ΤΕΙ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΟΥΡΙΣΤΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΜΕΘΟΔΟΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ ΕΡΕΥΝΑ ΑΣΦΑΛΕΙΑ ΣΥΝΑΛΛΑΓΩΝ-ΤΡΑΠΕΖΕΣ

Επιβλέπων Καθηγητής: Ιωάννης Νίκας

Ονοματεπώνυμο Σπουδαστή: Μάλο Κωνσταντίνος

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Στην παρούσα πτυχιακή εργασία παρουσιάζεται το θέμα των μεθόδων οι οποίες χρησιμοποιούνται στις ηλεκτρονικές συναλλαγές. Η εργασία αυτή διαχωρίζεται σε δύο (2) κύρια μέρη. Το πρώτο μέρος αναπτύσσει το βιβλιογραφικό κομμάτι του θέματος, αναλύοντας τις έννοιες των πληροφοριακών συστημάτων, της ηλεκτρονικής τραπεζικής, των μεθόδων που χρησιμοποιούνται στις ηλεκτρονικές συναλλαγές, την ασφάλεια δεδομένων στα πληροφοριακά συστήματα και τα ηλεκτρονικά τουριστικά προϊόντα, μέσω βιβλιογραφικής ανασκόπησης των ήδη υπάρχων επιστημονικών άρθρων και βιβλίων. Το δεύτερο μέρος της συγκεκριμένης πτυχιακής εργασίας, αποτελείται από την έρευνα η οποία διατελέσθηκε σε μεγάλο ξενοδοχείο της Αθήνας και αφορά την ασφάλεια των ηλεκτρονικών συναλλαγών. Στην έρευνα αυτή επιλέχθηκε ως δείγμα το προσωπικό μεγάλης αλυσίδας ξενοδοχείων (Ξενοδοχείο Μεγάλη Βρετάνια) και συγκεκριμένα το ξενοδοχείο του Συντάγματος.

Abstract

In this document presents the methods of electronic transactions. So, the document categorized in the two (2) parts. The first part develops the bibliographic part of the subject by analyzing the concepts of information systems, e-banking, methods used in electronic transactions, data security in computer systems and electronic tourism products, through a bibliographic review of existing scientific articles and books. Also, the second part consists of the research that was carried out in a large hotel in Athens and concerns the security of electronic transactions. This survey was selected as a sample of the staff of a large hotel chain (Grand Hotel Bretagne) and specifically the hotel of the area Syntagma.

ΕΥΧΑΡΙΣΤΙΕΣ

Ολοκληρώνοντας την παρούσα πτυχιακή εργασία, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όσους βοήθησαν τόσο στα πλαίσια της παρούσας πτυχιακής, όσο και κατά τη διάρκεια των σπουδών μου. Θα ήθελα να ευχαριστήσω πρώτα από όλους τον καθηγητή κ. Ιωάννη Νίκα για την βοήθεια και την επίβλεψη της πτυχιακής μου εργασίας καθώς και για την άψογη συνεργασία και καθοδήγηση του σε όλη τη διάρκεια της εκπόνησης αυτής.

Επίσης θα ήθελα, να ευχαριστήσω, ακόμη, τα μέλη της εξεταστικής επιτροπής, καθώς και όλους τους διδάσκοντες του τμήματος για τις γνώσεις που μου παρείχαν σε όλη την διάρκεια της φοίτησής μου στο εκπαιδευτικό αυτό ίδρυμα.

Τέλος, επειδή με την εργασία αυτή ολοκληρώνονται και οι σπουδές μου ως προπτυχιακός φοιτητής, θα ήθελα να ευχαριστήσω τους γονείς μου για την ηθική και οικονομική βοήθεια που μου παρείχαν.

Εισαγωγή

Το internet τα τελευταία χρόνια, λόγω της ταχείας ανάπτυξης της τεχνολογίας, έχει καταλάβει σημαντική θέση στην ζωή των σύγχρονων ανθρώπων, γλυτώνοντας μέσω αυτού αρκετό από τον διαθέσιμο ελεύθερο χρόνο που διαθέτει ο καθένας. Οι τραπεζικές συναλλαγές επί σειρά ετών, αποτελούσαν δύσκολη και χρονοβόρα, πολλές φορές, διαδικασία για τα άτομα κυρίως λόγω των ατελείωτων ουρών αναμονής ειδικά τις μέρες αιχμής στα τραπεζικά ιδρύματα.

Με την ανάπτυξη του internet και την ταυτόχρονη εξέλιξη των τραπεζικών συστημάτων, δημιουργήθηκαν οι ηλεκτρονικές τραπεζικές συναλλαγές οι οποίες απαλλάσσουν τα άτομα από ουρές αναμονής έχοντας έτσι την επιλογή ευελιξίας του ελεύθερου χρόνου τους και την ταχεία εξυπηρέτησή τους μέσα από μία πληθώρα παρεχόμενων υπηρεσιών.

Στην παρούσα πτυχιακή εργασία, πραγματοποιείται μία εμπεριστατωμένη έρευνα σχετικά με τις μεθόδους οι οποίες χρησιμοποιούνται στις ηλεκτρονικές συναλλαγές τόσο μέσω βιβλιογραφικής επισκόπησης όσο και μέσα από έρευνα, με εργαλείο το γνωστό σε όλους ερωτηματολόγιο.

ΚΕΦΑΛΑΙΟ 1: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

1.1 Λίγα λόγια για τα πληροφοριακά συστήματα

Η εποχή που διανύουμε χαρακτηρίζεται από τη ολοένα αυξανόμενη χρήση της πληροφορικής τεχνολογίας. Πιο συγκεκριμένα, τα πληροφοριακά συστήματα, αποτελούν ένα σημαντικό και αναπόσπαστο εργαλείο στον επιχειρηματικό τομέα διότι υποστηρίζουν όλες τις λειτουργικές και παραγωγικές διαδικασίες που λαμβάνουν χώρο σε μια εταιρεία ή έναν οργανισμό.

Αν εξετάσουμε διεξοδικά μια εταιρεία ή ένα οργανισμό ως σύστημα μπορούμε να θεωρήσουμε ότι αποτελείται από τρία διαφορετικά υποσυστήματα (Κάτσικας κ' συν, 2004):

- Το φυσικό σύστημα παραγωγής, που μετασχηματίζει την πρώτη ύλη που εισέρχεται στο σύστημα σε προϊόν και εν συνεχεία σύμφωνα με τις εντολές που παίρνει από το σύστημα διοίκησης.
- Το σύστημα διοίκησης ή λήψης αποφάσεων που παραλαμβάνει πληροφορίες και δεδομένα από το πληροφοριακό σύστημα και παράγει εντολές προς το φυσικό σύστημα παραγωγής και οδηγίες για τις προσδοκίες και επιδιώξεις της διοίκησης, που επιθυμεί να επιτευχθούν.
- Το πληροφοριακό σύστημα που συνδέει το φυσικό σύστημα παραγωγής με το σύστημα διοίκησης και λήψης αποφάσεων. Κατορθώνει και μετασχηματίζει τα δεδομένα που υπάρχουν στο φυσικό σύστημα διοίκησης και συνδέονται με την απόδοση της παραγωγικής διαδικασίας με πληροφορίες που απαιτεί το σύστημα της διοίκησης για να πάρει αποφάσεις. Ακόμα μετασχηματίζει με κατάλληλο τρόπο τις εντολές του συστήματος οδηγίες για το φυσικό σύστημα παραγωγής.

Από όλα τα παραπάνω που προαναφέραμε προκύπτει το συμπέρασμα ότι τα τρία προαναφερθέντα υποσυστήματα αποτελούν στην πραγματικότητα μια ενιαία ενότητα για την εκάστοτε επιχείρηση ή έναν πιο μεγάλο οργανισμό.

Ωστόσο το θέμα που απασχολεί πολλούς είναι το τι εννοούμε με τον όρο πληροφοριακά. Στη βιβλιογραφία δεν υπάρχει ένας σαφής ορισμός των συστημάτων με τον οποίο να μπορούν να συμφωνούν όλοι. Υπάρχει δηλαδή ένα μεγάλο πλήθος ορισμών, από τους οποίους θα αναφέρουμε ορισμένους.

Συγκεκριμένα σύμφωνα με τους Davis και Olson (1985) το πληροφοριακό σύστημα ορίζεται ως μια συλλογή ανθρώπων, επεξεργασιών, δεδομένων, μοντέλων, τεχνολογίας και μερικώς τυποποιημένης γλώσσας που δημιουργεί μια ενιαία δομή που μπορεί εξυπηρετεί ένα οργανωσιακό σκοπό ή μια λειτουργία (Davis & Olson, 1985). Επίσης με βάση τους K. C. Laudon και J.P. Laudon, ένα πληροφοριακό σύστημα μπορεί να ορισθεί ως ένα σύνολο αλληλοσυσχετιζομενων συνιστωσών που συλλέγουν, μπορούν να επεξεργαστούν, να αποθηκεύσουν και να διανείμουν πληροφορίες για θέματα που αφορούν την υποστήριξη της λήψης αποφάσεων, του συντονισμού και του ελέγχου σε ένα οργανισμό (Laudon K. & Laudon J.P, 2009).

Επιπλέον ένας ακόμη ορισμός που έχει δοθεί από τον Κάτσικα (2002), είναι ότι ορίζει το πληροφοριακό σύστημα ως ένα οργανωμένο σύνολο αποτελούμενο από πέντε (5) στοιχεία, το οποίο μπορεί να επεξεργάζεται δεδομένα και να παράγει πληροφορίες για λογαριασμό μιας εταιρείας ή ενός οργανισμού. Μάλιστα οι πέντε συνιστώσες του πληροφοριακού συστήματος που συνδέονται με τους ηλεκτρονικούς υπολογιστές είναι οι άνθρωποι, τα δεδομένα, το λογισμικό, ο υλικός εξοπλισμός και οι διαδικασίες.

1.2 Η ιστορική εξέλιξη των πληροφοριακών συστημάτων

Η ιστορική εξέλιξη των πληροφοριακών συστημάτων έχει τις ρίζες της την δεκαετία του ’50. Πιο συγκεκριμένα οι πρώτες εφαρμογές πληροφοριακών συστημάτων που σχεδιάστηκαν και υλοποιηθήκαν είχαν στόχο να απλοποιήσουν τις επαναλαμβανόμενες διαδικασίες των επιχειρήσεων, όπως είναι για παράδειγμα η μισθοδοσία και η τιμολόγηση προϊόντων. Οπότε η ανάγκη λοιπόν, ήταν κυρίως να απλουστευτούν οι λογιστικές διαδικασίες κατά βάση, και πιο γενικά οι γραφειοκρατικές διαδικασίες που απασχολούσαν τις τότε επιχειρήσεις της δεκαετίας

εκείνης. Στη συνέχεια την δεκαετία του 1960 τα πληροφοριακά συστήματα έγιναν βασικό εργαλείο των ανώτερων στελεχών των επιχειρήσεων ή των οργανισμών. Μάλιστα το πλήθος των εφαρμογών που αναπτύχθηκαν βοήθησαν σε μεγάλο βαθμό τα στελέχη στη συλλογή των στοιχείων, προκειμένου να αξιοποιηθούν στην υποβοήθηση της παραγωγικής διαδικασίας και στον καθορισμό των αναγκών των επιχειρήσεων (Αναστασιάδης, 2000).

Η τεχνολογία εκείνης της εποχής συμβάλει στην περαιτέρω ανάπτυξη και εξέλιξη των δυνατοτήτων των πληροφοριακών συστημάτων, όταν τη δεκαετία του 1980 αποτελούν ένα από τα πιο αποτελεσματικά και χρήσιμα εργαλεία για τα στελέχη μια επιχείρησης. Οι διαδικασίες της παραγωγής και της διαχείρισης είναι άρρηκτα συνδεδεμένες με τη χρήση τους και αποτελούν το πλέον μεγαλύτερο πλεονέκτημα των επιχειρήσεων (Αναστασιάδης, 2000).

Στην δεκαετία του 1990, τα πληροφοριακά συστήματα αποτελούν αναπόσπαστο κομμάτι της εκάστοτε επιχείρησης, διότι αποτελούν μια στρατηγική πλατφόρμα που στοχεύει άμεσα στην λήψη αποφάσεων με μακροχρόνιο ορίζοντα (Αναστασιάδης, 2000).

Στον αιώνα που διανύουμε τα πληροφοριακά συστήματα αποτελούν το κυριότερο εργαλείο των οργανισμών. Αυτό συμβαίνει γιατί παρέχουν πληροφορίες που είναι απαραίτητες που μπορούν να επεξεργαστούν και να διαχειριστούν οι οργανισμοί με αποδοτικό και αποτελεσματικό τρόπο τα δεδομένα που έχουν στη διάθεσή τους, κάνοντας χρήση της τεχνολογία των δικτύων για να μπορούν να παρέχουν εφαρμογές καθώς και για να αποθηκεύουν δεδομένων ανεξαρτήτως τοποθεσίας, διάταξης χώρου, φύσης ή υλικού. Μάλιστα μαζί εξέλιξη της τεχνολογίας των κινητών τηλεφώνων και των ασύρματων δικτύων οδήγησαν σε ένα νέο επίπεδο κινητικότητας όπου οι διαχειριστές έχουν πρόσβαση σχεδόν από παντού με τη βοήθεια των φορητών υπολογιστών.

1.3 **Η ασφάλεια των πληροφοριακών συστημάτων**

Η ασφάλεια που παρέχουν τα πληροφοριακά συστήματα είναι ένα θέμα που απασχολεί μεγάλη μερίδα ανθρώπων με έντονο τρόπο στις μέρες μας. Η διαρκώς ολοένα αυξανόμενη χρήση των τεχνολογιών που βασίζονται σε βάσεις δεδομένων και δίκτυα καθώς και ο σημαντικός ρόλος των πληροφοριακών συστημάτων σε μια επιχείρηση, καθιστούν απαραίτητη τη λήψη μέτρων ασφάλειας για την προστασία των πληροφοριών τους.

Η έννοια της ασφάλειας των πληροφοριακών συστημάτων έχει σχέση με την ικανότητα ενός οργανισμού να μπορεί να προστατεύσει τις πληροφορίες του από πιθανότητα αλλοιώσεων, καταστροφών καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του (Πάγκαλος & Μαυρίδης, 2003)

Οπότε με το προαναφερθέν ορισμό η ασφάλεια σχετίζεται με (Πάγκαλος & Μαυρίδης, 2003):

- Την έννοια της πρόληψης, που περιλαμβάνει μέτρα προκειμένου να προληφθούν πιθανές μελλοντικές φθορές στα μέρη του εκάστοτε πληροφοριακού συστήματος.

- Την έννοια της ανίχνευσης, που περιλαμβάνει την αναζήτηση του πότε, πως και από ποιόν προκλήθηκε φθορά σε ένα στοιχείο του εκάστοτε πληροφοριακού συστήματος.

- Την έννοια της αντίδρασης που περιλαμβάνει την αποκατάσταση ή ανάκτηση δεδομένων του εκάστοτε πληροφοριακού συστήματος.

Ο τομέας της πληροφορικής ξεκίνησε να ασχολείται με ζήλο για την ασφάλεια των πληροφοριακών συστημάτων την δεκαετία του 1970. Συγκεκριμένα, η πρώτη σχετική δημοσίευση προερχόταν από την Ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Αμύνης των ΗΠΑ, που εξέταζε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως. Για να μπορούσε κανείς να έχει πρόσβαση στα διαθέσιμα υπολογιστικά συστήματα, προϋπέθετε την φυσική παρουσία και την πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή.

Η στρατηγική επίλυσης προβλημάτων ασφάλειας μέχρι τότε στηριζόταν στον φυσικό αποκλεισμό, την απομόνωση, την προστασία του κεντρικού υπολογιστή, στον έλεγχο πρόσβασης σε αυτόν. Μάλιστα ένα από τα πιο σημαντικά συμπεράσματα που κατέληξε η Ομάδας Εργασίας ήταν ότι ο εκάστοτε χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικό πρόσβασης, μια πρόταση που ποτέ δεν έγινε ευρέως αποδεκτή και δεν εφαρμόστηκε.

Ωστόσο άλλες ιδέες που πρότεινε η Ομάδα εργασίας στην ανάλυση είχαν μεγαλύτερη απήχηση. Για παράδειγμα, αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει να αποτελεί δομικό λίθο στη δημιουργία πολιτικών ασφάλειας.

Στις αρχές της δεκαετίας του 1970 εμφανίστηκε ο πρώτος ιός, ο Creeper και 2 δεκαετίες αργότερα, το 1998 εμφανίστηκε το πρώτο δικτυακό «σκουλήκι» το αποκαλούμενο σκουλήκι «Morris». Από εκτιμήσεις που προέκυψαν, εκτιμάται ότι περίπου 6.000 συστήματα προσβλήθηκαν από το σκουλήκι Morris. Επίσης, αξίζει να σημειωθεί ότι το 2007 ανακαλύφθηκαν περισσότεροι από 700.000 καινούργιοι ιοί, γεγονός που καθιστά επιτακτική την ανάγκη για προστασία των πληροφοριακών συστημάτων.

Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται στενά με τρεις θεμελιώδεις έννοιες όπως είναι η εμπιστευτικότητα (Confidentiality), η ακεραιότητα (Integrity) και η διαθεσιμότητα (Availability). Πιο ειδικά η έννοια της εμπιστευτικότητας έχει να κάνει με την πρόληψη από την μη εξουσιοδοτημένη ανάγνωση. Πρακτικά αυτό σημαίνει ότι τα δεδομένα που υπάρχουν σε ένα υπολογιστικό σύστημα, καθώς και τα δεδομένα τα οποία διακινούνται θα πρέπει να αποκαλύπτονται και αν είναι ορατά μόνο σε άτομα που είναι εξουσιοδοτημένα. Οπότε από όλα τα παραπάνω, καταλήγουμε στο ότι τα δεδομένα δεν θα πρέπει απλά να προστατεύονται από τη μη εξουσιοδοτημένη ανάγνωση, αλλά και από την πληροφόρηση ότι αυτά τα δεδομένα υπάρχουν. Επίσης, από όλα τα παραπάνω προκύπτει το συμπέρασμα ότι η

εμπιστευτικότητα σχετίζεται και με άλλες έννοιες όπως είναι η ιδιωτικότητα και η μυστικότητα (Πάγκαλος & Μαυρίδης, 2000).

Η έννοια της ακεραιότητας σχετίζεται με την απαίτηση να είναι τα πράγματα όπως πρέπει να είναι, δηλαδή πρόληψη από μη εξουσιοδοτημένη μεταβολή δεδομένων, όπως είναι η διαδικασία της εγγραφής, της διαγραφής ή και την δημιουργία δεδομένων**.** Η έννοια της διαθεσιμότητας έχει να κάνει με την ιδιότητα του πληροφοριακού συστήματος, όπου όλες οι υπηρεσίες του είναι διαθέσιμες και προσπελάσιμες, χωρίς καμία καθυστέρηση και όταν τις χρειάζεται ένας εξουσιοδοτημένος χρήστης. Η διαθεσιμότητα είναι ένας από τους πιο σημαντικούς και απαραίτητους παράγοντες για την καλή και ομαλή λειτουργία ενός συστήματος και είναι καθοριστικός παράγοντας για την αντιμετώπιση του προβλήματος της άρνησης εξυπηρέτησης (denial of service) σε περίπτωση που ένας εξουσιοδοτημένος χρήστης θέλει να προσπελάσει τους πόρους του (Πάγκαλος & Μαυρίδης, 2000).

Εκτός από τις προαναφερθείσες θεμελιώδεις έννοιες υπάρχουν και μερικές ακόμη δευτερευούσης σημασίας αλλα εξίσου σημαντικές έννοιες ασφάλειας πληροφοριακών συστημάτων. Αυτές είναι η εξουσιοδοτημένη χρήση όπου μόνο εξουσιοδοτημένοι χρήστες μπορούν να χρησιμοποιούν το πληροφοριακό σύστημα με προκαθορισμένους τρόπους. Έπειτα είναι η αυθεντικοποίηση των μηνυμάτων όπου διασφαλίζεται η βεβαιότητα ότι το άτομο που φέρεται να έχει στείλει το μήνυμα, σύμφωνα με το σύστημα, το έχει όντως στείλει. Ακόμα υπάρχει και η έννοια της μη απάρνησης όπου εξασφαλίζεται ότι το μήνυμα αποστολής έχει παραδοθεί στον αποστολέα του. Η έννοια της απόδοσης ευθυνών είναι και αυτή σημαντική γιατί ορίζει ότι οι χρήστες θα πρέπει να είναι υπεύθυνοι για τις πράξεις τους. Επιπλέον οι έννοιες της αξιοπιστίας και της σιγουριάς είναι απαραίτητες γιατί θέτουν σαν προϋπόθεση ότι τα πληροφοριακά συστήματα θα πρέπει να συνεχίζουν να λειτουργούν κανονικά ακόμα και σε αντίξοες συνθήκες (Πάγκαλος & Μαυρίδης, 2000).

Ωστόσο κάθε πληροφοριακό σύστημα είναι ευάλωτο σε πολλών ειδών κινδύνους. Συχνά τα πληροφοριακά συστήματα παρουσιάζουν τρωτά σημεία ή κενά στο σύστημα ασφαλείας που ονομάζονται ευπάθειες. Οι ευπάθειες μπορούν να χωριστούν στις παρακάτω κατηγορίες: τις φυσικές ευπάθειες (Physical), εκ φύσεως (Natural),

υλικού και λογισμικού (Hardware and Software), ευπάθειες μέσων (Media), ευπάθειες εκπομπών (Emanation), ευπάθειες επικοινωνιών (Communications), καθώς και ανθρώπινες (Human) (Πάγκαλος & Μαυρίδης, 2000).

Συνήθως απειλή για ένα πληροφοριακό σύστημα μπορεί να αποτελέσει οποιαδήποτε κατάσταση μπορεί να προκαλέσει ζημιά ή απώλεια, όπως είναι για παράδειγμα η εκούσια ανθρώπινη επίθεση ή η ακούσια (ανθρώπινο λάθος), φυσικές καταστροφές ή ακόμα και εσωτερικό πρόβλημα που αντιμετωπίζει ο εξοπλισμός τους συστήματος ή του λογισμικού. Τα πιο γνωστά είδη απειλών για τους πόρους του πληροφοριακού συστήματος που έχουν να κάνουν με το υλικό και το λογισμικό είναι η υποκλοπή δεδομένων (data interception), μεταβολή (modification), η πλαστογραφία (fabrication) και η διακοπή (interruption). Για να μπορέσουν να περιοριστούν και να αντιμετωπιστούν οι αδυναμίες σε ένα πληροφοριακό σύστημα θα πρέπει να προβλεφθούν και να εφαρμοστούν κατάλληλα μέτρα προστασίας. Πιο ειδικά, τα μέτρα προστασίας είναι το σύνολο των διαδικασιών, των τεχνικών, των ενεργειών και των συσκευών που μπορούν να καλύψουν τις αδυναμίες που έχει το εκάστοτε πληροφοριακό σύστημα. Τα διαφορετικά είδη μέτρων προστασίας έχουν σαν αποτέλεσμα την ανάλυση του προβλήματος ασφαλείας των πληροφοριακών συστημάτων στις λεγόμενες συνιστώσες όπως είναι η φυσική ασφάλεια συστήματος (physical security), η ασφάλεια υπολογιστικού συστήματος (computer security), η ασφάλεια βάσεων δεδομένων (database security) και η ασφάλεια δικτύων επικοινωνιών (network security) (Πάγκαλος & Μαυρίδης, 2000).

Τέλος, υπάρχουν και άλλοι τύποι μέτρων προστασίας για την αντιμετώπιση των ευπαθειών που υπάρχει σε ένα πληροφοριακό σύστημα. Τα πιο ενδεικτικά μέτρα προστασίας είναι, η τα μέτρα λογισμικού (software controls), τα μέτρα υλικού (hardware controls), η κρυπτογραφία (encryption), τα φυσικά μέτρα υλικού (physical controls) και οι πολιτικές ασφαλείας (security policies) (Πάγκαλος & Μαυρίδης, 2000).

1.4 Τα τραπεζικά πληροφοριακά συστήματα

Είναι γενικά παραδεκτό ότι η ανάπτυξη των πληροφοριακών συστημάτων, δεν θα μπορούσε σε καμιά περίπτωση να μην έχει επηρεάσει τον χρηματοπιστωτικό κλάδο. Μάλιστα στην σημερινή εποχή το συνολικό πλήθος των διαδικασιών που πραγματοποιεί μια τράπεζα, γίνεται με την χρήση των τεχνολογιών της πληροφορικής. Επίσης, οι μεγάλες ουρές που σχηματίζονται στα γκισέ της τράπεζας ολοένα και μειώνονται διότι οι τράπεζες λειτουργούν σε Online σύνδεση το μεγαλύτερο μέρος των παρεχόμενων υπηρεσιών.

Σε αυτό το σημείο είναι απαραίτητο να κατανοήσει κανείς την πολυπλοκότητα των τραπεζικών πληροφοριακών συστημάτων μέσα από την παράθεση των πιο χαρακτηριστικών εφαρμογών που υποστηρίζει ένας τραπεζικός οργανισμός (Κάτσικας κ' συν, 2004).

Αυτές οι εφαρμογές online τραπεζικού δικτύου είναι (Κάτσικας κ' συν, 2004):

- ✓ ATM
- ✓ Οι καταθέσεις
- ✓ οι χορηγήσεις
- ✓ Η κίνηση κεφαλαίων
- ✓ Η αγοραπωλησία Συναλλάγματος
- ✓ Οι τίτλοι Δημοσίου
- ✓ Οι εισαγωγές
- ✓ Οι εξαγωγές
- ✓ Οι κάρτες

Επίσης, οι τράπεζες χρησιμοποιούν Διεθνή Δίκτυα Τραπεζικών Εφαρμογών. Το πιο γνωστό και ευρέως χρησιμοποιούμενο δίκτυο είναι το SWIFT (Society for Worldwide Interbank Telecommunication), το οποίο χρησιμοποιείται από την πλειονότητα των

ελληνικών τραπεζών παρόλο που παρουσιάζει υψηλό κόστος συντήρησης και απαιτεί εξειδικευμένη γνώση για την υποστήριξή του. Μάλιστα, το συγκεκριμένο δίκτυο SWIFT εμπεριέχει πολύ υψηλές προδιαγραφές ασφάλειας, μέσω της οποίας εξασφαλίζεται απόλυτα η ορθότητα και η εμπιστευτικότητα των μηνυμάτων. Επίσης, υπάρχουν διεθνή δίκτυα που έχουν την δυνατότητα παροχής οικονομικών πληροφοριών στους πολίτες και έχουν αναπτυχθεί από τεράστιες τράπεζες του εξωτερικού, όπως είναι για παράδειγμα, το διεθνές πρακτορείο REUTERS.

Ακόμα, οι ελληνικές τράπεζες έχουν σχεδιάσει και αναπτύξει, συστήματα επικοινωνίας σε εθνικό επίπεδο. Πιο ειδικά, η πλειονότητα των ελληνικών τραπεζών χρησιμοποιούν μισθωμένες γραμμές ή και διεπιλεγμένες και συνάμα αναπτύσσουν εφαρμογές για την αποστολή ή τη λήψη στοιχείων από και προς διαφορετικούς οργανισμούς. Είναι δε κατανοητό, ότι οι συγκεκριμένες εφαρμογές θα πρέπει να δημιουργούνται με βάση ένα ασφαλή σχεδιασμό δικτύου.

Επιπρόσθετα η πλειονότητα των τραπεζικών εφαρμογών λειτουργούν εξυπηρετώντας τους πολίτες και όταν είναι κλειστοί οι τραπεζικοί οργανισμοί. Για να μπορούν να λειτουργήσουν σωστά, οι εφαρμογές αυτές θα πρέπει να έχουν την ανάγκη για κάποια batch επεξεργασία που περιλαμβάνει ενημέρωση λογαριασμών, την έκδοση τόκων και τις εκτυπώσεις. Ωστόσο, υπάρχουν και άλλου είδους εφαρμογές που λόγω της μικρής συχνότητας παραγωγής τους είναι σχεδιασμένες να λειτουργούν σε μορφή Batch και συνήθως με παράλληλο τρόπο με τα online συστήματα ή τον εφεδρικό ηλεκτρονικό υπολογιστή της Τράπεζας, προκειμένου να μην επηρεάζουν την απόκριση και την ομαλή λειτουργία του δικτύου.

Τέτοιες εφαρμογές είναι προγράμματα που αφορούν μισθοδοσίες εργαζομένων, συντάξεις, πληρωμή λογαριασμών και άλλα. Στην πραγματικότητα, οι batch εφαρμογές περιλαμβάνουν τα οικονομικά στοιχεία ιδιωτών ή υπαλλήλων και απαιτούν ιδιαίτερη μεταχείριση από την πλευρά της ασφάλειας. Οπότε εκτός από τις μεθόδους που έχουν σαν αντικείμενο την διατήρηση της ακεραιότητας των προγραμμάτων που χρησιμοποιούνται είναι απαραίτητο να πραγματοποιηθούν ιδιαίτερες διαδικασίες ελέγχου κατά την διάρκεια προετοιμασίας των ενημερωτικών καταστάσεων και των μεταβολών των προγραμμάτων.

Τέλος, οι εφαρμογές σε PC ή αλλιώς τα αυτόνομα συστήματα πολλαπλών χρηστών περιλαμβάνουν κυρίως διοικητικής φύσης εργασίες που αφορούν διαδικασίες όπως είναι τα πρωτόκολλα, οι άδειες, και αντιμετωπίζονται με μικρά πληροφοριακά συστήματα που αναπτύσσονται και από το εκάστοτε προσωπικό της Τράπεζας ή μικρά πακέτα της αγοράς. Μάλιστα τα πιο διαδεδομένα πακέτα είναι εκείνα των λογιστικών φύλλων. Επιπλέον γίνεται μεγάλη χρήση σε εκδοτικά πακέτα που αφορούν προετοιμασία εγγράφων, ανακοινώσεων ή πακέτα ειδικού σκοπού που χρησιμοποιούνται για το σχεδιασμό παρουσιάσεων. Ακόμα, μεγάλος αριθμός τραπεζών αξιοποιούν μικροϋπολογιστές σε δίκτυα προκειμένου να μπορέσουν να εγκαταστήσουν εφαρμογές ειδικού σκοπού όπως είναι οι εφαρμογές οπτικής ανάγνωσης και οι εφαρμογές επεξεργασίας επιταγών. Επιπρόσθετα, γίνεται ευρέως χρήση των πακέτων CAD/ CAM, στατιστικών εφαρμογών και εφαρμογών γραμματειακής υποστήριξης (Κάτσικας κ' συν, 2004).

