ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος εργασίας:

«ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΩΝ:

ΔΙΑΚΟΛΟΥΚΑ ΔΕΣΠΟΙΝΑ

ΧΑΤΖΗΜΙΧΑΛΗ ΜΑΡΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΒΛΑΧΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ

Πάτρα-2009

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ Β΄

ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΠΕΡΙΛΗΨΗ

Είναι πλέον φανερό ότι η τεχνολογία μετασχηματίζει τον τραπεζικό κλάδο. Σήμερα η ηλεκτρονική τραπεζική υπόσχεται την επανάσταση στις συναλλαγές μας με τις τράπεζες καθώς μεταφέρει την τράπεζα στην οθόνη του υπολογιστή μειώνοντας έτσι δραστικά το κόστος τόσο για τους πελάτες όσο και για την ίδια την τράπεζα.

Το νέο κανάλι διανομής των τραπεζικών προϊόντων και υπηρεσιών έχει πολλά πλεονεκτήματα, η υιοθέτησή του όμως κρύβει και κινδύνους για τους οποίους πρέπει να βρεθούν αποτελεσματικοί τρόποι διαχείρισης. Για να μπορέσει η τράπεζα να παραμείνει ανταγωνιστική στο νέο περιβάλλον, πρέπει να εντάξει την ηλεκτρονική τραπεζική στους στρατηγικούς της στόχους.

Τέλος η καινοτομία και η εφαρμογή βέλτιστων πρακτικών προσφέρουν ανταγωνιστικά πλεονεκτήματα στις επιχειρήσεις που τα εφαρμόζουν δημιουργώντας με αυτό τον τρόπο ηγέτες στο χώρο της ηλεκτρονικής τραπεζικής.

Οι συναλλαγές μέσω Internet χαρακτηρίζονται από πολλά πλεονεκτήματα, με αποτέλεσμα να αποτελούν ολοένα και μεγαλύτερο τμήμα της σύγχρονης ψηφιακής ζωής μας. Όπως κάθε αγορά όμως, έτσι και η ψηφιακή δεν είναι άμοιρη κινδύνων. Στην πραγματικότητα, οι κίνδυνοι είναι σημαντικά μικρότεροι από σχεδόν οποιονδήποτε άλλο τρόπο αγοράς, αλλά επειδή η τεχνολογία είναι κάτι άγνωστο για τους περισσότερους, ο οποιοσδήποτε φόβος αφενός πολλαπλασιάζετε και αφετέρου "δαιμονοποιείται" με εξαιρετική ευκολία.

Pharming, phising, key loggers, και δεκάδες άλλες απειλές, αποκτούν ξαφνικά ασύμμετρα μεγάλες διαστάσεις, κυρίως αφενός της άγνοιας και αφετέρου λόγω έλλειψης κοινής λογικής[1].

Οι ηλεκτρονικές συναλλαγές λοιπόν είναι απαραίτητο να ενδυναμωθούνε με την λήψη ισχυρών μέτρων ασφαλείας τελευταίας τεχνολογίας.

[1] *www.pcw.gr/Step-By-Step/secure_purchases_internet/233.html - 109k «Ασφαλείς συναλλαγές μέσω Internet»*

ΕΙΣΑΓΩΓΗ

Η μεγάλη ανάπτυξη του Διαδικτύου που πραγματοποιείται την τελευταία δεκαετία δε θα μπορούσε να αφήσει ανεπηρέαστο και τον τραπεζικό κλάδο.

Παραδοσιακά οι τραπεζικοί οργανισμοί ανταγωνίζονταν μεταξύ τους χρησιμοποιώντας ως κανάλια διανομής για τα προϊόντα και τις υπηρεσίες τους τα δίκτυα των υποκαταστημάτων τους.

Οι τεχνολογικές όμως εξελίξεις άλλαξαν τα δεδομένα του παιχνιδιού. Ο όρος ηλεκτρονική τραπεζική που εμπεριέχει όρους όπως web banking, Internet banking, online banking και mobile banking μέχρι πριν μερικά χρόνια ήταν άγνωστος. Στις μέρες μας οι περισσότερες τράπεζες έχουν υιοθετήσει την ηλεκτρονική τραπεζική παράλληλα με την παραδοσιακή εκτέλεση τραπεζικών εργασιών στα υποκαταστήματα, ενώ μη τραπεζικοί οργανισμοί όπως αλυσίδες λιανικής πώλησης, ασφαλιστικές εταιρίες και εταιρίες πληροφορικής έχουν μπει στην αγορά του e-banking καθιστώντας τον ανταγωνισμό ακόμα πιο έντονο.

Το χαμηλό κόστος σε συνδυασμό με την εύκολη πρόσβαση που προσφέρει το Διαδίκτυο σε κάθε χρήστη έχουν σαν αποτέλεσμα η ηλεκτρονική τραπεζική να κερδίζει διαρκώς έδαφος καθώς παρέχει σημαντική εξοικονόμηση χρόνου, χρήματος αλλά και ταλαιπωρίας για τη διεκπεραίωση των τραπεζικών συναλλαγών.[2]

Η ραγδαία όμως εξάπλωση των ηλεκτρονικών συναλλαγών έχει να αντιμετωπίσει και ισχυρές απειλές και κινδύνους από ιούς, υποκλοπές δεδομένων, καταστροφές αρχείων οι οποίοι πολύ έξυπνα ακολουθούν την πορεία της τεχνολογίας.

Σε ένα τέτοιο περιβάλλον, όλες οι τράπεζες ακολουθούν ιδιαίτερα αυστηρούς και επαρκείς κανόνες ασφαλείας στα site τους και ανταποκρίνονται άμεσα και αποτελεσματικά σε ανάλογα περιστατικά. Γεγονός που σημαίνει ότι για την προστασία των προσωπικών δεδομένων τους την αρχική ευθύνη έχουν οι ίδιοι οι χρήστες, που θα πρέπει να επαγρυπνούν για οποιαδήποτε ύποπτη κίνηση[3].

---

[2] *Κραπης Βασίλειος, (2007) «Η ηλεκτρονική τραπεζική ως ανταγωνιστικό πλεονέκτημα στη σύγχρονη δικτυακή οικονομία»*

[3] *Αν. Παπαϊωάννου, (2005) (www.economia.gr/index.php?Itemid=28&id=414&option= om_content&task=view -* 53k «Internet*banking: Συμφέρει, αλλά προσοχή στους χάκερ*»

Η εργασία αυτή διαπραγματεύεται το θέμα: «ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ».

Από την αρχή το θέμα μας φάνηκε πάρα πολύ ενδιαφέρον γιατί το Internet θα μπορούσε να χαρακτηριστεί ως ένα κοινωνικό ή ακόμα και πολιτισμικό φαινόμενο, αφού μέσα σ'αυτό διακινούνται πληροφορίες που καλύπτουν κάθε δραστηριότητα πάνω σ' αυτόν τον πλανήτη.

Στόχος της εργασίας είναι να τονίσουμε την ραγδαία εξέλιξη των ηλεκτρονικών συναλλαγών, τα πλεονεκτήματά τους και τα μειονεκτήματά τους και να οριοθετήσουμε τις συνηθέστερες απειλές και υποκλοπές βάσει θεωριών καταγεγραμμένων σε βιβλία, άρθρα εφημερίδων και περιοδικών και στο Διαδίκτυο.

Η μεθοδολογία που ακολουθήθηκε είναι η εξής: Αφού συγκεντρώσαμε το υλικό μας από βιβλία, εφημερίδες, περιοδικά και το Διαδίκτυο και το μελετήσαμε, χωρίσαμε την εργασία μας σε τρία μέρη. Με τον τρόπο αυτό κατηγοριοποιήσαμε τα δεδομένα που συλλέξαμε και τα χωρίσαμε σε κεφάλαια.

Το πρώτο μέρος «INTERNET – ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ – ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ» το χωρίσαμε σε τρία κεφάλαια.

Το δεύτερο μέρος «ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ» σε δύο κεφάλαια .

Το τρίτο «ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑ ΤΩΝ ΚΙΝΔΥΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ» σε δύο επίσης και

Το τέταρτο «ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ σε ένα.

Κλείνουμε την εργασία μας με τα συμπεράσματα. Στο τέλος της εργασίας παραθέτουμε το γλωσσάριο στο οποίο ερμηνεύουμε τα πιο σημαντικές διεθνείς ξένες λέξεις του διαδικτύου που χρησιμοποιούμε στην εργασίας μας.

ΜΕΡΟΣ Α΄

INTERNET – ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ – ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΚΕΦΑΛΑΙΟ 1

1. INTERNET

1.1. Γενικά για το Internet

Ο αγγλικός όρος Internet προκύπτει από τη σύνθεση λέξεων Inter-network. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη του μορφή, με τους όρους Διαδίκτυο, Ιντερνέτ ή Ίντερνετ περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του.

Το Internet είναι μια ομάδα παγκόσμιων πόρων πληροφοριών. Αυτοί οι πόροι έχουν μεγάλο εύρος ώστε να είναι δύσκολο να τους κατανοήσει ανθρώπινο ον. Οι «λεωφόροι» πληροφοριών του Internet βρίσκονται σε μια μεγάλη συλλογή δικτύων υπολογιστών που αναπτύχθηκε τη δεκαετία του 1970. Οι «λεωφόροι» ξεκινούν από ένα δίκτυο που ονομάζεται ARPANET το οποίο αναπτύχθηκε από το Υπουργείο Άμυνας των Η.Π.Α. για να συνδέει το Πεντάγωνο με τους πανεπιστημιακούς ερευνητές. Το πρώτο πειραματικό δίκτυο που χρησιμοποίησε τεχνολογία παρόμοια με αυτή του Internet αποτελούταν από 4 υπολογιστές. Το αρχικό ARPANET έχει αναπτυχθεί και σήμερα οι απόγονοί του σχηματίζουν τη ραχοκοκαλιά αυτού που ονομάζουμε Internet.

Το Διαδίκτυο έχει την ικανότητα να συνδέει εκατομμύρια ανθρώπους παγκοσμίως εύκολα και φτηνά και αποτελεί σήμερα τη μεγαλύτερη «υπερλεωφόρο της πληροφορικής» στον κόσμο. Δεν διοικείται αλλά ούτε ανήκει σε κανένα. Η γλώσσα που χρησιμοποιείται περισσότερο για την επικοινωνία στο Διαδίκτυο είναι η Αγγλική. Αυτό συμβαίνει κυρίως λόγω της Αμερικανικής καταγωγής του Ίντερνετ και της χρήσης της Αγγλικής στον προγραμματισμό λογισμικού. Τα τελευταία χρόνια, το Διαδίκτυο περιλαμβάνει πλέον επαρκές περιεχόμενο και στις υπόλοιπες γλώσσες των περισσότερο ανεπτυγμένων χωρών.[4]

[4] *www.google.gr*

1.2. Υπηρεσίες που παρέχει το διαδίκτυο

Έτσι όπως είναι σήμερα η κατάσταση είναι απαραίτητο και δυνατόν να μπει ο καθένας μας στο Διαδίκτυο. Οι καιροί των προνομιούχων έχουν περάσει. Όμως πρώτα απ' όλα θα πρέπει να τονίσουμε ότι δεν μπορούμε να είμαστε σίγουροι πως είναι αληθινά όλα όσα διαβάζουμε. Στο διαδίκτυο υπάρχει ένα είδος ανωνυμίας. Ο καθένας γράφει ότι θέλει και αυτό που θέλει, οπότε λείπει η σιγουριά της αλήθειας.

Παραδοσιακά, στο Διαδίκτυο προσφέρονται πέντε βασικές υπηρεσίες:

• Το παγκόσμιο δίκτυο (WWW) είναι ίσως η μεγαλύτερη υπηρεσία που προσφέρει το Διαδίκτυο. Το δίκτυο είναι η εμπορική περιοχή του Internet και κάθε επιχείρηση ή άτομο που θέλει να προσφέρει ή να αντλήσει κάθε είδους πληροφορία μπορεί να χρησιμοποιήσει ένα νοητό χώρο στο Διαδίκτυο. Ο νοητός αυτός χώρος αποτελεί την ιστοσελίδα (site). Το σημαντικό είναι η δημιουργία αυτής της σελίδας να έλκει τη προσοχή των χρηστών. Οι χρήστες έχουν τη δυνατότητα να μεταφέρουν στην οθόνη τους όλα τα είδη των δεδομένων, όπως κείμενο εικόνα, γραφικά, ήχο, βίντεο σε μορφή ιστοσελίδων κ.α. Το WWW λειτουργεί με τις λεγόμενες ιστοσελίδες ή web pages οι οποίες βρίσκονται σε ειδικούς εξυπηρετητές που λέγονται web servers. Για την αναζήτηση αυτών των σελίδων χρησιμοποιείται κάποιος φυλλομετρητής browser. Τέτοιοι φυλλομετρητές είναι ο Navigator της Netscape και ο Internet Explorer της Microsoft.

• Το ηλεκτρονικό ταχυδρομείο (e-mail) που είναι γνωστό και σαν «ταχυδρομείο σαλιγκάρι» είναι η πιο φτηνή και εύκολη εναλλακτική λύση στο κανονικό ταχυδρομείο. Η υπηρεσία αυτή δίνει τη δυνατότητα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου, μέσω του οποίου μπορούμε να στείλουμε συνημμένα και αρχεία οποιασδήποτε μορφής. Η ηλεκτρονική διεύθυνση περιλαμβάνει το όνομα και τη θέση του χρήστη π.χ. gpap@teipat.gr.[5]

• Usenet και Netnews: Είναι μια υπηρεσία που περιλαμβάνει χιλιάδες διαφορετικά newsgroups, δηλαδή Ομάδες Συζήτησης , στα οποία χρήστες με κοινά ενδιαφέροντα ανταλλάσσουν μηνύματα. Υπάρχουν χιλιάδες τέτοιες ομάδες με θέματα

[5] *Harley Hahn&Rick Stout, Το μεγάλο βιβλίο του Internet, Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ Αθήνα 1995*

τόσο τεχνικά όσο και μη τεχνικά, μέσα στα οποία περιλαμβάνονται οι υπολογιστές, η επιστήμη, η ψυχαγωγία και η πολιτική. Στη πραγματικότητα Netnews είναι το ανεπίσημο όνομα για το Usenet. Το Usenet διαχειρίζεται μόνο "νέα".

• Σύνδεση σε υπολογιστή από απόσταση-Telnet: Το πρωτόκολλο TELNET χρησιμοποιείται για την σύνδεση με απομακρυσμένους ηλεκτρονικούς υπολογιστές οι οποίοι έχουν μία συγκεκριμένη διεύθυνση (αριθμητική, κειμένου) στο Internet. Χρησιμοποιείται επίσης πολύ από μεγάλους υπολογιστές (mainframes) εκπαιδευτικών ιδρυμάτων, μεγάλων εταιρειών και παρόμοιων φορέων, επειδή παρέχει εξαιρετικές δυνατότητες ελέγχου στα επιμέρους στοιχεία ενός δικτύου.

• Μεταφορά δεδομένων: Με το πρόγραμμα «ftp», που πήρε το όνομά του από το αντίστοιχο πρωτόκολλο FTP (File Transfer Protocol), ή ανάλογα προγράμματα που «μιλούν» το ίδιο πρωτόκολλο, είναι εφικτό να αντιγραφούν αρχεία από μια μηχανή στο Διαδίκτυο σε άλλη. Τεράστιος όγκος άρθρων, δεδομένων κτλ. είναι διαθέσιμος με αυτόν τον τρόπο.[6]

[6] *www.tovima.gr/default.asp?pid=2&artid=127395&ct=34&dt*

ΚΕΦΑΛΑΙΟ 2

2. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Εισαγωγή

Στο πρόσφατο παρελθόν οι συναλλαγές και οι αγορές των καταναλωτών και αντίστοιχα οι πωλήσεις των εμπόρων γίνονταν με καθαρά συμβατικά μέσα. Οι καταναλωτές προκειμένου να αγοράσουν αυτό που επιθυμούσαν ή να δεχτούν μία υπηρεσία έπρεπε να μεταβούν στην έδρα του προμηθευτή των αγαθών ή των υπηρεσιών. Στις μέρες μας ο τρόπος διεξαγωγής των συναλλαγών έχει αλλάξει ριζικά.

Ένας από τους νέους και τάχιστους τρόπους εξυπηρέτησης των καταναλωτών είναι το Ηλεκτρονικό Εμπόριο το οποίο αναπτύσσεται ραγδαία στο εξωτερικό αλλά και στην Ελλάδα με πιο αργούς όμως ρυθμούς.

2.1. Ορισμός

Ως ηλεκτρονικό εμπόριο ορίζεται το εμπόριο που πραγματοποιείται με ηλεκτρονικά μέσα, βασίζεται δηλαδή στην ηλεκτρονική μετάδοση δεδομένων.

Το ηλεκτρονικό εμπόριο αποτελεί μια ολοκληρωμένη συναλλαγή που πραγματοποιείται μέσω του διαδικτύου χωρίς να είναι απαραίτητη η φυσική παρουσία των συμβαλλομένων μερών, δηλαδή του πωλητή και του αγοραστή, οι οποίοι μπορούν να βρίσκονται ακόμα και σε διαφορετικές χώρες. Είναι οποιαδήποτε συναλλαγή που ενέχει διαδικτυακή δέσμευση για αγορά η πώληση αγαθών ή υπηρεσιών.[7]

2.2. Μορφές του ηλεκτρονικού εμπορίου

Το ηλεκτρονικό εμπόριο με βάση το εύρος χρήσης των νέων τεχνολογιών διακρίνεται σε άμεσο και έμμεσο.

[7] *www.go-online.gr/ebusiness/specials/article.html?article_id=315*

1. Στο άμεσο ηλεκτρονικό εμπόριο όλα τα στάδια της εμπορικής διαδικασίας (παραγγελία, πληρωμή και παράδοση) πραγματοποιούνται μέσω ηλεκτρονικών μέσων. Γι' αυτό το λόγο το άμεσο ηλεκτρονικό εμπόριο αφορά άϋλα αγαθά και υπηρεσίες (όπως λογισμικού, υπηρεσιών πληροφόρησης, κ.α.) Η πληρωμή των υπηρεσιών αυτών γίνεται είτε με πιστωτικές κάρτες είτε με ηλεκτρονικό χρήμα με την αρωγή πάντα και τη σύμπραξη των τραπεζών.

2. Στο έμμεσο ηλεκτρονικό εμπόριο μόνο η διαδικασία παραγγελίας πραγματοποιείται μέσω ηλεκτρονικού υπολογιστή. Η παράδοση των προϊόντων διεκπεραιώνεται με συμβατικό, παραδοσιακό τρόπο όπως ταχυδρομείο και εταιρίες διανομής.

Οι συνηθέστερες μορφές ηλεκτρονικού εμπορίου ανάλογα με τα μέρη που εμπλέκονται σε μια ηλεκτρονική συναλλαγή διακρίνεται σε:

- 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.
- 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.[8]

- Επιχείρηση προς δημόσια διοίκηση: Καλύπτει όλες τις συναλλαγές μεταξύ επιχειρήσεων και δημόσιων οργανισμών. Προς το παρόν, αυτή η κατηγορία είναι σε νηπιακό στάδιο, αλλά μπορεί να αναπτυχθεί ραγδαία όσο οι κυβερνήσεις χρησιμοποιούν τις δικές τους λειτουργίες για να προωθήσουν την αντίληψη τους για το ηλεκτρονικό εμπόριο. Επιπροσθέτως, οι διοικήσεις πρέπει να παρέχουν την ευκαιρία ηλεκτρονικών συναλλαγών για καταστάσεις όπως επιστροφές ΦΠΑ και φόρων.

- Πελάτης προς δημόσια διοίκηση: Δεν έχει ακόμα ενεργοποιηθεί. Στον βωμό της ανάπτυξης των 2 προηγούμενων κατηγοριών, οι επιχειρήσεις πρέπει να αναπτύξουν τις ηλεκτρονικές συναλλαγές σε περιοχές όπως πληρωμές κοινωνικής πρόνοιας και ιδιωτικών φόρων.

2.3. Επιχειρησιακά μοντέλα ηλεκτρονικού εμπορίου

Το ηλεκτρονικό εμπόριο δημιουργεί καινούργια είδη επιχειρηματικών μοντέλων. Αυτό δεν σημαίνει ότι τα υπάρχοντα μοντέλα δεν λειτουργούν στο περιβάλλον του δικτύου.

Μάλιστα ορισμένα παλιά μοντέλα χρησιμοποιώντας τις ιδιαιτερότητες του web, κατόρθωσαν να αναγεννηθούν και να γνωρίσουν και πάλι επιτυχία. Ένα από τα χαρακτηριστικότερα παραδείγματα είναι οι δημοπρασίες. Αποτελούσαν ένα από τα παλαιότερα επιχειρηματικά μοντέλα. Χρησιμοποιήθηκαν στο παρελθόν από πολλές εταιρίες σε όλο τον πλανήτη. Η έλευση του Internet και η χρησιμοποίηση τους από εταιρίες όπως η e-bay (www.e-bay.com) έδειξε ότι το συγκεκριμένο πρότυπο ταιριάζει απόλυτα στις ιδιαιτερότητες του δικτύου.

- *Τι όμως εννοούμε με τον όρο επιχειρηματικό μοντέλο (business model);*

Η Ευρωπαϊκή Επιτροπή προσπαθώντας να προσεγγίσει τον όρο δίνει τον παρακάτω ορισμό. Επιχειρησιακό μοντέλο-πρότυπο είναι:

[8] *www.go-online.gr/ebusiness/specials/article.html?article_id=550 - 31k*

• Μια αρχιτεκτονική για τις ροές προϊόντων, υπηρεσιών και πληροφοριών, συμπεριλαμβανομένης μιας περιγραφής των βασικών επιχειρησιακών δράσεων και των ρόλων τους.

• Περιγραφή των πιθανών ωφελειών για τις διάφορες επιχειρησιακές δράσεις.

• Περιγραφή των πηγών εσόδων.

Ένδεκα επιχειρησιακά μοντέλα είναι σε χρήση σύμφωνα με την έρευνα του Paul Timmers (Head of Unit eGovernment - European Commission – DG INFSO) για την Ευρωπαϊκή Ένωση και παρατίθενται πιο κάτω μαζί με αναλυτική περιγραφή για το καθένα:

2.3.1. E-shop

Το e-shop (ηλεκτρονικό κατάστημα) ή virtual store αποτελεί την ηλεκτρονική παρουσία μιας επιχείρησης. Τα ηλεκτρονικά καταστήματα προωθούν τα αγαθά ή τις υπηρεσίες της επιχείρησης και έχουν τη δυνατότητα on line παραγγελιών και πληρωμών. Τα επιδιωκόμενα οφέλη για την επιχείρηση είναι η χαμηλού κόστους παγκόσμια παρουσία και η μείωση των εξόδων της προώθησης. Τα οφέλη για τους πελάτες μπορεί να είναι οι χαμηλότερες τιμές έναντι της παραδοσιακής προσφοράς, η ευρύτερη επιλογή, η καλύτερη πληροφόρηση, η ευκολία της επιλογής, της αγοράς και της παράδοσης, συμπεριλαμβανομένης της εικοσιτετράωρης διαθεσιμότητας. Τα έσοδα για την επιχείρηση έρχονται εκτός από τις πωλήσεις και από πιθανή ενοικίαση διαφημιστικού χώρου στον ιστοχώρο της.

Οι περισσότεροι εμπορικοί ιστοχώροι είναι ηλεκτρονικά καταστήματα επιχείρησης προς καταναλωτή, όπως το http://www.flowershop.gr ηλεκτρονικό κατάστημα ενός παραδοσιακού ανθοπωλείου της Αθήνας (επισημαίνεται ως επιτυχημένο παράδειγμα στο πλαίσιο του προγράμματος «Δικτυωθείτε), το www.oro.gr, το www.aromatica.gr και το www.kosmima.gr για αγορές δώρων, το www.toys.gr και το www.toysacademy.gr για αγορές παιχνιδιών.[9]

[9] *Κατσουλάκος Γιάννης, (2001)*

2.3.2. E-procurement

Τα συστήματα ηλεκτρονικών προμηθειών (e-procurement) δεν είναι κάτι καινούργιο στην οργάνωση του κύκλου προμηθειών. Ήδη, με την εμφάνιση της τεχνολογίας EDI (Electronic Data Interchange) πριν από αρκετά χρόνια, η αυτοματοποίηση για την εξασφάλιση αποδοτικότερης διαχείρισης της εφοδιαστικής αλυσίδας ήταν γεγονός.

Ωστόσο, η ραγδαία ανάπτυξη του Διαδικτύου, ως ανοιχτής και εύκολα προσβάσιμης αρχιτεκτονικής λύσης, καθιερώνει πλέον νέες προοπτικές στην ηλεκτρονική υποβολή προσφορών και προμήθειας αγαθών ή υπηρεσιών. Οι μεγάλες επιχειρήσεις καθώς και κάποιες υπηρεσίες του Δημοσίου έχουν υλοποιήσει τέτοιες λύσεις.

Οι βασικές λειτουργίες αυτού του επιχειρηματικού μοντέλου είναι η παρουσίαση καταλόγων προϊόντων, η διαχείριση παραγγελιών και πληρωμών, ο μηχανισμός αξιολόγησης προσφορών.

Τα επιδιωκόμενα οφέλη είναι να υπάρξει μια ευρύτερη επιλογή των προμηθευτών που αναμένεται να οδηγήσει σε χαμηλότερο κόστος, καλύτερη ποιότητα και βελτιωμένη διανομή. Για τους προμηθευτές τα οφέλη είναι οι περισσότερες ευκαιρίες υποβολής προσφορών, ενδεχομένως σε μια παγκόσμια κλίμακα και χαμηλότερο κόστος στην (ηλεκτρονική) αποστολή προσφορών.

Το simap.eu.int, είναι ο ιστοχώρος της Ε.Ε. σχετικά με τις ηλεκτρονικές κρατικές προμήθειες, με πλούσιο υλικό που αποσκοπεί στην ενθάρρυνση των προμηθευτών και των αναθετουσών αρχών να υιοθετήσουν τις βέλτιστες πρακτικές και να γνωρίζουν όλες τις διαθέσιμες πληροφορίες για την αποτελεσματική εκτέλεση όλων των δημοσίων συμβάσεων με τρόπο συστηματικό (προδιαγραφές) αξιοποιώντας τις νέες τεχνολογίες.

Λύσεις ηλεκτρονικών προμηθειών στο διαδίκτυο βρίσκουμε τόσο στο διεθνή χώρο με το www.ariba.com όσο και στον Ελληνικό χώρο με το www.yassas.com (που δραστηριοποιείται στο χώρο των προμηθειών των ξενοδοχείων, caterings, νοσοκομείων, πλοίων και χώρων εστίασης), το www.be24.gr και το www.cosmoOne.gr που λειτουργούν και ως ηλεκτρονικές αγορές.

