει δημιουργήσει μία τεράστια αγορά γνώσεων/πληροφοριών. Παραδοσιακές μορφές τέχνης (όπως για παράδειγμα ο κινηματογράφος και η μουσική) μέσω της ψηφιακής τεχνολογίας παίρνουν την ίδια μορφή (αρχείων δεδομένων) με αντικείμενα που εκ πρώτης όψεως είναι εντελώς διαφορετικά (όπως για παράδειγμα η ιατρική επιστήμη ή κάποιο πρόγραμμα λογισμικού). Παρατηρείται λοιπόν μία συγκέντρωση γνώσης ή, αν είναι δυνατό να λεχτεί, πολιτιστικής κληρονομιάς, που σχετίζεται άμεσα με το Ίντερνετ. Το μεγάλο ερώτημα που προκύπτει πλέον είναι το "ποιος θα διοικήσει, ποιος θα ελέγξει την γνώση αυτή".

Από τη στιγμή που το Διαδίκτυο είναι ένα δίκτυο συνδεδεμένων υπολογιστών, κάθε χρήστης έχει την δυνατότητα να μοιραστεί πληροφορίες με άλλους χρήστες γενόμενος, πολλές φορές, ο ίδιος δημιουργός και πάροχος των πληροφοριών αυτών. Δεν υπάρχει άμεσος έλεγχος των πληροφοριών που "ανεβαίνουν" στο Διαδίκτυο από κάποιον ιεραρχικά ανώτερο χρήστη ή οργανισμό. Το θέμα της μη ιεραρχημένης πληροφορίας, όμως, τίθεται υπό αμφισβήτηση. Ο όγκος της πληροφορίας στο Διαδίκτυο είναι πράγματι μεγάλος. Παρ' όλα αυτά, υπάρχουν πληροφορίες ευκολότερα και δυσκολότερα προσβάσιμες από τον χρήστη.

Το Ίντερνετ έκανε δυνατή την συγκέντρωση μεγάλου όγκου πληροφοριών και επηρέασε σημαντικά τον τρόπο διάθεσής τους. Δεν συμβαίνει, όμως, στον ίδιο βαθμό το ίδιο και στον τρόπο παραγωγής αυτών. Για παράδειγμα, ο τρόπος παραγωγής μιας κινηματογραφικής ταινίας δεν έχει επηρεαστεί σημαντικά από την ύπαρξη του Ίντερνετ, ανεξάρτητα από το αν έχει

επηρεαστεί ή όχι από την ψηφιακή τεχνολογία. Παρ' όλα αυτά, και σύμφωνα με την ιντερνετοφιλική προσέγγιση, το Διαδίκτυο ασκεί μεγάλη επίδραση στην διαδικασία παραγωγής δημοσιογραφικών προϊόντων. Η δημιουργία της είδησης παύει να είναι πλέον μονοπώλιο λίγων, αφού ο κάθε χρήστης μπορεί εάν το επιθυμεί να δημιουργήσει πληροφορία ανά πάσα στιγμή. Το πιο τρανταχτό παράδειγμα της επίδρασης αυτής είναι τα ιστολόγια (blogs), όπου μπορεί κανείς να εκφέρει απόψεις και να σχολιάσει γεγονότα πάσης φύσεως . Ως αποτέλεσμα της επιρροής αυτής του Ίντερνετ στη παραγωγή ειδήσεων τα όρια μεταξύ ενός απλού χρήστη του διαδικτύου και ενός επαγγελματία δημοσιογράφου γίνονται περισσότερο δυσδιάκριτα.

Επίσης, λόγω της μεγάλης συγκέντρωσης γνώσης στο Διαδίκτυο, η έννοια της κοινωνικής ισότητας παίρνει και πάλι μεγάλη σημασία. Το χάσμα ανάμεσα σε πληροφοριακά πλούσιους και πληροφοριακά φτωχούς θα διευρύνεται όσο αυξάνεται η συγκέντρωση της γνώσης αυτής. Το παραπάνω αποτελεί ακόμα έναν λόγο που κάνει πιο επιτακτική την ανάγκη για διερεύνηση του αρχικού ερωτήματος "ποιος θα ελέγξει τη γνώση αυτή".

Η γλώσσα που χρησιμοποιείται περισσότερο στη διακίνηση της πληροφορίας στο Διαδίκτυο είναι η Αγγλική. Έχοντας αναπτυχθεί τα τελευταία χρόνια, το Διαδίκτυο περιλαμβάνει πλέον ποιοτικά και ποσοτικά ευρύ περιεχόμενο και στις υπόλοιπες γλώσσες των περισσότερο αναπτυγμένων χωρών. Ωστόσο, υπάρχουν ακόμα δυσλειτουργίες και τεχνικά προβλήματα σχετικά με την κωδικοποίηση, όπως το mojibake.

2.4 ΝΟΜΙΚΑ ΚΑΙ ΗΘΙΚΑ ΖΗΤΗΜΑΤΑ

Η παραβίαση πνευματικών δικαιωμάτων, η πορνογραφία, η ψευδοπροσωπία και η προσφορά παρανόμων προϊόντων είναι φαινόμενα υπαρκτά στο Ίντερνετ και ο περιορισμός τους είναι ιδιαίτερα δύσκολος. Για παράδειγμα, η λέξη "sex" παραμένει μία από τις πλέον δημοφιλείς στις μηχανές αναζήτησης. Συχνά, η ανησυχία αυτή, που θεωρείται από κάποιους αβάσιμη, μπορεί να υποστηριχθεί από κάποια εγκλήματα ή αποτρόπαιες καταστάσεις (συνήθως περιπτώσεις παιδεραστίας κ.ά.).

Το Διαδίκτυο έχει κατηγορηθεί ως παράγοντας που έπαιξε ρόλο σε θανάτους . Ο Μπράντον Βέντας (Brandon Vedas) πέθανε από υπερβολική δόση ενός μίγματος νομίμων και παρανόμων ναρκωτικών παρακινούμενος από συνομιλητές του στο IRC. Ο Σων Γούλεϊ (Shawn Woolley) αυτοκτόνησε με πιστόλι για λόγους που σχετίζονται με τον εθισμό του με το EverQuest, ένα Μαζικά Πολυχρηστικό Διαδικτυακό Παιχνίδι Ρόλων (MMORPG), όπως ισχυρίστηκε η μητέρα του. Ο Άρμιν Μάιβες (Armin Meiwes) μαχαίρωσε μέχρι θανάτου και έφαγε μέρος του σώματος του Μπέρντ-Γιούργκεν Μπράντες (Bernd Jürgen Brandes)όταν ο τελευταίος απάντησε στην αγγελία του

πρώτου που ζητούσε έναν «μεγαλόσωμο άνδρα έτοιμο να σφαγιαστεί και μετά να καταβροχθιστεί».

Επιπλέον, το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη, αντίστοιχη, αρχή, η οποία να ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί - σύμφωνα με πολλούς χρήστες αυτό θα αποτελούσε λογοκρισία. Όπως χαρακτηριστικά λέγεται "το Διαδίκτυο ελέγχεται από τους χρήστες του". Βεβαίως, οι κρατικές υπηρεσίες και αστυνομίες σε κάθε χώρα, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου.

Επίσης, ένα ακόμη ηθικό ζήτημα είναι ο συγκεντρωτισμός των Μ.Μ.Ε. και αναφέρεται στο ολιγοπώλιο μικρού σχετικά αριθμού εταιριών που κατέχουν τα μέσα και ελέγχουν όλη την αλυσίδα διανομής του προϊόντος. Στα πλαίσια του Διαδικτύου τίθεται το ερώτημα του κατά πόσο οι οικονομικές διαδικασίες στο παρόν καπιταλιστικό γίγνεσθαι περιορίζουν τη δημόσια σφαίρα και το αν είναι αποδεκτή ή κατακριτέα η πρωτοφανής ισοτιμία στην παρουσία και διαχείριση της πληροφορίας και του εμπορεύματος στο χώρο του Ίντερνετ. Επίσης παρά το γεγονός ότι το Ίντερνετ συχνά περιγράφεται ως *αποκεντρωμένο*, με απροσπέλαστο όγκο πληροφοριών και, συνεπώς, χωρίς κεντρικό έλεγχο, είναι εμφανής η εκτενής ιεράρχηση του περιεχομένου από μηχανές αναζήτησης και η γενικότερη διαιώνιση των ιστοτόπων με την υψηλότερη επισκεψιμότητα. [2]

2.5 ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Κοινές μέθοδοι πρόσβασης στο Διαδίκτυο είναι η επιλογική και η ευρυζωνική. Δημόσιοι χώροι για χρήση του Διαδικτύου περιλαμβάνουν τις βιβλιοθήκες και τα Internet cafes, όπου υπάρχουν διαθέσιμοι Η/Υ με σύνδεση στο Διαδίκτυο. Υπάρχουν, επίσης, σημεία πρόσβασης στο Διαδίκτυο σε δημόσιους χώρους όπως αίθουσες αναμονής αεροδρομίων, μερικές φορές μόνο για σύντομη χρήση ενόσω βρισκόμαστε σε αναμονή. Τέτοια σημεία είναι γνωστά και με διάφορους άλλους όρους, όπως «δημόσια περίπτερα Διαδικτύου», «δημόσια τερματικά Διαδικτύου» και «ιστο - τηλέφωνα».

Η δικτύωση μέσω Wi-Fi παρέχει ασύρματη πρόσβαση στο Διαδίκτυο. Ασύρματα σημεία πρόσβασης (hotspot) που παρέχουν τέτοια πρόσβαση περιλαμβάνουν τα Wifi-cafes, όπου κάποιος αρκεί να φέρει τις δικές του/της ασύρματες συσκευές όπως φορητό Η/Υ ή PDA. Οι υπηρεσίες αυτές μπορεί να είναι δωρεάν σε όλους, είτε δωρεάν μόνο σε πελάτες, είτε επί πληρωμή. Ένα hotspot δεν χρειάζεται να περιορίζεται σε ένα συγκεκριμένο περιβάλλον. Ολόκληρες πανεπιστημιουπόλεις και πάρκα έχουν αυτή τη δυνατότητα, ακόμα

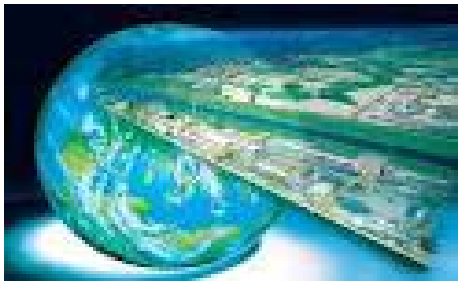
[2] http://www.awmn.net

και ολόκληρες περιοχές. Προσπάθειες να συνδεθεί και ο αγροτικός πληθυσμός έχουν οδηγήσει στα ασύρματα κοινοτικά δίκτυα.

Τα πλεονεκτήματα της πρόσβασης ενός χρήστη μέσω του δικού του υπολογιστή (αντί μέσω δημόσιου τερματικού) περιλαμβάνουν τη δυνατότητα για κατέβασμα και ανέβασμα αρχείων χωρίς περιορισμούς, τη χρήση του αγαπημένου του φυλλομετρητή (web browser) και των ρυθμίσεων αυτού (το μενού των ρυθμίσεων μπορεί να απενεργοποιηθεί σε έναν δημόσιο υπολογιστή) και την εκτέλεση δραστηριοτήτων στο Ίντερνετ με τη χρήση δικών του προγραμμάτων και δεδομένων.

Χώρες με πολύ καλή πρόσβαση στο Ίντερνετ περιλαμβάνουν την Νότια Κορέα, όπου το 50% του πληθυσμού έχει ευρυζωνική πρόσβαση, τη Σουηδία και τις ΗΠΑ.

2.6 Η ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ



Οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο έχουν ενταχθεί για τα καλά πια στην καθημερινή ζωή των Ελλήνων. Συγκεκριμένα, σύμφωνα με στοιχεία που έδωσε στη δημοσιότητα το Παρατηρητήριο για την Κοινωνία της Πληροφορίας (ΚτΠ), ο μισός πληθυσμός της χώρας μας (51%) χρησιμοποιεί πλέον ηλεκτρονικό υπολογιστή, ενώ το 44% των Ελλήνων έχουν πρόσβαση στο διαδίκτυο, ανεξαρτήτως αν διαθέτουν προσωπική σύνδεση ή όχι.

Μεταξύ άλλων, από την έρευνα προκύπτει ότι:

" Τα πρωτεία στη χρήση του διαδικτύου κατέχουν οι άνδρες, οι νέοι ηλικίας

16-24 ετών, τα άτομα υψηλού μορφωτικού επιπέδου και οι κάτοικοι των μεγάλων αστικών κέντρων.

" Σε περιφερειακό επίπεδο, σημαντικές αποκλίσεις παρουσιάζονται μεταξύ των μεγάλων αστικών και των αγροτικών περιοχών.

" Οι γυναίκες υπολείπονται των ανδρών στη χρήση του διαδικτύου, ενώ μένουν σταθερά πίσω και από τον ευρωπαϊκό μέσο όρο.

" Υπάρχει σύγκλιση πια μεταξύ των νέων της χώρας μας ηλικίας 16-24 ετών και των συνομήλικών τους στην ΕΕ, η οποία επιτεύχθηκε με εντυπωσιακή άνοδο στη χρήση Η/Υ και διαδικτύου στην χώρα μας μεταξύ 2007 και 2008.

Το 2008, σύμφωνα με το Παρατηρητήριο, σημειώθηκε η μεγαλύτερη άνοδος στη χρήση του διαδικτύου σε σχέση με τα προηγούμενα έτη, ενώ, εκτός από την αυξητική τάση, σημειώνεται πλέον και εντατικοποίηση ως προς τη συχνότητα χρήσης, καθώς το 34% των Ελλήνων συνδέεται σε εβδομαδιαία βάση.

Σε τέσσερα από τα δέκα ελληνικά νοικοκυριά υπάρχει πλέον σύνδεση στο διαδίκτυο. Κύριο λόγο μη κατοχής σύνδεσης στο σπίτι αποτελεί η αντίληψη ότι το περιεχόμενο του διαδικτύου θεωρείται επιζήμιο, ενώ ακολουθεί η έλλειψη δεξιοτήτων για τη χρήση του, η οποία γίνεται εντονότερη όσο αυξάνεται η ηλικία των ατόμων.

Δημοφιλέστερος τόπος πρόσβασης στο διαδίκτυο παραμένει το σπίτι (77%), ενώ ακολουθούν ο χώρος εργασίας (37%) και τα Internet cafe (14%). Παράλληλα με τις "παραδοσιακές" δραστηριότητες στο διαδίκτυο, οι Έλληνες φαίνεται να στρέφονται πλέον και να αξιοποιούν τις νέες δυνατότητες επικοινωνίας και ψυχαγωγίας που προσφέρονται ηλεκτρονικά. Χαρακτηριστικά αναφέρεται ότι το 45% περίπου των τακτικών χρηστών διαβάζουν ηλεκτρονικές εφημερίδες και περιοδικά, ακούνε ραδιόφωνο και παρακολουθούν τηλεόραση μέσω του διαδικτύου.

Ωστόσο, δραστηριότητες, όπως η ηλεκτρονική τραπεζική, συγκεντρώνουν χαμηλά ποσοστά (12%), έναντι πολύ υψηλότερων σε ευρωπαϊκό επίπεδο (47%), ενδεικτικά της έλλειψης εμπιστοσύνης των Ελλήνων χρηστών στο διαδίκτυο σχετικά με την ασφάλεια των συναλλαγών.

Περισσότεροι από οκτώ στους δέκα Έλληνες είναι κάτοχοι κινητού τηλεφώνου (84%), ωστόσο, πέρα από την επικοινωνία, η χρήση των επιπλέον δυνατοτήτων που παρέχονται, είναι περιορισμένη.

2.6.1Ανάγκηενίσχυσηςτηςπεριφέρειας

Σύμφωνα με τα αποτελέσματα της έρευνας του Παρατηρητηρίου για την ΚτΠ, ανοδική τάση στη χρήση Η/Υ και διαδικτύου σημειώθηκε το 2008 στο σύνολο σχεδόν των Περιφερειών της χώρας. Με αναφορά στους τακτικούς χρήστες του διαδικτύου, τα υψηλότερα ποσοστά παρατηρούνται στις Περιφέρειες Αττικής (57%), Νοτίου Αιγαίου (47,2%) και Κρήτης (43,8%). Αντίθετα, τα

χαμηλότερα ποσοστά εμφανίζουν οι Περιφέρειες Πελοποννήσου, Δυτικής Μακεδονίας, Ηπείρου και Θεσσαλίας, υπολειπόμενες κατά 10 και πλέον ποσοστιαίες μονάδες του μέσου όρου της επικράτειας (39%).

Οι μισές και πλέον Περιφέρειες της χώρας έχουν υπερδιπλασιάσει μέσα στην περίοδο 2005 - 2008 το πλήθος των τακτικών χρηστών του διαδικτύου, ενώ υπάρχουν και περιπτώσεις όπου υπάρχει τριπλασιασμός των χρηστών (Βόρειο Αιγαίο, Πελοπόννησος). Την ίδια περίοδο, οι αγροτικές περιοχές εμφανίζουν τους μεγαλύτερους ρυθμούς αύξησης, τόσο στην χρήση του Η/Υ όσοκαιτουδιαδικτύου.