1.5**Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων**

Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων είναι η ικανότητα του εκάστοτε Τραπεζικού Ιδρύματος να μπορεί να παρέχει αξιόπιστες πληροφορίες που θα είναι διαθέσιμες για κάθε στιγμή αναζήτησης. Οπότε είναι λογικό ότι για αυτό το σκοπό θα πρέπει να ληφθούν μέτρα που να μπορούν να εξασφαλίζουν την ακεραιότητα των δεδομένων, καθώς και τη συνεχή και ομαλή λειτουργία του κέντρου πληροφορικής (Κάτσικας κ' συν, 2004)

Η ασφάλεια είναι αναγκαία και απαραίτητη συνθήκη ώστε σε συνδυασμό με άλλες βασικές προϋποθέσεις λειτουργίας ενός οργανισμού να μπορεί να εξασφαλιστεί η ομαλή λειτουργία του. Μάλιστα η έννοια της ασφάλειας είναι μια δυναμική παράμετρος και όχι στατική. Οπότε, η εκάστοτε πολιτική ασφαλείας θα πρέπει να επανεξετάζεται και να ελέγχεται συνεχώς προκειμένου να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων μπορεί να διακριθεί σε δύο κατηγορίες όπως είναι η ασφάλεια σε περίπτωση έκτακτης ανάγκης και η ασφάλεια

στις καθημερινές διεργασίες. Πιο ειδικά τα πιο συνηθισμένα προβλήματα που μπορούν να συμβούν σε περιπτώσεις έκτακτης ανάγκης είναι για παράδειγμα η διακοπή ηλεκτρικής ενέργειας, οι προσωρινές βλάβες λόγω πυρκαγιάς ή λόγω πλημμυρών, η διακοπή λειτουργίας μέρους του εξοπλισμού του υπολογιστή. Για την αντιμετώπιση των παραπάνω δυσκολιών γίνεται μετάπτωση στο εφεδρικό σύστημα (disaster recovery facility, D.R.F.) που υπάρχει στις περισσότερες Τράπεζες. Σε περίπτωση που ούτε και αυτό είναι εφικτό, τότε σταματά η λειτουργία, μέχρι να αποκατασταθεί η βλάβη και επανέρθει η πλήρης λειτουργία του συστήματος. Οπότε είναι αναγκαίο σε ότι τα σχέδια έκτακτης ανάγκης θα πρέπει να ελέγχεται αλλά και να διορθώνεται όπου τυχόν υπάρχουν κενά σε συγκεκριμένα χρονικά διαστήματα (Κάτσικας κ' συν, 2004).

Ωστόσο από την άλλη μεριά, η ασφάλεια των καθημερινών λειτουργιών των πληροφοριακών συστημάτων, θα πρέπει να καλύπτει τα κτήρια, τις εγκαταστάσεις, το μηχανογραφικό εξοπλισμό και το λογισμικό. Επίσης, θα πρέπει η ασφάλεια να μεριμνά για το ποιοι και για το πως αναπτύσσουν, χειρίζονται τα διάφορα πληροφοριακά συστήματα, για το ποιοι έχουν πρόσβαση σε συγκεκριμένους χώρους όπου διακινούνται εμπιστευτικές πληροφορίες, το είδος των δεδομένων που φυλάσσονται κ.α (Κάτσικας κ' συν, 2004).
Η δε ασφάλεια των καθημερινών τραπεζικών εργασιών θα μπορούσε να διακριθεί σε τέσσερις κατηγορίες (Κάτσικας κ' συν, 2004):

- Τη φυσική ασφάλεια των πληροφοριακών συστημάτων
- Τη λογική ασφάλεια των πληροφοριακών συστημάτων
- Την ασφάλεια δικτύων και του εξοπλισμού συναλλαγών
- Την ασφάλεια περιφερειακού και βοηθητικού εξοπλισμού

Τα μέτρα προστασίας που λαμβάνονται έχουν σαν σκοπό στην φυσική ασφάλεια των πληροφοριακών συστημάτων και πιο ειδικά, την προστασία των χώρων πληροφορικής. Ακόμα, είναι απαραίτητη σε πολλές περιπτώσεις η προστασία του υλικού καθώς και η προστασία των αντιγράφων (back-up). Επίσης, στους χώρους πληροφορικής είναι απαραίτητη η εγκατάσταση ενός συστήματος αδιάλειπτου

λειτουργίας (U.P.S) και ενός συστήματος πυρόσβεσης. Οπότε, με τα προαναφερθέντα μέτρα, μπορούν να αποφευχθούν τυχόν καταστροφές ή βλάβες του εξοπλισμού ή μόνιμη απώλεια δεδομένων.
Η Λογική Ασφάλεια σχετίζεται με την προφύλαξη του λογισμικού και των δεδομένων, προκειμένου να μπορούν να αποφευχθούν τυχόν αλλοιώσεις στις παραμέτρους του συστήματος, όπως είναι η απώλεια δίσκων, η ενεργοποίηση κακόβουλων λογισμικών κ.α.

Η Ασφάλεια Δικτύου και εξοπλισμού συναλλαγών, έχει σχέση με την εξέταση του δικτύου των online συναλλαγών της Τράπεζας. Συνήθως τα μηνύματα που μεταφέρονται στις τραπεζικές συναλλαγές είναι άκρως σημαντικά, πράγμα που σημαίνει ότι είναι απαραίτητη η προστασία των μηνυμάτων που μπορεί να επιτευχθεί μέσω διαφόρων μεθόδων όπως είναι η κρυπτογραφία. Οπότε τα μέτρα που πρέπει να εφαρμοστούν ώστε να επιτευχθεί η ασφάλεια στο On-Line δίκτυο συναλλαγών είναι η μέθοδος της κρυπτογραφίας κατά την διακίνηση των δεδομένων, η χρήση εναλλακτικών τηλεφωνικών γραμμών , οι διαδικασίες restart/recovery καθώς και μέτρα συντήρησης που αφορούν την φυσική προστασία της εγκατάστασης. Αν τα μέτρα αυτά δεν τηρηθούν τότε μπορεί να προκληθεί φαινόμενα υποκλοπής και τροποποίησης μηνυμάτων λόγω παγίδευσης γραμμών, λανθασμένη δρομολόγηση εξόδων και διασταυρούμενη επικοινωνία.

Τέλος η ασφάλεια, περιφερειακού και μηχανολογικού εξοπλισμού περιλαμβάνει την εξέταση των παραμέτρων ασφαλείας που ισχύουν για τον λοιπό «μηχανογραφικό» εξοπλισμό και έχει την δυνατότητα να υποστηρίζει τις υπηρεσίες της Τράπεζας που είναι που συνδεδεμένες με κάποιας μορφής δίκτυο είτε λειτουργούν ως αυτόνομοι μικροϋπολογιστές. Τέτοια μέτρα είναι, η συστηματική λήψη ασφαλείας, η εγκατάσταση και χρησιμοποίηση προγραμμάτων ανίχνευσης ιών (antivirus), η εκπαίδευση των χρηστών σε τεχνικές προστασίας, η φύλαξη των εμπιστευτικών αρχείων σε δισκέτες ή CD-ROM σε ασφαλή χώρο και η φυσική προστασία του χώρου του προσωπικού υπολογιστή, των περιφερειακών και βοηθητικών συσκευών. Μάλιστα οι κίνδυνοι που μπορεί να προκύψουν από την μη υλοποίηση των ανωτέρω μέτρων είναι η μορφοποίηση δίσκου (formatting), το σβήσιμο αρχείων, με τα τοπικά

δίκτυα (LAN) να διατρέχουν άμεσο κίνδυνο. Η παντελής έλλειψη δημιουργίας εφεδρικών αντιγράφων (back-up) ή αποθήκευσης, η αδυναμία ενημέρωσης των κωδικών μπορούν να δημιουργήσουν τεράστιο πρόβλημα.

ΚΕΦΑΛΑΙΟ 2: Η ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ

2.1 Η ιστορική εξέλιξη της ηλεκτρονικής τραπεζικής

Η πρώτη μορφή ηλεκτρονικής τραπεζικής που εμφανίστηκαν τη δεκαετία του ‘60 είναι τα Αυτόματα Ταμειολογιστικά Μηχανήματα ή αλλιώς ATM. Το πρώτο μηχάνημα ATM τοποθετήθηκε στην Αμερική από την City Bank of New York το 1961 αλλά εν συνεχεία αποσύρθηκε μετά από 6 μήνες, λόγω έλλειψης εμπιστοσύνης από τους πελάτες της τράπεζας. Έπειτα από πολλές βελτιώσεις που πραγματοποιήθηκαν, το πρώτο σύγχρονο ATM, εγκαταστάθηκε στο Essex της Αγγλίας, από την Τράπεζα «Lloyd Bank» το 1972 (Davis & Olson, 1985).

Η εμφάνιση της ηλεκτρονικής τραπεζικής, με τη σημερινή μορφή της μετράει κιόλας περίπου 23 χρόνια. Πιο ειδικά η πρώτη ηλεκτρονική τράπεζα, η Security First Network Bank (SFNB), ιδρύθηκε στο Κεντάκυ των ΗΠΑ τον Οκτώβριο του 1995. Οπότε η συγκεκριμένη τράπεζα χωρίς να διαθέτει δίκτυο καταστημάτων είχε την δυνατότητα να εξυπηρετεί του πελάτες της μόνο μέσα από το διαδίκτυο (Internet). Ο σχεδιασμός και η ανάπτυξη αυτού του τραπεζικού οργανισμού πραγματοποιήθηκε από ένα μικρό οργανισμό την χρηματοοικονομική εταιρεία Cardinal Bancshares, η οποία μετέπειτα χρηματοδοτήθηκε με περίπου 2,5 εκατομμύρια δολάρια από δύο άλλες αμερικανικές τράπεζες την Huntington Bancshares και την Wachovia Corporation (Τσάμης, 2003).

Η αιτία που οι δύο (2) προαναφερθέντες τράπεζες επένδυσαν τόσα χρήματα είναι ότι ήταν οι πρώτες που διέκριναν ότι η πλειονότητα των τραπεζών είχαν την ανάγκη να πραγματοποιούν συναλλαγές τους με απλό τρόπο, σε όλη την διάρκεια της ημέρας, όλο το χρόνο και από οποιοδήποτε σημείο της γης και αν ευρίσκονταν. Επίσης αναγνώρισαν το μεγάλο πλεονέκτημα που παρουσίαζε η τράπεζα Cardinal Bancshares στο ότι είχε σχεδιάσει την πιο προηγμένη αρχιτεκτονική ασφαλείας πληροφοριακών

συστημάτων εκείνης της εποχής, αρχιτεκτονική που αποτέλεσε προϋπόθεση για την αποδοχή της ηλεκτρονικής τραπεζικής από τους πελάτες (Τσάμης, 2003).

Λίγα χρόνια μετά (αρχές του 2000) σημειώθηκε μεγάλη αύξηση στην ίδρυση και λειτουργία διαδικτυακών τραπεζών. Οπότε οι παραδοσιακές τράπεζες, που προωθούσαν υπηρεσίες και εξυπηρετούσαν όλες τις συναλλαγές των πελατών τους μέσα από τα καταστήματά, ένιωσαν μια απειλή διότι διαπίστωναν ότι ένα μεγάλο ποσοστό των πελατών άρχιζε να χρησιμοποιεί τις νέες αυτές τράπεζες. Οπότε οι τράπεζες αυτές αναγκάστηκαν να ακολουθήσουν την τάση της ηλεκτρονικής τραπεζικής, και αρκετές φορές, αναγκάστηκαν να αναθεωρήσουν τα πληροφοριακά συστήματα και ορισμένων επιχειρησιακών λειτουργιών τους, προκειμένου να ανταποκρίνονται στα αιτήματα των πελατών που τους διαβιβάζονταν ηλεκτρονικά (Τσάμης, 2003).

Όπως είναι λογικό οι παραδοσιακές τράπεζες άρχισαν να περιλαμβάνουν τον τρόπο λειτουργίας των ηλεκτρονικών τραπεζών, δίνοντας περισσότερη έμφαση στην συνεργασία ανάμεσα στα δίκτυα του φυσικού και του ηλεκτρονικού κόσμου, διότι έγινε κατανοητό ότι η μία μορφή συμπληρώνει την άλλη και αντίστροφα. Οπότε τα ηλεκτρονικά δίκτυα είναι σε θέση να εξυπηρετούν τραπεζικές και χρηματοοικονομικές εργασίες, να πληροφορούν, να ειδοποιούν έγκαιρα τον πελάτη και να τον διευκολύνου στις χρηματοοικονομική διαχείριση. Επίσης τα δίκτυα αυτών των τραπεζών μπορούν να εξυπηρετούν τους πελάτες σε θέματα που έχουν να κάνουν με την επεξήγηση νέων προϊόντων ή υπηρεσιών (Τσάμης, 2003).

Στην Ελλάδα η πρώτη τράπεζα που εισήγαγε την ηλεκτρονική τραπεζική ήταν η Εγνατία Τράπεζα το 1997 και περιελάμβανε κατά βάση πληροφορίες συναλλαγών και μεταφοράς κεφαλαίων. Η πρώτη πλήρης και ολοκληρωμένη πλατφόρμα ηλεκτρονικών υπηρεσιών, πραγματοποιήθηκε από τη Τράπεζα Πειραιώς το 2000, με το brand name «WINBANK» (Αγγέλης, 2005).

Στην σημερινή εποχή, όλα σχεδόν τα χρηματοπιστωτικά ιδρύματα της χώρας διαθέτουν υπηρεσίες ηλεκτρονικής τραπεζικής και παρέχουν ένα μεγάλο εύρος τραπεζικών υπηρεσιών, όπως είναι η μεταφορά χρημάτων, η πληρωμή λογαριασμών, η κατάθεση αιτήσεων για κάρτα. Οπότε από όλα τα παραπάνω, μπορούμε να

συμπεράνουμε ότι η ηλεκτρονική τραπεζική αποτελεί στόχο για βελτιστοποίηση των επιχειρησιακών λειτουργιών στις παραδοσιακές τράπεζες, που αναγκαστικά πλέον, ακολουθούν τα πρότυπα της ηλεκτρονικής τραπεζικής (Αγγέλης, 2005).

2.2 Ορισμός της ηλεκτρονικής τραπεζικής

Με την έννοια e-banking η αλλιώς ηλεκτρονική τραπεζική, εννοούμε το σύνολο όλων των υπηρεσιών που παρέχουν οι τράπεζες μέσο του διαδικτύου χωρίς δηλαδή τη φυσική παρουσία του εκάστοτε πελάτη σε κάποιο υποκατάστημα της τράπεζας. Επιπλέον, ένας άλλος τρόπος με τον οποίον θα μπορούσαμε να ορίσουμε το e -banking είναι ως η αυτοματοποιημένη παροχή νέων και παραδοσιακών προϊόντων και υπηρεσιών χρηματοοικονομικής φύσης απευθείας στους πελάτες μέσω ηλεκτρονικών καναλιών επικοινωνίας. Μάλιστα ανάλογα με το κανάλι χρήσης για την πραγματοποίηση των συναλλαγών μπορούμε να χωρίσουμε το e - banking σε τρία (3) είδη.

2.2.1 Είδη ηλεκτρονικής τραπεζικής

Η ηλεκτρονική τραπεζική, κατά βάση χωρίζεται σε τρία είδη, με βάση τον εξοπλισμό και τα προγράμματα λογισμικού που χρησιμοποιούνται. Πιο συγκεκριμένα τα είδη αυτά είναι (Αγγέλης, 2005):

- ✓ Internet banking (Τραπεζική μέσω διαδικτύου), όπου η πρόσβαση στις συναλλαγές γίνεται μέσω διαδικτύου.
- ✓ Phone banking (Τραπεζική μέσω τηλεφώνου) όπου οι συναλλαγές πραγματοποιούνται μέσω τηλεφώνου.
- ✓ Mobile banking (Τραπεζική μέσω κινητού) όπου οι συναλλαγές γίνονται μέσω κινητού.

2.2.1.1 Internet banking

Το Internet banking που ονομάζεται και online Banking, χρησιμοποιεί το διαδίκτυο ως τρόπο διεξαγωγής τραπεζικών δραστηριοτήτων. Πιο ειδικά, για να μπορέσει ο εκάστοτε χρήστης να χρησιμοποιεί τις υπηρεσίες της ηλεκτρονικής τραπεζικής θα πρέπει να διαθέτει ηλεκτρονικό υπολογιστή και να έχει πρόσβαση στο διαδίκτυο. Εντούτοις, σε ορισμένες περιπτώσεις είναι απαραίτητη η ύπαρξη συσκευών ασφαλείας, όπως είναι για παράδειγμα η εγκατάσταση ειδικού λογισμικού ασφαλείας ή ψηφιακό πιστοποιητικό. Ο πελάτης μίας τράπεζας, μέσω του Internet banking, έχει τη δυνατότητα να εκτελεί μεγάλο πλήθος τραπεζικών συναλλαγών και να λαμβάνει την πληροφόρηση που επιθυμεί.

Η πλειονότητα των τραπεζικών ιδρυμάτων έχουν πλέον την τεχνογνωσία και τις δυνατότητες να προσωποποιούν τις ηλεκτρονικές τους υπηρεσίες, με βάση κάθε φορά την κατηγορία πελατών που αντιπροσωπεύει ο χρήστης και οπότε με αυτό το τρόπο υπάρχουν για παράδειγμα επιπρόσθετες δυνατότητες για εταιρικούς χρήστες σε σχέση με ιδιώτες. Επίσης, γίνονται επενδύσεις και μελέτες και σε θέματα ασφάλειας που είναι ιδιαίτερα κρίσιμο για την αξιοπιστία και την ομαλή λειτουργία των ηλεκτρονικών τραπεζικών συστημάτων (Αγγέλης, 2005).

2.2.1.2 Phone banking

Ο κάθε τραπεζικός οργανισμός μέσω Phone Banking, γίνεται προσιτός από οπουδήποτε και να είναι ο πελάτης, ενώ την ίδια στιγμή διατηρείται ως ένα βαθμό και η παραδοσιακή τραπεζική σχέση μεταξύ υπαλλήλου και πελάτη. Μάλιστα συσκευές όπως είναι τα κινητά τηλέφωνα ή τα PDAs που είναι περιέχουν την τεχνολογία WAP μπορούν να συνδεθούν στο Internet και να παρέχουν στους χρήστες τους τη δυνατότητα τραπεζικών συναλλαγών.

Οι δε υπηρεσίες που προσφέρονται μέσω phone banking μπορούν να χωριστούν σε δυο κατηγορίες. Η πρώτη κατηγορία είναι αυτή που διεκπεραιώνονται από υπαλλήλους μέσω τηλεφωνικού κέντρου και στην δεύτερη κατηγορία είναι αυτές που

διεκπεραιώνονται μέσω συστημάτων αναγνώρισης φωνής. Στην πρώτη περίπτωση, ο εκάστοτε πελάτης επικοινωνεί φωνητικά με τον υπάλληλο της τράπεζας και εκφέρει τα αιτήματα του ή τα παραπόνα του. Οι υπάλληλοι αυτοί πρέπει να ταυτοποιήσουν τα στοιχεία του πελάτη, προκειμένου να εξασφαλίσουν την ακεραιότητα, αλλά και την εμπιστευτικότητα των συναλλαγών και αιτημάτων του. Στη δεύτερη περίπτωση, η διαδικασία είναι αυτοματοποιημένη και ο χρήστης απαντά στα φωνητικά μηνύματα που ακούει στο τηλέφωνο του. Στην δεύτερη περίπτωση ακολουθούνται όπως και στην πρώτη διαδικασίες πιστοποίησης και ταυτοποίησης του πελάτη προκειμένου να εξασφαλιστεί ασφάλεια των συναλλαγών του. Τελικά η υπηρεσία του phone banking, δίνει τη δυνατότητα στον εκάστοτε πελάτη ενός τραπεζικού οργανισμού, να έχει στη διάθεση του και να μπορεί να έχει πρόσβαση σε όλες σχεδόν τις συναλλαγές είτε οικονομικές είτε πληροφοριακές που έχει και μέσω της υπηρεσίας του Internet banking (Αγγέλης, 2005)

2.2.1.3 Mobile banking

Η υπηρεσία του Mobile banking παρά τα μεγάλα πλεονεκτήματα που παρουσιάζει όπως είναι, η ευκολία στις συναλλαγές και η γενικότερη ευχρηστία δεν έχει καταφέρει ακόμη να πείσει το ελληνικό καταναλωτικό κοινό και οπότε μοιραία δεν έχει εδραιωθεί ακόμα σε σχέση με τις άλλες υπηρεσίες όπως είναι το internet banking και το phone banking. Μάλιστα, αν αναλογιστούμε ότι η ανάπτυξη της κινητής τηλεφωνίας στη Ελλάδα έχει αναπτυχθεί αρκετά, τότε είναι σίγουρο ότι το Mobile banking έχει την δυνατότητα να αποτελέσει ένα ευρέως χρησιμοποιούμενο κανάλι διεκπεραίωσης ηλεκτρονικών συναλλαγών. Επίσης δίνεται μεγάλη έμφαση σημασία δίνεται επίσης σε ότι αφορά το Mobile banking, στην ασφάλεια των συναλλαγών και στην πιστοποίηση του χρήστη. Επίσης, ο εκάστοτε πελάτης έχει την δυνατότητα με την υπηρεσία του Mobile banking να μπορεί να παρακολουθεί τις κινήσεις των λογαριασμών του, να διακινεί χρήματα, να πληρώνει λογαριασμούς και να μπορεί να ζητήσει τραπεζικά προϊόντα και υπηρεσίες (Σινανιώτη – Μαρουδή & Φαρσαρώτας, 2005).

2.3 **Οι υπηρεσίες της ηλεκτρονικής τραπεζικής**

Οι υπηρεσίες που παρέχει η ηλεκτρονική τραπεζική μελετώνται ξεχωριστά για κάθε μία από τις προαναφερθείσες κατηγορίες. Συγκεκριμένα, το internet banking αποτελεί τον βασικό πυλώνα της ηλεκτρονικής τραπεζικής σε ότι έχει να κάνει με το πλήθος των υπηρεσιών που προσφέρει. Οι παρεχόμενες υπηρεσίες μπορούν να διακριθούν στις ακόλουθες κατηγορίες: α) τις οικονομικές συναλλαγές, β) τις πληροφοριακές συναλλαγές, γ) τις αιτήσεις, δ) άλλα είδη υπηρεσιών (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

Α) Οι οικονομικές συναλλαγές

Οι οικονομικές συναλλαγές καλύπτουν όλο το εύρος των συναλλαγών που μπορεί να κάνει ο εκάστοτε πελάτης και στο κατάστημα της τράπεζας. Επίσης οι συναλλαγές αυτές αφορούν μεταφορές κεφαλαίων, πληρωμή καρτών και δανείων, συναλλαγές που υλοποιούνται μέσω τραπέζης και αφορούν τρίτο οργανισμό όπως είναι η πληρωμή ΔΕΚΟ και οι πληρωμές λογαριασμών εταιριών σταθερής και κινητής τηλεφωνίας. Μερικές από τις οποίες είναι:

- ✓ Οι μεταφορές εντός τράπεζας: Οι μεταφορές κεφαλαίων εντός ενός τραπεζικού οργανισμού μπορεί να διακριθεί σε μεταφορές στο λογαριασμό ιδίου, όπου ο πελάτης μπορεί να επιλέξει τον τραπεζικό λογαριασμό χρέωσης και τον τραπεζικό λογαριασμό πίστωσης, πληκτρολογώντας το ποσό που θέλει να μεταφέρει και την ημερομηνία που επιθυμεί να γίνει η πληρωμή και έχει και τη δυνατότητα να εκτυπώσει την εντολή μεταφοράς, που υπέχει θέση παραστατικού της συναλλαγής. Μάλιστα σε μπορεί να κάνει μεταφορές σε λογαριασμό τρίτου, και εδώ ο χρήστης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και εν συνεχεία καλείται να πληκτρολογήσει τον αριθμό του λογαριασμού πίστωσης του δικαιούχου, όπου θα πρέπει να είναι ιδιαίτερα προσεκτικός στο σημείο αυτό, ώστε τα λεφτά να πιστωθούν στο σωστό λογαριασμό (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

- ✓ Τα εμβάσματα εσωτερικού – εξωτερικού: Για την αποστολή εμβάσματος εντός και εκτός μια χώρας ο εκάστοτε πελάτης μπορεί να επιλέξει τον τραπεζικό λογαριασμό χρέωσης και εν συνεχεία να επιλέξει την τράπεζα του ατόμου που επιθυμεί να μεταφέρει τα χρήματα Στην συνέχεια, πληκτρολογεί τον αριθμό του λογαριασμού δικαιούχου και την επωνυμία του (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).
- ✓ Οι αποπληρωμές δανείων: Η αποπληρωμή δανείων είναι η συναλλαγή μεταφορά που λαμβάνει χώρα εντός του τραπεζικού καταστήματος και μπορεί να διεκπεραιώνεται άμεσα. Έπειτα, ο πελάτης επιλέγει τον τραπεζικό λογαριασμό χρέωσης και το λογαριασμό δανείου και πληκτρολογεί το χρηματικό ποσό που θέλει να μεταφέρει για την πληρωμή της δόσης του δανείου (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).
- ✓ Η πληρωμή πιστωτικών καρτών: Οι πληρωμές πιστωτικών καρτών διακρίνονται σε τρεις (3) κατηγορίες. Αρχικά είναι η πληρωμή πιστωτικών καρτών ιδίου όπου ο εκάστοτε πελάτης μπορεί να επιλέξει τον τραπεζικό λογαριασμό χρέωσης και τον αριθμό της πιστωτικής κάρτας που επιθυμεί να πληρώσει. Εν συνεχεία μπορεί να ακολουθήσει το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή. Μάλιστα ο χρήστης έχει την δυνατότητα να μπορεί να διευκολυνθεί αφού μπορεί να προγραμματίσει τις πληρωμές.
- ✓ Η πληρωμή πιστωτικών καρτών τρίτων: όπου ο εκάστοτε πελάτης μπορεί να επιλέξει τον τραπεζικό λογαριασμό χρέωσης και μετά να πληκτρολογήσει τον αριθμό της πιστωτικής κάρτας. Όπως αναφέραμε και νωρίτερα ο χρήστης θα πρέπει να είναι ιδιαίτερα προσεκτικός προκειμένου τα λεφτά να πιστωθούν στη σωστή πιστωτική κάρτα. Στη συνέχεια, πληκτρολογεί το ποσό που θέλει να μεταφέρει για την πληρωμή της πιστωτικής κάρτας και την ημερομηνία που επιθυμεί να γίνει η πληρωμή.