2.3.3. E-auction

Οι ηλεκτρονικές δημοπρασίες προσφέρουν μια ηλεκτρονική εφαρμογή του γνωστού από τις παραδοσιακές δημοπρασίες μηχανισμού προσφοράς. Αυτό μπορεί

να συνοδευτεί από την πολυμεσική παρουσίαση των αγαθών. Οι εταιρίες που δραστηριοποιούνται σε αυτόν τον τομέα συνήθως προσφέρουν και την ολοκλήρωση της διαδικασίας, δηλαδή την online πληρωμή και την παράδοση των προϊόντων. Οι πηγές εσόδων των εταιριών αυτών είναι από τις αμοιβές της συναλλαγής και τη διαφήμιση. Τα οφέλη για τους προμηθευτές και τους αγοραστές είναι η εξοικονόμηση χρόνου, η παγκόσμια πρόσβαση και η μη φυσική παρουσία τους για την ολοκλήρωση της διαπραγμάτευσης.

Ο πιο γνωστός ιστοχώρος δημοπρασιών είναι φυσικά το www.e-bay.com όπου

μπορεί κανείς να αγοράσει σχεδόν τα πάντα. Παραδείγματα τέτοιων εταιριών στο Ελληνικό web είναι το www.124sold.gr, το www.emarket.gr, και το www.usurum.gr

2.3.4. E-mall

Ένα e-mall στη βασική του μορφή, αποτελείται από μια συλλογή ηλεκτρονικών καταστημάτων, κάτω από μια κοινή ομπρέλα, ενός γνωστού εμπορικού σήματος το οποίο μπορεί να προσφέρει και μία εγγυημένη μέθοδο πληρωμής. Τα έσοδα μπορούν να έρθουν από το χώρο διαφήμισης ή την ενίσχυση των εμπορικών σημάτων. Τα οφέλη για τον πελάτη είναι η εύκολη πρόσβαση σε άλλα ηλεκτρονικά καταστήματα και η ευκολία χρήσης ενός κοινού user interface. Τα οφέλη για τα καταστήματα των e-mall είναι το χαμηλότερο κόστος για την ηλεκτρονική τους παρουσία, η παροχή έτοιμων λύσεων σε δύσκολους τομείς όπως οι ηλεκτρονικές πληρωμές, οι παραδόσεις κ.α. Η πρόσθετη κυκλοφορία που παράγεται από άλλα καταστήματα στο e-mall, και η έλξη του εμπορικού σήματος στο οποίο φιλοξενούνται είναι επίσης οφέλη για τα e-shops. Όταν μάλιστα το εμπορικό σήμα είναι αρκετά γνωστό, τότε οι πελάτες νιώθουν μεγαλύτερη εμπιστοσύνη να προβούν σε αγορά. Τα έσοδα των e-malls πηγάζουν από συνδρομές των μελών τους, από τη διαφήμιση, και ενδεχομένως από προμήθεια σε κάθε συναλλαγή.

Παραδείγματα από τον Ελληνικό χώρο είναι το www.hellasmall.com ένα δικτυακό εμπορικό κέντρο συνεργαζόμενο με καταστήματα από όλο τον κόσμο και το www.agora.gr που ανήκει στον όμιλο της Hellas On Line.

Η εμπορική βιωσιμότητα του μοντέλου των e-mall έχει εξεταστεί στην παρούσα εφαρμογή της και δεν απέδωσε τα αναμενόμενα. Ένας από τους λόγους μπορεί να είναι ότι η

έννοια της γειτνίασης στο δίκτυο δεν είναι πολύ δόκιμη καθώς όλα τα καταστήματα είναι μόλις ένα κτύπημα μακριά. Επομένως, δεν μπορεί να λεχθεί ως σημαντικό πλεονέκτημα των e-mall η εύκολη εύρεση των καταστημάτων.

2.3.5. E-marketplace

Τα e-marketplaces (ηλεκτρονικές αγορές) αποτελούν τη σύγχρονη τάση στο χώρο του ηλεκτρονικού εμπορίου και προσανατολίζονται στη δημιουργία διαδραστικών εμπορικών κοινοτήτων που προσφέρουν δυναμικές -και όχι στατικές- λύσεις.

Τα e-marketplaces αναφέρονται σε μια νέα αυτοματοποιημένη ηλεκτρονική διαδικασία παραγγελιών η οποία συνδέει άμεσα τους πελάτες με τους προμηθευτές τους και επιτρέπει στους συμμετέχοντες αγοραστές και πωλητές να ανταλλάσσουν πληροφορίες για τιμές και προσφορές προϊόντων. Η λογική λειτουργίας τους είναι εξαιρετικά απλή και βασίζεται στη δημιουργία μιας ηλεκτρονικής πλατφόρμας όπου συνευρίσκονται προμηθευτές και αγοραστές. Μέσω της πλατφόρμας αυτής διενεργούνται αγοραπωλησίες ειδών ή υπηρεσιών. Κατά συνέπεια, τα εμπλεκόμενα μέρη στις ηλεκτρονικές αγορές είναι τρία: οι προμηθευτές, οι αγοραστές και αυτός που έχει δημιουργήσει την πλατφόρμα της ηλεκτρονικής αγοράς.

Αρκετά ενδιαφέρον είναι το γεγονός ότι τίποτα δεν εμποδίζει κάποιο από τα παραπάνω μέρη να έχει και άλλο ή ακόμα και άλλους ρόλους στην όλη διαδικασία, καθώς ο προμηθευτής κάποιων ειδών μπορεί να γίνει αγοραστής κάποιων άλλων και το αντίστροφο, ο δημιουργός της πλατφόρμας μπορεί να λειτουργήσει και ως προμηθευτής ή αγοραστής ειδών/υπηρεσιών.

Η λογική της ηλεκτρονικής αγοράς είναι τέτοια που σε καμία περίπτωση οι πολλαπλοί ρόλοι δεν αποτελούν πρόβλημα, καθώς υπάρχει διάκριση των ιδιοτήτων σε κάθε στάδιο (είναι αδιάφορο εάν ο προμηθευτής είναι και αγοραστής ή εάν ο αγοραστής είναι αυτός που έχει δημιουργήσει την πλατφόρμα).

Έσοδα δημιουργούνται από το ενοίκιο συμμετοχής, από πιθανές αμοιβές υπηρεσιών, ή από ποσοστό επί της αξίας συναλλαγών. Τα οφέλη για τους αγοραστές είναι η μείωση του λειτουργικού κόστους εφοδιαστικής αλυσίδας και η δυνατότητα νέων συνεργασιών. Οφέλη για τους προμηθευτές είναι η αξιοποίηση νέων καναλιών διανομής, η εύρεση νέων πελατών και η μείωση του κόστους πωλήσεων- marketing.

Παράδειγμα ηλεκτρονικής αγοράς για επιχειρήσεις που δραστηριοποιούνται στο χώρο των πλαστικών είναι το www.polysort.com.

Στον Ελληνικό χώρο μπορούμε να βρούμε παραδείγματα όπως το www.be24.gr που είναι αποτέλεσμα της συνεργασίας δύο κορυφαίων ελληνικών εταιριών, της EFG Eurobank Ergasias και της Vodafone, το www.cosmoOne.gr που είναι μια συνεργασία του ΟΤΕ, της Alpha Bank και της Εθνική Τράπεζας και το www.yassas.com.

2.3.6. Virtual communities

Η αξία των εικονικών κοινοτήτων προέρχεται από τα μέλη τους, ανθρώπους με κοινά ενδιαφέροντα, τα οποία βρίσκονται στο κοινό εικονικό περιβάλλον τους και επικοινωνούν ανταλλάσοντας πληροφορίες. Τα έσοδα δημιουργούνται από την συνδρομή των μελών καθώς επίσης και από πώληση διαφημιστικού χώρου. Οι εικονικές κοινότητες είναι πολλές στο Διαδίκτυο, ενδιαφέρον παρουσιάζουν το www.experts-exchange.com μία εικονική κοινότητα που δίνει λύσεις σε προβλήματα τεχνολογίας, το www.ivillage.com μία κοινότητα που απευθύνεται κυρίως σε γυναίκες και το www.about.com με αρκετά και ενδιαφέροντα θεματικά κανάλια.

2.3.7. Value chain service provider

Το μοντέλο αυτό ειδικεύεται σε ένα συγκεκριμένο κομμάτι-λειτουργία της αλυσίδας αξιών, όπως οι ηλεκτρονικές πληρωμές ή τα logistics, με την πρόθεση να γίνει αυτό το κομμάτι το ανταγωνιστικό πλεονέκτημά τους. Οι τράπεζες είναι ένα παράδειγμα αυτού του μοντέλου. Τα έσοδα έρχονται από τις εφ' άπαξ αμοιβές ή με κάποιο προκαθορισμένο ποσοστό από τις συναλλαγές.

2.3.8 Value chain integrators

Το συγκεκριμένο μοντέλο εστιάζει στην ενοποίηση πολλαπλών βημάτων στην αλυσίδα αξιών, με τη δυνατότητα να χρησιμοποιηθεί η ροή πληροφοριών μεταξύ των βημάτων ως περαιτέρω προστιθέμενη αξία. Τα έσοδα προέρχονται κυρίως από αμοιβές για τις συμβουλευτικές υπηρεσίες ή ενδεχομένως αμοιβές από τις συναλλαγές. Παράδειγμα του συγκεκριμένου μοντέλου για τη βιομηχανία πλαστικών αποτελεί το www.omnexus.com

2.3.9. Collaboration platforms

Οι πλατφόρμες συνεργασίας παρέχουν ένα σύνολο εργαλείων και ένα περιβάλλον πληροφοριών για τη συνεργασία μεταξύ των επιχειρήσεων. Εστιάζονται σε συγκεκριμένες λειτουργίες, όπως στην παροχή υπηρεσιών υποστήριξης προγραμμάτων από εικονικές ομάδες συμβούλων. Τα έσοδα έρχονται από τη διαχείριση της πλατφόρμας (αμοιβές ιδιότητας μέλους/ αμοιβές χρήσης), και από την πώληση των ειδικών εξειδικευμένων εργαλείων. Παράδειγμα αποτελεί η Deutsche Telecom.

2.3.10 Telekom/Globana's ICS.

Μια ολόκληρη σειρά νέων υπηρεσιών έχει δημιουργηθεί, για να προσθέσει αξία στα τεράστια ποσά δεδομένων που είναι διαθέσιμα στα ανοικτά δίκτυα. Δεδομένα που προέρχονται από τις επιχειρησιακές διαδικασίες, όπως η αναζήτηση πληροφοριών.

Εταιρίες δημοσκοπήσεων, σκιαγράφησης προφίλ πελατών, συμβουλευτικές εταιρίες και εταιρίες marketing εντάσσονται σε αυτό το μοντέλο. Έσοδα προέρχονται από την πληρωμή των πληροφοριών ή της γνωμοδότησης επίσης, όπως στο παράδειγμα της www.icap.gr η χρήση των πληροφοριών να γίνεται μέσω συνδρομής είτε με πληρωμή ανά χρήση. Έσοδα όμως μπορεί να υπάρξουν και από τη διαφήμιση.

2.3.11. Trust and other services

Μία ειδική κατηγορία στις υπηρεσίες εμπιστοσύνης (trust services) είναι οι εταιρίες πιστοποίησης καθώς και άλλες έμπιστες τρίτες οντότητες. Πηγές εσόδων αποτελούν οι συνδρομές, οι πωλήσεις λογισμικού, καθώς και οι πληρωμές για συμβουλευτικές υπηρεσίες. Ένα παράδειγμα ενός φορέα παροχής υπηρεσιών εμπιστοσύνης είναι η www.verisign.com.[10]

2.4. Τα πλεονεκτήματα του ηλεκτρονικού εμπορίου.

Όλα τα πλεονεκτήματα του ηλεκτρονικού εμπορίου μπορούν να συνοψιστούν με τη φράση: «Το ηλεκτρονικό εμπόριο μπορεί να αυξήσει τις πωλήσεις και να

[10] *«Certified e□Commerce Consultant» deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf*

μειώσει το κόστος». Επιπλέον, όμως μπορούμε να διακρίνουμε και τα παρακάτω θετικά:

- Παρέχει στους καταναλωτές έναν ακόμη μηχανισμό για ην αγορά προϊόντων και υπηρεσιών που λειτουργεί επί μονίμου βάσεως 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, 365 ημέρες το χρόνο, με το πλεονέκτημα ότι όλα μπορούν να γίνουν από την πολυθρόνα του σπιτιού τους ή του γραφείου τους.
- Παρέχει τη δυνατότητα πρόσβασης σε ένα ευρύ φάσμα πληροφοριών πραγματικού χρόνου
- Παρέχει τη δυνατότητα άμεσης σύγκρισης τιμών και χαρακτηριστικών των προϊόντων.
- Κάποια προϊόντα (π.χ. λογισμικό, φωτογραφίες κλπ)μπορούν να παραδοθούν απευθείας μέσω Διαδικτύου, χωρίς να απαιτείται η μεσολάβηση του ταχυδρομείου.
- Παρέχεται στους αγοραστές η δυνατότητα τακτικής λήψης πληροφοριών σχετικά με προϊόντα ή υπηρεσίες που τους ενδιαφέρουν.
- Αυξάνει την ταχύτητα και την ακρίβεια με την οποία οι επιχειρήσεις ανταλλάσσουν πληροφορίες.
- Μειώνει το κόστος συναλλαγών με την βοήθεια αυτοματοποιημένων επιχειρησιακών διαδικασιών
- Επεκτείνει τα γεωγραφικά όρια μιας επιχείρησης εισάγοντας την σε περιοχές που ήταν φυσικά μη προσβάσιμες στο παρελθόν.
- Αυξάνεται η γνώση μια επιχείρησης γύρω από τις επιθυμίες των πελατών της και
- Διευρύνει το πιθανό πελατολόγιο της επιχείρησης, αφού απευθύνεται σε ένα μεγαλύτερο αγοραστικό κοινό.

2.5. Μειονεκτήματα του ηλεκτρονικού εμπορίου

Ως βασικό μειονέκτημα μπορεί να θεωρηθεί το γεγονός ότι οι καταναλωτές δεν εμπιστεύονται πλήρως για τις συναλλαγές τους το Διαδίκτυο και διστάζουν να αποστείλουν τον αριθμό της πιστωτικής τους κάρτας. Παρόλο που τα περισσότερα ζητήματα ασφαλείας έχουν τώρα πι λυθεί μέσω συστημάτων κρυπτογράφησης και

πιστοποίησης, τα οποία αναλύονται στο κεφ.7, εν τούτοις δεν έχει ακόμη δημιουργηθεί εκείνο το κλίμα εμπιστοσύνης που θα πείσει τους καταναλωτές ότι οι συναλλαγές τους στο Διαδίκτυο είναι απόλυτα ασφαλείς. Επιπλέον μπορούμε να παρατηρήσουμε και κάποια ακόμη αρνητικά:

- Μερικές επιχειρήσεις είναι αδύνατον να ελεγχθούν ως προς την φερεγγυότητα και την αξιοπιστία τους.
- Τα πιο συνηθισμένα προϊόντα που διακινούνται μέσω Διαδικτύου είναι μικρά και ελαφριά αντικείμενα.
- Συνήθως απαιτούνται μεγάλα ποσά για τον εκσυγχρονισμό και την αναβάθμιση των τεχνολογιών που χρησιμοποιεί ένα ηλεκτρονικό κατάστημα.
- Υπάρχει δυσκολία ενσωμάτωσης των ήδη υπαρχόντων βάσεων δεδομένων που χρησιμοποιούν οι επιχειρήσεις για τις εμπορικές τους συναλλαγές.[11]

[11] *users.otenet.gr*

ΚΕΦΑΛΑΙΟ 3

3. ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

3.1. Γενικά

Στα συστήματα ηλεκτρονικών συναλλαγών εντάσσεται κάθε μέθοδος που χρησιμοποιείται για να εξυπηρετήσει την πραγματοποίηση αγορών μέσω του Internet. Ορίζοντας τις ηλεκτρονικές συναλλαγές με αυτό τον τρόπο, μπορούμε να συμπεριλάβουμε σε αυτές εκτός από τις αμιγώς ψηφιακές- και κάποιες παραδοσιακές μεθόδους. Έτσι, σύστημα ηλεκτρονικών συναλλαγών θεωρούνται όχι μόνο η χρήση πιστωτικών καρτών, το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές, αλλά και το έμβασμα, η αντικαταβολή, η μεταφορά χρημάτων σε λογαριασμό κ.ά. Κοινό χαρακτηριστικό των παραπάνω μεθόδων είναι ότι μπορούν να ενσωματωθούν στη λειτουργία ενός online καταστήματος εξυπηρετώντας τις αγοραπωλησίες και το εν γένει ηλεκτρονικό εμπόριο.

3.2. Τύποι συστημάτων πληρωμών

Υπάρχουν διεθνώς περισσότερα από 100 διαφορετικά συστήματα ηλεκτρονικών συναλλαγών, άλλα λιγότερο και άλλα περισσότερο επιτυχημένα.[12]

- **χρήση πιστωτικών καρτών**
- **προπληρωμένες κάρτες**
- **το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές,**
- **το έμβασμα,**
- **η αντικαταβολή**
- **η μεταφορά χρημάτων σε λογαριασμό κ.ά.**
- ***M-payment***
- **Επιταγές**

[12] *www.go-online.gr/ebusiness/specials/article.html?article_id=1331 - 28k – «Συστήματα ηλεκτρονικών συναλλαγών»*

3.2.1. Πιστωτικές κάρτες

Αποτελούν τον πιο συχνό τρόπο πληρωμής στο διαδίκτυο. Σύμφωνα με έρευνα του US Census Bureau το 2005, το 80% των online αγορών στις Ηνωμένες Πολιτείες έγιναν με χρήση πιστωτικής κάρτας.

Πρόκειται για δοκιμασμένη μέθοδο από τις παραδοσιακές αγορές, με την οποία είναι εξοικειωμένοι οι καταναλωτές. Η χρήση πιστωτικών καρτών σε ένα δικτυακό κατάστημα ακολουθεί την ίδια διαδικασία με τα πραγματικά καταστήματα.

Διαδικασία πληρωμής με πιστωτική κάρτα

Οι πιο δημοφιλείς πιστωτικές κάρτες είναι οι Visa, Diner's Club, MasterCard και American Express. Για να ενεργοποιηθεί η διαδικασία υποδοχής πληρωμών μέσω πιστωτικής από ένα ηλεκτρονικό κατάστημα, θα πρέπει αρχικά να υπάρχει συνεργασία με κάποια από τις εταιρείες εκτέλεσης δικτυακών πληρωμών μέσω πιστωτικών καρτών όπως η Cybercash ή η PaymentNet κ.α. Οι εταιρείες αυτές παρέχουν το απαραίτητο λογισμικό το οποίο θα πρέπει να εγκατασταθεί στον secure server της επιχείρησης προκειμένου να πραγματοποιηθούν οι συναλλαγές.

Μόλις ένας πελάτης πληκτρολογήσει τον αριθμό της πιστωτικής του κάρτας και τα υπόλοιπα στοιχεία που του ζητούνται και πατήσει το πλήκτρο επικύρωσης της συναλλαγής, ενεργοποιείται το λογισμικό της εταιρίας εκτέλεσης πληρωμών. Η διαδικασία είναι απόλυτα ασφαλής εφόσον πραγματοποιείται με ασφαλές (secure) πρωτόκολλο επικοινωνίας. Η διαδικασία ολοκληρώνεται όταν έρθει η επιβεβαίωση της συναλλαγής από την εταιρία πληρωμών. Με την ολοκλήρωση της συναλλαγής κατατίθενται από την εταιρία πληρωμών τα χρήματα στο λογαριασμό της επιχείρησής.[13]

Τέλος, όπως και στις παραδοσιακές πληρωμές μέσω πιστωτικής κάρτας, θα πρέπει να υπάρχει συνεργασία με μια τράπεζα για ένα λογαριασμό ειδικού τύπου.

Οι πιστωτικές κάρτες αποτελούν παγκοσμίως το δημοφιλέστερο μέσο διεκπεραίωσης συναλλαγών στο Διαδίκτυο. Η ευκολία στη χρήση τους, το γεγονός ότι επιτρέπουν στους εμπλεκομένους να συναλλάσσονται online χωρίς πολλές διατυπώσεις, όπως και το ότι μπορούν να χρησιμοποιηθούν για αγορές σε ολόκληρο τον κόσμο, τις καθιστούν το πιο ελκυστικό διαδικτυακό μέσο πληρωμής.

Παρουσιάζουν ωστόσο και ορισμένα μειονεκτήματα.

---

[13] *dspace.lib.uom.gr/bitstream/2159/3749/2/karakizosMsc2007.pdf*

1) ***Οι απάτες***, καθώς συχνά καταγράφονται κρούσματα μη εξουσιοδοτημένης χρήσης πιστωτικών καρτών στο Διαδίκτυο, υπεξαίρεσης αριθμών, υποκλοπής κωδικών κ.λπ.

2) ***Οι περιορισμοί στην απόκτησή τους***, καθώς ο κάτοχος θα πρέπει να έχει συμπληρώσει το 18ο έτος της ηλικίας του και να διαθέτει τραπεζικό λογαριασμό με κάποιο σεβαστό ποσό και την οικονομική άνεση για να πληρώνει συνδρομές, προμήθειες κ.λπ.

Παρά τις ανωτέρω ενστάσεις, η πρωτοκαθεδρία των πιστωτικών καρτών στις δικτυακές συναλλαγές δεν μπορεί να αμφισβητηθεί. Ελάχιστα είναι τα ηλεκτρονικά καταστήματα που δεν τις δέχονται ως μέσο πληρωμής. Σχεδόν το σύνολο των e-shops παγκοσμίως κάνουν αποδεκτές όλες τις κάρτες τύπου Visa και MasterCard, ενώ αρκετά ακόμη δέχονται και άλλα είδη καρτών (λ.χ. American Express). Οι πιστωτικές κάρτες μπορούν να εξυπηρετήσουν όλα τα είδη ηλεκτρονικών καταστημάτων και η ενσωμάτωσή τους στους τρόπους πληρωμής κρίνεται απαραίτητη.

Βασική προϋπόθεση ομαλής λειτουργίας είναι οι πληρωμές με πιστωτική κάρτα να πραγματοποιούνται σε περιβάλλον ασύμμετρης κρυπτογράφησης και υψηλής ασφάλειας 128 bit, έτσι ώστε τα κρίσιμα δεδομένα των καρτών να μη διαρρέουν. Υπεύθυνοι για αυτό είναι οι ιθύνοντες του ηλεκτρονικού καταστήματος, που οφείλουν να λαμβάνουν τις μέγιστες δυνατές προφυλάξεις.[14]

3.2.2. *Κάρτες προπληρωμένης αξίας*

Οι προπληρωμένες πιστωτικές κάρτες αποτελούν ένα καινούργιο προϊόν των χρηματοπιστωτικών ιδρυμάτων, που αποσκοπεί στην ενθάρρυνση των οικονομικών συναλλαγών μέσω Διαδικτύου.

Η φιλοσοφία των εν λόγω καρτών συνοψίζεται στο ότι ο χρήστης που θέλει να πραγματοποιήσει online αγορές προμηθεύεται από κάποιο τραπεζικό κατάστημα την κάρτα προκαταβάλλοντας την αξία της. "Αγοράζει" δηλαδή κάποιο ποσό, το οποίο και μπορεί να χρησιμοποιήσει για ηλεκτρονικές αγορές με την κάρτα, χωρίς διατυπώσεις και χωρίς την ύπαρξη τραπεζικού λογαριασμού.

Η διαδικασία απόκτησης και χρήσης αυτού του είδους καρτών είναι παρόμοια με τη διαδικασία απόκτησης και χρήσης μιας τηλεφωνικής κάρτας (τηλεκάρτας, χρονοκάρτας κ.λπ.) και έτσι ακόμη και ένας ανήλικος μπορεί να τις αποκτήσει και να τις χρησιμοποιήσει.

[14] *www.go-online.gr/ebusiness/specials/article.html?article_id=1332*

Μέχρι στιγμής, οι προπληρωμένες κάρτες που διατίθενται στην ελληνική αγορά είναι δύο: Η egnatia Prepay, από την Εγνατία Τράπεζα, και η Attica Gift Card Visa, από την Τράπεζα Αττικής, χωρίς να αποκλείεται σύντομα και άλλες τράπεζες να παρουσιάσουν κάποιο αντίστοιχο προϊόν.

Ειδικότερα, η egnatiaPrepay κοστίζει 100 ευρώ και επιτρέπει στον κάτοχό της να προβεί σε συνολικές αγορές ισόποσης αξίας, στα περίπου 20 ελληνικά ηλεκτρονικά καταστήματα, που κάνουν δεκτό (μέχρι τώρα) το συγκεκριμένο τρόπο πληρωμής.[15]

Εννοείται ότι ο ενδιαφερόμενος, για να ικανοποιήσει τις ανάγκες του, μπορεί να αγοράσει περισσότερες από μία κάρτες. Το κόστος της Attica Gift Card Visa ξεκινά από τα 50 ευρώ και φθάνει μέχρι και τα 3.000 ευρώ (πλέον μικρής τραπεζικής προμήθειας που βαρύνει τον αγοραστή της κάρτας) και επιτρέπει στον κάτοχό της την πραγματοποίηση αγορών ισόποσης αξίας σε όλα τα e-shops της Ελλάδας και του εξωτερικού που δέχονται πιστωτικές κάρτες τύπου Visa. Ουσιαστικά πρόκειται για μία πιστωτική Visa, με προκαθορισμένο από τον πελάτη χρηματικό απόθεμα.

Οι κάρτες αυτές κάρτες καλύπτουν ένα σημαντικό κενό στο χώρο των ηλεκτρονικών συναλλαγών, γιατί επιτρέπουν στον Έλληνα χρήστη να απολαύσει όλα τα θετικά που συνοδεύουν τη χρήση πιστωτικών καρτών, επιλέγοντας εκείνος το χρηματικό ποσό που θα κεφαλαιοποιήσει στην κάρτα του και χωρίς καμία τραπεζική δέσμευση. Πολύ περισσότερο, ακόμα και αν η κάρτα χαθεί ή υποκλαπούν τα στοιχεία της, το μόνο που μπορεί να απολέσει ο κάτοχος είναι το ποσό της κάρτας. Αν, φερ' ειπείν, χάσει κανείς την egnatiaPrepay, δεν πρόκειται να ζημιωθεί περισσότερο από την ονομαστική αξία (100 ευρώ).

Τα μειονεκτήματα του πρακτικού αυτού τρόπου πληρωμής είναι ελάχιστα. Για την κάρτα της Τράπεζας Εγνατία, το πρόβλημα εστιάζεται κυρίως στο ότι ο πελάτης μπορεί να πραγματοποιήσει τις αγορές του μόνο στα περίπου 20 εγχώρια ηλεκτρονικά καταστήματα που κάνουν αποδεκτή τη συγκεκριμένη κάρτα. Το γεγονός αυτό περιορίζει κάπως τους χρήστες και ενδεχομένως να λειτουργεί αποτρεπτικά. Πάντως, αφενός τα e-shops που αποδέχονται την egnatiaPrepay καλύπτουν μεγάλη προϊοντική γκάμα, αφετέρου αυξάνονται συνεχώς.