2.6.2 Το ψηφιακό χάσμα μεταξύ ανδρών και γυναικών

Το ποσοστό ανδρών και γυναικών που έχουν πρόσβαση στο διαδίκτυο, διαμορφώνεται στο 52% και 37% αντίστοιχα. Τόσο για τους άνδρες όσο και τις γυναίκες, παρατηρείται σημαντική αύξηση στη χρήση του Η/Υ και του διαδικτύου στο διάστημα 2005-2008, ωστόσο το μεταξύ τους χάσμα φαίνεται να διευρύνεται.

Σε σχέση με το ευρωπαϊκό περιβάλλον, υπάρχει υστέρηση του ποσοστού των Ελλήνων χρηστών έναντι των Ευρωπαίων. Ωστόσο, ο ανδρικός πληθυσμός της Ελλάδας εμφανίζει τάση σύγκλισης με τον αντίστοιχο της ΕΕ, έχοντας μειώσει την "ψαλίδα" από τις 23 στις 14 ποσοστιαίες μονάδες κατά την περίοδο 2005-2008. Αντίθετα, οι γυναίκες στην Ελλάδα υπολείπονται σταθερά του ευρωπαϊκού μέσου όρου, με διαφορά που ξεπερνά τις 20 ποσοστιαίες μονάδες.

Σύμφωνα με την έρευνα, το ψηφιακό χάσμα μεταξύ ανδρών και γυναικών στην Ελλάδα μειώνεται όσο υψηλότερο είναι το μορφωτικό επίπεδο των ατόμων και όσο πιο μικρή είναι η ηλικία τους. Στις νεαρότερες ηλικίες έχει επέλθει σύγκλιση μεταξύ των ανδρών και γυναικών, με εννέα στα δέκα νεαρά άτομα να είναι χρήστες του διαδικτύου.

Σημαντικό μέρος του χάσματος μεταξύ των δύο φύλων οφείλεται στο μικρότερο βαθμό ένταξης των γυναικών στην αγορά εργασίας σε σχέση με τους άνδρες. Ως προς τους λόγους χρήσης του διαδικτύου, οι γυναίκες υπερτερούν των ανδρών σε θέματα αναζήτησης πληροφοριών για ταξίδια, εκπαίδευση και εργασία, ενώ η υπεροχή των ανδρών είναι ξεκάθαρη σε ότι έχει να κάνει με ηλεκτρονικά παιχνίδια, λήψη λογισμικού για τον Η/Υ, τηλεφωνία μέσω διαδικτύου, αλλά και συναλλαγές μέσω ηλεκτρονικής τραπεζικής.

Εμφανές το "ψηφιακό χάσμα γενεών", πλήρως εξοικειωμένοι οι νέοι

Μεγάλες αποκλίσεις παρατηρούνται μεταξύ των διαφόρων ηλικιακών ομάδων ως προς τη χρήση των νέων τεχνολογιών. Η χρήση των τεχνολογιών πληροφορικής κυμαίνεται σε πολύ υψηλά επίπεδα στους νέους 16-24 ετών, ενώ όσο αυξάνεται η ηλικία των ατόμων, μειώνεται ο βαθμός εξοικείωσής τους με τις νέες τεχνολογίες. Σημειώθηκε σημαντική αύξηση των ποσοστών

χρήσης στο διάστημα 2005-2008, η οποία είναι ιδιαίτερα έντονη στις ηλικιακές κατηγορίες 25-34 και 35-44 ετών.

2.7 ΣΤΑΤΙΣΤΙΚΑ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ ΙΝΤΕΡΝΕΤ ΣΤΗΝ ΕΛΛΑΔΑ.

Η Google Greece στα πλαίσια εκδήλωσης που πραγματοποίησε για το Adsense πριν από μερικές μέρες στην Αθήνα ανακοίνωσε κάποια ενδιαφέροντα στατιστικά για τη χρήση του διαδικτύου στην Ελλάδα. Τα πιο αξιοσημείωτα στοιχεία είναι τα εξής:

- Πάνω από 4 εκατομμύρια κάτοικοι έχουν πρόσβαση στο ίντερνετ.
- Πάνω από 200.000 smartphones πουλήθηκαν κατά το τελευταίο τρίμηνο του 2010 – αριθμός που ξεπερνά τον αντίστοιχο των επιτραπέζιων υπολογιστών.
- 30 εκατομμύρια βίντεο προβάλλονται κάθε μήνα μέσω του YouTube.
- Ο αριθμός των λογαριασμών σε υπηρεσίες κοινωνικής δικτύωσης φτάνει τα 4 εκατομμύρια.
- Ο μέσος εβδομαδιαίος χρόνος που αφιερώνει κάποιος online φτάνει τις 10 ώρες.
- Καθημερινά πραγματοποιούνται πάνω από 500.000 αναζητήσεις.
- Η άνοδος της χρήσης του διαδικτύου μέσω κινητών συσκευών αυξάνεται με ταχείς ρυθμούς. Συγκεκριμένα, 8 φορές ταχύτερα σε σχέση με τον αντίστοιχο.

Όσο αυξάνεται η ηλικία των ατόμων, αυξάνεται και το χάσμα μεταξύ Ελλάδας και Ευρώπης, φτάνοντας σχεδόν τις 20 ποσοστιαίες μονάδες για τις ηλικίες

65-74 ετών. Ωστόσο, υπάρχει πλέον σύγκλιση μεταξύ των νέων της χώρας μας ηλικίας 16-24 ετών και των συνομήλικών τους στην ΕΕ, η οποία επιτεύχθηκε με εντυπωσιακή άνοδο στην Ελλάδα στη χρήση Η/Υ και διαδικτύου μεταξύ 2007 και 2008 (από 87% σε 92% και από 75% σε 87% αντίστοιχα).

Τα νεαρότερα άτομα χρησιμοποιούν κυρίως το διαδίκτυο για λόγους επικοινωνίας με άλλους χρήστες και ψυχαγωγίας. Στην ηλικιακή κατηγορία 35-44 ετών παρατηρείται υψηλότερη ιεράρχηση του πληροφοριακού χαρακτήρα του διαδικτύου, ενώ χρησιμοποιούνται σημαντικά και οι υπηρεσίες που αφορούν σε ταξίδια και διαμονή. Αξιοσημείωτο είναι ότι χρήστες ηλικιών 55-64 ετών είναι δεύτεροι σε ανάγνωση ιστολογιών (blogs), με ποσοστό 33,9% μετά τους νέους 16-24 ετών (37%).[3]

[3] http://www.insomnia.gr

3. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Ως Ηλεκτρονικό Εμπόριο (Η.Ε.),ή ευρέως γνωστό ως e-commerce, eCommerce ή e-comm,ορίζεται το εμπόριο παροχής αγαθών και υπηρεσιών που πραγματοποιείται εξ αποστάσεως με ηλεκτρονικά μέσα, βασιζόμενο δηλαδή στην ηλεκτρονική μετάδοση δεδομένων, χωρίς να καθίσταται αναγκαία η φυσική παρουσία των συμβαλλομένων μερών, πωλητή - αγοραστή. Περιλαμβάνει το σύνολο των διαδικτυακών διαδικασιών: ανάπτυξης , προώθησης, πώλησης ,παράδοσης, εξυπηρέτησης και πληρωμής για προϊόντα και υπηρεσίες. Το εύρος των ανταλλαγών που διεξάγονται ηλεκτρονικά, έχει αυξηθεί ασυνήθιστα με την ευρεία χρήση του internet. Η χρήση του εμπορίου διεξάγεται κατ ’αυτόν τον τρόπο, παρακινώντας και απορροφώντας καινοτομίες στην ηλεκτρονική μεταφορά χρηματικών πόρων(electronic funds transfer), στη διαχείριση της εφοδιαστικής αλυσίδας(supply chain management), στο διαδικτυακό marketing (Internet marketing), στη διεκπεραίωση διαδικτυακών διαδικασιών(online transaction processing) , στην ανταλλαγή ηλεκτρονικών δεδομένων(electronic data interchange (EDI)), ,στην καταγραφή συστημάτων διοίκησης(inventory management) και στην αυτοματοποίηση συστημάτων συγκέντρωσης δεδομένων. Το ηλεκτρονικό εμπόριο μπορεί να οριστεί από τέσσερις διαφορετικές οπτικές γωνίες.

Επιχειρήσεις: Ως εφαρμογή νέων τεχνολογιών προς την κατεύθυνση του αυτοματισμού των συναλλαγών και της ροής εργασιών.

Υπηρεσίες: Ως μηχανισμός που έχει στόχο να ικανοποιήσει την κοινή επιθυμία προμηθευτών και πελατών για καλύτερη ποιότητα υπηρεσιών, μεγαλύτερη ταχύτητα εκτέλεσης συναλλαγών και μικρότερο κόστος.

Απόσταση: Ως δυνατότητα αγοραπωλησίας προϊόντων και υπηρεσιών μέσω του Internet ανεξάρτητα από τη γεωγραφική απόσταση.

Επικοινωνία: Ως δυνατότητα παροχής πληροφοριών, προϊόντων ή υπηρεσιών, και πληρωμών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.,έντυπα όπως παραγγελίες αγοράς, συνοδευτικά έγγραφα και

επιταγές πληρωμής, μπορούν να γίνουν κατά ένα μέρος ή στο σύνολό τους ηλεκτρονικά, με δομημένο τρόπο, χάρη στα συστήματα EDI ή μέσω του ηλεκτρονικού ταχυδρομείου

3.1 ΤΟ ΙΣΤΟΡΙΚΟ ΤΗΣ ΑΝΑΠΤΥΞΗΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

3.1.1 Δεκαετία του 1970

Εμφανίζονται τα συστήματα ηλεκτρονικής μεταφοράς χρηματικών πόρων μεταξύ τραπεζών που χρησιμοποιούν ασφαλή ιδιωτικά δίκτυα. Τα συστήματα EFT αλλάζουν τη μορφή των αγορών.

3.1.2 Δεκαετία του 1980

Οι τεχνολογίες ηλεκτρονικής επικοινωνίας που βασίζονται στην αρχιτεκτονική της ανταλλαγής μηνυμάτων (συστήματα EDI και ηλεκτρονικό ταχυδρομείο) αποκτούν σημαντική διάδοση. Πολλές δραστηριότητες που παραδοσιακά διεκπεραιώνονταν με βασικό μέσο το χαρτί μπορούν πλέον να γίνουν ταχύτερα και με μικρότερο κόστος.

3.1.3 Τέλη της δεκαετίας του 1980 - αρχές της δεκαετίας του 1990

Τα ηλεκτρονικά δίκτυα προσφέρουν μια νέα μορφή κοινωνικής επικοινωνίας με δυνατότητες, όπως: ηλεκτρονικό ταχυδρομείο (e-mail), ηλεκτρονική διάσκεψη (conferencing) και ηλεκτρονική συνομιλία (IRC), ομάδες συζήτησης (newsgroups, forums), μεταφορά αρχείων (FTP), κτλ. Η πρόσβαση στο δίκτυο γίνεται φτηνότερη λόγω της διεθνούς απελευθέρωσης της αγοράς τηλεπικοινωνιών.

3.1.4 Μέσα της δεκαετίας του 1990

Η εμφάνιση του Παγκόσμιου Ιστού(www) στο Internet και η επικράτηση των προσωπικών ηλεκτρονικών υπολογιστών (PC) που χρησιμοποιούν λειτουργικά συστήματα τύπου Windows προσφέρουν μεγάλη ευκολία χρήσης λύνοντας το πρόβλημα της δημοσίευσης και της εύρεσης πληροφοριών στο διαδίκτυο. Το ηλεκτρονικό εμπόριο γίνεται ένας πολύ φτηνότερος τρόπος για την πραγματοποίηση μεγάλου όγκου συναλλαγών, ενώ συγχρόνως διευκολύνει την παράλληλη λειτουργία πολλών διαφορετικών επιχειρηματικών

δραστηριοτήτων επιτρέποντας σε μικρές επιχειρήσεις να ανταγωνιστούν μεγαλύτερες, με πολύ ευνοϊκότερες προϋποθέσεις.

3.1.5 Τέλη της δεκαετίας του 1990

Η καθιέρωση μεθόδων κρυπτογράφησης του περιεχομένου και. εξακρίβωσης της ταυτότητας του αποστολέα ηλεκτρονικών μηνυμάτων, καθώς και η σχετική προσαρμογή της νομοθεσίας στους τομείς των εισαγωγών-εξαγωγών και των επικοινωνιών καθιστούν δυνατή την πραγματοποίηση ασφαλών διεθνών ηλεκτρονικών συναλλαγών.

3.2 ΝΟΜΙΚΕΣ ΠΤΥΧΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ: Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου.

ΣΚΟΠΟΣ: Ενίσχυση νομικής ασφάλειας του ηλεκτρονικού εμπορίου και αύξηση της εμπιστοσύνης των χρηστών του διαδικτύου.

ΣΤΟΧΟΣ: Να μπορεί να εφαρμοστεί σε όλη την ευρωπαϊκή κλίμακα, σε όλα τα κράτη μέλη.

ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ: Σε όλους τους φορείς υπηρεσιών της κοινωνίας της πληροφορίας.

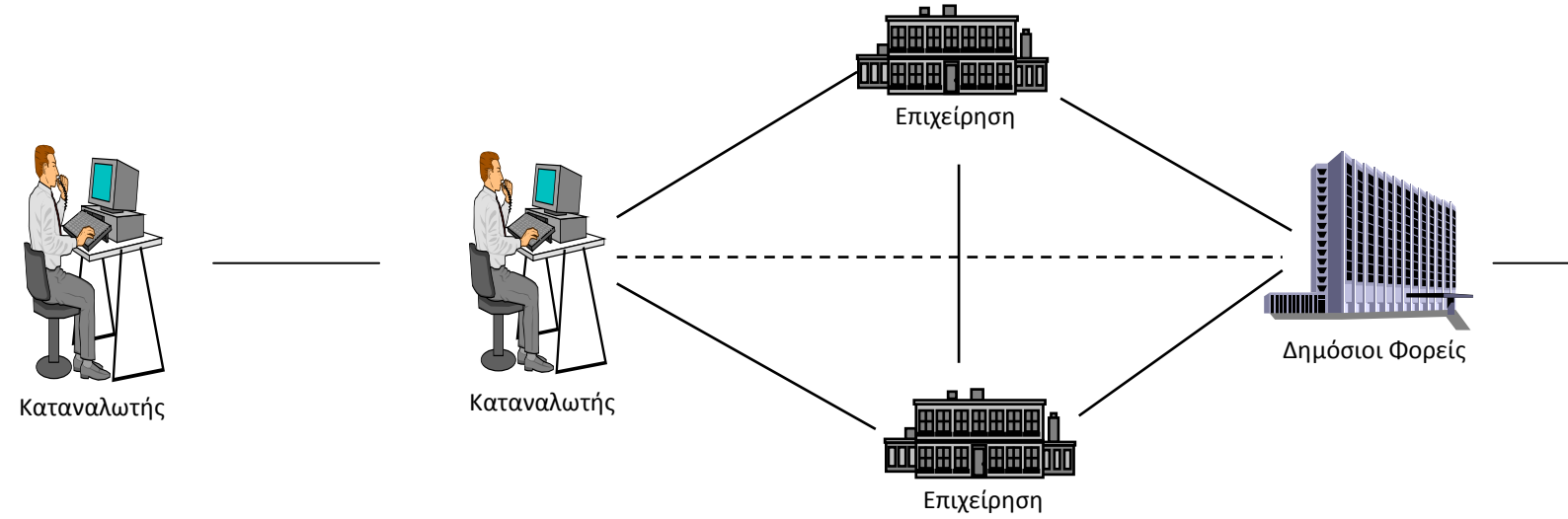
3.3 ΟΙ ΜΟΡΦΕΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Ως προς την επικοινωνία και τις συναλλαγές που πραγματοποιούνται μεταξύ των εμπλεκομένων φορέων, το ηλεκτρονικό εμπόριο διακρίνεται κυρίως σε έξι κύρια μοντέλα :

Οι βασικοί μορφές του είναι :

- Επιχείρηση με Επιχείρηση (Business-to-Business ή B2B)
- Επιχείρηση με Κράτος (business-to-government ή B2G)
- Καταναλωτή με Κράτος (consumer-to government ή C2G)
- Κράτος με Κράτος (government-to-government ή G2G)
- Επιχείρηση με Καταναλωτή (business-to-consumer ή B2C)

- Καταναλωτή με Καταναλωτή (consumer-to-consumer ή C2C)



- **3.3.1 Εσωτερικό εμπόριο**

Στόχος είναι η αποτελεσματικότερη λειτουργία των δραστηριοτήτων μιας επιχείρησης, ώστε να μπορεί να προσφέρει καλύτερα προϊόντα και υπηρεσίες στους πελάτες της. Οι εφαρμογές του συνήθως εντάσσονται στη λειτουργία ενός τοπικού δικτύου (Intranet) και μπορούν να είναι: επικοινωνία μεταξύ ομάδων εργασίας, ηλεκτρονική δημοσίευση (άμεση διανομή πληροφοριών) κτλ.