Β) Οι πληροφοριακές συναλλαγές

Στο κομμάτι των πληροφοριακών συναλλαγών πολύ μεγάλο μέρος του καλύπτεται από το Internet banking. Αυτό συμβαίνει γιατί ο πελάτης μπορεί να πάρει

πληροφορίες για όλα τα διαθέσιμα προϊόντα της τράπεζας. Οι συγκεκριμένες συναλλαγές μπορούν να ταξινομηθούν στις δύο (2) παρακάτω κατηγορίες που περιγράφονται αναλυτικά. Η πρώτη κατηγορία περιλαμβάνει τις πληροφορίες των λογαριασμών. Ειδικότερα ο πελάτης είναι σε θέση να δει όλες τις πληροφορίες που αφορούν τον τραπεζικό του λογαριασμό online. Μάλιστα ο αριθμός λογαριασμού εμφανίζεται με την διεθνή μορφή IBAN. Επίσης, μπορεί να δει το όνομα του δικαιούχου, το είδος του τραπεζικού λογαριασμού, το επιτόκιο και το νόμισμα του. Επιπλέον, μπορεί να γνωρίζει το διαθέσιμο υπόλοιπό, το τοκιζόμενο υπόλοιπο και ότι άλλο έχει σχέση με τον λογαριασμό του. Επιπλέον, ορισμένες τράπεζες εμφανίζουν την τελευταία πίστωση και τελευταία χρέωση του λογαριασμού του χρήστη και τα στοιχεία των συνδικαιούχων, αν τυχόν υπάρχουν τέτοιοι λογαριασμοί. Στην δεύτερη κατηγορία είναι οι πληροφορίες καρτών. Πιο ειδικά, ο πελάτης παρατηρεί τον αριθμό πιστωτικής κάρτας, το ονοματεπώνυμο του δικαιούχου, το επιτόκιο της και το πιστωτικό όριο. Έπειτα κάνουν την εμφάνιση τους πληροφορίες για το επιτόκιο υπερημερίας, το ποσό συνδρομής, το διαθέσιμο υπόλοιπο, το οφειλόμενο υπόλοιπο και το ποσό μη εκκαθαρισμένων συναλλαγών, την ημερομηνία έκδοσης του τελευταίου statement, το ελάχιστο ποσό καταβολής, και την ημερομηνία προθεσμίας καταβολής. Επιπλέον ορισμένες τράπεζες εμφανίζουν την τελευταία πληρωμή και την ημερομηνία καταβολής του ποσού. Στις πληροφορίες επιταγών, ο εκάστοτε χρήστης έχει την δυνατότητα να επιλέξει τον τραπεζικό λογαριασμό του, να τον συνδέσει με το μπλοκ επιταγών του και να δει αναλυτικά την κατάσταση των επιταγών του. Αρκετοί τραπεζικοί οργανισμοί παρέχουν την δυνατότητα στους πελάτες να πραγματοποιήσουν ανάκληση επιταγής. Ωστόσο υπάρχουν και αρκετές τράπεζες που δίνουν την δυνατότητα για επεξεργασία επιταγών, προκειμένου να διευκολύνουν τους πελάτες τους στην παρακολούθηση αυτών. Η Τρίτη κατηγορία περιλαμβάνει τις πληροφορίες δανείων, όπου ο πελάτης που έχει κατορθώσει να πάρει δάνειο οποιαδήποτε μορφής από οποιοδήποτε τραπεζικό οργανισμό του δίνεται η δυνατότητα να ενημερώνεται μέσα από το διαδίκτυο. Δηλαδή μπορεί οποιαδήποτε στιγμή να μπορεί να δει το ποσό που του έχει απομείνει για την αποπληρωμή του, τον αριθμό των δόσεων για τα δάνεια που εκκρεμούν, το εναπομείναν ποσό για την

αποπληρωμή του, το επιτόκιο και άλλες χρήσιμες πληροφορίες (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

Γ) Αιτήσεις

Οι τραπεζικοί οργανισμοί προκειμένου να διευκολύνουν τους πελάτες τους, ενσωμάτωσαν στο internet banking, ηλεκτρονικές αιτήσεις για τα περισσότερα από τα προϊόντα τους. Μερικές από τις ηλεκτρονικές αιτήσεις είναι η αίτηση ανοίγματος λογαριασμού, η αίτηση δανείου, η αίτηση παραγγελίας συναλλάγματος και η αίτηση παραγγελίας μπλοκ επιταγών (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

Δ)Οι βοηθητικές υπηρεσίες

Πολλοί τραπεζικοί οργανισμοί εκτός των προαναφερθέντων υπηρεσιών που προσφέρουν στους χρήστες τους, έχουν την δυνατότητα να παρέχουν βοηθητικά εργαλεία προκειμένου να κάνουν πιο εύκολη τη ζωή των πελατών τους. Τα εργαλεία αυτά είναι διαθέσιμα και σε οποιοδήποτε επισκέπτεται. Τέτοιες βοηθητικές υπηρεσίες είναι: ο υπολογισμός IBAN, η μετατροπή νομισμάτων και ο υπολογισμός δόσεων δανείων (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

Η υπηρεσία του Phone Banking αποτελεί ένα εναλλακτικό κανάλι του e - banking, που δίνει την δυνατότητα στους πελάτες ενός τραπεζικού οργανισμού να διεκπεραιώνει τραπεζικές συναλλαγές χρησιμοποιώντας οποιοδήποτε τηλέφωνο όλο το 24ωρο. Οι πελάτες μπορούν να εξυπηρετηθούν μέσω ενός συστήματος προ - μαγνητοφωνιμένων μηνυμάτων, όπου γίνεται ταυτοποίηση και πιστοποίηση του εκάστοτε πελάτη, μόνο μέσω της πληκτρολόγησης κωδικών στο τηλέφωνο. Επίσης, υπάρχει και ο τρόπος εξυπηρέτησης από εξειδικευμένους υπαλλήλους που απασχολούνται σε τηλεφωνικό κέντρο. Συγκεκριμένα, οι υπάλληλοι του τραπεζικού οργανισμού που βρίσκονται στην άλλη άκρη της τηλεφωνικής γραμμής χρησιμοποιώντας ειδικά συστήματα μπορούν να υποστηρίξουν με κατάλληλο τρόπο τους πελάτες για υπηρεσίες και προϊόντα. Συνοπτικά, οι συναλλαγές που παρέχονται μέσω του phone banking είναι οι ακόλουθες (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005):

- ✓ η ενεργοποίηση και ακύρωση της κάρτας ανάληψης χρημάτων.
- ✓ η ακύρωση της πιστωτικής κάρτας.
- ✓ η αλλαγή στοιχείων αλληλογραφίας καρτούχων.
- ✓ η ενημέρωση για απόδοση και αποτίμηση αμοιβαίων κεφαλαίων.
- ✓ η ενημέρωση για όλα τα προϊόντα που έχει ο πελάτης στην τράπεζα.
- ✓ η ανάλυση υπολοίπου των λογαριασμών.
- ✓ η ανάλυση υπολοίπου πιστωτικής κάρτας και ενημέρωση κινήσεων.
- ✓ η κίνηση λογαριασμού.
- ✓ η έκδοση και ανάκληση μπλοκ επιταγών.
- ✓ οι μεταφορές χρηματικών ποσών και πληρωμών.
- ✓ οι αιτήσεις.

Τέλος, οι υπηρεσίες που παρέχονται από το Mobile Banking δεν είναι τόσο ευρέως διαδεδομένες στην Ελλάδα, με αποτέλεσμα να το διαθέτουν ορισμένες ς τράπεζες. Η συγκεκριμένη υπηρεσία του Mobile Banking υποστηρίζει συσκευές νέας τεχνολογίας με ενσωματωμένο web browser. Τέτοιες συσκευές είναι οι υπολογιστές χειρός (PDAs) και τα λεγόμενα έξυπνα κινητά (smartphones).

Η πρόσβαση στις διαθέσιμες υπηρεσίες είναι εφικτή για τους περισσότερους πελάτες όλων των εταιριών κινητής τηλεφωνίας και διακρίνεται για την γρήγορη και άμεση απόκριση χωρίς να απαιτούνται να γίνουν ρυθμίσεις από τον πελάτη. Επιπλέον, ο πελάτης μπορεί να έχει πρόσβαση στην ιστοσελίδα των ηλεκτρονικών υπηρεσιών του εκάστοτε τραπεζικού οργανισμού είτε μέσω της ηλεκτρονικής διεύθυνσης η είτε μέσω του i-mode. Εντούτοις, μοναδική προϋπόθεση για να μπορεί κανείς να έχει πρόσβαση στις ηλεκτρονικές υπηρεσίες είναι ο κάθε πελάτης να γνωρίζει εκ των προτέρων ότι τους κωδικούς πρόσβασης για να μπορεί να ανοίξει την εφαρμογή και να έχει σαφώς πρόσβαση στο διαδίκτυο. Συνοπτικά η υπηρεσία του mobile banking παρέχει τις ακόλουθες συναλλαγές (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005):

- ✓ την διαχείριση λογαριασμών.
- ✓ την διαχείριση καρτών.
- ✓ την διαχείριση δανείων.
- ✓ τις πληρωμές και τις μεταφορές λογαριασμών.
- ✓ την παραγγελία για πλήρη statements.

- ✓ την αγορά και πώληση μετοχών.
- ✓ την ενημέρωση εντός ολίγων λεπτών για εκτέλεση εντολής.
- ✓ την ενημέρωση σε πραγματικό χρόνο για την τιμή των μετοχών.
- ✓ την παρακολούθηση και την αποτίμηση του τρέχοντος χαρτοφυλακίου.
- ✓ πληροφορίες για υπηρεσίες, προϊόντα της τράπεζας.
- ✓ αλλαγή του απόρρητου κωδικού PIN.

2.4 Πλεονεκτήματα και μειονεκτήματα της ηλεκτρονικής τραπεζικής

Στην περίπτωση της ηλεκτρονικής τραπεζικής, υπάρχουν δύο (2) μοναδικοί συμμετέχοντες. Στην μία άκρη βρίσκεται ο τραπεζικός οργανισμός και στην άλλη βρίσκεται ο πελάτης. Ανάμεσα σε αυτούς τους δυο, δημιουργούνται, σχέσεις αμφίδρομου τύπου χρησιμοποιώντας το e - banking ως μέσο για την διεκπεραίωση κάθε εντολής. Οπότε, η σχέση αυτή, δημιουργεί πολλά πλεονεκτήματα και μειονεκτήματα που σημαίνει ότι επηρεάζουν τόσο τους τραπεζικούς οργανισμούς όσο και τους πελάτες αυτών και τα οποία περιγράφονται παρακάτω αναλυτικά.

2.4.1 Τα πλεονεκτήματα για τους πελάτες

Τα πλεονεκτήματα των προσφερόμενων υπηρεσιών είναι ότι παρέχουν μεγάλη ευκολία στους χρήστες διότι είναι διαθέσιμα όλες τις ημέρες και όλες τις ώρες. Επίσης, διακρίνονται από ταχύτητα που σημαίνει ότι δεν υπάρχουν ατελείωτες ουρές στο γκισέ των τραπεζών και οπότε μέσω της πρόσβασης στο διαδίκτυο μπορούν να κάνουν οποιαδήποτε συναλλαγή. Επιπρόσθετα, η πρόσβαση των πελατών γίνεται από οποιοδήποτε σημείο του χάρτη και να είναι, δηλαδή δεν υπάρχουν γεωγραφικά όρια. Ακόμα ο πελάτης μπορεί να ενημερώνεται για το τρέχων λογαριασμό του. Οι δε τραπεζικοί οργανισμοί στην προσπάθεια τους να κάνουν πιο ελκυστική την ηλεκτρονική τραπεζική έχουν εφαρμόσει χαμηλές χρεώσεις στις συναλλαγές μέσω διαδικτύου, που σε ορισμένες τράπεζες είναι και μηδενικές. Οι πελάτες μπορούν μέσω της χρήσης του διαδικτύου να ολοκληρώνουν τις όποιες συναλλαγές επιθυμούν

και ταυτόχρονα να μπορούν να ελέγξουν αν για παράδειγμα έχει μεταφορά του χρηματικού ποσού σε πραγματικό χρόνο και αν τυχόν υπάρχει κάποια επιβάρυνση στην μεταφορά αυτή. Τέλος, μέσω της ηλεκτρονικής τραπεζικής ο πελάτης μπορεί να αποφασίσει χαλαρά και χωρίς κάποια πίεση για τη αγορά ενός προϊόντος ή υπηρεσίας (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

2.4.2 Τα πλεονεκτήματα για τις τράπεζες

Εκτός από τα πλεονεκτήματα που έχει η ηλεκτρονική τραπεζική για τους πελάτες, έχει και για τους τραπεζικούς οργανισμούς. Πιο συγκεκριμένα, το πρώτο και βασικό χαρακτηριστικό είναι ότι μέσω της διανομής υπηρεσιών, προϊόντων όλο το 24ωρο για όλες τις ημέρες πετυχαίνουν να γίνονται ανταγωνιστικοί σε σχέση με άλλους τραπεζικούς οργανισμούς. Επιπλέον, μέσω της διεύρυνσης των γεωγραφικών ορίων είναι δυνατόν να μπορούν να χρησιμοποιήσουν τις υπηρεσίες και άτομα που δεν μπορούν να έχουν φυσική πρόσβαση στο εκάστοτε τραπεζικό ίδρυμα. Ακόμα έχει αποδειχθεί ότι μέσω της εξυπηρέτησης των πελατών μέσα από ένα σύνολο υπηρεσιών διαδικτύου ενισχύεται το αίσθημα της αφοσίωσης και οπότε ο πελάτης σε καμιά περίπτωση δεν εγκαταλείπει την τράπεζα και να πάει σε κάποια άλλη. Τα λειτουργικά έξοδα μειώνονται διότι η πλειονότητα των συναλλαγών πραγματοποιούνται μέσω διαδικτύου και πολύ λιγότερο από τα φυσικά καταστήματα, που όλο αυτό σημαίνει ότι οι πελάτες εξυπηρετούνται πιο αποτελεσματικά και πιο αποδοτικά (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

Ακόμα, μέσω της ηλεκτρονικής τραπεζικής, οι τραπεζικοί οργανισμοί μπορούν να προωθήσουν νέα προϊόντα, υπηρεσίες και τυχόν προσφορές που υπό άλλες συνθήκες θα ήταν δύσκολο και αρκετά χρονοβόρο.

Τελικά το συμπέρασμα που προκύπτει είναι ότι είναι απαραίτητο και χρήσιμο για το κάθε τραπεζικό ίδρυμα να μπορεί να προσελκύσει τους ήδη υπάρχοντες πελάτες ή και καινούργιους και να δημιουργήσει ένα περιβάλλον ασφάλειας προκειμένου να μπορεί ο πελάτης να νιώσει άνετα όπως και με τις παραδοσιακές συναλλαγές. Όλο αυτό αποτελεί και την στρατηγική που εφαρμόζεται από πλειονότητα των τραπεζικών ιδρυμάτων που έγκειται στην δαπάνη μεγάλων ποσών για την εξέλιξη των παρόντων

πληροφοριακών συστημάτων όσο και την αντιμετώπιση κενών σημείων που υπάρχουν στα συστήματα αυτά.

2.4.3 Τα μειονεκτήματα για τους πελάτες

Η ηλεκτρονική τραπεζική έχει εκτός από πλεονεκτήματα και αρκετά μειονεκτήματα για τους εκάστοτε πελάτες. Ένα εξ' αυτών είναι σε κάποιες περιπτώσεις απαιτείται αρκετός χρόνος για να μπορέσει να γραφεί ηλεκτρονικά. Πιο ειδικά για να μπορέσει να γραφεί κάποιος στο online πρόγραμμα της εκάστοτε τράπεζας θα πρέπει να δώσει στοιχεία της ταυτότητας του και να υπογράψει ένα έντυπο στο τραπεζικό κατάστημα ή αν είναι μια αποκλειστικά ηλεκτρονική τράπεζα, τα έντυπα θα πρέπει να αποσταλούν ταχυδρομικώς προκειμένου να συμπληρωθούν και να σταλούν ξανά στην τράπεζα. Επίσης, υπάρχουν περιπτώσεις ατόμων που δεν έχουν γνώσεις πληροφορικής και οπότε δεν μπορούν να εισέλθουν στην ηλεκτρονική πλατφόρμα της τράπεζας. Τέλος, ένα από τα πιο σημαντικά χαρακτηριστικά της ηλεκτρονικής τραπεζικής είναι η δυσπιστία που αντιμετωπίζει από μεγάλη μερίδα του κόσμου. Αυτό προκύπτει από την επιθυμία τους να θέλουν να βλέπουν αυτόν που κάνει την μεταφορά των χρημάτων, θεωρώντας ότι δεν υπάρχει κάποιο πρόβλημα, ενώ με την διαδικασία της ηλεκτρονικής τραπεζικής διακατέχονται από αισθήματα αμφιβολίας (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

2.4.4 Τα μειονεκτήματα για τις τράπεζες

Τα μειονεκτήματα για τους τραπεζικούς οργανισμούς είναι αρκετά. Ένα από αυτά είναι το υψηλό κόστους εγκατάστασης. Ειδικότερα κατά την διαδικασία δημιουργίας μιας ιστοσελίδας που διαφημίζει προϊόντα και υπηρεσίες είναι πολλές φορές δύσκολη διαδικασία γιατί απαιτεί εξειδικευμένες γνώσεις από τα άτομα που απασχολούνται με αυτό. Είναι λογικό ότι το κόστος των νέων τεχνολογιών να είναι ιδιαίτερο υψηλό, οπότε ο εκάστοτε τραπεζικός οργανισμός θα πρέπει να επιλέγει τεχνολογίες που θα ταιριάζουν με το προφίλ της και την πολιτική που εφαρμόζει. Επίσης, ένα άλλο

μειονέκτημα της ηλεκτρονικής τραπεζικής είναι η έλλειψη ασφάλειας που παρουσιάζουν τα πληροφοριακά συστήματα που εκδηλώνεται είτε μέσω ηλεκτρονικών επιθέσεων ή μη εξουσιοδοτημένης πρόσβασης στο εκάστοτε τραπεζικό σύστημα. Οπότε προτεραιότητα των τραπεζικών ιδρυμάτων είναι η αύξηση των επιπέδων ασφάλειας στα συστήματα αυτά. Επιπλέον, είναι συνήθως αρκετά μεγάλο το ποσόν που δαπανάται από τον τραπεζικό οργανισμό για την συντήρηση λειτουργίας της αντίστοιχης ιστοσελίδας και επειδή όπως αναφέραμε καμιά ιστοσελίδα δεν είναι ασφαλής από διαδικτυακές επιθέσεις, θα πρέπει ο τραπεζικός οργανισμός να ενημερώνει τα προγράμματα ασφαλείας διαρκώς δαπανώντας αρκετά χρήματα. Τέλος, ο εκάστοτε τραπεζικός οργανισμός θα πρέπει να εκπαιδεύει συνεχώς τους υπαλλήλους για τυχόν αλλαγές που υπάρχουν στην ηλεκτρονική σελίδα με σκοπό να είναι ενημερωμένοι για τυχόν αλλαγές στην πολιτική της τράπεζας και να είναι σε θέση να μπορούν να ενημερώνουν τους πελάτες για απορίες που έχουν. Μια διαδικασία που είναι μια αρκετά μεγάλη επιβάρυνση για τον τραπεζικό οργανισμό (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005).

ΚΕΦΑΛΑΙΟ 3: ΜΕΘΟΔΟΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΠΛΗΡΩΜΩΝ

3.1 Πιστωτικές κάρτες

Οι πιστωτικές κάρτες αποτελούν, ίσως, την πιο δημοφιλή μέθοδο ηλεκτρονικών πληρωμών στις μέρες μας. Η ύπαρξη αυτού του είδους των καρτών, χρονολογείται πριν ακόμα, από την έναρξη του ηλεκτρονικού εμπορίου. Το πιο σημαντικό πλεονέκτημα στην ευρεία χρήση των πιστωτικών καρτών, αποτέλεσε το γεγονός του χαμηλού λειτουργικού τους κόστους. Σε αυτό το σημείο πρέπει, βεβαία, προς καλύτερη κατανόηση, να αναφερθεί ότι οι κάρτες αυτές συνδέονται άμεσα με τις πελατειακές βάσεις δεδομένων του ηλεκτρονικού εμπορίου, με αποτέλεσμα η διαδικασία των πληρωμών στο χώρο του διαδικτύου να αποτελεί μια εξαιρετικά απλά καθώς και γρήγορη δραστηριότητα (Lauren & Traver, 2011).

Εκτός βέβαια, από τα πλεονεκτήματα τα οποία αναφέρθηκαν παραπάνω, οι πιστωτικές κάρτες διέπονται και από πολύ σημαντικά μειονεκτήματα τα οποία έχουν ως εξής (Lauren & Traver, 2011):

- ✓ Ο υψηλός κίνδυνος εξαπάτησης του καταναλωτικού κοινού στο χώρο του διαδικτυακού εμπορίου.
- ✓ Το περιορισμένο εύρος συναλλαγών που διαθέτουν.

3.2 Paypal

Η PayPal λειτουργεί ως διαμεσολαβητής μεταξύ αγοραστή και πωλητή. Ο πελάτης δίνει τα τραπεζικά στοιχεία του στην PayPal, η οποία διαχειρίζεται την πληρωμή, αλλά ποτέ δεν δίνει τα στοιχεία αυτά στην εταιρεία που πραγματοποίησε την πώληση. Παρέχει ασφάλεια λοιπόν σε αμφότερα μέρη, είναι διαθέσιμη σε πολλές χώρες, ενώ διαμεσολαβεί σε περιπτώσεις σύγκρουσης. Για τους λόγους αυτούς, θα πρέπει να προσφέρουμε την PayPal ως τρόπο πληρωμής.

Για να πληρώσουμε μέσω PayPal πρέπει να έχουμε μόνο μια κάρτα και δεν χρειάζεται να δημιουργήσουμε λογαριασμό. Το μεγαλύτερο μειονέκτημα είναι οι υψηλές προμήθειες που χρεώνονται για την υπηρεσία, συνεπώς η PayPal ως η μόνη διαθέσιμη μέθοδος δεν συνιστάται. Είναι ένας απαραίτητος τρόπος πληρωμής για το ηλεκτρονικό μας κατάστημα, αλλά όχι και ο μοναδικός (Laudon & Traver, 2011).

3.3 Ψηφιακό χρήμα

Το ψηφιακό χρήμα έχει δώσει την θέση του, τα τελευταία χρόνια στο παραδοσιακό χρήμα με το οποίο είχαν συνηθίσει τα άτομα να συναλλάσσονται. Ένα κύριο όφελος από τη χρήση του ηλεκτρονικού χρήματος είναι ότι αποφεύγονται τα έξοδα διεκπεραίωσης που παρακρατούν οι τράπεζες για πληρωμές μικροποσών. Άλλα πλεονεκτήματα που προσφέρουν είναι η ανωνυμία του χρήστη, η ευκολία στη χρησιμοποίησή τους και η υποστήριξη στις δια-συνοριακές συνοριακές συναλλαγές (Lauden & Traver, 2011).

Το πιο δημοφιλή ψηφιακό νόμισμα αποτελεί το bitcoin. Το συγκεκριμένο είδος ψηφιακού χρήματος αποτελεί ένα συνολικό σύστημα πληρωμών το οποίο αναπτύχθηκε σε μορφή λογισμικού ανοικτού κώδικα (Matonis, 2013) και δόθηκε για ενεργοποίηση των ηλεκτρονικών συναλλαγών το έτος 2009 στο κοινό (Nakamoto, 2008). Το ίδιο έτος έλαβε την σημερινή του ονομασία γίνονταν με ταχείς ρυθμούς το πιο γνωστό ψηφιακό νόμισμα συναλλαγών (Matonis, 2013).

Οι ηλεκτρονικές συναλλαγές (πληρωμές) οι οποίες πραγματοποιούνται μέσω του συγκεκριμένου συστήματος, αρχειοθετούνται σε ένα βιβλίο διαχειρήσιμο από το δημόσιο, εφαρμόζοντας μία ανεξάρτητη μονάδα μέτρησης η οποία καλείται ως bitcoin. Επίσης, οι συναλλαγές λαμβάνουν χώρα διαμέσου ενός είδους ομότιμου συστήματος, χωρίς την παρουσία βασικό προσώπου ως διαχειριστή (Nakamoto, 2008). Σύμφωνα με τον Joyner (2014), το bitcoin ως νόμισμα ψηφιακού χαρακτήρα

έχει επικριθεί σε πολύ μεγάλο βαθμό από τα μέσα μαζικής ενημέρωσης, σε παγκόσμιο επίπεδο.

Οι βασικές ιστοσελίδες οι οποίες επιτρέπουν να πραγματοποιείται πληρωμή διαμέσου των bitcoins είναι οι ακόλουθες (Stelton, 2012; Franceschi-Bicchierai, 2013; Dahlberg, 2014; Vaishampayan, 2014; Biggs, 2014):

- ✓ Overstock.com.
- ✓ Okcypid.
- ✓ WordPress.
- ✓ AtomicMall.
- ✓ Μη κερδοσκοπικό ίδρυμα Electromic Frontier.
- ✓ TigerDirect.

3.4 Internet banking

Το Internet banking που ονομάζεται και online Banking, χρησιμοποιεί το διαδίκτυο ως τρόπο διεξαγωγής τραπεζικών δραστηριοτήτων. Πιο ειδικά, για να μπορέσει ο εκάστοτε χρήστης να χρησιμοποιεί τις υπηρεσίες της ηλεκτρονικής τραπεζικής θα πρέπει να διαθέτει ηλεκτρονικό υπολογιστή και να έχει πρόσβαση στο διαδίκτυο. Εντούτοις, σε ορισμένες περιπτώσεις είναι απαραίτητο η ύπαρξη συσκευών ασφαλείας όπως είναι για παράδειγμα η εγκατάσταση ειδικού λογισμικού ασφαλείας ή ψηφιακό πιστοποιητικό. Ο πελάτης μίας τράπεζας, μέσω του Internet banking, έχει τη δυνατότητα να εκτελεί μεγάλο πλήθος τραπεζικών συναλλαγών και να λαμβάνει την πληροφόρηση που επιθυμεί.

Η πλειονότητα των τραπεζικών ιδρυμάτων έχουν πλέον την τεχνογνωσία και τις δυνατότητες να προσωποποιούν τις ηλεκτρονικές τους υπηρεσίες, με βάση κάθε φορά την κατηγορία πελατών που αντιπροσωπεύει ο χρήστης και οπότε με αυτό το τρόπο

υπάρχουν για παράδειγμα επιπρόσθετες δυνατότητες για εταιρικούς χρήστες σε σχέση με ιδιώτες. Επίσης, γίνονται επενδύσεις και μελέτες και σε θέματα ασφάλειας που είναι ιδιαίτερα κρίσιμο για την αξιοπιστία και την ομαλή λειτουργία των ηλεκτρονικών τραπεζικών συστημάτων (Αγγέλης, 2005).

3.5 Mobile Phone payment

Η υπηρεσία του Phone Banking αποτελεί ένα εναλλακτικό κανάλι του e- banking, που δίνει την δυνατότητα στους πελάτες ενός τραπεζικού οργανισμού να διεκπεραιώνει τραπεζικές συναλλαγές και πληρωμές, χρησιμοποιώντας οποιοδήποτε τηλέφωνο όλο το 24ωρο. Οι πελάτες μπορούν να εξυπηρετηθούν μέσω ενός συστήματος προ - μαγνητοφωνιμένων μηνυμάτων, όπου γίνεται ταυτοποίηση και πιστοποίηση του εκάστοτε πελάτη, μόνο μέσω της πληκτρολόγησης κωδικών στο τηλέφωνο. Επίσης, υπάρχει και ο τρόπος εξυπηρέτησης από εξειδικευμένους υπαλλήλους που απασχολούνται σε τηλεφωνικό κέντρο. Συγκεκριμένα, οι υπάλληλοι του τραπεζικού οργανισμού που βρίσκονται στην άλλη άκρη της τηλεφωνικής γραμμής χρησιμοποιώντας ειδικά συστήματα μπορούν να υποστηρίξουν με κατάλληλο τρόπο τους πελάτες για υπηρεσίες και προϊόντα. Συνοπτικά οι συναλλαγές που παρέχονται μέσω του phone banking είναι οι ακόλουθες (Σινανιώτη – Μαρούδη & Φαρσαρώτας, 2005):

- ✓ η ενεργοποίηση και ακύρωση της κάρτας ανάληψης χρημάτων.
- ✓ η ακύρωση της πιστωτικής κάρτας.
- ✓ η αλλαγή στοιχείων αλληλογραφίας καρτούχων.
- ✓ η ενημέρωση για απόδοση και αποτίμηση αμοιβαίων κεφαλαίων.
- ✓ η ενημέρωση για όλα τα προϊόντα που έχει ο πελάτης στην τράπεζα.
- ✓ η ανάλυση υπολοίπου των λογαριασμών.
- ✓ η ανάλυση υπολοίπου πιστωτικής κάρτας και ενημέρωση κινήσεων.
- ✓ η κίνηση λογαριασμού.
- ✓ η έκδοση και ανάκληση μπλοκ επιταγών.
- ✓ οι μεταφορές χρηματικών ποσών και πληρωμών.
- ✓ οι αιτήσεις.

ΚΕΦΑΛΑΙΟ 4: Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΝΑΛΑΓΩΝ

4.1 Εισαγωγή

Με βάση όλα τα προηγούμενα που έχουμε αναφέρει εύκολα κανείς διαπιστώνει ότι η ηλεκτρονική τραπεζική μπορεί να διευκολύνει τις καθημερινές συναλλαγές των πολιτών τράπεζας αλλά δημιουργεί αρκετά θέματα ασφάλειας που έχουν να κάνουν με οικονομικές, πληροφοριακές συναλλαγές και οτιδήποτε άλλου τύπου δεδομένα διακινούνται στο διαδίκτυο. Οπότε δημιουργούνται 2 ειδών ερωτήματα. Το πρώτο έχει να κάνει, κατά πόσο είναι ασφαλή τα δεδομένα των πελατών της τράπεζας που είναι αποθηκευμένα στα τραπεζικά πληροφοριακά συστήματα των τραπεζών και το δεύτερο έχει να κάνει με το εάν υπάρχουν τρόποι προστασίας των δεδομένων αυτών.

4.2 Οι στόχοι των μηχανισμών ασφάλειας στα πληροφοριακά συστήματα

Οι μηχανισμοί ασφαλείας ενός πληροφοριακού συστήματος της ηλεκτρονικής τραπεζικής, λέμε ότι επιτυγχάνουν τον σκοπό τους, όταν έχουν επιτευχθεί οι ακόλουθοι στόχοι. Ο πρώτος στόχος έχει να κάνει με την προστασία της ακεραιότητας των περιουσιακών στοιχείων. Πιο ειδικά, είναι ο πιο σημαντικός στόχος γιατί θα πρέπει το χρηματικό ποσό να μην αλλοιώνεται, όσον αφορά την ποσότητα σε οποιοδήποτε υποσύστημα και αν αποθηκευτούν. Επίσης, θα πρέπει οι μηχανισμοί ασφαλείας να παρέχουν εμπιστευτικότητα όσον αφορά τα δεδομένα. Με λίγα λόγια τα δεδομένα που διακινούνται μέσα στο πληροφοριακό σύστημα θα πρέπει να γνωστοποιούνται αποκλειστικά και μόνο στους εξουσιοδοτημένους χρήστες. Δηλαδή, οι πελάτες δεν μπορούν να γνωρίζουν τους κωδικούς πρόσβασης του διαχειριστή και ο διαχειριστής δεν πρέπει να γνωρίζει τα υπόλοιπα των λογαριασμών των πελατών.

Μια άλλη αρμοδιότητα των συστημάτων ασφαλείας είναι η διαρκής πιστοποίηση του ηλεκτρονικού χρήματος που μετακινείται μεταξύ των συστημάτων και η πιστοποίηση των συστημάτων που ανταλλάσσουν δεδομένα μεταξύ τους. Επίσης, τα συστήματα ασφαλείας θα πρέπει να κάνουν έλεγχο πρόσβασης. Δηλαδή οι πελάτες θα πρέπει να έχουν στην κατοχή τους μοναδικούς κωδικούς με απώτερο σκοπό τον περιορισμό της πρόσβασης στα αντίστοιχα δεδομένα που τους ενδιαφέρουν. Η δέσμευση και η επιβεβαίωση της αξιοπιστίας των συναλλαγών είναι ένας ακόμη στόχος, διότι κάθε συναλλαγή πραγματοποιείται με συγκεκριμένο χρηματικό ποσό και σε ορισμένα τραπεζικά υποκαταστήματα. Μάλιστα αν δεν μπορεί να καθοριστεί με συγκεκριμένο τρόπο τότε η συναλλαγή θεωρείται αδύνατη. Επιπλέον, σε περιπτώσεις που προκύψει πρόβλημα πριν την τελική επιβεβαίωση η οποιαδήποτε συναλλαγή θα πρέπει να θεωρείται άκυρη.