Η διαδικασία ενσωμάτωσης της μιας ή και των δύο καρτών στο ηλεκτρονικό σας κατάστημα είναι σχετικά απλή. Για τη μεν Attica Gift Card Visa ισχύει ό,τι και

[15] *www.go-online.gr/ebusiness/specials/article.html?article_id=1333*

για όλες τις συναλλαγές που γίνονται με πιστωτικές Visa. Για την egnatiaPrepay απαιτείται η διασύνδεση του ηλεκτρονικού καταστήματος με το σύστημα ηλεκτρονικών συναλλαγών "WebShop" της τράπεζας. Το σύστημα αυτό συνδέει το ηλεκτρονικό κατάστημα με τον server της Εγνατίας, όπου πραγματοποιείται η συναλλαγή σε περιβάλλον ασύμμετρης κρυπτογράφησης.

Για κάθε αγοραπωλησία, η τράπεζα παρακρατά από τον έμπορο περίπου ένα 3%, ενώ για τη χρήση του συστήματος απαιτείται ένα ποσό της τάξης των 150 ευρώ, σε ετήσια βάση, με τη σημείωση ότι τα μεγέθη αυτά είναι διαπραγματεύσιμα.[16]

3.2.3. Το ψηφιακό χρήμα και οι ηλεκτρονικές επιταγές

3.2.3.1. Το ψηφιακό χρήμα

Το ψηφιακό χρήμα είναι ένας μηχανισμός εξόφλησης μικροποσών μέσω του Internet. Ένας τέτοιος μηχανισμός μπορεί να αποτελέσει το επόμενο βήμα στις εφαρμογές ηλεκτρονικών πληρωμών. Σε ένα σύστημα ψηφιακού χρήματος, το νόμισμα δεν είναι τίποτα άλλο παρά μια σειρά από ψηφία.

Ένας χρήστης μπορεί να κάνει ανάληψη ψηφιακού χρήματος από μια τράπεζα μεταφέροντας το ποσό αυτό στον ηλεκτρονικό του υπολογιστή. Το ψηφιακό χρήμα που παραχωρείται από την τράπεζα σημαδεύετε κατάλληλα για λόγους εγκυρότητας και ασφάλειας. Σε περίπτωση αγοράς προϊόντων μέσω του Internet, ο αγοραστής αποστέλνει στον προμηθευτή το αντίτιμο σε ψηφιακό χρήμα. Ο τελευταίος με τη σειρά του, προωθεί στην τράπεζα τη ψηφιακή-ροή που έλαβε προκειμένου να διερευνηθεί κατά πόσο η ροή αυτή αποτελεί έγκυρη χρηματο-ροή ή όχι.

Για να διασφαλίσει ότι κάθε χρηματο-ροή (token) χρησιμοποιείται μόνο μια φορά, η τράπεζα καταγράφει τον σειριακό αριθμό κάθε token που ξοδεύεται. Αν ο σειριακός αριθμός του token υπάρχει ήδη στην βάση δεδομένων, τότε η τράπεζα έχει εντοπίσει κάποιον που προσπάθησε να χρησιμοποιήσει περισσότερες από μια φορές το token και θα, πληροφορήσει τον έμπορο ότι αυτή η χρηματική μονάδα είναι άχρηστη.

Μία εναλλακτική λύση που αναπτύχθηκε από την DigiCash επιτρέπει στους χρήστες να διατηρήσουν την ανωνυμία τους. Ο εν λόγω μηχανισμός, που ονομάζεται "blind signature", επιτρέπει στον αγοραστή να λάβει ηλεκτρονικό χρήμα από μια τράπεζα χωρίς η τράπεζα να μπορεί να συσχετίσει το όνομα του αγοραστή με τα

[16] *www.go-online.gr/ebusiness/specials/article.html?article_id=1333* <<*κάρτες προπληρωμένης αξίας*>>

tokens που του διανέμονται. Η τράπεζα πρέπει να εκτιμήσει το token που λαμβάνει από τον έμπορο, μέσο της ψηφιακής στάμπας που έχει αρχικά τοποθετηθεί στα tokens του χρήστη αλλά η τράπεζα δεν μπορεί να καταλάβει ποιος έκανε την πληρωμή.

3.2.3.2. Ηλεκτρονικές Επιταγές

Μία έντυπη επιταγή είναι ουσιαστικά μία εντολή μεταφοράς κεφαλαίων από ένα λογαριασμό σε έναν άλλο. Η εντολή αυτή αποστέλλεται αρχικά στον αποδέκτη των κεφαλαίων, ο οποίος με τη σειρά του, παρουσιάζει την επιταγή στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Μια ηλεκτρονική επιταγή έχει όλα τα χαρακτηριστικά που διαθέτει μια έντυπη επιταγή και χρησιμοποιείται σαν ένα μήνυμα προς την τράπεζα του αποστολέα για την μεταφορά κεφαλαίων από ένα λογαριασμό σε ένα άλλο. Σε αντιστοιχία, με την παραδοσιακή διαδικασία, η ηλεκτρονική επιταγή αποστέλλεται αρχικά στον αποδέκτη ο οποίος την υπογράφει και την προωθεί στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό.

Από άποψη ασφάλειας, η ηλεκτρονική επιταγή θεωρείται καλύτερη από την έντυπη επιταγή. Και αυτό, γιατί ο αποστολέας, μπορεί να προστατέψει τον εαυτό του από μία απάτη. Αυτό γίνεται με την κωδικοποίηση του αριθμού του λογαριασμού του με το δημόσιο κλειδί της τράπεζας, χωρίς έτσι να αποκαλύπτει τον αριθμό τον λογαριασμού του στον έμπορο.

Το FSTC αποτελεί μια συνεργασία, τραπεζών και πιστωτικών οργανισμών, που έχουν υλοποιήσει μια, ηλεκτρονική επιταγή. Στηριγμένη στην παραδοσιακή επιταγή, η επιταγή του FSTC επιτρέπει την ψηφιακή υπογραφή του αποδέκτη. Για την προσθήκη μεγαλύτερης ευελιξίας σε αυτό το σύστημα πληρωμών, το FSTC προσφέρει στους χρήστες διάφορες επιλογές επιταγών ανάλογα με τις ανάγκες του χρήστη. Οι ηλεκτρονικές επιταγές μπορούν να παραδοθούν είτε με άμεση παράδοση μέσο ενός δικτύου ή μέσο ηλεκτρονικού ταχυδρομείου. Σε κάθε περίπτωση, τα υπάρχοντα τραπεζικά κανάλια, μπορούν να εκκαθαρίσουν τις πληρωμές, μέσο των δικτύων τους. Κάτι τέτοιο οδηγεί σε μια ικανοποιητική αναβάθμιση της υπάρχουσας τραπεζικής υποδομής και του Internet.[17]

[17] *www.geocities.com/zak_gr_2000/ - 8k*

3.2.4. Αντικαταβολή

Η αντικαταβολή ως μέθοδος πραγματοποίησης εμπορικών συναλλαγών δεν αποτελεί, ως γνωστόν, κάποια νέα πρακτική ή καινοτομία. Πρόκειται για μία παλιά διαδικασία του φυσικού εμπορίου, που μπορεί να εξυπηρετήσει την ολοκλήρωση και των ηλεκτρονικών συναλλαγών.

Ο τρόπος λειτουργίας της βασίζεται στην ταυτόχρονη ("χέρι με χέρι") παράδοση του προϊόντος στον πελάτη και την πληρωμή (αντικαταβολή) του τιμήματος από τον τελευταίο στον υπάλληλο του καταστήματος, που εκτελεί συγχρόνως χρέη μεταφορέα και εισπράκτορα. Τα χαρακτηριστικά αυτά καθιστούν την αντικαταβολή ασφαλή συναλλακτική μέθοδο τόσο για τον πελάτη όσο και για τον προμηθευτή.

Τα πλεονεκτήματα της αντικαταβολής είναι πολλά και σημαντικά. Κατ' αρχάς, η συγκεκριμένη μέθοδος δεν απαιτεί πιστωτική κάρτα, συνεπώς ένα υπολογίσιμο ποσοστό των χρηστών που δεν διαθέτει πιστωτική κάρτα (και δεν επιθυμεί να αποκτήσει) έχει εναλλακτική λύση. Επιπλέον -όπως έχει επισημανθεί σε πληθώρα σχετικών ερευνών- ακόμη και ανάμεσα σε εκείνους που διαθέτουν και χρησιμοποιούν πιστωτική κάρτα στη φυσική ζωή, υπάρχει ένα υπολογίσιμο ποσοστό που διστάζει να κάνει χρήση της κάρτας του στο Internet.

Ο φόβος για πιθανή απώλεια χρημάτων, προσωπικών δεδομένων, κωδικών κ.λπ. λειτουργεί αποτρεπτικά στους κατόχους όταν πρόκειται για αγορές μέσω Διαδικτύου. Ξεκινώντας από αυτήν τη διαπίστωση, η αντικαταβολή "θεραπεύει" την ανασφάλεια και συντελεί στη διεύρυνση του αγοραστικού κοινού και κατ' επέκταση της αγοράς. Την ίδια ώρα, ο πελάτης μπορεί να αισθάνεται βέβαιος ότι η πιστωτική του κάρτα ούτε θα υποκλαπεί ούτε θα πληρώσει προκαταβολικά για κάτι που μπορεί να μην του παραδοθεί ποτέ.

Επιπλέον, η εγκατάσταση και λειτουργία της μεθόδου της αντικαταβολής είναι εύκολη και φθηνή.

Εύκολη, γιατί το μόνο που χρειάζεται είναι η τοποθέτηση μιας απλής φόρμας παραγγελιών στο ηλεκτρονικό κατάστημα, όπου θα ζητούνται τα βασικά στοιχεία του πελάτη (ονοματεπώνυμο, διευθύνσεις, τηλέφωνα επικοινωνίας), τα οποία οι υπάλληλοι θα χρησιμοποιούν για να επιβεβαιώσουν την παραγγελία. Είναι αυτονόητο ότι το ηλεκτρονικό σας κατάστημα μπορεί να προβαίνει σε διασταύρωση των στοιχείων του πελάτη για την ορθότητά τους, στο μέτρο που δεν παραβαίνει το διεθνές και εγχώριο Δίκαιο.

Φθηνή, γιατί σε σύγκριση με τη χρήση κάποιου άλλου συστήματος (όπου θα έπρεπε να καταβληθούν χρήματα ως προμήθεια σε τραπεζικούς ή λοιπούς χρηματοοικονομικούς φορείς), τα λειτουργικά έξοδα που απαιτούνται για την είσπραξη των χρημάτων από τον πελάτη αποσοβούνται πλήρως, εφόσον ο μεταφορέας/παραδίδων είναι και εισπράκτορας.

Πέρα από τα ανωτέρω θετικά, η μέθοδος της αντικαταβολής παρουσιάζει και ορισμένες αδυναμίες. Εκτός του αναχρονιστικού της χαρακτήρα, στις περιπτώσεις εκείνες που το παρεχόμενο προϊόν δεν είναι κάποιο αντικείμενο αλλά μια άυλη υπηρεσία, π.χ. συνδρομή σε κάποιο online μέσο, η αντικαταβολή δεν είναι η κατάλληλη μέθοδος, γιατί και ο πελάτης θα πρέπει να περιμένει αρκετά μέχρι να πληρώσει το αντίτιμο και να αποκτήσει το αγαθό, και ο πάροχος/έμπορος επιβαρύνεται με το λειτουργικό κόστος που απαιτείται για την είσπραξη του αντιτίμου (ανθρωποώρες, μεταφορικά κ.ά.).

Στο ίδιο πλαίσιο, η αντικαταβολή σε διεθνείς προορισμούς επιβαρύνει με σημαντικό κόστος τα προϊόντα γιατί στην όλη διαδικασία εμπλέκονται αρκετοί μεσάζοντες. Για παράδειγμα, η τιμή πώλησης ενός προϊόντος με αντικαταβολή, από την Ελλάδα που βρίσκεται το ηλεκτρονικό κατάστημα στις Ηνωμένες Πολιτείες που βρίσκεται π.χ. ο πελάτης, επιβαρύνεται με σημαντικά λειτουργικά έξοδα που προκύπτουν από την εμπλοκή των διαφόρων μεσαζόντων, αλλά και με δυσλειτουργίες (λ.χ. καθυστερήσεις) που προκύπτουν από την ίδια αιτία.

Συμπερασματικά, η αντικαταβολή προκρίνεται ως μέθοδος συναλλαγών για αγοραπωλησίες υλικών αγαθών εντός της χώρας. Στον αντίποδα, η αντικαταβολή δεν ενδείκνυται για πώληση προϊόντων σε διεθνείς προορισμούς, όπως επίσης και για πώληση άυλων προϊόντων και υπηρεσιών.

3.2.5. Κατάθεση σε λογαριασμό, έμβασμα και μεταφορά

Η κατάθεση χρημάτων σε λογαριασμό τρίτου, το έμβασμα και η μεταφορά επί πιστώσει σε λογαριασμό τρίτου μέσω της φυσικής ή ηλεκτρονικής τραπεζικής (e-banking) είναι οι πιο γνωστές από αυτές. Για την ενσωμάτωση των τριών αυτών συναλλακτικών μεθόδων στη λειτουργία του ηλεκτρονικού καταστήματος, αρκεί ο έμπορος να ενημερώσει τον πελάτη για τον αριθμό λογαριασμού όπου επιθυμεί να πιστωθούν ή να κατατεθούν τα χρήματα. Προκειμένου να εξυπηρετηθεί ο πελάτης, πρέπει να συμπληρώσει την ηλεκτρονική φόρμα και να καταθέσει (ή να μεταφέρει)

τα χρήματα στο λογαριασμό που θα του υποδειχθεί. Για την ολοκλήρωση της παραγγελίας, χρειάζεται η τράπεζα του παρόχου να επιβεβαιώσει την κατάθεση των χρημάτων.

Οι εν λόγω τρόποι συναλλαγής για ηλεκτρονικές αγορές είναι και οι λιγότερο ελκυστικοί τόσο για τους καταναλωτές όσο και για τους εμπόρους για μια σειρά από λόγους. Καθυστέρηση ολοκλήρωσης συναλλαγής (καθώς απαιτείται επιβεβαίωση από την τράπεζα), δαπάνη χρόνου για τον καταναλωτή (όταν πρόκειται για καταθέσεις μέσω της φυσικής οδού), οικονομικές επιβαρύνσεις από τις τράπεζες (ειδικά στα εμβάσματα αλλά και στις μεταφορές χρημάτων) είναι ορισμένοι από αυτούς. Εντούτοις, οι παραπάνω μέθοδοι μπορούν να φανούν αρκετά εξυπηρετικές όταν το προϊόν είναι άϋλο και αφορά στην παροχή υπηρεσιών. Για παράδειγμα, η κράτηση ενός δωματίου από τον πελάτη στο δικτυακό τόπο ενός ξενοδοχείου ή, άλλο παράδειγμα, η δυνατότητα απόκτησης δικαιώματος πρόσβασης σε κάποιο συνδρομητικό site, μπορεί να πραγματοποιηθεί εύκολα με τη συμπλήρωση της σχετικής φόρμας ενδιαφέροντος και είτε με τη χρήση πιστωτικής κάρτας είτε με κατάθεση χρημάτων για την ολοκλήρωσή της.[18]

3.2.6. *M-payment*

Κινητό εμπόριο (M-commerce) είναι κάθε είδους ηλεκτρονικής συναλλαγής που περιλαμβάνει την αγορά προϊόντων ή υπηρεσιών μέσω ασύρματων, φορητών συσκευών όπως είναι τα κινητά τηλέφωνα, τα PDA κ.α.

M-payment ή πιο σύντομα mobile-payment, είναι μία πληρωμή που μπορεί να γίνει και από συσκευή κινητού τηλεφώνου ή από κάποιο PDA

Η κινητή τηλεφωνία και το Internet αποτέλεσαν τα κύρια σχήματα της Ευρωπαϊκής Βιομηχανίας τηλεπικοινωνιών την τελευταία δεκαετία και χωρίς αμφιβολία είχαν μεγάλη επίδραση στο σύγχρονο επιχειρείν. Νέες τεχνολογίες όπως το GPRS (General Packet Radio Service) και το UMTS (Universal Mobile Telecommunications System) επέτρεψαν την ανάπτυξη μιας σειράς νέων υπηρεσιών προστιθέμενης αξίας μέσω ασυρμάτων ευρυζωνικών συνδέσεων. Παράλληλα, μια σειρά από άλλες ενσύρματες και ασύρματες τεχνολογίες επικοινωνίας αναπτύχθηκαν με την συνεπακόλουθη δημιουργία νέων επιχειρησιακών μοντέλων στο χώρο.

[18] *www.go-online.gr/ebusiness/specials/article.html?article_id=1334*

Σε αυτό το κλίμα όλοι οι αναλυτές συγκλίνουν στην άποψη ότι το κινητό ηλεκτρονικό εμπόριο (M-commerce) βρίσκεται σε ένα κρίσιμο σταυροδρόμι τόσο σε Ευρωπαϊκό όσο και παγκόσμιο επίπεδο[19].

[19] *Richard I. Hillman & Kane Wong (2000), «Electronic Banking», Diane Publishing Co.*

ΜΕΡΟΣ Β΄

ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΚΕΦΑΛΑΙΟ 4

4. ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ – e-banking

4.1. Τι είναι e-banking

Η ηλεκτρονική τραπεζική (e-banking) είναι ένα σχετικά νέο εναλλακτικό τραπεζικό κανάλι. Είναι μία αυτοματοποιημένη παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών, απευθείας στους πελάτες, μέσω ηλεκτρονικών, αλληλεπιδραστικών καναλιών επικοινωνίας.

Περιλαμβάνει τα συστήματα που επιτρέπουν σε οικονομικούς οργανισμούς, ιδιώτες και επιχειρήσεις να έχουν πρόσβαση σε λογαριασμούς, να πραγματοποιούν ποικίλες χρηματοοικονομικές συναλλαγές και να λαμβάνουν χρήσιμες πληροφορίες για σχετικά προϊόντα και υπηρεσίες μέσω δημόσιων ή ιδιωτικών δικτύων, συμπεριλαμβανόμενου του Internet.

Στην Ελλάδα πρωτοεμφανίσθηκε το 1997 από την Εγνατία τράπεζα, περιλαμβάνοντας αρχικά πληροφοριακές συναλλαγές, δηλαδή ερώτηση υπολοίπου, μικρή κατάσταση λογαριασμών και μεταφορές κεφαλαίων εντός της τράπεζας. Κατόπιν ακολούθησαν και οι υπόλοιπες τράπεζες του εσωτερικού. Σήμερα υπηρεσίες ηλεκτρονικής τραπεζικής διαθέτει η πλειοψηφία των εγχώριων τραπεζικών οργανισμών[20].

Τράπεζες που προσφέρουν υπηρεσίες e-banking στην Ελλάδα είναι οι ακόλουθες:

- Η Aspis bank, http://www.aspisbank.gr/
- Η Alpha bank, http://www.alpha.gr/Alpha Web Banking
- Η Citibank, http://www.citibank.gr/ Citibank Online
- Η Εγνατία τράπεζα, http://www.egnatiabank.gr/
- Η Εθνική τράπεζα , http://www.nbg.gr/
- Η Εμπορική τράπεζα, http://www.combank.gr/ Emporiki e.Banking
- Η Eurobank-Ergasias, http://www.eurobank.gr/

[20] *Αγγελής Γ.Β(2005) «Η βίβλος του E-BANKING» κεφ.2*

http://www.ebusinessforum.gr/taxidistointernet/moneyandother/index.php?language=el

- Η Τράπεζα Κύπρου, http://www.bankofcyprus.gr/
- Η Λαϊκή τράπεζα, http://www.laiki.gr/
- Η Nova bank, http://www.novabank.gr/
- Η Winbank-Πειραιώς, http://www.winbank.gr/
- Η HSBC, http://www.hsbc.gr.[21]

4.2. Εγγραφή στο e-banking

Η διαδικασία εγγραφής ενός πελάτη τράπεζας, σε υπηρεσίες e- banking, έχει απλοποιηθεί τα τελευταία χρόνια. Οι περισσότεροι πιστεύουν πως η διαδικασία είναι χρονοβόρα, η αλήθεια είναι πως δεν παίρνει περισσότερο από μερικά λεπτά. Παρακάτω αναφέρονται όλες οι προϋποθέσεις και απαιτήσεις που χρειάζονται για να εγγραφή κάποιος σε ηλεκτρονικές υπηρεσίες.

4.2.1. Προϋποθέσεις εγγραφής

Οι απαραίτητες προϋποθέσεις για την πραγματοποίηση ηλεκτρονικών συναλλαγών είναι:

[21] *www.in.gr*

- Ο χρήστης να είναι πελάτης της τράπεζας, δηλαδή να διατηρεί τραπεζικό λογαριασμό σε αυτήν. Εξαιρέσεις αποτελούν υπηρεσίες που έχουν να κάνουν περισσότερο με ηλεκτρονικό εμπόριο, όπως η υπηρεσία προπληρωμένης κάρτας άμεσων αγορών στο διαδίκτυο egnatiaPrepay και η υπηρεσία πληρωμής και κράτησης εισιτηρίων θεαμάτων, τις οποίες προσφέρει η ΕΓΝΑΤΙΑ Τράπεζα, η υπηρεσία easy pay που προσφέρει η Τράπεζα ΠΕΙΡΑΙΩΣ που είναι υπηρεσία ηλεκτρονικών πληρωμών με χρήση πιστωτικής κάρτας, η υπηρεσία open24 του ομίλου Eurobank, που είναι και οι πλέον γνωστές. Κοινό χαρακτηριστικό των προαναφερόμενων συναλλαγών είναι ότι ο χρήστης μπορεί να πραγματοποιεί ηλεκτρονικές πληρωμές, με την χρήση πιστωτικής κάρτας ή προπληρωμένης κάρτας, χωρίς να είναι απαραίτητα πελάτης της τράπεζας.

- Ο χρήστης να είναι άνω των 18 ετών, με κάποιες μικρές εξαιρέσεις, που υπάρχουν στον χώρο του e-Commerce.

- Ο χρήστης να διαθέτει ηλεκτρονικό υπολογιστή που να πληροί τις ελάχιστες τεχνικές απαιτήσεις, σε υλικό και λογισμικό που θέτει η τράπεζα, την οποία έχει επιλέξει για να πραγματοποιεί ηλεκτρονικά τις συναλλαγές του, και βέβαια να διαθέτει σύνδεση στο διαδίκτυο.

Από την στιγμή που τηρούνται οι παραπάνω προϋποθέσεις, μπορεί οποιοσδήποτε να εγγραφεί στις υπηρεσίες ηλεκτρονικής τραπεζικής. Η εγγραφή ενός ιδιώτη ή μιας εταιρίας γίνεται δωρεάν από την πλειοψηφία των ελληνικών τραπεζών. Επίσης η εγγραφή γίνεται με την συμπλήρωση μιας αίτησης είτε στην τράπεζα είτε ηλεκτρονικά από τον υπολογιστή σου και να την αποστείλει ηλεκτρονικά, ωστόσο η επίσκεψη στην τράπεζα είναι απαραίτητη για την υπογραφή της αίτησης.

Μετά από μερικά λεπτά ή μερικές μέρες ο χρήστης παραλαμβάνει τους κωδικούς πρόσβασης στις υπηρεσίες της ηλεκτρονικής τραπεζικής, δηλαδή το όνομα χρήστη και τον προσωπικό κωδικό αναγνώρισης. Με την χρήση των κωδικών και πολλών άλλων μέτρων ασφαλείας που λαμβάνουν οι τράπεζες, ο πελάτης έχει πιστοποιημένη πρόσβαση στις ηλεκτρονικές υπηρεσίες.

4.3. Πρόσβαση στο e-banking

Το e-banking (ή Internet banking) υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές. Μεταφέρει την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου, με άμεση πρόσβαση στους τραπεζικούς λογαριασμούς, παρέχοντας τη δυνατότητα διεκπεραίωσης συναλλαγών, εντολές αγοραπωλησίας μετοχών, παραγγελία μπλοκ επιταγών και πληροφορίες για συνάλλαγμα, πληρωμές λογαριασμών κινητής και σταθερής τηλεφωνίας, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ, ΔΕΗ και πιστωτικών καρτών, καθώς και πλήθος άλλων υπηρεσιών εύκολα, γρήγορα 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) το όφελος είναι ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος, ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος. Με το e-banking οι τραπεζικές υπηρεσίες προσφέρονται ανά πάσα στιγμή, ο δε καταναλωτής μπορεί να ενημερωθεί για κάθε προϊόν ή υπηρεσία ανέξοδα και χωρίς χρόνους αναμονής

Για την πρόσβαση τώρα στις διαθέσιμες υπηρεσίες οι πελάτες μπορούν να χρησιμοποιήσουν έξυπνες ηλεκτρονικές συσκευές, όπως προσωπικούς υπολογιστές, υπολογιστές χειρός (PDA), ATM ακόμη και κινητά τηλέφωνα.

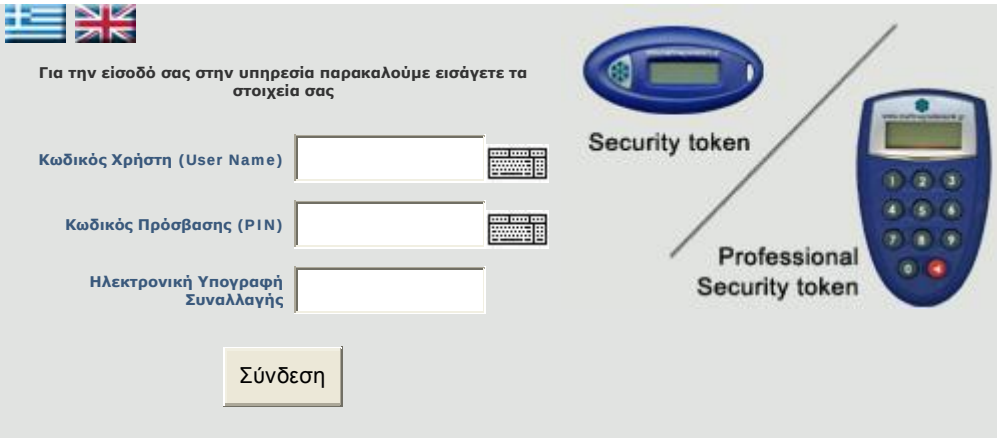
Ο ανταγωνισμός έχει συμβάλει στη βελτίωση των παρεχόμενων υπηρεσιών e-banking, όπως έγκριση δανείων, άνοιγμα λογαριασμών, ηλεκτρονικές πληρωμές, portals με χρηματοοικονομικό περιεχόμενο, προσαρμοσμένο στις προτιμήσεις κάθε πελάτη, συναλλαγές B2B (Business To Business) κ.ά.[22]

Για να αποκτήσουμε πρόσβαση στην υπηρεσία e-Banking, είναι απαραίτητο να είμαστε κάτοχοι μιας οποιασδήποτε κάρτας της τράπεζας που θα κάνουμε την συναλλαγή (αναλήψεων, πιστωτικής, κτλ). Με την πρώτη μας είσοδο, θα μας ζητηθεί να δηλώσουμε ένα **Username** της αρεσκείας μας, το οποίο θα χρησιμοποιούμε στο εξής για την είσοδο μας στο e-Banking.