- **3.3.2 Συναλλαγές μεταξύ επιχειρήσεων (Business-to-Business - B2B)**

Το ηλεκτρονικό εμπόριο επιτρέπει σε επιχειρήσεις να βελτιώσουν τη μεταξύ τους συνεργασία, απλοποιώντας τις διαδικασίες και το κόστος των προμηθειών, την ταχύτερη αποστολή των προμηθειών και τον αποτελεσματικότερο έλεγχο του επιπέδου αποθεμάτων. Επιπλέον καθιστά ευκολότερη την αρχειοθέτηση των σχετικών εγγράφων και ποιοτικότερη την εξυπηρέτηση πελατών. Η δυνατότητα ηλεκτρονικής σύνδεσης με προμηθευτές και διανομείς καθώς και η πραγματοποίηση ηλεκτρονικών πληρωμών βελτιώνουν ακόμη περισσότερο την αποτελεσματικότητα: οι ηλεκτρονικές πληρωμές περιορίζουν το ανθρώπινο σφάλμα, αυξάνουν την ταχύτητα και μειώνουν το κόστος των συναλλαγών. Το ηλεκτρονικό εμπόριο προσφέρει τη δυνατότητα αυξημένης πληροφόρησης σχετικά με τα προσφερόμενα προϊόντα - είτε από τους προμηθευτές είτε από ενδιάμεσους οργανισμούς που προσφέρουν υπηρεσίες ηλεκτρονικού εμπορίου.

- **3.3.3 Λιανικές πωλήσεις - Ηλεκτρονικό εμπόριο μεταξύ επιχείρησης και καταναλωτών (Business-to-Consumer - B2C)**

Πρόκειται για την πιο διαδεδομένη μορφή ηλεκτρονικού εμπορίου. Ο καταναλωτής έχει πρόσβαση σε μια τεράστια ποικιλία προϊόντων σε

δικτυακούς κόμβους-καταστήματα, βλέπει, επιλέγει, αν επιθυμεί να αγοράσει είδη ένδυσης μπορεί ενίοτε και να τα δοκιμάζει (μέσω ειδικών προγραμμάτων), ανακαλύπτει προϊόντα τα οποία δεν θα μπορούσε να βρει εύκολα στη χώρα του, συγκρίνει τιμές και τέλος αγοράζει. Κι όλα αυτά χωρίς να βγει από το σπίτι του, κερδίζοντας πολύτιμο χρόνο και κόπο.

- **3.3.4 Καταναλωτής προς καταναλωτή (consumer-to consumer - C2C)**

Η μορφή ηλεκτρονικού εμπορίου από καταναλωτή σε καταναλωτή εμφανίζεται μεταξύ ιδιωτών ή καταναλωτών. Παραδείγματα C2C ηλεκτρονικού εμπορίου είναι τα εξής:

πύλες δημοπρασιών, όπως το eBay, το οποίο επιτρέπει σε πραγματικό χρόνο υποβολή προσφορών για τα είδη που πωλούνται στο διαδίκτυο. Στις περιπτώσεις αυτές ο καταναλωτής είναι αυτός να οδηγεί και κατευθύνει τις συναλλαγές.
συστήματα ομότιμων κόμβων (peer-to-peer) όπου τα αρχεία που περιέχουν διαφορετικό είδος δεδομένων διαμοιράζονται από έναν χρήστη προς άλλους χρήστες.
πύλες διαφήμισης όπου οι χρήστες μπορούν να πωλούν ή να αγοράζουν μεταξύ τους διάφορα προϊόντα.
μικρές αγγελίες σε ιστοσελίδες, ένα διαδραστικό περιβάλλον άμεσα συνδεδεμένων αγορών όπου οι αγοραστές και οι πωλητές μπορούν να διαπραγματεύονται την αγορά και πώληση αγαθών.

- **3.3.5 Επιχείρηση προς κυβέρνηση (business-to-government - B2G)**

Η μορφή ηλεκτρονικού εμπορίου από επιχείρηση σε κυβέρνηση αναφέρεται σε
συναλλαγές μεταξύ των επιχειρήσεων και του δημόσιου τομέα. Στην πράξη αυτό σημαίνει τη χρήση του διαδικτύου για τις διαδικασίες αδειοδότησης, τις δημόσιες συμβάσεις, καθώς και άλλες συναφείς με την κυβέρνηση δραστηριότητες. Στο B2G ο δημόσιος τομέας έχει πρωταγωνιστικό ρόλο και βασίζεται στην ανάγκη του δημόσιου τομέα για ένα πιο αποτελεσματικό σύστημα προμηθειών. Η διαδικτυακή πολιτική αγορών αυξάνει τη διαφάνεια της διαδικασίας ανάθεσης έργων και τη μείωση του κινδύνου παρατυπιών. Σήμερα ωστόσο, το μέγεθος της χρήσης της μορφής B2G επί του συνόλου των ηλεκτρονικών συναλλαγών είναι περιορισμένο

3.4 ΔΥΝΑΤΟΤΗΤΕΣ, ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Δυνατότητες :

- Αναζήτηση προϊόντων ανά κατηγορία ή είδος.
- Καλάθι αγορών.
- Ο συνεργάτης μας έχει τη δυνατότητα να καταχωρεί τα στοιχεία του και με τη χρήση κωδικού και username να βλέπει το αρχείο των παραγγελιών.
- Διαφορετικά είδη συναλλάγματος.
- Υπολογισμός φόρων με βάση διάφορα στοιχεία (βάρος, περιοχή, κ.α.).
- Υπολογισμός εξόδων αποστολής με βάση διάφορα στοιχεία (βάρος, περιοχή, κ.α.).

Πλεονεκτήματα:

- εισαγωγή σε νέες αγορές
- απόκτηση νέων πελατών
- αύξηση παραγωγικότητας
- ασφαλείς συναλλαγές τοις μετρητοίς
- ανταγωνιστικά πλεονεκτήματα

Μειονεκτήματα

- Δεν υπάρχει εμπιστευτικότητα και ασφάλεια όσον αφορά το περιεχόμενο κάποιων πληροφοριών.
- Δεν υπάρχει ακεραιότητα, ώστε να προφυλάσσεται το υποκείμενο των πληροφοριών που διακινούνται.
- Συνεπώς:, το ηλεκτρονικό εμπόριο ελλοχεύει κινδύνους για τον ανυποψίαστο χρήστη.

Αναλυτικότερα πλεονεκτήματα όσων αφορά τον καταναλωτή και την εταιρία:

3.4.1 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για τον καταναλωτή:

- Τα ηλεκτρονικά καταστήματα είναι ανοιχτά 24 ώρες το 24ωρο. Με άλλα λόγια οποιαδήποτε στιγμή το επιθυμείτε, μπορείτε να αγοράσετε π.χ. ένα CD, ένα αεροπορικό εισιτήριο, ή ακόμα και τα μονωτικά υλικά που χρειάζονται για την οικοδομή σας.
- Το κόστος των προϊόντων που πωλούνται μέσω Internet είναι κατά γενικό κανόνα πολύ χαμηλότερο από τις τιμές του εμπορίου, αφού ένα ηλεκτρονικό κατάστημα είναι απαλλαγμένο από μεγάλο μέρος του

λειτουργικού κόστους ενός πραγματικού καταστήματος (ενοικίαση χώρου και «αέρα», ηλεκτρικό, νερό κλπ) και γενικά απαιτεί πολύ λιγότερο υπαλληλικό προσωπικό.

- Η αγορά είναι πραγματικά παγκόσμια. Με άλλα λόγια, μπορείτε μέσω του υπολογιστή σας να αγοράσετε ακόμα και κάτι το οποίο δεν κυκλοφορεί στην Ελλάδα, χωρίς να πρέπει πια να περιμένετε πότε κάποιος φίλος σας θα ταξιδέψει στο εξωτερικό για να σας το φέρει.
- Η συναλλαγή είναι γρήγορη και άμεση. Με άλλα λόγια, από τη στιγμή που ολοκληρώνετε την παραγγελία σας, το αργότερο σε 3-4 ημέρες την έχετε λάβει, ακόμα και αν εκείνη τη στιγμή το προϊόν βρισκόταν στην άλλη άκρη του πλανήτη.
  Αλλά το πιο πρακτικό και πιο σημαντικό όφελος για τον καταναλωτή από το ηλεκτρονικό εμπόριο είναι το ότι:
- Ο καθένας βρίσκει αυτό που θέλει, όποτε το θέλει, χωρίς να κάνει βήμα, χωρίς δηλαδή κόπο και χωρίς καμία σπατάλη χρόνου. Με άλλα λόγια απλά και εύκολα ψώνια από το σπίτι ή το γραφείο!

3.4.2 Πλεονεκτήματα του ηλεκτρονικού εμπορίου για την εταιρία

- Όπως προαναφέραμε, κάθε εταιρία που έχει ηλεκτρονική παρουσία μπορεί να διευρύνει τον κύκλο εργασιών της επεκτείνοντας τα γεωγραφικά όρια των συναλλαγών της. Αυτό σημαίνει πως κάθε επιχείρηση που διαθέτει τα προϊόντα της online μπορεί και αποκτά πελάτες σε περιοχές που βρίσκονται μακριά από την έδρα της, ακόμα και στο εξωτερικό. Με άλλα λόγια, κάθε επιχείρηση που έχει ένα ηλεκτρονικό κατάστημα, είναι σαν να έχει υποκαταστήματα σε πολλές περιοχές και μάλιστα με ελάχιστο λειτουργικό κόστος.
- Κάθε εταιρία που χρησιμοποιεί τις νέες τεχνολογίες- όπως το Internet- γίνεται εξ ορισμού πιο ανταγωνιστική, αφού μπορεί να ενημερώνεται πιο εύκολα για τις τρέχουσες εξελίξεις στο χώρο της. Με άλλα λόγια και με δεδομένο το ότι σε λίγα χρόνια όλες οι εμπορικές δραστηριότητες θα γίνονται μέσω Internet, το ηλεκτρονικό εμπόριο είναι η νέα μεγάλη πρόκληση για κάθε εταιρία που θέλει να είναι ανταγωνιστική.
- Οι ηλεκτρονικές συναλλαγές επιτρέπουν την αμφίδρομη σχέση μεταξύ επιχείρησης και καταναλωτή (interaction). Αυτό σημαίνει πως κάθε εταιρία μέσω των ηλεκτρονικών συναλλαγών μπορεί να συλλέξει πολλά στοιχεία για τις συνήθειες, τις ανάγκες και τα γούστα των καταναλωτών και σύμφωνα με αυτά να αναπροσαρμόσει την πολιτική της προς το θετικότερο.
- Τέλος, γνωρίζοντας τις συγκεκριμένες ανάγκες των πελατών τους, οι εταιρίες μπορούν να προχωρήσουν στη δημιουργία συγκεκριμένων προϊόντων είτε ανταποκρινόμενων σε έναν καταναλωτή, είτε σε μια ομάδα καταναλωτών που χρειάζονται ένα νέο προϊόν το οποίο δεν υπάρχει ακόμα στην αγορά.

3.5 ΠΟΣΟ ΠΡΟΣΟΔΟΦΟΡΟ ΕΙΝΑΙ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ?

Αρκετές εταιρείες που δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου δεν παρουσιάζουν ικανοποιητικά κέρδη. Ορισμένες, μάλιστα, έρευνες κάνουν λόγο για το ένα τρίτο των on-line εμπόρων. Από την άλλη πλευρά όμως, οι μελέτες δείχνουν ότι οι περισσότεροι χρήστες του Internet ενημερώνονται για ένα προϊόν on-line και στη συνέχεια το αγοράζουν από αλλού. Έτσι, ακόμη κι αν ένα δικτυακό κατάστημα δεν σημειώνει αρκετές πωλήσεις, μπορεί να συνεισφέρει σημαντικά στην αύξηση των αγορών μέσα από άλλα κανάλια. Όσον αφορά τις εταιρείες που εστιάζουν στην ανάπτυξη επιχειρηματικών σχέσεων με άλλες εταιρείες μέσα από το ηλεκτρονικό εμπόριο, στόχος τους δεν είναι τόσο η άντληση οικονομικού κέρδους, όσο η περικοπή των εξόδων και η βελτίωση των υπηρεσιών προς τους πελάτες.

3.6 Βασικά οφέλη της διαδικτυακής δραστηριοποίησης για τις επιχειρήσεις:

• **Ευρεία γεωγραφική κάλυψη:** οι επιχειρήσεις έχουν τη δυνατότητα να απευθυνθούν σε πελάτες που βρίσκονται παντού, χωρίς τη σύσταση τοπικού υποκαταστήματος.
• **Ελαχιστοποίηση της προμηθευτικής αλυσίδας:** ο προμηθευτής μπορεί να απευθυνθεί απευθείας στον πελάτη, χωρίς την ανάμειξη «ενδιάμεσων».
• **Μείωση λειτουργικού κόστους:** η μείωση του λειτουργικού κόστους οφείλεται στο γεγονός ότι οι επιχειρήσεις μπορούν να εξυπηρετήσουν τους πελάτες με ελάχιστο κόστος. Επίσης, όσο αυξάνεται ο αριθμός των πελατών ενός ηλεκτρονικού καταστήματος, τόσο μειώνεται το συνολικό κόστος εξυπηρέτησής τους.
• **Συνεχής λειτουργία:** το διαδίκτυο είναι ίσως τα μοναδικό κανάλι εξυπηρέτησης πελατών που επιτρέπει την πραγματοποίηση αγορών οποιαδήποτε στιγμή το 24ωρο.
• **Εργαλείο μάρκετιγκ:** οι επιχειρήσεις μπορούν να εκμεταλλευτούν τις δυνατότητες του διαδικτύου για προσφορές, διαχείριση και ενημέρωση πελατών, στατιστικά στοιχεία πρόσβασης και πωλήσεων.
• **Αύξηση των πωλήσεων**
• **Άμεση ικανοποίηση των πελατών**
• **Άμεση ενημέρωση των πελατών** για καινούρια προϊόντα
• **Βελτίωση της επικοινωνίας** με τους πελάτες
• **Βέλτιστη διαχείριση** των προϊόντων και των παραγγελιών

4. ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΛΗΡΩΜΕΣ

Οι ηλεκτρονικές πληρωμές αποτελούν πλέον αναπόσπαστο τμήμα του ηλεκτρονικού εμπορικούς ηλεκτρονική πληρωμή μπορεί να ορίσει μια οικονομική συναλλαγή η οποία λαμβάνει χώρα on-line μεταξύ πωλητών και αγοραστών οι οποίοι βρίσκονται σε μεγάλη ή μικρή απόσταση μεταξύ τους χωρίς να απαιτείται η παρουσία τους. Το περιεχόμενο αυτής της συναλλαγής έχει την μορφή ψηφιακού μέσου το οποίο υποστηρίζεται από κάποιο χρηματοπιστωτικό οργανισμό ή τράπεζα ή άλλο ενδιάμεσο φορέα Η ανάγκη για νέα συστήματα πληρωμών που θα πραγματοποιούνταν γρήγορα και σε πραγματικό χρόνο έγινε επιτακτικη.Για την εκπλήρωση την ανάγκης των ηλεκτρονικών πληρωμών προταθήκαν και εφαρμόστηκαν 3 κυρίως λυσεις.ηλεκτονικη μεταφορά κεφαλαίων χρήση πιστωτικών καρτών και ηλεκτρονικό χρήμα που περικλείονται στο όρο ηλεκτρονική πληρωμή.

Οι ηλεκτρονικές πληρωμές παρουσιάζουν τρία κύρια οφέλη

Ευκολία . Μια ηλεκτρονική πληρωμή δεν απαιτεί την μεταφορά μεγάλου ποσού σε μετρητά και έτσι αποτελεί τον εύκολο τρόπο πληρωμής.

Χαμηλότερο κόστος. Λόγων των αυτοματοποιημένων λειτουργιών οι ηλεκτρονικές πληρωμές έχουν μειώσει το κόστος των συναλλαγών

Αύξηση των συναλλαγών . απλοί καταναλωτές που χρησιμοποιούν τα ηλεκτρονικά συστήματα συναλλαγών και περισσότερο εκείνοι που επιλέγουν τις πιστωτικές κάρτες για τις συναλλαγές τους έχει αποδεδειχθεί ότι πραγματοποιούν περισσότερες συναλλαγές.

Οι μέθοδοι που έχουν αναπτυχθεί για την επίτευξη πληρωμών στο internet κατά κύριο λόγο αποτελούν ηλεκτρονικές εκδοχές των παραδοσιακών συστημάτων πληρωμής δηλαδή μετρητά επιταγές και πιστωτικές κάρτες. Η θεμελιώδης διαφορά μεταξύ των ηλεκτρονικών πληρωμών και των παραδοσιακών είναι ότι στην πρώτη περίπτωση όλα είναι σχεδιασμένα ώστε να είναι ηλεκτρονικά διαχειρισιμα

4.1 ΔΙΑΚΡΙΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Οι ηλεκτρονικές πληρωμές διακρίνονται σε αυτές που στηρίζονται στην μεταφορά αξίας και σε αυτές που στηρίζονται στην μεταφορά πληροφοριών.