Τα συστήματα ασφαλείας είναι υπεύθυνα για την ορθή τήρηση των συναλλαγών και των διαδικασιών διότι διαφορετικά η μη τήρηση της σειράς σε μια διαδικασία μπορεί να οδηγήσει σε απρόσμενες καταστάσεις. Ακόμα η αποφυγή απωλειών μονάδων ηλεκτρονικού χρήματος είναι ένας στόχος της ασφάλειας των συστημάτων. Διότι οι ποσότητες χρημάτων που εισέρχονται στο πληροφοριακό σύστημα θα πρέπει να παραμένουν ίδιες κατά την διάρκεια διαφόρων συναλλαγών χωρίς να εμφανίζουν απώλειες. Ένας άλλος στόχος είναι η τήρηση ορίων στα χρηματικά ποσά. Δηλαδή σε οποιεσδήποτε συναλλαγές θα πρέπει να υπάρχει ένα ανώτατο ποσό χρημάτων το οποίο θα μπορούν να διακινήσουν οι πελάτες.

Άλλος στόχος των συστημάτων ασφαλείας είναι η ανιχνευσιμότητα των συναλλαγών, ένας στόχος που αφορά κατά βάση τον διαχειριστή διότι είναι σε θέση να παρακολουθεί όλα τα βήματα που λαμβάνουν χώρα κατά την διάρκεια μιας συναλλαγής. Επίσης η ασφάλεια έχει να κάνει και με τον εντοπισμό κάθε μη φυσιολογικής ενέργειας στα πληροφοριακά συστήματα όπως είναι η προσπάθεια παράνομης πρόσβασης σε δεδομένα και υποκλοπής αυτών, την χρήση ειδικών πρωτοκόλλων κρυπτογράφησης για προστασία των δεδομένων, την ενημέρωση των λογισμικών ασφαλείας όπως είναι τα αντιικά (antivirus) και την δυνατότητα διαθεσιμότητας των πληροφοριακών συστημάτων ακόμα και έχουν προσβληθεί από κάποιο είδους ιού.

4.3 Κίνδυνοι της ηλεκτρονικής τραπεζικής

Οι κίνδυνοι που έχουν να αντιμετωπίσουν τα συστήματα ηλεκτρονικής τραπεζικής, ολοένα και αυξάνονται. Μάλιστα, οι περισσότερες ηλεκτρονικές απάτες, έχουν σαν στόχο πρωτίστως να εξαπατήσουν τον εκάστοτε πελάτη υποκλέπτοντας τους κωδικούς εισόδου του στις ηλεκτρονικές υπηρεσίες του τραπεζικού οργανισμού. Στα επόμενα εδάφια παρουσιάζονται αναλυτικά οι πιο συχνά χρησιμοποιούμενοι τρόποι εξαπάτησης των χρηστών της ηλεκτρονικής τραπεζικής.

4.3.1 Η μέθοδος Phishing

Εύκολα κανείς καταλαβαίνει ότι το όνομα είναι παραλλαγή του αγγλικού «fishing» δηλαδή του «ψαρέματος». Με τον όρο phishing εννοούμε τη διαδικασία κατά την οποία ο επίδοξος υποκλοπέας προσπαθεί να αποσπάσει τα προσωπικά στοιχεία με περισσότερο οικονομικό χαρακτήρα. Μάλιστα η διαδικασία περιλαμβάνει την απόσπαση στοιχείων των τραπεζικών λογαριασμών και πιστωτικών καρτών. Συνήθως το δόλωμα που χρησιμοποιείται είναι μια ψεύτικη αιτία.

Η συνήθης πρακτική που χρησιμοποιεί ο υποκλοπέας είναι η προσπάθεια υποκλοπής των προσωπικών στοιχείων του υποψήφιου θύματος και συμβαίνει με την αποστολή κάποιου spam e-mail στην αλληλογραφία αυτού. Στο συγκεκριμένο e-mail ο υποκλοπέας μπορεί να συστηθεί ως υπάλληλος που εργάζεται σε κάποια μεγάλη επιχείρηση και μέσω του email ζητά από το θύμα κάποια προσωπικά στοιχεία.
Εν συνεχεία, το υποψήφιο θύμα, πείθεται ότι όντως τι το e-mail προέρχεται από τον ισχυριζόμενο αποστολέα, αποστέλλει τα προσωπικά του στοιχεία. Έτσι τα στοιχεία αυτά θα χρησιμοποιηθούν από τους υποκλοπείς για την πραγματοποίηση παράνομων οικονομικών συναλλαγών.

Το πιο βασικό εργαλείο του phishing είναι οι λεγόμενοι αποπλανητικοί σύνδεσμοι (link manipulation). Πιο ειδικά ο χρήστης βρίσκεται σε μία ιστοσελίδα μέσω ενός

e-mail ή μέσω sms που του έχεις σταλεί στο κινητό μήνυμα και παραπέμπεται σε έναν σύνδεσμο που φαίνεται αληθοφανής, αλλά στην ουσία είναι φτιαγμένος προκειμένου να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται.

Στην πραγματικότητα αυτό είναι κάτι πολύ κρίσιμο και πολύ εύκολο στη δημιουργία του, αφού σε έναν απλό κώδικα HTML δίνεται η δυνατότητα να μετατρέψει κανείς τον τίτλο του συνδέσμου όπως επιθυμεί. Πάνω σε αυτό λειτουργούν και οι ιστοσελίδες που χρησιμοποιούν παραπλανητικούς συνδέσμους, και οδηγούν τους χρήστες σε σελίδες φαινομενικά πανομοιότυπες με τις αυθεντικές ιστοσελίδες, αλλά έχουν την ατυχία να ανήκουν στον server του υποκλοπέα. Μάλιστα σε κάποιες περιπτώσεις, η αναγραφή είναι τόσο καλή, που και ο ίδιος ο φυλλομετρητής μπορεί να ξεγελαστεί και να εμφανίσει στην γραμμή διευθύνσεων την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας

Οπότε σε μια προσπάθεια μείωσης του χρόνου αντίδρασης του υποψήφιου θύματος, ορισμένα μηνύματα περιέχουν απειλές τύπου ότι εάν δεν προβεί ο εκάστοτε χρήστης στις απαιτούμενες ενέργειες όπως είναι η επιβεβαίωση των στοιχείων μέσα σε συγκεκριμένο χρονικό διάστημα ο λογαριασμός του θα μπλοκαριστεί και δε θα μπορεί να πραγματοποιήσει οποιαδήποτε άλλη συναλλαγή. Έτσι αναγκάζουν το υποψήφιο θύμα να δώσει τα στοιχεία που του ζητούνται, χωρίς να μπει στην διαδικασία να ελέγξει την γνησιότητα του μηνύματος.

Οι βασικοί πυλώνες που καθορίζουν αν μια επίθεση τύπου phishing είναι επιτυχημένη είναι η έλλειψη γνώσεων του υποψήφιου θύματος για την ύπαρξη τέτοιου είδους επιθέσεων, την έλλειψη προσοχής του θύματος που συνδέεται από οπτική εξαπάτηση. Γενικά, η πλειονότητα των ανθρώπων ξέρει να χειρίζεται τις βασικές λειτουργίες του υπολογιστή και των λειτουργιών του διαδικτύου χωρίς να γνωρίζει σε βάθος τον τρόπο λειτουργίας αυτού. Επίσης, σε περιπτώσεις που ο χρήστης έχει τις κατάλληλες γνώσεις για να μπορεί να ανιχνεύει τα κακόβουλα στοιχεία, δεν θα προσέξει τα σημάδια, αφού μπορεί να είναι απασχολημένος με κάτι άλλο ή απλά να είναι αφηρημένος. Μάλιστα έχει διαπιστωθεί ότι οι επιθέσεις Phishing είχαν αυξηθεί κατά 30% σε εορταστικές ημέρες όπως είναι τα Χριστούγεννα, την πρωτοχρονιά και

το Πάσχα. Οπότε ο εκάστοτε πελάτης μπορεί να μην δίνει αρκετή σημασία στις υπάρχουσες προειδοποιήσεις ασφάλειας ή στην έλλειψη αυτών.

Τέλος ο σκοπός του υποκλοπέα είναι σε κάθε περίπτωση να πείσει το υποψήφιο θύμα για την αυθεντικότητα και την αξιοπιστία που πρεσβεύει. Αυτό επιτυγχάνεται με συγκεκριμένους τρόπους. Ο πρώτος τρόπος είναι η αποστολή ενός κειμένου παραπλανητικού χαρακτήρα, όπου έχει σκόπιμα λανθασμένη σύνταξη και αναγραμματισμούς γραμμάτων. Ένας δεύτερος τρόπος είναι η χρήση εικόνων που μοιάζουν με εκείνες που χρησιμοποιούν οι ιστοσελίδες αλλά πατώντας το ο χρήστης ανακατευθύνεται σε άλλη ιστοσελίδα. Επίσης σε πολλές περιπτώσεις υπάρχουν ιστοσελίδες που μοιάζουν επακριβώς έχουν ίδιο design αλλά σε καμιά περίπτωση δεν είναι η πραγματική ιστοσελίδα. Ο συνδυασμός όλων αυτών τρόπων εξασφαλίζει δυστυχώς για το υποψήφιο θύμα μεγάλη επιτυχία για τον υποκλοπέα (Τσάμης, 2003).

4.3.2 Η μέθοδος Pharming

Η μέθοδος του pharming παρουσιάζει παρόμοια χαρακτηριστικά με αυτά του phishing και έχει σαν σκοπό την υποκλοπή των προσωπικών στοιχείων των χρηστών του διαδικτύου. Η συγκεκριμένη μέθοδος θεωρείται από τις πιο επικίνδυνες μεθόδους εξαπάτησης του υποψήφιου θύματος, καθώς πρόκειται για ένα πολύ εξειδικευμένο πρόγραμμα που εντοπίζει με ευκολία κενά ασφαλείας και στη συνέχεια τα εκμεταλλεύεται. Ειδικότερα, οι χρήστες έχουν την εντύπωση ότι βρίσκονται σε μια γνήσια ιστοσελίδα, που όμως στην πραγματικότητα έχουν οδηγηθεί σε μια ψεύτικη. Ο υποκλοπέας καταφέρνει να ανακατευθύνει τα υποψήφια θύματα σε άλλες ιστοσελίδες , όπου συμπληρώνουν τα στοιχεία τους νομίζοντας ότι θα αγοράσουν τα προϊόντα που θέλουν, ενώ στην πραγματικότητα τα στοιχεία ναι μεν καταχωρούνται αλλά με στόχο την οικονομική εξαπάτηση αυτών από τους υποκλοπείς. Ακόμα και στην περίπτωση που ο χρήστης γράφει πληκτρολογώντας σωστά την διεύθυνση του διαδικτυακού τόπου που επιθυμεί να επισκεφτεί, ο συγκεκριμένος υπολογιστής τον "οδηγεί" μόνο σε πλαστές ιστοσελίδες. Μάλιστα σε περιπτώσεις που έχουν να κάνουν με την ιστοσελίδα τραπεζικών οργανισμών, η προσπάθεια του υποψήφιου θύματος να

πραγματοποιήσει τις συναλλαγές του μέσω ηλεκτρονικής τραπεζικής καταλήγει στη μεταφορά των χρημάτων του στους υποκλοπείς. Με λίγα λόγια η μέθοδος του pharming, εξελίσσεται διαρκώς σε μία από τις σοβαρότερες μορφές εγκληματικότητας στο διαδίκτυο (Κάτσικας & Γκριτζάλη, 2003).

4.3.3 Η μέθοδος cross – site - scripting

Η μέθοδος του Cross Site Scripting είναι από τις πιο ευρέως και γνωστές επιθέσεις που λαμβάνουν χώρα στο διαδίκτυο. Έχουν το χαρακτηριστικό ότι μπορούν να εκμεταλλεύονται τα τρωτά σημεία των υπολογιστικών συστημάτων προκείμενου να μπορούν να πραγματοποιούν επιθέσεις στο διαδίκτυο. Οι δε επιθέσεις αυτές έχουν σαν στόχο την κλοπή των προσωπικών στοιχείων ταυτότητας του κάθε υποψήφιου θύματος, την πρόσβαση σε πληροφορίες εμπιστευτικού χαρακτήρα και την προώθηση ψεύτικων διαφημίσεων (Τσάμης, 2003).

4.3.4 Η μέθοδος Scamming

Γενικά οι απάτες που είναι γνωστές ως «scam» έχουν να κάνουν με κάποιου είδους συναλλαγή που για να μπορέσει να ολοκληρωθεί απαιτείται να μεταφέρει ένα χρηματικό ποσό το υποψήφιο θύμα, στον υποκλοπέα αφού του έχει στείλει νωρίτερα ένα ψεύτικο μήνυμα (email). Ωστόσο, το θύμα δεν παραλαμβάνει ποτέ αυτό που έχει πληρώσει.

Η προσέγγιση του υποψήφιου θύματος γίνεται αποκλειστικά μέσω της ηλεκτρονικής αλληλογραφίας. Πιο αναλυτικά ο υποκλοπέας αποστέλλει ένα μήνυμα, που παρουσιάζει έντονα συναισθηματικά χαρακτηριστικά προκειμένου να πείσει το θύμα να καταβάλει ένα χρηματικό ποσό με αντάλλαγμα συνήθως την απολαβή ενός ακόμα μεγαλύτερου ποσού που μπορεί να είναι της τάξης των εκατομμυρίων. Ακόμα για την υποτιθέμενη ενημέρωση που παρέχει ο υποκλοπέας συμφωνείται ότι θα λάβει ένα μικρό ποσό -προμήθεια από το τεράστιο ποσό που θα κερδίσει.

Οι πιο γνωστές συναλλαγές που γίνονται μέσω αυτής της μεθόδου έχει να κάνει με αποδέσμευση χρημάτων από τραπεζικούς λογαριασμούς, συμμετοχή σε λογαριασμούς, διεκδίκηση υποτιθέμενων κληρονομιών, παραλαβή και αποθήκευση των χρημάτων του αποστολέα σε ασφαλές μέρος και η επένδυση των χρημάτων αυτών στη χώρα του θύματος. Μάλιστα η πλειονότητα των μηνυμάτων προέρχεται από τη Νιγηρία. Για αυτό το λόγο τότε η πρακτική αυτή αποκαλείται «νιγηριανό scam» ή και «απάτη 419» από το άρθρο του ποινικού κώδικα της Νιγηρίας.

Ο υποκλοπέας προκειμένου να πείσει το θύμα διατηρεί την επικοινωνία και στέλνει σε αρκετές περιπτώσεις και ατομικά στοιχεία που είναι πλαστά προκειμένου το θύμα να μην έχει καθόλου υποψίες. Στη συνέχεια ζητάει χρηματικά ποσά από το θύμα για να καλύψουν τα έξοδα της συναλλαγή, με αποτέλεσμα από την στιγμή που θα λάβουν τα χρήματα, να διακόψουν κάθε είδος επικοινωνίας.

Μια άλλη πρακτική που περιλαμβάνει η μέθοδος αυτή είναι η αποκαλούμενη διεθνής λαχεία όπου στέλνονται e-mail, που περιέχουν μηνύματα για απολαβή τεράστιων κερδών από κληρονομιές, διαγωνισμούς και άλλα. Έπειτα ζητούν από τα υποψήφια θύματα να καταβάλλουν χρήματα για διαδικαστικά έξοδα. Έτσι κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά.

Πάνω στο ίδιο μοτίβο λειτουργούν και οι αποκαλούμενες δημοπρασίες. Μάλιστα σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνεται πλειστηριασμός ανύπαρκτων αντικειμένων. Οπότε το υποψήφιο θύμα πληρώνει διαδικαστικά έξοδα, και δεν παραλαμβάνει ποτέ το αντικείμενο για το οποίο έχει πληρώσει.

Τέλος, ένας εναλλακτικός τρόπος scamming είναι η αποστολή στο υποψήφιο θύμα e-mail με που περιέχει ένα συνημμένο αρχείο ή πρόγραμμα. Αμέσως μόλις το ανοίξει το υποψήφιο θύμα αρχίζει μια διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του. Με συνέπεια το θύμα να μην μπορεί να ανοίξει κανένα αρχείο εκτός από το μήνυμα που του άφησε ο υποκλοπέας όπου του εξηγούν ότι μόνο αν πληρώσει ένα συγκεκριμένο ποσό θα του αποσταλεί ο κωδικός πρόσβασης ώστε να ξεμπλοκάρει ο υπολογιστής του (Πάγκαλος & Μαυρίδης, 2002).

4.3.5 Η μέθοδος Keylloggers

Η μέθοδος των keyloggers αφορά επιβλαβή προγράμματα που εκτελούνται σχεδόν αόρατα, χωρίς να μπορεί να το αντιληφθεί το υποψήφιο θύμα και εν συνεχεία καταγράφει όλες τις πληροφορίες που εισάγει ο χρήστης και εν συνεχεία στέλνει πληροφορίες στον υποκλοπέα που έχει μολύνει το χρήστη με το keylogger.
Τα προγράμματα keyloggers είναι πολύ επικίνδυνα, καθώς είναι σε θέση να μπορούν να υποκλέπτουν τα προσωπικά στοιχεία του χρήστη, όπως είναι ο αριθμός της πιστωτικής κάρτας, και οι κωδικοί πρόσβασης. Μάλιστα ο χρήστης δεν μπορεί να αντιληφθεί ότι έχει μολυνθεί από keyloggers και οπότε μπορεί να χρησιμοποιήσει τον δικτυακό τόπο της ηλεκτρονικής τραπεζικής της τράπεζας του και να γνωστοποιήσει άθελά του τους προσωπικούς κωδικούς του (Πάγκαλος & Μαυρίδης, 2002).

4.3.6 Η μέθοδος Trojan Horse

Η μέθοδος Trojan Horses ή αλλιώς δούρειος ίππος, είναι πρόγραμμα με κρυφές λειτουργίες που δεν περιλαμβάνεται στην τεκμηρίωση που τα συνοδεύει. Στην πραγματικότητα ο δούρειος ίππος εκτελεί υποθετικά μια εργασία ενώ στην πραγματικότητα εκτελεί μια διαφορετική. Στην πραγματικότητα αυτή η διαφορετική λειτουργία είναι αυτή που εκτελεί συγκαλυμμένες ενέργειες, όπως για παράδειγμα η κλοπή κωδικών.

Η πλειονότητα των προγραμμάτων αυτών δεν επιτελούν τη λειτουργία την οποία ισχυρίζονται και όταν εκτελούνται καταστρέφουν τα διαθέσιμα αρχεία του συστήματος. Ωστόσο, υπάρχουν και προγράμματα, που ναι μεν επιτελούν συγκεκριμένες λειτουργίες αλλά την ίδια στιγμή λειτουργούν συγχρόνως επιτελούν και μια δεύτερη λειτουργία χωρίς να μπορούν να προκαλέσουν υποψίες στον εκάστοτε χρήστη. Οπότε δεν χρειάζεται να αναπαράγονται μόνοι τους, αλλά στην πραγματικότητα ο ίδιος ο χρήστης βοηθά τα προγράμματα αυτά να μολύνουν τα αρχεία και τους πόρους του συστήματος. Οπότε η καλύτερη μέθοδος για την

αντιμετώπιση των προγραμμάτων αυτών είναι η ενημέρωση των χρηστών (Πάγκαλος & Μαυρίδης, 2002).

4.4 Μέθοδοι προφύλαξης των ηλεκτρονικών συναλλαγών

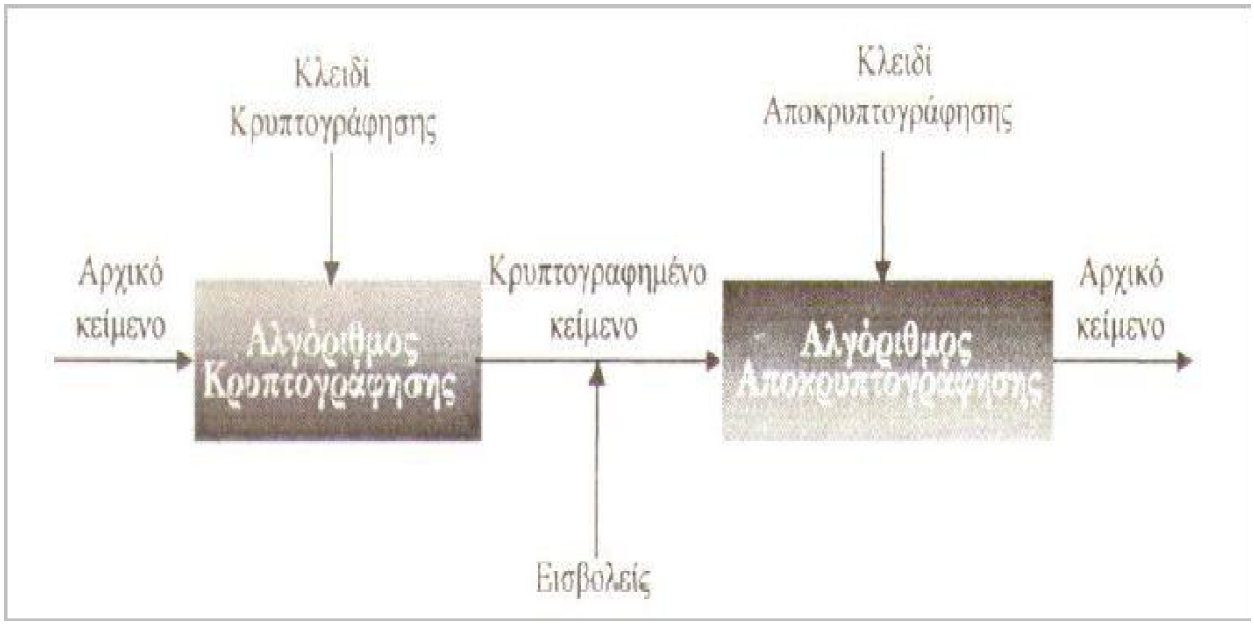
4.4.1 Η μέθοδος κρυπτογράφησης

Ένας από τους πιο σημαντικούς τρόπους αντιμετώπισης των κινδύνων που προέρχονται από κακόβουλα λογισμικά, είναι η μέθοδος της κρυπτογράφησης ή της κρυπτογραφίας που εφαρμόζεται σήμερα σε όλα τα πληροφοριακά συστήματα μεταξύ των οποίων και τα τραπεζικά.

Η έννοια της κρυπτογραφίας αποτελείται από τα συνθετικά των λέξεων «κρύπτος» και «γράφος», που περιλαμβάνουν τη μελέτη της μυστικογραφίας. Η μυστικογραφία είναι η μελέτη, ανάπτυξη και χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη των περιεχομένων των μηνυμάτων και την διευκόλυνση της ανίχνευσης κακόβουλων μετατροπών στα μηνύματα (Πάγκαλος & Μαυρίδης, 2002).

Η μέθοδος της κρυπτογράφησης είναι γνωστή από την αρχαιότητα. Στην σημερινή εποχή η διαδικασία της κρυπτογράφησης έχει γίνει πιο σύνθετη σαν διαδικασία και αποτελεί συνάμα μια ολόκληρη επιστήμη. Κατά βάση η μέθοδος της κρυπτογραφίας χρησιμοποιείται για την προστασία της ακεραιότητας των δεδομένων και για την προστασία συναλλαγών μέσω του διαδικτύου (Αλεξανδρής & Κιουντούζης, 1995).

Ο τρόπος λειτουργίας ενός συστήματος κρυπτογράφησης είναι ο εξής. Πιο ειδικά τα δεδομένα κρυπτογραφούνται και το παραγόμενο μήνυμα αποστέλλεται στον παραλήπτη και εν συνεχεία αποκρυπτογραφείται προκειμένου να αναπαραχθεί το αρχικό μήνυμα. Μάλιστα στο σχήμα 1, παρουσιάζουμε ένα τυπικό σύστημα κρυπτογράφησης, όπου φαίνεται και το σημείο όπου μπορεί να γίνει η παρέμβαση από τους εισβολείς (Σχήμα 1).



Σχήμα 1. Σύστημα μεθόδου κρυπτογράφησης (Πάγκαλος & Μαυρίδης, 2003)

Το μεγαλύτερο μέρος των επικοινωνιών στο διαδίκτυο στηρίζεται στην χρήση του πρωτοκόλλου επικοινωνίας TCP/IP (Transmission Control Protocol/ /internet Protocol), όπου μέσω αυτού επιτρέπεται η αποστολή πληροφοριών από το έναν υπολογιστή στον άλλο μέσω της χρήσης ενδιάμεσων υπολογιστών και του δικτύου. Οπότε οι λεγόμενοι εισβολείς μπορούν να παρεμβαίνουν στην επικοινωνία με διαφόρους τρόπους όπως είναι η υποκλοπή, η παραποίηση πληροφοριών και η παραπλάνηση. Για την αντιμετώπιση του παραπόνων προβλήματος είναι όπως καταλαβαίνει κανείς είναι η χρήση της κρυπτογραφίας που δίνει την δυνατότητα για την εφαρμογή των ακόλουθων βημάτων όπως είναι η κρυπτογράφηση και η αποκρυπτογράφηση, ο εντοπισμός πιθανών αλλοιώσεων, η αυθεντικοποίηση και εξακρίβωση του αποστολέα και η αδυναμία απάρνησης του αποστολέα.

Τέλος, έχει αναπτυχθεί η λεγόμενη τεχνολογία Υποδομής Δημοσίου Κλειδιών (ΥΔΚ) που βοηθά σε σημαντικό βαθμό στην αντιμετώπιση των παραπάνω θεμάτων ασφάλειας. Αναλυτικά, η υποδομή δημοσίου κλειδιού περιλαμβάνει τεχνολογίες όπως είναι η κρυπτογράφηση δημοσίου κλειδιού, τα ψηφιακά πιστοποιητικά και οι ψηφιακές υπογραφές. Επίσης, υπάρχουν ποικίλοι τύποι κρυπτογραφικών αλγορίθμων που ταξινομούνται με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων και τα

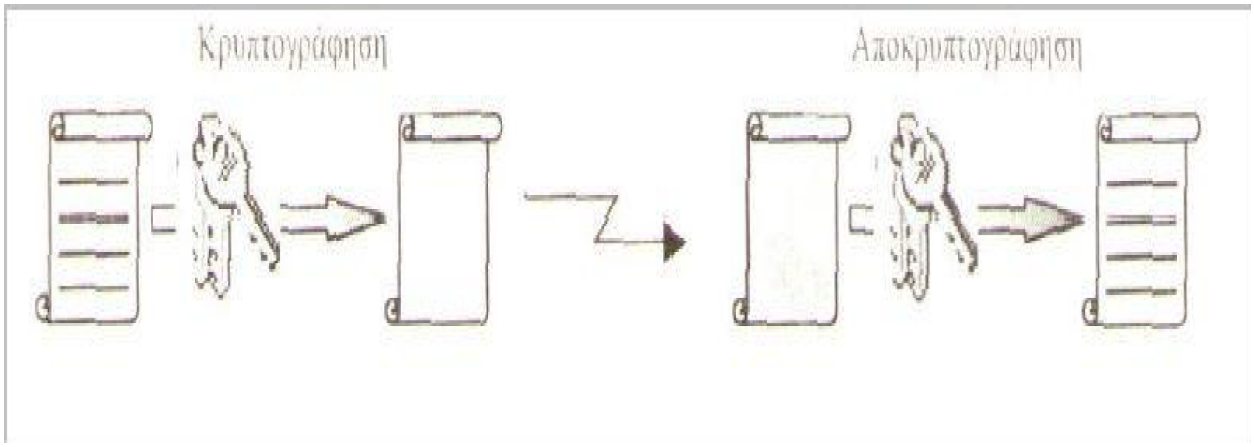
κλειδιά. Σε επόμενα εδάφια θα μιλήσουμε για τους αλγορίθμους με βάση τα κλειδιά που χωρίζονται στους κρυπτογραφικούς αλγόριθμους μυστικού ή συμμετρικού κλειδιού και στους κρυπτογραφικούς αλγόριθμους δημοσίου ή ασύμμετρου κλειδιού.

4.4.1.1 Η κρυπτογράφηση του μυστικού ή ασύμμετρου κλειδιού

Η μέθοδος της κρυπτόγραφησης του μυστικού ή συμμετρικού κλειδιού στηρίζεται την ύπαρξη και την παρουσία ενός μυστικού κλειδιού που είναι γνωστό μόνο μεταξύ των ατόμων που συναλλάσσονται. Μάλιστα το μυστικό αυτό κλειδί χρησιμοποιείται στην μέθοδο της κρυπτογράφησης και την μέθοδο της αποκρυπτογράφησης (Σχήμα 2).

Η συγκεκριμένη μέθοδος, δεν εγγυάται την έννοια της εμπιστευτικότητας διότι ναι μεν κρυπτογραφεί και αποκρυπτογραφεί το μήνυμα με την χρήση του μυστικού κλειδιού αλλά δεν μπορεί να εξασφαλίσει την εμπιστευτικότητα, διότι δεν μπορεί να εγγυηθεί τον τρόπο που θα πραγματοποιηθεί η ανταλλαγή του κλειδιού. Για να εξασφαλιστεί η ασφάλεια της επικοινωνίας θα πρέπει να γίνει αποστολή και ανταλλαγή του μυστικού κλειδιού μέσω ενός ασφαλούς κλειδιού. Επιπρόσθετα ένα ακόμη πρόβλημα που έχει να αντιμετωπίσει η μέθοδος αυτή είναι η εξασφάλιση της ταυτοποίησης, διότι πολλοί άνθρωποι μπορεί να διαθέτουν ένα κοινό κλειδί αλλά να μην μπορούν να διασταυρώσουν ποιος τελικά το έχει στείλει (Πάγκαλος & Μαυρίδης, 2002).

Τέλος το πιο μεγάλο πλεονέκτημα που παρουσιάζει η μέθοδος της κρυπτογράφησης είναι η ταχύτητα διεκπεραίωσης των διαδικασιών της κρυπτογράφησης και της αποκρυπτογράφησης. Όσον αφορά το θέμα της ασφάλειας της συμμετρικής κρυπτογράφησης εξαρτάται από τη όσο δυνατή διαφύλαξη του μυστικού κλειδιού κρυπτογράφησης/ αποκρυπτογράφησης.