Το δεύτερο στοιχείο ταυτοποίησης είναι ο προσωπικός κωδικός πρόσβασης (password), μοναδικός για κάθε χρήστη της υπηρεσίας. Ο συνδυασμός αριθμού κάρτας και **Password** παρέχει πρόσβαση στις ενημερωτικές υπηρεσίες του e-Banking (πληροφορίες, υπόλοιπα και κινήσεις λογαριασμών, καρτών, δανείων,

[22] *«Certified e□Commerce Consultant» deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf*

χρηματοοικονομική ενημέρωση, κ.α.) αλλά και στη διενέργεια συναλλαγών στις οποίες είτε είμαστε ο ίδιος δικαιούχος του λογαριασμού στον οποίο μεταφέρονται τα χρήματα είτε η μεταφορά αφορά σε πληρωμή οφειλών σας π.χ. ΔΕΗ, δόση δανείου κ.λπ.



https://ebanking.marfinegnatiabank.gr/

Για τη διενέργεια συναλλαγών στις οποίες ο παραλήπτης δεν είναι γνωστός και συνεπώς εμπεριέχουν ρίσκο (πχ. μεταφορές σε τρίτους, εμβάσματα), η Τράπεζα δεν αρκείται σε αυτό το επίπεδο ταυτοποίησης του χρήστη αλλά απαιτεί μια επιπλέον δικλείδα ασφαλείας, **την ψηφιακή πιστοποίηση**. Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί το μέσο που παρέχει τη δυνατότητα στον κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-Banking. Για την έκδοση προσωπικού ψηφιακού πιστοποιητικού, απαιτείται ο κωδικός έκδοσης πιστοποιητικού (Certificate).

Για να αποκτήσουμε κωδικούς για την υπηρεσία e-Banking (password & certificate) πρέπει να υποβάλλουμε Τράπεζα τη σχετική «Αίτηση και τους Όρους Διενέργειας Συναλλαγών μέσω Ηλεκτρονικών Δικτύων»[23].

[23] *Αγγελής Γ.Β(2005) «Η βίβλος του E-BANKING»*

Email ενημέρωσης αίτησης πιστοποιητικού

Subject: OpenCA Certificate and PIN information
From: ca@ntua.gr
To: csiat@noc.ntua.gr
Date: Mon, 6 Dec 2004 15:45:54 +0200 (EET)

Αγαπητέ χρήστη,
το πιστοποιητικό σας με Αύξοντα Αριθμό Α/Α 18 και Διακεκριμένο Όνομα (DN)

serialNumber=18,CN=CHRISTOS SIATERLIS,OU=people,O=ntua,C=gr

δημιουργήθηκε με επιτυχία.

Παρακαλούμε εισάγετε αρχικά το πιστοποιητικό της Αρχής Πιστοποίησης (Α.Π.) στο σύστημα σας ακολουθώντας τους συνδέσμους "Πληροφορίες Α.Π.", "Πιστοποιητικό Α.Π." από το δικτυακό τόπο της Α.Π.:

https://ca.ntua.gr/

Για την παραλαβή του πιστοποιητικού σας από τον δικτυακό τόπο της Α.Π, παρακαλούμε χρησιμοποιήστε τον Α/Α στην φόρμα που εμφανίζεται ακολουθώντας τους συνδέσμους "Χρήστες", "Παραλαβή Πιστοποιητικού". Εναλλακτικά μπορείτε επίσης να εισάγετε το πιστοποιητικό στον browser σας αυτόματα αν επισκεφτείτε:

https://ca.ntua.gr/cgi-bin/pub/pki?cmd=getcert&key=18&type=CERTIFICATE

Παρακαλούμε να κρατήσετε ένα ασφαλές αντίγραφο του προσωπικού σας κλειδιού. Σε περίπτωση απώλειας του δεν μπορεί να ανακτηθεί.

Τέλος για να ελέγξετε την εγκυρότητα και τη σωστή εγκατάσταση του πιστοποιητικού στο σύστημα σας, μπορείτε να ακολουθήσετε τους συνδέσμους "Χρήστες", "Έλεγχος Πιστοποιητικού".

Ευχαριστούμε πολύ,
Υπηρεσία Αρχής Πιστοποίησης ΕΜΠ (NTUA.GR)

4.4. Ηλεκτρονική ή ψηφιακή υπογραφή και η προστασία του καταναλωτή

Με τον όρο Ηλεκτρονική η Ψηφιακή υπογραφή εννοούμε δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.

Η Ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του περιεχομένου των ηλεκτρονικών εγγράφων

Έχει από τη μία επιβεβαιωτική λειτουργία βοηθώντας τον παραλήπτη να βεβαιωθεί ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις και από την άλλη εμπιστευτική λειτουργία, όπου μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα και όχι ανεπιθύμητοι τρίτοι.

Η ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή πρέπει να πληροί τους εξής όρους:

α) Να συνδέεται μονοσήμαντα με τον υπογράφοντα,

β) Να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος

γ) Να δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και

δ) Να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Η ηλεκτρονική υπογραφή έχει την ίδια ισχύ με την ιδιόχειρη υπογραφή;

Σύμφωνα με το άρθρο 3 του Προεδρικού Διατάγματος 150/2001 η ψηφιακή υπογραφή εξομοιώνεται με την ιδιόχειρη. Η ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.[24]

Στην περίπτωση που η εταιρεία έχει επιλέξει ανώτατο ημερήσιο όριο συναλλαγών ανά χρήστη άνω των 200.000 Ευρώ, το πιστοποιητικό του χρήστη εγκαθίσταται στην ειδική συσκευή eToken την οποία του αποστέλλει η Τράπεζα. Το eToken περιέχει έναν κρυπτογραφικό μηχανισμό ο οποίος όταν συνδεθεί με οποιονδήποτε υπολογιστή παρέχει τη δυνατότητα στον κάτοχό του να δημιουργήσει και να αποθηκεύσει σε αυτό το ψηφιακό του πιστοποιητικό.

Το πλεονέκτημα του eToken είναι η αυξημένη **ευελιξία** που παρέχει, διότι ο κάτοχος του έχει τη δυνατότητα χρήσης του σε περισσότερους από έναν υπολογιστές.

Το eToken είναι μια ειδική συσκευή στο μέγεθος ενός κλειδιού, η οποία περιέχει έναν κρυπτογραφικό μηχανισμό που δίνει τη δυνατότητα στον κάτοχό του να δημιουργήσει και να αποθηκεύσει το απαραίτητο λογισμικό ώστε να λειτουργεί σαν την ηλεκτρονική του υπογραφή. Όταν συνδεθεί με οποιονδήποτε υπολογιστή μέσω της USB θύρας, το eToken δίνει στον χρήστη τη δυνατότητα να υπογράφει ψηφιακά όλες τις προσωπικές του συναλλαγές. Έτσι, μέσω της προσωπικής ταυτοποίησης επιτυγχάνεται η μέγιστη δυνατή παροχή ασφάλειας. Η χρήση του είναι απαραίτητη σε οποιαδήποτε χρηματική συναλλαγή επιχειρήσετε μέσα από το e-Banking, από μεταφορά χρημάτων μεταξύ λογαριασμών μέχρι εκτέλεση διάφορων πληρωμών[25].

[24] *www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=98 - 32k*

[25] PC MAGAZINE, (2005), τεύχ.3, άρθρο με θέμα: «Οι καλύτερες λύσεις για προστασία στο Internet»

4.5. Δυνατότητες του e-banking

Οι ηλεκτρονικές συναλλαγές προσφέρουν μεγάλη ποικιλία υπηρεσιών στον Έλληνα χρήστη.

4.5.1. Internet Banking

Το Internet Banking είναι η σπουδαιότερη ηλεκτρονική συναλλαγή. Οι υπηρεσίες που προσφέρει χωρίζονται σε τέσσερις μεγάλες κατηγορίες:

- Οικονομικές συναλλαγές
- Πληροφοριακές συναλλαγές
- Αιτήσεις
- Άλλες υπηρεσίες[26]

4.5.1.1. Οικονομικές συναλλαγές

Οικονομικές συναλλαγές εννοούμε όλες τις συναλλαγές που μπορεί να κάνει ο συναλλασμένος στο ταμείο της τράπεζας. Όπως: μεταφορές κεφαλαίων, πληρωμή καρτών και δανείων, συναλλαγές που κατόπιν συμφωνιών της τράπεζας με τρίτο οργανισμό (πληρωμές εταιρειών σταθερής και κινητής τηλεφωνίας και συναλλαγές που υλοποιούνται στα πλαίσια διατραπεζικών συστημάτων, κυρίως της ΔΙΑΣ Α.Ε. και άλλων όπως το σύστημα «ΕΡΜΗΣ»).

4.5.1.1.1. Μεταφορές εντός Τράπεζας

Τις μεταφορές εντός της τράπεζας τις χωρίζουμε σε:

- ***μεταφορές σε λογαριασμό ιδίο***υ: εκτελούνται on – line (άμεσα). Ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και τον τραπεζικό λογαριασμό πίστωσης. Πολλές τράπεζες εμφανίζουν και το τρέχον διαθέσιμο υπόλοιπο που έχει ο χρήστης, διευκολύνοντάς τον ώστε να ξέρει ανά πάσα στιγμή πόσα έχει.
- ***Μεταφορές σε λογαριασμό τρίτου***: εκτελούνται on – line (άμεσα).
- ***Εμβάσματα εσωτερικού***: τα περισσότερα εμβάσματα εσωτερικού διεκπεραιώνονται μέσω του διατραπεζικού συστήματος DIASTRANSFER.

[26] *Αγγελής Γ.Β(2005) «Η βίβλος του E-BANKING»*

- ***Εμβάσματα εξωτερικού***: είναι εμβάσματα που αποστέλλονται σε τράπεζες εξωτερικού και συνήθως η μεταφορά τους χρειάζεται αρκετές εργάσιμες ημέρες.
- ***Πληρωμές δανείων***: είναι συναλλαγή μεταφοράς εντός τράπεζας και εκτελείται επίσης on – line.
- ***Πληρωμές πιστωτικών καρτών:*** Διακρίνονται σε τρεις κατηγορίες: α) Πληρωμή πιστωτικής κάρτας ιδίου, β) Πληρωμή πιστωτικής κάρτας τρίτου και πληρωμή πιστωτικής κάρτας άλλης τράπεζας.

4.5.1.1.2. Πληρωμές Δημοσίου

Οι συναλλασσόμενοι μπορούν να πληρώνουν πολλές υποχρεώσεις τους έναντι του Δημοσίου μέσω e-banking όπως: ΦΠΑ, εργοδοτικές εισφορές π.χ. ΙΚΑ, Ασφαλιστικές εισφορές π.χ. ΤΕΒΕ, είσπραξη φόρου εισοδήματος φυσικών προσώπων, τέλη κυκλοφορίας, πληρωμές λογαριασμών ΔΕΚΟ, ΟΤΕ, ΔΕΗ, ΕΥΔΑΠ,

4.5.1.1.3. Πληρωμές κινητής τηλεφωνίας

Κάποιες από τις πληρωμές λογαριασμών σταθερής και κινητής τηλεφωνίας παρέχονται μέσω του διατραπεζικού συστήματος DIAS DEBIT και άλλες είναι προϊόν διμερούς συμφωνίας μεταξύ τραπεζών και εταιριών. Π.χ. Cosmote, Vodafone, TIM, Q Telecom, Forthnet, Tellas, Alphyra Hellas, Πληρωμή Ανανέωσης Χρόνου Ομιλίας Καρτοκινητής Vodafone.

4.5.1.1.4. Πληρωμές Ασφαλιστικών

Κατόπιν συμφωνίας μεταξύ ασφαλιστικών εταιρειών και τραπεζών πολλοί πελάτες τους έχουν την δυνατότητα να πληρώνουν τα ασφάλιστρά τους μέσω αυτών (π.χ. εταιρεία ALLIANZ).

4.5.1.1.5. Πληρωμές Τρίτων

Αρκετές εταιρείες κατόπιν συμφωνίας που συνάπτουν με την τράπεζα που συνεργάζονται, προσφέρουν την δυνατότητα στους πελάτες τους να πληρώνουν τις υποχρεώσεις τους μέσω των υπηρεσιών της τράπεζας.

4.5.1.1.6. Μαζικές πληρωμές – Μισθοδοσίες

Πολλές εταιρίες και οργανισμοί εκτελούν τις μισθοδοσίες ή τις μαζικές πληρωμές που έχουν να κάνουν μέσω τραπέζης. Οι τράπεζες ορίζουν μία σταθερή γραμμογράφηση ascii αρχείου που περιλαμβάνει μία γραμμή επικεφαλίδας και τις γραμμές των συναλλαγών.

4.5.1.1.7. Κατάσταση Εντολών

Επίσης το internet banking προσφέρει στον συναλλασσόμενο την δυνατότητα να ενημερώνεται εύκολα για την κατάσταση των οικονομικών του. Μία εντολή που καταχωρείται μέσα στο internet μπορεί να περάσει από διάφορες καταστάσεις, έτσι είναι καλό να ενημερώνεται για την κατάσταση των συναλλαγών του και να γνωρίζει ποιες εντολές δεν εκτελέστηκαν.

4.5.1.1.8. Προμήθειες Συναλλαγών

Ένα βασικό πλεονέκτημα των ηλεκτρονικών συναλλαγών είναι οι μειωμένες τους προμήθειες.

Είναι καλό ο χρήστης πριν ξεκινήσει τις οικονομικές συναλλαγές μέσω του Internet να ενημερώνεται για τις προμήθειες των συναλλαγών. Λόγω του μεγάλου ανταγωνισμού οι τράπεζες δεν χρεώνουν προμήθεια στις μεμονωμένες μεταφορές κεφαλαίου εντός της τράπεζας και στις πληρωμές Δημοσίου.

4.5.1.2. Πληροφοριακές συναλλαγές

Ο συναλλασσόμενος έχει την δυνατότητα να πάρει πληροφορίες για όλα τα προϊόντα που διαθέτει στην τράπεζα. Αυτές οι συναλλαγές χωρίζονται σε τέσσερις μεγάλες κατηγορίες:

- πληροφορίες λογαριασμών
- πληροφορίες πιστωτικών καρτών
- πληροφορίες επιταγών
- πληροφορίες δανείων

4.5.1.3. Αιτήσεις

Οι συναλλασσόμενοι έχουν την δυνατότητα να κάνουν ηλεκτρονικές αιτήσεις για τα περισσότερα των προϊόντων τους. Π.χ. αίτηση ανοίγματος λογαριασμού,

αίτηση για δάνειο, αίτηση για παραγγελία συναλλάγματος, αίτηση παραγγελίας μπλοκ επιταγών.[27]

4.5.1.4. Βοηθητικές υπηρεσίες

Πολλές τράπεζες προσφέρουν στο site τους υπηρεσίες για να διευκολύνουν την ενημέρωση των ενδιαφερομένων γενικά και όχι μόνο των πελατών τους π.χ. υπολογισμός IBAN (διεθνή μορφή λογαριασμού), μετατροπή νομισμάτων, υπολογισμός δόσεων δανείων.

4.5.2. Phone Banking

Μέσω του phone banking οι πελάτες της τράπεζας έχουν την δυνατότητα να πραγματοποιούν τραπεζικές συναλλαγές χρησιμοποιώντας τηλέφωνο (σταθερό ή κινητό) όλο το 24ωρο.

Έχουν τη δυνατότητα εξυπηρέτησης μέσω:

- του συστήματος προ-μαγνητοφωνημένων μηνυμάτων (IVR) όπου πιστοποιείται ο χρήστης χωρίς παρέμβαση ανθρώπινου παράγοντα πληκτρολογώντας τους κωδικούς στη συσκευή τηλεφώνου.
- του εξειδικευμένου αντιπροσώπου

4.5.3. Mobile Banking

Το Mobile Banking υποστηρίζει συσκευές νέας τεχνολογίας με ενσωματωμένο web server, όπως:

- κινητά τηλέφωνα προηγμένης τεχνολογίας (smart phones)
- υπολογιστές χειρός (PDAs)

Προς το παρόν δεν είναι διαδεδομένος τρόπος συναλλαγής μεταξύ των ελληνικών τραπεζών.

Η πρόσβαση στις υπηρεσίες Mobile Banking είναι διαθέσιμη στους πελάτες όλων των εταιριών κινητής τηλεφωνίας και γίνεται γρήγορα χωρίς επιπλέον ρυθμίσεις.

[27] *Αγγελής Γ.Β(2005) «Η βίβλος του E-BANKING»*

4.5.4. Συστήματα e-banking

Τα συστήματα e-banking μπορεί να παρουσιάζουν σημαντικές διαφορές, ανάλογα με ποικίλους παράγοντες.

Οι τραπεζικοί οργανισμοί πρέπει να διαμορφώσουν το σύστημα e-banking και να επιλέξουν με προσοχή τους συνεργάτες τους (outsourcing) βάσει των παρακάτω:

- Στρατηγικοί στόχοι των υπηρεσιών e-banking
- Σκοπός, έκταση υλοποίησης και πολυπλοκότητα εξοπλισμού, συστημάτων και λειτουργιών
- Τεχνολογική εξειδίκευση
- Προδιαγραφές ασφάλειας και εσωτερικού ελέγχου

Οι τραπεζικοί οργανισμοί μπορούν να αναλάβουν εσωτερικά την υποστήριξη των υπηρεσιών e-banking ή να την αναθέσουν σε τρίτους.

Το ίδιο φυσικά ισχύει για οτιδήποτε αφορά στην εύρυθμη λειτουργία του συστήματος. Οι συνεργάτες μπορεί να είναι άλλοι τραπεζικοί οργανισμοί με εμπειρία και ευχέρεια υλοποίησης και διαχείρισης συστημάτων e-banking, εταιρείες παροχής υπηρεσιών Internet (ISPs), ανάπτυξης και προσαρμογής σχετικών εφαρμογών, παροχής και διαχείρισης υπηρεσιών ασφάλειας κ.ά. Τα συστήματα e-banking βασίζονται σε ένα μεγάλο αριθμό συστημάτων και λειτουργιών, όπως οι εξής:

- Σχεδίαση και φιλοξενία web sites
- Παραμετροποίηση και διαχείριση συστημάτων Firewall
- Εγκατάσταση και ρύθμιση συστημάτων IDS (Intrusion Detection Systems), τόσο σε επίπεδο δικτύου όσο και σε κάθε κόμβο ξεχωριστά
- Διαχείριση δικτύου και ασφάλειας
- Εξειδικευμένοι e-banking servers
- Εφαρμογές e-commerce, π.χ. για την πληρωμή οφειλών, το δανεισμό, την αγορά μετοχών
- Κεντρικό σύστημα επεξεργασίας αιτήσεων
- Υποστήριξη και προσαρμογή υπηρεσιών

Συνδυάζοντας εσωτερικά και εξωτερικά προερχόμενες λύσεις, οι υπεύθυνοι διαχείρισης έχουν στη διάθεση τους αρκετές εναλλακτικές λύσεις κατά τον καθορισμό των προδιαγραφών για κάθε τμήμα του συστήματος e-banking.

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

Είναι πολύ σημαντικό ο πελάτης να τα γνωρίζει. Θα πρέπει να διαχωρίσουμε τα οφέλη του ιδιώτη πελάτη από αυτά της εταιρίας, ωστόσο να σημειώσουμε ότι τα οφέλη του ιδιώτη ισχύουν και για την εταιρία, όμως επειδή πολλές υπηρεσίες e-banking απευθύνονται αποκλειστικά σε επιχειρήσεις υπάρχουν επιπλέων οφέλη για αυτές.

4.6.1. Πλεονεκτήματα του e-banking *για τον ιδιώτη-πελάτη και για την εταιρεία-πελάτη*

4.6.1.1. Για τον ιδιώτη- πελάτη

- Εξυπηρέτηση 24 ώρες το εικοσιτετράωρο, 7 μέρες την εβδομάδα. Συνεπώς ο πελάτης μπορεί να εξυπηρετηθεί οποιαδήποτε στιγμή αυτός επιθυμεί.
- Αποφυγή ουράς εξυπηρέτησης: ο πελάτης δεν χρειάζεται να περιμένει σε ουρά εξυπηρέτησης είτε σε ταμείο καταστήματος τράπεζας είτε σε ATM.
- Εξοικονόμηση χρόνου: ο χρήστης του e-banking κερδίζει χρόνο γιατί δεν είναι αναγκασμένος να φύγει από το σπίτι του ή την εργασία του για να πάει σε κάποιο κατάστημα της τράπεζας προκειμένου να εκτελέσει την συναλλαγή που θέλει.
- On line παρακολούθηση τραπεζικών προϊόντων: οποιοδήποτε τραπεζικό προϊόν κατέχει ένας πελάτης της τράπεζας, είναι προσβάσιμα on line.
- Μείωση χρήσης χαρτιού: δεν είναι απαραίτητη πλέον η χρήση μεγάλου όγκου χαρτιού εκ μέρους του πελάτη αφού τα πάντα είναι διαθέσιμα στο internet. Επίσης όποτε θέλει ο χρήστης μπορεί να εκτυπώσει μόνο την πληροφορία που επιθυμεί.
- Εύκολη πρόσβαση από οποιοδήποτε σημείο του κόσμου: από την στιγμή που ο πελάτης διαθέτη πρόσβαση στο internet μπορεί ανά πάσα στιγμή και από οποιοδήποτε μέρος του κόσμου να έχει άμεση πρόσβαση στο τραπεζικό του χαρτοφυλάκιο και να εκτελεί τις

συναλλαγές. Αρκεί να συνδεθεί στο site της e- banking υπηρεσίας της τράπεζας.

- Διενέργεια τραπεζικών συναλλαγών από το γραφείο ή/ και από το σπίτι: η δυνατότητα τέλεσης τραπεζικών συναλλαγών από το γραφείο ή το σπίτι, εστιάζει στην άνεση που παρέχει στον πελάτη της, η τράπεζα να συναλλάσσεται μαζί της.
- Μεγάλη γκάμα εξόφλησης λογαριασμών Επιχειρήσεων και Οργανισμών: οι πελάτες βρίσκουν μια συνεχώς αυξανόμενη γκάμα επιχείρησης για να εξοφλήσουν τις οφειλές- λογαριασμούς τους από ένα σημείο πρόσβασης, ώστε να έχουν συγκεντρωτική ενημέρωση αλλά και να κάνουν καλύτερα προγραμματισμό των υποχρεώσεων τους.
- Δυνατότητα επενδυτικών συναλλαγών: οι χρήστες μπορούν να εκτελούν επενδυτικές συναλλαγές και να ελέγχουν οι ίδιοι τις εντολές τους, τα χαρτοφυλάκια τους και την αποτίμηση τους.
- Μικρότερο κόστος συναλλαγών: πολλές συναλλαγές, για τις οποίες στα καταστήματα τραπεζών υπάρχει προμήθεια, παρέχονται εντελώς δωρεάν μέσω του e-banking.
- Εύκολες συναλλαγές για άτομα με ειδικές ανάγκες: αρκετοί άνθρωποι με κινητικά προβλήματα μπορούν να συναλλάσσονται με την τράπεζα εύκολα και γρήγορα χωρίς να χρειάζεται να μετακινούνται.
- Γνωριμία με νέες τεχνολογίες: η διενέργεια συναλλαγών μέσω e-banking φέρνει αντιμέτωπο τον πελάτη της τράπεζας με νέες τεχνολογίες.

4.6.1.2. Για την εταιρεία -πελάτη

Πέραν τον πλεονεκτημάτων που αναφέρθηκαν υπάρχουν και κάποια επιπρόσθετα για τις επιχειρήσεις που χρησιμοποιούν το e- banking.

- Ολοκληρωμένα πακέτα υπηρεσιών πληρωμών για επιχειρήσεις: μια εταιρία έχει ένα ολοκληρωμένο περιβάλλον πληρωμών, τόσο των οφελών της στο δημόσιο, όσο και της σε ΔΕΚΟ και οργανισμούς.
- Εύκολη ενημέρωση των μηχανογραφικών συστημάτων της εταιρίας: μέσω του download που προσφέρουν οι τράπεζες μέσω του e-banking, οι επιχειρήσεις μπορούν να ενημερώνουν τα μηχανογραφικά

και λογιστικά τους συστήματα με τις κινήσεις των λογαριασμών της εταιρίας.

- Εκτέλεση μισθοδοσίας προσωπικού ή μαζικών πληρωμών προμηθευτών: η επιχείρηση μπορεί να εκτελεί την μισθοδοσία του προσωπικού της ή να πληρώνει τους προμηθευτές της και να παρακολουθεί on line την κατάσταση των λογαριασμών της.
- Διαφορετικά δικαιώματα χρήσης και πρόσβασης: η εταιρία μπορεί να επιλέξει ποιοι υπάλληλοι της θα χρησιμοποιούν ηλεκτρονικές τραπεζικές υπηρεσίες και τι δικαιώματα θα έχουν. Στους εταιρικούς πελάτες δίνεται η δυνατότητα της έγκρισης συναλλαγών.
- Δημιουργία εναλλακτικού δικτύου εξόφλησης λογαριασμών: πολλές εταιρίες μπορούν να εκμεταλλευτούν το e-banking, ως ένα επιπλέον δίκτυο είσπραξης των υποχρεώσεων των πελατών της.
- Δημιουργία εναλλακτικού δικτύου πώλησης προϊόντων και υπηρεσιών: με συνεργασίες στο χώρο του e-commerce και του e-payments, ασφαλή και εξ αποστάσεως τρόπο αγορών και πληρωμής των οφειλών τους.

4.6.1.3. Μειονεκτήματα

- **Χρονοβόρα εγγραφή πελατών:** Για να γραφτεί κάποιος στο online πρόγραμμα της τράπεζάς του, θα πρέπει να δώσει στοιχεία ταυτότητας και να υπογράψει ένα έντυπο στο τραπεζικό κατάστημα ή αν πρόκειται για μια αποκλειστικά ηλεκτρονική τράπεζα, τα έντυπα θα του αποσταλούν ταχυδρομικώς έτσι ώστε να συμπληρωθούν και να σταλούν ξανά στην τράπεζα.
- **Δυσκολία στο χειρισμό:** Οι τραπεζικοί δικτυακοί τόποι ίσως φανούν δύσχρηστοι σε κάποιον που δεν ξέρει να χειρίζεται καλά το Internet. Το άνοιγμα ενός online λογαριασμού ή η online λήψη ενός δανείου μπορεί να τρομάζει κάποιους λόγω ελλιπών γνώσεων πάνω στις νέες τεχνολογίες.
- **Δυσπιστία του χρήστη**: Πολλοί άνθρωποι δεν εμπιστεύονται την ηλεκτρονική τραπεζική. Θέλουν να βλέπουν αυτόν που θα επεξεργαστεί το λογαριασμό τους, ενώ η ηλεκτρονική μεταφορά χρημάτων τους προκαλεί αμφιβολίες.