Στην πρώτη κατηγορία πραγματοποιείται η μεταφορά χρηματικών πόσων μέσω των συστημάτων των ηλεκτρονικών πληρωμών. Αντίθετα στην δεύτερη κατηγορία αυτό που μεταφέρεται μεταξύ των συναλλασσομένων μερών είναι πληροφορίες αφενός για την συναλλαγή και αφετέρου για τους τραπεζικούς λογαριασμούς των εμπλεκόμενων.

Ένας δεύτερος πιο διαδεδομένος τρόπος ταξινόμησης των ηλεκτρονικών πληρωμών μπορεί να γίνει με βάση την τεχνολογία που χρησιμοποιεί ένα ηλεκτρονικό δίκτυο διανομής. Έτσι οι συναλλαγές μπορούν να πραγματοποιηθούν:

4.1.1 -μέσω τηλέφωνου

Οι πληρωμές μέσω τηλεφωνικού δικτυού αποτελούν μια καινούργια μορφή ηλεκτρονικών πληρωμών. Στόχος είναι η εκμετάλλευση της υπάρχουσας τεχνικής υποδομής αλλά και της σημαντικής διείσδυσης που έχει το τηλέφωνο ως τεχνολογία σε όλα τα κοινωνικά στρωματά. Πολλές επιχειρήσεις, τράπεζες αλλά και οι δημοσιές υπηρεσίες επιτρέπουν την εξόφληση λογαριασμών μέσω τηλέφωνου με αποτέλεσμα αυτά τα συστήματα ηλεκτρονικών πληρωμών να κερδίζουν σημαντικά την εμπιστοσύνη του καταναλωτικού κοινού.

4.1.2 -Μέσω διαδικτύου

Πρόκειται για την πιο σύγχρονη μορφή ηλεκτρονικών πληρωμών. Η άνθηση των ηλεκτρονικού επιχειρεί καθιστά ιδιαίτερα σημαντική την ύπαρξη τέτοιων συστημάτων πληρωμής που χρησιμοποιούν το διαδίκτυο ως κανάλι διανομής. Επιπλέον η πλέον εύκολη πρόβας στο διαδίκτυο καθιστά αυτά τα συστήματα ηλεκτρονικών πληρωμών ιδιαίτερα δημοφιλή.

4.1.3 -Μέσω κινητής τηλεφωνίας

Η ανάπτυξη τεχνολογιών όπως το WAP επιτρέπουν την εκτέλεση βασικών χρηματικών συναλλαγών από κινητές και ασύρματες συσκευές ανεξαρτήτως χώρου και χρόνου. Πρόκειται για ένα μέσο πιο αυτόνομο ενώ η ευρεία αποδοχή και χρήση του από το καταναλωτικό κοινό το καθιστούν ιδιαίτερα δημοφιλή λυση,συχνα ανταγωνιστική των πληρωμών μέσω διαδικτύου.

4.2 ΜΕΘΟΔΟΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

Δημοφιλέστερη μέθοδος πληρωμής για κυβερνοαγορες είναι είναι η πιστωτική κάρτα ενώ άλλες είναι οι ηλεκτρονικές επιταγές και το ψηφιακό χρήμα κ.α.

4.2.1 ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ

Οι πιστωτικές κάρτες αποτελούν την πλέον επικρατέστερη μέθοδο ηλεκτρονικής πληρωμής και πολλοί καταναλωτές αντιμετωπίζουν με αρκετή καχυποψία αυτού του είδους τις συναλλαγές. Στην σημερινή εποχη,στις on-line ψηφιακές συναλλαγές ο έλεγχος και η χρέωση της πιστωτικής πραγματοποιείται από τη στιγμή που οι καταναλωτές κάνουν την αιτηση.Μια επιχείρηση μπορεί να προμηθευτεί ένα σύστημα on-line συναλλαγών μέσω πιστωτικών καρτών.Πολλες είναι οι τράπεζες και οι εταιρείες που παρέχουν τέτοιες υπηρεσίες ενώ ο καταναλωτής αρκεί να συμπληρώσει τα προσωπικά του στοιχειά και τα στοιχειά της πιστωτικής του κάρτας στην ειδική φόρμα συναλλαγών και να περιμένει ένα μικρό διάστημα για την έγκριση της συναλλαγής του.

Οι οντότητες συμμετοχής στα ηλεκτρονικά συστήματα πληρωμής με πιστωτικές κάρτες είναι.

- Ο κάτοχος της κάρτας .Ο κάτοχος της πιστωτικής κάρτας μπορεί να είναι ένας καταναλωτής μια επιχείρηση ή ένας οργανισμός.
- Ο έμπορος . Ο έμπορος μπορεί να είναι οποιαδήποτε επιχείρηση διαθέτει προς πώληση τα προϊόντα της και τις υπηρεσίες της .
- Η τράπεζα έμπορος . Είναι ένας οικονομικός οργανισμός (συνήθως τράπεζα)που καθορίζει ένα λογαριασμό για τις επιχειρήσεις.

- Η τράπεζα που εκδίδει την κάρτα. Είναι ένας οικονομικός οργανισμός που καθορίζει έναν λογαριασμό για τους κατόχους πιστωτικών καρτών και εκδίδει την κάρτα.

4.2.2ΗΛΕΚΤΡΟΝΙΚΟ Η ΨΗΦΙΑΚΟ ΧΡΗΜΑ

Το ηλεκτρονικό χρήμα είναι ένα νεότερο και πιο σύγχρονο μέσο πληρωμής στο διαδίκτυο. Βασίζεται στην ανταλλαγή πραγματικού χρήματος σε μια τράπεζα με ηλεκτρονικό τρόπο. Ο καταναλωτής μετατρέπει ένα χρηματικό ποσό από τον λογαριασμό σε ψηφιακό χρήμα. Τα ο ψηφιακό χρήμα αποθηκεύεται ηλεκτρονικά και είναι διαθέσιμο για συναλλαγές μέσω διαδικτύου. Όταν κάποιος χρήστης κάνει κάποια αγορά μεταφέρει το απαιτούμενο ποσό στην επιχείρηση και η επιχείρηση με την σειρά της επικοινωνεί με την τράπεζα για την έγκριση της συναλλαγής.

Τα χαρακτηριστικά που πρέπει να έχει το ηλεκτρονικό χρήμα είναι τα εξής.

1. Ικανοποιητικό σύστημα ασφάλειας όπως τα υπόλοιπα συστήματα πληρωμών.
2. Ανωνυμία
3. Μεταφερσιμότητα (από χρηματικό ποσό σε ψηφιακό χρήμα και αντίστροφα)
4. Απεριόριστη διάρκεια
5. Αμφίδρομη κινητικότητα (κάθε κάτοχος με την ίδια ευκολία να μπορεί να πάρει και να δώσει
6. Διαιρετότητα (να μπορεί να διαιρεθεί σε όσα τμήματα ίσης συνολικής αξίας θέλει ο κάτοχος .
7. Ευρεία αποδοχή
8. Ευχρηστία
9. Σταθερή αξία

4.2.3 ΈΞΥΠΝΕΣ ΚΑΡΤΕΣ (SMART CARDS)

Η έξυπνη κάρτα είναι μια μικρή πλαστική κάρτα που περιέχει ένα τσιπ υπολογιστή. Οι έξυπνες κάρτες χρησιμοποιούνται μαζί με προσωπικούς αναγνωριστικούς αριθμούς (PIN) για σύνδεση σε ένα δίκτυο, έναν υπολογιστή ή μια συσκευή. Η χρήση έξυπνης κάρτας αυξάνει την ασφάλεια κατά ένα επίπεδο σε σύγκριση με τον κωδικό πρόσβασης, καθώς είναι δυσκολότερο για κάποιον να κλέψει μια έξυπνη κάρτα και να μάθει το PIN σας απ΄ότι να μάθει τον κωδικό πρόσβασής σας.

Οι έξυπνες κάρτες εκδίδονται συνήθως από τα τμήματα τεχνολογίας πληροφορικής (IT) μεγάλων οργανισμών. Για να χρησιμοποιήσετε μια έξυπνη κάρτα, θα χρειαστείτε επίσης μια συσκευή ανάγνωσης έξυπνων καρτών—είναι μια συσκευή που εγκαθίσταται ή συνδέεται στον υπολογιστή σας και μπορεί να διαβάζει τις πληροφορίες που είναι αποθηκευμένες στην έξυπνη κάρτα.

Η ιδέα της έξυπνης κάρτας ξεκίνησε στη Γαλλία το 1974. Το 1975 τα δικαιώματα ανάπτυξης πέρασαν σε μεγάλες εταιρίες ηλεκτρονικού εξοπλισμού. Η νέα αυτή τεχνολογία παρουσιάστηκε στο κοινό το 1981. Μια σειρά από πιλοτικά σχέδια ξεκίνησε αμέσως, και το 1984 με μια συλλογική αξιολόγησή τους εκδόθηκαν νέες ολοκληρωμένες προδιαγραφές.

Σήμερα επικρατεί η λανθασμένη εντύπωση ότι οι Smart Cards είναι τραπεζικές ή πιστωτικές κάρτες, με αποτέλεσμα να μην αναγνωρίζεται το μεγάλο εύρος των δυνατοτήτων τους. Η τεχνολογία των έξυπνων καρτών προσφέρει απεριόριστες δυνατότητες χρήσης στη βιομηχανία, το εμπόριο και τη δημόσια διοίκηση.

4.2.4ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΤΑΓΕΣ

Πρόκειται για μια εντολή μεταφοράς χρημάτων αντίστοιχη των παραδοσιακών επιταγών. Μια παραδοσιακή επιταγή αποτελείται από μια εντολή προς την τράπεζα του καταναλωτή να μεταφέρει κάποιο ποσό στην επιχείρηση. Με το ίδιο τρόπο ο αγοραστής αποστέλλει μια ηλεκτρονική επιταγή σε ένα άλλο πρόσωπο ή μια εταιρία. Αυτός με την σειρά του εμφανίζει την επιταγή στην τράπεζα για να εισπράξει το ποσό, και η επιταγή επιστρέφει στον πρώτο ως απόδειξη εξόφλησης. Οι ηλεκτρονικές επιταγές μπορούν να αποσταλούν είτε με απευθείας μετάδοση πάνω στο δίκτυο είτε μέσω ηλεκτρονικού ταχυδρομείου. Ακόμα μπορούν να προσφέρουν μεγαλύτερη ασφάλεια στον αποστολέα ο όποιος μπορεί να προστατέψει τον εαυτό του με την κωδικοποίηση είτε με την απόκρυψη του αριθμού λογαριασμού του χρησιμοποιώντας το δημόσιο κλειδί της τράπεζας.

4.2.5 ΗΛΕΚΤΡΟΝΙΚΗ ΜΕΤΑΦΟΡΑ ΚΕΦΑΛΑΙΩΝ

Πρόκειται για την μεταφορά κάποιων πόσων από ένα λογαριασμό σε ένα δεύτερο λογαριασμό στην ίδια ή σε διαφορετική τράπεζα. Αυτή η μεταφορά μπορεί να γίνει πλέον και μέσω διαδικτύου. Με αυτόν τον τρόπο οι χρηστές μπορούν να πληρώσουν και αντί να πάνε στην τράπεζα να καταθέσουν το χρηματικό ποσό στον λογαριασμό που θα τους δοθεί από την εκάστου επιχείρηση μπορούν να μεταφέρουν το ποσό αυτό στον διαδικτυακό τόπο της τράπεζας.

4.2.6 ΧΡΕΩΣΤΙΚΕΣ ΚΑΡΤΕΣ

Οι χρεωστικές κάρτες είναι επίσης ένας τρόπος ηλεκτρονικής πληρωμής, είναι παρόμοιες με τις πιστωτικές κάρτες με την βασική διαφορά ότι το ποσό της συναλλαγής μεταφέρεται αυτόματα από τον λογαριασμού του κάτοχου στον λογαριασμό του εμπόρου και δεν πιστώνεται στον λογαριασμό του χρηστή όπως στην πιστωτική κάρτα. Αν δεν ύπαρχε δηλαδή διαθέσιμο ποσό στον λογαριασμό με το όποιο είναι συνδεδεμένη η χρεωστική κάρτα η συναλλαγή δεν θα πραγματοποιηθεί. Χρεωστικές κάρτες είναι αυτές που χρησιμοποιούμε όλοι μας από κάποιο ATM. Οι κάρτες αυτές εξασφαλίζουν μεγαλύτερη ασφάλεια και στις συναλλαγές μέσω internet καθώς μπορούμε να δημιουργήσουμε έναν ξεχωριστό λογαριασμό με ποσό που θα ελέγχουμε για χρήση αποκλειστικά με την συγκεκριμένη κάρτα.

4.2.7 ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟ EDI

Το EDI αναφέρεται στην ηλεκτρονική ανταλλαγή εμπορικών δεδομένων (παραστατικά) μεταξύ επιχειρήσεων.

Η χρηματοοικονομική ανταλλαγή δεδομένων αποτελεί μια εξειδικευμένη μορφή EDI στις περιπτώσεις οπού ο ένας από τους δυο συναλλασσομένους είναι τράπεζα ή άλλο χρηματοπιστωτικό ίδρυμα. Εφαρμογές αυτής της τεχνολογία έχουν ήδη αναπτυχτεί για διεξαγωγή τραπεζικών συναλλαγών από το σπίτι (home banking) καθώς και για την πληρωμή εμπορικών συναλλαγών (οπού πελάτης και προμηθευτής δίνουν αντίστοιχες οδηγίες στις τράπεζες για την διευθέτηση των λογαριασμών).

Αν και το e-banking δεν αποτελεί μέθοδο ηλεκτρονικής πληρωμής ωστόσο είναι ένας τρόπος διεκπεραίωσης τους έτσι το κατατάσσουμε στις ηλεκτρονικές πληρωμές.

4.3 E -BANKING[4]

Όσο η τεχνολογία εξελίσσεται και η εξοικείωση των ανθρώπων με το διαδίκτυο μεγαλώνει, τόσες περισσότερες υπηρεσίες παροχής υπηρεσιών εμφανίζονται σε αυτό. Μια τέτοια υπηρεσία είναι και το online banking (ή Internet banking), Τι είναι το “e” στο e-banking; Προέρχεται από την αγγλική λέξη electronic, στα ελληνικά ηλεκτρονικό.
Πρόκειται για τον αντικαταστάτη της γνωστής σε όλους μας τράπεζα. Της τράπεζας, με τις πολύωρες ουρές στα ταμεία, το άγχος να τελειώσεις γρήγορα για να προλάβεις να πας και σε άλλη τράπεζα να μεταφέρεις χρήματα σε λογαριασμός σε μια τρίτη τράπεζα. Με το e-banking όλα αυτά είναι παρελθόν αρκεί να έχεις στην κατοχή σου έναν ηλεκτρονικό υπολογιστή ή ένα κινητό τηλέφωνο. Δίνει την δυνατότητα στους χρήστες της να διεκπεραιώνουν ένα μεγάλο μέρος των συναλλαγών τους με μια τράπεζα εύκολα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες τον χρόνο. Το online banking προσφέρει μια τεράστια γκάμα υπηρεσιών που παλαιότερα απαιτούσαν την παρουσία του πελάτη στην τράπεζα, ενώ τώρα μπορούν να πραγματοποιηθούν από τον προσωπικό του υπολογιστή όποια ώρα αυτός θελήσει. Ενδεικτικά παραθέτω μερικές από αυτές παρακάτω :

• Πληροφορίες υπολοίπων για τους τηρούμενους λογαριασμούς.
• Μεταφορές ποσών μεταξύ των τηρούμενων λογαριασμών του ιδίου νομίσματος.
• Πληροφορίες σχετικά με τις πρόσφατες κινήσεις των τηρούμενων λογαριασμών.

[4] Αγγελής Γ. Βασίλειος, η βίβλος του e-banking,2005,εκδόσεις νέων τεχνολογιών

• Δυνατότητα έκδοσης και αποστολής παλαιότερων κινήσεων των τηρούμενων λογαριασμών
• Δυνατότητα υποβολής αίτησης για ανάκληση επιταγών ή ολόκληρου του μπλοκεπιταγών.
•Εντολές αγοραπωλησίας μετοχών.
• Ενημέρωση για την κίνηση των προσωπικών αμοιβαίων κεφαλαίων.
•Δυνατότητα υποβολής αιτήσεων εμβασμάτων.
•Αλλαγή του απορρήτου κωδικού PIN.
•Προσωπικάμηνύματα.

Οι μεγάλοι όμιλοι τραπεζών βλέποντας την επιτυχία που είχε στους πελάτες τους το online banking έκαναν ακόμα ένα βήμα μπροστά στην εξυπηρέτηση τους, δημιουργώντας το mobile banking. Η συγκεκριμένη υπηρεσία πρόκειται για μια εφαρμογή κινητού τηλεφώνου (κυρίως «έξυπνων κινητών») η οποία προσφέρει στον πελάτη ακριβώς ανάλογες υπηρεσίες με το online banking.Μέσω αυτής της εφαρμογής οι πελάτες μπορούν να διεκπεραιώσουν σχεδόν όλες τους τις τραπεζικές συναλλαγές από το κινητό τους τηλέφωνο κερδίζοντας πολύτιμο χρόνο.