Σχήμα 2. Τρόπος κρυπτογράφησης και αποκρυπτογράφησης του κλειδιού (Πάγκαλος & Μαυρίδης, 2002)

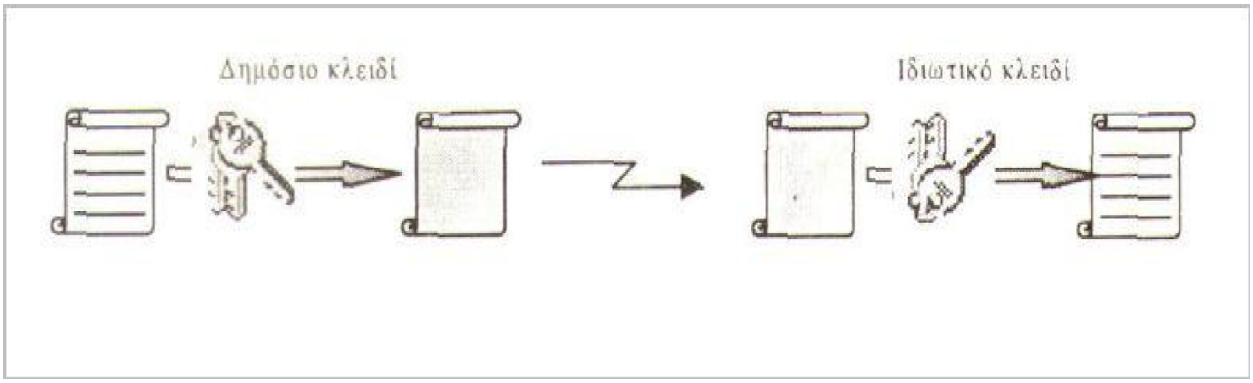
4.4.1.2 Η κρυπτογράφηση του δημόσιου ή συμμετρικού κλειδιού

Η μέθοδος της κρυπτογραφίας δημοσίου κλειδιού χρησιμοποιήθηκε για πρώτη φορά στις αρχές της δεκαετίας του 1970 από τους Diffie & Hellman και βασίζεται στην λογική ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται από κοινού το ίδιο μυστικό κλειδί. Αντίθετα, έχουν στην διάθεση τους διαφορετικά κλειδιά για διαφορετικές λειτουργίες που τυχόν θέλουν να πραγματοποιήσουν.

Η κρυπτογραφία του δημοσίου ή ασύμμετρου κλειδιού εφευρέθηκε προκειμένου να συμβάλει στην αντιμετώπιση προβλημάτων που προέκυπταν από τη συμμετρική κρυπτογράφηση, όπως η διασφάλιση της εγγύησης της ταυτότητας του αποστολέα καθώς και την δυσκολία διανομής του μυστικού κλειδιού σε αποστολέα και παραλήπτη.

Με λίγα λόγια η μέθοδος αυτή έχεις σαν βάση τη χρήση δύο κλειδιών, όπου το ένα αποτελεί το δημόσιο κλειδί και το δεύτερο αποτελεί το προσωπικό κλειδί (Σχήμα 3) Δηλαδή το δημόσιο κλειδί χρησιμοποιείται από τον εκάστοτε παραλήπτη για την κρυπτογράφηση των δεδομένων και εν συνεχεία όταν παραληφθούν από τον

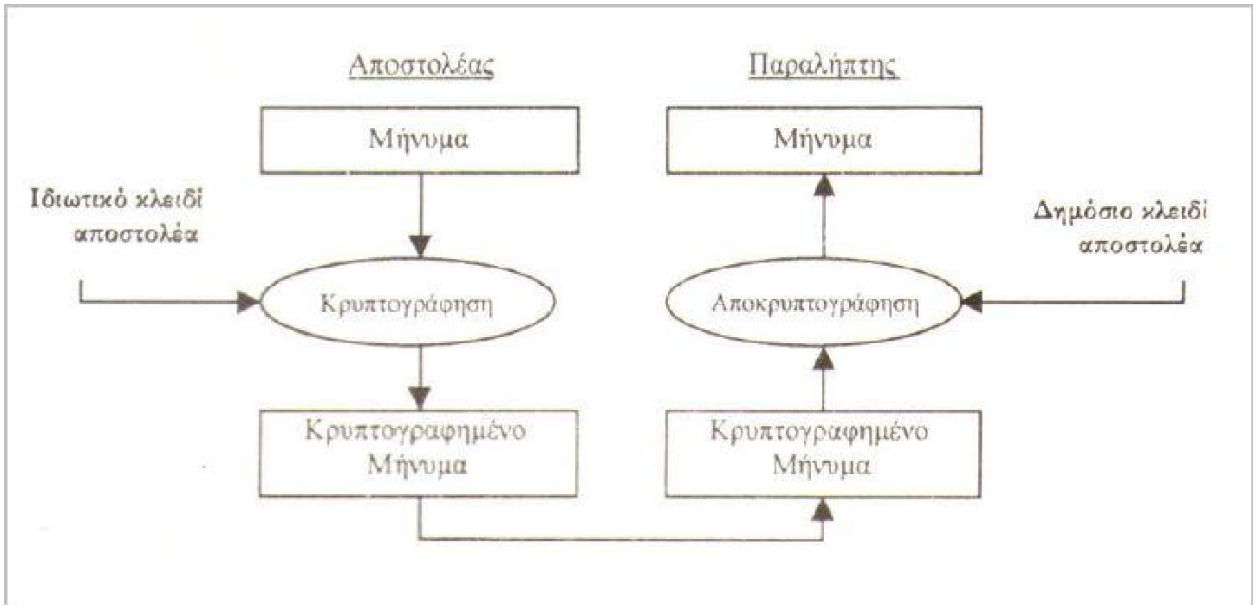
παραλήπτη γίνεται χρήση του προσωπικού κλειδιού ώστε να γίνει η αποκρυπτογράφηση (Πάγκαλος & Μαυρίδης, 2002).



Σχήμα 3. Η μέθοδος κρυπτογράφησης του δημόσιου και του ιδιωτικού κλειδιού (Πάγκαλος & Μαυρίδης, 2002)

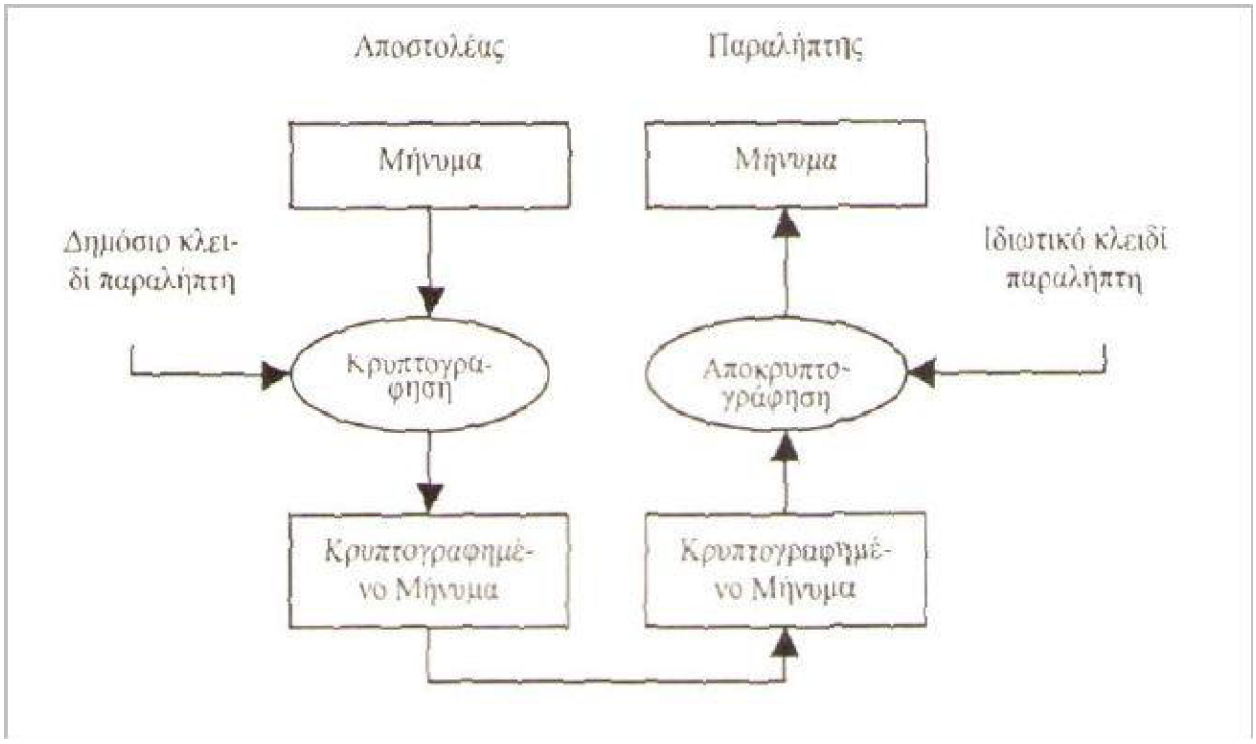
Το δημόσιο και το προσωπικό κλειδί παρουσιάζουν μια ιδιαίτερη σχέση μεταξύ τους. Πιο ειδικά, στην περίπτωση που το δημόσιο κλειδί χρησιμοποιηθεί στην προσπάθεια κρυπτογράφησης της πληροφορίας τότε το προσωπικό κλειδί θα χρησιμοποιηθεί για την διαδικασία της αποκρυπτογράφησης και αντίστροφα. Μάλιστα η γνώση του δημοσίου κλειδιού κρυπτογράφησης δεν δίνει την δυνατότητα σε καμιά περίπτωση για την ανακάλυψη του ιδιωτικού κλειδιού αποκρυπτογράφησης. Από την γνώση του αλγορίθμου που δίνει σαν αποτέλεσμα το κλειδί της αποκρυπτογράφησης είναι πολύ δύσκολο από άποψη καθαρά υπολογιστική να βρει το κλειδί αυτό.

Όσον αφορά την διαδικασία της κρυπτογράφησης μπορεί να γίνει με την χρήση των κλειδιών μπορεί να γίνει με τρεις διαφορετικούς τρόπους. Ο πρώτος τρόπος έχει το πλεονέκτημα ότι μπορεί να εξασφαλίζει την ταυτότητα του αποστολέα, καθώς για την κρυπτογράφηση ο αποστολέας μπορεί να χρησιμοποιεί το ιδιωτικό του κλειδί. Οπότε η αποκρυπτογράφηση πραγματοποιείται με το δημόσιο κλειδί του αποστολέα, με αποτέλεσμα ο εκάστοτε παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα. Ωστόσο σε αυτή την αποστολή δεν μπορεί να εξασφαλίζεται η έννοια της εμπιστευτικότητας διότι το δημόσιο κλειδί του αποστολέα είναι γνωστό (Σχήμα 4).



Σχήμα 4. Ο πρώτος τρόπος της κρυπτογράφησης (Πάγκαλος & Μαυρίδης, 2002)

Στην περίπτωση του δεύτερου τρόπου, ο αποστολέας χρησιμοποιεί το ιδιωτικό κλειδί για την διαδικασία της αποκρυπτογράφησης του μηνύματος και ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί για την διαδικασία της αποκρυπτογράφησης του. Με αυτό τον τρόπο διασφαλίζεται η εμπιστευτικότητα κατά την διαδικασία αποστολής του μηνύματος καθώς ο παραλήπτης ναι μεν μπορεί μέσω της αποκρυπτογράφησης να διαβάσει το μήνυμα με την χρήση του ιδιωτικού κλειδιού αλλά δεν μπορεί σε καμιά περίπτωση να εξασφαλιστεί και να εξακριβωθεί η ταυτότητα του αποστολέα (Πάγκαλος & Μαυρίδης, 2002). (Σχήμα 5)



Σχήμα 5. Ο δεύτερος τρόπος της κρυπτογράφηση (Πάγκαλος & Μαυρίδής)

Όσον αφορά το τρίτο τρόπο, αυτός είναι ένας συνδυασμός των δύο προαναφερθέντων τρόπων και τελικά εξασφαλίζει και την εμπιστευτικότητα αλλά και την ταυτότητα του αποστολέα στην επικοινωνία. Επίσης, σε αυτή την περίπτωση ο αποστολέας κρυπτογραφεί τα δεδομένα με το ιδιωτικό του κλειδί και στη συνέχεια ο παραλήπτης τα αποκρυπτογραφεί με το δημόσιο κλειδί. Οπότε λαμβάνοντας το μήνυμα ο παραλήπτης, είναι σε θέση να αποκρυπτογραφήσει με την χρήση του ιδιωτικού κλειδιού και οπότε με αυτό τον τρόπο εξασφαλίζεται η εμπιστευτικότητα και έπειτα αποκρυπτογραφεί κάνοντας χρήση του δημόσιου κλειδιού του αποστολέα, όπου καταφέρνει και τον ταυτοποιεί.

Τέλος, το πρώτο σύστημα δημοσίου κλειδιού αναπτύχθηκε από τους Rivest, Shamir και Adleman στα τέλη της δεκαετίας του ’70 και έχει το όνομα RSA, από τα αρχικά των κατασκευαστών του. Μάλιστα η ασφάλειά του στηρίζεται στη δυσκολία εύρεσης των κοινών παραγόντων πολύ μεγάλων αριθμών. Το πλεονέκτημα του δημοσίου κλειδιού είναι ότι κατά την διαδικασία της κρυπτογράφησης, το δημόσιο κλειδί μπορεί να διανεμηθεί δωρεάν, πράγμα που διευκολύνει σημαντικά την επικοινωνία

των απομακρυσμένων χρηστών. Η δε συμμετρική διαδικασία της κρυπτογράφησης είναι πιο γρήγορη σε σχέση με τη ασύμμετρη γιατί απαιτεί πολύ λιγότερους υπολογισμούς.

4.4.2 Οι ψηφιακές υπογραφές

Αναφέραμε σε προηγούμενο εδάφιο ότι, στις περιπτώσεις που απαιτείται μόνο η αυθεντικοποίηση του αποστολέα με την διαδικασία της κρυπτογράφησης του ασύμμετρου κλειδιού, τότε το μήνυμα δεν έχει παρά να κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα και να αποκρυπτογραφηθεί με το δημόσιο κλειδί του αποστολέα από τον παραλήπτη. Οπότε όλο το κρυπτογραφημένο μήνυμα που αποστέλλεται αποτελεί μια ψηφιακή υπογραφή του αποστολέα. Έτσι κατά αυτόν τον τρόπο εξασφαλίζονται δυο πράγματα: η αυθεντικότητα του αποστολέα και η ακεραιότητα του μηνύματος, διότι ο αποστολέας χωρίς την χρήση του ιδιωτικού κλειδιού δεν μπορεί σε καμιά περίπτωση να λάβει χώρα οποιαδήποτε παραποίηση του μηνύματος (Κατσίκας & Γκριτζάλη, 2003).

Επιπλέον, ένα πρόβλημα που προκύπτει σε αυτή την περίπτωση είναι οι απαιτήσεις σε χώρο αποθήκευση, καθώς κάθε μήνυμα θα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή και θα πρέπει να φυλάσσεται και ένα αντίγραφο ασφαλείας αυτού σε κρυπτογραφημένη μορφή, προκειμένου τα περιεχόμενά του να μπορούν να εντοπιστούν και να αναλυθούν εύκολα. Μάλιστα για την επίλυση του παραπάνω προβλήματος, κρυπτογραφείται ένα μικρό τμήμα από bits, που αποτελεί συνήθως μέρος του κειμένου και ονομάζεται αυθεντικοποιητής. Στη περίπτωση που ο αυθεντικοποιητής κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα, τότε μπορεί να χαρακτηριστεί ως ψηφιακή υπογραφή. Για την δημιουργία της ψηφιακής υπογραφής ενός μηνύματος, γίνεται κρυπτόγραφηση με το ιδιωτικό κλειδί του αποστολέα (Κατσίκας & Γκριτζάλη, 2003).

Τέλος, αξίζει να επισημάνουμε ότι η ψηφιακή υπογραφή δεν προσφέρει εμπιστευτικότητα στο μήνυμα αλλά διασφαλίζει την ακεραιότητα του μηνύματος και την αυθεντικοποίηση του αποστολέα.

4.4.3 Τα ψηφιακά πιστοποιητικά

Είναι κατανοητό ότι τα δημόσια κλειδιά της ασύμμετρης κρυπτογραφίας προκειμένου να είναι αποτελεσματικά θα πρέπει να είναι γνωστά σε όσους ενδιαφέρονται. Οπότε για την αντιστοίχιση και την δέσμευση ενός δημοσίου κλειδιού σε ένα άτομο ή έναν οργανισμό ή είναι απαραίτητη η διαδικασία της πιστοποίησης. Οπότε για την αντιμετώπιση του προβλήματος αυτού γίνεται χρήση των ψηφιακών πιστοποιητικών, που αποτελούν τρόπο μετάδοσης με ασφαλή τρόπο των τιμών των δημοσίων κλειδιών και των πληροφοριών του κατόχου που σχετίζονται με αυτά. Η διαδικασία της πιστοποίηση αποτελεί βασικό πυλώνα λειτουργίας όλων των Υποδομών Δημοσίου Κλειδιού (ΥΔΚ) (Κατσίκας & Γκριτζάλη, 2003).

Για να αποκτήσει κανείς το ψηφιακό πιστοποιητικό θα πρέπει να κάνει αίτηση στην Αρχή Πιστοποίησης (ΑΠ), που μπορεί να επιβεβαιώσει την ταυτότητα του αιτούντος και να εκδώσει το πιστοποιητικό. Το πιστοποιητικό περιλαμβάνει τα ακόλουθα στοιχεία, Αυτά είναι το όνομα και οι πληροφορίες αναγνώρισης του εκάστοτε χρήστη που αναφέρεται το πιστοποιητικό, το δημόσιο κλειδί του εκάστοτε χρήστη, την ημερομηνία λήξης του πιστοποιητικού και το όνομα και την υπογραφή του πιστοποιητικού.

Τέλος, αξίζει να τονίσουμε ότι τα πιστοποιητικά χαρακτηρίζονται και από το είδος της πληροφορίας που περιλαμβάνουν. Οπότε υπάρχουν πιστοποιητικά ταυτότητα, που ταυτοποιούν ένα άτομο ή ένα οργανισμό και πιστοποιητικά χαρακτηριστικών, που περιγράφουν τις ιδιότητες του ατόμου ή του οργανισμού.

4.4.4 Το πρωτόκολλο Secure Socket Layer

Το πρωτόκολλο Secure Socket Layer (SSL), είναι υπεύθυνο για τη μεταφορά δεδομένων μεταξύ δύο συσκευών. Ο σκοπός που δημιουργήθηκε ήταν η παροχή και η διασφάλιση της ιδιωτικότητας και της ακεραιότητας των δεδομένων που μεταφέρονται μέσω του διαδικτύου. Ακόμα το συγκεκριμένο πρωτόκολλο διαχειρίζεται την εμπιστευτικότητα, την ακεραιότητα του καναλιού μετάδοσης, την αυθεντικοποίηση του εξυπηρετητή και του πελάτη όταν και όπου είναι απαραίτητο.
Ο σχεδιασμός του πρωτοκόλλου SSL προήλθε από την εταιρεία NETSCAPE, με στόχο την παροχή ασφάλειας κατά τη μετάδοση δεδομένων με βάση το πρωτόκολλο TCP/IP. Επίσης παρέχει υπηρεσίες όπως είναι η κρυπτογράφηση δεδομένων, η αυθεντικοποίηση εξυπηρετητή και η ακεραιότητα των μηνυμάτων που μεταδίδονται στο διαδίκτυο. Ένα άλλο πρωτόκολλο που σχεδιάστηκε για την μετάδοση των δεδομένων στο διαδίκτυο είναι το Secure HTTP (S-HTTP), που έχει σχεδιαστεί για τη μυστική μετάδοση δεδομένων-μηνυμάτων. Τα προαναφερθέντα πρωτόκολλα είναι συμπληρωματικά (Πάγκαλος & Μαυρίδης, 2002).

Το πρωτόκολλο SSL είναι κατά τέτοιο τρόπο σχεδιασμένο ώστε να μπορεί να εξασφαλίσει τη ασφαλή μετάδοση, κάνοντας χρήση της κρυπτογράφησης RSA δημόσιου κλειδιού. Πιο ειδικά όταν ο φυλλομετρητής συνδεθεί με μια SSL προστατευμένη σελίδα, ο SSL εξυπηρετητής στέλνει μια αίτηση για την έναρξη μιας SSL συνόδου. Στην περίπτωση που το ίδιο το πρωτόκολλο υποστηρίζει, είναι σε θέση να ενημερώσει τον εξυπηρετητή για τους αλγορίθμους κρυπτογράφησης, τις μεθόδους συμπίεσης που υποστηρίζει και την ταυτότητα της συνόδου. Οπότε ο εξυπηρετητής κάνει τις αντίστοιχες επιλογές και ξεκινά η επικοινωνία. Πριν ξεκινήσει η επικοινωνία πραγματοποιείται ανταλλαγή ψηφιακών πιστοποιητικών. Στη συνέχεια ο πελάτης καθορίζει ένα κλειδί συνόδου, που είναι κατάλληλο για τον αλγόριθμο κρυπτογράφησης που επιλέχθηκε. Τελικά, ο εκάστοτε πελάτης με το δημόσιο κλειδί του εξυπηρετητή, μπορεί να κρυπτογραφήσει το κλειδί συνόδου και ο εξυπηρετητής

με το ιδιωτικό του κλειδί να αποκρυπτογραφήσει και να αποκτήσει το κλειδί συνόδου (Πάγκαλος & Μαυρίδης, 2002).

4.4.5 Τείχος προστασίας

Το τείχος προστασίας μπορεί να οριστεί ως το λογισμικό και ο εξοπλισμός που τοποθετείται μεταξύ του διαδικτύου και του υπό προστασία δικτύου. Πιο ειδικά, το λογισμικό αυτό δίνει την δυνατότητα για προσπέλαση των δεδομένων των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά, όπως είναι ονόματα χρηστών και συνθηματικά και διευθύνσεις IP (Πάγκαλος & Μαυρίδης, 2002).
Η εγκατάσταση του τείχους προστασίας γίνεται κατά βάση για να προστατευτούν τα δίκτυα από εξωτερικούς εισβολείς (hackers) που προσπαθούν να μπουν στα δεδομένα ενός τοπικού δικτύου. Με λίγα λόγια τα firewalls προστατεύουν τους χρήστες από απειλές όπως είναι η άρνηση εξυπηρέτησης και η προσποίηση.

Τα δίκτυα που έχουν τείχος προστασίας παρουσιάζουν πολλά πλεονεκτήματα. Πιο αναλυτικά δίνουν την δυνατότητα για αποτελεσματική επιβολή ασφάλειας ανάλογα τις ανάγκες του χρήστη. Μπορεί καθένας να ορίσει τον αριθμό των χρηστών και το ποιος θα έχει πρόσβαση σε ποιο πόρο. Παρέχουν ικανή προστασία από ευπαθείς υπηρεσίες δικτύων διότι είναι γνωστό ότι η πλειονότητα των πρωτοκόλλων παρουσιάζουν μεγάλα κενά ασφαλείας. Είναι ένας τρόπος καταγραφής της χρήσης και συνάμα συναγερμού για παράνομη χρήση του δικτύου.

Ωστόσο από τα αρκετά πλεονεκτήματα, τα τείχη προστασίας παρουσιάζουν και ορισμένα μειονεκτήματα. Αρχικά δεν προστατεύουν το σύστημα από εσωτερικούς χρήστες. Ακόμα μπορούν να προστατεύουν ένα περιβάλλον, μόνο όταν υπάρχει πλήρης έλεγχος, οπότε δεν θα πρέπει να υπάρχουν συνδέσεις που να μην διοχετεύονται μέσω firewall. Επιπλέον, είναι ορατός και συνάμα ελκυστικός στόχος επίθεσης διότι αποτελεί το πιο ορατό σημείο του δικτύου. Τα τείχη προστασίας

χρειάζονται διαρκώς ενημερώσεις και κατάλληλες ρυθμίσεις διότι διαφορετικά παρουσιάζουν πολλά κενά ασφαλείας (Πάγκαλος & Μαυρίδης, 2002).

ΚΕΦΑΛΑΙΟ 5: ΗΛΕΚΤΡΟΝΙΚΑ ΤΟΥΡΙΣΤΙΚΑ ΠΡΟΙΟΝΤΑ

5.1 Marketing και διαδίκτυο

Το διαδίκτυο έχει συμβάλλει μοναδικά στον τομέα του marketing παρέχοντας οφέλη ιδιαίτερης σημασίας με τη διανομή των παρεχόμενων πληροφοριών σε παγκόσμιο επίπεδο σε συνδυασμό με το κατά πολύ μειωμένο κόστος. Το μεγαλύτερο ανταγωνιστικό του πλεονέκτημα, σε σύγκριση με άλλα μέσα διάδοσης πληροφοριών, είναι η αμεσότητα η οποία το χαρακτηρίζει, γεγονός που βοηθά τον καταναλωτή να έχει πρόσβαση ανά πάσα στιγμή στην πληροφορία που εκείνος έχει ανάγκη.

Η προώθηση των διάφορων προϊόντων, μέσω διαδικτύου συνδυάζει τη δημιουργική και την τεχνική άποψη, συμπεριλαμβάνοντας το σχέδιο, την κατασκευή, τη διαφήμιση και τις πωλήσεις. Οι μέθοδοι του μάρκετινγκ μέσω ίντερνετ απαρτίζονται από τη βελτίωση της κατάταξης σε διάφορες μηχανές αναζήτησης, την αποστολή newsletter και την παρουσίαση διαφημιστικών γραφικών.

Το μάρκετινγκ μέσω ίντερνετ είναι η διαδικασία ανάπτυξης και προώθησης μιας επιχείρησης χρησιμοποιώντας ηλεκτρονικά μέσα. Το μάρκετινγκ μέσω διαδικτύου δεν αναφέρεται μόνο στη δημιουργία ή την ύπαρξη μιας ιστοσελίδας. Είναι απαραίτητο οι χρήστες του ίντερνετ, αλλά και η αγορά γενικότερα, να γνωρίζουν την ύπαρξη αυτής της ιστοσελίδας ώστε να αντιλαμβάνονται την ύπαρξη της επιχείρησης στην οποία ανήκει η ιστοσελίδα και κατ’ επέκταση να συμβάλλουν στην επιτυχία των στόχων της επιχείρησης. Αυτό επιτυγχάνεται μέσω της διαφήμισης.

Το Μάρκετινγκ στο Διαδίκτυο είναι ένα παλιό παιχνίδι με νέους κανόνες. Είναι ένας κόσμος των συμμαχιών, της διαφήμισης σε banner, e-mail marketing, τις τεχνικές και μηχανή αναζήτησης. Αν κάποιος είναι σε απευθείας σύνδεση έμπορος οποιουδήποτε κλάδου, μπορεί να καταλάβει και να ενσωματώσει τις νέες τακτικές, όπως μπορεί να αναπτύξει μια στρατηγική μάρκετινγκ για να προσεγγίσει το κοινό-στόχο. Διαφορετικά, το site του θα αγωνιστεί στον κυβερνοχώρο (Σ. Καλαιτζής, 1998).

Πλέον όλο και περισσότεροι καταναλωτές ψωνίζουν on-line και δεν είναι λίγοι εκείνοι που χρησιμοποιούν το Διαδίκτυο για να ερευνήσουν τις μελλοντικές αγορές. Ωστόσο, το μάρκετινγκ δεν σημαίνει απαραιτήτως πώληση. Το Διαδίκτυο μπορεί να μην είναι το καλύτερο μέσο για τη διενέργεια των πωλήσεων. Για παράδειγμα, η λήψη παραγγελιών σε απευθείας σύνδεση δεν είναι μια καλή μέθοδος για να πωλούνται τα προϊόντα καθώς διαφημίζονται ως «υπέρ το άρτιο» νέα εναλλακτική πρόταση στα άλλα προϊόντα." Όπως και κάθε άλλη αγορά, η πώληση μέσω Διαδικτύου εξαρτάται από τη γνωριμία με τους πελάτες. Οι παραγωγοί θα πρέπει να θέσουν κάποια βασικά ερωτήματα για τους πελάτες τα οποία απαντώνται από τους ίδιους. Για παράδειγμα: Ποιοι είναι αυτοί; Έχουν Πρόσβαση στο Διαδίκτυο; Χρησιμοποιούν e-mail; Μια σαφή ιδέα για το ποιοι είναι οι πελάτες και πώς χρησιμοποιούν το Διαδίκτυο θα τους επιτρέψει να αναπτύξουν μια ιστοσελίδα που ανταποκρίνεται στις ανάγκες των πελατών (Turban et al., 2006).

Στον τουριστικό κλάδο (ο οποίος και εξετάζεται στο παρών κεφάλαιο) ανθεί ιδιαίτερα, τα τελευταία χρόνια, το marketing μέσω διαδικτύου διότι αποτελεί ένα σημαντικό μέσο το οποίο εκμεταλλεύονται οι επιχειρήσεις μέσα από ποικίλες στρατηγικές, έτσι ώστε να δημοσιοποιήσουν τις υπηρεσίες τους ο ιστό με σκοπό την μεγιστοποίηση των κερδών τους (Κοκκώσης & Τσάρτας, 2001).

5.2 Η ηλεκτρονική διαφήμιση στον τουριστικό κλάδο

Η εξέλιξη της τεχνολογίας σε συνδυασμό με τις σύγχρονες κοινωνίες αλλά και τις ανάγκες των πολιτών, που συνεχώς αλλάζουν και εξελίσσονται με ιδιαίτερα γρήγορους ρυθμούς, έφερε την εξ ολοκλήρου αλλαγή στα παραδοσιακά μέσα διαφήμισης με μετεξέλιξης αυτών σε ηλεκτρονική διαφήμιση. Με τον όρο ηλεκτρονική διαφήμιση στον τουριστικό κλάδο, ορίζεται η προώθηση/γνωστοποίηση των τουριστικών προϊόντων μίας επιχείρησης, που εντάσσετε στον τουριστικό κλάδο, σε καταναλωτικό κοινό παγκόσμιας εμβέλειας, με σκοπό να στοχεύσει στα

κατάλληλα target group έτσι ώστε να μεγιστοποιήσει τα κέρδη της (Sigalas et al., 2007).