4.6.2. Πλεονεκτήματα(οφέλη)-μειονεκτήματα του e-banking από την πλευρά των τραπεζών

Η χρήση των ηλεκτρονικών υπηρεσιών και δει του e- banking, δίνει την δυνατότητα στις τράπεζες που το χρησιμοποιούν να μεγιστοποιήσουν τα πλεονεκτήματα που προσφέρει η χρήση του.

4.6.2.1. Πλεονεκτήματα

- Εναλλακτικά Δίκτυα: οι τράπεζες έχουν τη δυνατότητα να επεκτείνουν τα δίκτυα εξυπηρέτησης πελατείας τους.

- Καινοτομικές υπηρεσίες: το e- banking παρέχει την δυνατότητα στις τράπεζες να εκμεταλλευτούν τα προνόμια που προσφέρει η τεχνολογία και να δημιουργήσουν καινοτόμες και πρωτοποριακές υπηρεσίες.

- Μείωση λειτουργικού κόστους: η εξοικονόμηση που κάνει η τράπεζα μέσω των καναλιών του e- banking είναι σημαντικότατη, αν συγκρίνουμε τα κόστη που έχει για την διεκπεραίωση συναλλαγών μέσω ταμείου σε σχέση με τα αντίστοιχα κόστη των εναλλακτικών δικτύων.

- Αύξηση ποιότητας εξυπηρέτησης: μέσω του e-banking και της αυτοματοποίησης των τραπεζικών εργασιών προσφέρονται υπηρεσίες που αυξάνουν την ποιότητα εξυπηρέτησης των πελατών των τραπεζών. Ακόμη η ποιότητα μπορεί να πιστοποιείται από εξουσιοδοτημένους φορείς, προσφέροντας έτσι κύρος στις μονάδες ηλεκτρονικής τραπεζικής.

- Αύξηση πελατειακής βάσης: η δημιουργία φιλικών προς τον χρήστη πλατφορμών βοηθούν στην προσέλκυση νέων πελατών και στην αύξηση της πελατειακής βάσης. Η προώθηση τραπεζικών προϊόντων είναι πιο ελκυστική όταν συνοδεύονται και από την προοπτική μιας σωστής και ολοκληρωμένης ηλεκτρονικής διαχείρισης του.

- Καλή φήμη: τράπεζες με αξιόπιστες και αξιόλογες ηλεκτρονικές υπηρεσίες, ενισχύουν την καλή τους φήμη. Το e- banking αποτελεί είδος βιτρίνας για τους τραπεζικούς οργανισμούς. Υπάρχουν περιπτώσεις μικρών τραπεζών που στηρίζουν την καλή τους εικόνα στο e- banking.

4.6.2.2. Μειονεκτήματα

- **Υψηλό αρχικό κόστος εγκατάστασης** : Όπως συμβαίνει με όλες τις νέες τεχνολογίες, το αρχικό κόστος εγκατάστασης είναι υψηλό. Η επένδυση που πρέπει να κάνει η τράπεζα για να αγοράσει τον απαιτούμενο εξοπλισμό αλλά και για να εκπαιδεύσει το προσωπικό της πάνω στις νέες τεχνολογίες είναι μεγάλη και πρέπει να γίνει με προσοχή και να είναι συμβατή με τη γενικότερη επιχειρηματική στρατηγική της τράπεζας.
- **Ασφάλεια**: Οι ηλεκτρονικές επιθέσεις και η μη εξουσιοδοτημένη πρόσβαση στα τραπεζικά ηλεκτρονικά συστήματα είναι συχνή. Η ασφάλεια λοιπόν των συναλλαγών και η προστασία των συναλλασσομένων είναι θέματα ύψιστης σημασίας για τις τράπεζες. Καθώς κανένα υπολογιστικό σύστημα δεν είναι 100% ασφαλές, οι τράπεζες πρέπει με κάποιο τρόπο να διασφαλίσουν τα περιουσιακά στοιχεία των πελατών τους από επιθέσεις hacker και ηλεκτρονικές απάτες. Από έρευνες που πραγματοποιήθηκαν στις ΗΠΑ, έχει υπολογιστεί ότι κάθε χρόνο χάνονται περίπου 11δις. δολάρια λόγω της ελλιπούς ασφάλειας. Για να καταστήσουν οι τράπεζες την ηλεκτρονική τραπεζική ασφαλή για τους πελάτες τους, πρέπει να επενδύσουν σε εξοπλισμό που περιλαμβάνει firewalls και συστήματα ενεργούς παρακολούθησης, καθώς και σε ανθρώπινο δυναμικό προσλαμβάνοντας ειδικούς συμβούλους σε θέματα ασφαλείας δικτύων.[28]

[28] *Κραπης Βασίλειος, (2007) «Η ηλεκτρονική τραπεζική ως ανταγωνιστικό πλεονέκτημα στη σύγχρονη δικτυακή οικονομία»*

ΚΕΦΑΛΑΙΟ 5

5. ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

5.1. Γενικά

Ιδιαίτερα ανησυχητικά είναι τα κρούσματα δικτυακής απάτης που έχουν ως στόχο τους ανυποψίαστους καταναλωτές ή τις μικρομεσαίες επιχειρήσεις που χρησιμοποιούν το Διαδίκτυο για ηλεκτρονικές συναλλαγές. Οι δικτυακοί απατεώνες έχουν πλέον ως στόχο το εύκολο κέρδος και προσπαθούν να αποσπάσουν προσωπικά δεδομένα όπως αριθμούς πιστωτικών καρτών, τραπεζικών λογαριασμών. Παραδείγματα τέτοιων απειλών αποτέλεσαν και τα περιστατικά που ενέπλεκαν γνωστούς οργανισμούς όπως η Citibank, eBay,και PayPal για την εξαπάτηση των χρηστών του Διαδικτύου.[29]

5.2. SNIFFERS

Ένας sniffer είναι ένα πρόγραμμα υποκλοπής δεδομένων που παρακολουθεί κρυφά την κίνηση ενός δικτύου με σκοπό να αρπάξει πληροφορίες που ταξιδεύουν σε αυτό. Αυτό το πρόγραμμα λειτουργεί επειδή το Ethernet κατασκευάστηκε γύρω από την αρχή του sharing. Τα περισσότερα δίκτυα χρησιμοποιούν τεχνολογία εκπομπής, όπου τα μηνύματα από ένα υπολογιστή διαβιβάζονται σε άλλο υπολογιστή σε αυτό το δίκτυο. Πρακτικά όλοι οι υπολογιστές του δικτύου αγνοούν το μήνυμα, εκτός αυτού που είναι ο παραλήπτης του. Πάντως, υπολογιστές μπορούν να διαμορφωθούν, ώστε να δέχονται τα μηνύματα ακόμα και αν δεν είναι για αυτούς. Αυτό γίνεται με την χρήση ενός sniffer[30].

[29] *News .pramnos. net/story58-976.html – 3 l k – (2009)<<Οι δικτυακές απειλές… δεν πάνε διακοπές*
[30] *Αγγελής Βασίλης,(2005) «Η βίβλος του e-Banking»*

5.2.1. ΠΩΣ ΔΟΥΛΕΥΕΙ ΕΝΑΣ SNIFFER

Ένας υπολογιστής που είναι συνδεδεμένος σε ένα τοπικό δίκτυο έχει δυο διευθύνσεις. Η πρώτη λέγεται MAC (Media Access Control) διεύθυνση που ταυτοποιεί μοναδικά κάθε κόμβο σε ένα δίκτυο και αποθηκεύεται στην κάρτα δικτύου. Η MAC είναι αυτή που χρησιμοποιείται από το πρωτόκολλο Ethernet όταν δημιουργεί πακέτα για να μεταφέρει δεδομένα από τον ένα υπολογιστή στον άλλο. Η άλλη διεύθυνση είναι η IP διεύθυνση, που χρησιμοποιείται από τις εφαρμογές. Το επίπεδο σύνδεσης δεδομένων χρησιμοποιεί μια Ethernet κεφαλίδα με την MAC διεύθυνση της μηχανής προορισμού αντί της IP διεύθυνσης. Το επίπεδο δικτύου είναι υπεύθυνο για την αντιστοίχηση των IP διευθύνσεων με τις MAC διευθύνσεις που απαιτούνται από το data link layer. Αρχικά αναζητά τη MAC διεύθυνση της μηχανής προορισμού σε ένα πίνακα που καλείται ARP (Address Resolution Protocol). Αν δεν βρεθεί εγγραφή για την συγκεκριμένη IP, ο ARP εκπέμπει ένα πακέτο αίτησης σε όλες τις μηχανές του δικτύου. Η μηχανή με αυτή τη διεύθυνση απαντά στην αρχική μηχανή με τη δική της MAC διεύθυνση. Η MAC διεύθυνση τότε προστίθεται στον πίνακα ARP. Η αρχική μηχανή σε όλες τις επικοινωνίες της με τη μηχανή προορισμού χρησιμοποιεί πλέον την MAC διεύθυνση.

Υπάρχουν δυο τύποι Ethernet περιβαλλόντων και ο τρόπος που δρουν οι sniffers και στις δυο περιπτώσεις είναι λίγο διαφορετικός.

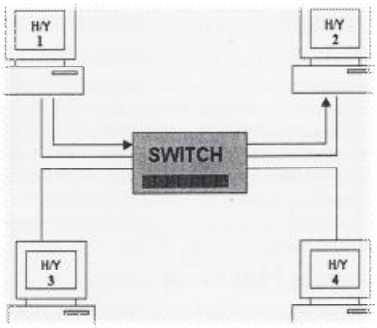
- Shared Ethernet: σε ένα Shared Ethernet όλοι οι σύνδεσμοι μοιράζονται το ίδιο εύρος ζώνης του δικτύου. Είτε συνδέονται με ένα καλώδιο είτε με ένα hub(διανομείς), η μεταβίβαση βασίζεται στην λογική του πρώτο λαμβάνεται, πρώτο εξυπηρετείται. Σε ένα τέτοιο περιβάλλον τα πακέτα που είναι για ένα μηχάνημα λαμβάνονται από όλα τα υπόλοιπα.

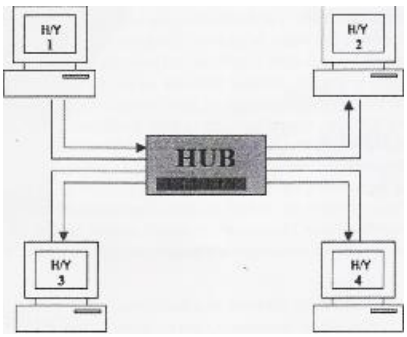
Μια μηχανή με sniffer σπάει αυτό το κανόνα και δέχεται όλα τα πακέτα. Το sniffing σε ένα Shared Ethernet περιβάλλον είναι εντελώς παθητικό, αδρανές και εξαιρετικά δύσκολο να ανιχνευτεί.

- Switched Ethernet: σε ένα Switched Ethernet όλοι οι υπολογιστές είναι συνδεδεμένοι σε ένα διακόπτη (Switch). Αυτό μεταφέρει πακέτα μόνο στον υπολογιστή για τον οποίο είναι προορισμένα και δεν εκπέμπει τα πακέτα στους υπόλοιπους του δικτύου. Αυτό όμως δεν σημαίνει ότι είναι πιο ασφαλής.

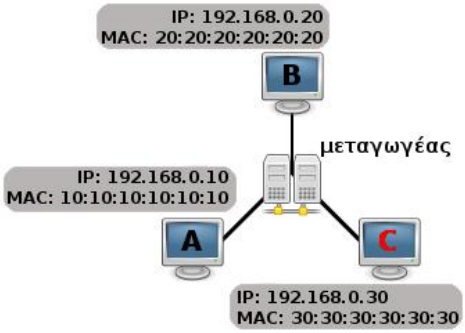
Αν και το switch(μεταγωγείς) είναι πιο ασφαλές από το hub υπάρχουν μέθοδοι με τους οποίους μπορεί να γίνει sniffing σε ένα switch.

1. ARP Spoofing (εξαπάτηση): ο sniffer στέλνει request στο ARP και λαμβάνει απάντηση, αφού ο ARP δεν ελέγχει αν το μήνυμα που λαμβάνει είναι από συγκεκριμένη μηχανή.
2. MAC Flooding (πλημμύρα): η μνήμη switch είναι περιορισμένη. Στην προκειμένη περίπτωση ο sniffer υπερφορτώνει τη μνήμη(με διευθύνσεις MAC) του switch και αυτό έχει ως αποτέλεσμα το switch να διοχετεύει τα πακέτα οπουδήποτε.





Παράδειγμα παραβίασης ARP (Spoofing)



Σκοπός του **C** είναι να "μπει" ανάμεσα από τον **A** και το **B**. Για να γίνει αυτό, στέλνει πακέτα ARP στον **A** με διεύθυνση πρωτοκόλλου *192.168.0.20* και διεύθυνση MAC *30:30:30:30:30:30*. Όταν λοιπόν ο **A** θέλει να στείλει δεδομένα στον **B**, θα χρησιμοποιήσει την διεύθυνση MAC του **C**. Με τον ίδιο τρόπο, εξαπατεί τον **B**, ώστε στον κατάλογο ARP του τελευταίου να βρίσκεται το ζεύγος *192.168.0.10 → 30:30:30:30:30:30* αντί του *192.168.0.10 → 10:10:10:10:10:10*. Σ'αυτό το σημείο, ο **A** στέλνει τα πακέτα με αποδέκτη τον **B** στον κακόβουλο χρήστη **C** (και αντιστρόφως). Παρόλα αυτά, για να λειτουργήσει σωστά η παραβίαση αυτή, ο **C** πρέπει επίσης να δρομολογήσει όποιο πακέτο δεν του απευθύνεται (με βάση την διεύθυνση πρωτοκόλλου) ή όποιο πακέτο δεν θα έπρεπε να λαμβάνει στον επιθυμητό τελικό αποδέκτη, έτσι ώστε οι δυο host (εδώ **A** και **B**) να μην καταλάβουν πως η επικοινωνία τους παρακολουθείται.

Ο καλύτερος τρόπος άμυνας απέναντι σε ένα packet sniffer είναι η χρήση κρυπτογράφησης. Η ιδιαίτερα ισχυρή κρυπτογράφηση αχρηστεύει το sniffer, αφού τα συλληφθέντα πακέτα δεν μπορούν να αποκωδικοποιηθούν, ώστε να διαβαστούν οι

πληροφορίες που περιέχουν. Η κρυπτογράφηση μπορεί να γίνει σε αρκετές υπηρεσίες (services) με τη χρήση ανάλογων πρωτοκόλλων όπως πχ. SSL(αναλύεται παρακάτω).

5.3. KEY LOGGERS

Το key logging συμβαίνει όταν καταγράφεται ότι πληκτρολογεί ο χρήστης, χωρίς ο ίδιος να το ξέρει ή να το επιτρέπει. Χρησιμοποιείται από επιτήδειους για την κλοπή των στοιχείων της πιστωτικής κάρτας, των τραπεζικών συναλλαγών και των προσωπικών κωδικών και αποτελεί σοβαρή απειλή για τη διαρροή προσωπικών/ εταιρικών στοιχείων.

Η κλοπή γίνεται από ένα ειδικό υλικό, το οποίο είναι εύκολο να εγκατασταθεί και δύσκολο να εντοπιστεί. Τα key loggers καταγράφουν και αποθηκεύουν τις πληκτρολογήσεις και τα mouse clicks σε ειδικό αρχείο, το οποίο αποστέλλεται μέσω του internet σε αυτόν που κατασκοπεύει τον χρήστη.

5.4. Κοινωνική Μηχανική

Η κοινωνική μηχανική είναι ένα μη τεχνικό είδος παράνομης εισβολής που βασίζεται κατά βάση στην ανθρώπινη επικοινωνία και συχνά υπάρχουν κόλπα τα οποία ωθούν τους ανθρώπους να καταργήσουν τις οριζόμενες διαδικασίας ασφάλειας. Κάποια από αυτά τα σενάρια είναι:

- Τηλεφωνική επικοινωνία του κοινωνικού μηχανικού με τον χρήστη, όπου ο κοινωνικός μηχανικός προσποιείται ότι είναι μέλος της ομάδας IT, που έχει ανάγκη τους κωδικούς πρόσβασης του χρήστη και άλλες πληροφορίες με σκοπό να διορθώσει προβλήματα που εμφανίστηκαν στο λογαριασμό του χρήστη στο δίκτυο.
- Τηλεφωνική επικοινωνία με το τμήμα IT μιας εταιρίας, προσποιούμενος ένα υψηλό διευθυντικό στέλεχος της εταιρίας που έχει ξεχάσει το password του και απαιτεί άμεσα την πληροφορία για λόγους εξαιρετικής επαγγελματικής ανάγκης.
- Δημιουργία μιας προσωπικής σχέσης με ένα χρήστη ή μέλος ομάδας IT με σκοπό την κουβέντα και το κοινωνικό σχόλιο, ώστε να αποκτήσει την εμπιστοσύνη του και να εκμαιεύσει εμπιστευτικές πληροφορίες.

Ένας κοινωνικός μηχανικός δεν είναι μόνο καλός ηθοποιός, είναι καλός στο να «διαβάζει» τους ανθρώπους και να αποφασίζει πια μέθοδο θα ακολουθήσει. Όταν δε αυτό συνδυάζεται με τις ικανότητες ενός hacker μπορεί πολύ εύκολα να διεισδύσει σε οποιοδήποτε δίκτυο.[31]

5.5. Δούρειοι ίπποι

Ο **δούρειος ίππος** (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

5.5.1.Τύποι δούρειων ίππων

Υπάρχουν δύο είδη δούρειων ίππων:

- Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία διάφοροι χάκερς μεταβάλλουν προσθέτοντας κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν για παράδειγμα διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων (peer-to-peer), προγράμματα ανακοίνωσης καιρικών συνθηκών κοκ.
- Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι

[31] *Αγγελής Βασίλης,(2005) «Η βίβλος του e-Banking»*

- η διαγραφή αρχείων στον μολυσμένο υπολογιστή
- η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές,
- το ανοιγόκλεισμα του οδηγού CD-ROM,
- η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες
- απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή
- απενεργοποίηση προγραμμάτων firewall ή αντιϊκών και πολλά άλλα

Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι χρήστες πάντα προτρέπονται να μην ανοίγουν ύποπτα αρχεία επισυναπτόμενα σε e-mail. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη με e-mail. Μπορεί να το έχει κατεβάσει από έναν ιστοχώρο, μέσω προγραμμάτων Instant Messaging, σε CD ή DVD.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κοκ), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα[32].

5.6. Phishing

Πρόκειται για τη διαδικασία όπου οι επίδοξοι απατεώνες στέλνουν e-mails σε χρήστες, τα οποία φαίνεται να προέρχονται από κάποια τράπεζα ζητώντας επιβεβαίωση των προσωπικών τους στοιχείων. Οι τεχνικές που χρησιμοποιούνται, φυσικά, είναι ποικίλες αλλά βασίζονται στη φιλοσοφία ότι κάποια έμπιστη εταιρία-οργανισμός επικοινωνεί μαζί του ζητώντας τα προσωπικά του στοιχεία για κάποιο λόγο που φαίνεται αληθοφανής. Αυτές οι περιπτώσεις είναι μάλιστα και οι πιο επικίνδυνες, αφού η επιτυχία της εξαπάτησης στηρίζεται στο γεγονός ότι ο χρήστης είναι ήσυχος ότι αποστέλλει τα στοιχεία του σε έναν έμπιστο παραλήπτη.

[32] *el.wikipedia.org/wiki*

Σε αυτά τα e-mails, υπάρχει συνήθως ένας **σύνδεσμος** στον οποίο καλείται να κάνει κλικ ο χρήστης. Ο φαινομενικά αθώος **σύνδεσμος** οδηγεί σε ένα **site** -που ανήκει φυσικά στον απατεώνα- και στο οποίο ο χρήστης εισάγει όλα τα στοιχεία που του ζητούνται. Η συνέχεια φυσικά είναι προφανής. Δυστυχώς οι έρευνες δείχνουν ότι πολλοί χρήστες ανταποκρίνονται σε αντίστοιχα e-mails και αυτό συμβαίνει λόγω έλλειψης ενημέρωσης.

Θα πρέπει να θυμόμαστε εκ των προτέρων, πως κανένας σοβαρός οργανισμός ή εταιρία δεν θα μας ζητήσει ταυτοποίηση των στοιχείων μας μέσω e-mail. Αν λοιπόν λάβουμε ποτέ ένα παρόμοιο ηλεκτρονικό μήνυμα από μια εταιρία που όντως γνωρίζουμε και συνεργαζόμαστε, σε καμιά περίπτωση δεν θα πρέπει να απαντήσουμε.

Αντίθετα, να καλέσουμε τηλεφωνικά την εταιρία και να μιλήσουμε με κάποιον υπεύθυνο ενημερώνοντάς τον για το περιστατικό.[33]

5.6.1. Εναλλακτική μέθοδος Phishing

Στον υπολογιστή-θύμα εγκαθίσταται ένας "αόρατος" **ιός**, είτε μέσω e-mail είτε μέσω φυσικής πρόσβασης από τον ίδιο τον θύτη. Στη συνέχεια, ο χρήστης επισκέπτεται για παράδειγμα την ιστοσελίδα μιας τράπεζας πληκτρολογώντας κανονικά τη διεύθυνση στην μπάρα διευθύνσεων του **Internet browser**. Τότε επεμβαίνει ο **ιός**, ο οποίος ανακατευθύνει (redirect) τον χρήστη σε ένα άλλο **site** παρόμοιο με αυτό που περιμένει να δει ο χρήστης (της τράπεζας). Ο ανυποψίαστος χρήστης εισάγει φυσικά τα στοιχεία του στις φόρμες του **site**, έχοντας στο μυαλό του ότι δεν υπάρχει κανένας κίνδυνος. Στην πραγματικότητα όμως τα στοιχεία αυτά καταλήγουν στον επίδοξο απατεώνα που μπορεί πλέον να τα χρησιμοποιήσει όπως επιθυμεί προς όφελος του.

Η "τεχνολογία" της απάτης έχει μάλιστα προχωρήσει τόσο πολύ, ώστε ο **ιός** έχει τη δυνατότητα να αντιγράψει γραφικά και στοιχεία από το αυθεντικό **site** και να τα μεταφέρει στο ψεύτικο δημιουργώντας ένα ακριβές αντίγραφο. Κάθε φορά που εισάγουμε τα στοιχεία μας σε κάποια ιστοσελίδα στο **Internet**, θα πρέπει να ελέγχουμε αν αυτή έχει τη "σφραγίδα" κάποιας εταιρίας κρυπτογράφησης δεδομένων.

[33] *www.computeractive.gr*

5.7. Pharming

Πλέον οι χρήστες και οι οργανισμοί είναι πολύ προσεκτικοί στις επιθέσεις phishing, έτσι οι επιτήδειοι προχώρησαν ακόμα παραπέρα. Η νέα μορφή υποκλοπής κωδικών λέγεται pharming. Η απειλή αυτή αποτελεί μια επιβλαβή δικτυακή δραστηριότητα στο πλαίσιο της οποίας, μόλις ο χρήστης ενός υπολογιστή αναγράψει την ηλεκτρονική διεύθυνση (URL) την οποία θέλει να επισκεφτεί, μεταφέρεται αυτόματα και ακούσια σε μια πλαστή ιστοσελίδα, που μοιάζει όμως πολύ με την πραγματική, την οποία εξαρχής σκόπευε να επισκεφτεί.

Υπάρχουν δύο τρόποι δράσης των απατεώνων και είναι οι εξής:

• Αποστολή ιών μέσω e- mail: αυτοί οι ιοί αντικαθιστούν τα τοπικά host αρχεία του υπολογιστή του χρήστη με άλλα. Τα host αρχεία μετατρέπουν τα URLs σε αριθμητικές συμβολοσειρές που είναι κατανοητές από τον υπολογιστή. Ένας υπολογιστής με αλλαγμένα host αρχεία θα μεταβεί σε λανθασμένο site ακόμα και αν ο χρήστης πληκτρολογήσει το σωστό URL.

• Παραποίηση DNS: η πιο σημαντική απειλή του pharming είναι η παραποίηση του DNS (Domain Name System) – το μηχάνημα που κατευθύνει τους χρήστες στη σωστή ιστοσελίδα με βάση το δικτυακό όνομα της– όπου δίνεται η δυνατότητα στους hackers να χρησιμοποιήσουν την ονομασία της ιστοσελίδας (domain name) και να κατευθύνουν όσους θέλουν να την ανοίξουν σε μια άλλη που είναι πλαστή, αποτέλεσμα αυτού είναι η μετάβαση μεγάλου αριθμού χρηστών σε sites απατεώνων χωρίς να το αντιλαμβάνονται.

Πολύ διαδεδομένη είναι και η περίπτωση των ψεύτικων τραπεζικών sites (Fake Banks). Σε αυτή την περίπτωση οι εισβολείς δημιουργούν sites πανομοιότυπα με αυτά των τραπεζών ή και νέα sites που υποτίθεται πως είναι ηλεκτρονικές τράπεζες. Οι χρήστες που εξαπατώνται διενεργούν εικονικές συναλλαγές χωρίς καμία υπόσταση, δίνοντας έτσι κωδικούς, αριθμούς λογαριασμών και καρτών χωρίς να το ξέρουν.

Το pharming έχει δύο βασικές διαφορές με το phishing, αυτές είναι:

1. Η επίθεση μπορεί να γίνει μαζικά σε πολλούς χρήστες.
2. Η μετακίνηση σε pharming site γίνεται χωρίς την παρεμβολή του χρήστη.[34]

[34] *Αγγελής Βασίλης, «Η βίβλος του e-Banking»*

ΜΕΡΟΣ Γ΄

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑ ΤΩΝ ΚΙΝΔΥΝΩΝ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

ΚΕΦΑΛΑΙΟ 6

6. ΜΕΘΟΔΟΙ ΓΙΑ ΤΗ ΔΙΑΣΦΑΛΙΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΩΝ ΣΥΝΑΛΛΑΓΩΝ

6.1. Εισαγωγή

Δεν υπάρχει καμία μυστική συνταγή για την επίτευξη της απόλυτης ασφάλειας. Κανένα σύστημα και καμία τεχνολογία δεν μπορεί να υποστηρίξει ότι καλύπτει με απόλυτη ασφάλεια τον κύκλο μιας συναλλαγής. Αυτό που συνήθως κάνουν όλοι οι δικτυακοί τόποι είναι η διαχείριση των πιθανών κινδύνων και η ελαχιστοποίηση των κενών ασφαλείας που μπορεί να εξελιχθούν σε απειλές.