Αν και το ηλεκτρονικό έγκλημα δεν αποτελεί καινούργιο φαινόμενο, εντούτοις οι επιθέσεις παρουσιάζουν αύξηση τα τελευταία χρόνια λόγω της ευρύτερης και πιο διαδεδομένης χρήσης του e-banking.Το νέο αυτό σύστημα προσφέρει στους πελάτες των τραπεζών την δυνατότητα διεκπεραίωσης συναλλαγών, την παρακολούθηση της πορείας χαρτοφυλακίων, την εξόφληση λογαριασμών και πολλές άλλες υπηρεσίες. Με άλλα λόγια "μεταφέρει" την τράπεζα στην οθόνη του υπολογιστή μας .Όμως η ραγδαία ανάπτυξη και άμεση ανταπόκριση των ανθρώπων στις παροχές του νέου αυτού συστήματος επιτρέπουν στους λεγόμενους "hacker" να "εισβάλλουν" στους λογαριασμούς των πελατών, υποκλέπτοντας προσωπικά δεδομένα και στις περισσότερες περιπτώσεις μετακινώντας μεγάλα χρηματικά ποσά Οι επίδοξοι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους,οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό ασφαλείας. Στην προσπάθεια τους να αποφύγουν όσο το δυνατόν περισσότερα περιστατικά κλοπής, οι υπεύθυνοι των τραπεζικών καταστημάτων κρίνουν απαραίτητη την εφαρμογή ορισμένων μέτρων γ α το σκ ποό αυτό. Προτείνουν τη προστασία του κ ωδικ ό πρόσβασής μας στην υπηρεσία e-banking και φυσικά τη προστασία του υπολογιστή μας από ¨κακόβουλο ¨λογισμικό. Με τον τρόπο αυτό θα μπορούμε να ολοκληρώνουμε τις συναλλαγές μας με τις τράπεζες γρήγορα και με ασφάλεια

4.3.1ΤΑ ΕΙΔΗ ΤΟΥ Ε- BANKING

Το e-banking, κατά βάση χωρίζεται σε τρία είδη, ανάλογα με τον εξοπλισμό και τα
προγράμματα λογισμικού που χρησιμοποιούνται. Τα είδη αυτά είναι2:
1. Internet banking (Τραπεζική μέσω διαδικτύου)
2. Phone banking (Τραπεζική μέσω τηλεφώνου)
3. Mobile banking (Τραπεζική μέσω κινητού)
Ανάλογα με το κανάλι που χρησιμοποιείται για τη διενέργεια συναλλαγών, εντοπίζοντας ιδιαίτερα χαρακτηριστικά για το κάθε ένα από αυτά.

4.3.1 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.

4.3.2 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 και

- αυτές που διεκπεραιώνονται αυτόματα μέσω συστημάτων αναγνώρισης φωνής

(IVR)

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.

*4.3.3 **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.

4.4 ΤΑ ΠΡΟΙΟΝΤΑ ΚΑΙ ΟΙ ΥΠΗΡΕΣΙΕΣ ΠΟΥ ΠΡΟΣΦΕΡΟΝΤΑΙ

Τα προϊόντα και οι υπηρεσίες που προσφέρονται μέσω της ηλεκτρονικής τραπεζικής αυξάνονται συνεχώς σε ποικιλία και ευελιξία. Στόχος όλων των τραπεζών που έχουν επενδύσει στο web banking είναι να αποκτήσουν ένα σημαντικό ανταγωνιστικό πλεονέκτημα, προσφέροντας μακροχρόνια το σύνολο των προϊόντων και υπηρεσιών τους μέσω διαδικτύου, παρέχοντας τη μέγιστη δυνατή ευκολία διαφάνεια και ασφάλεια στο πελάτη- χρήστη.

Παράλληλα, ο παράγοντας που θα επηρεάσει ίσως στο μεγαλύτερο βαθμό την αφοσίωση των πελατών σε αυτές τις υπηρεσίες είναι η διαθεσιμότητα πληροφοριών και η ευκολία πρόσβασης σε ανταγωνιστικές υπηρεσίες άλλων παροχέων χρηματοοικονομικών υπηρεσιών, χωρίς τους περιορισμούς που θέτει η φυσική τοπογραφία. Αυτή η εξέλιξη δίνει αναμφίβολα την ευκαιρία στους πελάτες να επιλέγουν από που θα προμηθευτούν το κάθε τραπεζικό προϊόν που πρόκειται να χρησιμοποιήσουν, συγκρίνοντας διαφορετικές προσφορές. Περιορίζονται έτσι οι δεσμοί των πελατών με την κάθε τράπεζα και εντείνεται ο ανταγωνισμός μεταξύ των τραπεζών.

Οι τράπεζες δεν μπορούν, με κανένα τρόπο πια, να εφησυχάζουν και να θεωρούν δεδομένο ότι οι πελάτες θα διατηρήσουν το βασικό τραπεζικό τους λογαριασμό στην τράπεζα που συνεργάζονταν μέχρι τώρα. Οι συναλλαγές που οι πελάτες θα δοκιμάσουν να εμπιστευτούν σε άλλες τράπεζες δεν θα είναι λίγες και μπορεί ακόμη να συμπεριλαμβάνουν και το βασικό τους λογαριασμό. Το ενδιαφέρον που δείχνουν οι πελάτες στις υπηρεσίες Internet banking είναι αυξημένο. Ταυτόχρονα οι πελάτες δίνουν έμφαση στα θέματα της ασφάλειας, της προστασίας των ατομικών τους δεδομένων κ α στο να είναι οι προσφερόμενες υπηρεσίες σε πραγματικό χρόνο (real time).
Το internet banking απευθύνεται τόσο στους ιδιώτες πελάτες των τραπεζών, όσο και στις επιχειρήσεις. Οι δυνατότητές του καλύπτου όλο το φάσμα των τραπεζικών υπηρεσιών και εναπόκειται στην κρίση κάθε τράπεζας ποιες από αυτές θα διαθέσει στους πελάτες της μέσα από αυτό το κανάλι

4.4.1 Μεταφορές κεφαλαίων: Οι μεταφορές κεφαλαίων αφορούν την μεταφορά χρημάτων του χρήστη από τον υπολογιστή του και διακρίνονται σε…:
- Μεταφορές κεφαλαίων εντός τράπεζας σε λογαριασμούς του ιδίου, όπου ο χρήστης έχει τη δυνατότητα να μεταφέρει χρήματα από έναν λογαριασμό του σε κάποιον άλλον, σε on-line χρόνο ή να επιλέξει την ημερομηνία που επιθυμεί να πραγματοποιηθεί η συναλλαγή.
- Μεταφορές κεφαλαίων εντός τράπεζας σε λογαριασμούς τρίτων: Σε αυτή την περίπτωση ο χρήστης επιλέγει το λογαριασμό από τον οποίο επιθυμεί να μεταφέρει χρήματα σε on-line χρόνο ή να επιλέξει την ημερομηνία που επιθυμεί να πραγματοποιηθεί η συναλλαγή και στη συνέχεια πληκτρολογεί το λογαριασμό και το ό-
Η εμπιστοσύνη των συναλλασσόμενων στο e-bankingνομα του δικαιούχου στον οποίον θέλει να μεταφέρει χρήματα. Οι τράπεζες έχουν προβλέψει και σε περίπτωση λάθος πληκτρολόγησης λογαριασμού είναι αδύνατη η μεταφορά
- Μεταφορές κεφαλαίων εκτός τράπεζας-εμβάσματα: Ο χρήστης, ο οποίος επιθυμεί τη
μεταφορά κεφαλαίου εκτός της τράπεζας, θα πρέπει να γνωρίζει και τον αριθμό IBAN του δικαιούχου καθώς και το SWIFT της τράπεζας που στέλνει τα χρήματα. Ειδικά αν πρόκειται για μεταφορά εκτός Ελλάδας θα πρέπει να αναφέρεται και η χώρα αποστολής.
Όπως και στην προηγούμενη περίπτωση, έτσι και εδώ ο χρήστης πρέπει να είναι ιδιαίτερα προσεκτικός στην πληκτρολόγηση των λογαριασμών. Στο σημείο αυτό θα πρέπει να αναφέρουμε ότι η αποστολή εμβάσματος πάνω από ορισμένο ποσό είναι αδύνατη και υπόκεινται στη νομοθεσία για το ξέπλυμα χρήματος.

4.4.2 Πληρωμές*:* Οι πληρωμές αναφέρονται στην εξόφληση των μηνιαίων δόσεων
του χρήστη οι οποίες αφορούν:
- Πληρωμές πιστωτικών καρτών Οι πληρωμές πιστωτικών καρτών διακρίνονται σε τρεις κατηγορίες:
Α. *Πληρωμή πιστωτικών καρτών ιδίου:* Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και τον αριθμό της πιστωτικής κάρτας που επιθυμεί να πληρώσει. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Ο χρήστης έχει την πολυτέλεια και μεταχρονολογημένων

πληρωμών, γεγονός που τον διευκολύνει να προγραμματίζει τις πληρωμές του

Β. *Πληρωμή πιστωτικών καρτών τρίτου:* Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης, στη συνέχεια καλείται να πληκτρολογήσει τον αριθμό της πιστωτικής κάρτας. Ο χρήστης πρέπει να είναι ιδιαίτερα προσεκτικός στο σημείο αυτό, ώστε τα λάφτά να πιστωθούν στη σωστή πιστωτική κάρτα. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή

Γ. *Πληρωμή πιστωτικών καρτών άλλης τράπεζας:* Οι πληρωμές πιστωτικών καρτών άλλης τράπεζας διεκπεραιώνεται μέσω του διατραπεζικού συστήματος

Dias transfer. Για την πληρωμή πιστωτικών καρτών άλλης τράπεζας, ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης στη συνέχεια επιλέγει την τράπεζα δικαιούχου, από ένα σύνθετο πεδίο που περιέχει όλες τις τράπεζες εσωτερικού. Έπειτα ο πελάτης καλείται να πληκτρολογήσει τον αριθμό της πιστωτικής κάρτας. Ακολούθως πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή

- *Πληρωμές δημοσίου*: Πολλές πληρωμές ενός πελάτη έναντι του δημοσίου, μπορούν να ολοκληρώνονται μέσω e-banking. Οι περισσότερες εξ αυτών διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIAS DEBIT. Οι πληρωμές δημοσίου παρέχουν όλο το πακέτο των ηλεκτρονικών πληρωμών, καθιστώντας το πολύ ελκυστικό για πολλούς επαγγελματίες της χώρας μας

-Οι πληρωμές δημοσίου, αναφέρονται σε πληρωμές :

- Φ.Π.Α
- Εργοδοτικές εισφορές Ι.Κ.Α
- Ασφαλιστικές εισφορές Τ.Ε.Β.Ε
- Είσπραξη Φόρου Εισοδήματος Φυσικών Προσώπων
- Τέλη κυκλοφορίας

- Πληρωμές Λογαριασμών ΔΕΚΟ

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

οι πληρωμές αυτές είναι:

- ΟΤΕ
- ΔΕΗ
- ΔΕΥΑΠ

- Πληρωμές σταθερής και κινητής τηλεφωνίας: Η πληρωμή λογαριασμών σταθερής

και κινητής τηλεφωνίας παρέχεται πλέον στις περισσότερες τράπεζες. Κάποιες από αυτές τις πληρωμές διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIAS DEBIT, ενώ άλλες αποτελούν προϊόν διμερούς συμφωνίας μεταξύ τραπεζών και εταιριών

- *Πληρωμές Ασφαλιστικών*: Αρκετές ασφαλιστικές εταιρίες συνάπτουν συμφωνίες με τράπεζες, δίνοντας τη δυνατότητα στους πελάτες τους να πληρώνουν τα ασφάλιστρα τους μέσω αυτών*. Εκτέλεση εντολών:*

- Εκτέλεση μισθοδοσίας, υπηρεσία η οποία προσφέρεται αποκλειστικά σε επαγγελματίες πελάτες. Με την εφαρμογή αυτή παρέχεται στο χρήστη η δυνατότητα μαζικής μεταφοράς κεφαλαίων που αφορούν την πληρωμή των υπαλλήλων της επιχείρησης του, - Χρηματιστηριακές εντολές, με τις οποίες ο

χρήστης μπορεί άμεσα να δώσει μία εντολή που αφορά αγορά ή πώληση μετοχών στην τιμή που επιθυμεί, υποδεικνύοντας το λογαριασμό χρέωσης ή πίστωσης, την τιμή για την οποία επιθυμεί να πραγματοποιηθεί η συναλλαγή και τα τεμάχια διαπραγμάτευσης. Σε τέτοιες εντολές εμφανίζονται και τα έξοδα-προμήθειες που επιβαρύνουν τον πελάτη.

Αιτήσεις: Μέσω της ιστοσελίδας τους οι τράπεζες παρέχουν και τη δυνατότητα στο χρήστη για ηλεκτρονικές αιτήσεις για απόκτηση των προϊόντων τους. Μετά την αίτηση ακολουθεί και η αποδοχή των όρων συναλλαγής. Μερικά είδη αιτήσεων είναι:

- Αίτηση ανοίγματος λογαριασμού
- Αίτηση χορήγησης δανείου
- Αίτηση έκδοσης πιστωτικής κάρτας
- Αίτηση χορήγησης καρνέ επιταγών

Βοηθητικές Υπηρεσίες: Πολλές τράπεζες πέραν των υπηρεσιών που προσφέρουν στους χρήστες τους, παρέχουν και βοηθητικά εργαλεία που διευκολύνουν τη ζωή των πελατών τους. Συνήθως τα εργαλεία αυτά είναι διαθέσιμα και στους απλούς επισκέπτες του site της τράπεζας. Τέτοιες βοηθητικές υπηρεσίες είναι :

- Υπολογισμός IBAN
- Μετατροπή νομισμάτων
- Υπολογισμός δόσεων δανείων.

5. ΑΝΑΛΥΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

5.1 ΕΧΘΡΟΙ

1. Ποιος ή ποιοι είναι οι εχθροί μας;
2. Τι σκοπεύουν – Ποιοι είναι οι σκοποί τους – τι ακριβώς επιδιώκουν;
3. Τι μέσα διαθέτουν;

Πιθανοί εχθροί

- Crackers
- Οι Ερευνητές
- Criminals
- Οι ανταγωνιστές
- Οι εισβολείς
- Οποιοσδήποτε έχει φυσική πρόσβαση στα συστήματα

.

Είναι σημαντικό στην προσπάθεια παροχής ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου, να αναγνωρίζονται αρχικά «εχθροί». Οποιοσδήποτε εμπλέκεται με ζητήματα ασφάλειας ηλεκτρονικού εμπορίου θα πρέπει να τον απασχολούν οι εχθροί του συστήματος, οι προθέσεις τους καθώς και τα μέσα που
διαθέτουν. Οι «εχθροί» κατηγοριοποιούνται ως εξής:

☐**5.1.1 Crackers**: Οι crackers αρέσκονται στο δημιουργούν προβλήματα για πλάκα, για βανδαλισμούς ή για επίδειξη. Χρησιμοποιούν συνήθως υπάρχοντα προϊόντα επίθεσης από το διαδίκτυο. Οι προθέσεις τους συχνά δεν είναι εχθρικές, αλλά ωστόσο προκαλούν ουσιαστικές ζημιές, είτε προκαλώντας βανδαλισμούς, είτε διακόπτοντας λειτουργίες.

☐**5.1.2 Ερευνητές** (Researchers): Ένας ερευνητής μπορεί να εργαστεί πολύ σκληρά στην προσπάθεια του να ανακαλύψει αδυναμίες σε πρωτόκολλα ασφάλειας και στη συνέχεια εκδίδει τα αποτελέσματα του στο διαδίκτυο.

☐ **5.1.3 Εγκληματίες** (Criminals): Το διαδίκτυο έχει γίνει πολύ ελκυστικό μέρος για εγκλήματα, λόγω της μεγάλης διάδοσης και ανωνυμίας που παρέχει. Το δικτυακά εγκλήματα εκτείνονται από απλές απάτες με κλοπή αριθμών πιστωτικών καρτών έως προσεκτικές επιθέσεις για πρόσβαση σε χρήμα ή πληροφορίες. Πρόθεση τους είναι το οικονομικό όφελος.

☐ **5.1.4 Ανταγωνιστές** (Competitors): Ένας ανταγωνιστής δεν κλέβει χρήματα, ούτε καταστρέφει αρχεία, αλλά έχει ως στόχο την πρόσβαση στα διάφορα επιχειρηματικά σχέδια, που είναι πολύτιμα για αυτόν.

5.1.5 Εσωτερικοί εχθροί: Δυσαρεστημένοι ή άπληστοι υπάλληλοι μπορούν να αποτελέσουν την πιο σοβαρή απειλή για την ασφάλεια των συστημάτων του οργανισμού. Οι «εσωτερικοί εχθροί» εξ ορισμού έχουν πρόσβαση σε ευαίσθητα συστήματα και πληροφορίες.