Για την επίτευξη, λοιπόν, της άρτιας ηλεκτρονικής διαφήμισης, που σκοπό όπως αναφέραμε, έχει την προώθηση/γνωστοποίηση των τουριστικών προϊόντων της επιχείρησης, μέσω στρατηγικών, οι συνήθης μέθοδοι/εργαλεία που χρησιμοποιούν οι τουριστικές επιχειρήσεις, αναφέρονται παρακάτω (Buhalis, 2003):

- ✓ Δημιουργία Web-Site: Αποτελεί μία ευρέως γνωστή στρατηγική e- marketing στον τουριστικό κλάδο. Ουσιαστικά, είναι η επίσημη ιστοσελίδα της επιχείρησης μέσω της οποίας γίνεται γνωστή παρέχοντας την δυνατότητα στους πελάτες της, να τη γνωρίσουν, να μάθουν για την ιστορία της, τα τουριστικά προϊόντα που διαθέτει αλλά και τις παρεχόμενες υπηρεσίες. Μέσω της επίσης ιστοσελίδας μπορεί να πραγματοποιηθεί άμεση πώληση των τουριστικών προϊόντων αλλά και έμμεση πώληση. Η ιστοσελίδα αυτή παρέχει όλες τις χρήσιμες πληροφορίες για τον καταναλωτή ώστε ο ίδιος να μπορέσει να επικοινωνήσει με εκπρόσωπο της επιχείρησης για επιπλέον πληροφορίες ή τυχόν απορίες που μπορούν να παρουσιαστούν.

- ✓ Search engine marketing: Το συγκεκριμένο εργαλείο έχει άμεση σχέση με την δημοσιοποίηση του ονόματος της επιχείρησης και της φήμης αυτής, καθώς συνδέεται με την αναζήτηση, μέσω συγκεκριμένων λέξεων – κλειδιών, της επιχείρησης στους διάφορους μηχανισμούς αναζήτησης του διαδικτύου. Το εργαλείο αυτό χρησιμοποιείται με απώτερο σκοπό οι επιχειρήσεις στον τομέα του τουρισμού να αυξήσουν τα ποσοστά επισκεψιμότητας των καταναλωτών στο επίσημο site τους.

- ✓ Pay per click: Ιδιαίτερο είδος ηλεκτρονικής διαφήμισης που έχει κάνει την εμφάνιση του στην αγορά τα τελευταία χρόνια. Η μέθοδος που ακολουθούν είναι ανάλογη του ονόματός της διότι το αντίτιμο για την διαφήμιση αυτή καταβάλλεται μόνο όταν ο καταναλωτής επιλέξει να «κλικάρει» πάνω στην συγκεκριμένη διαφήμιση. Συνδέεται με τις μηχανές αναζήτησης οι οποίες οδηγούν σε διάφορα αποτελέσματα. Αυτού του είδος η διαφήμιση, συνήθως,

εμφανίζεται στο πλάι της οθόνης αποτελεσμάτων των μηχανών αναζήτησης. Χρησιμοποιείται για την δημοσιοποίησης τουριστικών προορισμών.

- ✓ Banner marketing: Σύμφωνα με τη συγκεκριμένη μέθοδο, οι επιχειρήσεις τουριστικού ενδιαφέροντος, αποφασίζουν να διαφημίσουν τα προϊόντα τους, μέσω γνωστών σελίδων του διαδικτύου που ασχολούνται με τον κλάδο.

- ✓ Blog Marketing: Το συγκεκριμένο εργαλείο προωθεί την επικοινωνία μεταξύ της επιχείρησης και του καταναλωτικού κοινού λόγω της αλληλεπίδρασης αυτών των δύο μερών. Η επιχείρηση μέσω του site της παρέχει ένα πεδίο στο οποίο δημοσιεύει έρευνες και τρέχοντα ζητήματα σχετικά με τον κλάδο που ακολουθεί ενώ ταυτόχρονα αφήνει την ελευθερία σχολιασμού στον οποιοδήποτε επισκέπτη της σελίδας. Με αυτόν τον τρόπο η επιχείρηση είναι σε θέση να αφουγκραστεί τις ανάγκες και τις γνώμες του καταναλωτικού κοινού που την αφορά.

- ✓ E-zines: Αποτελεί μία οργανωμένη μορφή ηλεκτρονικών περιοδικών σχετικά με θέματα τουρισμού και θεμάτων που ενδιαφέρουν το καταναλωτικό κοινό στον τουριστικό τομέα.

- ✓ Συστήματα διαχείρισης πελατειακών σχέσεων: Βοηθούν με καταλυτικό τρόπο στην οριοθέτηση και τη συστηματική διαχείριση του υπάρχοντος πελατολογίου με τέτοιο τρόπο ώστε να βοηθούν στην μεγιστοποίηση της αξίας του πελάτη για την επιχείρηση. Τα συστήματα αυτά περιλαμβάνουν συγκεκριμένες διαδικασίες οι οποίες αφορούν την πώληση και την σωστή εξυπηρέτηση των πελατών της επιχείρησης.

- ✓ Sponsorships: Η μέθοδος αυτή αποτελεί την εξέλιξη των παραδοσιακών μεθόδων της χορηγίας, στο διαδίκτυο. Οι επιχειρήσεις τουριστικού ενδιαφέροντος που υιοθετούν την συγκεκριμένη μέθοδο παρέχουν δωρεάν τα προϊόντα τους ή τις υπηρεσίες του σε συγκεκριμένα μέσα (ηλεκτρονικά περιοδικά, ηλεκτρονικές επιχειρήσεις, πλατφόρμες κ.α) με αντάλλαγμα της προβολή της επιχείρησης του σε αυτά τα μέσα. Με αυτόν τον τρόπο η

τουριστική επιχείρηση επιχειρεί αύξηση της προβολής της με ιδιαίτερα χαμηλό κόστος γι αυτή.

- ✓ Viral Marketing: Αποτελεί την μετάδοση συγκεκριμένου μηνύματος της επιχείρησης προς το target group που αυτή στοχεύει.
- ✓ E-mail Marketing: Η μέθοδος αυτή βασίζεται στην γνωστοποίηση συγκεκριμένων πληροφοριών (π.χ προσφορών) μέσω της αποστολής αυτών σε μία μεγάλη λίστα email. Η στρατηγική αυτή, απευθύνεται κυρίως, στο υπάρχον πελατολόγιο της επιχείρησης και αποσκοπεί στην γνωστοποίηση αυτών των πληροφοριών και σε νέους πελάτες μέσω των ήδη υπαρχόντων.

Η ηλεκτρονική διαφήμιση αποτελεί αναπόσπαστο μέρος της σύγχρονης επιχείρησης και ανθεί ιδιαίτερα τα τελευταία χρόνια στον τουριστικό κλάδο ο οποίος χαρακτηρίζεται υψηλού ενδιαφέροντος για την οικονομίας μίας οποιασδήποτε χώρας.

5.3 Τα Social Media στον τομέα του τουρισμού

Τα τελευταία χρόνια τα social media έχουν εδραιωθεί στις ζωές των σύγχρονων ανθρώπων και αποτελούν αναπόσπαστο κομμάτι των καθημερινών συνηθειών τους, ειδικότερα, από τότε που εξελίχθηκε το γνωστό σε όλους Internet. Η εξέλιξη αυτών εντοπίζεται στο γεγονός της ανάγκης των ανθρώπων για αλληλεπίδραση και επικοινωνία (Βλαχόπουλος, 2003).

Οι επιχειρήσεις στον τουριστικό κλάδο ήταν από τις πρώτες μορφές επιχειρήσεων, οι οποίες άρχισαν να εκμεταλλεύονται την ανάπτυξη των social media για επιχειρηματικούς σκοπούς, κυρίως, προώθησης και προβολής των

προϊόντων/υπηρεσιών τους. Τα social media μπορούν να προσδώσουν σε μία επιχείρηση τα παρακάτω χαρακτηριστικά (Βλαχόπουλος, 2003):

- ➢ Επιπλέον διαφήμιση.
- ➢ Αυξημένη ποσοστά φήμης.
- ➢ Ισχυροποίηση του brand name της επιχείρησης.

Τα πιο γνωστά social media που βοηθούν τις επιχειρήσεις στον τομέα του τουρισμού είναι το Facebook, Το Youtube, το Flictr, το Twitter, το Linkens in, το Pinterest, το Google plus, το Booking, το Trip Advisor, airbnb και το Trivago. Παρακάτω αναλύονται αυτά τα social media και η συμβολή τους στις επιχειρήσεις του κλάδου:

- ✓ Facebook: Το δεύτερο δημοφιλέστερο κατά σειρά κατάταξης social media. Εφευρέθηκε, αρχικά, το 2004 από μία μικρή ομάδα του πανεπιστημίου Harvard και εν συνεχεία το 2006 έγινε ευρέως γνωστό σε παγκόσμιο επίπεδο δίνοντας στους χρήστες του τη δυνατότητα να επικοινωνούν μέσω μηνυμάτων, να ανεβάζουν φωτογραφικό υλικό, να ενημερώνουν για τα προσωπικά ή επαγγελματικά επιτεύγματα και να δημιουργούν σταδιακά το προφίλ που αυτοί επιθυμούν. Όσο αναφορά τις επιχειρήσεις που ασχολούνται με τον τουριστικό κλάδο, μέσω του Facebook, έχουν την δυνατότητα να ισχυροποιήσουν την εταιρική εικόνα τους, να προβάλουν τα προϊόντα και τις υπηρεσίες όπως και τις εγκαταστάσεις τους. Ουσιαστικά σε συνδυασμό με την εταιρική ιστοσελίδα είναι σε θέση να ολοκλήρωση την εικόνα προβολής της επιχείρησης με χαμηλό σχετικά κόστος για την επιχείρηση. Τέλος, μέσω της συγκεκριμένης εφαρμογής η επιχείρηση μπορεί να οργανώσει εκδηλώσεις με σκοπό την προσέλευση νέων πελατών.

- ✓ Twitter: Μια ακόμα πλατφόρμα κοινωνικής δικτύωσης που χρησιμοποιούν οι τουριστικές επιχειρήσεις είναι το γνωστό Twitter το οποίο κατασκευάστηκε αρχικά το 2006 και εμφανίστηκε στο ευρύ κοινό λίγους μήνες μετά. Μέσω της συγκεκριμένης κοινωνικής πλατφόρμας οι χρήστες έχουν την δυνατότητα να δημοσιεύσουν μικρής έκτασης κείμενα και να επικοινωνήσουν με άτομα ή επιχειρήσεις με τα οποία έχουν κοινά ενδιαφέροντα. Απαραίτητη προϋπόθεση

είναι μόνο η ύπαρξη λογαριασμού χρήστη στην πλατφόρμα που δεν συνεπάγει κανένα απολύτως κόστος. Οι τουριστικές επιχειρήσεις χρησιμοποιούν το Twitter, κυρίως, για την προώθηση των προϊόντων/υπηρεσιων τους και την δημοσιοποίηση νέων ιδεών. Με αυτόν τον τρόπο η επιχείρηση επικεντρώνεται στην επικοινωνία με τους εν δυνάμει πελάτες της, δημιουργώντας σχέσεις με αυτούς, μέσω της δημοσιοποίησης των εσωτερικών πληροφοριών της.

- ✓ Flictr: Εδώ και λίγα χρόνια αποτελεί προϊόν της Yahoo διότι εξαγοράστηκε πρόσφατα από την αρχική εταιρία που το δημιούργησε. Κύριος σκοπός της πλατφόρμας είναι η ανταλλαγή και μεταβίβαση οπτικοακουστικού υλικού (βίντεο και φωτογραφίες). Η εγγραφή του χρήστη στο πρόγραμμα αποτελεί δωρεάν διαδικασία για τις απλές λειτουργίες αυτού, με τη δυνατότητα επέκτασης των δυνατοτήτων με επιπλέον κόστος για επαγγελματική, κυρίως, χρήση. Οι επιχειρήσεις στον τουριστικό κλάδο χρησιμοποιούν της εφαρμογή αυτή για να μεταφέρουν τα αντίστοιχα αρχεία μεγάλου μεγέθους στα blog των ιστοσελίδων τους, που παρουσιάζουν μέσω αυτού τις εγκαταστάσεις τους και τα τοπία της περιοχής όπου βρίσκονται. Μεγάλο πλεονέκτημα του Flictr για τις επιχειρήσεις είναι η παροχή σχετικά με την άδεια χρήσης του υλικού (creative commons) με σκοπό την ασφάλεια του υλικού αυτού.

- ✓ Google plus: Αποτελεί μία επιπλέον εφαρμογή η οποία ανήκει στην εταιρία Google. Η συγκεκριμένη εφαρμογή βοηθά στην επικοινωνία των χρηστών και την ανταλλαγή οπτικοακουστικού υλικού. Η δημιουργία των αντίστοιχων λογαριασμών χρηστών παρέχεται δωρεάν και επιτρέπεται η κοινή χρήση του υλικού μεταξύ των χρηστών. Οι τουριστικές επιχειρήσεις χρησιμοποιούν την συγκεκριμένη εφαρμογή με στόχο την προώθηση των πωλήσεων, μέσα από στοχευμένες πωλήσεις στο αντίστοιχο πελατολόγιο και τη δημιουργία ενός κύκλου πελατών (Schmidt & Rosenberg, 2015).

- ✓ Trip Advisor: Αποτελεί την μεγαλύτερη διαδικτυακή πλατφόρμα σε παγκόσμιο επίπεδο, που αφορά αποκλειστικά τους τουρίστες. Ιδρύθηκε το 2000 και στο ευρύ κοινό παρουσιάστηκε το 2001. Ανήκει στην κατηγορία των μέσων κοινωνικής δικτύωσης γιατί δεν αποκλείει την αλληλεπίδραση των

ατόμων. Αποτελείται αποκλειστικά από δεδομένα τα οποία εισχωρούν, οι χρήστες, στο σύστημα και περιλαμβάνουν εικόνες, βίντεο και πληροφορίες σχετικές με τις επιχειρήσεις που ασχολούνται με τον κλάδο του τουρισμού. Επιπλέον, υπάρχει αρκετά λεπτομερής περιγραφή και σχολιασμός για αυτών των επιχειρήσεων πράγμα το οποίο το καθιστά ως την πιο έγκυρη πηγή για την οργάνωση ενός ταξιδιού. Οι τουριστικές επιχειρήσεις με την σωστή διαχείριση αυτού, έχουν την δυνατότητα να προσελκύσουν νέους πελάτες και ταυτόχρονα να ενισχύσουν ουσιαστικά και κυρίως χωρίς κανένα κόστος την εικόνα τους.

- ✓ Trivago: Ιδρύθηκε το 2004 και η ελληνική πλατφόρμα παρουσιάστηκε στο κοινό το 2009. Η συγκεκριμένη ιστοσελίδα αποτελεί μέσο, για την προώθηση τουριστικών προϊόντων. Η Trivago, αποτελεί μία μηχανή αναζήτησης ειδικά προσαρτημένη στις ανάγκες των τουριστών και παρέχει σε αυτούς τη δυνατότητα να εντοπίζουν τιμές καταλυμάτων και άλλες πληροφορίες για τουριστικούς προορισμούς που επιθυμούν (Wikipedia, 2018). Ο πραγματικός σκοπός της ιστοσελίδας αυτής, είναι η σύγκριση των τιμών των καταλυμάτων σε πραγματικό χρόνο απαίτησης του χρήστη. Συγκεκριμένα, έχει τη δυνατότητα να συγκρίνει τιμές από 700.000 ξενοδοχεία τα οποία με τη σειρά τους συνδέονται με έτερες ιστοσελίδες ξενοδοχειακών κρατήσεων. Μέσω της ιστοσελίδας, οι χρήστες αποκτούν μία ολοκληρωμένη εικόνα για τα καταλύματα και τους προορισμούς που τους ενδιαφέρουν λαμβάνοντας υπόψην κριτικές που έχουν παρατεθεί από πελάτες της αντίστοιχης επιχείρησης. Με αυτόν τον τρόπο, οι τουριστικές επιχειρήσεις έχουν την δυνατότητα να ενισχύσουν, καταλυτικά, την εικόνα τους και τον αριθμό των κρατήσεων (Trivago, 2018).

- ✓ Booking: Αποτελεί μία ιστοσελίδα η οποία ιδρύθηκε το 1996 στην Ολλανδία και μέσω αυτής πραγματοποιούνται διαδικτυακές κρατήσεις καταλυμάτων (Wikipedia, 2018). Η booking είναι μία ιστοσελίδα τουριστικού ενδιαφέροντος η οποία περιλαμβάνει 1.033.483 ξενοδοχεία σε 225 χώρες για όλες τις εποχές του χρόνου. Είναι μία επιχείρηση η οποία απασχολεί μεγάλο

αριθμό εργατικού δυναμικού, έχει 184 γραφεία σε πολλές πόλεις του κόσμου όπως επίσης και στην χώρα μας και έχει μεταφραστεί σε 35 γλώσσες λόγω του ιδιαίτερα μεγάλου και ποικίλου εθνικότητας πελατολογίου της. Ο χρήστης έχει τη δυνατότητα να δημιουργήσει έναν προσωπικό λογαριασμό μέσω του οποίου θα μπορεί να κάνει μία κράτηση ή να παρατηρήσει το συνολικό του προφίλ ως τουρίστας. Η διαδικασία κράτησης περιλαμβάνει ορισμένα προσωπικά στοιχεία του χρήστη όπως όνομα, διεύθυνση, email, τηλέφωνο και στοιχεία πιστωτικής κάρτας τα οποία όμως αποθηκεύονται για δέκα μέρες μόνο κρυπτογραφούμενα για επιπλέον ασφάλεια του χρήστη. Μετά την διαδικασία της κράτησης ο χρήστης παραλαμβάνει από το σύστημα ένα κωδικό κράτησης και το αντίστοιχο pin της για την επιβεβαίωση. (Booking, 2018). Οι τουριστικές επιχειρήσεις χρησιμοποιούν την ιστοσελίδα αυτή για να αυξήσουν τις κρατήσεις τους ταυτόχρονα με το brand name διότι σύμφωνα με έρευνα σε καθημερινή βάση μέσω της ιστοσελίδας πραγματοποιούνται πάνω από 1.000.000 διανυκτερεύσεις στα ξενοδοχεία. Τέλος, πρέπει να αναφερθεί ότι οι τουριστικές επιχειρήσεις καταβάλλουν μία προμήθεια στην booking της τάξεως του 12% του συνολικού τιμήματος που καταβάλει στην επιχείρηση ο χρήστης για την παροχή της διανομής του (Booking, 2018).

- ✓ Youtube: Αποτελεί μία ακόμα υπηρεσία η οποία αγοράστηκε τα τελευταία χρόνια από την Google. Το υλικό της συγκεκριμένης πλατφόρμας απαρτίζεται από βίντεο, μουσική και τηλεόραση. Η υπηρεσία αυτή προωθεί την αλληλεπίδραση των χρηστών μετά από την εγγραφή τους, παρέχοντας την δυνατότητα των σχολίων αλλά και των αναρτήσεων που πραγματοποιούν οι ίδιοι οι χρήστες. Οι τουριστικές επιχειρήσεις, εκμεταλλεύονται τα κανάλια του youtube έτσι ώστε μέσω αυτών να διοχετεύουν στο καταναλωτικό κοινό σχετικά βίντεο με το αντικείμενο δραστηριοτήτων τους, αυξάνοντας έτσι την ισχύ του brand name τους (Schmidt & Rosenberg, 2015).

- ✓ Linkend in: Αποτελεί μία πλατφόρμα κοινωνικής δικτύωσης κυρίως επαγγελματικοί χαρακτήρα. Γνωστοποιήθηκε στο ευρύ κοινό το 2003 και από τότε χρησιμοποιείται κατά κόρον από επαγγελματίες και επιχειρήσεις. Οι

χρήστες μέσω του Linkend in δημιουργούν ένα εταιρικό προφίλ της επιχείρησης και αντίστοιχα οι επαγγελματίες ως φυσικά πρόσωπα αποθηκεύουν το βιογραφικό τους. Μέσω των προφίλ των διαφόρων χρηστών δημιουργείται η αλληλεπίδραση μεταξύ τους. Μέσω αυτού, οι επιχειρήσεις τουριστικού ενδιαφέροντος εντοπίζουν το ανθρώπινο δυναμικό τους, ενισχύουν την εικόνα τους προς το ευρύ κοινό και διευρύνουν το πελατολόγιο τους αφού παρέχουν πληροφορίες για τα τουριστικά προϊόντα που διαθέτουν.

- ✓ Pinterest: Και αυτή η εφαρμογή αποτελεί ένα μέσο κοινωνικής δικτύωσης για τους χρήστες στους οποίους παρέχετε δωρεάν εγγραφή και δημιουργίας ενός συνολικού προφίλ. Απαραίτητη προϋπόθεση είναι η ύπαρξη ενός email ή facebook έτσι ώστε να πραγματοποιηθεί η απαραίτητη σύνδεση για την τυπική διαδικασία των έγκυρων στοιχείων του χρήστη. Το Pinterest αποτελεί μέσο αποθήκευσης βίντεο, φωτογραφιών κειμένων και ιστοσελίδων του χρήστη, που τον ενδιαφέρουν. Τα αποτελέσματα της αποθήκευσης των επιλεγμένων δεδομένων για τον χρήστη συσσωρεύονται σε ένα συνολικό πίνακα ο οποίος συνθέτει το αντίστοιχο προφίλ χρήστη. Επιτρέπεται η αλληλοσύνδεση των χρηστών και ο ελεύθερος σχολιασμός. Οι τουριστικές επιχειρήσεις χρησιμοποιούν τον συγκεκριμένο διαδικτυακό τόπο με σκοπό να εντοπίσουν τις ανάγκες του καταναλωτικού κοινού (διότι αυτές συσσωρεύονται όπως είπαμε πιο πάνω στους αντίστοιχους πίνακες) και να ικανοποιήσουν αυτές μέσω των διαθέσιμων προϊόντων τους ή των υπηρεσιών τους.

ΚΕΦΑΛΑΙΟ 6: ΕΡΕΥΝΑ ΑΣΦΑΛΕΙΑΣ ΣΥΝΑΛΛΑΓΩΝ ΣΤΟΝ ΤΟΥΡΙΣΤΙΚΟ ΚΛΑΔΟ

6.1 Σκοπός της έρευνας – Ερωτηματολόγιο

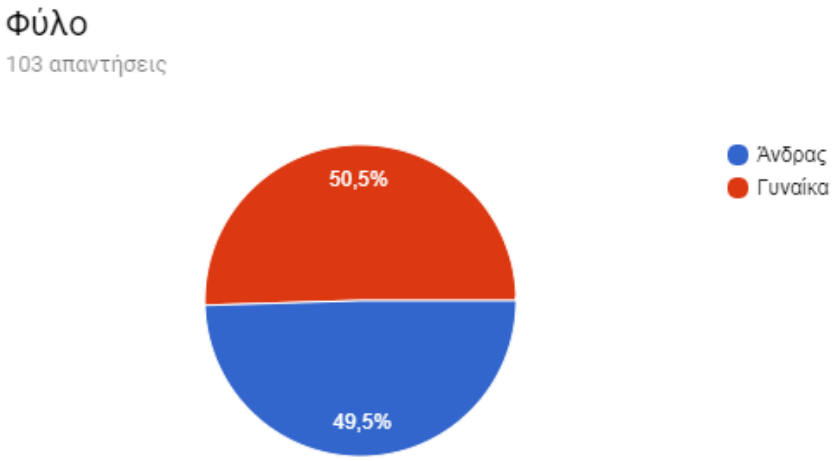
Σκοπό της παρούσας έρευνας μέσω ερωτηματολογίου, είναι η ασφαλή διεξαγωγή συμπερασμάτων σχετικά με τη διερεύνηση της εμπιστοσύνης των καταναλωτών και ιδιαίτερα των ατόμων που δραστηριοποιούνται στον τουριστικό τομέα, στις ηλεκτρονικές τραπεζικές συναλλαγές. Για το λόγο αυτό μετά από συνεννόηση, με το τμήμα ανθρώπινου δυναμικού του ξενοδοχείου Μεγάλη Βρετάνια, στο Σύνταγμα, διαμοιράστηκε το συγκεκριμένο ερωτηματολόγιο σε ηλεκτρονική μορφή σε όλους τους υπαλλήλους αυτού. Το δείγμα αποτελείται από 103 άτομα τα οποία ήταν πρόθυμα να απαντήσουν στις σχετικές ερωτήσεις του ερωτηματολογίου που τους παραδόθηκε.

Για τις ανάγκες του ερωτηματολογίου αυτού, χρησιμοποιήθηκαν ερωτήσεις κλειστού τύπου με πέντε (5) εναλλακτικές απαντήσεις στην διάθεση του δείγματος και ερωτήσεις βασισμένες στην κλίμακας Likert . Η κλίμακα αυτή, αποτελεί ένα βασικό εργαλείο για την εκτίμηση απόψεων και γενικότερων συμπεριφορών του δείγματος (Παρασκευόπουλος, 1993). Το πλεονέκτημα της κλίμακας Likert εντοπίζεται στην ευκολία των απαντήσεων και αποτελεί ένα μη εξειδικευμένο εργαλείο έρευνας, δίνοντας έτσι την δυνατότητα σε άτομα που δεν είναι γνώστες του αντικειμένου να αναλύσουν και να αξιολογήσουν τα αποτελέσματα της έρευνας (Spooren at al, 2007). Φυσικά, εκτός από πλεονεκτήματα, η συγκεκριμένη κλίμακα διαθέτει και κάποια μειονεκτήματα τα οποία συνοψίζονται παρακάτω(Hassont & Arnetz, 2007):

- Η δυσκολία στην επιλογή της απάντησης από πλευράς δείγματος.
- Η συνολική βαθμολόγηση των αποτελεσμάτων που προκύπτει από την συγκεκριμένη κλίμακα, αποτελεί προϊόν πολλών διαφορετικών συνδυασμών απαντήσεων με αποτέλεσμα πολλές φορές να χάνονται κάποιες πληροφορίες.

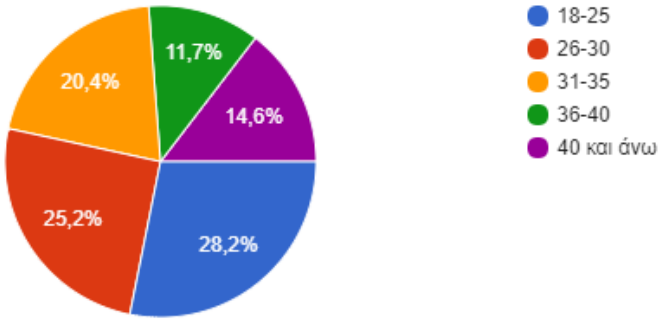
- Ο τρόπος της διατύπωσης των ερωτήσεων υπάρχει σοβαρή πιθανότητα να επηρεάσει τις απαντήσεις του δείγματος.
- Η αθροιστική βαθμολόγηση, μπορεί να οδηγήσει σε λανθασμένα τελικά συμπεράσματα σε κάποιες περιπτώσεις.

6.2 Αποτελέσματα έρευνας



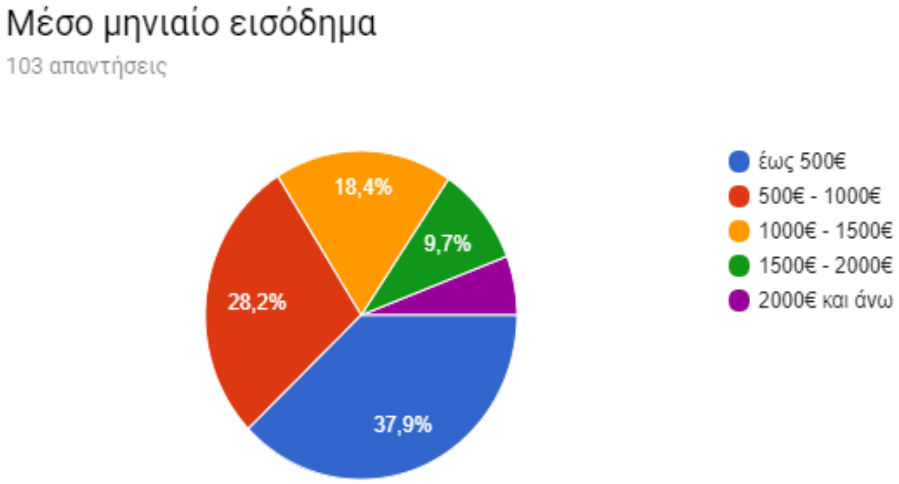
Ηλικία

103 απαντήσεις

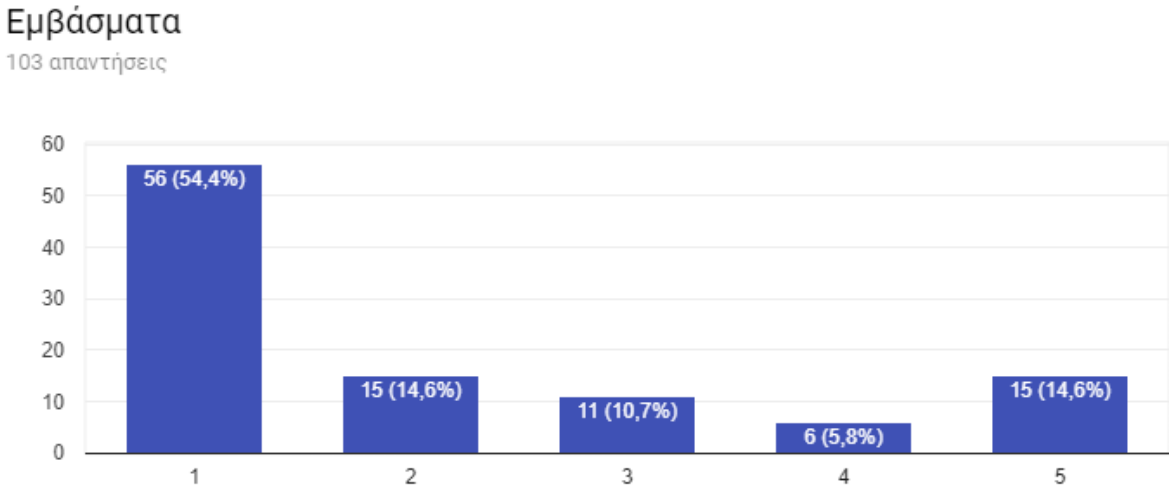


Επίπεδο Εκπαίδευσης

103 απαντήσεις

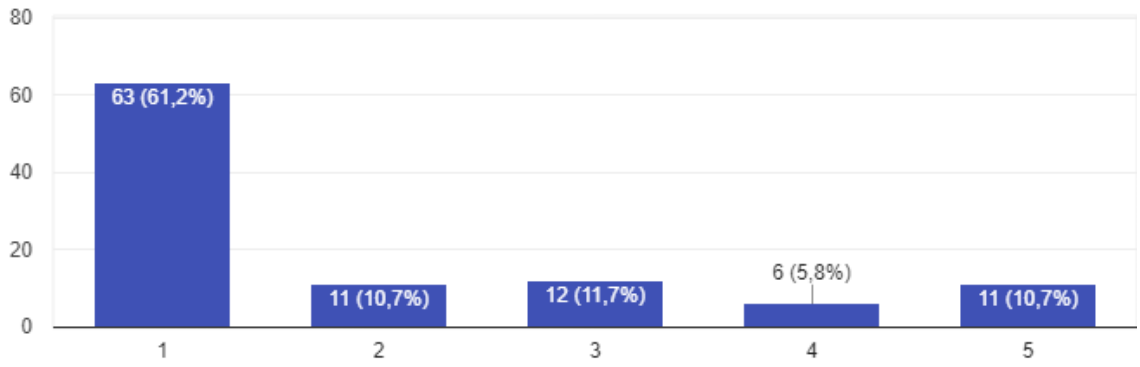


Πόσο συχνά χρησιμοποιείται τα ακόλουθα τραπεζοασφαλιστικά προϊόντα;



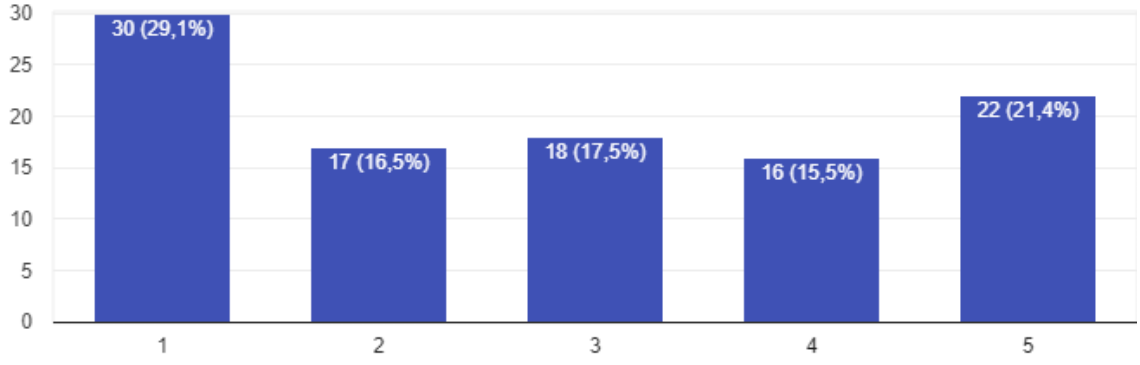
Δάνεια

103 απαντήσεις



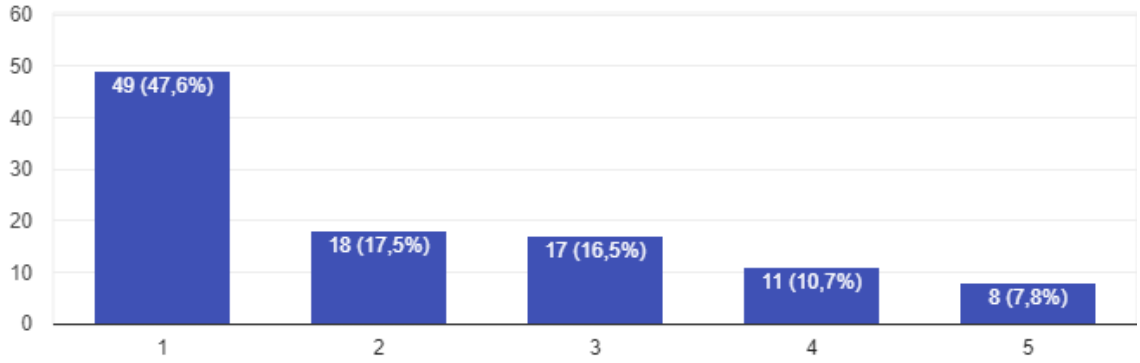
Καταθέσεις - πληρωμές

103 απαντήσεις



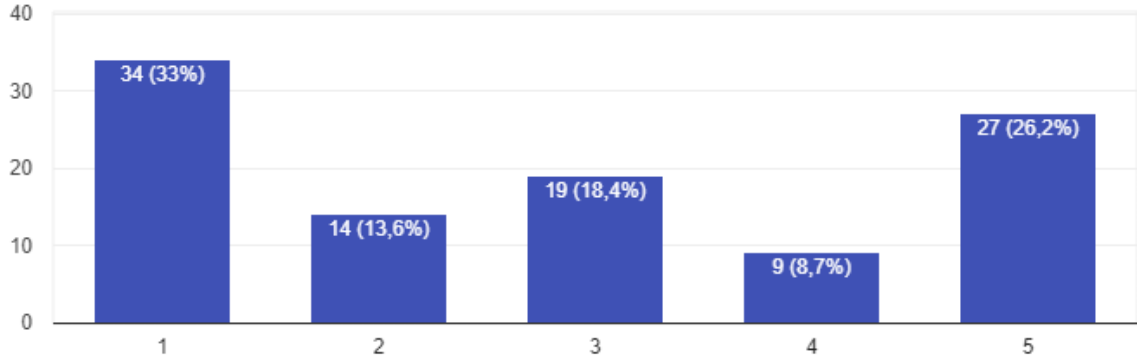
Ασφάλειες

103 απαντήσεις



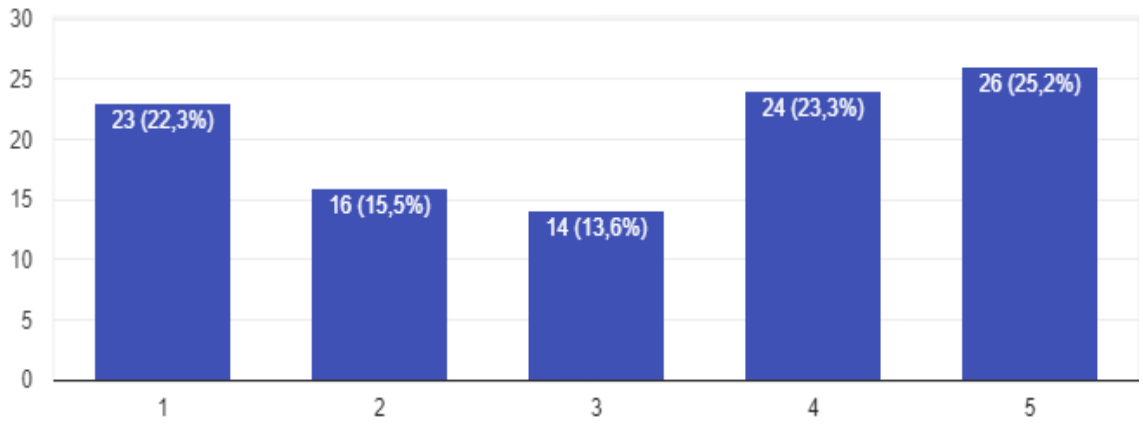
Κάρτες

103 απαντήσεις



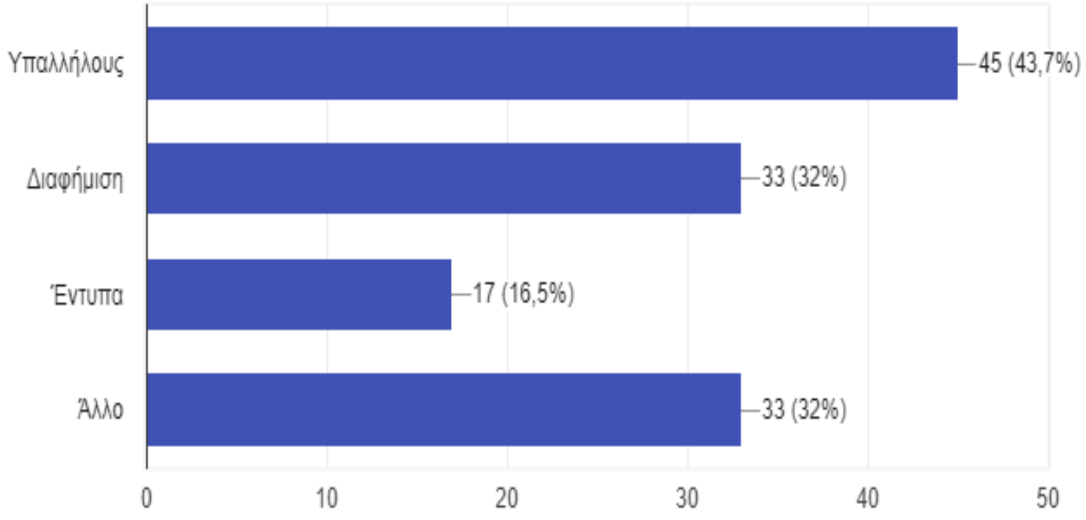
Αναλήψεις

103 απαντήσεις



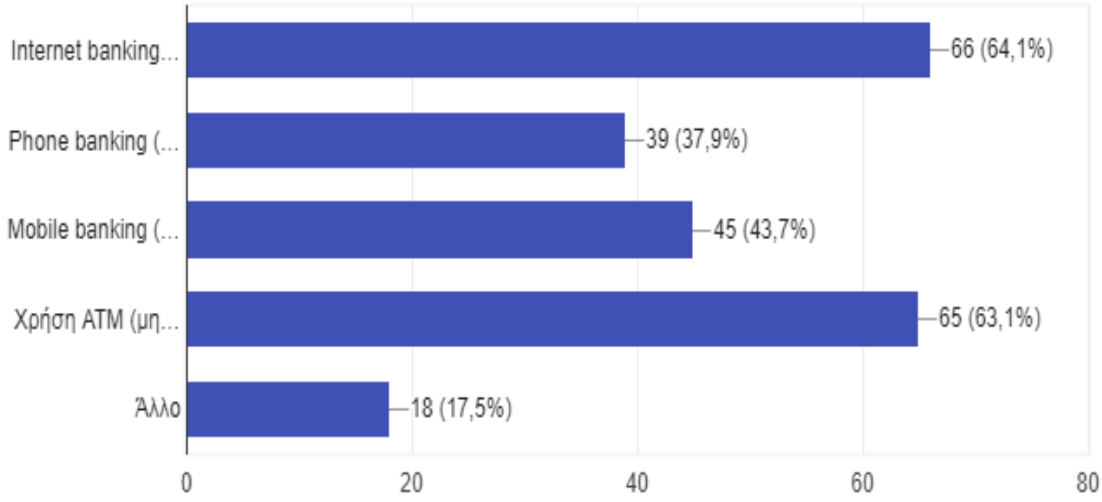
Από πού ενημερώνεστε για τις υπηρεσίες των τραπεζών;

103 απαντήσεις



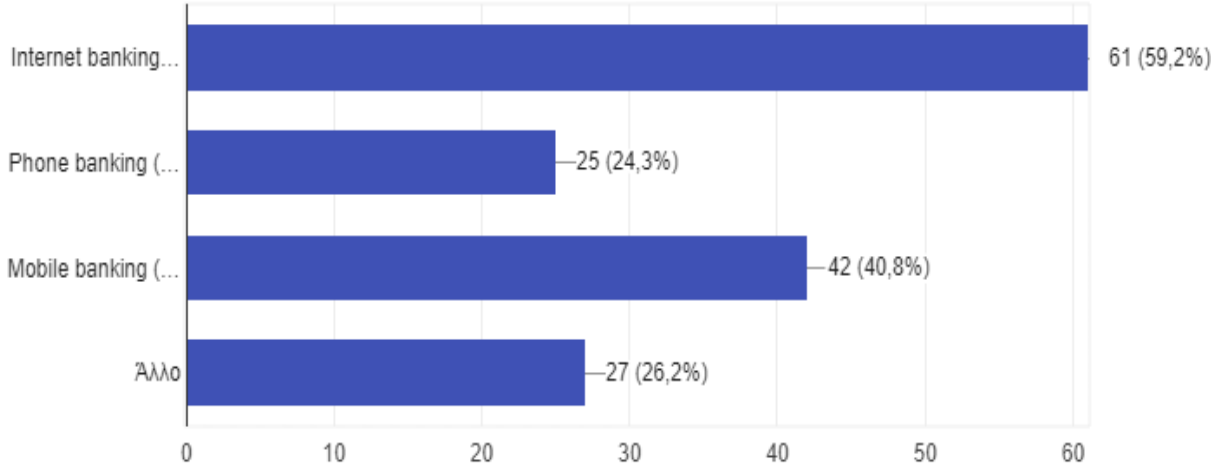
Ποιες από τις παρακάτω υπηρεσίες γνωρίζετε;

103 απαντήσεις



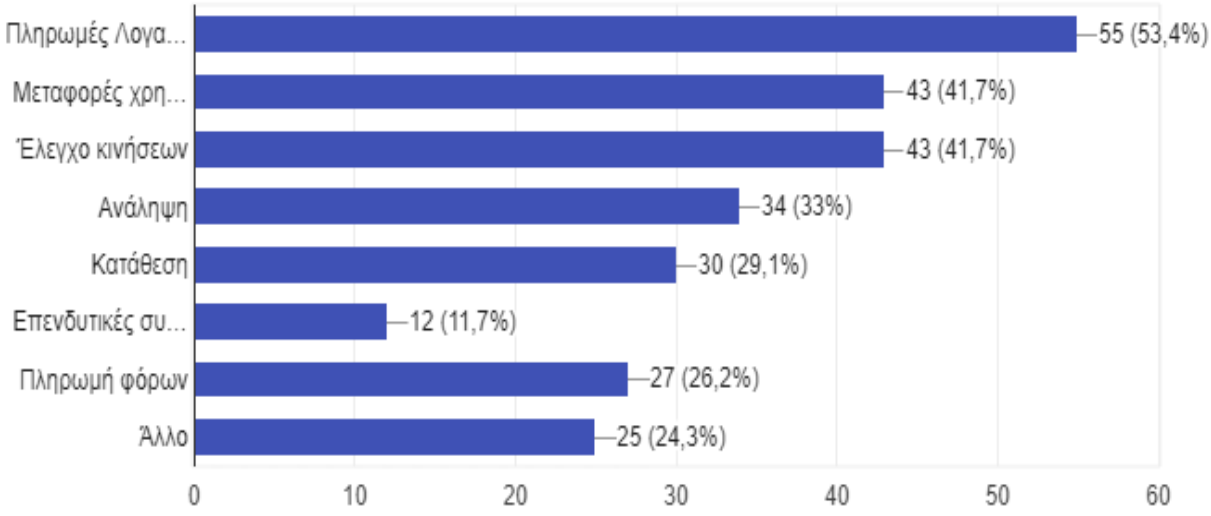
Ποια είδη e-banking χρησιμοποιείτε;

103 απαντήσεις



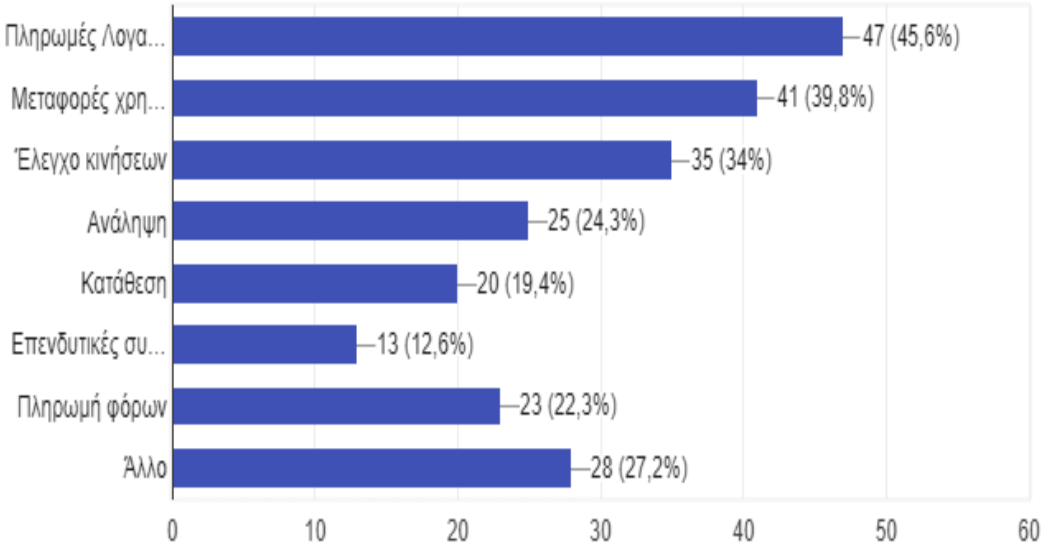
Τι είδους συναλλαγές πραγματοποιείτε μέσω του e-banking;

103 απαντήσεις



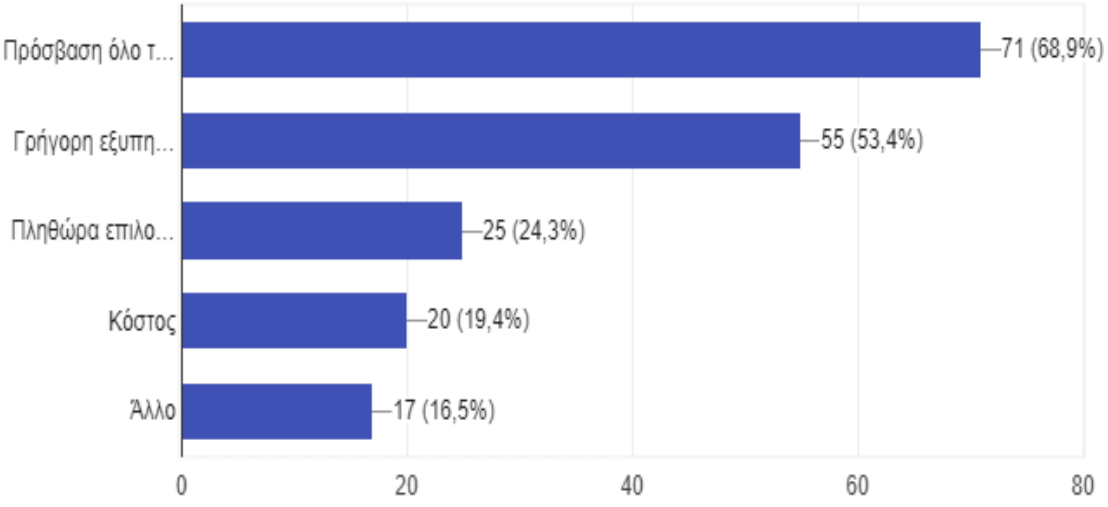
Υπάρχουν συναλλαγές για τις οποίες χρησιμοποιείται αποκλειστικά τις υπηρεσίες e-banking;

103 απαντήσεις



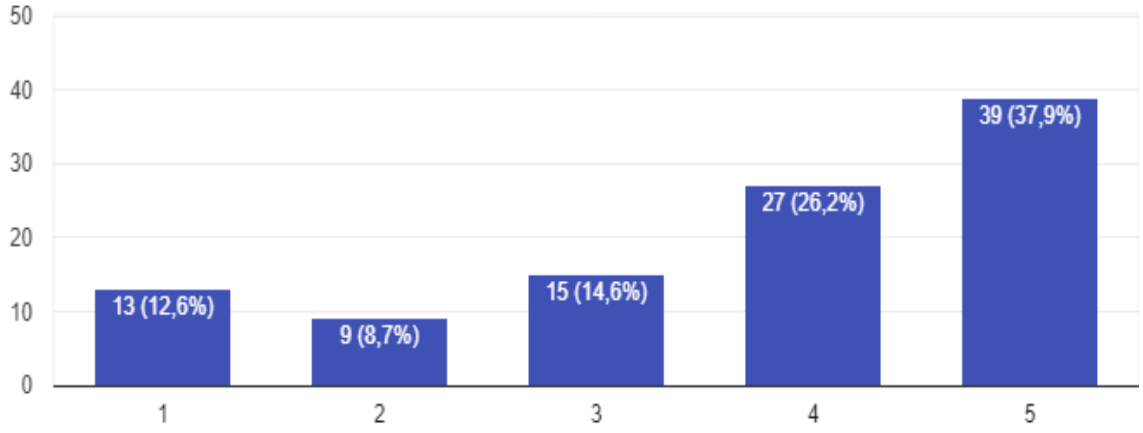
Ποιες οι ευκολίες που σας προσφέρει το e-banking;

103 απαντήσεις



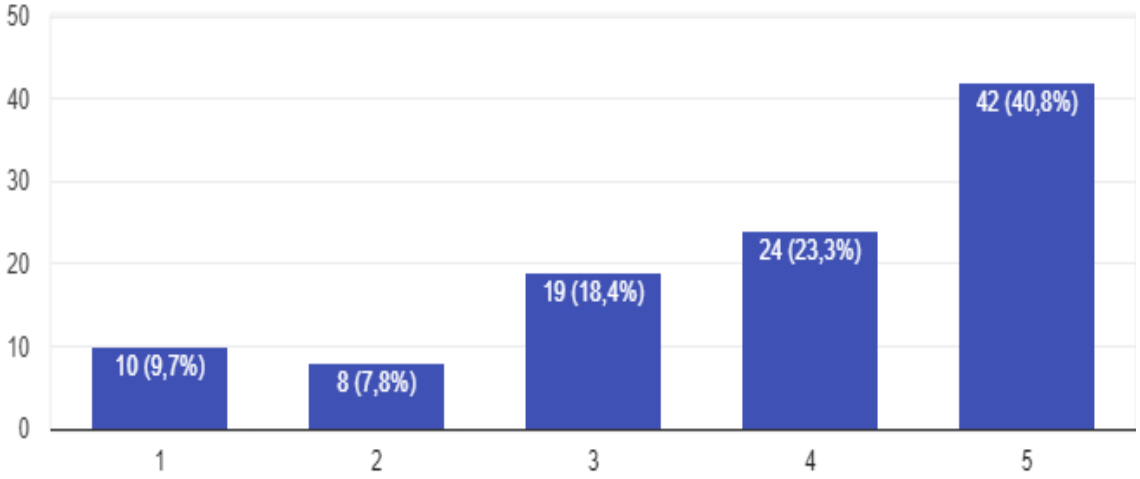
Είστε ικανοποιημένος/η από τις υπηρεσίες που σας προσφέρονται από το e-banking;

103 απαντήσεις



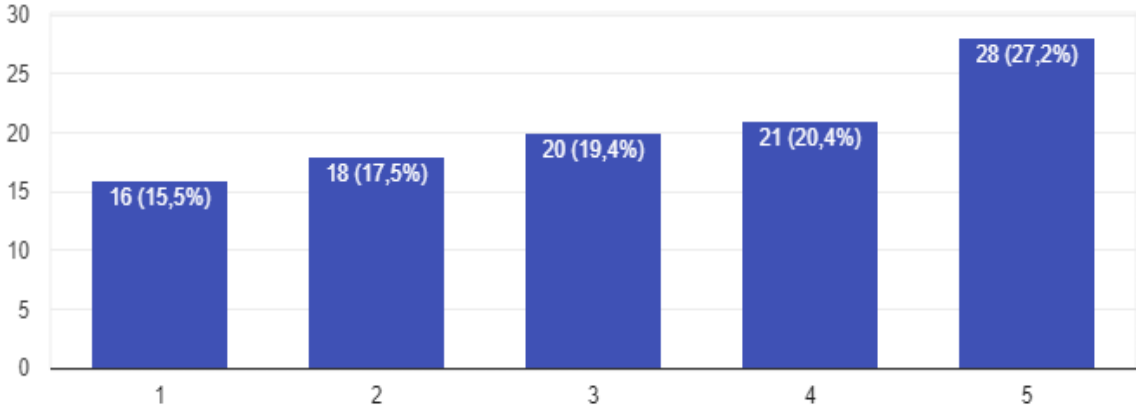
Θα προτείνατε σε κάποιον άλλο την χρήση Internet Banking ;

103 απαντήσεις



Κατά πόσο θα χρησιμοποιούσατε τις υπηρεσίες e-banking για να πραγματοποιήσετε αγορές που αφορο...ς τουριστικές σας δραστηριότητες;

103 απαντήσεις

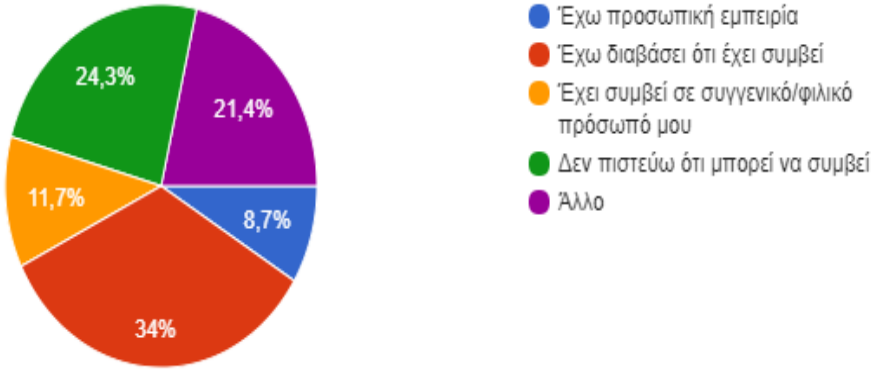


Όσον αφορά τις κρατήσεις των διακοπών σας ποιο από τα παρακάτω περιγράφει περισσότερο την χρήση π...πεζικές συναλλαγές μέσω e-banking;

103 απαντήσεις

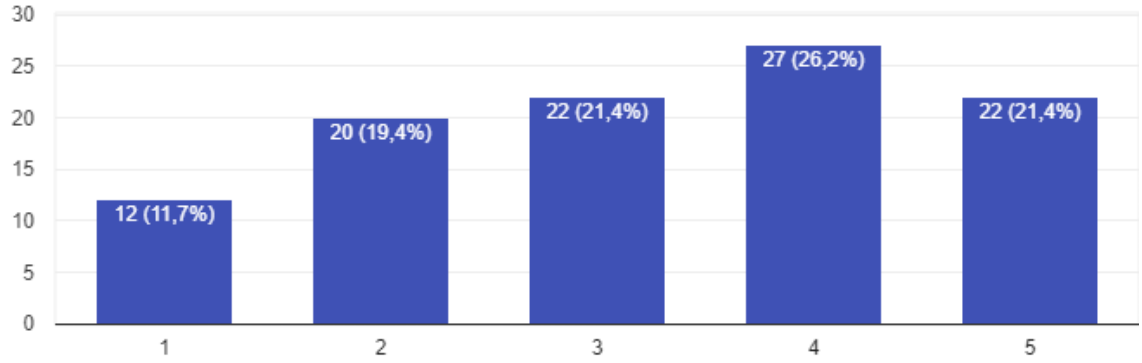
Γνωρίζετε αν έχει διαπραχθεί ηλεκτρονική κλοπή

103 απαντήσεις



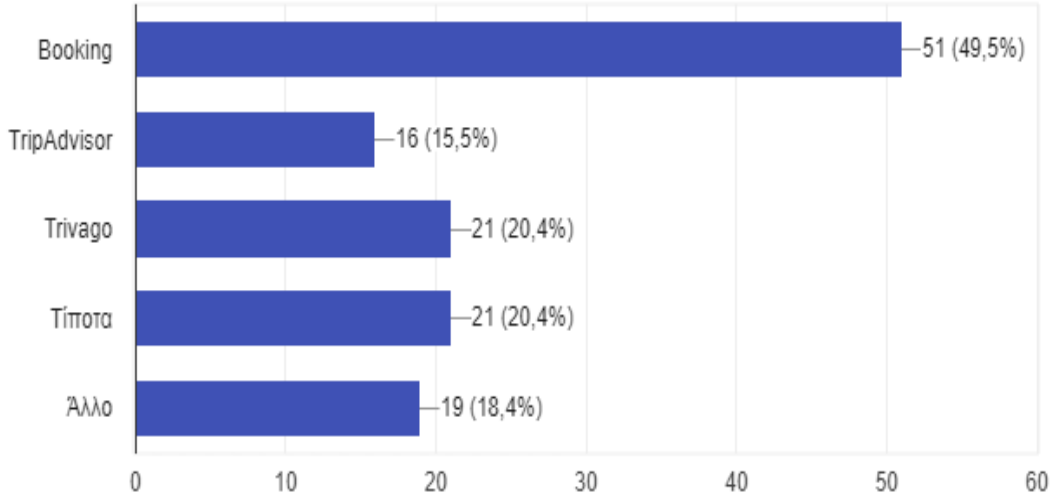
Έχετε εμπιστοσύνη στις online τραπεζικές συναλλαγές;

103 απαντήσεις



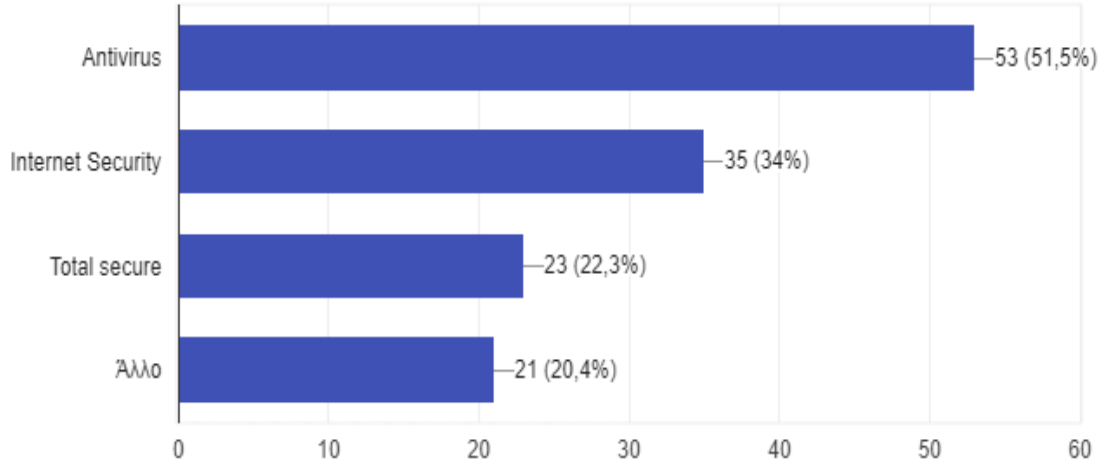
Έχετε χρησιμοποιήσει πρόσφατα κάποια υπηρεσία προγραμματισμού διακοπών;

103 απαντήσεις



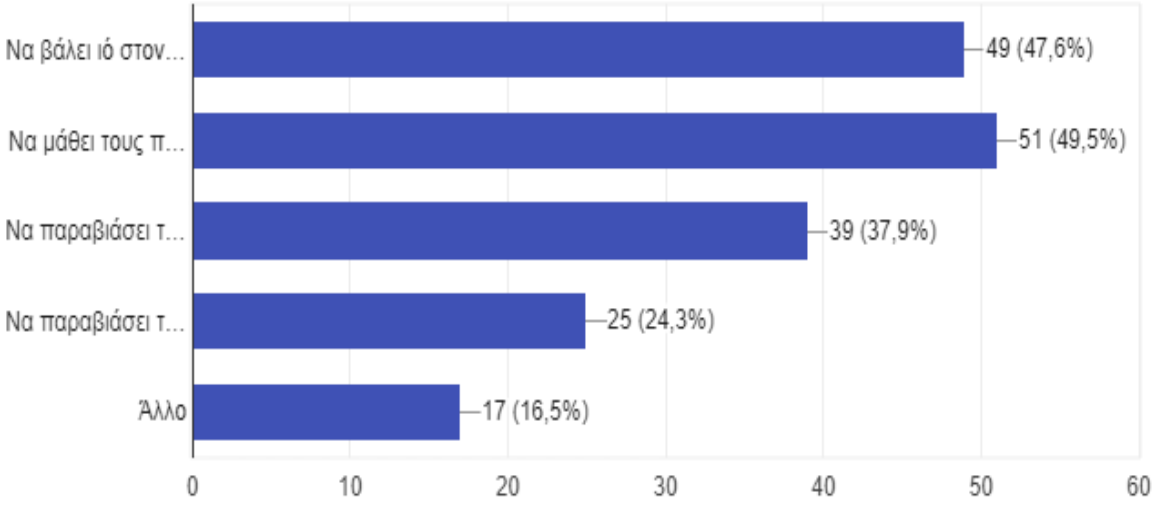
Χρησιμοποιείτε κάποιο λογισμικό για επιπλέον ασφάλεια στις online τραπεζικές σας συναλλαγές (antivirus, internet security, total secure κλπ.);

103 απαντήσεις



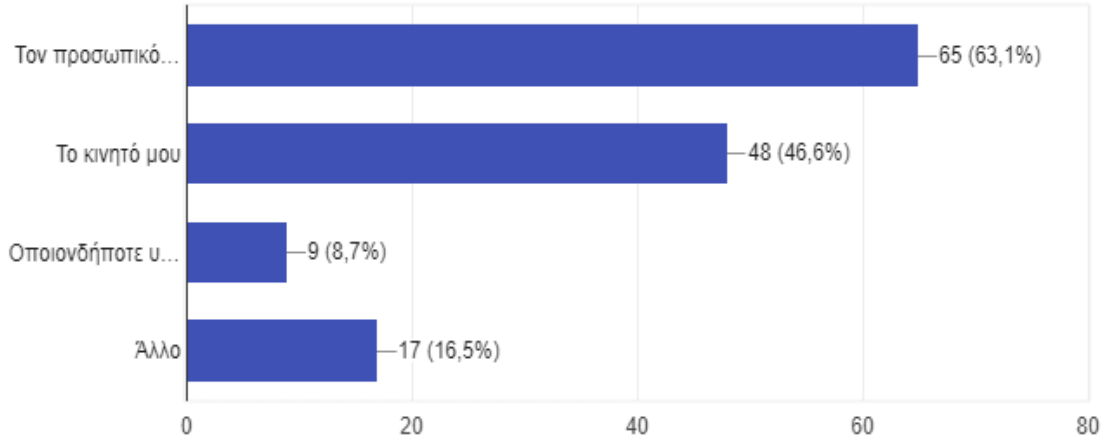
Με ποιο τρόπο θα μπορούσε να υποκλέψει ηλεκτρονικά κάποιος τα προσωπικά σας στοιχεία και να σας εξαπατήσει;

103 απαντήσεις



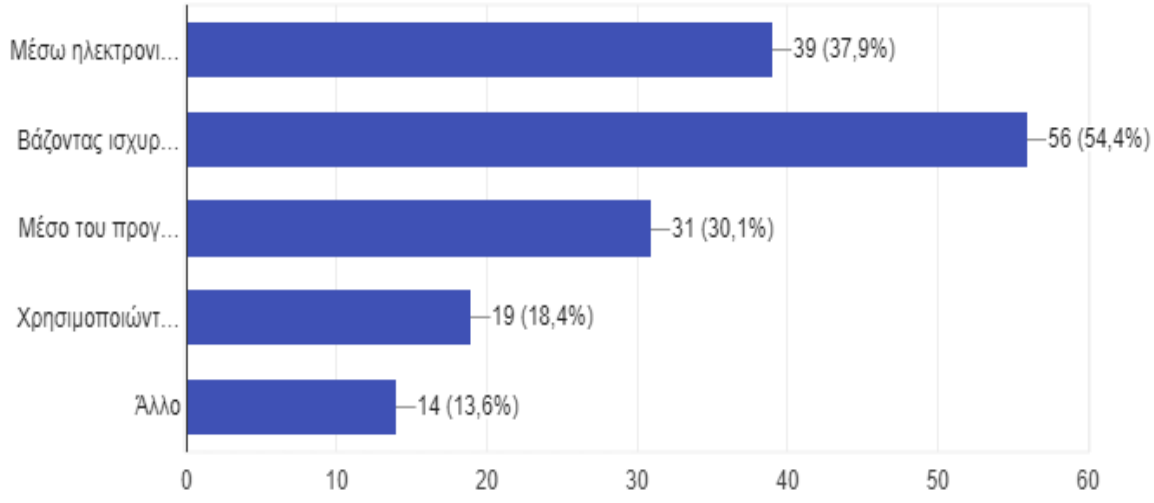
Όταν πρόκειται να χρησιμοποιήσετε τις υπηρεσίες e-banking ποιο μέσο σύνδεσης προτιμάτε;

103 απαντήσεις



Με ποιους τρόπους γνωρίζετε ότι διασφαλίζονται οι ηλεκτρονικές συναλλαγές σας;

103 απαντήσεις



6.3 Σχολιασμός αποτελεσμάτων

Το εξεταστέο δείγμα αποτελούνταν από άνδρες και γυναίκες σχεδόν ισομοιρασμένου αριθμού, αφού στο συγκεκριμένο ερωτηματολόγιο το 50,5% των ερωτώμενων είναι γυναίκες και το 49,5% άνδρες. Όσον αναφορά την ηλικία των ατόμων το 28,2% του δείγματος ανήκε στο ηλικιακό γκρουπ 18-25 ετών, το 25,2% ήταν μεταξύ 26-30 ετών, το 20,4% μεταξύ 31-35 ετών, το 11,7% ανήκε στην ηλικιακή ομάδα μεταξύ 36-40 ετών και το 14,6% ήταν πάνω από 40 ετών. Το εκπαιδευτικό επίπεδο του δείγματος, πιθανός λόγω του ισχυρού brand name του ξενοδοχείου, εντοπίστηκε κατά συντριπτική πλειοψηφία ότι ήταν πανεπιστημιακής εκπαίδευσης. Συγκεκριμένα, το 42,7 % κατείχε τίτλο πανεπιστημιακής εκπαίδευσης, το 15,5% ήταν κάτοχοι μεταπτυχιακού ή διδακτορικού, το 29,1% ήταν απόφοιτοι δευτεροβάθμιας εκπαίδευσης και μόνο το 12,6% ήταν απόφοιτοι δημοτικού. Το μέσο μηνιαίο εισόδημα αυτών, κυμάνθηκε σε αρκετά μεγάλο εύρος, εντοπίζοντας μέσα από τις αντίστοιχες απαντήσεις ότι το 37,9% του προσωπικού σε μηνιαία βάση τα εισοδήματα του κυμαίνονται έως 500 ευρώ, το 28,2% από 500-1000 ευρώ, το 18,4% από 1000-1500 ευρώ, το 9,7% από 1500-2000 ευρώ και μόλις το 5,8% κυμαίνεται από 2000 ευρώ και άνω όσον αναφορά τις μηνιαίες αποδοχές του.

Στην ερώτηση για το πόσο συχνά το δείγμα χρησιμοποιεί κάποια τραπεζικά προϊόντα, επικεντρωθήκαμε στα εξής προϊόντα: Εμβάσματα, δάνεια, καταθέσεις/πληρωμές, ασφάλειες, κάρτες και αναλήψεις. Για τις ανάγκες της συγκεκριμένης ερώτησης χρησιμοποιήθηκε η κλίμακα Likert έτσι ώστε να πραγματοποιηθεί μέτρηση των απόψεων και των γενικότερων συμπεριφορών του δείγματος. Συγκεκριμένα, παρατηρήθηκε όσον αναφορά τη χρήση των εμβασμάτων, ότι το 54,4% του δείγματος δεν χρησιμοποιεί καθόλου συχνά τη χρήση του τραπεζικού προϊόντος αυτού, το 14,6% χρησιμοποιεί το προϊόν αυτό πολύ λίγο, το 10,7% λίγο, το 5,8% πολύ και το 14,6% χρησιμοποιεί πάρα πολύ τα εμβάσματα. Όσον αναφορά τη χρήσης των δανείων, το 61,2% του δείγματος δεν χρησιμοποιεί καθόλου συχνά το προϊόν αυτό, το 10,7% το χρησιμοποιεί πολύ λίγο, το 11,7% λίγο, το 5,8% πολύ και το 10,7% χρησιμοποιεί πάρα πολύ τα δάνεια. Στις καταθέσεις/ πληρωμές παρατηρείται ότι τα

ποσοστά αυξάνονται σε όλες τις κλίμακες σε σχέση με τα προηγούμενα τραπεζικά προϊόντα. Συγκεκριμένα το 29,1% του δείγματος δεν χρησιμοποιεί καθόλου συχνά τις καταθέσεις/πληρωμές, το 16,5% τις χρησιμοποιεί πολύ λίγο, το 17,5% λίγο, το 15,5% πολύ και τέλος το 21,4% χρησιμοποιεί πάρα πολύ τις καταθέσεις/ πληρωμές. Στις ασφάλειες, το 47,6% δεν κάνει χρήση καθόλου του συγκεκριμένου προϊόντος, το 17,5% το χρησιμοποιεί πολύ λίγο, το 16,5% λίγο, το 10,7% πολύ και το 7,8% το χρησιμοποιεί πάρα πολύ. Οι κάρτες αποτελούν ένα ακόμη γνωστό τραπεζικό προϊόν. Στην αντίστοιχη ερώτηση για το πόσο συχνά το δείγμα χρησιμοποιεί τις κάρτες, το 33% δήλωσε ότι δεν τις χρησιμοποιεί καθόλου, το 13,6% ότι τις χρησιμοποιεί πολύ λίγο, το 18,4% λίγο, το 8,7% τις χρησιμοποιεί πολύ ενώ το 26,2% χρησιμοποιεί το προϊόν αυτό πάρα πολύ. Και τέλος, όσον αναφορά τις αναλήψεις, το 22,3% των ερωτώμενων δήλωσε ότι δεν χρησιμοποιεί καθόλου τις αναλήψεις, το 15,5% δήλωσε ότι χρησιμοποιεί το τραπεζικό προϊόν πολύ λίγο, το 13,6% λίγο, το 23,3% πολύ και το 25,2% πάρα πολύ.

Στην ερώτηση σχετικά με την πηγή την οποία προσφέρει πληροφόρηση στο δείγμα για τις υπηρεσίες των τραπεζών, το 43,7% δήλωσε ότι ενημερώνεται από υπαλλήλους, το 32% από την διαφήμιση, το 16,5% από τα διαθέσιμα έντυπα των τραπεζών και το 32% από άλλα μέσα που δεν αναφέρονται. Παρατηρείται ιδιαίτερο αυξημένο ποσοστό ενημέρωσης των πελατών από τον παραδοσιακό τρόπο πληροφόρησης ο οποίος είναι οι υπάλληλοι της επιχείρησης.

Στην σχετική ερώτηση σχετικά με το ποιες τραπεζικές υπηρεσίες γνωρίζει το εξεταστέα δείγμα, το 64,1% δήλωσε το e-banking, το 37,9% το Phone banking, το 43,7% το mobile banking, το 63,1% το ATM και το 17,5% δήλωσε ότι γνωρίζει και άλλες υπηρεσίες. Το είδη e-banking, που χρησιμοποιούν οι ερωτώμενοι είναι κατά 59,2% το Internet Banking, κατά 24,3% το Phone banking, με ποσοστό 40,8% το Mobile Banking και το 26,2% επέλεξε την επιλογή άλλο. Όσον αναφορά το είδος των συναλλαγών που πραγματοποιούν τα άτομα μέσω e-banking, το 53,4% δήλωσε ότι μέσω αυτού πληρώνει λογαριασμούς, το 41,7% ότι πραγματοποιεί μεταφορές χρημάτων, το 41,7% ότι ελέγχει τις κινήσεις των λογαριασμών, το 33% πραγματοποιεί αναλήψεις, το 29,1% καταθέσεις, το 11,7% πραγματοποιεί

επενδυτικές συναλλαγές, το 26,2% εξοφλεί φόρους και το 24,3% πραγματοποιεί και άλλες συναλλαγές μέσω αυτού.

Στην ερώτηση για το αν υπάρχουν συναλλαγές για τις οποίες το δείγμα χρησιμοποιεί αποκλειστικά τις υπηρεσίες e-banking, το 45,6% δήλωσε ότι είναι οι πληρωμές λογαριασμών, το 39,8% οι μεταφορές χρημάτων, το 34% ο έλεγχος τραπεζικών κινήσεων, το 24,3% η ανάληψη, το 19,4% η κατάθεση, το 12,6% οι επενδυτικές συναλλαγές, το 22,3% η πληρωμή φόρων και το 27,2% δήλωσε ότι υπάρχουν και άλλες συναλλαγές που πραγματοποιεί αποκλειστικά μέσω του e-banking. Στην αντίστοιχη ερώτηση για το ποιες είναι οι ευκολίες που παρέχονται από το e-banking, το 68,9% δηλώνει ότι η μεγαλύτερη ευκολία που προσφέρει είναι η πρόσβαση που παρέχει όλο το 24ωρο, το 53,4% θεωρεί ότι είναι η εύκολη πρόσβαση, το 24,3% δηλώνει ότι είναι η πληθώρα των παρεχόμενων επιλογών, το 19,4% είναι το κόστος και το 16,5% επιλέγει κάποια άλλη ευκολία η οποία δεν αναφέρεται. Όσον αναφορά το βαθμό ικανοποίησης του εξεταστέου δείγματος από τις παρεχόμενες υπηρεσίες το e-banking, το 12,6% δήλωσε ότι δεν είναι καθόλου ευχαριστημένοι, το 8,7% ότι είναι πολύ λίγο ευχαριστημένοι, το 14,6% δήλωσε λίγο, το 26,2% δήλωσε ότι είναι πολύ ευχαριστημένοι και το 37,9% πάρα πολύ.

Στην ερώτηση για το αν θα πρότειναν σε κάποιον άλλο άτομο τη χρήση του Internet Banking, το 9,7% δεν θα το πρότεινε καθόλου, το 7,8% θα το πρότεινε πολύ λίγο, το 18,4% θα το πρότεινε ίσως, το 23,4% θα το πρότεινε και το 40,8% θα το πρότεινε σίγουρα. Παρατηρείται επομένως, το συντριπτικό ποσοστό της ικανοποίησης των πελατών από τις υπηρεσίες του e-banking , πράγμα το οποίο καταλαβαίνουμε διότι θα το πρότειναν σε άλλα πρόσωπα για χρήση.

Στην ερώτηση για το κατά πόσο το δείγμα θα χρησιμοποιούσε τις υπηρεσίες e-banking, για να πραγματοποιήσει τις αγορές του, που αφορούν τουριστική δραστηριότητα, το 15,1% δεν θα το διάλεγε καθόλου, το 17,5% θα το διάλεγε πολύ λίγο, το 19,4% λίγο, το 20,4% πολύ και το 27,2% θα το διάλεγε πάρα πολύ. Συμπερασματικά, το μεγαλύτερο ποσοστό του δείγματος θα πραγματοποιούσε τις αγορές του σχετικά με τουριστικές δραστηριότητες μέσω e-banking. Συγκεκριμένα, το 32% θα πραγματοποιούσε μέσω e-banking κράτηση για ξενοδοχείο, το 29,1% για

αεροπορικά εισιτήρια, το 13,6% για προπληρωμή υπηρεσιών ψυχαγωγίας all in clusive, το 6,9% για ακτοπλοϊκά εισιτήρια και το 18,4% θα το χρησιμοποιούσε για άλλες τουριστικές κρατήσεις.

Κύριος φόβων όλων των χρηστών του e-banking αποτελεί η ηλεκτρονική κλοπή. Σε σχετική ερώτηση για το αν γνωρίζει το δείγμα μας, αν έχει διαπραχθεί ηλεκτρονική κλοπή, το 8,7% δήλωσε ότι έχει προσωπική εμπειρία, το 34% ότι έχει διαβάσει ότι έχει συμβεί, το 11,7% δήλωσε ότι έχει συμβεί σε κοντινό του πρόσωπο, το 24,3% θεωρεί ότι δεν μπορεί να συμβεί κάτι τέτοιο και το 21,4% επέλεξε την επιλογή άλλο. Σχετικά με την εμπιστοσύνη την οποία έχουν τα άτομα στις online τραπεζικές συναλλαγές, το 11,7% δεν έχει καθόλου εμπιστοσύνη στην συγκεκριμένη διαδικασία, το 19,4% έχει πολύ λίγη εμπιστοσύνη, το 21,4% διαθέτει λίγη εμπιστοσύνη για το θέμα αυτό, το 26,2% έχει εμπιστοσύνη και το 21,4% έχει πάρα πολύ εμπιστοσύνη στην διαδικασία των τραπεζικών ιντερνετικών συναλλαγών.

Σε ερώτηση για το αν τα άτομα έχουν χρησιμοποιήσει πρόσφατα κάποια υπηρεσία προγραμματισμού διακοπών, το 49,5% έχει χρησιμοποιήσει πρόσφατα το booking, το 15,5% το Tripadvisor, το 20,4% το Trivago, το 20,4% δεν έχει χρησιμοποιήσει πρόσφατα καμία τέτοια υπηρεσία και το 18,4% έχει χρησιμοποιήσει κάποια υπηρεσία που δεν αναφέρεται πιο πάνω. Για την ασφάλεια των online συναλλαγών, το 51,5% του δείγματος χρησιμοποιεί ως μέσο προστασίας το Antivirus, το 34% το Internet Security, το 22,3% το Total Secure και το 20,4% χρησιμοποιεί για την ασφάλειά του κάποιο άλλο μέσο.

Σε ερώτηση σχετικά με τον τρόπο που πιστεύουν με τον οποίο θα μπορούσε κάποιος να υποκλέψει προσωπικά στοιχεία ασφάλειας, το 47,6% θεωρεί ότι μπορεί να γίνει βάζοντας κάποιον ιό στον υπολογιστή, το 49,5% μαθαίνοντας τους προσωπικούς κωδικούς ασφαλείας, το 37,9% παραβιάζοντας τον προσωπικό υπολογιστή, το 24,3% παραβιάζοντας τον κωδικό ασύρματου δικτύου και το 16,5% έχει στον μυαλό του κάποιον άλλο τρόπο. Όσον αναφορά το μέσο το οποίο χρησιμοποιούν όταν πρόκειται να προβούν σε συναλλαγές μέσω e-banking, το 63,1% των ερωτώμενων δήλωσε ότι προτιμά τον προσωπικό υπολογιστή, το 46,6% το κινητό, το 8,7% δηλώνει ότι κάνει την σύνδεση από οπουδήποτε και το 16,5% πραγματοποιεί την σύνδεση με κάποιο

άλλο μέσο. Τέλος, στην ερώτηση σχετικά με τους τρόπους τους οποίους γνωρίζουν ότι μέσω αυτών διασφαλίζονται οι ηλεκτρονικές συναλλαγές, το 37,9% θεωρεί ότι αυτό μπορεί να επιτευχθεί μέσω των ηλεκτρονικών υπηρεσιών όπως το paypal, το 54,4% βάζοντας ισχυρά password, το 30,1% μέσω του προγράμματος ασφάλισης που παρέχει η τράπεζα, το 18,4% χρησιμοποιώντας μόνο έμπιστα σημεία σύνδεσης και το 13,6% έχει υπόψην του κάποιον άλλο τρόπο.

Συμπεράσματα

Τα συμπεράσματα τα οποία εξήχθησαν μέσα από την παρούσα πτυχιακή εργασία παρουσιάζονται αναλυτικά παρακάτω:

- Τα πληροφοριακά συστήματα αποτελούν πολύ σημαντικό εργαλείο του επιχειρηματικού τομέα διότι υποστηρίζουν όλες τις λειτουργίες και παραγωγικές διαδικασίες εντός της επιχείρησης.

- Η ασφάλεια των πληροφοριακών συστημάτων έχει άμεση σχέση με την ικανότητα προστασίας των προσωπικών δεδομένων από την αντίστοιχη επιχείρηση/οργανισμό.

- Τα τραπεζικά πληροφοριακά συστήματα έχουν καταφέρει να μειώσουν τις ουρές αναμονής στα τραπεζικά ιδρύματα.

- Η ασφάλεια των τραπεζικών εργασιών διακρίνεται σε τέσσερις (4) κατηγορίες, τη φυσική ασφάλεια, τη λογική ασφάλεια, την ασφάλεια δικτύων και την ασφάλεια περιφερειακού και βοηθητικού εξοπλισμού.

- Τα πιο γνωστά είδη ηλεκτρονικής τραπεζικής είναι το internet banking, το phone banking και το mobile banking.

- Μέσω της ηλεκτρονικής τραπεζικής πραγματοποιούνται οικονομικές συναλλαγές, πληροφοριακές συναλλαγές, αιτήσεις και άλλων ειδών υπηρεσίες.

- Οι πιο γνωστές μέθοδοι ηλεκτρονικών πληρωμών είναι οι πιστωτικές/χρεωστικές κάρτες, το paypal, το ψηφιακό χρήμα, το internet banking, το mobile banking και η αντικαταβολή.

- Οι πιο συχνοί τρόποι με τους οποίους μπορεί να εξαπατηθεί ένας χρήστης ηλεκτρονικής τραπεζικής είναι η μέθοδος Phishing, η μέθοδος Pharming, η μέθοδος cross-site-scripting, η μέθοδος Scamming, η μέθοδος Keylloggers και η μέθοδος Trojan Horse.

- Η μέθοδος της κρυπτογράφησης έχει τη δυνατότητα να αποτρέπει κίνδυνους υποκλοπής.

- Το πρωτόκολλο Secure Socket Layer είναι ένα εργαλείο ασφάλειας της ιδιωτικότητας και ακεραιότητας των δεδομένων που μεταφέρονται μέσω διαδικτύου.

- Το τείχος προστασίας είναι το λογισμικό που τοποθετείται μεταξύ του διαδικτύου και των υπό πρόσβαση δικτύων.

- Οι μέθοδοι/εργαλεία που χρησιμοποιούν οι τουριστικές επιχειρήσεις ώστε τα προωθήσουν τα τουριστικά τους προϊόντα είναι το web-site, το search engine marketing, το pay per click, το banner marketing, το blog marketing, το e-zine, τα συστήματα διαχείρισης πελατειακών σχέσεων, το sponsorships, το viral marketing και το e-mail marketing.

- Τα social media στον τουριστικό τομέα παρέχουν επιπλέον διαφήμιση, αυξημένα ποσοστά φήμης και ισχυροποίηση του brand name.

- Τα πιο γνωστά social media και προγράμματα τουριστικών προϊόντων στις τουριστικές επιχειρήσεις είναι το Facebook, το Youtube, το Flictr, το Twitter, το Linkend in, το Pinterest, το Google plus, το booking, το Trip Advisor, το Airbnb και το Trivago.

- Η μεγαλύτερη μερίδα του καταναλωτικού κοινού χρησιμοποιεί τις ηλεκτρονικές συναλλαγές για την εξυπηρέτησή της.

- Το μεγαλύτερο ποσοστό χρήσης των ηλεκτρονικών συναλλαγών για διακοπές, χρησιμοποιείται με σκοπό να κλείσουν κάποιο ξενοδοχείο.

Βιβλιογραφία

Laudon K., Traver C., (2011)., *Ηλεκτρονικό Εμπόριο.*, Εκδόσεις: Παπασωτηρίου., 7η έκδοση., Αθήνα.

Efraim Turban, JaeLee, DavidKing, MichaelChung, Ηλεκτρονικό εμπόριο: Αρχές, Εξελίξεις, Στρατηγική από τη σκοπιά του manager, Έκδοση Μ. Γκιούρδας Αθήνα 2002

Κάτσικας Σωκράτης Κ., Γκριτζάλης Δ., Γκριτζάλης Σ. (2004), *Ασφάλεια Πληροφοριακών Συστημάτων.,* Εκδόσεις Νέων Τεχνολογιών

Davis G.B., Olson M.H., (1985)., *Management Information Systems, conceptual foundation, structure and development.,* 2nd., New York., McGraw-Hill.

Laudon, K. C., Laudon, J.P. (2009)., *Πληροφοριακά Συστήματα Διοίκησης*., Εκδόσεις: Κλειδάριθμος

Αναστασιάδης, Π. (2000),, *Στον Αιώνα της Πληροφορίας*., Αθήνα., Εκδόσεις: Λιβάνη**.**

Παγκάλος Γ., Μαυρίδης Ι. (2002)., *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.*, Εκδόσεις Ανικούλα.

Τσάμης, Α. (2003)., *Εξελίξεις, διαπιστώσεις και διλήμματα στη σύγχρονη ηλεκτρονική τραπεζική.*, Δελτίο Ένωσης Ελληνικών Τραπεζών.

Αγγέλης, Β. (2005)., *Η βίβλος του e-banking*., Αθήνα: Εκδόσεις Νέων Τεχνολογιών ΕΠΕ

Σινανιώτη – Μαρούδη Αριστέα., Φαρσαρώτας Ιωάννης Δ., (2005)., *Ηλεκτρονική Τραπεζική*., Εκδόσεις: Σάκκουλα

http://www.ecb.europa.eu, 2003

Παγκάλος Γ. & Μαυρίδης Ι. (2002)., *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.,* Εκδόσεις: Ανικούλα

Αλεξανδρής Ν., Γκρίτζαλης Δ., Κιουντούζης Ε. (1995)., *Μια προσέγγιση της κοινωνικά αποδεκτής αξιοποίησης της Πληροφορικής σε ΕΠΥ, Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα.*, Αθήνα

Κάτσικας Σωκράτης Κ., Γκριτζάλης Δ., Γκριτζάλης Σ. (2003)., *Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε Περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης*., Αθήνα: Εκδόσεις Παπασωτηρίου

Καλαϊτζής Σωκράτης (1998)., *Η διαφήμιση όπως θα θέλατε να την ξέρετε.,* Εκδόσεις:Leader Books., Αθήνα

Κοκκώσης Χ., Τσάρτας Π., (2001)., *Βιώσιμη Τουριστική Ανάπτυξη και Περιβάλλον.,* Εκδόσεις: Κριτική

Sigalas., M. Mich., S. Murphy (2007)., *Information and Communication Technologies in Tourism.,* 1st Ed: Editor Springer., New York

Buhalis D. (2003)., *Etourism: Information Technology for Strategic Tourism Management.,* 1st Edition., London

Βλαχόπουλος Μ. (2003)., *E- Marketing/Διαδικτυακό Μάρκετινγκ.,* Εκδόσεις: Rosili., Αθήνα

Eric Schmidt., Jonathan Rosenberg (2015)., *Πως λειτουργεί η Google.,* Εκδόσεις: Rosili., Αθήνα

Trivago (2018)., available at: https://www.trivago.gr/

Wikipedia (2018)., available at: https://en.wikipedia.org/wiki/Trivago

Booking (2018)., available at: https://www.booking.com/index.en-gb.html?

Spooren P., Mortelmans D., Denekens J. (2007)., Student evaluation of teaching quality in higher education: development of an instrument based on 10 Likert-scales., Assessment & Evaluation in Higher Education, 32/6: 667-679.

Παρασκευόπουλος Ιωάννης (1993)., *Μεθοδολογία επιστημονικής έρευνας.,* Εκδόσεις: Αθηνά., Αθήνα

Hasson D., Arnetz B. B. (2007)., Validation and Findings Comparing VAS vs. Likert Scales for Psychosocial Measurements., International Electronic Journal of Health Education, 8: 178-192.

Πάγκαλος Γ., Μαυρίδης Ι. (2003)., *Ασφάλεια πληροφοριακών συστημάτων και δικτύων.,* Εκδόσεις: ΑΝΙΚΟΥΛΑ.

Σινανιώτη – Μαρούδη Α., Φαρσαρώτας Ι. (2005)., *Ηλεκτρονική τραπεζική.,* Εκδόσεις: Σάκκουλας Αντ. Ν.

Matonis J. (2013)., *Bitcoin gaining market – based legitimacy as XBT.,* Coindesk.

Nakamoto S. (2008)., *Bitcoin: A peer – to peer electronic cash system.*

Joyner A. (2014)., *How bitcoin is moving money in Africa.,* Available at : www.usatoday.com.

Skelton A. (2012)., *Pay another way: Bitcoin.,* WordPress.

Franceschi – Bichierai L. (2013)., *Okcuid now accepts bitcoin.,* Mashable.

Dablerg N. (2014)., *TigerDirect.com to accept bitcoin.,* Miami Herald Business., Miami.

Biggs J. (2014)., *Expedia Now Accepts Bitcoin for your cryptovacations.,* Techcrunch.

Παράρτημα