Η προστασία των συναλλαγών και των δεδομένων που περιέχουν είναι ένα θέμα που καλούνται να αντιμετωπίσουν όλοι οι οργανισμοί και όχι μόνο αυτοί που επιχειρούν online.

Η ασφάλεια ενός δικτυακού τόπου μπορεί να οριστεί ως η δυνατότητα να αντισταθεί σε τυχαία συμβάντα ή σε προμελετημένες ενέργειες. Οι βασικοί κίνδυνοι που απειλούν την ασφάλεια των ηλεκτρονικών συναλλαγών έχουν να κάνουν με τη διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα των δεδομένων και την εξακρίβωση της γνησιότητας, αναλυτικότερα:

− **Διαθεσιμότητα – Availability**: Αναφέρεται στη δυνατότητα πρόσβασης στις πληροφορίες, στις υπηρεσίες και σε όλους τους πόρους ενός ιστοχώρου παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές ατυχήματα ή επιθέσεις. Απαιτεί τεχνολογίες που θα πιστοποιούν την εύρυθμη και συνεχή λειτουργία του χώρου.

− **Ακεραιότητα – Integrity**: Αναφέρεται στην αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται. Πρέπει να διασφαλιστεί ότι τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς τους στο δίκτυο. Με αυτόν τον τρόπο διαφυλάσσεται η ακρίβεια και πληρότητα των δεδομένων, η ακεραιότητα παρέχεται μέσω τεχνολογιών ψηφιακής υπογραφής.

− **Εμπιστευτικότητα - Confidentiality:** Η εμπιστευτικότητα είναι απαραίτητο στοιχείο τόσο της ιδιωτικότητας του χρήστη (user privacy) όσο και της προστασίας των πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσω

κρυπτογράφησης. Σε ένα ηλεκτρονικό περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.

− **Μη αποποίηση της ευθύνης - Non-repudiation**. Αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια στο ηλεκτρονικό εμπόριο. Για να ολοκληρωθεί μια συναλλαγή θα πρέπει να μην μπορεί κάποιος να ισχυρισθεί ότι δεν συμμετείχε σε αυτή.

− **Επαλήθευση ταυτότητας - Authenticity**: Για την επαλήθευση της ταυτότητας χρησιμοποιούνται διάφορες μέθοδοι, ενδιαφέρον παρουσιάζει η μέθοδος που χρησιμοποιούν οι τράπεζες για την επιβεβαίωση της ταυτότητας χρηστών. Η επαλήθευση δεν γίνεται μόνο μέσω των συνθηματικών αλλά και μέσω ειδικών συσκευών παραγωγής κωδικού ή μέσω προσωπικών ερωτήσεων

6.2. Μέσα προστασίας της επικοινωνίας

Οι λύσεις που ακολουθούνται για τη διασφάλιση των ηλεκτρονικών συναλλαγών είναι τεχνολογίες που προστατεύουν τα δεδομένα μιας συναλλαγής σε όλες της φάσης εξέλιξης της. Αυτές οι τεχνολογικές λύσεις μπορούν να χωριστούν σε τέσσερις μεγάλες κατηγορίες.

6.2.1. Προστασία της επικοινωνίας με κρυπτογραφία

6.2.1.1.Εισαγωγή στην κρυπτογραφία

Η ανάγκη για εμπιστευτικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την κρυπτογράφηση, που είναι η καλύτερη ασπίδα προστασίας των δεδομένων. Ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης, έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί.

Οι διάφορες μέθοδοι κρυπτογράφησης βασίζονται στη χρήση ενός "κλειδιού", ενός μαθηματικού δηλαδή κώδικα - αλγόριθμου, ο οποίος διασφαλίζει το μη

"αναγνώσιμο" από τρίτους, και χρησιμοποιείται στην κρυπτογράφηση και την αποκρυπτογράφηση.

Κάθε αλγόριθμος παίρνει την ονομασία του από τον αριθμό που μεταλλάσσεται και πρέπει να βρεθεί με μια σειρά μαθηματικών πράξεων.

Αρχικά το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα (symmetric cryptosystem). Το σύστημα αυτό χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων. Αργότερα η εξέλιξη οδήγησε στη χρησιμοποίηση δύο κλειδιών, ενός ιδιωτικού και ενός δημόσιου (ασύμμετρο κρυπτογραφικό σύστημα - asymmetric or public key cryptosystem).

Το ιδιωτικό κλειδί (private key) χρησιμοποιείται για το σφράγισμα του ηλεκτρονικού μηνύματος και είναι απόρρητο, ενώ το δημόσιο κλειδί (public key) αντιστοιχεί στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο. Συνεπώς, το πρώτο κλειδί το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο, ενώ το δεύτερο το γνωστοποιεί σε κάθε συναλλασσόμενό του για να μπορεί να αποκρυπτογραφεί/διαβάζει τα μηνύματα του πρώτου.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.[35]

6.2.1.2. Μέθοδοι κρυπτογράφησης

<u>Συμμετρικά κρυπτοσυστήματα</u>

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία

[35] «Certified e□Commerce Consultant»deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf – deicec.files.wordpress.com/2008/10

θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

Ασύμμετρα κρυπτοσυστήματα

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

− Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα

− Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο

χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής[36].

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Τα πιο γνωστά είναι :

1. ***PGP (Pretty Good Privacy)***

Το PGP είναι το δημοφιλέστερο πρόγραμμα για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων. Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντάς το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

2. X.509:

Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO (International Standards Organization - Διεθνή Οργανισμό Τυποποίησης) και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει

[36] *www.go-online.gr/ebusiness/specials/article.html?article_id=713*

στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών. Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων (browsers), εξυπηρετητές (servers) και προγράμματα λογισμικού, για τη διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ., από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.)[37].

6.2.2. *Η τεχνολογία PKI (Public Key Infrastructure)*

Η τεχνολογία **PKI (Public Key Infrastructure)** είναι μια πολύ γνωστή τεχνολογία που μπορεί να χρησιμοποιηθεί για να αναγνωρίσει οντότητες, να κρυπτογραφήσει πληροφορία και να υπογράψει ηλεκτρονικά έγγραφα. Η PKI αναγνωρίζει και διαχειρίζεται σχέσεις μεταξύ των μελών μιας ηλεκτρονικής ανταλλαγής δεδομένων, εξυπηρετεί ένα μεγάλο εύρος αναγκών ασφαλείας, συμπεριλαμβανομένων ελέγχου πρόσβασης, εμπιστευτικότητα, ακεραιότητα, πιστοποίηση και μη αποποίηση ευθύνης. Η PKI χρησιμοποιεί επίσης μοναδικά **Ψηφιακά Πιστοποιητικά** για να ασφαλίσει το e-Banking και e-Commerce, το e-mail, την ανταλλαγή δεδομένων καθώς και τα VPNs και intranets. Τέλος η PKI τεχνολογία χρησιμοποιείται για να πιστοποιήσει την ταυτότητα και τα δικαιώματα του κάθε χρήστη.

Επιπρόσθετα η **Αρχή Πιστοποίησης (Certificate Authority),** που είναι αυτή που εγγυάται την PKI τεχνολογία, παρέχει έναν ολοκληρωμένο πακέτο διαχείρισης των δημόσιων κλειδιών και πιστοποιητικών, που περιλαμβάνει την έκδοση, την πιστοποίηση, την αποθήκευση, την πρόσβαση, την ενημέρωση και την ανανέωση. Όλοι οι χρήστες της PKI πρέπει να έχουν μια εγκεκριμένη ταυτότητα, η οποία είναι αποθηκευμένη σε ένα ψηφιακό πιστοποιητικό που εκδίδει η Αρχή Πιστοποίησης. Αυτό λειτουργεί ως ο σύνδεσμος της εμπιστοσύνης στην PKI. Απομακρυσμένοι χρήστες και δικτυακοί τόποι που χρησιμοποιούν δημόσια και ιδιωτικά κλειδιά και πιστοποιητικά δημοσιών κλειδιών μπορούν να πιστοποιηθούν με υψηλό βαθμό εμπιστοσύνης. Η πιστοποίηση αυτή εξαρτάται από τρεις συνθήκες:

- Πρέπει να κατοχυρώνεται ότι το δημόσιο κλειδί που κατέχει το κάθε μέρος, δεν έχει κλαπεί ή αντιγραφεί από τον ιδιοκτήτη του
- Το πιστοποιητικό πρέπει να εκδίδεται στον ιδιοκτήτη σε αρμονία με την καταγεγραμμένη πολιτική του εκδότη πιστοποιητικών, και
- Οι πολιτικές του εκδότη πιστοποιητικών πρέπει να ικανοποιούν τα

[37] *www.go-online.gr/ebusiness/specials/article.html?article_id=716*

εμπλεκόμενα μέρη, όσον αφορά την πιστοποίηση της ταυτότητας.

Από τη στιγμή που ικανοποιούνται οι τρεις αυτές συνθήκες, τότε υπάρχει η σωστή βάση για την εξασφάλιση της ασφάλειας.[38]

6.2.2.1. Δημόσια και ιδιωτικά κλειδιά

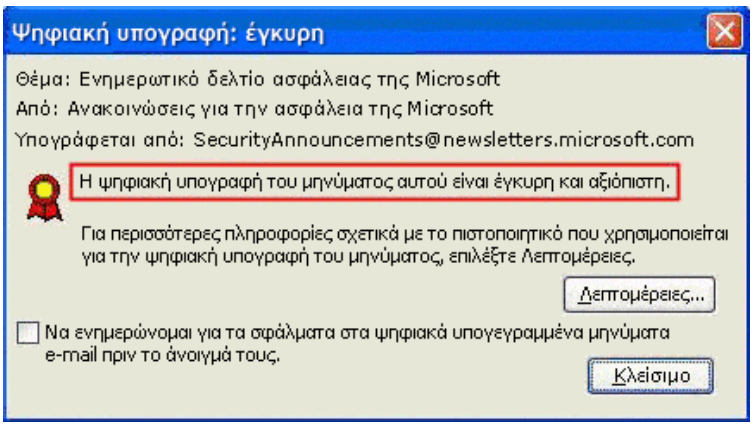
Η PKI χρησιμοποιεί ένα σύστημα ζευγαριών κλειδιών, που είναι ασύμμετρα, συνδέονται μαθηματικά μεταξύ τους και εκτελούν αντίθετες ενέργειες, δηλ. οτιδήποτε κλειδώνει το ένα κλειδί, μόνο το άλλο κλειδί μπορεί να ξεκλειδώσει. Τα δημόσια (public) και ιδιωτικά (private) κλειδιά είναι μοναδικά για κάθε χρήστη σε ένα PKI σύστημα. Το ιδιωτικό κλειδί δημιουργείται πρώτα. Μια μαθηματική συνάρτηση εφαρμόζεται στο ιδιωτικό κλειδί για την δημιουργία του δημόσιου κλειδιού. Είναι πρακτικά αδύνατο να ανιχνευτεί το ιδιωτικό κλειδί κάποιου από το δημόσιο κλειδί του. Τα ιδιωτικά κλειδιά πρέπει να προστατεύονται από υποκλοπές και συνήθως αποθηκεύονται σε φυσικές συσκευές όπως είναι οι έξυπνες κάρτες ή τα tokens. Τα δημόσια κλειδιά από την άλλη μεριά, είναι διαθέσιμα σε όλους.

Οποιοσδήποτε επιθυμεί να κάνει ασφαλείς συναλλαγές χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη ως μέρος της διαδικασίας κρυπτογράφησης. Κρυπτογραφώντας κάτι με το δημόσιο κλειδί κάποιου άλλου, εξασφαλίζεται ότι μόνο αυτός μπορεί να το αποκωδικοποιήσει. Αν για οποιοδήποτε λόγο το μήνυμα αποστολής μιας κρυπτογραφημένης συναλλαγής παραβιαστεί, είναι απίθανο αυτό το μήνυμα να αποκωδικοποιηθεί και εκτελεστεί.

6.2.2.2. Ψηφιακές υπογραφές

Όταν παραλαμβάνεται ένα κρυπτογραφημένο μήνυμα ή συναλλαγή, είναι σημαντικό να υπάρχει η δυνατότητα πιστοποίησης ότι ο αποστολέας του, είναι όντως αυτός που ισχυρίζεται. Αυτό επιτυγχάνεται μέσω της ψηφιακής υπογραφής - μιας μοναδικής διαδικασίας υπογραφής μηνύματος που αποκαλύπτει την ταυτότητα του αποστολέα και πιστοποιεί την ακεραιότητα του μηνύματος. Οι ψηφιακές υπογραφές είναι αδιάψευστες, μοναδικές για κάθε συναλλαγή και είναι σχεδόν απίθανο να αντιγραφούν ή μεταφερθούν.

[38] Αγγελής Γ. Β.,(2005) «e-banking».



Η υπογραφή είναι μια μαθηματική συνάρτηση που περιλαμβάνει το πρωτότυπο μήνυμα και το ιδιωτικό κλειδί του αποστολέα. Το πρώτο βήμα στην διαδικασία υπογραφής περιλαμβάνει εκτέλεση ενός μαθηματικού αλγορίθμου, που είναι γνωστός ως hash. Ο hash παίρνει το πρωτότυπο μήνυμα και το μειώνει σε ένα καθορισμένο μέγεθος 160 bit χαρακτήρων, γνωστό ως ανασκόπηση μηνύματος (message digest). Η ανασκόπηση μηνύματος είναι η μαθηματική αναπαράσταση του πρωτότυπου μηνύματος. Αν ένας και μόνο χαρακτήρας αλλάξει, αλλάζει και η ανασκόπηση. Ακολούθως η ανασκόπηση κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Το αποτέλεσμα της κρυπτογράφησης είναι γνωστό ως ψηφιακή υπογραφή.

Το επόμενο στάδιο της PKI διαδικασίας είναι η ασφάλιση του μηνύματος και της υπογραφής. Αυτό γίνεται κρυπτογραφώντας το μήνυμα και την υπογραφή. Η κρυπτογράφηση περιλαμβάνει μια μοναδική μαθηματική συνάρτηση που μετασχηματίζει τα δεδομένα σε μια κωδικοποιημένη μορφή που απαιτεί ένα κλειδί κρυπτογράφησης για να ξεκλειδωθεί. Η ισχύς του κλειδιού εξαρτάται από τον αριθμό των bits που έχει. Για παράδειγμα ένα 20-bit κλειδί κρυπτογράφησης έχει 1,048,576 πιθανούς συνδυασμούς. Αν και φαίνεται δύσκολο να σπάσει, εν τούτοις ένας κανονικός υπολογιστής μπορεί να επεξεργαστεί εκατομμύρια συνδυασμούς γρήγορα και να το μαντέψει. Η πρόοδος στην υπολογιστική και επεξεργαστική ισχύ οδήγησε σε κλειδιά με υψηλότερο αριθμό bits. Σήμερα το εμπορικό standard για ισχυρή κρυπτογράφηση είναι τα 128 bit τα οποία δημιουργούν 680,565,000,000,000,000,000,000,000,000,000,000,000 πιθανούς συνδυασμούς. Οι ειδικοί υπολογίζουν ότι η κρυπτογράφηση των 2048 bit θα γίνει σύντομα το νέο εμπορικό standard αφού οι υπολογιστές θα είναι σε θέση να σπάσουν την κρυπτογράφηση των 128-bit σε 15 χρόνια.

Από την στιγμή που θα κρυπτογραφηθεί το μήνυμα και η υπογραφή, το επόμενο στάδιο είναι η ασφαλής μεταφορά του κλειδιού που απαιτείται για την αποκρυπτογράφηση. Ο τύπος του κλειδιού που χρησιμοποιείται σε κρυπτογράφηση

μηνύματος είναι γνωστό ως συμμετρικό κλειδί. Ένα συμμετρικό κλειδί είναι μοναδικό κλειδί που δημιουργείται για χρήση μιας φοράς και είναι ικανό τόσο να κλειδώσει όσο και να ξεκλειδώσει το μήνυμα. Και ο αποστολέας και ο παραλήπτης χρειάζονται το ίδιο κλειδί για την κωδικοποίηση και αποκωδικοποίηση του μηνύματος. Όταν ταξιδεύει ένα συμμετρικό κλειδί είναι κρίσιμο να μην πέσει σε χέρια άλλου πλην του κανονικού του παραλήπτη. Αν το συμμετρικό κλειδί πέσει σε εσφαλμένα χέρια, το μήνυμα μπορεί εύκολα να αποκωδικοποιηθεί και να πληγεί η ιδιωτικότητα του.

Η PKI προσθέτει ένα επιπλέον επίπεδο ασφάλειας κρυπτογραφώντας το συμμετρικό κλειδί μιας χρήσης με το δημόσιο κλειδί του παραλήπτη, ώστε μόνο αυτός να μπορεί να το αποκωδικοποιήσει με το ιδιωτικό του κλειδί. Το κρυπτογραφημένο συμμετρικό κλειδί μιας χρήσης επισυνάπτεται στο κρυπτογραφημένο μήνυμα και το μήνυμα είναι έτοιμο να σταλεί[39].

6.2.3. Firewall (τείχος προστασίας)

Στην επιστήμη των υπολογιστών ο όρος **firewall** ή **τείχος προστασίας** χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίσουν το

[39] *«Certified e□Commerce Consultant»* deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf –

firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες[40].

6.2.4. Ψηφιακά πιστοποιητικά

Τα ψηφιακά πιστοποιητικά, ή πιστοποιητικά δημοσίου κλειδιού είναι ηλεκτρονικές φόρμες ταυτοποίησης που μπορούν να επικυρωθούν από μια αναγνωρισμένη αρχή. Όλοι οι PKI χρήστες πρέπει να έχουν αυτή την μορφή ταυτοποίησης. Τα πιστοποιητικά μπορούν να περιέχουν μια ποικιλία πληροφοριών, συμπεριλαμβανομένων της επωνυμίας του κατόχου, του δημοσίου κλειδιού,

της ημερομηνίας λήξης του πιστοποιητικού, των λειτουργιών που μπορεί να εκτελέσει το δημόσιο κλειδί (κρυπτογράφηση, αποκρυπτογράφηση, ή επαλήθευση ψηφιακής υπογραφής), της ψηφιακής υπογραφής του εκδότη, του σειριακού του αριθμού και της μεθόδου κρυπτογράφησης. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιήσουν ή επαληθεύσουν ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.

6.2.4.1. Αρχές πιστοποίησης

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

Η διαδικασία πιστοποίησης περιγράφεται παρακάτω:

1. Ο συνδρομητής (αποστολέας) αιτείται στην αρχή πιστοποίησης ένα ψηφιακό πιστοποιητικό.
2. Η αρχή πιστοποίησης επαληθεύει τον συνδρομητή και εκδίδει το ψηφιακό πιστοποιητικό.
3. Η αρχή πιστοποίησης δημοσιεύει το πιστοποιητικό δημόσια, σε ένα on-line repository.
4. Ο συνδρομητής υπογράφει τα μηνύματα του με ένα ιδιωτικά κλειδί και τα στέλνει στους παραλήπτες.
5. Ο παραλήπτης επαληθεύει την ψηφιακή υπογραφή με χρήση του δημοσίου κλειδιού του αποστολέα και αιτείται επαλήθευση του

[40] *thegreekz.com/forum/showthread.php?t=386452 - 59k -*

ψηφιακού πιστοποιητικού του αποστολέα από το δημόσιο repository.

Το repository αναφέρει το status του ψηφιακού πιστοποιητικού του αποστολέα.

6.2.4.2. SSL

Πιστοποιητικά Ασφαλείας Servers (SSL certificates)

Για τις δουλειές μέσω διαδικτύου, το κλειδί είναι η δημιουργία εμπιστοσύνης. Για να μπορεί μια Τράπεζα να έχει επιτυχημένες ηλεκτρονικές υπηρεσίες, απαιτείται οι πελάτες της να την εμπιστεύονται για την ασφάλεια των ευαίσθητων δεδομένων τους από υποκλοπές και επιθέσεις. Εγκαθιστώντας ένα 128-bit SSL πιστοποιητικό ασφαλείας server από μια αναγνωρισμένη αρχή πιστοποίησης στο site της, μια Τράπεζα ασφαλίζει τις υπηρεσίες της και δημιουργεί αίσθημα σιγουριάς στον πελάτη, κρυπτογραφώντας όλες τις on line συναλλαγές. Με το SSL πιστοποιητικό ασφαλείας server οι πελάτες γνωρίζουν ότι ο δικτυακός τόπος είναι ασφαλής.

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

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

Το ασφαλές SSL πιστοποιητικό server είναι ένα ψηφιακό πιστοποιητικό που πιστοποιεί την ταυτότητα του δικτυακού τόπου στους browsers που χρησιμοποιούνται για την πρόσβαση σε αυτόν και κρυπτογραφεί την πληροφορία για τον server μέσω SSL (Secure Sockets Layer) τεχνολογίας. Το πιστοποιητικό λειτουργεί ως ηλεκτρονικό «διαβατήριο» που κατοχυρώνει τα αναγνωριστικά μιας on line οντότητας όταν αυτή κάνει δουλειές στο Internet. Όταν ένας χρήστης προσπαθήσει να στείλει εμπιστευτική πληροφορία σε ένα web server, ο browser του χρήστη διαβάζει το ψηφιακό πιστοποιητικό του server και εγκαθιστά μια ασφαλή σύνδεση. Ένα SSL πιστοποιητικό περιέχει την ακόλουθη πληροφόρηση:

- Το όνομα του κατόχου του πιστοποιητικού
- **Τον σειριακό αριθμό του πιστοποιητικού και την ημερομηνία λήξης του**
- Αντίγραφο του δημοσίου κλειδιού του κατόχου του

- Την ψηφιακή υπογραφή της αρχής πιστοποίησης που έκδωσε το πιστοποιητικό

Για να αποκτήσει μια Τράπεζα ένα SSL πιστοποιητικό πρέπει να το αιτηθεί από μια αναγνωρισμένη αρχή πιστοποίησης, η οποία θα πιστοποιήσει την ταυτότητα του αιτούντος και την κατοχή του domain ονόματος προτού εκδώσει το πιστοποιητικό.

Οι ορατές ενδείξεις ότι μια ασφαλής διαδικασία βρίσκεται σε εξέλιξη είναι το εικονίδιο της κλειδαριάς που υπάρχει στην γραμμή κατάστασης του browser και Όταν ένας χρήστης προσπαθήσει να καταχωρήσει προσωπικές πληροφορίες σε ένα μη ασφαλές site, ο μηχανισμός ασφαλείας του browser θα εμφανίσει μια προειδοποίηση στον χρήστη, υπενθυμίζοντας του ότι το site δεν είναι ασφαλές. Αντικρίζοντας μια τέτοια προειδοποίηση, οι χρήστες συνήθως δεν ολοκληρώνουν τις συναλλαγές τους και αναζητούν παρόμοιο ασφαλές site.[41]

6.2.4.3. Http

Το HTTPS (Secure HTTP) χρησιμοποιείται στην επιστήμη των υπολογιστών για να δηλώσει μία ασφαλή http σύνδεση. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα (443 αντί 80) και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες (πχ αριθμοί πιστωτικών καρτών, passwords κοκ)

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αναφέρεται στον συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Σε servers που χρησιμοποιούν το λειτουργικό σύστημα UNIX αυτό μπορεί να γίνει μέσω του προγράμματος OpenSSL.

[41] *Αγγελής Γ. Β.,(2005) «e-banking».*

Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.

Όπως αναφέρθηκε προηγουμένως, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας που περιγράφηκε στην προηγούμενη ενότητα και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται. Πολλοί χρήστες πιστωτικών καρτών θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση. Αυτό όμως δεν ισχύει: Όπως αναφέρθηκε και στην προηγούμενη παράγραφο το HTTPS (και το SSL) χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον server. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον server χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι να έχουν επιτεθεί στον server και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.[42]

6.*2.5. Ταυτοποίηση Τράπεζας*

Είναι απαραίτητο η ιστοσελίδα στην οποία καταχωρείτε τους προσωπικούς σας κωδικούς εισόδου να είναι πιστοποιημένη από έναν ανεξάρτητο παροχέα πιστοποίησης (Trusted Third Party). Για παράδειγμα η Eurobank έχει επιλέξει την εταιρία Verisign ως παροχέα πιστοποίησης της ταυτότητά της στο διαδίκτυο. Αυτό μπορεί εύκολα να αναγνωριστεί από την εμφάνιση ενός μικρού εικονιδίου με μορφή λουκέτου στο κάτω μέρος των σελίδων e-Banking, μέσω του οποίου μπορείτε να επιβεβαιώσετε ότι βρίσκεστε στο σωστό προορισμό.

6.2.6. *Μπλοκάρισμα Κωδικών*

Οι προσωπικοί κωδικοί χρήστη μπλοκάρονται μετά από 3 συνεχόμενες λανθασμένες προσπάθειες εισαγωγής στο σύστημα ή σε συνολικά 9 λανθασμένες

[42] *PC MAGAZINE, (2005), τεύχ.3, άρθρο με θέμα: «Οι καλύτερες λύσεις για προστασία στο Internet».*

μέσα σε μια εβδομάδα, καθώς η συνεχής λανθασμένες προσπάθειες θεωρούνται ύποπτες.

Παράλληλα με την απαραίτητη τεχνολογική υποδομή, η Eurobank διασφαλίζει τις ηλεκτρονικές συναλλαγές και με την υιοθέτηση αυστηρών διαδικασιών όσον αφορά την ανάπτυξη, διαχείριση και προσφορά της υπηρεσίας e-Banking[43].