5.2 ΑΠΕΙΛΕΣ

- Διακοπή της λειτουργίας ενός υπολογιστικού συστήματος και πρόκληση προβλημάτων στη λειτουργία του
- Κλοπή- Υποκλοπή – Απάτη
- Ιδιοποίηση – Σφετερισμός – Κατάχρηση
- Μολυσμένα Δεδομένα
- Κλοπή Αρχείων
- Αλλοίωση Δεδομένων ή Περιεχομένου
- Μεταμφίεση

Απειλή είναι οποιοδήποτε πιθανό περιστατικό, κακόβουλο ή όχι, που μπορεί να βλάψει κάποιο αγαθό. Με άλλα λόγια, απειλή είναι οτιδήποτε κακό μπορεί να συμβεί στα αγαθά.
Ευπάθεια είναι μια αδυναμία που κάνει δυνατή την απειλή. Αυτό μπορεί να γίνει λόγω αδυναμιών στη σχεδίαση, λάθη στη διαμόρφωση ή λόγω ακατάλληλων και επισφαλών τεχνικών κωδικοποίησης. Επίθεση είναι μια ενέργεια που εκμεταλλεύεται τις ευπάθειες και υλοποιεί μια απειλή. Προκειμένου να σχεδιαστεί και να αναπτυχθεί μια ασφαλής web εφαρμογή, απαιτείται η γνώση τόσο των απειλών όσο και των εχθρών του συστήματος. Είναι
σημαντικό να αναλυθεί η αρχιτεκτονική της εφαρμογής και να καθοριστούν οι πιθανές ευπαθείς περιοχές που μπορούν να επιτρέψουν σε ένα χρήστη ή σε έναν επιτιθέμενο με κακόβουλες προθέσεις, να παραβιάσει την ασφάλεια του συστήματος.
Παρακάτω ακολουθούν αναλυτικά οι κατηγορίες των εχθρών, παρουσιάζονται οι πιο συνήθεις απειλές καθώς και οι τεχνικές επιθέσεων που κάνουν πραγματικότητα αυτές τις απειλές.

Η πραγματοποίηση οποιασδήποτε από τις παραπάνω θεμελιώδεις απειλές, μπορεί να γίνει με μια από τις παρακάτω τεχνικές επίθεσης:

5.2.1 Denial of service attacks: Μια από τις πλέον διάσημες κ α αποτελεσματικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι με στόχο τη διακοπή παροχής υπηρεσιών από ένα δικτυακό κόμβο ή πληροφοριακό σύστημα είναι οι επιθέσεις τύπου Denial of service. Τα προγράμματα που συνήθως χρησιμοποιούν οι επιτιθέμενοι ακολουθούν την τακτική μαζικής αποστολής μηνυμάτων-αιτημάτων στο στόχο ώστε να προκαλέσουν την αποτυχία ανταπόκρισης του και την κατάρρευση του συστήματος.
5.2.2 Επιθέσεις μεταμφίεσης (Spoofing): Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» σε κάποιο νόμιμο χρήστη, ώστε να αποκτήσει πρόσβαση σε μια εφαρμογή. Δηλαδή ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι
αποτέλεσμα των εξής: **α)** οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, **β)** οι κωδικοί πρόσβασης είτε διακινούνται
μέσω του δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση, και **γ)** οι χρήστες
χρησιμοποιούν εύκολους κωδικούς.
5.2.3 E-mail Spoofing: Το e-mail spoofing αποτελεί πρακτική παραποίησης ή απόκρυψης της πραγματικής πηγής από την οποία προήρθε το μήνυμα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται συνήθως για να παραπλανήσει το χρήστη ώστε να συλλεχθούν από αυτόν χρήσιμα δεδομένα. Ενδεικτικά αποστέλλονται μηνύματα με υποτιθέμενο αποστολέα τον διαχειριστή του συστήματος, ζητώντας από το χρήστη να
επιβεβαιώσει το password που χρησιμοποιεί.
5.2.4 Επιθέσεις παρακολούθησης (Sniffing): Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές

συστημάτων για να αναλύουν τη συμπεριφορά συστημάτων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «προγράμματα sniffing». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Οι συσκευές με δυνατότητες sniffing μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης
εισβολών IDS (Intrusion Detection System). Συνεπώς τέτοιου είδους συσκευές είναι χρήσιμες και απαραίτητες. Ωστόσο, είναι προφανές ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις υπηρεσίες που προσφέρουν τα προγράμματα sniffing για την
υλοποίηση των παράνομων δραστηριοτήτων τους. Υπάρχουν ειδικά προγράμματα sniffing, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση: **α)** password, **β)** στοιχείων οικονομικών συναλλαγών (π.χ.
κωδικοί πιστωτικών καρτών), **γ)** εμπιστευτικών δεδομένων (π.χ. προσωπικά στοιχεία χρηστών, e-mail).

5.2.5 Ιοί (viruses) - σκουλήκια (worms): Οι ιοί είναι προγράμματα ή εντολές που προσαρτώνται σε προγράμματα ή δεδομένα και εκτελούνται παράλληλα με αυτά. Μπορούν να προκαλέσουν την αλλοίωση ή καταστροφή δεδομένων. Τα σκουλήκια αντίστοιχα, είναι προγράμματα που κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Και οι δύο κατηγορίες προγραμμάτων έχουν ως στόχο να πλήξουν το σύστημα στο οποίο εκτελούνται, προκαλώντας ζημιές όπως διαγραφή δεδομένων.

5.2.6 Buffer overflow attacks (υπερχείλιση καταχωρητή): Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο να πλήξουν τις εφαρμογές που αποθηκεύουν δεδομένα σε
προσωρινό χώρο μνήμης (buffer) μέχρι να έρθει η ώρα τους για επεξεργασία. Οι επιτιθέμενοι βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της
εφαρμογής με τις δικές τους εντολές. Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών, οι επιτιθέμενοι αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.

5.2.7 Cookie Poisoning: Τα Cookies είναι αρχεία υπολογιστών που αποθηκεύονται στον σκληρό δίσκο του υπολογιστή του πελάτη ή στην μνήμη cache, κατά την πρόσβαση του σε μια εφαρμογή διαδικτύου μέσω ενός browser. Αυτά τα αρχεία περιέχουν πληροφορίες όπως όνομα χρήστη, κωδικός πρόσβασης και στοιχεία συνόδου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες με σκοπό τη χρήση του υπολογιστή του πελάτη για κακόβουλες πράξεις. Τα Cookies χωρίζονται σε δύο κατηγορίες: αυτά που μένουν στον υπολογιστή του χρήστη μόνο
κατά τη διάρκεια της επίσκεψης του χρήστη στην εφαρμογή διαδικτύου, και αυτά που έχουν ημερομηνία λήξης και παραμένουν στον σκληρό δίσκο του πελάτη μέχρι την ημερομηνία λήξης τους οπότε και διαγράφονται.

5.3 ΑΝΤΙΚΕΙΜΕΝΙΚΟΙ ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ

Το σύνολο των μηχανισμών ασφαλείας ενός συστήματος ηλεκτρονικής τραπεζικής θεωρείται ότι πετυχαίνουν το σκοπό τους, όταν επιτυγχάνονται μία σειρά από αντικειμενικούς στόχους. Οι
κυριότεροι είναι:

5.3.1 Η ακεραιότητα των δεδομένων. Το πιο σημαντικό από αυτά είναι το ηλεκτρονικό χρήμα, το οποίο δεν πρέπει να αλλοιώνεται ούτε ως προς την ποσότητα, ούτε ως προς κάποιο άλλο χαρακτηριστικό του, σε όποιο υποσύστημα και αν αποθηκευτεί.

5.3.2 Η εμπιστευτικότητα των δεδομένων. Τα δεδομένα όλων των κατηγοριών που κυκλοφορούν μέσα στο σύστημα πρέπει να γνωστοποιούνται μόνο στους εξουσιοδοτημένους χρήστες. Οι
καταναλωτές δεν μπορούν να γνωρίζουν τους κωδικούς πρόσβασης του διαχειριστή και ο διαχειριστής δεν πρέπει να γνωρίζει τα υπόλοιπα των λογαριασμών των καταναλωτών, εκτός από τις περιπτώσεις που αυτό προβλέπεται.

5.3.3 Η πιστοποίηση του ηλεκτρονικού χρήματος που μετακινείται μεταξύ των υποσυστημάτων και η πιστοποίηση των υποσυστημάτων που ανταλλάσσουν δεδομένα μεταξύ τους.

5.3.4 Ο έλεγχος πρόσβασης στο σύστημα. Κάθε χρήστης, καταναλωτής ή διαχειριστής, πρέπει να διαθέτει ένα σύνολο μοναδικών κωδικών, με σκοπό τον περιορισμό της πρόσβασης στα αντίστοιχα δεδομένα που τον αφορούν.

5.3.5 Η πραγματοποίηση ολοκληρωμένων συναλλαγών. Εφόσον προκύψει κάποιο πρόβλημα πριν την τελική επιβεβαίωση, η συναλλαγή πρέπει να ακυρώνεται εξ ολοκλήρου. Απαγορεύεται η τμηματική πραγματοποίηση μιας συναλλαγής.

5.3.6 Η μη αποκήρυξη εμποδίζει μια οντότητα να αρνηθεί συναλλαγές οι πράξεις που συνέβησαν στο παρελθόν. Για παράδειγμα, μια τράπεζα πρέπει να μπορεί να αποδείξει σε κάποιον τρίτο ότι ένας
χρήστης διεξήγαγε μια συγκεκριμένη συναλλαγή, σε περίπτωση που ο χρήστης το αρνείται.

5.3.7 Ο εντοπισμός κάθε μη φυσιολογικής ενέργειας στο σύστημα, όπως η παράνομη πρόσβαση ή η προσπάθεια αλλοίωσης των δεδομένων.

5.3.8 Η αντίδραση του συστήματος σε κάθε απρόοπτη αλλαγή της κατάστασής του, όπως η απότομη πτώση τάσης ή η διακοπή οποιασδήποτε προσπάθειας για παράνομη πρόσβαση.

5.3.9Τα ασφαλή μέσα μεταφοράς δεδομένων και οι ***ασφαλείς χώροι εγκατάστασης των μηχανημάτων***, ώστε να μην είναι εύκολη η φυσική πρόσβαση σε σημαντικά μέρη του συστήματος.

5.3.10 Η ενημέρωση του λογισμικού ασφαλείας με τις τελευταίες εκδόσεις για την καταπολέμηση κάθε νέας απειλής.

5.4 Η ΤΕΧΝΟΛΟΓΙΑ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Ο προβληματισμός και οι ανησυχίες που προκαλεί η ασφάλεια στο Ηλεκτρονικό Εμπόριο μπορούν να καταταχθούν σε δύο κατηγορίες
1. σε προβληματισμούς σχετικούς με την **εξουσιοδότηση του χρήστη** και
2. σε προβληματισμούς σχετικά με την **ασφάλεια τόσο των στοιχείων** όσο και της **διαδικασίας της συναλλαγής**

Για τις επιχειρήσεις:
Κανείς δεν είναι 100% ασφαλής on-line. Επιτήδειοι πάντοτε υπάρχουν, αλλά η κρυπτογράφηση και τα συστήματα ασφαλείας αναπτύσσονται συνεχώς. Ωστόσο, επενδυτές και αναλυτές συμφωνούν ότι οι συναλλαγές είναι λιγότερο επικίνδυνες στο Internet συγκριτικά με το «φυσικό» κόσμο. Για τις μικρομεσαίες επιχειρήσεις το ηλεκτρονικό εμπόριο είναι περισσότερο ασφαλές από ένα «πραγματικό» κατάστημα, το οποίο μπορεί να λεηλατηθεί, να καεί, να πλημμυρίσει. Η δυσκολία έγκειται στο να κάνουν τους πελάτες να εξοικειωθούν με την ιδέα ότι το ηλεκτρονικό εμπόριο είναι ασφαλές γι' αυτούς.

Για τους πελάτες:
Παρόλο που τα προηγούμενα χρόνια, υπήρχε η εντύπωση ότι οι συναλλαγές μέσω πιστωτικής κάρτας στο Internet δεν ήταν ασφαλείς, οι ειδικοί υποστηρίζουν ότι το ηλεκτρονικό εμπόριο και οι on-line συναλλαγές εν γένει είναι ασφαλέστερες από τις αγορές με πιστωτικές κάρτες σε «φυσικά» καταστήματα. Κάθε φορά που ο πελάτης πληρώνει με πιστωτική κάρτα σε ένα κατάστημα ή εστιατόριο και κάθε φορά που πετά την απόδειξη μιας πιστωτικής κάρτας γίνεται περισσότερο ευάλωτος στην απάτη. Παράλληλα, έχουν αναπτυχθεί και αναπτύσσονται συνεχώς νέοι και ασφαλέστεροι τρόποι πληρωμής μέσω διαδικτύου, όπως οι υπηρεσίες onlíne μεταφοράς χρημάτων, οι προπληρωμένες και εξειδικευμένες πιστωτικές κάρτες για πληρωμή μέσω διαδικτύου, κλπ

Τα κυριότερα από τα μετρά ενίσχυσης της ασφάλειας των ηλεκτρονικών συναλλαγών περιλαμβάνουν την κατασκευή firewalls, την υιοθέτηση κρυπτογράφησης και γνησιότητας και την χρήση ασφαλών συνδέσεων.

5.4.1 Κρυπτογράφηση

Είναι η επιστήμη που παρέχει ασφαλή επικοινωνία μεταξύ ευάλωτων καναλιών και είναι πολύ σημαντική για την επιτυχία του διαδικτύου και του ηλεκτρονικού εμπορίου.

(όσον αφορά την κρυπτογραφία θα αναφερθώ εκτενεστέρα στο επόμενο κεφάλαιο)

5.4.2 FIREWALL

Για την ασφάλεια των ηλεκτρονικών συναλλαγών χρησιμοποιούνται ευρέως τα firewalls. Το firewall αποτελεί λογισμικό ή υλικό, που επιτρέπει μόνο στους εξωτερικούς χρήστες που έχουν τα κατάλληλα δικαιώματα, να προσπελάσουν το προστατευόμενο δίκτυο. Ένα firewall επιτρέπει στους εσωτερικούς χρήστες να έχουν πλήρη πρόσβαση στις παρεχόμενες υπηρεσίες, ενώ οι εξωτερικοί χρήστες πρέπει να πιστοποιηθούν. Υπάρχουν πολλοί τύποι firewalls, καθένας από τους οποίους παρέχει διαφορετικά επίπεδα προστασίας. Ο συνηθέστερος τρόπος χρησιμοποίησης ενός firewall είναι η τοποθέτηση ενός υπολογιστή ή δρομολογητή μεταξύ συγκεκριμένου δικτύου και του Internet, και η παρακολούθηση όλης της κυκλοφορίας μεταξύ του εξωτερικού και του τοπικού δικτύου. Η εμπιστευτική πληροφορία που διακινείται στο δίκτυο μπορεί να προστατευθεί με κρυπτογράφηση και χρήση μυστικών κωδικών. Η ασφάλεια του ηλεκτρονικού εμπορίου βασίζεται κατεξοχήν στην κρυπτογράφηση, δηλαδή στην κωδικοποίηση του μεταδιδόμενου κειμένου κατά τέτοιο τρόπο ώστε να μπορεί να αποκρυπτογραφηθεί μόνο με τη χρήση του ειδικού κλειδιού αποκρυπτογράφησης. Η κρυπτογράφηση συνοδεύεται πολλές φορές και από την ψηφιακή υπογραφή του αποστολέα, έτσι ώστε ο παραλήπτης να μπορεί να βεβαιωθεί για την ταυτότητα του πρώτου.

Η αποστολή προσωπικών δεδομένων, όπως τα στοιχεία της κάρτας, θα πρέπει να γίνεται σε ασφαλές περιβάλλον, με τη χρήση ειδικών πρωτοκόλλων κρυπτογράφησης δεδομένων και ασφάλειας οικονομικών συναλλαγών. Για την εξασφάλιση της μυστικότητας, της ακεραιότητας και της προέλευσης μιας πληροφορίας κατά τη μετάδοση, χρησιμοποιείται η τεχνολογία δικτυακού πρωτοκόλλου ασφαλείας, όπως το **Secure Sockets Layer** (SSL) ή το **Secure ElectronicTransaction** (SET), με τη χρήση του οποίου οι πληροφορίες κρυπτογραφούνται προτού μεταδοθούν στο δίκτυο και αποκρυπτογραφούνται από τον παραλήπτη

5.4.3 Επίπεδο Ασφαλών Συνδέσεων (SSL - Secure Sockets Layer)

Το πρωτόκολλο αυτό σχεδιάστηκε προκειμένου να πραγματοποιεί ασφαλή σύνδεση με τον εξυπηρετητή (server). Το SSL χρησιμοποιεί "κλειδί" δημόσιας

κρυπτογράφησης, με σκοπό να προστατεύει τα δεδομένα καθώς "ταξιδεύουν" μέσα στο Internet. Το πρωτόκολλο αυτό σχεδιάστηκε από την εταιρία NETSCAPE. Η έκδοση 3.0 κυκλοφόρησε το 1996 και αποτέλεσε τη βάση για την μετέπειτα ανάπτυξη του πρωτόκολλου TLS(TRANSFER LAYER SECYRITY) το όποιο πλέον τείνει και να αντικαταστήσει το ssl.Τα δυο αυτά πρωτοκολλά χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου. Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτοκολλά TCP/IP(Transfer control protocol/internet protocol). Το ssl λειτουργούσε πριν το TCP/IP και μετά τις εφαρμογές υψηλού επίπεδου όπως είναι για παράδειγμα το HTTP(προβολή ιστοσελίδων) το FTP μεταφορά αρχείων και το IMAP (e-mail). Άρα λοιπόν αυτό που ουσιαστικά κάνει το ssl είναι να παίρνει πληροφορίες από τις εφαρμογές υψηλοτέρων επίπεδων, τις κρυπτογραφεί και στη συνέχεια να τις μεταδίδει στο internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε .

5.4.4 Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET - Secure Electronic Transactions)

Το SET κωδικοποιεί τους αριθμούς της πιστωτικής κάρτας που αποθηκεύονται στον εξυπηρετητή του εμπόρου. Το πρότυπο αυτό, που δημιουργήθηκε από τη Visa και τη MasterCard, απολαμβάνει μεγάλης αποδοχής από την τραπεζική κοινότητα.

6. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΟΙ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΣΤΙΣ ΜΕΘΟΔΟΥΣ ΔΙΑΣΦΑΛΙΣΗΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ[5]

Η κρυπτογράφηση αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet καθώς η μετάδοση εμπιστευτικών δεδομένων μέσω του Διαδικτύου έχει γίνει κοινός τόπος σήμερα και θα πρέπει να βρεθούν μηχανισμοί προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των χρηστών του Internet.Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Το αρχικό μήνυμα αποκαλείται *απλό κείμενο (plaintext)*, ενώ το ακατανόητο μήνυμα που προκύπτει από την κρυπτογράφηση (μετατροπή) του απλού κειμένου αποκαλείται *κρυπτογράφημα (ciphertext)*. *Κρυπτογράφηση (encryption)* αποκαλείται η μετατροπή ενός απλού και κατανοητού κειμένου (plaintext) σε μια μη κατανοητή μορφή (κρυπτογράφημα, ciphertext) με την εφαρμογή ενός κατάλληλου αλγορίθμου, ενώ *αποκρυπτογράφηση (decryption)* αποκαλείται η ανάκτηση του αρχικού απλού κειμένου από το κρυπτογράφημα αφού εφαρμοσθεί ο αντίστροφος αλγόριθμος.

Οι αλγόριθμοι κρυπτογράφησης λειτουργούν σε συνδυασμό μ' ένα *κλειδί* ή *κλείδα (key)*, για να μπορέσει να γίνει η κρυπτογράφηση του απλού κειμένου.

[5] Πουλάκης Δημήτριος, Κρυπτογραφία η επιστήμη της ασφαλούς επικοινωνίας,εκδόσεις ΖΗΤΗ , 2004

Αν για το ίδιο απλό κείμενο χρησιμοποιήσουμε διαφορετικά κλειδιά, θα δημιουργηθούν και διαφορετικά κρυπτογραφήματα.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει τέσσερις βασικές λειτουργίες (Αντικειμενικοί σκοποί):

- ***Εμπιστευτικότητα*:** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- ***Ακεραιότητα*:** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- ***Μη απάρνηση***: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- ***Πιστοποίηση*:** Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

6.1 ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών

5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

6.2 Οι μέθοδοι κρυπτογράφησης

Δύο είναι οι βασικές μέθοδοι κρυπτογράφησης, η συμμετρική και η ασύμμετρη κρυπτογράφηση. Στη ***συμμετρική κρυπτογράφηση*** χρησιμοποιούμε το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση ενός μηνύματος. Το κοινό αυτό κλειδί θα πρέπει να είναι γνωστό μόνο στα δύο επικοινωνούντα μέρη και κατά συνέπεια η μετάδοσή του από το ένα μέρος στο άλλο θα πρέπει να γίνει με απόλυτη ασφάλεια, κάτι που δεν είναι πάντα εφικτό και καθιστά έτσι τη μέθοδο της συμμετρικής κρυπτογράφησης ως μη απόλυτα αποτελεσματική.

Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος *DES (Data Encryption Standard)*, που χρησιμοποιείται και από την κυβέρνηση των ΗΠΑ, και το σύστημα *Kerberos* του γνωστού Πανεπιστημίου MIT.

Στην ***ασύμμετρη κρυπτογράφηση*** ή *κρυπτογράφηση δημόσιου κλειδιού* χρησιμοποιούμε διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος. Αυτά είναι το *δημόσιο κλειδί (public key)* και το *ιδιωτικό κλειδί (private key)*, τα οποία έχουν τις εξής πολύ σημαντικές ιδιότητες :

- Ένα μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί και αντίστροφα.

- Αν μας είναι γνωστό το ένα κλειδί δεν μπορούμε να δημιουργήσουμε το άλλο κλειδί.

6.2.1 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Η **κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography)** βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.

Ένα πρόβλημα το οποίο υφίσταται στους αλγόριθμους κρυπτογράφησης είναι η αδυναμία ανταλλαγής του κλειδιού με κάποιο ασφαλή τρόπο. Στην σύγχρονη ψηφιακή εποχή ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δεν γνωρίζονται, οπότε για την μετάδοση του κλειδιού από τον έναν στον άλλο θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου, ανταλλαγής ηλεκτρονικών μηνυμάτων κοκ ουσιαστικά δεν υφίσταται.

Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

6.2.2 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η **κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography)** επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει έναν εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

mQGiBDmXx8cRBADd0Dko7J7Gb5G/FINwO48AgrlYE87wCT5dlqSXl2uoDmR0/dKp
pJmvDeLQw+Z02yGx7TKf7PC5dfh61tIHyeI0SfCZVA5DtRDk3keNXy2WLnLMg2yS
J44JG3I/o1QKXL8PKD2bkv/vUl7gtXe3qa57oC+2ZmxzptnLeBh08QrWXwCg/8A2
L7WHGKbhYKCApM+0FJStYrcD/1iTYhNsiZnW2tc86e/uHiX8rg7tD7VGm/Wg2E4V
Hadsb4wMLhlfi/vCSEZmlH3hFxvGk6YCWXkdFxzqhq2ZJRWQStqZqjSPWTI3HvOK
Nzjq5DbRMQY2O025g1FyWB62ZDrUWXqzybi4okoEdXT/lQA7Xe95T8uy1zfTUmBg
ieTtA/0RU3MYboVDyDgGvJ7fVyFNdk8+v6Hzcn6EZMWYJifE5hw/tSLnRAXb7ejh
wsLDDCGsjloUj4TnMHH0LUTZSWbgDZwCF6tig3mbhk7YH21zWrVQwPidSpS5O3Oh
85V3nJx5r0406nM4N1cp46yKUMekE6nhubCpVme6o+f9sUMXkLQhR2VydCBLYXNw
ZXJzZW4gPGdla2FzQHdtkGF0YS5jb20+iQBLBBARAgALBQI5l8fHBAsDAgEACgkQ
Ls3rBj/p+6oQGwCgv5ML3xAatvJtY1mKnwz1SH2YbJ8AoPeBkUY73P+QDc5aFdHC
rCkobzlYuQQNBDmXx8cQEAD5GKB+WgZhek0QldwFbIeG7GHszUUfDtjgo3nGydx6
C6zkP+NGlLYwSlPXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHY
UMoiV0MpvpXoVis4eFwL2/hMTdXjqkbM+84X6CqlFGHjhKlP0YOEqHm274+nQ0YI
xswdd1ck0ErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHId0HX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZC
LQI2wSbLaF6dfJgkCol+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHT
UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYllIhkmuquiXsNV6z3W
FwACAhAAumPF6HT301BhkfuMTVI2jFXUJ7prdWy4pwZArvdDVYQ35M8sG/ISJjwg
B2GdpK9i02B25Cen309snDSj/aJkz7PQgD8CyBlV0KiDFX+KxR8S0le2k1tdbiP3
wNYxw7MDiz757IY9/hmv6YDwSeS2sWnyjgfQXR5z2RBs4r+UZ8YWk8h4YQsLSL2B
Z/PImaiopMScDJy1m4AzasXNdyr1SywU4tlwOXZhZh6ccZB/z6nlZJgMnwfVw1fZ
8wyiTKGoyOp5eh9edDFwtcAVNHVoI0hj9kDfa5sfA9zcKfeLH7TouYLuMcdws9Uc
fNeJI6AgzUvGwzvG9HVuVGf7n5b1j9Kp+jcSjvWqpQX1/iDEN8KG6/yk5mtok4lv
JBieGM2SahP1cTk1P4kcrlwJ419EhKtC6xZS96J0+TmyLBTSrJHazWR+n/lQsXvz
g7wNUycZx+/v1QDGO3HyekqZR76BSMVrpNEYEWcBclTeJ6nBJCPTGxqvP4IQhzhJ
3znANVOsViJZ7rG3DrygE+8vQ32GjbBZzouN/gHxmSKOuvw6yjFdki5MNNdlIeKm
05Z5aVSXPuE7+TfkbFGHy+GCxjsH6FNhU/8QKtr712NO9laDARGCVaOiVvBVevVO
PXajFSW19F7Rswmh7kD5jUEy9E7ANAa0YD5i07ee0wvmaGSwfKKIRgQYEQIABgUC
OZfHxwAKCRAuzesGP+n7qj2kAJ48xQqu8b8kzQHmmUvMFr8z+bfivQCgxXhBHUT1
LsvbbxbTJ/Da6n5YSYE=
=9v+B
-----END PGP PUBLIC KEY BLOCK-----
```

Ένα δημόσιο κλειδί 1024 bits το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται **ιδιωτικό κλειδί (private key)** και το άλλο **δημόσιο κλειδί (public key)**. Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

6.3 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ – DIGITAL SIGNATURE

Η ψηφιακή υπογραφή αποτελεί έναν κρυπτογραφικό μηχανισμό ο οποίος επιτελεί την ίδια λειτουργία όπως οι γραπτές υπογραφές, δηλαδή χρησιμοποιείται για την απόδειξη της αυθεντικότητας του αποστολέα εφαρμόζοντας την κρυπτογράφηση δημοσίου κλειδιού αντίστροφα.

6.4 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ –DIGITAL CERTIFICATES

Ένα ψηφιακό πιστοποιητικό συνήθως αναφέρεται σε μία ψηφιακά υπογεγραμμένη δήλωση που εκδίδεται από μία αρχή πιστοποίησης που τυγχάνει δημόσιας εμπιστοσύνης (Έμπιστη Τρίτη Οντότητα-(ΕΤΟ) (Trusted third party certificate
Authority –CA). Ένα ψηφιακό πιστοποιητικό περιλαμβάνει στοιχεία όπως :

- Το όνομα του κατόχου,
- Έναν σειριακό αριθμό,
- Τα δημόσια κλειδιά του κατόχου (ένα για μυστική ανταλλαγή κλειδιού ως αποδοχέα και ένα για ψηφιακή υπογραφή ως αποστολέα)
- Τον αλγόριθμο που χρησιμοποιεί αυτά τα κλειδιά
- Τον τύπο του Πιστοποιητικού (κάτοχος κάρτας, έμπορος, ή πύλη πληρωμής),
- Το όνομα της Αρχής Πιστοποίησης,
- Την ημερομηνία λήξης της ισχύος του πιστοποιητικού,
- Την ψηφιακή υπογραφή της Αρχής Πιστοποίησης

6.5 ΨΗΦΙΑΚΟΣ ΦΑΚΕΛΛΟΣ –DIGITAL ENVELOPE

Η ψηφιακή εμφακέλωση είναι η διαδικασία κρυπτογράφησης ενός μυστικού κλειδιού (όπως αυτό του DES) με το δημόσιο κλειδί του παραλήπτη. Το μυστικό κλειδί DES που κρυπτογραφείται με αυτόν τον τρόπο καλείται ψηφιακός φάκελος, διότι θα πρέπει πρώτα να ανοιχθεί, για να μπορέσει στη συνέχεια να
αποκωδικοποιηθεί το περιεχόμενο του μηνύματος
με αυτό.

6.6 ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΣΥΝΑΛΛΑΓΗΣ ΚΑΙ ΧΡΟΝΙΚΗ ΣΦΡΑΓΙΔΑ

Ένα **πιστοποιητικό συναλλαγής** (transaction certificate) αποτελεί επιβεβαίωση για την πραγματοποίηση μίας συναλλαγής και με αυτό μπορεί να αποφευχθεί η αποποίηση ευθύνης. Με τον ίδιο τρόπο, η **χρονική σφραγίδα**, είναι μία ψηφιακή πιστοποίηση μη επιδεχόμενη πλαστογράφησης και η οποία πιστοποιεί ότι κάποιο έγγραφο υπήρξε σε συγκεκριμένη χρονική στιγμή.

7. ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΜΕΘΟΔΩΝ ΣΤΙΣ ΕΛΛΗΝΙΚΕΣ ΤΡΑΠΕΖΕΣ

7.1 ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ[6]

Κάθε φορά που κάποιος χρησιμοποιεί την υπηρεσία της τράπεζας Πειραιώς θα πρέπει να πληκτρολογήσει 2 κωδικούς που του έχει δώσει η τράπεζα. Ο ένας είναι ο κωδικός εισόδου (USER ID) και ο άλλος ο κωδικός ασφάλειας

[6] http://www.piraeusbank.gr

(PIN). Για μεγαλύτερη ασφάλεια το σύστημα ζητά από τον πελάτη την πρώτη φορά που θα το χρησιμοποιήσει να αλλάξει τον κωδικό. Επίσης η αλλαγή του κωδικού ζητείται κάθε 2 μήνες. Η τράπεζα αυτή χρησιμοποιεί το πρωτόκολλο ssl 128 bit για την εξασφάλιση του απορρήτου των συναλλαγών. Εάν δεν υπάρξει καμιά ενεργεία για 7 λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία. Επίσης χρησιμοποιεί firewalls για τον έλεγχο της πρόσβασης, επιτρέπει στους χρηστές να χρησιμοποιούν συγκεκριμένες υπηρεσίες απαγορεύοντας παράλληλα την πρόσβαση σε απόρρητα στοιχεία της τράπεζας. Σε περίπτωση που ο χρήστης εισάγει 3 φόρες λάθος κωδικό ασφάλειας κλειδώνονται αυτόματα οι κωδικοί του και δεν του επιτρέπει την πρόσβαση στην υπηρεσία.

7.2 ΑΓΡΟΤΙΚΗ ΤΡΑΠΕΖΑ ΕΛΛΑΔΟΣ (ATE BANK)[7]

Το σύστημα της ΑΓΡΟΤΙΚΗΣ ΤΡΑΠΕΖΑΣ αναγνωρίζει την ταυτότητα του χρήστη ώστε μόνο εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στις υπηρεσίες. Για να υπάρξει επιτυχής είσοδος στην υπηρεσία θα πρέπει να γίνει συνδυασμός χρήσης των προσωπικών κωδικών ασφάλειας, Κωδικός χρηστή και κωδικός εισόδου όταν η υπηρεσία χρησιμοποιείται από ιδιώτες όταν όμως χρησιμοποιείται από επιχειρήσεις ζητείται ένας παραπάνω κωδικός ο Μυστικός Κωδικός. Για ακόμα μεγαλύτερη ασφάλεια απαιτείται η καταχώρηση ενός προσθετού κωδικού από την ειδική συσκευή security token. Οι κωδικοί κλειδώνονται αυτόματα όταν καταχωρηθούν λανθασμένα 3 φόρες ο μυστικός κωδικός ή 5 φόρες ο πρόσθετος κωδικός. Εάν μέσα σε 10 λεπτά δεν έχει γίνει καμιά ενέργεια στην υπηρεσία τότε τερματίζεται αυτόματα η επικοινωνία με την υπηρεσία web banking. Το web banking της ATE BANK έχει πιστοποιηθεί από διεθνούς κύρους οργανισμό VeriSign ο όποιος εξειδικεύεται σε θεματα ασφαλειας συναλλαγών.

[7] http://www.atebank.gr

7.3 ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ[8]

Η ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ διασφαλίζει το απόρρητο και απαραβίαστο των συναλλαγών και των προσωπικών στοιχείων με προηγμένες και πρωτοποριακές μεθόδους. Για την μυστικότητα και το αναλλοίωτο των συναλλαγών χρησιμοποίει πρωτόκολλο ασφαλής επικοινωνίας ssl με ισχυρή κρυπτογραφία στα 128 bit. Η αυθεντικότητα της τράπεζας εξασφαλίζεται με το πιστοποιητικό της VeriSign. Η ταυτοποίηση του χρήστη για την πρόσβαση στην υπηρεσία γίνεται με τον κωδικό χρήστη και τον μυστικό κωδικό, και για την διενέργεια συναλλαγών μέσω τηλέφωνου (phone banking) η ταυτοποίηση γίνεται με τον εξαψήφιο αριθμητικό κωδικό εισόδου (user id) και έναν κωδικό μιας χρήσης που παράγεται από μια συσκευή I-code. Επιπλέον ζητείται από τον χρήστη να αλλάζει το password κάθε 2 μήνες.

7.4 ΕΜΠΟΡΙΚΗ ΤΡΑΠΕΖΑ[9]

Ο έλεγχος πρόσβασης στις υπηρεσίες της Εμπορικής Τράπεζας διενεργείται με την χρήση προσωπικών κωδικών, του κωδικού πελάτη και του κωδικού πρόσβασης. Εάν εισήχθη 5 φόρες λανθασμένα ο κωδικός πρόσβασης ή κωδικός πελάτη τότε ο λογαριασμός κλειδώνεται. Το e-banking της τράπεζας υποστηρίζεται από σύστημα που χρησιμοποιεί την μεγίστη δυνατή κρυπτογραφία η οποία εξασφαλίζει ότι οι πληροφορίες που ανταλλάσσονται

[8] http://www.nbg.gr

[9] http://www.ebank-emporiki.gr

μεταξύ του συστήματος του πελάτη και του συστήματος του e-banking δεν μπορούν να υποκλαπούν, και οι συναλλαγές προστατεύονται από το πρωτόκολλο ssl με 128 bit. Σε περίπτωση που υπηρεσία δεν χρησιμοποιείται για χρονικό διάστημα πέραν των 5 λεπτών τότε αποσυνδέεται αυτόματα. Επιπλέον η τράπεζα προσφέρει τον πρόσθετο κωδικό αφέλειας (one time password). Περά της κρυπτογραφίας η υπηρεσία e-banking προστατεύεται από πολλαπλά και τελευταίας τεχνολογίας εξειδικευμένου λογισμικού ασφάλειας συστήματα όπως firewalls και Intrusion Detection Systems (IDS). Τα συστήματα e-banking βρίσκονται σε καθεστώς διαρκούς έλεγχου και ενημέρωσης. Επιπλέον τα συστήματα ελέγχονται μια φορά τον χρόνο από εξωτερική εταιρία ασφάλειας.

7.5 ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ ΤΡΑΠΕΖΑ ΧΑΝΙΩΝ[10]

Για την ασφάλεια των συναλλαγών της η τράπεζα χρησιμοποιεί τεχνολογία ssl με κρυπτογράφηση στα 128 bit και πιστοποίηση ασφάλειας από την VeriSign. Για την πρόσβαση στην υπηρεσία web banking απαιτείται η χρήση του κωδικού πελάτη, του μυστικού αριθμού καθώς και του προσθετού κωδικού (e-token) που καθορίζουν το επίπεδο πρόσβασης του χρηστή και την δυνατή πραγματοποίηση συναλλαγών. Εάν εισήχθη 3 φόρες λανθασμένος κωδικός κλειδώνεται ο κωδικός του χρηστή και τέλος γίνεται αυτόματη αποσύνδεση όταν παρέλθει κάποιο χρονικό διάστημα.

[10] http://www.e-chaniabank.gr

7.6 ΤΑΧΥΔΡΟΜΙΚΟ ΤΑΜΙΕΥΤΗΡΙΟ[11]

Η ταυτοποίηση των στοιχείων του πελάτη επιτυγχάνεται με την συνδυασμένη χρήση του κωδικού πελάτη και του μυστικού κωδικού αναγνώρισης. Για την διασφάλιση του απορρήτου των συναλλαγών η τράπεζα χρησιμοποιεί το κατάλληλο κρυπτογραφημένο πρωτόκολλο επικοινωνίας. Η τράπεζα επίσης έχει προμηθευτεί πιστοποιητικό αυθεντικότητας το όποιο εμφανίζεται με το εικονίδιο ενός λουκέτου στο κάτω μέρος της οθόνης του υπολογιστή, προκειμένου ο πελάτης να βεβαιωθεί ότι η ιστοσελίδα που βρίσκεται είναι η αυθεντική. Εάν μέσα σε διάστημα 5 λεπτών δεν έχει πραγματοποιηθεί καμιά ενεργεία στο σύστημα της τράπεζας η επικοινωνία τερματίζεται αυτόματα. Εάν εισαχθεί 3 φόρες λανθασμένος κωδικός τότε ο κωδικός του χρηστή απενεργοποιείται αυτόματα.

7.7 EFG EUROBANK[12]

Στην Eurobank η ασφάλεια των συναλλαγών αποτελούν πρώτη προτεραιότητα. Η υιοθέτηση τεχνολογίας αιχμής καθιστούν την Euroobank πρωτοπόρο στην διασφάλιση των συναλλαγών. Η τράπεζα αυτή εξασφαλίζει το απόρρητο κατά την μεταφορά των δεδομένων με κρυπτογράφηση. Επίσης χρησιμοποιεί το πρωτόκολλο επικοινωνίας ssl μαζί με την κρυπτογράφηση στα 128 bit.

[11] http://www.ttbank.gr

[12] http://www.eurobank.gr

Επίσης έχει επιλέξει την εταιρία VeriSign ως παροχής πιστοποίησης της ταυτότητας της στο διαδίκτυο. Όταν βρίσκεται ο χρήστης σε ασφαλή ιστοσελίδα τότε εμφανίζεται το εικονίδιο με το λουκέτο.
Για την ταυτοποίηση των χρηστών η Eurobank χρησιμοποιεί έναν προσωπικό κωδικό εισόδου σε συνδυασμό με ένα username που έχει δηλώσει ο χρήστης. Για την διενέργεια συναλλαγών στις όποιες ο παραλήπτης είναι άγνωστος και συνεπώς εμπεριέχουν ρίσκο, η τράπεζα χρησιμοποιεί την ψηφιακή πιστοποίηση. Μέσω του πιστοποιητικού αυτού ο κάτοχος του έχει την δυνατότητα να υπογράψει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-banking.
Η πρόσβαση στα συστήματα της τράπεζας προστατεύεται από τελευταίας τεχνολογίας firewalls η οποία επιτρέπει την χρήση συγκεκριμένων υπηρεσιών απαγορεύοντας την πρόσβαση σε συστήματα με απόρρητα στοιχεία.
Η ολοκλήρωση μιας συναλλαγής επιτρέπεται σε χρονικό όριο 15 λεπτών έπειτα το σύστημα αποσυνδέει τον χρηστή αυτόματα. Το σύστημα επίσης υποχρεώνει τον χρηστή μετά την πρώτη εισαγωγή στο e-banking για άμεση αλλαγή του προσωπικού κωδικού. Οι προσωπικοί κωδικοί μπλοκάρονται μετά από 3 συνεχόμενα λανθασμένες προσπάθειες εισαγωγής στο σύστημα ή συνολικά 9 μέσα σε μια εβδομάδα.

7.8 ΕΛΛΗΝΙΚΗ ΤΡΑΠΕΖΑ[13]

Η ελληνική τράπεζα λαμβάνει όλα τα απαραίτητα μέτρα ώστε να διασφαλίζεται η ασφάλεια των λογαριασμών και των προσωπικών δεδομένων των πελατών της . Παρέχει κρυπτογράφηση δεδομένων στα 128 bit και χρησιμοποιεί πρωτόκολλο ασφάλειας ssl. Η ελληνική τράπεζα έχει προμηθευτεί πιστοποιητικό αυθεντικότητας παρουσίας της στο διαδίκτυο από την Thawte server. Και το εικονίδιο με το λουκέτο στο κάτω μέρος της οθόνης επιβεβαιώνει ότι ο πελάτης βρίσκεται σε νόμιμη σελίδα.

[13] http://www.helleninetbanking.com

7.9 ΤΡΑΠΕΖΑ ΚΥΠΡΟΥ[14]

Για πρόσβαση στις υπηρεσίες της τράπεζας απαιτείται η χρήση των κωδικών user id και του κωδικού ασφάλειας. Ο user id αποτελείται από 8 αριθμητικά ψηφιά και είναι ο πρώτος κωδικός που εισάγεται στο σύστημα. Ο κωδικός ασφάλειας είναι ο δεύτερος κωδικός πρόσβασης. Αποτελείται από 6 αριθμητικά και μπορεί να αλλάξει ανά πάσα στιγμή από τον χρηστή. Στην ιστοσελίδα της τράπεζας Κύπρου χρησιμοποιείται κρυπτογράφηση ssl. Η υπηρεσία e-banking διαθέτει πιστοποίηση από την Thawte Extended Validation ssl CA. Επιπλέον η τράπεζα προμηθεύει τον εκάστοτε πελάτη με μια συσκευή που ονομάζεται digipass για επιπρόσθετη ασφάλεια η οποία χρησιμοποιείται για χρηματικές συναλλαγές προς τρίτους. Η συσκευή digipass κάθε φορά που χρησιμοποιείται από τον χρήστη πιέζει το κουμπί και εμφανίζεται ένας 6ψηφιος κωδικός που είναι μοναδικός κάθε φορά. Επιπλέον η τράπεζα χρησιμοποιεί firewalls. Σε περίπτωση 3 συνεχόμενων ανεπιτυχών εισαγωγών των κωδικών τότε το σύστημα απενεργοποιεί την πρόσβαση. Εάν υπάρχει σύνδεση με το internet banking και για 10 λεπτά δεν γίνει καμιά ενεργεία τότε η σύνδεση με την υπηρεσία διακόπτεται αυτόματα.

7.10 MARGIN EGNATIA BANK[15]

Η MARFIN EGNATIA BANK χρησιμοποιεί προηγμένες μεθόδους για την διασφάλιση των ηλεκτρονικών συναλλαγών. Γίνεται ταυτοποίηση του χρήστη. Αυτό επιτυγχάνεται με την εισαγωγή των προσωπικών κωδικών, όταν ο

[14] http://www.bankofcyprus.gr

[15] http://www.marfinbank.gr

χρήστης επιχειρεί είσοδο στην υπηρεσία e-banking. Για ακόμα μεγαλύτερη ασφάλεια η τράπεζα ζητά να καταχωρηθεί η ηλεκτρονική υπογραφή συναλλαγής. Η υπηρεσία υποστηρίζεται από το πρωτόκολλο επικοινωνίας ssl με κρυπτογράφηση 128 bit η οποία είναι αδύνατον να παραβιαστεί. Επίσης ο πελάτης μπορεί να επιβεβαιώσει ότι βρίσκεται σε σελίδα με ενεργοποιημένη κρυπτογράφηση όταν το <<http>> στην ηλεκτρονική διεύθυνση της σελίδας έχει μετατραπεί σε <<https>>. Στην υπηρεσία της τράπεζας έχει εγκατασταθεί πιστοποιητικό αυθεντικότητας από την VeriSign. Επίσης τα δεδομένα της τράπεζας προστατεύονται από τα καλυτέρα φίλτρα έλεγχου, τα firewalls. Επίσης χρησιμοποιείται εικονικό πληκτρολόγιο το όποιο αντικαθιστά το κανονικό ώστε να είναι αδύνατον η υποκλοπή των κωδικών μέσω ιών που μπορούν να καταγράψουν τις πληκτρολογήσεις από το πραγματικό πληκτρολόγιο. Η επικοινωνία με την υπηρεσία τερματίζεται εάν δεν γίνει καμιά καμιά ενέργεια μέσασε 15 λεπτά και τέλος σε 3 συνεχόμενα λανθασμένες εισαγωγές του κωδικού οι κωδικοί πρόσβασης κλειδώνονται αυτόματα.

7.11 ΤΡΑΠΕΖΑ ALPHA BANK [16]

Σε κάθε συναλλαγή με την τράπεζα γίνεται κρυπτογράφηση (ssl 128 bit). Για χρήση της υπηρεσίας απατούνται οι προσωπικοί κωδικοί ασφάλειας. Σε περίπτωση που επιχειρηθεί επανειλημένη προσπάθεια συνδέσεων με λάθος κωδικό η συνδρομή κλειδώνεται αυτόματα για λογούς ασφάλειας. Υπάρχει η δυνατότητα ο πελάτης να δηλώσει εναλλακτικό κωδικό συνδρομητή. Η τράπεζα επιπρόσθετα χρησιμοποιεί συστήματα ασφάλειας firewalls τα οποία ελέγχουν και καταγράφουν την πρόσβαση στα συστήματα της και ταυτόχρονα εμποδίζει οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση στις βάσεις δεδομένων της.

[16] http://www.alphabank.gr

7.12 ΤΡΑΠΕΖΑ ΑΝΑΠΤΥΞΕΩΣ[17]

Η τράπεζα Αναπτύξεως χρησιμοποιεί αυστηρά πρότυπα ασφάλειας. Χρησιμοποιεί κρυπτογράφηση με 128 bit . Επίσης για πιο αποτελεσματική ασφάλεια για την πρόσβαση στην υπηρεσία χρησιμοποιείται ο κωδικός συνδρομητή, ο προσωπικός κωδικός και ο μυστικός αριθμός συναλλαγής. Εάν οι προσωπικοί κωδικοί πρόσβασης πληκτρολογηθούν 5 φόρες συνεχόμενα λανθασμένα τότε η υπηρεσία διακόπτεται αυτόματα. Επιπλέον χρησιμοποιεί και εικονικό πληκτρολόγιο . Εάν μετά την σύνδεση περάσουν 10 λεπτά αδράνειας χωρίς να γίνει κάποια συναλλαγή τότε η σύνδεση διακόπτεται. Μπορεί επίσης ο πελάτης να καθορίσει το ανώτατο όριο ποσού που θέλει να μεταφέρεται σε ημερησία βάση. Η τράπεζα χρησιμοποιεί επιπρόσθετα ειδικά συστήματα ασφάλειας (firewalls) τα οποία ελέγχουν και καταγράφουν την πρόσβαση στα συστήματα της.

[17] http://www.cyprusdevelopmentbank.gr

8. ΣΥΜΠΕΡΑΣΜΑ

Όπως είδαμε οι περισσότερες τράπεζες που λειτουργούν στην Ελλάδα έχουν σαν προτεραιότητα τους την ασφάλεια των συναλλαγών και την προστασία των πελατών τους. Όλες τους χρησιμοποιούν κρυπτογραφικές μεθόδους στα 128 bit μαζί με πρωτόκολλο επικοινωνίας ssl. Οι περισσότερες από αυτές έχουν επιλέξει την εταιρία VeriSign ως πάροχος πιστοποίησης της ταυτότητας τους στο διαδίκτυο. Όλες επίσης οι τράπεζες χρησιμοποιούν τεχνολογία firewalls η οποία επιτρέπει την χρήση συγκεκριμένων υπηρεσιών απαγορεύοντας την πρόσβαση σε απόρρητα αρχεία. Και τέλος όλες τους περά της κρυπτογράφησης χρησιμοποιών επιπλέον ασφαλιστικές δικλείδες που κατοχυρώνουν την ασφάλεια των υπηρεσιών τους όπως είναι οι προσωπικοί κωδικοί ,η αυτόματη αποσύνδεση το εικονικό πληκτρολόγιο κ.α. Επιπλέον η κρυπτογραφία είναι ίσως από τις πιο εξελίξιμες αρχαίες επιστήμες παγκοσμίως και δεν είναι τυχαίο αν αναλογιστεί κανείς την χρήση και την συμβολή της στην καθημερινότητα μας. Στην πλειοψηφία των καθημερινών μας συναλλαγών κυρίως ηλεκτρονικών η κρυπτογραφία παίζει σημαντικότατο ρόλο και είναι πλέον αναπόσπαστο κομμάτι της ζωής μας π.χ. στις τράπεζες στις τηλεπικοινωνίες. Σήμερα η κρυπτογραφία μαζί με την άνθηση της πληροφορίας γνωρίζει μια παράλληλη εξελικτική άνθηση. Είναι ένα χρήσιμο εργαλείο το οποίο όταν χρησιμοποιείται σωστά μας εξασφαλίζει ασφάλεια στις συναλλαγές μας, αξιόπιστη μεταφορά της πληροφορίας και γενικότερα μια καλύτερη ζωή.

10.ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία:

Πασχόπουλος Α, ηλεκτρονικό εμπόριο 3η έκδοση, κλειδάριθμος

William Stallings κρυπτογραφία και ασφάλεια δικτύων, Ιών 2011

Δουκίδης Γ. ηλεκτρονικό εμπόριο, εκδόσεις νέων τεχνολογιών

Αγγελής Γ. Βασίλειος, η βίβλος του e-banking,2005,εκδόσεις νέων τεχνολογιών

Πουλάκης Δημήτριος, Κρυπτογραφία η επιστήμη της ασφαλούς επικοινωνίας,εκδόσεις ΖΗΤΗ , 2004

Δ.Καρολίδης ,Κ Ξαρχάκος ,εισαγωγή στην πληροφορική και το διαδίκτυο, εκδόσεις Άβακας

Δημόπουλος Δημήτριος, συστήματα συναλλαγών, Εκδόσεις Σιατράς Ι. και Σία Ε.Ε 2006

ΗΛΕΚΤΡΟΝΙΚΟΙ ΤΟΠΟΙ (SITES)

http://www.i_reportergr.com

http://www.awmn.net.gr

http://www.e-papadakis.gr

http://www.freshweb.gr

http://el.wikipedia.org

http://www.moneyexpert.gr

http://www.insomnia.gr

http://www.piraeusbank.gr

http://www.atebank.gr

http://www.nbg.gr

http://www.ebank-emporiki.gr

http://www.e-chaniabank.gr

http://www.ttbank.gr

http://www.eurobank.gr

http://www.helleninetbanking.com

http://www.bankofcyprus.gr

http://www.marfinbank.gr

http://www.alphabank.gr

http://www.cyprusdevelopmentbank.gr