6.2.7. Τι είναι το λογισμικό antivirus;

Πρόκειται για λογισμικό που χρησιμοποιείται για την προστασία του υπολογιστή από τους ιούς, αλλά και από άλλο βλαβερό υλικό. Τα προγράμματα αυτά εγκαθίστανται στον υπολογιστή μας και ελέγχουν όλα τα αρχεία που βρίσκονται σε αυτόν αλλά και τα συνημμένα σε e-mail αρχεία. Αν εντοπιστούν ιοί, το πρόγραμμα μας ενημερώνει αμέσως και, στις περισσότερες περιπτώσεις, απομονώνει ή επιδιορθώνει τα αρχεία που έχουν προσβληθεί από τον ιό. Ένα πρόγραμμα antivirus πρέπει να ενημερώνεται συνεχώς και μπορεί επίσης να χρησιμοποιηθεί για φιλτράρισμα ιστοσελίδων.[44]

Norton Antivirus

Το Norton Antivirus είναι προϊόν της εταιρείας Symantec. Προσφέρει ολοκληρωμένη προστασία από τους ιούς που μπορεί να προέρχονται από δισκέτες, CD, DVD, ή ακόμη και από το διαδίκτυο μέσω ιστοσελίδων ή και e-mails. Ο χρήστης όμως πρέπει να κάνει τακτική ανανέωση των δεδομένων για τους ιούς για να μπορεί να έχει τη μέγιστη προστασία. Η ενημέρωση γίνεται με αυτόματο τρόπο (Live update) ή και με το κατέβασμα του σχετικού αρχείου από δικτυακό τόπο της εταιρείας.[45]

[43] «Certified e□Commerce Consultant» *deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf – deicec.files.wordpress.com/2008/10*
[44] www.ethnos.gr/article.asp?catid=11905&subid=2&tag=8967&pubid=131452 - 51k –
[45] *pacific.jour.auth.gr/articles/article2.htm - 16k* «Ιοί υπολογιστών

ΚΕΦΑΛΑΙΟ 7

7. ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΜΕΣΩ E-BANKING ΚΑΙ ΑΣΤΙΚΗ ΚΑΙ ΠΟΙΝΙΚΗ ΠΡΟΣΤΑΣΙΑ

7.1. *Απλά βήματα για την ασφάλεια δεδομένων*

Η ασφάλεια είναι ένα θέμα που πρέπει να απασχολεί όλους τους χρήστες Η/Υ. Ο καθένας από μας είναι ικανός να προστατεύσει εύκολα και αποτελεσματικά τα δεδομένα του χωρίς να απαιτούνται ιδιαίτερες τεχνικές γνώσεις.

Μερικά απλά βήματα που πρέπει να ακολουθούν όλοι οι χρήστες είναι να:

- έχουν εγκατεστημένο λογισμικό αντιμετώπισης ιών (antivirus)
- ενημερώνουν τακτικά (update) το λογισμικό προστασίας από τους ιούς
- εκτελούν τακτικά τις συνιστώμενες ενημερώσεις λειτουργικού συστήματος που χρησιμοποιούν πχ Windows updates
- έχουν ενεργοποιημένο το firewall του λειτουργικού τους συστήματος
- αλλάζουν τακτικά τους κωδικούς ασφαλείας (passwords) που χρησιμοποιούν
- μην χρησιμοποιούν ως κωδικό ασφαλείας (password), τμήμα του ονόματος τους , της ημερομηνίας γέννησης ,ή τμήμα του username τους
- χρησιμοποιούν στους κωδικούς τους διάφορους τύπους χαρακτήρων πχ πεζά, κεφαλαία, αριθμούς καθώς και χαρακτήρες όπως #&%@! Κτλ
- ελέγχουν πάντοτε τα προγράμματα που λαμβάνουν από το Διαδίκτυο με το λογισμικό αντιμετώπισης ιών
- ελέγχουν πάντοτε τα συνημμένα αρχεία (attachments) από μηνύματα ηλεκτρονικού ταχυδρομείου με το antivirus (πριν τα ανοίξουν)
- αποφεύγουν να ανοίγουν συνημμένα από άγνωστο αποστολέα ή συνημμένα με περίεργο όνομα.
- Αποφεύγουν τη λήψη (download) προγραμμάτων από μη αξιόπιστες ιστοσελίδες[46]

[46] kesapt.uop.gr/index.php?option=content&task=view&id=116 - 25k –«Ασφάλεια δεδομένων – Αντιμετώπιση ιών»(10-2-06)

7.2. Τρόποι αποτροπής εισόδου επιβλαβούς λογισμικού στον υπολογιστή μας

Είναι σημαντικό να μην ανοίγουμε τα e-mails που λαμβάνουμε από άγνωστο αποστολέα. Πολλά από αυτά έχουν τίτλους που προσελκύουν την προσοχή, όπως «Κερδίσατε στην κλήρωση!» ή «Χρόνια Πολλά, σου έχω ένα δώρο» κ.ο.κ. Μην ανοίγουμε ποτέ τα συνημμένα σε τέτοιου είδους e-mails αρχεία, γιατί είναι εξαιρετικά πιθανόν, κάποιο από αυτά να εγκαταστήσει ιό ή σκουλήκι στον υπολογιστή μας.

Πρέπει να εγκαταστήσουμε λογισμικό antivirus στον υπολογιστή μας. Αυτό θα μας προστατεύσει από ιούς, βλαβερό λογισμικό και άλλου είδους απειλές. Μπορούμε ακόμη να εγκαταστήσουμε **ένα firewall (τείχος προστασίας),** το οποίο θα ελέγχει όλα τα αρχεία που μπαίνουν ή βγαίνουν από τον υπολογιστή μας.

Επίσης πρέπει να προσπαθήσουμε να αποφύγουμε ύποπτες ιστοσελίδες και αν μπούμε σε κάποια από αυτές κατά λάθος και μας φαίνεται περίεργη, να φύγουμε αμέσως. Αν εμφανιστούν παράθυρα που μας ζητούν να συμφωνήσουμε σε οτιδήποτε, πρέπει να τα κλείσουμε αμέσως και μην πατάμε κουμπιά που βρίσκονται μέσα σε αυτά[47].

7.3. Προτεραιότητα των τραπεζών η ασφάλεια των συναλλαγών

Για τις περισσότερες Τράπεζες η ασφάλεια των συναλλαγών αποτελεί πρώτη προτεραιότητα και γι αυτό οι επενδύσεις σε αυτό τον τομέα υπήρξαν και συνεχίζουν να είναι ιδιαίτερα σημαντικές. Η υιοθέτηση τεχνολογίας αιχμής με πρωτόκολλα επικοινωνίας και μηχανισμούς ταυτοποίησης συμβάλλουν τα μέγιστα στη διασφάλιση των ηλεκτρονικών συναλλαγών.

Κάποιες βασικές Συμβουλές που πρέπει να γνωρίζουν οι χρήστες που πραγματοποιούν συναλλαγές (e-banking) μέσω του internet, περιγράφονται παρακάτω:

1. Αγνοούμε e-mail στα οποία ζητούνται προσωπικά σας στοιχεία (αριθμός λογαριασμού, μυστικοί προσωπικοί κωδικοί, ονοματεπώνυμο κ.α.). Οι Τράπεζες δεν πρόκειται για κανένα λόγο να μας ζητήσουν τα προσωπικά μας στοιχεία μέσω e-mail ή τηλεφώνου. Για το λόγο αυτό να διαγράφουμε τα e-mail αυτά ως πλαστά και να αγνοούμε αντίστοιχες πιθανές

[47] www.ethnos.gr/article.asp?catid=11905&subid=2&tag=8967&pubid=131452 - 51k –

τηλεφωνικές κλήσεις. Σε περίπτωση που έχουμε λάβει πλαστό e-mail και έχουμε ήδη απαντήσει παρέχοντας προσωπικά μας στοιχεία, επικοινωνούμε άμεσα με τη Τράπεζά σας και ακολουθούμε τις οδηγίες που θα μας δοθούν.

2. Μην εισάγουμε τους μυστικούς προσωπικούς κωδικούς μας, αν δεν βεβαιωθούμε πριν ότι βρισκόμαστε στη σωστή διεύθυνση της τράπεζάς μας. Πληκτρολογούμε πάντα εμείς τη διεύθυνση της ιστοσελίδας της Τράπεζας που θέλουμε να επισκεφθούμε.

3. Μην συνδέουμε ποτέ μέσω εξωτερικού συνδέσμου (link). Να βεβαιωθούμε ότι στην ιστοσελίδα ηλεκτρονικής τραπεζικής της Τράπεζάς μας εμφανίζεται κάτω δεξιά και το εικονίδιο με το «λουκέτο» μέσω του οποίου μπορούμε ανοίγοντας το με διπλό κλικ, να επιβεβαιώσουμε ότι βρισκόμαστε στο ασφαλές περιβάλλον της Τράπεζάς σας.

4. Οι προσωπικοί κωδικοί, που χρησιμοποιούμε για την είσοδό μας στην υπηρεσία e-Banking είναι αυστηρώς προσωπικοί και σε καμία περίπτωση δεν πρέπει να τους μοιραζόμαστε. Η Τράπεζα δεν πρόκειται για κανέναν λόγο να μας τους ζητήσει και με κανένα απολύτως τρόπο.

5. Είναι απαραίτητο να αποστηθίσετε τους προσωπικούς σας κωδικούς και να μην τους φυλάσσετε σε γραπτή μορφή, καθώς υπάρχει ο κίνδυνος κλοπής αυτών. Οι προσωπικοί σας κωδικοί χρησιμοποιούνται αποκλειστικά για την υπηρεσία e-Banking της Τράπεζας και ως εκ τούτου επιβάλλεται αφενός να μην τους χρησιμοποιείτε σε άλλες, μη ασφαλείς ιστοσελίδες του Διαδικτύου αλλά και να τους αλλάζετε ανά τακτά χρονικά διαστήματα[48].

Οι κακόβουλες ενέργειες υποκλοπής προσωπικών κωδικών στοχεύουν κυρίως σε χρήστες οι οποίοι δεν λαμβάνουν τα κατάλληλα μέτρα προστασίας του υπολογιστή τους.

Ενδεικτικά αναφέρονται τα κατωτέρω μέτρα προστασίας:

- Ενημέρωση και αναβάθμιση των παραμέτρων ασφάλειας του υπολογιστή σας, συμπεριλαμβανομένου και του λειτουργικού σας συστήματος.

[48] *Αγγελής Γ.Βασίλης, (2005), «Η βίβλος του e-banking», εκδ. Νέων Τεχνολογιών, Αθήνα.*aggelis.50megs.com/bible.html - 34k

- Ø Εγκατάσταση προγραμμάτων στον υπολογιστή σας για την προστασία του από ιούς. Η εμφάνιση νέων και εξελιγμένων ιών καθιστά τη συχνή ανανέωση των προγραμμάτων που τους καταπολεμούν απαραίτητη.

Προσοχή κατά τη χρήση της υπηρεσίας e-Banking από υπολογιστές οι οποίοι δεν σας ανήκουν, όπως ενδεικτικά σε αεροδρόμια, internet cafe, κ.λπ. Εφόσον αποκτήσετε πρόσβαση στον διαδικτυακό τόπο της Τράπεζάς σας μέσω τέτοιων υπολογιστών βεβαιωθείτε ότι δεν έχετε προβεί σε αποθήκευση των προσωπικών σας στοιχείων σε αυτούς (πχ. αριθμός κάρτας) και δεν έχετε αφήσει ίχνη των ενεργειών σας, όπως ενδεικτικά τη διεύθυνση της Τράπεζας. Επίσης, εάν έχετε εκτελέσει κάποια συναλλαγή, διαγράψτε το ψηφιακό σας πιστοποιητικό (εάν χρησιμοποιείτε κάτι τέτοιο) από τον υπολογιστή[49].

7.4. Συναλλαγές σε ATM

Θορυβημένη εμφανίζεται το τελευταίο διάστημα η Ελληνική Ένωση Τραπεζών με αφορμή την επανεμφάνιση και κυκλοφορία παραπλανητικών ηλεκτρονικών μηνυμάτων αλλά και ως προς τη χρήση του κωδικού "PIN" στα ATM.

Έτσι εξέδωσε ακόμη μια ανακοίνωση μέσα σε πολύ μικρό χρονικό διάστημα δίνοντας συμβουλές για ασφαλείς συναλλαγές.

Ένα κλασικό παράδειγμα είναι η φήμη που κυκλοφόρησε ότι με αντίστροφη πληκτρολόγηση του PIN μπορείτε να ειδοποιήσετε για ενδεχόμενη κλοπή:

Επιτυχείς συναλλαγές στα ATM γίνονται όταν πληκτρολογείτε αποκλειστικά το σωστό PIN, το οποίο πρέπει να γνωρίζετε μόνο εσείς. Δεν πρέπει σε καμιά περίπτωση να κάνετε ανάστροφη πληκτρολόγηση του όπως προτείνεται με παραπλανητικά ηλεκτρονικά μηνύματα που διακινούν διάφοροι κακόβουλοι στο Διαδίκτυο.

Τα ATM αναγνωρίζουν ως λάθος πληκτρολόγηση, όλους ανεξαιρέτως τους αριθμούς πλην του μοναδικού PIN , που σας δόθηκε από την τράπεζά σας ή επιλέξατε ο ίδιος. Συνεπώς είναι λάθος και η ανάστροφη πληκτρολόγησή του και σε τέτοια περίπτωση μόνη συνέπεια θα είναι να παρακρατηθεί η κάρτα σας αφού όλα τα ATM, για λόγους πρόληψης και ασφάλειας των συναλλαγών, παρακρατούν την κάρτα, αν

[49] www.dart.gov.gr/?q=node/96 - 28k

κατά τη διάρκεια μιας συναλλαγής πληκτρολογήσετε λάθος PIN τρεις συνεχόμενες φορές.

Οι πάγιες οδηγίες και συστάσεις για τη χρήση των ΑΤΜ πρέπει να ακολουθούνται απολύτως, διότι το ηλεκτρονικό έγκλημα «περισσεύει» το τελευταίο χρονικό διάστημα:

Ελέγχετε συχνά ότι η κάρτα βρίσκεται στο πορτοφόλι σας, αποστηθίστε το PIN και μην τον σημειώνετε με οποιονδήποτε τρόπο σε μέσο που μπορεί να συνδυαστεί με την κάρτα.

Προσέχετε κατά τη διάρκεια της συναλλαγής: αν υπάρχει επόμενος πελάτης βεβαιωθείτε ότι βρίσκεται σε απόσταση ασφαλείας ώστε να μην μπορεί να αντιληφθεί τι πληκτρολογείτε. Αν προηγείται άλλος συναλλασσόμενος, φροντίστε να διατηρείτε λογική απόσταση απ' αυτόν. Χρησιμοποιείστε το σώμα σας με τρόπο ώστε να μην φαίνεται η συναλλαγή.

Μην ανακοινώνετε το PIN σε τρίτα πρόσωπα ακόμα και συγγενείς και ποτέ μην επιλέγετε PIN που μπορεί να προβλεφθεί όπως ημερομηνία γέννησης, αριθμός αυτοκινήτου κλπ, ενώ τα ΑΤΜ σας δίνουν τη δυνατότητα να αλλάζετε τον αριθμό αυτό. Μπορεί να το κάνετε συχνά για αποφυγή δυσάρεστων περιστατικών.

Τον αριθμό αυτό δεν τον γνωστοποιούμε σε πρόσωπα τα οποία με οποιονδήποτε τρόπο επιδιώκουν να μας αποσπάσουν αυτή την πληροφορία, ισχυριζόμενοι ότι είναι υπάλληλοι τραπεζών ή άλλων φορέων ή Αρχών. Οι τράπεζες δεν έχουν αναθέσει σε υπαλλήλους τους ή τρίτους ποτέ τέτοια καθήκοντα.

Αν η κάρτα σας παρακρατηθεί από το ΑΤΜ, βεβαιωθείτε γι' αυτό, και επικοινωνήστε άμεσα με την τράπεζα ενώ αν την χάσετε ή σας την κλέψουν δηλώστε αμέσως την απώλεια ή την κλοπή στην Τράπεζα και μόνο στα τηλέφωνα που εμφανίζονται στις οθόνες των ΑΤΜ. Στα ίδια τηλέφωνα αναφέρατε στη τράπεζά σας οτιδήποτε ασυνήθιστο παρατηρήσετε στο ΑΤΜ ή κατά τη διάρκεια της συναλλαγής σ' αυτό.[50]

[50] *PC MAGAZINE, (2006), τεύχ.2, άρθρο με θέμα: «Ασφάλεια, νέες απειλές, νέα αντιμετώπιση».*

7.5. Νομικά θέματα ηλεκτρονικής τραπεζικής

7.5.1. Γενικά

Η εξάπλωση του διαδικτύου την τελευταία δεκαετία και η χρήση του για εμπορικούς σκοπούς δημιούργησε νέα δεδομένα στο χώρο των επιχειρήσεων. Οι νέες τεχνολογίες μετέβαλλαν ραγδαία τόσο το χώρο δράσης των επιχειρήσεων, την αγορά, όσο και την οργανωσιακή δομή των οικονομικών μονάδων. Στα πρώτα στάδια ανάπτυξης του ηλεκτρονικού εμπορίου οι πληρωμές γίνονταν εκτός του διαδικτύου με καταβολή των ποσών σε κάποια τράπεζα. Ο αναχρονιστικός όμως αυτός τρόπος χρηματικής εκκαθάρισης των διαδικτυακών συναλλαγών δεν συμβάδιζε με την ταχύτητα και την αξιοπιστία που απαιτούν οι σύγχρονες διαδικτυακές συναλλαγές[51].

Η παγκόσμια διάσταση του Internet πλέον επιβάλλει οποιαδήποτε εμπορική και επιχειρηματική δραστηριότητα σε αυτό να εξετάζεται υπό το πρίσμα της διεθνούς δραστηριότητας του και συνεπώς πρέπει va εξετάζεται το ρυθμιστικό πλαίσιο της διασυνοριακής παροχής τραπεζικών και χρηματοοικονομικών υπηρεσιών.

7.5.2. Το Internet banking υπό την εποπτεία των Κεντρικών Τραπεζών και της Ε.Ε.

Το Internet banking, ως παροχή . τραπεζικών υπηρεσιών ιδίως προς καταναλωτές, υπάγεται στην εποπτεία των Κεντρικών τραπεζών και τις σχετικές οδηγίες της ΕΕ για. τα πιστωτικά ιδρύματα. Επομένως ισχύει η νομοθεσία για τα χρηματοδοτικά και πιστωτικά ιδρύματα:

α) στην εποπτεία της Κεντρικής τράπεζας

β) στις διατάξεις για τον περιορισμό του σκοπού και των ποσοστών συμμετοχής φυσικών ή νομικών προσώπων σε πιστωτικά ιδρύματα ή της συμμετοχής των πιστωτικών ιδρυμάτων σε άλλες επιχειρήσεις, και

γ) Στις ειδικές διατάξεις για την δημοσιοποίηση των οικονομικών αποτελεσμάτων.

Οι ηλεκτρονικές συναλλαγές διέπονται από την οδηγία 2000/31 (οδηγία για ηλεκτρονικό εμπόριο) που εισάγει την αρχή του κράτους προέλευσης δηλαδή ο τόπος εγκατάστασης της εταιρείας που ασχολείται με ηλεκτρονικές συναλλαγές είναι εκεί που ασκεί την οικονομική της δραστηριότητα.

[51] *Αγγελής Γ.Βασίλης,(2005).*

Επομένως στις ελληνικές τράπεζες ως προς το σκέλος της τραπεζικής νομοθεσίας ισχύει ο Ν. 2076/92 για τα χρηματοδοτικά και πιστωτικά ιδρύματα,

Το θεσμικό πλαίσιο πληρωμών που μπορεί να χρησιμοποιηθεί και στο Internet banking ορίζεται από την Οδηγία 98/26 με την οποία έχει ήδη προσαρμοστεί το ελληνικό δίκαιο με το Ν.2789/2000. Το νομικό πλαίσιο για τις διασυνοριακές πληρωμές καθορίζεται επιπλέον από την οδηγία 97/5 για τις συνοριακές μεταφορές πιστώσεων μέχρι 50.000 Ευρώ. Σύμφωνα με την οδηγία αυτή:

- Για την εκτέλεση της εντολής ευθύνεται η τράπεζα του εντολέα,
- Θεσπίζεται υποχρέωση για αναλυτική πληροφόρηση των πελατών πριν και μετά από την εκτέλεση της εντολής
- Η εντολή πρέπει να διεκπεραιωθεί εντός πέντε εργάσιμων ημερών
- Προβλέπονται ειδικές δεσμεύσεις για τις προμήθειες και τα έξοδα, και
- Προβλέπεται ειδική αποζημίωση σε περίπτωση μη εκπλήρωσης.

Στην Ελλάδα ρητή αναφορά στο internet banking υπάρχει στην Πράξη Συμβουλίου Νομισματικής Πολιτικής 50/31.7.2002: «καθορισμός πλαισίου επίβλεψης συστημάτων πληρωμών», στην οποία προβλέπεται άσκηση επίβλεψης από την Τράπεζα της Ελλάδος και στους τρόπους πρόσβασης και στα υ-ποστηρικτικά προϊόντα των συστημάτων πληρωμής.

7.5.3. Προστασία του καταναλωτή

Οι μονάδες e-banking πρέπει να συμμορφώνονται με τον Ν. 2251/94 περί προστασίας του καταναλωτή ο οποίος ορίζει τα ακόλουθα:

- ακυρότητα υπέρ του καταναλωτή,
- υποχρέωση για ανακοίνωση της ταυτότητας της επιχείρησης και για λε-πτομερή περιγραφή των χαρακτηριστικών, της τιμής και του κόστους του προσφερόμενου προϊόντος.
- υποχρέωση περιγραφής του δικαιώματος υπαναχώρησης του καταναλωτή
- υποχρέωση περιγραφής της διάρκειας τυχόν προσφορών και της διάρκειας σύμβασης.
- Η οδηγία 2002/65 (σχετικά με την εξ αποστάσεως εμπορία χρηματοοικονομικών υπηρεσιών προς καταναλωτές) καθορίζει ότι καταναλωτής είναι κάθε πρόσωπο το οποίο στο πλαίσιο των συμβάσεων εξ αποστάσεως ενεργεί για σκοπούς εκτός του πεδίου της εμπορικής ή επαγγελματικής του δραστηριότητας». Η Οδηγία προβλέπει:

α) υποχρέωση για λεπτομερή πληροφόρηση του καταναλωτή πριν και μετά από την κατάρτιση της σύμβασης, για την υπηρεσία, τη σύμβαση και τα μέσα αποκατάστασης

β) υποχρέωση για ανακοίνωση των συμβατικών όρων σε χαρτί ή άλλο σταθερό μέσο,

γ) δικαίωμα υπαναχώρησης εντός 14 ημερών εκτός από

α. τις υπηρεσίες με διακυμάνσεις τιμών (π.χ. συνάλλαγμα, futures, swaps, options)

β. τις βραχυπρόθεσμες συμβάσεις (π.χ. ασφαλιστήρια για ταξίδια)

γ. τις συμβάσεις, η εκτέλεση των οποίων ολοκληρώθηκε και

δ. τις συμβάσεις ασφαλίσεων ζωής για τις οποίες προβλέπεται δικαίωμα υπαναχώρησης εντός 30 ημερών (Οδηγία 90/619)

δ) δυνατότητα ακύρωσης των συναλλαγών με πιστωτική κάρτα

ε) πρόβλεψη μέτρων για τις μη αιτηθείσες υπηρεσίες και την αυτόκλητη επικοινωνία (π.χ. με ανεπιθύμητα ηλεκτρονικά μηνύματα).

7.5.4. Προστασία προσωπικών δεδομένων

Για την ασφάλεια των προσωπικών δεδομένων ισχύουν οι Ν. 2472/97 (προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα), Ν. 2772/99 (προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) και η οδηγία 2002/58 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Ιδιαίτερη σημασία για το internet banking αποκτά η απαγόρευση να διαβιβάζονται δεδομένα σε τρίτες χώρες εκτός ΕΕ, που δεν παρέχουν ικανοποιητικό επίπεδο προστασίας. Το πρόβλημα είναι σοβαρό, αφού στο Internet κάθε μετάδοση δεδομένων είναι διασυνοριακή, ενώ ακόμη και στη μετάδοση εντός των «κοινοτικών» συνόρων είναι πιθανό τα δεδομένα να διέλθουν από τρίτες χώρες.[52]

[52] *Αγγελής Β.,(2005). « Η βίβλος του e-banking »*

ΜΕΡΟΣ Δ΄

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΚΕΦΑΛΑΙΟ 8

8. ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

8.1. Γενικά

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

8.2. Πολιτική των τραπεζών η μη κοινοποίηση στοιχείων

Στοιχεία για το ηλεκτρονικό έγκλημα δεν κοινοποιούνται δημοσίως, αλλά υπολογίζεται ότι στις Η.Π.Α. χάνονται ετησίως περίπου 11 δισεκατομμύρια δολάρια από εταιρείες και καταναλωτές λόγω αυτής της μορφής εγκλήματος. Το μεγαλύτερο μέρος προέρχεται από οικονομικά ιδρύματα.

Μάλιστα το μεγαλύτερο μέρος των ζημιών δεν προκύπτει από τις κλοπές χρημάτων, αλλά από έξοδα που κάνουν οι εταιρείες μετά από τέτοιου είδους επιθέσεις, προκειμένου να διασφαλίσουν τα συστήματά τους ώστε να μην ξανασυμβούν. Ειδικοί σε θέματα ασφάλειας έχουν υπολογίσει ότι μια τράπεζα μπορεί να ξοδέψει μέχρι και 1 εκατομμύριο δολάρια σε εξοπλισμό και συμβούλους ασφάλειας προκειμένου να διορθώσει τις ατέλειες και να κλείσει τις «τρύπες» στο σύστημά της.

Το πρόβλημα πάντως δεν προβάλλεται στις πλήρεις του διαστάσεις για ευνόητους λόγους. Οι μεγαλύτερες και εντυπωσιακότερες επιθέσεις είναι αυτές που θα δοθούν στη δημοσιότητα, οι υπόλοιπες και περισσότερες, κρατούνται κρυφές[53].

[53] *www.go-online.gr/ebusiness/specials/article.html?article_id=4 - 33k -*

8.3. Εκμετάλλευση των αδυναμιών του συστήματος από τους εισβολείς

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

Και χωρίς τη βοήθεια εκ των έσω, πάντως, οι εισβολείς μπορούν να εκμεταλλευτούν την πρόσβαση που έχουν οι πελάτες της τράπεζας από το σπίτι τους, οι περισσότεροι από τους οποίους δεν χρησιμοποιούν λογισμικό για ασφάλεια. Οι άνθρωποι αυτοί αποτελούν τους πιο προκλητικούς στόχους, μια και δεν έχουν συνείδηση του μεγέθους της ζημιάς που μπορούν να κάνουν ανοίγοντας απλά μια επισύναψη στο ηλεκτρονικό τους ταχυδρομείο ή ακολουθώντας ένα link. Οι απλοί χρήστες πέφτουν πολύ εύκολα θύματα προγραμμάτων που υποτίθεται ότι κάνουν κάτι χρήσιμο για αυτούς, αλλά στην πραγματικότητα ανοίγουν «τρύπες» ασφάλειας στο σύστημα επιτρέποντας σε χάκερς, να έχουν πρόσβαση σε αυτό.

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

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

Ένας άλλος τρόπος είναι να χτυπήσουν τις μικρές, τοπικές τράπεζες οι οποίες μπήκαν στον τομέα του e-banking εσπευσμένα προκειμένου να διατηρήσουν τον ανταγωνισμό με τις μεγαλύτερες τράπεζες. Δυστυχώς όμως λόγω αυτής της βιασύνης,

οι τράπεζες αφήνουν πολλές «τρύπες» στα συστήματά τους, κάτι που οι επίδοξοι εισβολείς εκμεταλλεύονται πολύ εύκολα.

Οι ειδικοί μας πληροφορούν ότι κλοπές ποσών από 5 μέχρι 10 χιλιάδες δολαρίων μπορούν να πραγματοποιηθούν σε χρονικό διάστημα μερικών εβδομάδων. Για ποσά μέχρι και 1 εκατομμυρίου δολαρίων χρειάζονται 4 μέχρι και 6 μήνες.[54]

8.4. Το διεθνές ηλεκτρονικό έγκλημα

Κέρδη δισεκατομμυρίων ευρώ, η εγκληματικότητα στο Διαδίκτυο έχει περάσει προ πολλού από την εποχή της ερασιτεχνικής πειρατείας σ' εκείνη του οργανωμένου εγκλήματος, προειδοποιούν οι ειδικοί.

Η Γερμανική Υπηρεσία Ασφάλειας της Πληροφορικής (BSI) παρουσίασε την έκθεση που συντάσσει κάθε δύο χρόνια πάνω σ' αυτό το αντικείμενο και το συμπέρασμα είναι ξεκάθαρο: «η κατάσταση είναι ακόμη πιο καταστροφική απ' ό,τι φοβόμασταν» και κάνουν πλέον ανοιχτά λόγο για "οργανωμένο έγκλημα".

Η BSI εκτιμά ότι το ηλεκτρονικό έγκλημα αποφέρει κέρδη δισεκατομμυρίων ευρώ, ενώ ρώσος ειδικός από τους κορυφαίους στα προγράμματα κατά των ιών, ανεβάζει το ποσό στα 100 δισεκατομμύρια ευρώ το χρόνο.

Είναι δύσκολο να υπολογιστούν ακριβώς οι απώλειες, καθώς καμία εταιρεία δεν είναι διατεθειμένη να παραδεχθεί δημόσια ότι έχει πέσει θύμα απάτης.

Η πιο κερδοφόρα ηλεκτρονική απάτη είναι η αποστολή "σπαμ" ή η "ομηρία", όπου μπλοκάρουν μία ιστοσελίδα, για παράδειγμα, ηλεκτρονικού εμπορίου, και απαιτούν "λύτρα" για να την απελευθερώσουν!

Επίσης, η κλοπή εμπιστευτικών δεδομένων από μεγάλες εταιρείες ή από ιστοσελίδες όπως το Facebook ή το MySpace, οι οποίες είναι πλούσιες σε προσωπικά δεδομένα, καθώς και η υφαρπαγή τραπεζικών πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου από ανυποψίαστους χρήστες.

Το μεγάλο πρόβλημα είναι ότι η σύλληψη των "ηλεκτρονικών" εγκληματιών είναι σχεδόν αδύνατη, όπως εξάλλου και η ρύθμιση αυτού του εικονικού κόσμου, ο οποίος μεταβάλλεται ραγδαία και ακατάπαυστα. Οι ειδικοί συμβουλεύουν τους χρήστες του Διαδικτύου να είναι πάντα επιφυλακτικοί και προειδοποιούν ότι πρέπει να σταματούμε κάθε συναλλαγή αμέσως μόλις αντιληφθούμε ότι ο υπολογιστής μας

[54] www.go-online.gr/ebusiness/specials/article.html?article_id=**4** - 33k – «Κίνδυνοι του e-banking»

συμπεριφέρεται περίεργα. Η μόνη λύση είναι να εισαχθεί στα σχολεία "μάθημα ασφαλούς πληροφορικής", προκειμένου ο καθένας να μπορεί να αντιμετωπίσει την ηλεκτρονική πειρατεία, η οποία πλέον "δεν είναι παιχνίδι"!!![55]

8.5. Ηλεκτρονικό έγκλημα στην Ελλάδα

Η Ελλάδα καταλαμβάνει την 11η θέση σε παγκόσμια κλίμακα στη λίστα με τις 20 χώρες που δέχθηκαν, σύμφωνα με την έγκυρη εταιρεία ασφάλειας υπολογιστικών συστημάτων Symantec, τις περισσότερες επιθέσεις από ιούς υπολογιστών κατά το πρώτο εξάμηνο του έτους 2004, οπότε και καταγράφηκαν περί τις 5.500 επιθέσεις ανά 100 χιλιάδες χρήστες.

Αν λάβουμε υπόψη μας ότι οι Έλληνες χρήστες είναι περίπου 3 εκατομμύρια, οι συνολικές επιθέσεις από ιούς υπολογιστών κατά το πρώτο εξάμηνο του έτους 2004, υπολογίζονται σε περίπου 160.000, μόνο στην Ελλάδα. Οι ιοί που προτίμησαν περισσότερο τους υπολογιστές των Ελλήνων χρηστών ήταν ο Slammer και ο Gaobot, ενώ οι περισσότερες επιθέσεις προέρχονταν από τις ΗΠΑ και την Κίνα.

8.6. Περιπτώσεις ηλεκτρονικών επιθέσεων

1. **Citibank (1994).**

Περιστατικό: Ο Ρώσος χάκερ Βλαντιμίρ Λέβιν απέσπασε ποσό από λογαριασμούς της Citibank που υπολογίστηκε ότι ανερχόταν στα 10 εκατομμύρια δολάρια. Απέκτησε πρόσβαση στα δίκτυα της τράπεζας από την Αγία Πετρούπολη στη Ρωσία. Όταν συνελήφθη από την Σκότλαντ Γιαρντ και το FBI, παραδέχτηκε ότι χρησιμοποίησε κλεμμένους κωδικούς και passwords από πελάτες της τράπεζας και μετέφερε ποσά στο λογαριασμό του. Το 1998, ένα δικαστήριο στις Η.Π.Α. τον καταδίκασε σε 3 χρόνια κάθειρξη. Η τράπεζα ανέκτησε όλο το ποσό εκτός από 400.000 δολάρια.

[55] www.evdomi.gr/pub/starcms/repository/static/articles/ar_31258_1.asp - 22k - «Φλέβα χρυσού το διαδίκτυο για κάθε είδους απάτες»

2. **ABN AMRO (Ολλανδική Πολυεθνική Τράπεζα) Σεπτέμβριος 2000.**

Περιστατικό: Ένα ολλανδικό τηλεοπτικό πρόγραμμα αποκάλυψε πως χάκερς, έκλεβαν σημαντικές πληροφορίες των πελατών της τράπεζας. Οι χάκερς έστελναν στους πελάτες της τράπεζας μηνύματα ηλεκτρονικού ταχυδρομείου που υποτίθεται ότι προερχόταν από την τράπεζα. Τα mails αυτά εγκαθιστούσαν στους υπολογιστές των πελατών προγράμματα τα οποία επέτρεπαν στους χάκερς να έχουν πρόσβαση σε κρίσιμες πληροφορίες των λογαριασμών τους και με αυτόν τον τρόπο να μεταφέρουν χρήματα από αυτούς. Η τράπεζα διένειμε καινούργιες εκδόσεις του λογισμικού της.

3. **Charles Schwab (Η μεγαλύτερη χρηματιστηριακή εταιρεία στις Η.Π.Α.) Δεκέμβριος 2000.**

Περιστατικό: Ο δικτυακός τόπος της εταιρείας έδινε τη δυνατότητα σε χάκερς να έχουν πρόσβαση σε όλους τους λογαριασμούς των πελατών της. Μάλιστα, όσο ο πελάτης ήταν συνδεδεμένος στο σύστημα, ο χάκερ μπορούσε να αγοράσει και να πουλήσει μετοχές από το λογαριασμό του.

4. **Barclays Bank (Μια Αγγλική Τράπεζα που ισχυρίζεται ότι διαχειρίζεται τους περισσότερους online λογαριασμούς σε όλο το Ηνωμένο Βασίλειο) Ιούλιος 2000.**

Περιστατικό: Ένα ελάττωμα στο λογισμικό του συστήματος της τράπεζας επέτρεπε στους πελάτες της να βλέπουν τις λεπτομέρειες των λογαριασμών των υπολοίπων πελατών. Η τράπεζα έκλεισε το σύστημα μόλις ανακάλυψε το πρόβλημα.

5. **Nara Bank, Western Union, Central National Bank (Texas). Απρίλιος 2001.**

Περιστατικό: Αμερικανοί εισαγγελείς κατηγόρησαν δυο Ρώσους για ηλεκτρονικά εγκλήματα που σχετίζονταν με μια σειρά επιθέσεων σε δίκτυα τραπεζών και άλλων εταιρειών. Οι δύο χάκερς, εισέβαλαν στα συστήματα των εταιρειών, έκλεψαν πολύτιμες πληροφορίες και κατόπιν εμφανίζονταν στις εταιρείες ως σύμβουλοι ασφαλείας και προσέφεραν τις υπηρεσίες τους για να διορθωθούν τα σφάλματα.[56]

[56] *www.go-online.gr/ebusiness/specials/article.html?article_id=4 κίνδυνοι του e-banking.*

ΣΥΜΠΕΡΑΣΜΑΤΑ

Αποτελεί πλέον κοινή διαπίστωση του γεγονότος ότι οι τράπεζες δεν μπορούν να είναι σήμερα ανταγωνιστικές εντός και εκτός συνόρων χωρίς να έχουν στη διάθεση τους όλη τη σύγχρονη τεχνολογία. Με την εφαρμογή της ηλεκτρονικής τραπεζικής οι τράπεζες, παρά το αρχικά υψηλό κόστος που απαιτεί ένα σύστημα ηλεκτρονικής τραπεζικής για να εγκατασταθεί, κατορθώνουν να μειώσουν το λειτουργικό τους κόστος και να παραμείνουν ανταγωνιστικές προσελκύοντας ταυτόχρονα νέους πελάτες. Επίσης οι πελάτες των τραπεζών επωφελούνται από την πληθώρα των υπηρεσιών που τους παρέχονται χάρη στη νέα τεχνολογία, καθώς πλέον με το πάτημα ενός κουμπιού τελειώνουν δουλειές που παραδοσιακά απαιτούσαν πολλή ώρα.

Ωστόσο ιδιαίτερη προσοχή πρέπει να δοθεί στο θέμα της ασφάλειας (Κρυπτογράφηση, firewalls, Αρχές Πιστοποίησης, SSL) ώστε να ελαχιστοποιηθούν οι ηλεκτρονικές επιθέσεις (Phising, Key Loggers, Sniffers, Δούρειοι Ίπποι) και να διασφαλιστεί η αξιοπιστία των ηλεκτρονικών συναλλαγών, καθώς ένα ευάλωτο σε επιθέσεις σύστημα μπορεί να αποβεί καταστροφικό τόσο για τους πελάτες όσο και για τις τράπεζες. Η διοίκηση των χρηματοπιστωτικών οργανισμών καλείται να πάρει τη σωστή απόφαση για την υιοθέτηση της κατάλληλης στρατηγικής όσον αφορά το e-banking που θα μεγιστοποιεί την αξία της επιχειρηματικής μονάδας και θα δίνει συγκριτικό πλεονέκτημα έναντι του ανταγωνισμού.

Τέλος παρά το γεγονός ότι την Ελλάδα η διείσδυση της ηλεκτρονικής τραπεζικής είναι ακόμα πολύ μικρότερη σε σχέση με την Ευρώπη και τον υπόλοιπο κόσμο, αναμένεται τα επόμενα χρόνια με την επικράτηση του ευρυζωνικού internet σε συνδυασμό με την εξοικείωση των πολιτών με τις νέες τεχνολογίες να αρθούν τα όποια εμπόδια και να δοθεί νέα ώθηση στην ηλεκτρονική τραπεζική και τις ηλεκτρονικές πληρωμές.

Βιβλιογραφία

ΠΗΓΕΣ

1. Αγγελής Γ. Βασίλης, (2005), ***«Η βίβλος του e-banking»,*** εκδ. Νέων Τεχνολογιών, Αθήνα.
2. Κατσουλάκος Γιάννης, (2001), ***«Νέα Οικονομία, Διαδίκτυο και Ηλεκτρονικό Εμπόριο»,*** εκδ. Κέρκυρα, Αθήνα.
3. *Harley Hahn&Rick Stout,* ***Το μεγάλο βιβλίο του Internet****, Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ Αθήνα 1995*
4. *Richard I. Hillman & Kane Wong (2000),* ***«Electronic Banking»,*** *Diane Publishing Co.*

Διαδίκτυο

1. *www.pcw.gr/StepByStep/secure_purchases_internet/233.html - 109k «Ασφαλείς συναλλαγές μέσω Internet»*
2. *Κραπης Βασίλειος, (2007) «Η ηλεκτρονική τραπεζική ως ανταγωνιστικό πλεονέκτημα στη σύγχρονη δικτυακή οικονομία»*
3. *el.wikipedia.org/wiki/Διαδίκτυο -*
4. *www.go-online.gr*
5. *«Certified e□Commerce Consultant» deicec.files.wordpress.com/2008/10/acta_cec_textbook.pdf –*
6. *Αν. Παπαϊωάννου, (2005) (www.economia.gr/index.php?Itemid=28&id=414&option= om_content&task=view - 53k «Internetbanking: Συμφέρει, αλλά προσοχή στους χάκερ»*
7. *www.google.gr*
8. *www.tovima.gr/default.asp?pid=2&artid=127395&ct=34&dt*
9. *users.otenet.gr*
10. *www.in.gr*
11. *News .pramnos. net/story58-976.html – 3 l k – (2009)<<Οι δικτυακές απειλές… δεν πάνε διακοπές*

12. *www.computeractive.gr*
13. *www.geocities.com/zak_gr_2000/ - 8k – «Ηλεκτρονικό εμπόριο», Ζακ Μαισης*
14. *dspace.lib.uom.gr/**bit**stream/2159/3749/2/karakizosMsc2007.pdf*
15. *www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=98 - 32k*
16. *thegreekz.com/forum/showthread.php?t=386452 - 59k –*
17. *www.ethnos.gr/article.asp?catid=11905&subid=2&tag=8967&pubid=131452 - 51k –*
18. *pacific.jour.auth.gr/articles/article2.htm - 16k «Ιοί υπολογιστών*
19. *kesapt.uop.gr/index.php?option=content&task=view&id=116 - 25k –«Ασφάλεια δεδομένων – Αντιμετώπιση ιών»(10-2-06)*
20. *www.dart.gov.gr/?q=node/96 - 28k*
21. *www.evdomi.gr/pub/starcms/repository/static/articles/ar_31258_1.asp - 22k - «Φλέβα χρυσού το διαδίκτυο για κάθε είδους απάτες»*

Περιοδικά

1. **PC MAGAZINE, (2005), τεύχ.3, άρθρο με θέμα: «Οι καλύτερες λύσεις για προστασία στο Internet».**
2. **PC MAGAZINE, (2006), τεύχ.2, άρθρο με θέμα: «Ασφάλεια, νέες απειλές, νέα αντιμετώπιση».**

ΓΛΩΣΣΑΡΙΟ

Arpanet	Το πρώτο στον κόσμο επιχειρησιακών πακέτων δίκτυο και ο προκάτοχος του παγκόσμιου Διαδικτύου
Ascii (American Standard Code)	Κώδικας για ανταλλαγή πληροφοριών, η αριθμητική εκπροσώπηση ενός χαρακτήρα
Assembler	Συναρμολογητής
ATM (Asynchronous Transfer Mode)	Μέθοδος επικοινωνίας μεταξύ υπολογιστών που χρησιμοποιείται ευρέως σήμερα, σε εφαρμογές όπως οι τραπεζικές συναλλαγές
Barcode	γραμμωτός κώδικας
Browser	Πρόγραμμα που επιτρέπει στον χρήστη να «περιηγείται» στις ιστοσελίδες του Παγκόσμιου Ιστού (World Wide Web, ή απλώς w.w.w.) Οι πιο δημοφιλείς browser είναι οι Netscape Navigator και ο Microsoft Internet Explorer
Collaboration platforms	Οι πλατφόρμες συνεργασίας
Data Link Layer	Πρωτόκολλο το οποίο μεταφέρει δεδομένα μεταξύ γειτονικών κόμβων του δικτύου σε όλη την περιοχή του δικτύου
DES (Data Encryption Standard)	Ένα μπλοκ κρυπτογράφησης(μια μορφή κοινών μυστικών κρυπτογράφησης). Χρησιμοποιεί 56-bit, γεγονός που θωρείται επισφαλής για πολλές εφαρμογές
DIAS transfer	Διατραπεζικό Ηλεκτρονικό Σύστημα
DMZ (Demilitarized Zone)	Διαχείριση Δεδομένων Ζώνης ή διαχωριστική Ζώνη ή περίμετρος του δικτύου
DNS (Domain Name System)	Συστήματα Ονομάτων Τομέα
E-auction	Οι ηλεκτρονικές δημοπρασίες
E-banking (ή IInternet banking)	Ηλεκτρονική τραπεζική

EBay	Παγκόσμια Online αγορά, που επιτρέπει το εμπόριο σε τοπική, εθνική και διεθνή βάση. Προσφέρει μια ηλεκτρονική πλατφόρμα όπου εκατομμύρια αντικείμενα διακινούνται κάθε ημέρα
Electronic authentication	Ηλεκτρονική αυθεντικότητα
E-commerce	Ηλεκτρονικό εμπόριο
E-marketplaces	Ηλεκτρονικές αγορές
EDI (Electronic Data Interchange)	Ηλεκτρονική Ανταλλαγή Δεδομένων
E-payment	Ηλεκτρονική πληρωμή
E-procurement	Τα συστήματα ηλεκτρονικών προμηθειών
e-mail ή ηλεκτρονικό ταχυδρομείο	Υπηρεσία ανταλλαγής μηνυμάτων με ηλεκτρονικό τρόπο
Ethernet	Το συνηθέστερο χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά την δεκαετία του 1970
FTP (File Transfer Protocol)	Πρωτόκολλο που χρησιμοποιείται για τη διακίνηση δεδομένων ανάμεσα στους χρήστες ενός δικτύου
Hacker	Χρήστης που εισβάλλει παράνομα στους υπολογιστές άλλων χρηστών (ιδιωτών, εταιριών, οργανισμών). Σημειώνεται πάντως ότι οι χρήστες του Internet χρησιμοποιούν αυτό τον όρο σ' έναν πολύ έξυπνο χρήστη. Για τους παρανομούντες χρησιμοποιείται ο όρος cracker
IBM (International Business Machines)	Εταιρεία της οποίας η δραστηριότητα εκτείνεται στους τομείς του Υλικού, του Λογισμικού, των Δικτύων αλλά και των ολοκληρωμένων Υπηρεσιών Πληροφορικής
IDS (Intrusion Detection Systems)	Συστήματα ανίχνευσης διείσδυσης

Internet Protocol	Το πρωτόκολλο επικοινωνίας του Internet
IP	Διεύθυνση. Είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστή που χρησιμοποιεί το Internet Protocol Standard
ITU (International Telecommunication Union)	Διεθνής Ένωση Τηλεπικοινωνιών
MAC (Media Access Control)	Υπόστρωμα της Data Link Layer, γνωστό και ως Medium Access Control
Mailing List	Ομάδα χρηστών που επικοινωνούν μεταξύ τους ανταλλάσοντας ομαδικά ηλεκτρονικά μηνύματα
OpenSSL	Είναι μια συλλογική προσπάθεια για να αναπτυχθεί μια γενικής χρήσης κρυπτογραφίας βιβλιοθήκη
PayPal	Γρήγορες και ασφαλείς ηλεκτρονικές πληρωμές
Phishing	Ψάρεμα
(PKI: Public Key Infrastructure)	Υποδομή Δημόσιου Κλειδιού
PIN (Personal Identification Number)	Προσωπικός αριθμός αναγνώρισης
RSA	Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού. Το όνομα του προέρχεται από τους δημιουργούς του, Ron **R**ivest, Adi **S**hamir και Len **A**dleman
SET (Secure Electronic Transaction)	Ασφαλής ηλεκτρονική συναλλαγή
Server	Υπολογιστής που διαθέτει τα αρχεία του στους υπόλοιπους υπολογιστές
Spam e-mail	Ανεπιθύμητο ταχυδρομείο
Symantec	Εταιρεία με εκθέσεις, η οποία καταγράφει την αύξηση των δικτυακών απειλών που έχουν σχεδιαστεί για να διευκολύνουν το

	ηλεκτρονικό έγκλημα
TELNET	Δίκτυο τηλεπικοινωνιών
TELECOMMUNICATION NETWORK	
UNIX	Λειτουργικό σύστημα Ηλεκτρονικού Υπολογιστή, το οποίο αναπτύχθηκε κατά τη δεκαετία 1960 και 1970
URL (Uniform Recourse Locator)	Ενιαίος Εντοπιστής Πόρων
Verisign	Αμερικάνικη εταιρεία που εδρεύει στην Καλιφόρνια, γνωστή για τη Verisign Ασφαλής Seal. Είναι ο αξιόπιστος φορέας παροχής υπηρεσιών Internet.
VPNs (Virtual private network)	Εικονικό Ιδιωτικό Δίκτυο
Web	Ιστός

ΠΑΡΑΡΤΗΜΑ

Πίνακας 1. ΑΡΙΘΜΟΣ ΠΕΛΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΗΣ

ΑΡΙΘΜΟΣ ΠΕΛΑΤΩΝ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΗΣ

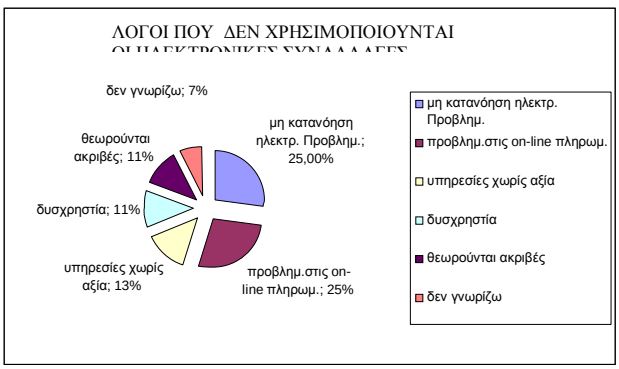
ΧΩΡΑ	2002 (εκατομμύρια)	2005(εκατομμύρια)
Μεγάλη Βρετανία	**9,8**	**14,0**
Γερμανία	**8,5**	**15,4**
Σκανδιναβία	**8,4**	**9,2**

Πίνακας 2. ΛΟΓΟΙ ΜΗ ΧΡΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΣΥΝΑΛΛΑΓΩΝ

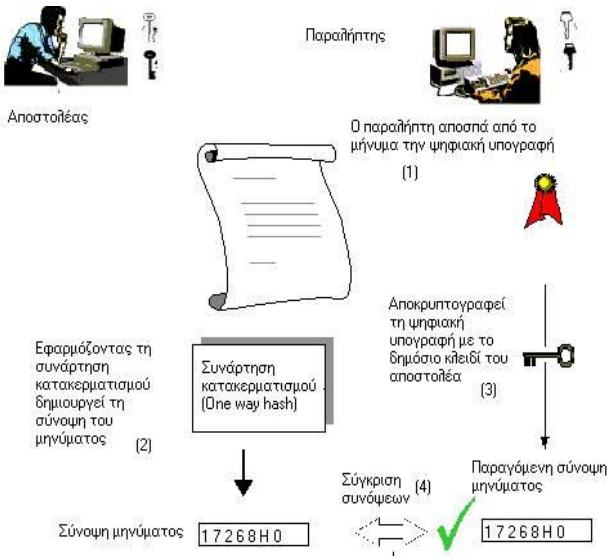
ΛΟΓΟΙ ΜΗ ΧΡΗΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΛΟΓΟΣ	ΠΟΣΟΣΤΟ
Μη κατανόηση των ηλεκτρονικών συστημάτων	25%
Προβλήματα στις on line πληρωμές	25%
Υπηρεσίες χωρίς αξία	13%
Δυσχρηστία	11%
Θεωρούνται ακριβές	11%
Δεν γνωρίζω	7%

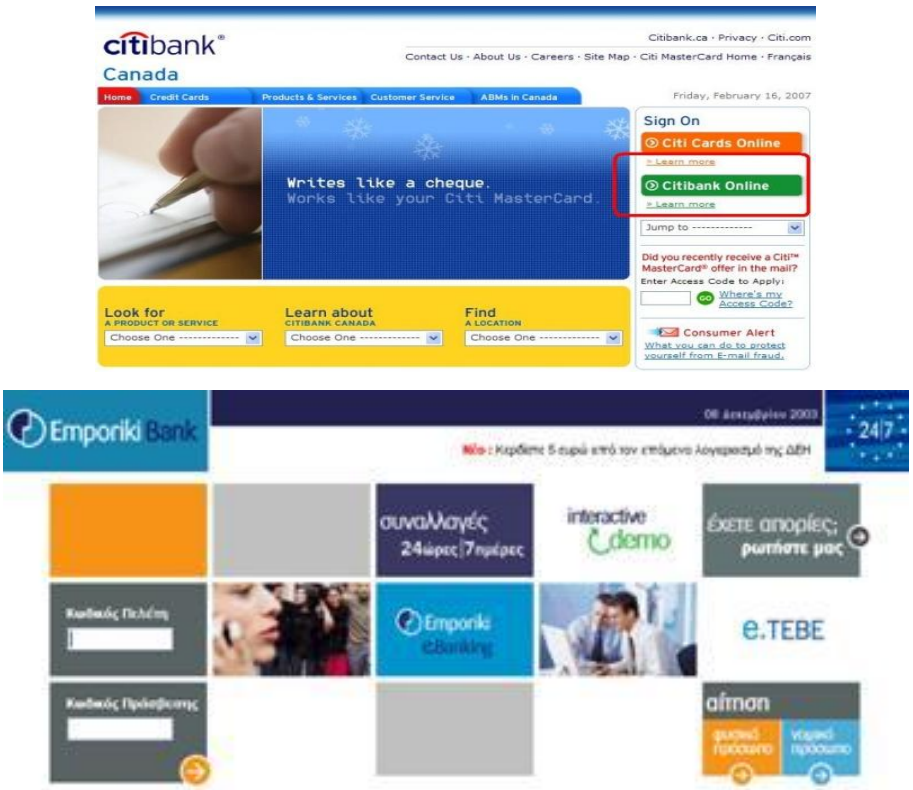
Γράφημα 1. Λόγοι μη χρήσης ηλεκτρονικής τραπεζικής.



Εικόνα 1. Επαλήθευση ψηφιακής υπογραφής



Εικόνες 2,3,4,5. Τράπεζες που προσφέρουν υπηρεσίες e-banking



Πίνακας 3. Πλεονεκτήματα και μειονεκτήματα των μεθόδων κρυπτογράφησης

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΜΕΘΟΔΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Συμμετρική κρυπτογράφηση	Ασύμμετρη κρυπτογράφηση
(-) Η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό.	(+) Παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους.
(+) Η κρυπτογράφηση πραγματοποιείται με ταχύτατους ρυθμούς.	(-) Έλλειψη ταχύτητας.
(+) Δεν υπάρχει ανάγκη για πιστοποίηση των κλειδιών.	(-) Ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς.