ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

Σχολή Διοίκησης και Οικονομίας

Τμήμα Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ – ΟΔΗΓΟΣ ΔΙΑΣΦΑΛΙΣΗΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΖΗΣ ΕΜΜΑΝΟΥΗΛ
ΠΑΠΠΑΣ ΠΑΝΑΓΙΩΤΗΣ
ΤΣΙΚΟΥΔΑΚΗΣ ΓΕΩΡΓΙΟΣ

Εποπτεύων Καθηγητής Στάμος Κωνσταντίνος

Πάτρα , Οκτώβριος 2011

ΠΡΟΛΟΓΟΣ

Στο πλαίσιο της ολοκλήρωσης των σπουδών μας, στο Τμήμα Επιχειρηματικού Σχεδιασμού & Πληροφοριακών Συστημάτων του Α.Τ.Ε.Ι. Πατρών, συντάξαμε την παρακάτω πτυχιακή εργασία. Το θέμα της πτυχιακής εργασίας είναι η "Ασφάλεια Ηλεκτρονικού Εμπορίου – Οδηγός Διασφάλισης Ηλεκτρονικών Συναλλαγών".

Ο σκοπός αυτής της πτυχιακής είναι αρχικά να καταγραφεί το ποσοστό των ανθρώπων που χρησιμοποιούν το Ίντερνετ για την πραγματοποίηση των αγορών τους και να διατυπωθεί κατά πόσο είναι ασφαλές ή όχι. Στη συνέχεια θα αναφερθούμε στις ευρύτερες έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων και της Κρυπτογράφησης, καθώς και στην Προστασία Προσωπικών Δεδομένων.

Φτάνοντας στο τέλος αυτής της εργασίας , που σηματοδοτεί παράλληλα και την ολοκλήρωση των σπουδών μας στο τμήμα του Επιχειρηματικού Σχεδιασμού & Πληροφοριακών Συστημάτων του Α.Τ.Ε.Ι. Πατρών, νιώθουμε την ανάγκη να ευχαριστήσουμε τους ανθρώπους που μας βοήθησαν και μας στήριξαν σε αυτή την προσπάθεια.

Πρώτα απ' όλα πρέπει να ευχαριστήσουμε όσους συμμετείχαν εθελοντικά στην έρευνά μας, τις οικογένειές μας, που στήριξαν και συνεχίζουν να στηρίζουν τις επιλογές μας , χωρίς ενδοιασμούς .

Επίσης θερμά θέλουμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή μας , Στάμο Κωνσταντίνο, για την πολύτιμη αρωγή και καθοδήγησή του στην εκπόνηση της παρούσας εργασίας.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ειδικεύεται πάνω στην ασφάλεια των πληροφοριακών συστημάτων στην Ελληνική πραγματικότητα. Ακόμα γίνεται θεωρητική ανάλυση όσον αφορά τον χρήστη, τα αγαθά, την προσπέλαση των δεδομένων και την ασφάλεια των πληροφοριών.

Παραθέτονται οι ευρύτερες έννοιες της κρυπτογραφίας αλλά και των ειδών κρυπτογράφησης. Ακόμα, αναλύονται έννοιες της αυθεντικοποίησης και ταυτοποίησης των χρηστών, με τα θετικά και τα αρνητικά τους στοιχεία. Επιπλέον γίνεται εκτενής αναφορά στα βιομετρικά συστήματα και την χρησιμότητά τους όπως και στην καταχώρηση και αποθήκευση των δεδομένων του χρήστη, ενώ συμπεριλαμβάνεται και μια αναφορά στην αρχή προστασίας προσωπικών δεδομένων.

Παρουσιάζεται ένα ερωτηματολόγιο στο οποίο ανταποκρίνονται άτομα από διάφορα μορφωτικά και ηλικιακά επίπεδα. Το ερωτηματολόγιο, μελετά το ποσοστό του Έλληνα χρήστη του διαδικτύου, που έχει γενικές γνώσεις πάνω στους ηλεκτρονικούς υπολογιστές και την θεωρία του. Αν γνωρίζει τι είναι ηλεκτρονική ασφάλεια, κατά πόσο χρησιμοποιεί στην καθημερινότητα του έναν ηλεκτρονικό υπολογιστή και αν κάνει με αυτόν ηλεκτρονικές συναλλαγές.

Καταλήγει σε ένα λίγο-πολύ γνωστό συμπέρασμα ότι, ο Έλληνας είναι γνώστης των ηλεκτρονικών υπολογιστών, γνωρίζει θεωρητικά πράγματα που τον κάνουν να κινείται ακόμα δειλά πάνω στις ηλεκτρονικές συναλλαγές και κυρίως στις αγορές, κάτι που φαίνεται σε σύγκριση με αντίστοιχα ερωτηματολόγια που τέθηκαν σε άλλες χώρες.

Παρά την προσπάθεια που κάνουν οι διάφοροι φορείς για την ανάπτυξη του ηλεκτρονικού εμπορίου χρειάζεται ακόμα αρκετή προσπάθεια τόσο από τους εμπόρους όσο και από τις τράπεζες έτσι ώστε να παρέχεται η απαραίτητή ανταγωνιστικότητα στις τιμές και πλήρης ασφάλεια. Ο χρήστης θα είναι σε θέση να επενδύσει τον χρόνο του και να προβεί σε μια ηλεκτρονική αγορά, ενώ παράλληλα εάν μείνει ικανοποιημένος να συνεχίσει να προμηθεύεται αγαθά μέσω του ηλεκτρονικού εμπορίου.

Οι ηλεκτρονικές συναλλαγές προσπαθούν να καθιερωθούν στο διαδικτυακό χώρο και διαγράφουν σημαντική πορεία προς την καθιέρωση εντούτοις, ελλοχεύουν κίνδυνοι για τον μη ενημερωμένο χρήστη αλλά είναι βέβαιο πως στο εγγύ μέλλον θα λάβουμε τα επιθυμητά αποτελέσματα.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΡΕΥΝΑ – ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

ΕΙΣΑΓΩΓΗ

Ο αιώνας που διανύουμε έχει χαρακτηριστεί ως αιώνας της πληροφόρησης. Ανέκαθεν οι άνθρωποι αναζητούσαν τρόπους να μεταφέρουν πληροφορίες και μηνύματα με ασφάλεια, χωρίς να κινδυνεύουν από παραποίηση ή υποκλοπή του περιεχομένου τους. Έτσι και στη σημερινή εποχή, η ανάγκη των ανθρώπων για ασφαλή και έγκυρη επικοινωνία δεν αποτελεί αποκλειστικά χαρακτηριστικό γνώρισμα.

Στις μέρες μας μπορούμε να επικοινωνούμε με ανθρώπους από όλον τον πλανήτη με κόστος μόνο την πρόσβαση στο διαδίκτυο. Διανοίχθηκαν νέες προοπτικές για το εμπόριο με την αναβίωση των καταστημάτων ταχυδρομικής αποστολής με τη μόνη διαφορά ότι η επιλογή των αγαθών δεν γίνεται πλέον μέσα από έναν κατάλογο που ταχυδρομήθηκε πριν ένα μήνα το λιγότερο, αλλά μέσα από μια σελίδα του διαδικτύου που ενημερώνεται σε καθημερινή βάση και αδιαλείπτως.

Η εφαρμογή τεχνολογιών πληροφορικής ενέχει κινδύνους, τους οποίους αναλαμβάνουν να μετριάσουν κατάλληλοι μηχανισμοί ασφάλειας. Κεντρικό ρόλο στην ασφάλεια ηλεκτρονικής διακυβέρνησης διαδραματίζουν οι έξυπνες κάρτες και οι Υποδομές Δημόσιου Κλειδιού. Οι έξυπνες κάρτες σε συνδυασμό με τις Υποδομές Δημόσιου Κλειδιού υπό την εποπτεία του Κράτους, μπορούν να υλοποιήσουν την ηλεκτρονική ταυτότητα. Συγκεκριμένα η ηλεκτρονική ταυτότητα αποτελεί το θεμέλιο της ασφάλειας στο πλαίσιο της ηλεκτρονικής διακυβέρνησης, καθώς επιτρέπει την ασφαλή πρόσβαση στις ηλεκτρονικές υπηρεσίες, την προστασία του ιδιωτικού χαρακτήρα των δεδομένων μέσω κρυπτογράφησης, τη δημιουργία και την επαλήθευση των ψηφιακών υπογραφών.

Είναι ξεκάθαρο, πως κύριο τροχοπέδη του διαδικτύου αποτελεί η ασφάλεια στο Internet. Θα περιγράψουμε μια από τις κύριες τεχνικές που χρησιμοποιούνται για ασφάλεια: την κρυπτογραφία. Επίσης εξετάζουμε μερικές τεχνολογίες, που βασίζονται στην κρυπτογραφία και μερικά εργαλεία λογισμικού, τα οποία χρησιμοποιούνται για να προστατέψουν ένα σύστημα (Kerberos).

Η συνεχής αυξανόμενη απαίτηση της Κοινωνίας της Πληροφορίας για ασφαλή και υγιή δίκτυα επικοινωνιών σε συνδυασμό με την πολλά υποσχόμενη τεχνολογία των έξυπνων καρτών σε επίπεδο ασφάλειας και αξιοπιστίας των δεδομένων που αποθηκεύουν όπως επίσης και των λειτουργιών που μπορούν να εκτελέσουν, πρόκειται να αποτελέσουν ένα δυναμικό συνδυασμό ασφάλειας για την επιστήμη των δικτύων, με ευεργετικά αποτελέσματα για τα επόμενα χρόνια.

1. Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση

Στο παρόν κεφάλαιο περιγράφονται οι βασικότερες έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων και Υποδομών. Οι έννοιες αυτές θα χρησιμοποιηθούν στη συνέχεια για την ομαδοποίηση επιμέρους όρων-εννοιων της γνωστικής αυτής περιοχής για την περιγραφή των όρων αυτών, καθώς και για την εννοιολογική συσχέτισή τους.

Η Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών αφορά οντότητες και αντικείμενα που αξίζει να προστατευθούν. Οτιδήποτε αξίζει να προστατευθεί ονομάζεται αγαθό (asset). Τα αγαθά αξίζουν να προστατευθούν επειδή έχουν αξία (value) και η αξία τους μπορεί να μειωθεί εάν υποστούν ζημιά. Τα αγαθά χρειάζονται προστασία μόνον εάν υπάρχουν κίνδυνοι (dangers) που μπορεί να τους προκαλέσουν ζημιά (harm). Ο ιδιοκτήτης (owner) ενός προστατευόμενου Αγαθού χρησιμοποιεί Μέσα Προστασίας (safeguards) είτε για να μειώσει τον κίνδυνο να προξενήσει ζημιά στο αγαθό είτε για να μειώσει τις συνέπειες της.

Παρόλα αυτά η χρήση Μέσων Προστασίας επιφέρει Κόστος. Δεδομένου του γεγονότος, ότι τα Μέσα Προστασίας δεν μπορούν να εγγυηθούν πλήρη ασφάλεια, το κόστος τους πρέπει να αναλογεί στην Επισφάλεια(Hazard) του Αγαθού αυτού, καθώς και στις συνέπειες που θα έχει μια ζημιά στον ιδιοκτήτη του. Ο ιδιοκτήτης είναι εκείνος που θα κρίνει όταν θέτει το Στόχο Ασφαλείας (Infosec goal), ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο Κόστος και την Επισφάλιση (Assurance). Έτσι θα είναι σίγουρος ότι ο στόχος του θα επιτευχθεί με τα Μέσα Προστασίας που θα χρησιμοποιήσει.

Αφού τα αγαθά υπάρχουν για να αξιοποιούνται, αρκετό ενδιαφέρον αποκτά η έννοια τόσο του Χρήστη όσο και του Ιδιοκτήτη τους. Κάθε αγαθό έχει Ιδιοκτήτες (Attributes) οι οποίοι πρέπει να προστατευθούν. Οι ζημιές που μπορεί να προκληθούν από Κινδύνους, αφορούν Ζημιές όχι στα Αγαθά, αλλά στις Ιδιότητές τους. Οι ζημιές εκτιμούνται από τον Ιδιοκτήτη ή το Χρήστη. Αρχικά ο Ιδιοκτήτης είναι αυτός που θα καθορίσει τους Στόχους, οι οποίοι προσδιορίζουν τη μέγιστη ανεκτή Ζημιά που οι Ιδιότητες μπορούν να υποστούν. Στη συνέχεια τα Μέσα Προστασίας αντιμετωπίζουν του Κινδύνους αποτρέποντας τις ζημιές και προστατεύουν τις Ιδιότητες και τα Αγαθά. Τέλος ο Όρος Εξασφάλιση υπονοεί ότι τα Μέσα Προστασίας μπορούν να αντιμετωπίσουν τους Κινδύνους προστατεύοντας τα Αγαθά και τις Ιδιότητες τους από Ζημιές.

Ακλουθώντας την παραπάνω τακτική θα μπορούσαμε να κάνουμε μια περιδιάβαση στις περισσότερες έννοιες της γνωστικής περιοχής. Στη συνέχεια θα εργαστούμε πιο συγκεκριμένα πάνω στην Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών.[1]

1.1 Αγαθά

Τα αγαθά που μας ενδιαφέρουν είναι δύο ειδών, η πληροφορία (η τα δεδομένα) και οι υπολογιστικοί ή άλλοι πόροι που χρησιμοποιούμε για να επεξεργαστούμε τις πληροφορίες και τα δεδομένα. Η ταξινόμηση αυτή είναι σημαντική επειδή οι κίνδυνοι που αντιμετωπίζει ένα Αγαθό, η Ζημιά που μπορεί να προκληθεί, καθώς και τα μέσα προστασίας για να αντιμετωπιστούν οι Κίνδυνοι και οι Ζημιές είναι διαφορετικά για κάθε είδος Αγαθού.

Ορισμοί:

- **Δεδομένα** (Data) Ένα σύνολο κατανοητών συμβόλων που έχουν καταγραφεί.

- **Πληροφορία** (Information) Τα δεδομένα μαζί με την έννοια που τους αποδίδεται.

Οι έννοιες Πληροφοριακό Σύστημα, Υπολογιστικό Σύστημα και Υπολογιστικό Συγκρότημα συγκροτούν μια ιεραρχία όρων, στην οποία το Πληροφοριακό Σύστημα βρίσκεται στο υψηλότερο επίπεδο και το Υπολογιστικό Συγκρότημα στο χαμηλότερο. Ένα Υπολογιστικό Σύστημα ορίζεται μέσω του Υπολογιστικού Συγκροτήματος και ένα πληροφοριακό Σύστημα ορίζεται μέσω Υπολογιστικού Συστήματος.

Ένα Υπολογιστικό Συγκρότημα αποτελεί μόνο μια συλλογή από υπολογιστικά και άλλα στοιχεία τα οποία ως σύνολο είναι από μόνα τους ικανά να επεξεργασθούν πληροφορίες και να παράσχουν ένα επίπεδο λειτουργικότητας.

Ένα Υπολογιστικό Σύστημα εκτός από τα τεχνικά συστατικά του και ένα λειτουργικό περιβάλλον. Στο πλαίσιο αυτό περιλαμβάνονται και οι άνθρωποι που κρίνονται απαραίτητοι στη λειτουργία των τεχνικών μερών του συστήματος και ονομάζονται Υπολογιστικοί Πόροι.

Ένα Πληροφοριακό Σύστημα περιλαμβάνει όλα τα τεχνικά συστατικά του Υπολογιστικού Συγκροτήματος, όπως για παράδειγμα το περιβάλλον στο οποίο λειτουργεί το σύστημα, το σκοπό αλλά και επιπλέον πληροφορίες.

Ακόμη, οι Υπολογιστικοί Πόροι περιλαμβάνουν κάθε στοιχείο του Υπολογιστικού Συστήματος, εκτός από τις Πληροφορίες ή τα δεδομένα που διαχειρίζεται. Αντίθετα, με το Υπολογιστικό Συγκρότημα, οι Υπολογιστικοί Πόροι δεν είναι απαραίτητο να διαχειρίζονται τις Πληροφορίες από μόνοι τους, με την προϋπόθεση πως είναι σε θέση να το πραγματοποιούν σε συνδυασμό με τη συνεργασία άλλων Υπολογιστικών Πόρων. Ένα Υπολογιστικό Συγκρότημα και ένα Υπολογιστικό Σύστημα είναι και τα δυο παραδείγματα

Υπολογιστικών Πόρων. Από την άλλη πλευρά ένα Πληροφοριακό Σύστημα δεν είναι Υπολογιστικός Πόρος.

Η Εφαρμογή είναι ένας συνδυασμός Υπολογιστικών Πόρων και Πληροφοριών.

Το Υπολογιστικό Αντικείμενο ορίζεται ως κάθε μέρος ενός συνόλου που αποτελείται από:

i. Υπολογιστικό Συγκρότημα.

ii. Υπολογιστικό Σύστημα.

iii. Πληροφοριακό Σύστημα.

iv. Υπολογιστικό Εξάρτημα.

v. Υπολογιστικό Προϊόν.

Ορισμοί:

- **Εφαρμογή** (Application) Πληροφορίες, λογισμικό και διαδικασίες που έχουν σχεδιαστεί για την επίτευξη συγκεκριμένων στόχων.

- **Υπολογιστικό Αντικείμενο** (IT Object) Υπολογιστικό Συγκρότημα ή υπολογιστικό σύστημα ή πληροφοριακό σύστημα ή υπολογιστικό εξάρτημα ή προϊόν.

- **Αξία** (Value) Σπουδαιότητα εκφραζόμενη σε χρηματικούς ή άλλους όρους.

- **Αγαθό** (Asset) Πληροφορίες, δεδομένα ή υπολογιστικοί πόροι που έχουν αξία.[1]

1.2 Ιδιοκτήτης και Χρήστης

Αν τα Αγαθά έχουν Αξία, αυτό σημαίνει ότι ανήκουν σε κάποιον και θα χρησιμοποιηθούν για κάποιο σκοπό. Στο σημείο αυτό εισάγονται οι έννοιες του Ιδιοκτήτη και του Χρήστη, οι οποίοι δεν είναι απαραίτητο να είναι υπαρκτά πρόσωπα. Η αστική έννοια της ιδιοκτησίας συνεπάγεται πως ο Χρήστης έχει το δικαίωμα να καθορίζει τον τρόπο διαχείρισης των Αγαθών.

Ορισμοί:

- **Ιδιοκτήτης** Πρόσωπο που κατέχει η είναι υπεύθυνο για ένα αγαθό και που έχει το δικαίωμα να καθορίσει πως μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί.

- **Εξουσιοδότηση** Άδεια που παρέχεται από έναν ιδιοκτήτη για κάποιο σκοπό.

- **Εξουσιοδοτημένος** Με την άδεια του ιδιοκτήτη για κάποιο σκοπό.

- **Μη Εξουσιοδοτημένος** Χωρίς την άδεια του ιδιοκτήτη για κάποιο σκοπό.

- **Χρήστης** Πρόσωπο ή διεργασία που χρησιμοποιεί ολόκληρο ή μέρος του πληροφοριακού συστήματος.[1]

1.3 Ιδιότητες

Δεν έχει νόημα να υπάρχουν Αγαθά αν δεν μπορούν να χρησιμοποιηθούν έτσι ώστε να εκπληρωθεί κάποιος σκοπός. Τα περισσότερα Αγαθά που έχουν σχέση με τα Πληροφοριακά Συστήματα χρησιμοποιούνται για να παράσχουν κάποιου είδους Υπηρεσίες.

Συχνά απαιτείται η συνεχής παροχή Υπηρεσιών στους Εξουσιοδοτημένους Χρήστες καθώς και η προστασία τους από τους Μη Εξουσιοδοτημένους. Για να αξιοποιηθεί ένα Αγαθό από ένα Χρήστη, πρέπει ο Χρήστης να μπορεί να το προσπελάσει. Υπάρχουν 2 είδη

Προσπέλασης: Προσπέλαση Πληροφορίας και Προσπέλαση Συστήματος.

Ορισμοί:

- **Προσπέλαση** (Access) Η δυνατότητα μια οντότητας να αξιοποιεί πληροφορίες ή υπολογιστικούς πόρους στο πλαίσιο ενός πληροφοριακού συστήματος.

- **Προσπέλαση Πληροφορίας** (Information Access) Η δυνατότητα κάποιου να χρησιμοποιεί συγκεκριμένες πληροφορίες ενός πληροφοριακού συστήματος.

- **Προσπέλαση Συστήματος** (System Access) Η δυνατότητα κάποιου να χρησιμοποιεί υπολογιστικούς πόρους στο πλαίσιο ενός πληροφοριακού συστήματος.

Στο παρακάτω πλαίσιο παρουσιάζεται η ταξινόμηση των ιδιοτήτων όπως προαναφέρθηκαν.

	Περιορίζουν	**Επιτρέπουν**	**Ουδέτεροι/Μικτοί**
Πληροφορία	Εμπιστευτικότητα Ακεραιότητα Αυθεντικότητα	Διαθεσιμότητα Πληροφοριών Εγκυρότητα	Προσπέλαση Πληροφοριών Ασφάλεια Ασφάλεια Πληροφοριών

Υπολογιστικοί Πόροι		Διαθεσιμότητα Συστήματος	Προσπέλαση Συστήματος Ασφάλεια Υπολογιστικού Συστήματος
Πληροφοριακό Σύστημα		Διαθεσιμότητα	Προσπέλαση Ασφάλεια Πληροφοριακών Συστημάτων

Ορισμοί:

- **Ακεραιότητα** (Integrity) Αποφυγή μη εξουσιοδοτημένης τροποποίησης μια πληροφορίας.

- **Αυθεντικότητα** (Authenticity) Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια εξουσιοδοτημένων τροποποιήσεων μιας πληροφορίας.

- **Εγκυρότητα** (Validity) Απόλυτη ακρίβεια και πληρότητα μια πληροφορίας.

- **Διαθεσιμότητα Πληροφοριών** (Information Availability) Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.

- **Εμπιστευτικότητα** (Confidentiality) Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους.

- **Ασφάλεια** (Security) Προστασία της διαθεσιμότητας πληροφοριών, της ακεραιότητας και της εμπιστευτικότητας.

- **Ασφάλεια Πληροφοριών** (Information Security) Διασφάλιση εμπιστευτικότητας, εγκυρότητας, αυθεντικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών.

- **Διαθεσιμότητα Συστήματος** (System Availability) Αποτροπή της μη διάθεσης υπολογιστικών πόρων σε εξουσιοδοτημένους χρήστες.

- **Ασφάλεια Υπολογιστικού Συστήματος** (IT System Security) Διασφάλιση διαθεσιμότητας συστήματος και ασφάλειας πληροφοριών, καθώς και των παραμέτρων που αποτελούν τμήμα του υπολογιστικού συστήματος.

- **Ασφάλεια Πληροφοριακού Συστήματος** (Information System Security) Ασφάλεια πληροφοριών και υπολογιστικού συστήματος για δεδομένο πληροφοριακό σύστημα.

- **Διαθεσιμότητα** (Availability) Αποφυγή μη εύλογων καθυστερήσεων στην εξουσιοδοτημένη προσπέλαση πληροφοριών ή υπολογιστικών πόρων.[1]

1.4 Ζημιά

Είναι ο περιορισμός μιας ή περισσοτέρων από τις Ιδιότητες των αγαθών που χρήζουν προστασίας. (π.χ. Απώλεια Εμπιστευτικότητας, Απώλεια Διαθεσιμότητας.) Οι σχετικές έννοιες με την Ζημιά μπορούν να κατανεμηθούν σε εκείνες που έχουν σχέση περισσότερο.[1]

2. Κρυπτογράφηση

2.1 Ιστορική Αναδρομή Κρυπτογραφίας

Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα βρίσκοντας αναφορές της στον ιστορικό Πολύβιο ενώ συνεχίζονται εώς και τον Ιούλιο Καίσαρα. Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. «3» , δηλαδή η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα το οποίο βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Διατηρώντας λοιπόν τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Ο πίνακας αντιστοίχισης των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα : **a b c d e f g h i j k v m n o p q r s t u v w x y z**

Αντικαθίσταται από το γράμμα: **d e f g h i j k l m n o p q r s t u v w x y z a b c**

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, το οποίο σε αυτήν την περίπτωση είναι ο αριθμός 3 .

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και εκείνων που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Αυτό είχε ως απόρροια η κρυπτογραφία να περάσει στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η

κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά, τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους.

Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι ποικίλα. Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας με σκοπό να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών.

Δεν θα ήταν υπερβολή, να πούμε, ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξαιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Από την δεκαετία του 60 και έπειτα, η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη εξαιτίας της ραγδαίας ανάπτυξης των υπολογιστών, αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν, δημιουργήθηκε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή. Αρχίζοντας με την εργασία του Feistel στην IBM στις αρχές της δεκαετίας του '70 και καταλήγοντας το 1977 με την υιοθέτηση του Αμερικανικού ομοσπονδιακού προτύπου για την επεξεργασία των πληροφοριών την κρυπτογράφηση των μη-διαβαθμισμένων πληροφοριών, DES, το πρότυπο κρυπτογράφησης στοιχείων, είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός της ιστορίας. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο. Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε αργότερα το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Η συγκεκριμένη επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια της κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή ήταν γεγονός και το θέμα κρίθηκε μείζονος σημασίας από την κρυπτογραφική κοινότητα. Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος, το λεγόμενο σχήμα RSA και βασιζόμενο σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό, οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης.

Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές! Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν η *ψηφιακή υπογραφή*.

2.2 Βασικές Έννοιες Κρυπτογραφίας

Οι ευρύτερα χρησιμοποιούμενες σήμερα τεχνολογίες για την ικανοποίηση βασικών απαιτήσεων ασφάλειας βασίζονται στην κρυπτογράφηση των ανταλλασσόμενων μηνυμάτων.

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.

Ως Κρυπτογράφηση (Encryption) ορίζεται ο μετασχηματισμός του αρχικού μηνύματος ή της πληροφορίας του αποστολέα σε μία εναλλακτική μορφή, η οποία μπορεί κατόπιν να αντιστραφεί για να επανέλθει στην αρχική της μορφή. Η εναλλακτική μορφή αναφέρεται σαν κρυπτογραφημένο κείμενο (ciphertext) ή απλώς κρυπτογράφημα ή και κρυπτομήνυμα και συνήθως δημιουργείται με την χρήση ενός αλγορίθμου και ενός κλειδιού κρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης είναι ένας μαθηματικός τύπος ο οποίος εφαρμόζεται στην πληροφορία που θέλει ο συναλλασσόμενος ή και χρήστης ενός επικοινωνιακού συστήματος της Δημόσιας Διοίκησης να κρυπτογραφήσει. Το κλειδί κρυπτογράφησης είναι μία επιπλέον μεταβλητή η οποία «εμφυτεύεται» στον αλγόριθμο κρυπτογράφησης για να διασφαλίσει το γεγονός ότι το κρυπτογράφημα δεν θα παράγεται με την ίδια ακριβώς ακολουθία υπολογισμών κάθε φορά που χρησιμοποιείται ο αλγόριθμος.[2]

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

Για την Κρυπτογράφηση ενός μηνύματος ή πληροφορίας απαιτούνται:

α) ένας Αλγόριθμος Κρυπτογράφησης (Encryption Algorithm) βάσει του οποίου από το αρχικό μήνυμα m υπολογίζεται το κρυπτομήνυμα E(m), και

β) ένα Κλειδί Κρυπτογράφησης (Encryption Key) το οποίο αποτελείται από μία σειρά χαρακτήρων ή bit, το οποίο χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης για τον υπολογισμό του κρυπτομηνύματος E(m). Άρα το κρυπτογραφημένο κείμενο είναι συνάρτηση τόσο του αρχικού μηνύματος όσο και του κλειδιού κρυπτογράφησης.

Ομοίως για την Αποκρυπτογράφηση ενός μηνύματος απαιτούνται:

α) ένας Αλγόριθμος Αποκρυπτογράφησης (Decryption Algorithm), βάσει του οποίου από το κρυπτομήνυμα E(m) υπολογίζεται το αρχικό μήνυμα m, και

β) ένα Κλειδί Αποκρυπτογράφησης (Decryption Key) το οποίο αποτελείται από μία σειρά χαρακτήρων ή bit, η οποία χρησιμοποιείται από τον αλγόριθμο αποκρυπτογράφησης για τον υπολογισμό του αρχικού μηνύματος m. Συνεπώς, κατά την αποκρυπτογράφηση το αρχικό μήνυμα υπολογίζεται ως συνάρτηση του κρυπτομηνύματος και του κλειδιού αποκρυπτογράφησης.

2.3 Συμμετρική/Ασύμμετρη Κρυπτογράφηση

Γενικότερα τόσο ο αλγόριθμος κρυπτογράφησης όσο και ο αλγόριθμος αποκρυπτογράφησης είναι ευρέως γνωστοί εν αντιθέσει με τα αντίστοιχα κλειδιά που αναφέρθηκαν παραπάνω. Με βάση αυτό το δεδομένο μπορούμε να διακρίνουμε δύο βασικά είδη κρυπτογράφησης, την:

a. ***Συμμετρική Κρυπτογράφηση*** ή ***Κρυπτογραφία Ιδιωτικού Κλειδιού*** (Symmetric Encryption-Private Key Encryption), της οποίας βασικό χαρακτηριστικό είναι ότι τόσο ο αποστολέας όσο και ο αποδέκτης του μηνύματος χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση αντιστοίχως του μηνύματος. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, μερικοί από αυτούς είναι οι εξής:

i. **DES**: Είναι ο περισσότερο γνωστός αλγόριθμος (**Data Encryption Standard**), ο οποίος όπως προαναφέρθηκε υιοθετήθηκε από την κυβέρνηση των Η.Π.Α., ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών. Ο DES μετασχηματίζει μπλοκ χαρακτήρων αντί για απλούς χαρακτήρες. Χρησιμοποιεί κλειδί μεγέθους 56 bit και μπορεί να λειτουργήσει με διάφορους τρόπους ανάλογα με το επίπεδο ασφαλείας που απαιτείται. Ο DES είναι ένας αρκετά ισχυρός αλγόριθμος κρυπτογράφησης, ωστόσο κάποιοι εμπειρογνώμονες ασφαλείας λένε πως μπορεί να σπάσει από έναν υπολογιστή ειδικού σκοπού σχεδιασμένο για το σπάσιμο κωδικών. Ένα ακόμα

πρόβλημα που παρουσιάζει όμως αυτή η τεχνική, είναι η διανομή των κλειδιών. Η εξασφάλιση δηλαδή, ότι τα κλειδιά που αποστέλλονται στους παραλήπτες που θα τα χρησιμοποιήσουν, δεν θα πέσουν σε λάθος χέρια. Κατά αυτόν τον τρόπο τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT. Η πιστοποίηση του DES ανακλήθηκε το 1998 και αντικαταστάθηκε από έναν άλλο αλγόριθμο γνωστό ως 3DES.

ii. ***Τριπλό DES***: Όπως είναι προφανές και από το όνομα του, αυτός είναι ο αλγόριθμος είναι μια παραλλαγή του DES. Γίνεται με την επανάληψη τρεις φορές του DES σε απλό κείμενο. Ο αλγόριθμος αυτός χρησιμοποιήθηκε από οικονομικούς οργανισμούς όπως τράπεζες σαν μια πιο ασφαλής λύση από τον DES.

iii. ***Blowfish:*** Αυτός είναι ένας αλγόριθμος που χρησιμοποιεί κλειδί μήκους 448 bit. Δεν υπάρχει πατέντα για αυτό τον αλγόριθμο και μπορεί να χρησιμοποιηθεί από οποιονδήποτε.

iv. ***IDEA***: Αυτός είναι ένας αλγόριθμος που αναπτύχθηκε στην Ελβετία και δημοσιοποιήθηκε το 1990. Χρησιμοποιεί ένα κλειδί μεγέθους 128 bit και δεν είναι πατενταρισμένος.

v. ***RC2***: Αυτός είναι ένας αλγόριθμος που αναπτύχθηκε από τον αμερικανό ερευνητή συστημάτων ασφαλείας Ronald Rivest. Μετασχηματίζει μπλοκ δεδομένων και χρησιμοποιεί ένα κλειδί μεγέθους από 1 έως 128 bits.

vi. ***RC4***: Αυτός είναι ένας αλγόριθμος που μετασχηματίζει το αρχικό κείμενο χαρακτήρα - χαρακτήρα. Αρχικά ήταν ένα εμπορικό μυστικό αλλά αργότερα δημοσιεύτηκε το σε ένα newsgroup το 1994. Μπορεί να χρησιμοποιήσει ένα κλειδί μεγέθους μεταξύ 1 και 2048 bits. Τέλος αυτός ο αλγόριθμος, όπως ο RC2, αναπτύχθηκε από τον Ronald Rivest.

vii. ***RC5***: Πρόκειται για έναν αλγόριθμος του Ronald Rivest και αναπτύχθηκε το 1994.

Ευνόητο θεωρείται, ότι όσο ο αριθμός των χρηστών αυτού του συστήματος ασφαλείας μεγαλώνει, μεγαλώνουν και τα προβλήματα της δημιουργίας, της διανομής, της ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών.

και την:

b. ***Ασύμμετρη Κρυπτογραφία*** ή ***Κρυπτογραφία Δημόσιου Κλειδιού*** (Asymmetric Encryption-Public Key Encryption) της οποίας βασικό χαρακτηριστικό είναι ότι το κλειδί που χρησιμοποιεί ο αποστολέας για την κρυπτογράφηση του μηνύματος είναι διαφορετικό από το κλειδί που χρησιμοποιεί ο αποδέκτης για την αποκρυπτογράφηση του μηνύματος.

Χρησιμοποιούνται δηλαδή διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση , το *δημόσιο* (public) και το *ιδιωτικό* (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

-Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.

-Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο. [3]

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

Για να αποκατασταθεί η επικοινωνία με τη χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό ενώ, ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Παράλληλα ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Αναλυτικότερα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό, καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο. Στην περίπτωση αυτή λέμε ότι το μήνυμα είναι κρυπτογραφημένο.

Συμπερασματικά, το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Εν κατακλείδι μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν ενώ, το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση αδυνατεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Ορισμένα άλλα δύσκολά υπολογιστικά προβλήματα προτάθηκαν για κρυπτογραφία δημοσίου κλειδιού. Η ανάλυση όμως ενός μεγάλου αριθμού άντεξε στο χρόνο και είναι η ιδέα η οποία βρίσκεται πίσω από την κρυπτογραφία δημοσίου κλειδιού. Υπάρχουν διάφορες τεχνολογίες και υλοποιήσεις της κρυπτογραφίας δημοσίου κλειδιού. Μερικές είναι οι εξής:

i. **Έξυπνες κάρτες, ιδιωτικά και δημόσια κλειδιά**: Ένας από τους πιο ασφαλείς τρόπους για να διασφαλιστεί η προστασία ενός ιδιωτικού κλειδιού είναι να το αποθηκεύσουμε σε μια έξυπνη κάρτα, αυτές έχουν μέγεθος πιστωτικής κάρτας και περιέχουν και το ιδιωτικό και το δημόσιο κλειδί. Επιπροσθέτως, μπορούν να συνδεθούν με ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί στον υπολογιστή, ώστε αυτός να εκτελέσει την κρυπτογράφηση. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να αποθηκευθεί στον υπολογιστή και ότι όποιος θέλει να αποκτήσει το ιδιωτικό κλειδί πρέπει να κλέψει την κάρτα. Έστω και εάν το παραπάνω συμβεί, είναι πιθανόν να μην μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί καθώς οι έξυπνες κάρτες μπορούν να προγραμματιστούν ώστε να ζητάνε ένα κωδικό πριν δώσουν το δημόσιο κλειδί.

ii. **Ανταλλαγή κλειδιού Diffie-Hellman:** Είναι η πρώτη τεχνολογία που θα εξετάσουμε. Αυτή είναι μια τεχνική για την ανταλλαγή ενός συμμετρικού κλειδιού χρησιμοποιώντας δημόσιο κλειδί. Οι δυο πλευρές που συμμετέχουν σε αυτή τη διαδικασία ανταλλάζουν αρχικά πληροφορίες σχετικά με κάποιο συμμετρικό κλειδί χρησιμοποιώντας μεθόδους δημοσίου κλειδιού και στη συνέχεια θέτουν σε λειτουργεία το συμφωνηθέν κλειδί για να επικοινωνήσουν.

iii. **RSA:** Αυτό είναι σίγουρα το πιο γνωστό σύστημα κρυπτογράφησης δημοσίου κλειδιού, αναπτυγμένο από τρεις καθηγητές στο MIT: τον Ronald Rivest, τον Adi Shamir και τον Leonard Adelman. το RSA μπορεί να χρησιμοποιηθεί για την αποστολή δεδομένων μέσω μιας μη ασφαλούς γραμμής και μπορεί επίσης να βοηθήσει στη δημιουργία ψηφιακών υπογραφών: σειρών χαρακτήρων δηλαδή που πιστοποιούν ότι ο αποστολέας του μηνύματος είναι ο ισχυριζόμενος.

iv. **ElGamel sytem:** Είναι ένα σύστημα δημοσίου κλειδιού που βασίζεται στην ανταλλαγή κλειδιού Diffie-Hellman. Μπορεί επίσης, να χρησιμοποιηθεί για ψηφιακές υπογραφές.

v. **Digital Signature Standard**: Είναι γνωστό ως **DSS**, αναπτύχθηκε από της αμερικανική εθνική υπηρεσία ασφάλειας και υιοθετήθηκε ως πρότυπο από την αμερικανική εθνική υπηρεσία τυποποιήσεων. Στην αρχική του μορφή μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, ωστόσο μπορεί να τροποποιηθεί για κανονική μεταφορά δεδομένων. Η τεχνική αυτή βασίζεται στον αλγόριθμο Digital Signature Algorithm.

Αξίζει σε αυτό το σημείο να συγκρίνουμε τις δυο μεθόδους κρυπτογράφησης:

- Όταν χρησιμοποιούνται αρκετά μεγάλα κλειδιά και οι δυο μέθοδοι είναι ασφαλείς.

- Η κρυπτογραφία δημοσίου κλειδιού είναι ευκολότερο να υλοποιηθεί γιατί δεν χρειάζεται να ανησυχούμε για την μετάδοση κλειδιών μέσω ενός ανασφαλούς δικτύου.

- Η υπολογιστική ισχύς που χρειάζεται για κρυπτογραφία δημοσίου κλειδιού είναι πολύ μεγαλύτερη από αυτή που χρειάζεται για κρυπτογραφία συμμετρικού κλειδιού.

Συνοπτικά, η Ασύμμετρη Κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη Συμμετρική. Χάσκει στο ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης. Αυτό σημαίνει ότι για την μεταφορά μεγάλων ποσοτήτων δεδομένων προτιμούνται συνήθως οι μέθοδοι συμμετρικού κλειδιού.[4]

2.4 Ψηφιακές Υπογραφές (Digital Signatures)

Ψηφιακή υπογραφή είναι κάποια δεδομένα τα οποία με μοναδικό τρόπο προσδιορίζουν κάποιο άτομο ή οργανισμό. Η χρήση ψηφιακών υπογραφών, κατά την ανταλλαγή πληροφοριών, εγγυάται την αυθεντικότητα της ταυτότητας του αποστολέα και την ακεραιότητα της πληροφορίας. Οι ψηφιακές υπογραφές βασίζονται σε συναρτήσεις ανασκόπησης μηνύματος και κρυπτογραφία δημοσίου κλειδιού. Το ιδιωτικό κλειδί χρησιμοποιείται για τη δημιουργία των ψηφιακών υπογραφών, ενώ το δημόσιο κλειδί χρησιμοποιείται για την επαλήθευση της εγκυρότητάς τους.

Για να περιγράψουμε πως λειτουργούν σκεφτείτε την αποστολή από ένα άτομα Α σε ένα άλλο άτομο Β όπου το άτομο Α έχει γνωστοποιήσει το δημόσιο κλειδί του. Υποθέτουμε ότι και οι δυο πλευρές χρησιμοποιούν την ίδια συνάρτηση ανασκόπησης μηνύματος. Τα παρακάτω βήματα γίνονται:

- Το άτομο Α υπολογίζει το αποτέλεσμα της συνάρτησης ανασκόπησης μηνύματος στο μήνυμα που θέλει να στείλει.

- Το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί. Αυτή είναι η ψηφιακή υπογραφή.

- Το μήνυμα μαζί με την ψηφιακή υπογραφή στέλνεται στο άτομο Β.

- Ο Β αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α για να πάρει τον αριθμό ανασκόπησης μηνύματος.

- Ο Β στη συνέχεια υπολογίζει το αποτέλεσμα της συνάρτησης ανασκόπησης μηνύματος (ίδια με αυτή που χρησιμοποίησε ο Α) και το συγκρίνει με την αποκρυπτογραφημένη τιμή. Αν ταιριάζουν το μήνυμα έχει σταλεί πράγματι από τον κάτοχο του κλειδιού που χρησιμοποιήθηκε.

Ένα σημαντικό στοιχείο είναι ότι οι ψηφιακές υπογραφές παρέχουν ακράδαντες αποδείξεις αν κάποιο μήνυμα παραποιήθηκε κατά τη μεταφορά του ή όχι, αλλά δεν κρύβουν το μήνυμα που στάλθηκε και συνεπώς δεν είναι κατάλληλες από μόνες τους όταν απαιτείται προστασία ανάγνωσης του περιεχομένου του μηνύματος από τρίτους.

Απαραίτητη προϋπόθεση για την ταυτοποίηση του αποστολέα, είναι να γνωρίζει με βεβαιότητα ο παραλήπτης, ότι το δημόσιο κλειδί που χρησιμοποιεί για τον έλεγχο εγκυρότητας της ψηφιακής υπογραφής και το αντίστοιχο ιδιωτικό κλειδί ανήκουν πράγματι σε εκείνον, που εμφανίζεται ως αποστολέας του μηνύματος. Διαφορετικά, η ψηφιακή υπογραφή αποδεικνύει μόνο την ακεραιότητα του μηνύματος. Γίνεται, λοιπόν, εμφανής η ανάγκη ύπαρξης ενός μηχανισμού, ο οποίος θα συσχετίζει με μοναδικό και εγγυημένο τρόπο το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί με την οντότητα, στην οποία αυτά ανήκουν. Ο μηχανισμός αυτός είναι τα ψηφιακά πιστοποιητικά (digital certificates) και περιγράφεται στη συνέχεια. Οι πιο γνωστοί αλγόριθμοι ψηφιακών υπογραφών είναι οι RSA και DSA.[5]

2.5 Ψηφιακά Πιστοποιητικά (Digital Certificates)

Ένα πρόβλημα με τα συστήματα δημοσίου κλειδιού είναι ότι ενώ παρέχουν τη δυνατότητα ασφαλούς επικοινωνίας δεν είναι από μόνα τους κατάλληλα για ασφαλή ελεύθερη δημόσια επικοινωνία. Ο λόγος οφείλεται στο ότι δεν υπάρχει τρόπος να πιστοποιηθεί σε ένα εντελώς ανοιχτό περιβάλλον ότι κάποιο άτομο το οποίο ισχυρίζεται ότι έχει ένα συγκεκριμένο κλειδί είναι πράγματι αυτός που λέει. Για παράδειγμα, κάποιος ο οποίος υποστηρίζει ότι έχει το κλειδί που αντιστοιχεί στον πρωθυπουργό ενώ δεν είναι θα μπορεί να διαβάζει μηνύματα τα οποία κάποιοι άλλοι νομίζουν ότι στέλνουν στον πρωθυπουργό.

Για να ξεπεραστεί το πρόβλημα αυτό, έχουν αναπτυχθεί τα ψηφιακά πιστοποιητικά. Ένα ψηφιακό πιστοποιητικό είναι ένα έγγραφο που εκδίδεται από έναν έμπιστο οργανισμό όπως για παράδειγμα τα εθνικά ταχυδρομεία μιας χώρας και που δίνει στοιχεία για έναν χρήστη. Τα ψηφιακά πιστοποιητικά είναι δομές δεδομένων, υπογεγραμμένες ψηφιακά, οι οποίες αντιστοιχίζουν κατά μοναδικό τρόπο, μια οντότητα με το δημόσιο κλειδί της. Το πιστοποιητικό θα περιέχει στοιχεία όπως το όνομα του χρήστη, ένας μοναδικός σειριακός αριθμός και φυσικά το δημόσιο κλειδί του. Το πιστοποιητικό θα έχει επίσης και μια ψηφιακή υπογραφή του οργανισμού που το εξέδωσε. Με σκοπό την πιστοποίηση της αυθεντικότητας ενός ψηφιακού πιστοποιητικού, ο παραλήπτης ενός μηνύματος θα πρέπει να έχει το δημόσιο κλειδί του έμπιστου οργανισμού που το εξέδωσε. Συχνά, πολλά από τα κλειδιά μεγάλων δημοσίων οργανισμών περιλαμβάνονται σε προγράμματα όπως οι browsers. [5]

Αφού έχει ληφθεί ένα πιστοποιητικό, αυτό που καλείται να κάνει κάποιος για να πιστοποιήσει πως υπάρχει αντιστοιχία στο άτομο ή τον οργανισμό που νομίζει, είναι να ακολουθήσει την παρακάτω διαδικασία:

- Ελέγχει ότι η υπογραφή του πιστοποιητικού από την υπηρεσία πιστοποίησης είναι έγκυρη χρησιμοποιώντας το δημόσιο κλειδί της υπηρεσίας πιστοποίησης. Πολλές φορές αυτό θα υπάρχει στον browser, σε περίπτωση που δεν υπάρχει, θα πρέπει να

ανακτηθεί μέσω μιας σειράς ιεραρχικής αναζήτησης από αρχές πιστοποίησης που ήδη γνωρίζουμε.

- Χρησιμοποιεί το δημόσιο κλειδί που υπάρχει στο ψηφιακό πιστοποιητικό για να κρυπτογραφήσει δεδομένα που θέλει να στείλει στον κάτοχο του πιστοποιητικού. Κάποιες φορές τα δεδομένα μπορεί απλά να είναι ένα κλειδί το οποίο θα χρησιμοποιηθεί στη συνέχεια μεταξύ των δυο πλευρών για επικοινωνία μέσω κάποιας απλούστερης μεθόδου συμμετρικού κλειδιού.

Ένα πρακτικό παράδειγμα αποτελούν τα ψηφιακά πιστοποιητικά που σχετίζονται με μια πολύ δημοφιλή τεχνολογία γνωστή ως Secure Sockets Layer (SSL) και η οποία θα περιγραφεί αργότερα. Το SSL συνήθως χρησιμοποιείται για την αποστολή κρυπτογραφημένων μηνυμάτων μεταξύ ενός browser και ενός server,π.χ. για αποστολή στοιχείων πιστωτικών καρτών.

Όταν ένας browser συνδέεται με έναν Web server που χρησιμοποιεί SSL, το πρώτο πράγμα που πραγματοποιείται είναι ότι ο server στέλνει στον browser ένα ψηφιακό πιστοποιητικό τύπου x509.v3 το οποίο περιλαμβάνει το δημόσιο κλειδί του server. Ο browser τότε ελέγχει την εγκυρότητα του πιστοποιητικού εξετάζοντας την ψηφιακή υπογραφή την οποία φέρει. Εάν ο έλεγχος είναι επιτυχής, τότε το δημόσιο κλειδί που υπάρχει μέσα στο πιστοποιητικό χρησιμοποιείται για την αποκωδικοποίηση των αρχικών πληροφοριών που στέλνει ο server για να γίνει η αρχική εγκατάσταση της σύνδεσης. Η αρχική εγκατάσταση της σύνδεσης περιλαμβάνει και κάποια συμφωνία για το πως θα επιτευχθεί στη συνέχεια η επικοινωνία μεταξύ των δυο πλευρών, όπως για παράδειγμα ότι θα χρησιμοποιηθεί κρυπτογραφία συμμετρικού κλειδιού. Ο λόγος για τον οποίο μπορεί να χρησιμοποιηθεί κρυπτογραφία συμμετρικού κλειδιού είναι ότι η επικοινωνία μπορεί να απαιτεί μεταφορά μεγάλου όγκου δεδομένων και συνεπώς η κρυπτογράφηση και αποκρυπτογράφηση δημοσίου κλειδιού μπορεί να είναι υπερβολικά αργή.

Υπάρχουν τέσσερα είδη ψηφιακών υπογραφών που χρησιμοποιούνται στο Internet. Όλα ακολουθούν το πρότυπο x509.v3.

- ***Πιστοποιητικά αρχών πιστοποίησης***. Αυτά χρησιμοποιούνται για την πιστοποίηση μια αρχής πιστοποίησης όπως ταχυδρομικά γραφεία, οργανισμοί τηλεπικοινωνιών κ.λ.π., που μπορούν να εκδώσουν ψηφιακά πιστοποιητικά.

- ***Πιστοποιητικά Server***. Αυτά πιστοποιούν ένα server και αποδεικνύουν ότι είναι αυτός που ισχυρίζεται ότι είναι. Αυτά τα πιστοποιητικά χρησιμοποιούνται σε συνδυασμό με κάποια άλλη τεχνολογία όπως το SSL.

- ***Προσωπικά πιστοποιητικά***. Αυτά πιστοποιούν ξεχωριστά άτομα.

- ***Πιστοποιητικά εταιρειών λογισμικού*.** Αυτά χρησιμοποιούνται για να πιστοποιούν προγράμματα τα οποία πωλούνται και διανέμονται.[6]

2.6 Έλεγχος Προσπέλασης και Εξουσιοδότηση (Access Control and Authorization)

Ο **Έλεγχος Προσπέλασης** είναι μια από τις κυριότερες τεχνολογίες ασφάλειας και αποτελεί μια περιοχή με σπουδαία σημασία για την επίτευξη σημαντικών αποτελεσμάτων σχετικών με την ασφάλεια σε ένα δίκτυο υπολογιστών. Η σχεδίαση και υλοποίηση αποδοτικών συστημάτων ελέγχου προσπέλασης των χρηστών προς τις πληροφορίες που αποθηκεύονται και διακινούνται σε αυτά αποτελεί επομένως σημαντικό βήμα για τη διαμόρφωση ασφαλών συστημάτων δικτύων υπολογιστών.

Συγκεκριμένα, ο έλεγχος προσπέλασης κανονίζει την ανάγνωση, την ενημέρωση, τη δημιουργία και τη διαγραφή των δεδομένων και των προγραμμάτων, αποτρέποντας την έκθεση, τη μετατροπή, τη παραποίηση ή τη καταστροφή τους από εισβολείς του δικτύου με μη *εξουσιοδοτημένη πρόσβαση*. Συγκεντρώνοντας τα παραπάνω, καταλήγουμε στο ότι ο έλεγχος προσπέλασης αποτελεί ένα σημαντικό θέμα που συνδέεται, εκτός από την εμπιστευτικότητα, με την ακεραιότητα και τη διαθεσιμότητα των υπηρεσιών και των δυνατοτήτων που παρέχει ένα τοπικό δίκτυο υπολογιστών στο προσωπικό για παράδειγμα μιας επιχείρησης.[7]

Ο έλεγχος προσπέλασης θα μπορούσαμε να πούμε ότι είναι δίπλευρος:

- Η πρώτη είναι ότι είναι επιθυμητό να μην επιτρέπεται η προσπέλαση

δεδομένων από αυτούς που δεν έχουν το δικαίωμα να το κάνουν.

- και η δεύτερη, εξίσου σημαντική, είναι η ανάγκη να είναι εγγυημένη η δυνατότητα προσπέλασης όλων των σχετικών δεδομένων από τους χρήστες που εφαρμόζουν κατάλληλα τα δικαιώματα προσπέλασης που τους ανήκουν.

Υπάρχει μεγάλη ποικιλία σχετικά με τον τρόπο και την τεχνική που μπορεί κανείς να εξασφαλίσει άρτιο έλεγχο στην προσπέλαση των δεδομένων που διακινούνται μέσω ενός δικτύου. Οι σημαντικότερες μέθοδοι είναι:

- Λίστες Ελέγχου Προσπέλασης – Access Control Lists ACLs.
- Ταυτότητες Ασφαλείας – Security Labels.
- Firewalls.
- Ψηφιακές Υπογραφές – Digital Signatures.

Authorization Requirements: Αυτή η απαίτηση ασφαλείας καθορίζει την παροχή πρόσβασης και τη χρήση δικαιωμάτων (privileges) και πόρων (resources) στους πιστοποιημένους χρήστες. Σκοπός του είναι να επιβεβαιώνει ότι οι χρήστες μπορούν να έχουν πρόσβαση στην πληροφορία αν και μόνο αν έχουν πάρει την εξουσιοδότηση από ένα διορισμένο άτομο. Η **Εξουσιοδοτημένη Πρόσβαση** έχει ως προαπαιτούμενα την αναγνώριση ταυτότητας και την πιστοποίηση αυθεντικότητας.[6]

3. Ταυτοποίηση και Αυθεντικοποίηση

Υπάρχουν πολλές τεχνικές αυθεντικότητας και ταυτοποίησης των χρηστών ενός πληροφοριακού συστήματος. Στην παρούσα ενότητα παρουσιάζονται οι θεμελιώδεις αρχές ταυτοποίησης και αυθεντικότητας καθώς και οι τρόποι με τους οποίους αυτές μπορούν να εφαρμοστούν σε αυτοματοποιημένα περιβάλλοντα. Εφαρμογές οι οποίες συνδράμουν στον έλεγχο της πρόσβασης και στην ορθή επιλογή του καταμερισμού των εξουσιοδοτήσεων των χρηστών, υπηρετούν τις αρχές της εμπιστευτικότητας των πληροφοριών. Πιο αναλυτικά,

παρατίθενται τα σημαντικότερα είδη αυθεντικοποίησης: τα συνθηματικά, τα ψηφιακά πιστοποιητικά, οι έξυπνες κάρτες και οι βιομετρικές μέθοδοι.[8]

3.1 Εισαγωγικές Παρατηρήσεις

Μέρος της ασφάλειας ενός συστήματος αποτελεί ο έλεγχος της ταυτότητας των χρηστών του. Αυτό πραγματοποιείται με την ταυτοποίηση και αυθεντικοποίηση του χρήστη.

- ***Ταυτοποίηση*** *(identification)* ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη κατά την οποία το λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους (resources) του.

- ***Αυθεντικοποίηση*** *(authentication)* ενός λογικού υποκειμένου καλείται η διαδικασία εκείνη κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να ελεχθεί η βασιμότητα της συσχέτισης που επετεύχθητε κατά τη διαδικασία της ταυτοποίησης.

Η ανάγκη αυθεντικοποίησης από ένα σύστημα οφείλεται σε δυο λόγους:

i. Η ταυτότητα του λογικού υποκειμένου αποτελεί παράμετρο για τον έλεγχο προσπέλασης στους πόρους του συστήματος.

ii. Η ταυτότητα του λογικού υποκειμένου πρέπει να καταγράφεται σε ημερολόγια ελέγχου κατά τη διαδικασία πρόσβασης.

Η ταυτοποίηση και η αυθεντικοποίηση αποτελούν τα δύο σκέλη του πρωτοκόλλου επικοινωνίας, που ενεργοποιείται όταν ένα λογικό υποκείμενο αιτείται προσπέλασης στους πόρους ενός ΠΣ. Το πρώτο, δηλαδή το λογικό υποκείμενο, αποκαλείται συνήθως «Επικειρωτής» (Prover), και είναι επιφορτισμένο με την υποχρέωση να παρέχει εκείνες τις πληροφορίες που απαιτούνται για να αποδειχθεί η ταυτότητα του. Το δεύτερο μέρος, αποκαλείται συνήθως

«Σκεπτικιστής» (Skeptic), και είναι επιφορτισμένο με τον έλεγχο και την επιβεβαίωση της ορθότητας ή την απόρριψη των πληροφοριών που του παρέχει ο Prover στο πρώτο μέρος.[8]

3.2 Κατηγορίες Αυθεντικοποίησης

Κυριαρχούν τέσσερις βασικοί τρόποι για την εφαρμογή ελέγχων αυθεντικοποίησης:

- *Τύπος Ι*: Κάτι που το λογικό υποκείμενο γνωρίζει (π.χ. pin).
- *Τύπος ΙΙ*: Κάτι που το λογικό υποκείμενο κατέχει (π.χ. έξυπνη κάρτα).
- *Τύπος ΙΙΙ*: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (π.χ. αναγνώριση φωνής και ίριδας ματιού).
- *Τύπος IV*: Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο (π.χ. διεύθυνση IP).

Η βέλτιστη πρακτική εφαρμογής ενός συστήματος αυθεντικοποίησης θα πρέπει να περιλαμβάνει ένα συνδυασμό δύο ή περισσοτέρων τρόπων από τις προαναφερθείσες κατηγορίες.

Η διαδικασία αυθεντικοποίησης περιλαμβάνει:

α) την παροχή της πληροφορίας από ένα λογικό υποκείμενο στο σύστημα,

β) την ανάλυση αυτής της πληροφορίας και

γ) τον έλεγχο ότι πράγματι αυτή η πληροφορία σχετίζεται με το ίδιο λογικό υποκείμενο.

Επομένως, ένα σύστημα αυθεντικοποίησης αποτελείται από τα παρακάτω πέντε βασικά μέρη:

- Το *σύνολο A* που περιέχει τις πληροφορίες με βάση τις οποίες κάθε λογικό υποκείμενο αποδεικνύει την ταυτότητά του.

- Το *σύνολο C* που περιέχει τις συμπληρωματικές πληροφορίες που αποθηκεύει και χρησιμοποιεί το σύστημα ώστε να επικυρώνει πληροφορίες αυθεντικοποίησης.

- Το *σύνολο F* των συμπληρωματικών συναρτήσεων που δημιουργούν τις συμπληρωματικές πληροφορίες για την αυθεντικοποίηση.

- Το *σύνολο L* των συναρτήσεων αυθεντικοποίησης που αναγνωρίζουν ένα λογικό υποκείμενο.

- Το *σύνολο S* των λοιπών συναρτήσεων επιλογής που δίνουν την δυνατότητα σε ένα λογικό υποκείμενο να δημιουργήσει ή να τροποποιήσει τις πληροφορίες της αυθεντικοποίησης ή τις συμπληρωματικές πληροφορίες.[8]

3.3 Πλεονεκτήματα και Μειονεκτήματα Δεδομένων Αυθεντικοποίησης

Τύπος Ι: Κάτι που το λογικό υποκείμενο γνωρίζει.

Μειονεκτήματα:

a. Τα τεκμήρια αυθεντικοποίησης εύκολα μπορούν να αντιγραφούν.

b. Είναι εύκολο να τα μαντέψει κανείς χωρίς ιδιαίτερες τεχνικές γνώσεις.

c. Συνήθως μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους.

Πλεονεκτήματα:

a. Εύκολη υλοποίηση και εφαρμογή.

b. Τροποποιούνται εύκολα.

c. Δεν χάνονται ή κλέβονται.

d. Αν και είναι απλά στη χρήση τους, στην περίπτωση που είναι ένας μοναδιαίος συνδυασμός αριθμών και γραμμάτων, δεν αποκαλύπτονται εύκολα.

Τύπος ΙΙ: Κάτι που το λογικό υποκείμενο κατέχει.

Μειονεκτήματα:

a. Υψηλό κόστος.

b. Μπορούν να χαθούν ή να κλαπούν.

Πλεονεκτήματα:

a. Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα.

Τύπος ΙΙΙ: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του.

Μειονεκτήματα:

a. Δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος.

b. Δεν είναι αλάνθαστα.

Πλεονεκτήματα:

a. Παρέχουν μεγαλύτερη ασφάλεια από τον *Τύπο Ι* και *Τύπο ΙΙ*.[8]

3.4 Τεχνικές Αυθεντικοποίησης

Οι τεχνικές που χρησιμοποιούνται για την αυθεντικοποίηση διακρίνονται σε:

Τεχνικές με βάση κάτι που γνωρίζει το λογικό υποκείμενο, όπως:

i. Συνθηματικά για λογαριασμούς σε υπολογιστικά συστήματα.

ii. Συνθηματικά μιας χρήσης.

iii. Διαδικασίες Πρόκλησης - Απόκρισης (Challenge - Response).

iv. Προσωπικοί Αριθμοί Αναγνώρισης (PINs) για τραπεζικές συναλλαγές.

Τεχνικές με βάση κάτι που κατέχει το λογικό υποκείμενο, όπως:

i. Κουπόνια (Tokens).

ii. Μαγνητικές Κάρτες (Magnetic Cards).

iii. Έξυπνες Κάρτες (Smart Cards).

a. Συνθηματικά/Συνθηματικά μιας Χρήσης

Η χρήση των **Συνθηματικών** (Passwords) είναι ο πλέον διαδεδομένος τρόπος αυθεντικοποίησης χρηστών. Μαζί με το όνομα χρήστη (user name) πρέπει να εισάγεται ένα συνθηματικό (password), οπότε το σύστημα αυθεντικοποίησης του επιτρέπει την πρόσβαση στο σύστημα εφόσον το συνθηματικό που εισήγαγε ταιριάζει με το αντίστοιχο που ήδη βρίσκεται αποθηκευμένο στο σύστημα.

Καθώς πολλά υπολογιστικά συστήματα επιτρέπουν στους χρήστες να ορίζουν εκείνοι το συνθηματικό τους, προκύπτουν σοβαρά προβλήματα ασφάλειας από τον αυξημένο κίνδυνο να μαντέψουν αυτά τα συνθηματικά οι πιθανοί εισβολείς είτε γνωρίζοντας προσωπικές πληροφορίες του κάθε χρήστη είτε χρησιμοποιώντας κάποιο λεξιλόγιο με συνηθισμένα συνθηματικά. Η εμπειρία έχει δείξει ότι οι περισσότεροι χρήστες διαλέγουν ‘κακά’ συνθηματικά, παρόλες τις σχετικές προειδοποιήσεις των διαχειριστών συστημάτων.

Αλλά ακόμη και αν γίνει σωστή επιλογή ενός συνθηματικού, απομένουν μια σειρά από σωστές ενέργειες που αποσκοπούν στην προφύλαξή του ώστε να μην αποκαλυφθεί σε τρίτα πρόσωπα. Οι διαδικασίες ασφάλειας που ακολουθούνται για να εξασφαλίζεται η σωστή χρήση των συνθηματικών περιλαμβάνουν:

- Ορισμό ξεχωριστού συνθηματικού για κάθε πρόσωπο και όχι για ομάδες χρηστών.
- Ορισμό συνθηματικών με χρήση μεγάλων σειρών χαρακτήρων προκειμένου να μην είναι εύκολο να τα μαντέψει κάποιος τρίτος.
- Αποφυγή σημείωσης των συνθηματικών σε ντοσιέ ή χαρτιά που βρίσκονται εκτεθειμένα πάνω σε γραφεία ή σε απροστάτευτα μέρη (π.χ. εκτός μιας φυσικά προστατευμένης περιοχής).
- Τακτική ανανέωση και χρήση των συνθηματικών με ιδιαίτερη προσοχή.

Μια εναλλακτική λύση αποτελεί η χρήση **Συνθηματικών μιας Χρήσης**. Για το σκοπό χρησιμοποιείται μια λίστα από συνθηματικά (ξεχωριστή για κάθε χρήστη) και κάθε φορά χρησιμοποιείται ένα από αυτά (για μια και μοναδική φορά) μέχρι να εξαντληθούν τα συνθηματικά της λίστας.

Για την υλοποίηση ενός συστήματος συνθηματικών μιας χρήσης πρέπει να δοθεί ιδιαίτερη προσοχή ώστε:

- να είναι ορθός και απόρρητος ο τρόπος διανομής των λιστών συνθηματικών
- να είναι εξασφαλισμένη η προστασία αυτών των λιστών από κλοπή.

Η πληροφορία των συνθηματικών αποθηκεύεται στον υπολογιστή προκειμένου να ελέγχονται επιτόπου οι χρήστες που τα χρησιμοποιούν. Παρόλα αυτά, η αποθήκευση των συνθηματικών παρουσιάζει και αυτή σημαντικά προβλήματα ασφάλειας, καθώς όταν αποθηκεύονται σε μια μορφή χωρίς προστασία τότε τουλάχιστον οι διαχειριστές του συστήματος μπορούν να τα διαβάσουν. Κάτι τέτοιο αποτελεί σημαντική παραβίαση της ασφάλειας του συστήματος, καθώς τα συνθηματικά αποτελούν αυστηρά προσωπική πληροφορία. Η γνώση του συνθηματικού μας από άλλον χρήστη μπορεί να του επιτρέψει να χρησιμοποιήσει τις υπηρεσίες του συστήματος προσποιούμενος ότι είμαστε εμείς. Αυτό έχει ως απόρροια οι ενέργειες που καταγράφονται από το σύστημα να θεωρούμαστε εμείς υπεύθυνοι και υπόλογοι.

Προτεινόμενη και συνήθης λύση σε αυτό το πρόβλημα είναι η χρήση ενός μονόδρομου αλγόριθμου (one-way function) κρυπτογράφησης, που να είναι εύκολο να υπολογίζεται και αδύνατο να αναστραφεί το αποτέλεσμά του. Οπότε, αντί να αποθηκεύονται τα συνθηματικά αυτά καθαυτά, αποθηκεύεται το αποτέλεσμα της εφαρμογής του μονόδρομου αλγόριθμου σε κάθε ένα συνθηματικό ξεχωριστά.

Κατόπιν, για την επιβεβαίωση του συνθηματικού που εισάγει ο χρήστης εφαρμόζεται σε αυτό ο ίδιος μονόδρομος αλγόριθμος και η τιμή που προκύπτει συγκρίνεται με την αποθηκευμένη τιμή στο σύστημα.

Εντούτοις, υπάρχουν διάφορα διαθέσιμα πακέτα λογισμικού τα οποία έχουν σχεδιασθεί για να εντοπίζουν κακώς επιλεγμένα συνθηματικά χρηστών, ψάχνοντας απλά στο αρχείο συνθηματικών. Τα πακέτα αυτά τυπικά υποστηρίζονται από τεράστια λεξιλόγια με συνηθισμένα συνθηματικά και η εμπειρία έχει δείξει ότι πάνω από το 50% των συνθηματικών χρήστη μπορούν να βρεθούν περίπου μέσα σε μια μέρα. Ως εκ τούτου, αν το αρχείο συνθηματικών είναι εκτεθειμένο σε δημόσια χρήση, τότε δεν πρέπει να χρησιμοποιούνται συνθηματικά που μπορεί κανείς να τα μαντέψει εύκολα. Φυσικά, μια καλή τακτική για τους διαχειριστές δικτύων υπολογιστών είναι να χρησιμοποιούν περιοδικά τέτοια προγράμματα για να εντοπίζουν τα ‘κακά’ συνθηματικά των χρηστών.[9]

b. Συστήματα Πρόκλησης και Απόκρισης

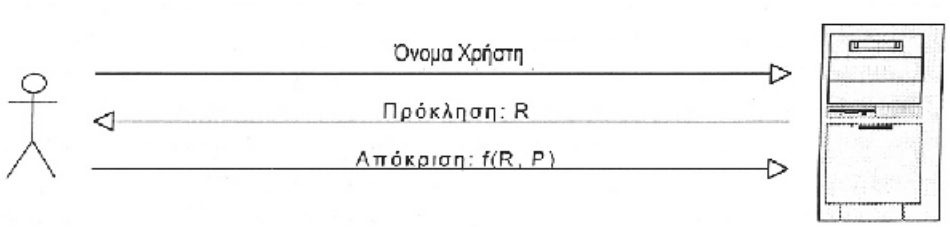
Στην περίπτωση που τα Συνθηματικά χρειάζεται να μεταφέρονται στα πλαίσια ενός ανασφαλούς δικτύου, όπως πολλές φορές είναι ένα επιχειρησιακό LAN, τότε είναι ιδιαίτερα ευπαθή για υποκλοπή. Μια απλή κρυπτογράφηση των συνθηματικών δεν είναι εύχρηστη καθώς ένα υποκλεμμένο κρυπτογραφημένο συνθηματικό μπορεί να χρησιμοποιηθεί ξανά ακριβώς όπως και το αρχικό συνθηματικό. Μια λύση άμεση είναι η αξιοποίηση των διαδικασιών **Πρόκλησης - Απόκρισης** (Challenge - Response) για την αυθεντικοποίηση των χρηστών.

Ένα σύστημα πρόκλησης-απόκρισης (challenge-response) απαιτεί από τον χρήστη να κατέχει ένα μυστικό συνθηματικό **P** και τα μέσα για να υπολογίζει μια μονόδρομη συνάρτηση **f**.

Όταν ο χρήστης ζητάει προσπέλαση από ένα σύστημα, αρχικά παρέχει το όνομα του (user name). Ο υπολογιστής (host) αποκρίνεται με μια τυχαία πρόκληση (challenge) R, τότε ο χρήστης αποκρίνεται με το αποτέλεσμα από την εφαρμογή της συνάρτησης f στον συνδυασμό των τιμών R και P, το σύστημα εκτελεί και εκείνο τον ίδιο υπολογισμό και έτσι μπορεί να αποδεχθεί ή να απορρίψει τον χρήστη.

Τα συνθηματικά των χρηστών αποθηκεύονται σε ένα φυσικά ασφαλές υποσύστημα για να αποτρέπεται μη εξουσιοδοτημένη προσπέλαση στο αρχείο συνθηματικών. Η μονόδρομη συνάρτηση *f* πρέπει να υποστηρίζει την ιδιότητα ότι πιθανή γνώση των *f(R,P),R* και του *f* αυτού καθαυτού δεν διακυβεύει την τιμή του *P*, τουλάχιστον σε ένα εύλογο χρονικό διάστημα. Αυτό πρέπει να ισχύει ακόμη και αν ο υποκλοπέας γνωρίζει μια σειρά από τέτοιες τιμές. Το σύστημα είναι μη ασφαλές εφόσον το σύνολο των πιθανών συνθηματικών *P* δεν είναι αρκετά μεγάλο. Αλλά ακόμη και αν υπάρχουν πολύ μικρές πιθανότητες για το *P*, τότε ο υποκλοπέας μπορεί να δοκιμάσει όλα τα πιθανά συνθηματικά μέχρι να βρεθεί κάποιο που να δίνει το σωστό αποτέλεσμα όταν ως είσοδος στην *f* δίνεται μια υποκλεμμένη πρόκληση και το συνθηματικό που μάντεψε.

Σχήμα



Να σημειώσουμε ότι ένα τέτοιο σύστημα αυθεντικοποίησης απαιτεί από τον χρήστη να διαθέτει τα μέσα για τον υπολογισμό της *f* γρήγορα και εύκολα. Πρόκειται για ένα κατεξοχήν παράδειγμα τύπου ‘αυθεντικοποίησης από κάτι που κατέχει ο χρήστης’.[9]

3.5 Σύστημα Kerberos

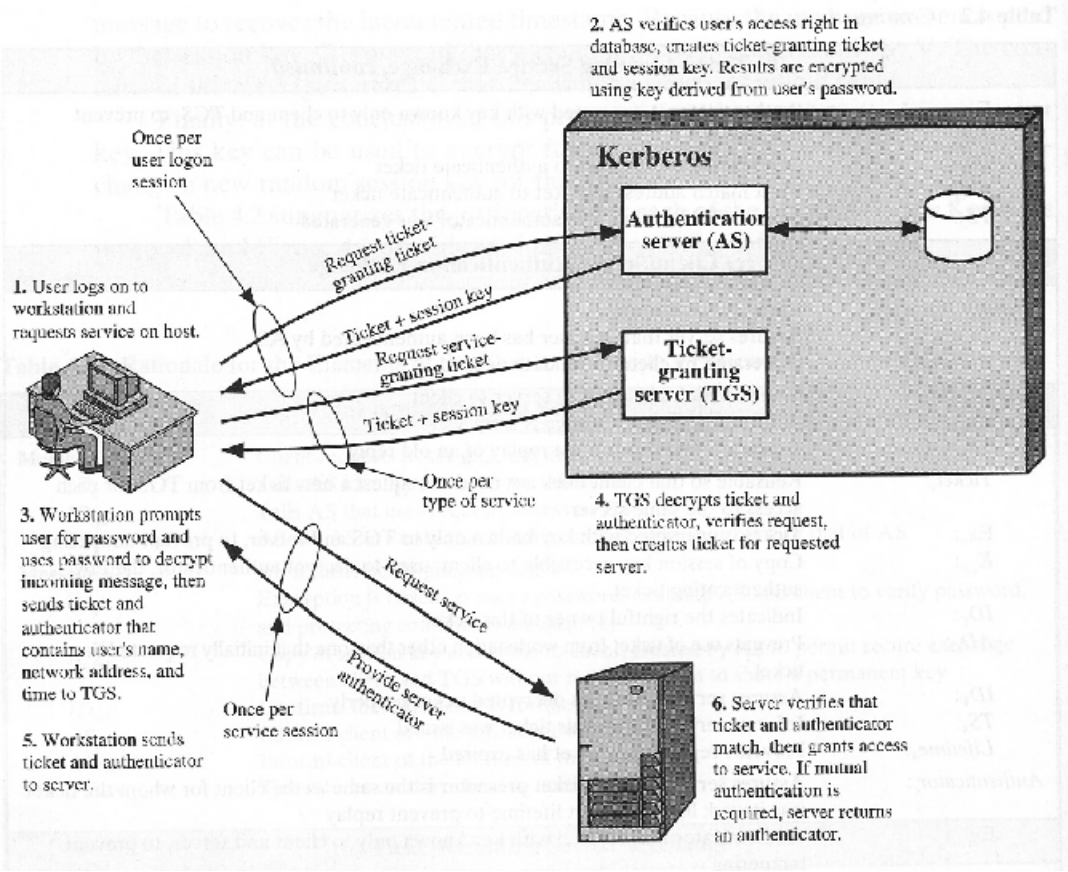
Λόγω της αυξημένης και βαρύνουσας σημασίας της αυθεντικοποίησης στα δίκτυα υπολογιστών, έχουν αναπτυχθεί πάρα πολλά συστήματα που είναι υπεύθυνα για ακριβώς αυτή την εργασία. Πρόκειται δηλαδή στην ουσία για συστήματα που στηρίζονται σε διαφορετικές συναρτήσεις που εκτελούν την διαδικασία της αυθεντικοποίησης. Μερικά τέτοια γνωστά συστήματα είναι το σύστημα **Kerberos**, το X.509, το NetSP, το SPX, το TESS, το SESAME, το OSF και το DCEH. Εξαιτίας της εκτεταμένης χρήσης του στη συνέχεια επιλέξαμε να περιγράψουμε το σύστημα αυθεντικοποίησης Kerberos.

Η πιστοποίηση Kerberos αναπτύχθηκε στο Massachusetts Institute of Technology (MIT) για να παρέχει ένα σύστημα εμπιστοσύνης ανάμεσα σε υπολογιστές, το οποίο να είναι σε θέση να επαληθεύσει την ταυτότητα των αρχών ασφαλείας όπως ένα χρήστη ή έναν υπολογιστή, επάνω σε ένα ανοικτό, ανασφαλές δίκτυο. Το Kerberos δεν βασίζεται στην πιστοποίηση από τους εμπλεκόμενους υπολογιστές ή την ιδιωτικότητα επικοινωνιών δικτύου. Επομένως, είναι ιδανικό για πιστοποίηση επάνω στο Internet και σε μεγάλα δίκτυα.[10]

Το Kerberos λειτουργεί όπως μια έμπιστη υπηρεσία πιστοποίησης χρησιμοποιώντας μυστικά κλειδιά κοινής χρήσης. Στην ουσία, ένας υπολογιστής εμπιστεύεται άρρητα το Κέντρο Διανομής Κλειδιών(Key Distribution Center-KDC) του Kerberos, επειδή γνωρίζει το ίδιο μυστικό κλειδί που γνωρίζει ο υπολογιστής, ένα μυστικό που πρέπει να τεθεί ως τμήμα της έμπιστης διαχειριστικής διεργασίας. Στα Windows, το κοινό μυστικό παράγεται όταν ο υπολογιστής συνδέεται στον τομέα. Εφόσον και τα δύο μέρη μιας συνόδου Kerberos εμπιστεύονται το KDC, μπορεί να θεωρηθεί ότι εμπιστεύονται το ένα το άλλο. Πρακτικά, αυτή η εμπιστοσύνη υλοποιείται ως μια ασφαλής ανταλλαγή κλειδιών κρυπτογράφησης, που αποδεικνύει τις ταυτότητες των εμπλεκομένων μερών.

Η πιστοποίηση Kerberos εργάζεται όπως εικονίζεται στο Σχήμα και περιγράφεται στη συνέχεια.

Σχήμα: Το σύστημα Kerberos



Ένας χρήστης ζητά ένα έγκυρο σύνολο διαπιστευτηρίων για ένα δεδομένο διακομιστή από το KDC στέλνοντας μια αίτηση χωρίς κρυπτογράφηση του κειμένου, που περιέχει το όνομα, δηλαδή την ταυτότητα του πελάτη.

Το KDC αποκρίνεται ψάχνοντας τα μυστικά κλειδιά του χρήστη και του διακομιστή μέσα στη βάση δεδομένων του (στον Ενεργό Κατάλογο) και δημιουργώντας ένα εισιτήριο που περιέχει ένα τυχαίο κλειδί συνόδου, την τρέχουσα ώρα στο KDC, μια ώρα λήξης, που καθορίζεται από την πολιτική και, προαιρετικά, τυχόν άλλες πληροφορίες που είναι αποθηκευμένες μέσα στη βάση δεδομένων. Το εισιτήριο κρυπτογραφείται κατόπιν χρησιμοποιώντας το μυστικό κλειδί του πελάτη. Στην συνέχεια, δημιουργείται ένα δεύτερο

εισιτήριο, που καλείται κλειδί συνόδου, αυτό λοιπόν περιλαμβάνει το κλειδί συνόδου και προαιρετικά δεδομένα πιστοποίησης, τα οποία κρυπτογραφούνται χρησιμοποιώντας το μυστικό κλειδί διακομιστή. Τα συνδυασμένα εισιτήρια μεταδίδονται πίσω στον χρήστη. Είναι αξιοσημείωτο ότι ο διακομιστής πιστοποίησης δεν χρειάζεται να πιστοποιήσει τον χρήστη ρητά, επειδή μόνο ο έγκυρος χρήστης θα μπορέσει να αποκρυπτογραφήσει το εισιτήριο.

Αφού ο χρήστης πάρει ένα έγκυρο εισιτήριο και κλειδί συνόδου για ένα διακομιστή, μπορεί να εκκινήσει την απευθείας επικοινωνία με το διακομιστή. Για να εκκινήσει μια επικοινωνία με ένα διακομιστή, ο πελάτης κατασκευάζει ένα πιστοποιητή, που αποτελείται από την τρέχουσα ώρα, το όνομα του πελάτη, ένα άθροισμα ελέγχου για τη συγκεκριμένη εφαρμογή, και ένα τυχαία παραγόμενο αρχικό αριθμό ακολουθίας και/ή ένα δευτερεύον κλειδί συνόδου, που χρησιμοποιείται για να επαναφέρει μια μοναδική ταυτότητα συνόδου, ειδικό για την υπηρεσία που ενδιαφέρει τον χρήστη. Οι πιστοποιητές είναι έγκυροι μόνο για μια προσπάθεια και δεν μπορούν να επαναχρησιμοποιηθούν ή να τύχουν εκμετάλλευσης μέσω μιας επίθεσης αναπαραγωγής, επειδή εξαρτώνται από την τρέχουσα ώρα. Ο πιστοποιητής κατόπιν κρυπτογραφείται και μεταδίδεται μαζί με το εισιτήριο συνόδου στο διακομιστή, από τον οποίο ζητήθηκε η υπηρεσία.

Όταν ο διακομιστής δεχθεί το εισιτήριο από τον πελάτη, αποκρυπτογραφεί το εισιτήριο συνόδου χρησιμοποιώντας το κοινό μυστικό κλειδί του διακομιστή (το οποίο μυστικό κλειδί, αν υπάρχουν περισσότερα του ενός, δηλώνεται στο τμήμα ακρυπτογράφητου κειμένου του εισιτηρίου). Συνεχίζοντας ανακτά από το κλειδί συνόδου το εισιτήριο και το χρησιμοποιεί για να αποκρυπτογραφήσει τον πιστοποιητή. Η δυνατότητα του διακομιστή να αποκρυπτογραφήσει το εισιτήριο αποδεικνύει ότι κρυπτογραφήθηκε χρησιμοποιώντας το ιδιωτικό κλειδί του διακομιστή, που είναι γνωστό μόνο στο KDC, οπότε υπάρχει εμπιστοσύνη στην ταυτότητα του πελάτη. Ο πιστοποιητής χρησιμοποιείται για να σιγουρέψει ότι η επικοινωνία είναι πρόσφατη και δεν είναι μια επίθεση αναπαραγωγής. Τα εισιτήρια μπορούν να επαναχρησιμοποιηθούν για μια διάρκεια που καθορίζεται από την πολιτική ασφαλείας του τομέα και δεν υπερβαίνει τις 10 ώρες. Αυτό μειώνει το φορτίο του KDC, που δεν χρειάζεται να κάνει περισσότερες από μια αιτήσεις ανά εργάσιμη ημέρα. Οι πελάτες αποθηκεύουν προσωρινά τα εισιτήρια συνόδου σε ένα ασφαλή χώρο που βρίσκεται μέσα στη RAM και τα καταστρέφουν όταν λήγουν.

Το σύστημα αυθεντικοποίησης Kerberos χρησιμοποιεί την ιδιότητα επαναχρησιμοποίησης εισιτηρίων για να συντομεύσει το χρόνο εκχώρησης εισιτηρίων, εκχωρώντας ένα εισιτήριο συνόδου για τον εαυτό του, καθώς και για το διακομιστή στόχου, την πρώτη φορά που έρχεται σε επαφή με έναν χρήστη. Μόλις γίνει η πρώτη αίτηση από έναν χρήστη το KDC αποκρίνεται πρώτα με ένα εισιτήριο συνόδου για να κάνει περαιτέρω αιτήσεις εισιτηρίων, που καλείται Εισιτήριο Απόδοσης Εισιτηρίων (Ticket Granting Ticket, TGT) και μετά με ένα εισιτήριο συνόδου για το διακομιστή. Το TGT αποφεύγει περαιτέρω αναζητήσεις στον Ενεργό Κατάλογο από τον πελάτη, πιστοποιώντας εκ των προτέρων επόμενες αιτήσεις εισιτηρίων με τον ίδιο ακριβώς τρόπο που το Kerberos πιστοποιεί όλες τις άλλες αιτήσεις. Όπως κάθε εισιτήριο συνόδου, το TGT είναι έγκυρο μέχρι να λήξει, πράγμα που εξαρτάται από την πολιτική ασφάλειας τομέα.

Το Kerberos διαιρείται, από τεχνικής σκοπιάς σε δύο υπηρεσίες, την υπηρεσία TGT που είναι η μόνη υπηρεσία που κάνει την πιστοποίηση ως προς τον Ενεργό Κατάλογο και την υπηρεσία Ticket Granting, η οποία εκδίδει εισιτήρια συνόδου, όταν της παρέχεται ένα έγκυρο TGT.[10], [11]

4. Βιομετρικά Συστήματα

Η διαδικασία ταυτοποίησης με εφαρμογή συστημάτων βιομετρικής τεχνολογίας αποτελεί μια ασφαλή μέθοδο ταυτοποίησης και βασίζεται σε φυσικά χαρακτηριστικά του ανθρώπινου σώματος ως αποδεικτικά στοιχεία για την αναγνωρισιμότητα του λογικού υποκειμένου από ένα ΠΣ. Τα δακτυλικά αποτυπώματα, η ίριδα ματιού, η χροιά φωνής, η γεωμετρία χεριού και το DNA αποτελούν τα κύρια τεκμήρια της διαδικασίας της αυθεντικοποίησης. Τα βιομετρικά συστήματα ανήκουν στην τρίτη κατηγορία συστημάτων αυθεντικοποίησης που χαρακτηρίζουν το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του.

Αρχικά η χρήση της βιομετρικής τεχνολογίας αναπτύχθηκε από κυβερνητικούς οργανισμούς προκειμένου να εφαρμοστεί σε εφαρμογές που αφορούσαν τον έλεγχο πρόσβασης σε εγκαταστάσεις κρίσιμες για την εθνική ασφάλεια. Στα πρώτα στάδια της εφαρμογής τους παρουσιάστηκαν πολλά προβλήματα. Ωστόσο οι σημαντικές εξελίξεις στον επιστημονικό αυτό χώρο βοήθησαν σημαντικά στην βελτίωση των βιομετρικών τεχνολογιών.[12]

4.1 Οι βιομετρικές τεχνικές διαχωρίζονται στις παρακάτω δύο κατηγορίες:

Α) Αφορά στην τεχνική μέτρησης ανθρώπινων φυσικών χαρακτηριστικών. Στην κατηγορία αυτή περιλαμβάνονται :δακτυλικά αποτυπώματα, ανάλυση ίριδας ματιού, γεωμετρία χεριού, αναγνώριση αυτιού, ανάλυση δείγματος DNA, ανάλυση ιδρώτα.

Β) Αφορά στην τεχνική μέτρησης της συμπεριφοράς .Σε αυτήν συμπεριλαμβάνονται η αναγνώριση της υπογραφής ,η ανάλυση πληκτρολόγησης και η ανάλυση ομιλίας.

Υπάρχουν δύο βασικές έννοιες στην τεχνολογία μέτρησης βιομετρικών χαρακτηριστικών:

i. Η ανοχή στο σφάλμα και

ii. Η μέθοδος αποθήκευσης των προτύπων ανάλυσης.

Η ρύθμιση του βαθμού σφάλματος σε αυτά τα συστήματα είναι κρίσιμη καθώς επηρεάζει τη ρυθμο-απόδοση του συστήματος .Γενικά, το επίπεδο ανοχής στο σφάλμα (σφάλμα αποδοχής και σφάλμα απόρριψης)πρέπει να είναι χαμηλό και να αναφέρεται ρητώς από τον κατασκευαστή του συστήματος.

Η αποτύπωση της βιομετρικής μέτρησης του γνωρίσματος του χρήστη, που συνήθως αποκαλείται πρότυπο (template) μπορεί να αποθηκευτεί σε διάφορα μέσα σύμφωνα με τις δυνατότητες της χρησιμοποιούμενης τεχνολογίας και της απαιτήσεις ασφαλείας της εφαρμογής. Τα πρότυπα μπορούν να αποθηκευθούν είτε στην ίδια την βιομετρική συσκευή, είτε σε μία κεντρική βάση δεδομένων είτε σε μια πλαστική κάρτα (πχ έξυπνη κάρτα).[12]

4.2 Χαρακτηριστικά βιομετρικών συστημάτων

Τα κύρια χαρακτηριστικά των βιομετρικών συστημάτων είναι η ακρίβεια, η ταχύτητα, η αξιοπιστία, η διαδικασία της αποθήκευσης και των απαιτήσεων της επεξεργασίας, οι διαδικασίες εγγραφής ενός χρήστη, η μοναδικότητα, το ποσοστό αντίστασης σε απάτη και η αποδοχή τους από τον χρήστη.

Ακρίβεια

Η ακρίβεια ενός βιομετρικού συστήματος ορίζεται ως το ποσοστό συχνότητας ορθής αναγνώρισης ενός εξουσιοδοτημένου ατόμου από ένα μη εξουσιοδοτημένο. Δύο είναι οι μονάδες μέτρησης που χρησιμοποιούνται: α) το ποσοστό απόρριψης εξουσιοδοτημένων ατόμων (σφάλμα απόρριψης) και β)το ποσοστό αποδοχής μη εξουσιοδοτημένων ατόμων (σφάλμα αποδοχής). Το σημείο τομής των δύο αυτών μετρήσεων είναι το Ολικό Επίπεδο Σφάλματος(Crossover Error Rate, CER). Τα παραπάνω χαρακτηριστικά ρυθμίζονται ανάλογα με τις απαιτήσεις ασφαλείας του βιομετρικού συστήματος.

Ταχύτητα

Η ταχύτητα απόκρισης αποτελεί ένα ακόμη σημαντικό χαρακτηριστικό ενός βιομετρικού συστήματος. Έρευνες έχουν καταλήξει σε ένα γενικά αποδεκτό χρονικό όριο των πέντε (5) δευτερολέπτων για τη διαδικασία της αναγνώρισης.

Αξιοπιστία

Η αξιοπιστία ενός τέτοιου συστήματος ορίζεται ως η συνεχής , ακριβής και γρήγορη λειτουργία του , χωρίς να απαιτείται υψηλό ποσοστό συντήρησης ή ελέγχου λειτουργίας.

Αποθήκευση δεδομένων και Απαιτήσεις επεξεργασίας

Τα δύο αυτά χαρακτηριστικά στο παρελθόν επηρέαζαν το χρόνο επεξεργασίας ενός χρήστη. Σε σύστημα με ορισμένο χαμηλό επίπεδο αποδοχής σφάλματος , η διαδικασία αναγνώρισης απαιτεί μεγαλύτερο χρόνο καθώς τα δεδομένα που εισάγονται πρέπει να συγκριθούν με όλα τα στοιχεία της βάσης δεδομένων. Η εμφάνιση ταχύτατων επεξεργαστών και η ελάττωση του κόστους σε συσκευές αποθήκευσης δεδομένων , καθιστούν σήμερα τις απαιτήσεις επεξεργασίας των βιομετρικών συσκευών ικανοποιητικές από άποψη λειτουργίας. Το μέσο μέγεθος ενός αρχείου με βιομετρικά στοιχεία κυμαίνεται μεταξύ 256 και 1000 bytes.

Διαδικασία Καταχώρησης

Ο συνολικός χρόνος που απαιτείται για την εισαγωγή των στοιχείων ταυτότητας και του βιομετρικού χαρακτηριστικού ενός νέου χρήστη στο σύστημα ονομάζεται διαδικασία καταχώρησης. Στα σημερινά συστήματα ο χρόνος καταχώρησης δεν αποτελεί πλέον χαρακτηριστικό αξιολόγησης καθώς η πλειοψηφία των συστημάτων εφαρμόζουν το γενικά αποδεκτό χρόνο καταχώρησης των δύο (2) λεπτών ανά άτομο.

Μοναδικότητα

Τα βιομετρικά συστήματα που βασίζονται σε μοναδικά χαρακτηριστικά του ανθρώπινου σώματος ενισχύουν την πιθανότητα της ορθής εφαρμογής της αναγνώρισης. Τα τρία φυσικά χαρακτηριστικά που ικανοποιούν αυτό το κριτήριο είναι το δακτυλικό αποτύπωμα , η ίριδα ματιού και ο αμφιβληστροειδής του ματιού.

Παραποίηση στοιχείων

Με τον όρο αυτό εννοούμε τη χρήση ενός συνθετικού αντιγράφου ενός βιομετρικού χαρακτηριστικού με σκοπό την επίτευξη μιας μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Τα βιομετρικά συστήματα πρέπει να απαιτούν σημαντικό ποσοστό ακρίβειας του βιομετρικού χαρακτηριστικού ώστε να μην είναι δυνατό να εισαχθούν ψευδή δεδομένα για την επίτευξη της πρόσβασης.

Αποδοχή του χρήστη

Τα βιομετρικά συστήματα , λόγω της ιδιομορφίας που παρουσιάζουν ως προς τα εισαγόμενα δεδομένα (πχ δακτυλικό αποτύπωμα , ίριδα ματιού) προκαλούν κοινωνικές αντιδράσεις. Οι χρήστες συχνά αντιδρούν , διότι αισθάνονται ότι πρέπει να καταχωρήσουν ένα γνώρισμα (πχ διαστάσεις παλάμης) του σώματός τους σε μία βάση δεδομένων του συστήματος κατά τη διαδικασία της εγγραφής τους. Κυριαρχεί το συναίσθημα ότι παρακολουθούνται από το σύστημα και ότι καταγράφονται οι κινήσεις τους. Επιπλέον , υπάρχει ο φόβος των μεταδιδόμενων ασθενειών και της πρόκλησης σωματικής βλάβης από το σύστημα (πχ η χρήση των κόκκινων φωτεινών ενδείξεων που χρησιμοποιούνται στην ίριδα του ματιού θυμίζει τις βλαβερές συνέπειες του laser). Παρόλα αυτά , δεν υπάρχουν αναφορές για πρόκληση σωματικών παρενεργειών από τα βιομετρικά συστήματα. Για το λόγο αυτό η

εκπαίδευση και η ενημέρωση των χρηστών σχετικά με την τεχνολογία αυτή αποτελεί ένα κρίσιμο παράγοντα για την επιτυχή εφαρμογή τους.[12]

4.3 Τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης των συστημάτων βιομετρικής τεχνολογίας:

Πλεονεκτήματα:

a. Δεν απαιτούν την χρήση κλειδιού , κάρτας ή άλλης συσκευής από το χρήστη.

b. Δεν απαιτούν την απομνημόνευση συνθηματικού πρόσβασης.

c. Δεν απαιτούν τη διαχείριση σχετικά με την τροποποίηση στοιχείων συνθηματικών για την πρόσβαση κλπ.

d. Η πιθανότητα ορθής αναγνώρισης βασίζεται σε μοναδικά χαρακτηριστικά.

e. Τα κριτήρια είναι μόνιμα και δεν απαιτούν ανανέωση(εξαίρεση αποτελεί η αναγνώριση φωνής , η σύγκριση υπογραφής και η αναγνώρισης πληκτρολόγησης, που απαιτούν ανανέωση με το γήρας του χρήστη).

***Μειονεκτήματα Παλαιότερων Βιομετρικών Συστημάτων*:**

a. Υψηλό κόστος.

b. Αργοί χρόνοι απόκρισης .

c. Απαιτήσεις για μεγάλες βάσεις δεδομένων.

d. Υψηλό ποσοστό απόρριψης , απαίτηση για εφαρμογή τεχνικών λήψης αντιγράφων ασφαλείας για την αυθεντικοποίηση με έμμεσο αποτέλεσμα την δυσαρέσκεια του χρήστη.

e. Υψηλές απαιτήσεις συντήρησης .

f. Μακροσκελείς διαδικασίες καταχώρησης.

g. Η κοινωνική αντίληψη ότι η λήψη δακτυλικών αποτυπωμάτων συνδυάζεται με εγκληματική δραστηριότητα.

h. Η κοινωνική αντίληψη ότι η χρήση laser βλάπτει την υγεία.

i. Η αντίσταση των χρηστών.[12]

5. Προστασία προσωπικών δεδομένων

Νομικό Πλαίσιο Προστασίας
 Ν. 2472/97

Ο ν. 2472/97 συνιστά ένα προστατευτικό πλαίσιο κανόνων που εδράζεται σε τρεις πυλώνες:

1) Στις ουσιαστικές ρυθμίσεις που θέτουν τις προϋποθέσεις νομιμότητας της επεξεργασίας,

2) Στην αναγνώριση δικαιωμάτων στα πρόσωπα και

3) Στην εισαγωγή θεσμικού ελέγχου προστασίας προσωπικών δεδομένων.[13]

5.1 Προϋποθέσεις νομιμότητας της επεξεργασίας

Ο νομοθέτης εισάγει ως βασική αρχή ότι η συλλογή και επεξεργασία είναι κατ'αρχήν παράνομες – και άρα απαγορεύονται – και καθίστανται νόμιμες μόνο αν πληρούν τις εξής προϋποθέσεις που θέτει ο νόμος δεσμευτικά και περιοριστικά:

- Η παροχή της ρητής συγκατάθεσης του υποκειμένου των δεδομένων ως εκδήλωση της εξουσίας αυτοδιάθεσης του ατόμου (α.5§1). Αποκλείεται η εικαζόμενη, η σιωπηρή και η τεκμαιρόμενη συγκατάθεση.

- Κατ'εξαίρεση επιτρέπεται η επεξεργασία χωρίς την προηγούμενη συγκατάθεση του ατόμου, όταν είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, την εκτέλεση έργου δημοσίου συμφέροντος, την ικανοποίηση εννόμου συμφέροντος του υπεύθυνου επεξεργασίας υπό τον όρο ότι αυτό υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων, κ.ά. (α.5§2)

- Τα δεδομένα πρέπει να έχουν ορισμένα ποιοτικά χαρακτηριστικά (α.4) και καταστρέφονται υποχρεωτικά μετά την πραγματοποίηση του σκοπού. Οι ποιοτικές

προδιαγραφές συγκροτούν τον «σκληρό πυρήνα» της προστασίας προσωπικών δεδομένων. Συγκεκριμένα, καθιερώνονται η αρχή του σκοπού, η αρχή της αναλογικότητας, η αρχή της ακρίβειας των δεδομένων και η αρχή της χρονικά πεπερασμένης διατήρησης των δεδομένων. Η αρχή του σκοπού είναι η ραχοκοκαλιά του συστήματος των ποιοτικών χαρακτηριστικών των δεδομένων. Ο σκοπός προσδιορίζει το μέτρο της νομιμότητας της συλλογής και της περαιτέρω επεξεργασίας των δεδομένων υπό την έννοια ότι είναι πρωτίστως το κριτήριο επί τη βάσει του οποίου κρίνεται αυτή καθεαυτή η «αναγκαιότητα» της επεξεργασίας.

- Έγγραφη γνωστοποίηση στην Αρχή Προστασίας Δεδομένων για τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας (α.6).

- Διάκριση των δεδομένων σε κοινά και ευαίσθητα και καταρχήν απαγόρευση της επεξεργασίας των ευαίσθητων (α.7§1). Η απαγόρευση όμως είναι σχετική καθώς ο νομοθέτης προβλέπει δεσμευτικά και περιοριστικά τις εξαιρέσεις (α.7§2). Η ελληνική ρύθμιση ανταποκρίνεται στην αντίστοιχη διάταξη της οδηγίας 95/46/ΕΚ (άρθρο 8). Η απόκλιση ως προς την οδηγία συνίσταται στην προσθήκη δεδομένων που αφορούν την «κοινωνική πρόνοια» και τις «ποινικές διώξεις και καταδίκες».

- Παροχή άδειας συλλογής κι επεξεργασίας ευαίσθητων δεδομένων από την Αρχή Προστασίας Προσωπικών Δεδομένων(α.7§3). Η ύπαρξη της άδειας και πολύ περισσότερο η συγκατάθεση δεν αναιρεί κατά κανένα τρόπο τις εξουσίες της αρχής να ελέγχει κατασταλτικά την τήρηση των ουσιαστικών και διαδικαστικών προϋποθέσεων νομιμότητας που θέτει ο νόμος.

5.2 Αναγνώριση δικαιωμάτων στα πρόσωπα

Ο δεύτερος πυλώνας συνίσταται στην κατοχύρωση δικαιωμάτων ελέγχου και στην απονομή «μέσων άμυνας» στα πρόσωπα που θίγονται από την επεξεργασία. Έτσι, ο Ν. 2472/97 προστατεύει τα άτομα που θίγονται από την επεξεργασία απονέμοντάς τους τα εξής δικαιώματα:

- Δικαίωμα προηγούμενης ενημέρωσης των προσώπων για τα στοιχεία της επεξεργασίας (α.11).

- Δικαίωμα πρόσβασης στα αρχεία (α.12). Απουσιάζουν εκτενείς εξαιρέσεις και οι όποιες εξαιρέσεις περιορίζονται στην περίπτωση που η άσκηση του δικαιώματος αυτού θα διακύβευε την εθνική ασφάλεια ή τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

- Δικαίωμα αντίρρησης για την επεξεργασία δεδομένων που αφορούν το υποκείμενο (α.13).

- Δικαίωμα προσωρινής δικαστικής προστασίας (α.14).

5.3 Θεσμικός έλεγχος προστασίας προσωπικών δεδομένων

Με τον Ν.2472/97 συνίσταται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή) ως Ανεξάρτητη Διοικητική Αρχή, διακηρύσσεται η προσωπική και λειτουργική ανεξαρτησία των μελών της και κατοχυρώνεται η μη υπαγωγή της σε οποιοδήποτε διοικητικό έλεγχο, που νοείται ως ιεραρχικός έλεγχος από την εκτελεστική εξουσία. Επίσης, το Κοινοβούλιο εμπλέκεται στη διαδικασία της επιλογής των μελών της Αρχής, αυξάνοντας έτσι τη νομιμοποίηση και την ανεξαρτησία της Αρχής έναντι της εκτελεστικής εξουσίας.

Οι αρμοδιότητες και η λειτουργία της Αρχής συνδέονται με την γνωστοποίηση των αρχείων προσωπικών δεδομένων και την άσκηση προληπτικού ελέγχου (α.7,8, 9). Το κύριο χαρακτηριστικό του προληπτικού ελέγχου δεν έγκειται στη χρονική μετατόπιση της στιγμής ελέγχου της νομιμότητας αλλά στη μετάθεση της απόφασης και κατά συνέπεια της ευθύνης σε μία Αρχή που βρίσκεται εκτός εκτελεστικής εξουσίας. Η Αρχή εκδίδει οδηγίες για ενιαία εφαρμογή των ρυθμίσεων που αφορούν την προστασία του ατόμου, και κανονιστικές πράξεις για ειδικά, τεχνικά και λεπτομερειακά θέματα. Επίσης, η Αρχή εξετάζει παράπονα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων και συμμετέχει στην εκπόνηση κανόνων δεοντολογίας από επαγγελματικά σωματεία και τις άλλες ενώσεις φυσικών ή νομικών προσώπων. Τέλος, θα πρέπει να

επισημανθεί η γνωμοδοτική και συμβουλευτική λειτουργία της Αρχής, καθώς και η δυνατότητα που έχει να επιβάλει διοικητικές, ποινικές αλλά και εξωνομικές, «πολιτικές» κυρώσεις. Οι μηχανισμοί καταστολής των παραβάσεων κλιμακώνονται από την προειδοποίηση για άρση της παράβασης και την επιβολή προστίμων ως και την οριστική ανάκληση της άδειας του αρχείου ή και την καταστροφή του.[13]

5.4 Αδυναμίες του συστήματος:

Η ισχυρή θεσμική πανοπλία της Αρχής Προστασίας Προσωπικών Δεδομένων συναντά ορισμένα προσκόμματα όσον αφορά τα όρια του ελέγχου και της εφαρμοσιμότητας του νόμου27. Τα εξωγενή προβλήματα δεν έχουν μόνο ποσοτική διάσταση, δεν αφορούν μόνο τον όγκο και την ευρύτητα του προς έλεγχο πεδίου, αλλά και την ελεγξιμότητα των διασυνοριακών ροών προσωπικών δεδομένων, καθώς η ανάπτυξη των δικτύων και η διάδοση του Διαδικτύου παγκοσμιοποιούν την επικοινωνία, την αγορά και συνακόλουθα την επεξεργασία προσωπικών δεδομένων αναδεικνύοντας τα όρια και την ανεπάρκεια των εθνικών νόμων. Είναι χαρακτηριστικό ότι η – αποτελούμενη από τις εθνικές αρχές ελέγχου – ομάδα εργασίας 29, που ονομάστηκε έτσι από το αντίστοιχο άρθρο της κοινοτικής οδηγίας 95/46/ΕΚ με το οποίο συστήθηκε, έκρινε ως μείζον πρόβλημα τη διασυνοριακή ροή δεδομένων σε τρίτες χώρες. Η παγκοσμιοποίηση που αίρει τους γεωγραφικούς περιορισμούς στη ροή των δεδομένων, η σύγκλιση των τεχνολογιών που οδήγησε στην εξάλειψη των τεχνολογικών εμποδίων μεταξύ των συστημάτων και τα πολυμέσα καθιστούν αμφίβολη τη ρύθμιση των ζητημάτων της ιδιωτικότητας (privacy) στον κυβερνοχώρο και αναδεικνύουν την κρίση των εθνικών νόμων και των εθνικών αρχών ελέγχου.

Ο εγγενής κίνδυνος για την Αρχή είναι να παγιδευτεί στην ίδια της την εξουσία, και να καταρρεύσει κάτω από το βάρος που συνεπάγεται το σύστημα προληπτικού ελέγχου με πιθανό επακόλουθο την παραμέληση του a Posteriori ελέγχου. Η «γραφειοκρατικοποίηση» της λειτουργίας της μπορεί να συνεπάγεται με περαιτέρω προβλήματα στη σχέση της με τους πολίτες. Για την προκειμένω αποτελεσματικότητα της Αρχής κρίσιμη προϋπόθεση είναι η υπεράσπιση της ανεξαρτησίας της στην καθημερινή της λειτουργία και ο εντοπισμός των περιοχών ελέγχου που εμφανίζουν τους περισσότερους κινδύνους για τους πολίτες και ο αντίστοιχος προσδιορισμός των προτεραιοτήτων. Εξίσου αποφασιστική σημασία έχει και η αντίληψη που θα αναπτύξει η ίδια η Αρχή για το ρόλο της και τη σχέση της με τους ελεγχόμενους και τους πολίτες.[13]

5.5 Ηλεκτρονικό εμπόριο

 Οδηγία 2000/31/ΕΚ

Η συγκεκριμένη οδηγία αφορά υπηρεσίες της Κοινωνίας της Πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά κι εκδόθηκε για να αρθούν τα νομικά εμπόδια στην ανάπτυξη των υπηρεσιών της ΚΤΠ, εμπόδια που απορρέουν από τις αποκλίσεις των νομοθεσιών και από την έλλειψη ασφάλειας δικαίου όσον αφορά την έκταση του ελέγχου που μπορούν να ασκούν τα κράτη-μέλη σε υπηρεσίες από άλλα κράτη- μέλη.

Στόχος της οδηγίας είναι να εξασφαλιστούν η ασφάλεια δικαίου, η εμπιστοσύνη του καταναλωτή, η δημιουργία του κατάλληλου νομικού πλαισίου για την ελεύθερη κυκλοφορία των υπηρεσιών της ΚΤΠ, η κατάργηση των εσωτερικών συνόρων για το ηλεκτρονικό εμπόριο και η προστασία του καταναλωτή, των ανηλίκων και της ανθρώπινης αξιοπρέπειας.

Η οδηγία επιβάλλει την ελεύθερη και απρόσκοπτη από τα κράτη- μέλη κυκλοφορία των υπηρεσιών της ΚΤΠ που προέρχονται από άλλο κράτος- μέλος και απαλλάσσει τα κράτη-μέλη από την υποχρέωση να υπαγάγουν σε καθεστώς προηγούμενης άδειας τους φορείς παροχής υπηρεσιών της ΚΤΠ που επιθυμούν να αναλάβουν την άσκηση αντίστοιχων δραστηριοτήτων. Στη συνέχεια, η οδηγία ορίζει μια σειρά από γενικές πληροφορίες που πρέπει να παρέχει ο φορέας παροχής υπηρεσιών στους αποδέκτες του και στις αρμόδιες αρχές και διασφαλίζει την ακεραιότητα των εμπορικών επικοινωνιών με εγγυήσεις που αφορούν τις παρεχόμενες πληροφορίες, τη μη ζητηθείσα εμπορική επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου και την παροχή υπηρεσιών από νομοθετικώς κατοχυρωμένα επαγγέλματα.

Επίσης, η οδηγία θέτει ένα πλαίσιο μεταχείρισης των συμβάσεων που συνάπτονται με ηλεκτρονικά μέσα, ορίζει το μέτρο ευθύνης των μεσαζόντων παροχής υπηρεσιών, προβλέπει μέσα έννομης προστασίας των ενεχομένων συμφερόντων κι επιδιώκει να ενθαρρύνει τη θέσπιση κωδίκων δεοντολογίας από τις ενώσεις ή οργανώσεις επαγγελματιών και καταναλωτών.

Η οδηγία 2000/31 δεν καλύπτει την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την εμπιστευτικότητα των επικοινωνιών, καθώς αυτά καλύπτονται από τις οδηγίες 95/46 και 97/66 αντίστοιχα. Η συγκεκριμένη οδηγία ορίζει ποιες οικονομικές δραστηριότητες σε απευθείας σύνδεση (on- line) συνιστούν υπηρεσίες της ΚΤΠ και προάγει τη λειτουργία του υγιούς ανταγωνισμού μέσα στην εσωτερική αγορά μέσω εγγυήσεων για την παροχή πληροφοριών και την προστασία του καταναλωτή, αλλά και ενθαρρύνει τη συνεργασία με τις τρίτες χώρες στον τομέα του ηλεκτρονικού εμπορίου λόγω της παγκόσμιας φύσης των ηλεκτρονικών επικοινωνιών.[14]

ΕΡΕΥΝΑ – ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

1. ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Ερωτηματολόγιο Πτυχιακής Εργασίας Ασφάλεια Ηλεκτρονικών Συνναλαγων: Οδηγός Διασφάλισης Των Ελληνικών Επιχειρήσεων

Α.Τ.Ε.Ι ΠΑΤΡΩΝ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ & ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επιμέλεια: Γιώργος Τσικουδάκης (george__chania@hotmail.com)
Μανώλης Ζης (gargadoun@hotmail.com)
Παναγιώτης Παππάς

1.Χρησιμοποιείτε Ηλεκτρονικό Υπολογιστή:

- ◯ Ναι
- ◯ Όχι

2.Αν "ναι", πόσες φορές την εβδομάδα:

1	2	3	4	5	6	7
◯	◯	◯	◯	◯	◯	◯

3.Διαθέτετε στην κατοικία σας δίκτυο;

(INTERNET)

- ◯ Ναι
- ◯ Όχι

4.Τι γραμμή παροχής διαθέτετε;

- ○ Dial-Up
- ○ DSL
- ○ Άλλη (Καλωδιακή,E1,E3,..)
- ○ Σύνδεση με κινητό (GSM,GPRS,UMTS,EDGE,..)

5.Πώς θα χαρακτηρίζατε τον εαυτό σας ως χρήστη του διαδικτύου;

- ○ Αρχάριος (χρησιμοποιώ το διαδίκτυο περιστασιακά, κυρίως για e-mail)
- ○ Μέτριος (καθημερινά στο διαδίκτυο για e-mail, ενημέρωση, διασκέδαση, αλλά δεν το εμπιστεύομαι για αγορές)
- ○ Έμπειρος (καθημερινή χρήση, έχω πραγματοποιήσει διαδικτυακές αγορές)
- ○ Εξειδικευμένος (έμπειρος χρήστης με γνώσεις προγραμματισμού)

6.Πραγματοποιείτε ηλεκτρονικές ενέργειες η φοβάστε κάτι;

(εξασφάλιση πληροφοριών,αγορές,διοικητικές υποθέσεις,κ.α)

- ○ Ναι
- ◉ Οχι

7.Αν παραπάνω επιλέξατε "ναι" και πραγματοποιείτε , ποιές είναι αυτές;

8.Αν παραπάνω επιλέξατε "οχι" και φοβάστε κάτι, τι είναι αυτό;

9.Θα μπορούσατε ενδεχομένως να ψωνίζετε ηλεκτρονικά αντί για παραδοσιακά;

- Ναι
- Όχι

10.Χρησιμοποιείσατε τον Η/Υ σας τον τελευταίο καιρό για ηλεκτρονικές συναλλαγές;

(Ψώνια,Ηλεκτρονικές Πληρωμές)

- Ναι
- Οχι

11. Έχετε χρησιμοποιήσει το δίκτυο για κάτι απο τα παρακάτω;

- [ ] Εξασφάλιση Πληροφοριών
- [ ] Λήψη εντύπων σε ηλεκτρονική μορφή
- [ ] Διαχείρηση διοικητικής υπόθεσης (π.χ φορ.δηλώσεις,εγγραφές,κ.α)
- [ ] Άλλο
- [ ] Όχι

12.Για ποιο λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet;

ΠΡΟΣΟΧΗ: Απαντήστε στην συγκεκριμένη ερώτηση μόνο αν ΔΕΝ έχετε πραγματοποιήσει αγορά/συναλλαγή από το Internet. (όπου 1 ελάχιστο, όπου 5 μέγιστο)

	1	2	3	4	5
Δεν έχω νιώσει την ανάγκη/ Είμαι ευχαριστημένος με το φυσικό κατάστημα	○	○	○	○	○
Δεν αισθάνομαι άνετα με το να μη μπορώ να αγγίξω/παρατηρήσω από κοντά κάτι πριν το αγοράσω	○	○	○	○	○
Τα προϊόντα μπορεί να αργήσουν κατά την αποστολή ή και να μη φτάσουν ποτέ	○	○	○	○	○
Οι παραγγελίες μέσω Internet είναι περίπλοκες και γενικά δεν αισθάνομαι άνετα.	○	○	○	○	○
Φοβάμαι ότι το προϊόν που θα παραλάβω δεν θα είναι αυτό που έχω παραγγείλει.	○	○	○	○	○
Φοβάμαι να δημοσιεύσω τα προσωπικά μου στοιχεία στο internet (π.χ.πιστωτική κάρτα)	○	○	○	○	○
Άλλο	○	○	○	○	○

13.Γνωρίζετε ποιά δεδομένα θεωρούνται προσωπικά;

- ○ Ναι
- ○ Όχι

14.Έχετε πέσει ποτέ θύμα ηλεκτρονικής υποκλοπής;

- ◯ Ναι
- ◉ Όχι

15.Γνωρίζετε κάτι σχετικά με ιούς,trojans,worms που μπορούν να αποκαλύψουν προσωπικά σας δεδομένα;

- ◯ Ναι
- ◯ Όχι

16.Γνωρίζετε τι είναι το e-fishing;

(ηλεκτρονικό ψάρεμα)

- ◯ Ναι
- ◯ Όχι

17.Ποια από τις παρακάτω ομάδες ατόμων θα συμβουλευόσασταν για πληροφορίες για αγορά από το internet;

Μπορείτε να επιλέξετε παραπάνω από μία ομάδα.

- ☐ Οικογένεια
- ☐ Φίλοι
- ☐ Συνάδελφοι
- ☐ Μέλη Forum
- ☐ Ειδικοί (Δημοσιογράφοι κλάδου πληροφορικής, πωλητές)
- ☐ Καμία, αποφασίζω μόνος μου

18.Θα ενθαρρύνατε τους φίλους και τους συγγενείς σας να πραγματοιήσουν αγορά προϊόντων μέσω ηλεκτρονικού καταστήματος;

- ◯ Ναι
- ◯ Όχι

19.Συμπληρώστε το φύλο σας:

- Άνδρας
- Γυναίκα

20.Σε ποια ηλικιακή ομάδα ανήκετε;

- 0-17
- 18-24
- 25-30
- 31-40
- 41-50
- 51 +

21.Ποιο είναι το μορφωτικό σας επίπεδο:

- Γυμνάσιο
- Λύκειο
- Α.Ε.Ι - Τ.Ε.Ι
- Μεταπτυχιακό
- Διδακτορικό

22.Ποια είναι η Επαγγελματική σας Κατάσταση;

- Άνεργος
- Φοιτητής
- Ημιαπασχόληση
- Πλήρης Απασχόληση
- Άλλο:

Ευχαριστούμε πολύ για τον χρόνο σας.

2. ΣΚΟΠΟΣ ΕΡΕΥΝΑΣ & ΣΧΕΔΙΑΣΜΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

I. Σκοπός της έρευνας

Η παρούσα ερευνητική μελέτη καλείται:

a. Να διερευνήσει τους παράγοντες που επηρεάζουν τις στάσεις και τις πεποιθήσεις των Ελλήνων χρηστών διαδικτύου σχετικά με τις ηλεκτρονικές συναλλαγές.

b. Να ερευνήσει τη συχνότητα χρήσης των ηλεκτρονικών συναλλαγών.

c. Να ερευνήσει τις προτιμήσεις των Ελλήνων σχετικά με τις ηλεκτρονικές συναλλαγές.

II. Αναγκαιότητα της έρευνας

Η αναγκαιότητα της παρούσας έρευνα απορρέει από το γεγονός ότι οι ηλεκτρονικές συναλλαγές αναπτύσσονται ταχύτατα την τελευταία δεκαετία και αποτελούν σημαντικό παράγοντα για την επιχειρηματικότητα και κατ' επέκταση και για την οικονομία.

III. Επιλογή μεθοδολογίας

Η παρούσα ερευνητική προσέγγιση αποτελεί μια έρευνα 'πεδίου/επισκόπησης'. Για την επίτευξη των στόχων αλλά και την διερεύνηση των υποθέσεων της συγκεκριμένης έρευνα χρησιμοποιήθηκε η μέθοδος του ηλεκτρονικού γραπτού ερωτηματολογίου, η επιλογή της

οποίας έγινε με τα παρακάτω κριτήρια:

a. Τα άτομα που συμμετέχουν στην έρευνα απαντούν απρόσωπα, ανώνυμα και εύκολα.

b. Παρέχεται αρκετός χρόνος για να σκεφτούν την απάντησή τους.

c. Η μέθοδος αυτή διευκολύνει τη στατιστική ανάλυση και επεξεργασία των δεδομένων.

d. Η συλλογή των στοιχείων γίνεται γρήγορα και εύκολα.

e. Μας δίνει τη δυνατότητα συλλογής μεγάλου όγκου πληροφοριών σε σύντομο χρονικό διάστημα.

Ωστόσο η μέθοδος αυτή εμφανίζει κάποια μειονεκτήματα όπως, οι πιθανές ανακριβείς απαντήσεις, οι στάσεις των ατόμων που συμμετέχουν στην έρευνα, η εξιδανίκευση των απαντήσεων και η έλλειψη αυθορμητισμού.

IV. Σχετικά με την έρευνα

Το ερωτηματολόγιο της έρευνας πραγματοποιήθηκε από τις 11-10-2010 έως τις 10-11-2010 και αναρτήθηκε σε ιστότοπο στο οποίο κατευθύνθηκαν άτομα από όλα τα κοινωνικά στρώματα και ηλικίες για να απαντήσουν.

Συγκεντρώθηκαν συνολικά 203 απαντήσεις τις οποίες καταχωρήθηκαν σε excel ανά απάντηση και ανά άτομο.

Στη συνέχεια επεξεργαστήκαμε τις απαντήσεις και επεξηγήσαμε το καθένα γραπτώς

εκφράζοντας και συμπεράσματα.

Επίσης κατασκευάστηκαν και διαγράμματα με ποσοστά και αποτελέσματα ανά ερώτηση.

Οι ερωτήσεις αποδόθηκαν εξαρχής για να κατανοήσουμε την ελληνική αγορά. Το κατά πόσο χρησιμοποιεί Η/Υ και τι τύπο σύνδεσης χρησιμοποιεί και από πού, μέχρι το αν γνωρίζει θεωρητικά θέματα όπως τι είναι το e-fishing και ποια δεδομένα θεωρούνται προσωπικά, όπως επίσης και το κατά πόσο έχει εμπιστοσύνη στις ηλεκτρονικές συναλλαγές.

Αρχικά, με τη χρήση του Η/Υ σε καθημερινή βάση και ανάλογα την ηλικία του κάθε χρήστη, φτάνουμε στο συμπέρασμα ότι ακόμα και μεγαλύτερη ηλικίας άτομα 50+ χρησιμοποιούν Η/Υ, ενώ για τους 18-24 είναι αναπόσπαστο κομμάτι της καθημερινότητας τους.

Ενθαρρυντικό ποσοστό εμφανίζεται το 47,3% των ερωτηθέντων οι οποίοι πραγματοποιούν ηλεκτρονικές συναλλαγές με το 95,2% να μην έχει πέσει ποτέ θύμα υποκλοπής.

3. ΑΠΑΝΤΗΣΕΙΣ ΕΡΩΤΗΘΕΝΤΩΝ

	A	B	C	D	E	F	G
1	Χρονική σήμανση	1.χρησιμοποιείτε Η/Υ;		2.αν ναί, πόσες φορές την εβδομάδα;		3.διαθέτετε στην κατοικία σας δίκτυο;	
2	ΠΛΗΘΟΣ	188					
3		ΟΧΙ	0,005319149	1	0	ΟΧΙ	0,037234043
4		ΝΑΙ	0,994680851	2	0,005319149	ΝΑΙ	0,957446809
5				3	0,005319149	Δεν ξέρω	0,005319149
6				4	0,005319149		
7				5	0,058510638		
8				6	0,085106383		
9				7	0,829787234		
10				Δεν ξέρω	0,010638298		

	H	I	J	K	L	M
1	4.τι γραμμή παροχής διαθέτετε;		5.πως θα χαρακτηρίζατε τον εαυτό σας σαν χρήστη του διαδικτύου;		6.πραγματοποιείτε ηλεκτρονικές συναλλαγές ή φοβάστε κατι;	
2						
3	DSL	0,882978723	εξειδικευμένος	0,154255319	ΟΧΙ	0,526596
4	Σύνδεση με κινητό	0,037234043	έμπειρος	0,462765957	ΝΑΙ	0,473404
5	Dial-Up	0,031914894	μέτριος	0,372340426		
6	Άλλη	0,021276596	αρχάριος	0,010638298		
7	Δεν ξέρω	0,026595745				

	N	O	P	Q
1	7.αν επιλέξατε "ναί" και πραγματοποιείτε, ποιές είναι αυτές;		8.αν παραπάνω επιλέξατε "όχι" και φοβάστε κάτι , τι είναι αυτό;	
2				
3	Εξασφάλιση	0,127	Παραβίαση προσωπικών δεδομένων	0,1
4	Αγορές	0,307	Εξαπάτηση	0,085
5	Πληρωμές	0,037	Άλλο	0,377
6	Παιχνίδια	0,019		
7				

	R	S	T	U	V	W
1	9.θα μπορούσατε ενδεχομένως να ψωνίζετε ηλεκτρονικά αντί για παραδοσιακά;		10.χρησιμοποιήσατε τον τελευταίο καιρό τον Η/Υ σας για ηλεκτρονικές συναλλαγές;		11.έχετε χρησιμοποιείσει το διαδίκτυο για κάτι από τα παρακάτω;	
2						
3	ΌΧΙ	0,340425532	ΌΧΙ	0,563829787		
4	ΝΑΙ	0,659574468	ΝΑΙ	0,436170213		
5						
6						
7						

	X	Y	Z	AA	AB	AC
1	12.για ποιό λόγο δεν έχετε προβεί σε ηλεκτρονική αγορά; [δεν έχω νιώσει την ανάγκη/είμαι		12.για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet; [δεν		12.για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet; [τα	
2						
3	1	0,04787234	1	0,058510638	1	0,042553191
4	2	0,04787234	2	0,037234043	2	0,095744681
5	3	0,127659574	3	0,085106383	3	0,138297872
6	4	0,079787234	4	0,10106383	4	0,069148936
7	5	0,164893617	5	0,14893617	5	0,079787234
8	dg/da	0,531914894	dg/da	0,569148936	dg/da	0,574468085

	AD	AE	AF	AG	AH	AI
1	12.για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet; [οι		12.για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet;		12..για ποιό λόγο δεν έχετε προβεί σε ηλεκτρονική αγορά; [φοβάμαι να δημοσιευσω τα	
2						
3	1	0,095744681	1	0,074468085	1	0,026595745
4	2	0,069148936	2	0,079787234	2	0,069148936
5	3	0,122340426	3	0,122340426	3	0,037234043
6	4	0,069148936	4	0,085106383	4	0,085106383
7	5	0,074468085	5	0,069148936	5	0,234042553
8	dg/da	0,569148936	dg/da	0,569148936	dg/da	0,531914894

	AJ	AK	AL	AM	AN	AO
1	12.για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet;		13.γνωρίζετε ποιά δεδομένα θεωρούνται προσωπικά;		14.έχετε πέσει ποτέ θύμα ηλεκτρονικής υποκλοπής;	
2						
3	1	0,069148936	ΟΧΙ	0,14893617	ΟΧΙ	0,95212766
4	2	0,021276596	ΝΑΙ	0,85106383	ΝΑΙ	0,04787234
5	3	0,026595745				
6	4	0,010638298				
7	5	0,037234043				
8	dg/da	0,819148936				

	AP	AQ	AR	AS	AT	AU
1	15.γνωρίζετε κάτι σχετικά με ιούς,trojans,worms που μπορούν να αποκαλύψουν		16.γνωρίζετε τι είναι το e-fishing?		17.ποιά από τις παρακάτω ομάδες ατόμων θα συμβουλευόσασταν για αγορές μέσω internet;	
2						
3	ΟΧΙ	0,324468085	ΟΧΙ	0,54787234	Μέλη φορουμ	0,2
4	ΝΑΙ	0,675531915	ΝΑΙ	0,45212766	Οικογένεια	0,29
5					Ειδικοί	0,29
6					Φίλοι	0,63
7					Συνάδελφοι	0,19
8					Καμία αποφασίζω μόνος μου	0,17

	AV	AW	AX	AY	AZ	BA
1	18.θα ενθαρρύνατε φίλους και συγγενείς σας να πραγματοποιήσουν αγορές μέσω		19.συμπληρώστε το φύλο σας:		20.σε ποιά ηλικιακή ομάδα ανήκετε;	
2						
3	ΟΧΙ	0,393617021	ΑΝΔΡΑΣ	0,430851064	0-17	0,031914894
4	ΝΑΙ	0,60106383	ΓΥΝΑΙΚΑ	0,569148936	18-24	0,771276596
5					25-30	0,154255319
6					31-40	0,026595745
7					41-50	0,010638298
8					51+	0

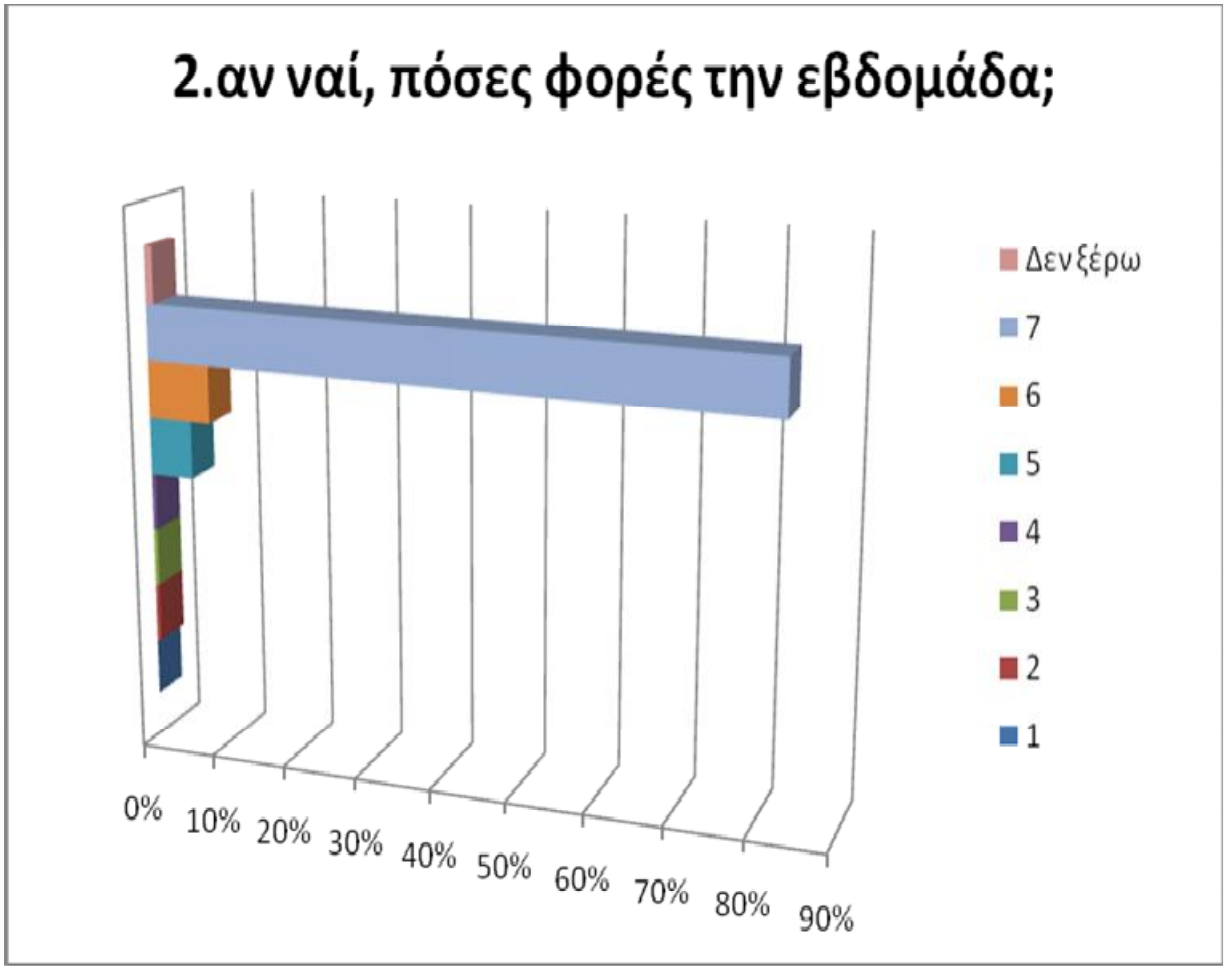
	BB	BC	BD	BE
1	21.ποιό είναι το μορφωτικό σας επίπεδο;		22.ποιά είναι η επαγγελματική σας κατάσταση;	
2				
3	gymnasium	0,010638298	ma8itis	0,015957447
4	Lyceum	0,132978723	Foititis	0,617021277
5	aei-tei	0,79787234	imiapasxolisi	0,074468085
6	master	0,04787234	pliris	0,196808511
7	doctora	0,010638298	anergos	0,04787234
8			strateusimos	0,005319149

4. ΔΙΑΓΡΑΜΜΑΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ & ΣΧΟΛΙΑΣΜΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ (*Επεξηγήσεις Ερωτηματολογίου*)

Διάγραμμα 1:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 1 η οποία είναι: χρησιμοποιείτε Η/Υ;

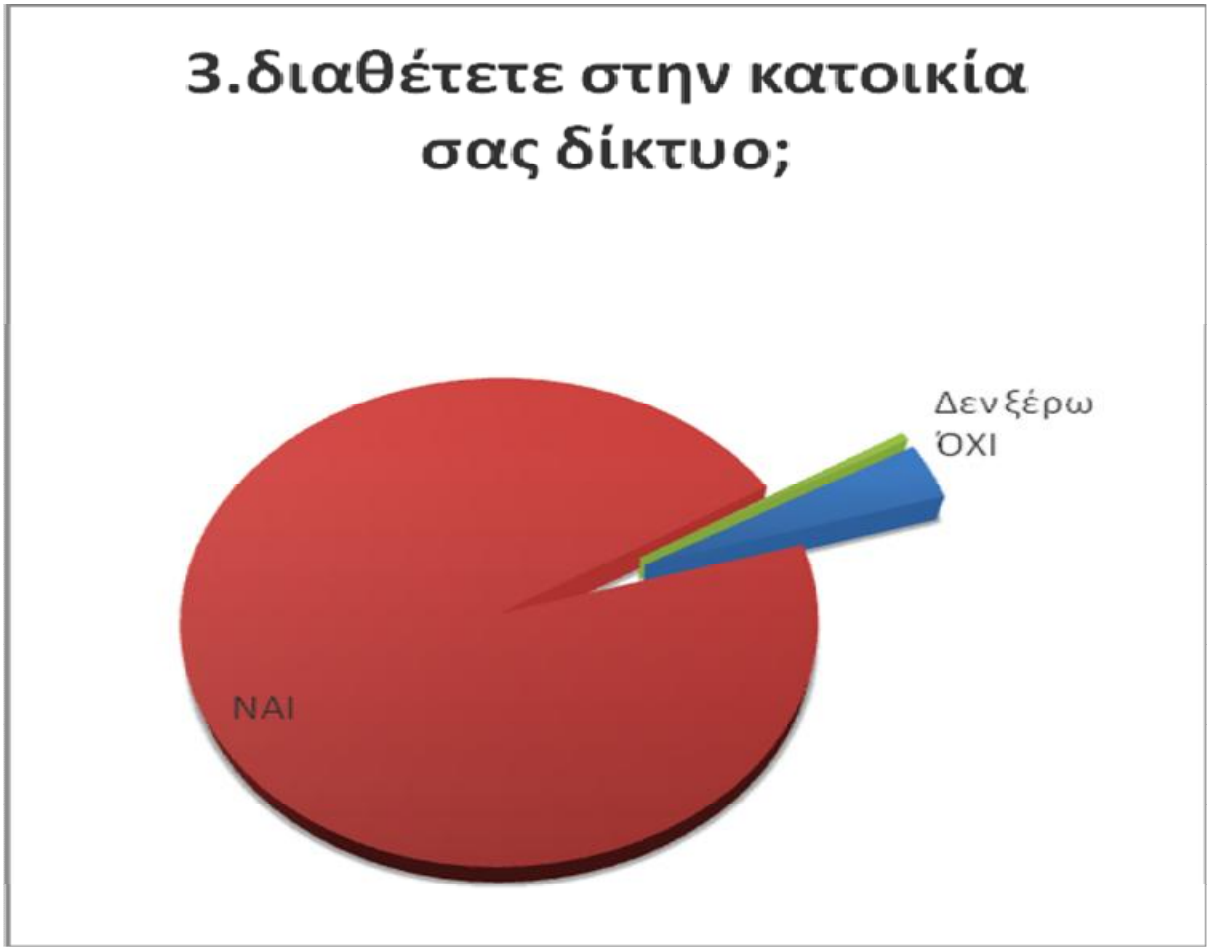
Από τους 188 που απάντησαν το 99,5% απάντησε ότι χρησιμοποιεί Η/Υ ενώ μόνο το 0,5% απάντησε ότι δεν χρησιμοποιεί.



Διάγραμμα2:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 2 η οποία είναι: αν ναι, πόσες φορές την εβδομάδα;

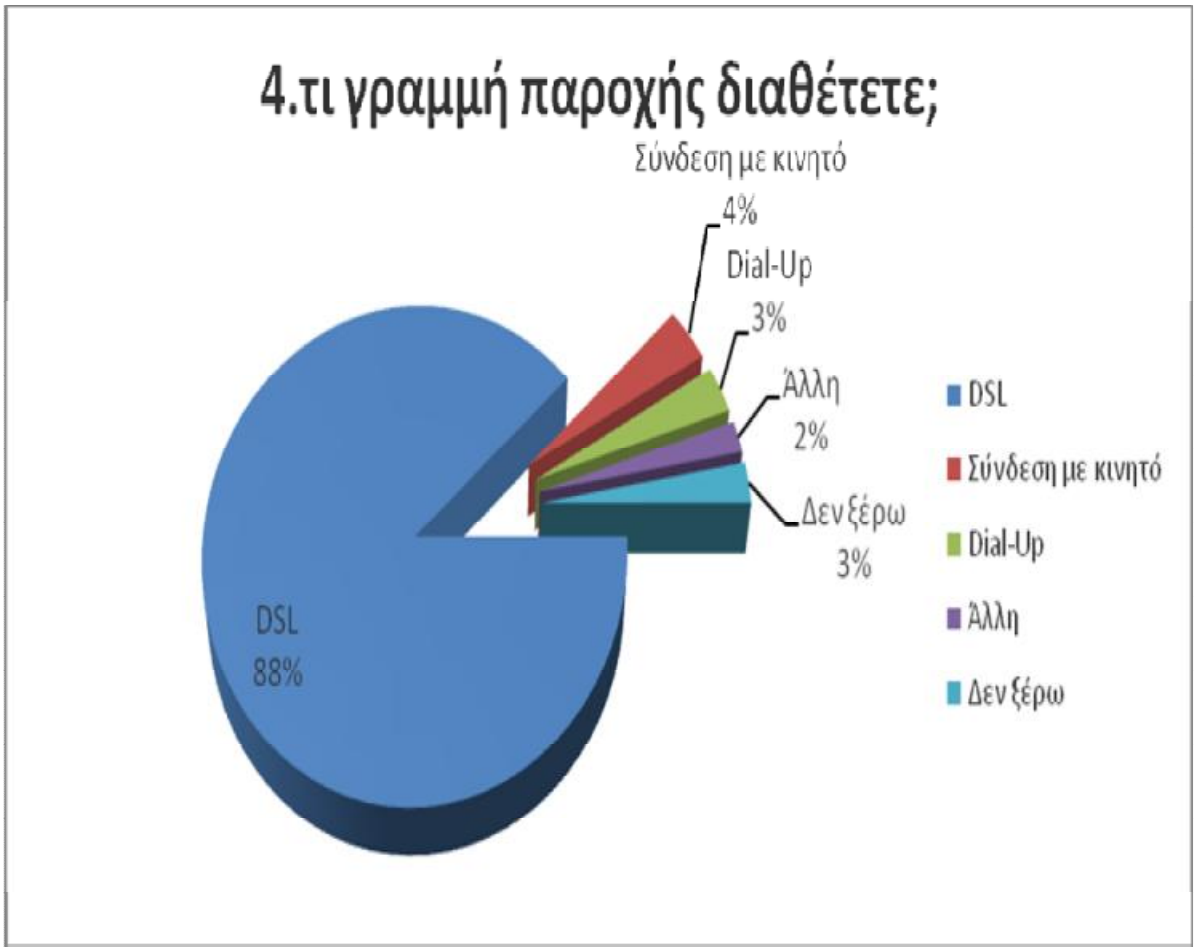
Από τους 188 που απάντησαν το 82,9% χρησιμοποιεί τον Η/Υ καθημερινά, το 8,5% 6 φορές την εβδομάδα, το 5,8% 5 φορές την εβδομάδα , το 0,5% 4,3 ή 2 ημέρες την εβδομάδα ενώ το 1% απάντησε ότι δεν γνωρίζει.



Διάγραμμα 3:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 3 η οποία είναι: διαθέτετε στην κατοικία σας δίκτυο;

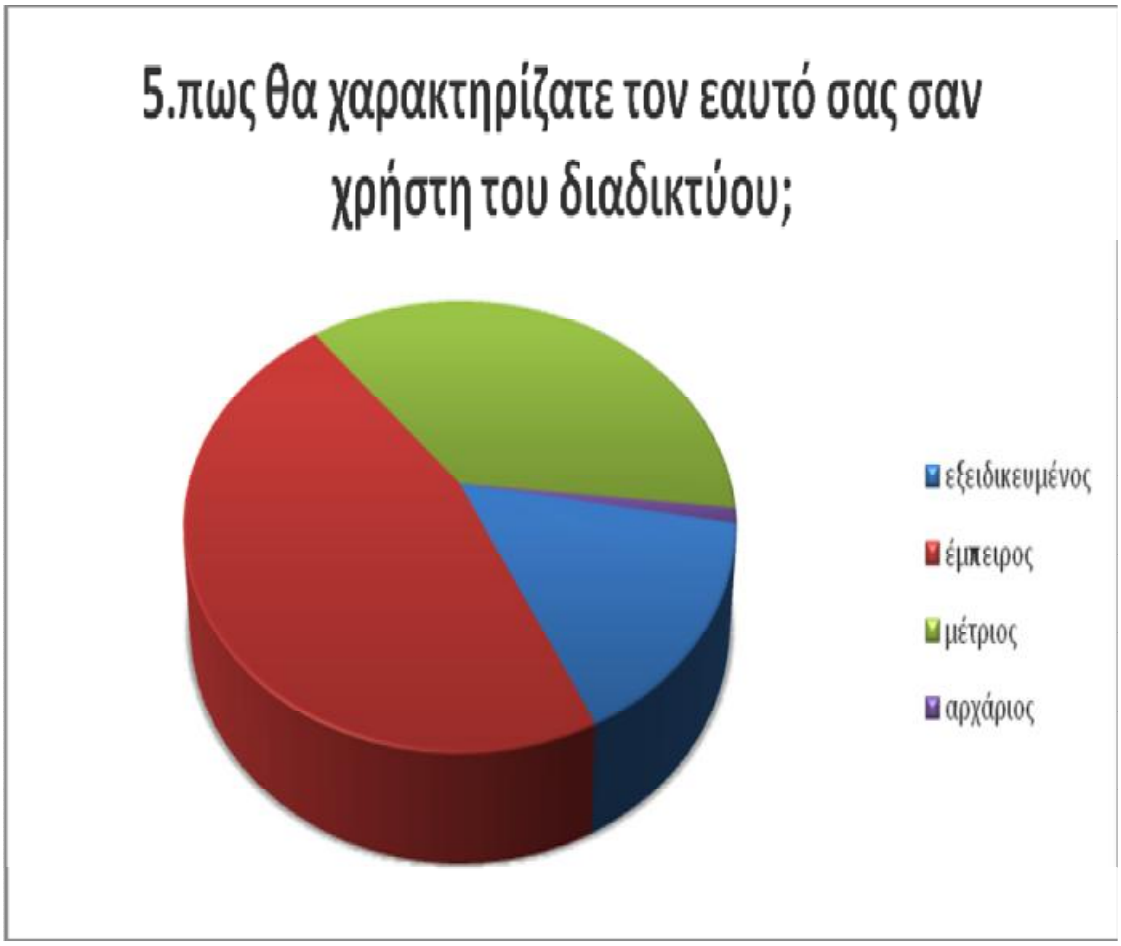
Από τους 188 που απάντησαν το 95,7% διαθέτει δίκτυο στο σπίτι του, το 3,7% δεν διαθέτει ενώ το 0,5% δεν γνωρίζει.



Διάγραμμα 4:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 4 η οποία είναι: τι γραμμή παροχής διαθέτετε;

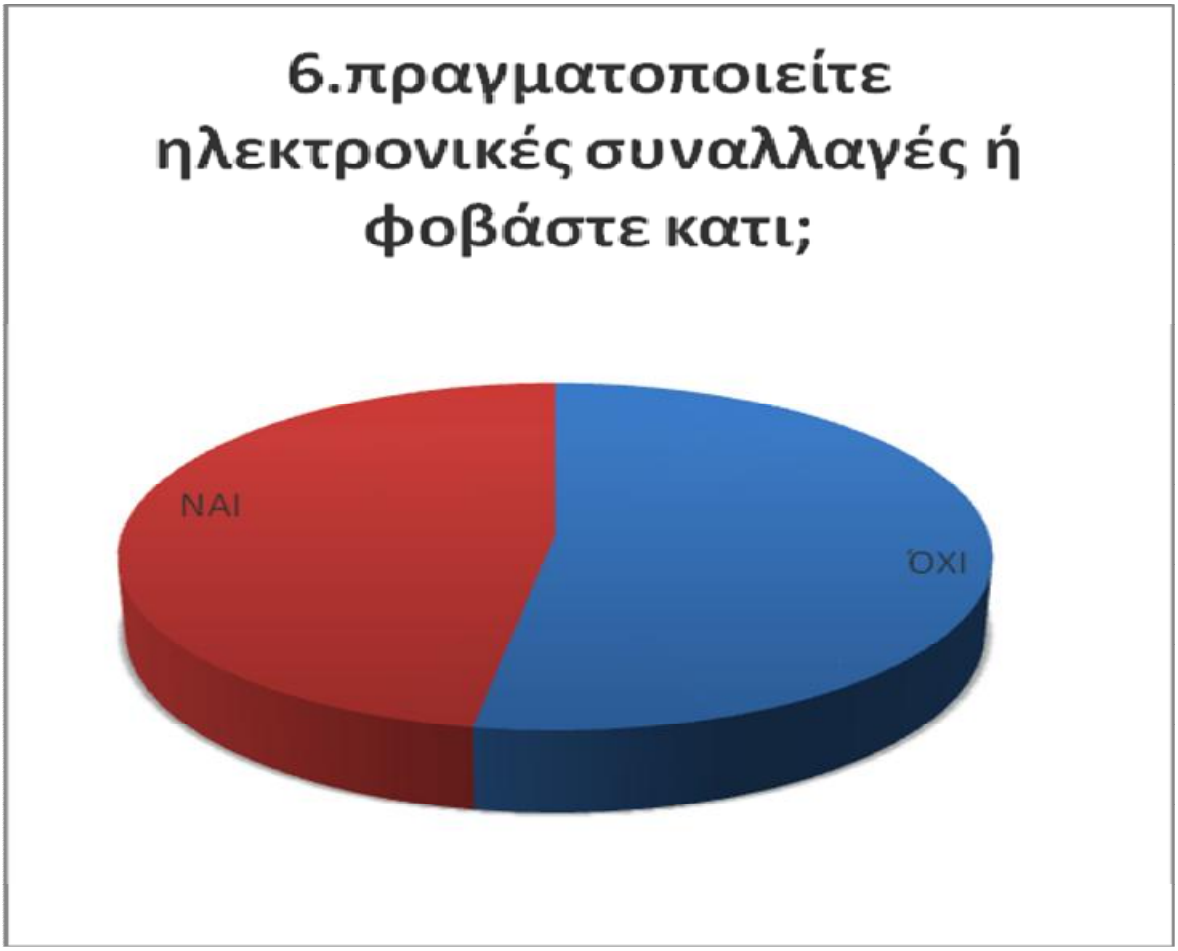
Από τους 188 που απάντησαν το 88% διαθέτει DSL σύνδεση, το 3,7% σύνδεση με κινητό, το 3,2% απλή σύνδεση dial-up, το 2,1% άλλου τύπου ενώ το 2,6% δεν γνωρίζει τον τύπο της γραμμής παροχής.



Διάγραμμα 5:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 5 η οποία είναι: πως θα χαρακτηρίζατε τον εαυτό σας σαν χρήστη του διαδικτύου;

Από τους 188 που απάντησαν το 46,2% χαρακτηρίζει τον εαυτό του ως έμπειρο χρήστη, το 37,2% ως μέτριο , το 15,4% εξειδικευμένο ενώ μόλις το 1% θεωρεί τον εαυτό του αρχάριο.



Διάγραμμα 6:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 6 η οποία είναι: πραγματοποιείτε ηλεκτρονικές συναλλαγές ή φοβάστε κάτι;

Από τους 188 που απάντησαν το 52,6% ΔΕΝ πραγματοποιεί ηλεκτρονικές συναλλαγές ενώ το 47,3% πραγματοποιεί.

Διάγραμμα 7:

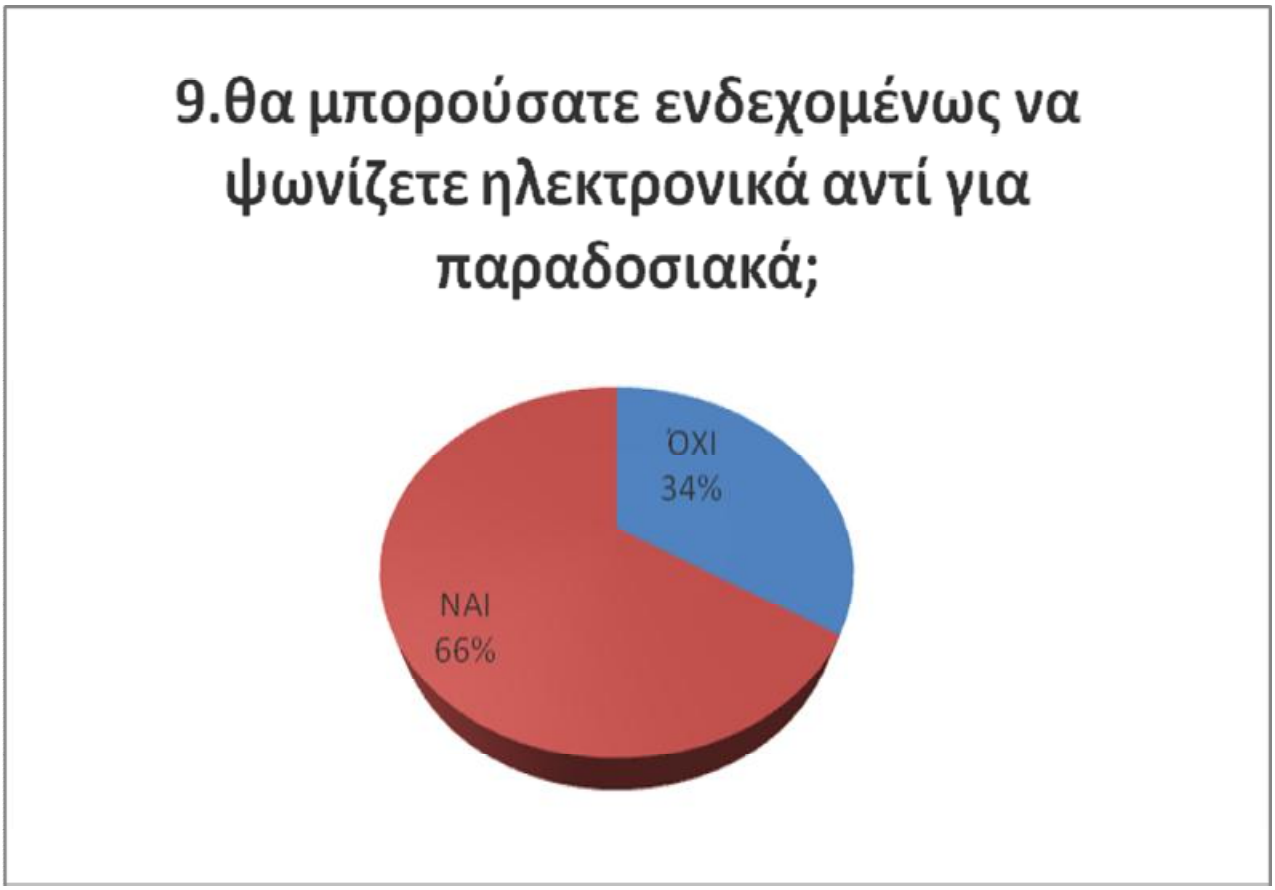
Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 7 η οποία είναι: αν επιλέξατε "ναι" και πραγματοποιείτε, ποιές είναι αυτές;

Από αυτούς που απάντησαν καταφατικά στην προηγούμενη ερώτηση το 30,7% πραγματοποιεί ηλεκτρονικές αγορές, το 12,7% εξασφαλίζει πληροφόρηση, το 3,7% πραγματοποιεί ηλεκτρονικές πληρωμές ενώ μόλις το 1,9% πραγματοποιεί συναλλαγές που αφορούν διαδικτυακά παιχνίδια.

Διάγραμμα 8:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 8 η οποία είναι: αν παραπάνω επιλέξατε "όχι" και φοβάστε κάτι , τι είναι αυτό;

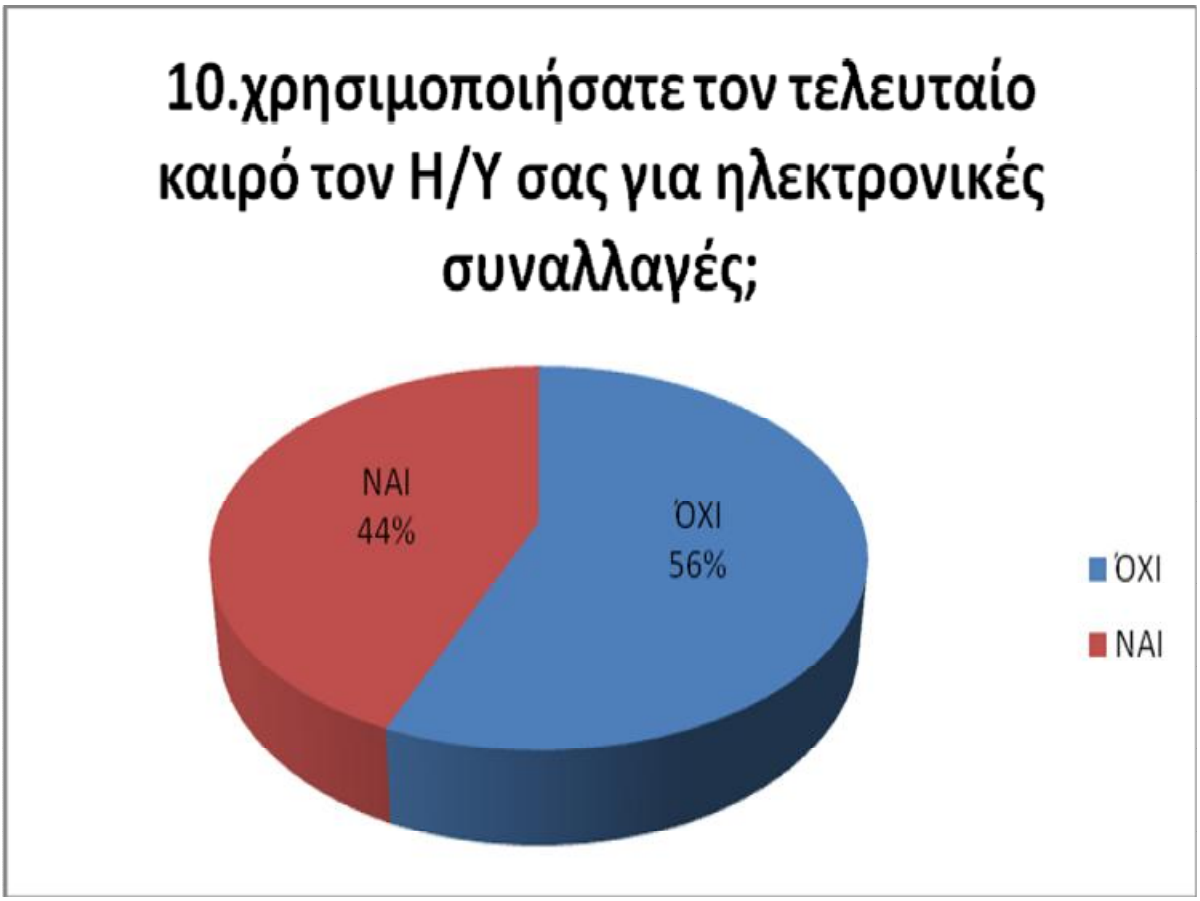
Από αυτούς που απάντησαν αρνητικά στην ερώτηση 6 το 10% φοβάται την παραβίαση προσωπικών δεδομένων, το 8,5% την εξαπάτηση ενώ το 37,7% φοβάται κάποιον άλλο παράγοντα.



Διάγραμμα 9:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 9 η οποία είναι: θα μπορούσατε ενδεχομένως να ψωνίζετε ηλεκτρονικά αντί για παραδοσιακά;

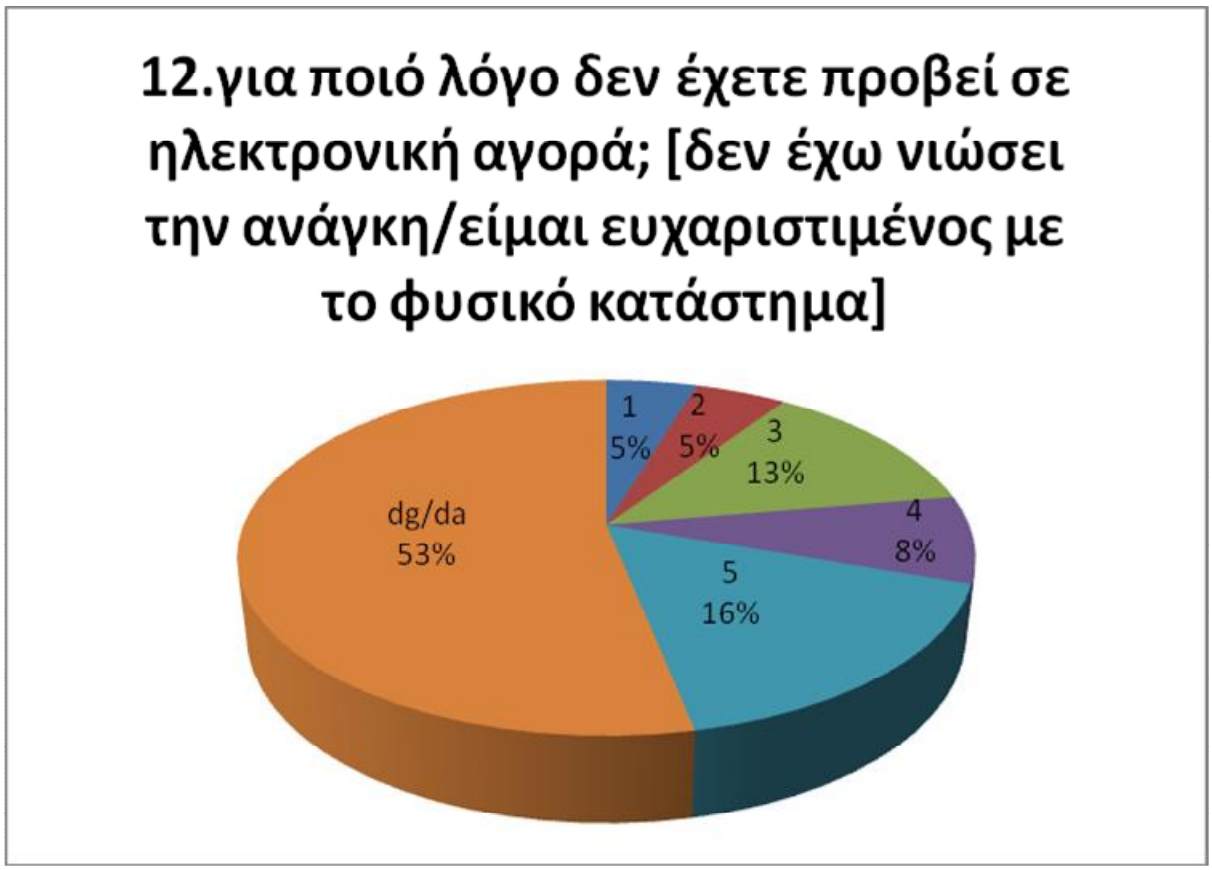
Από τους 188 που απάντησαν το 66% εμφανίζεται θετικό στις ηλεκτρονικές αγορές ενώ το 34% έρχεται σε αντίθεση με αυτές.



Διάγραμμα 10:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 10 η οποία είναι: χρησιμοποιήσατε τον τελευταίο καιρό τον Η/Υ σας για ηλεκτρονικές συναλλαγές;

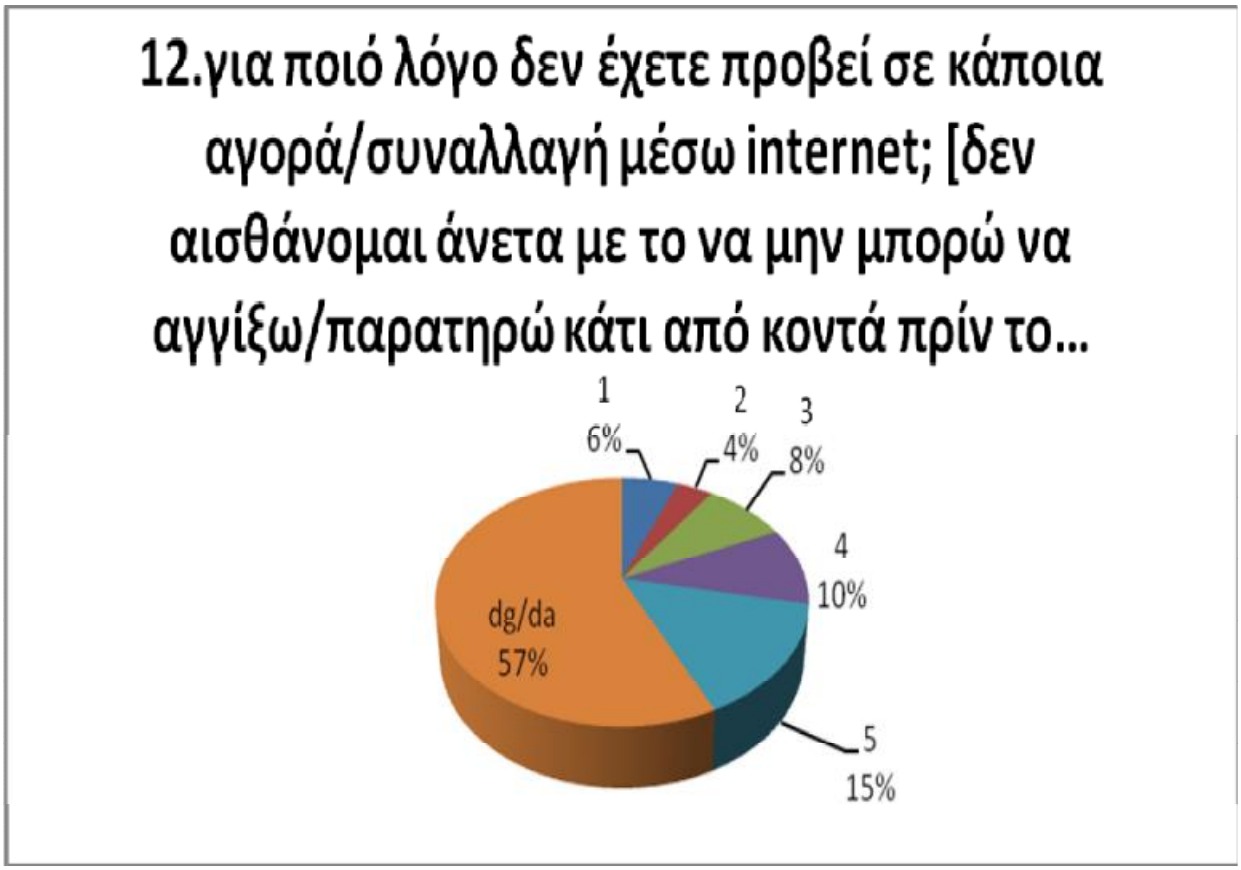
Από τους 188 που απάντησαν το 56,4% δεν έχει χρησιμοποιήσει τον Η/Υ του τελευταία για ηλεκτρονική συναλλαγή ενώ το 43,6% απάντησε ότι έχει χρησιμοποιήσει.



Διάγραμμα 12α:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε ηλεκτρονική αγορά; α.[δεν έχω νιώσει την ανάγκη/είμαι ευχαριστημένος με το φυσικό κατάστημα] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

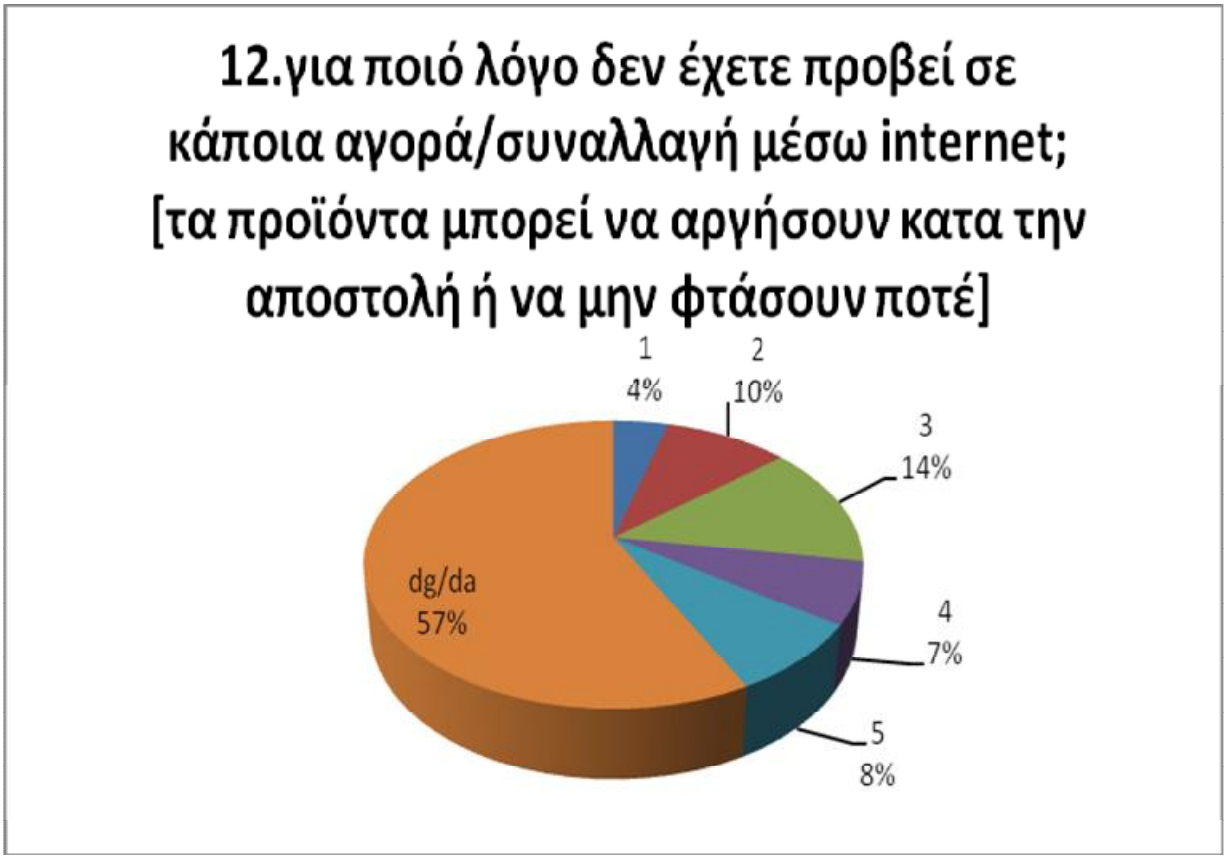
Από τους 188 που απάντησαν το 16,4% δεν έχω νιώσει την ανάγκη ή είναι ευχαριστημένο με το φυσικό κατάστημα με βαθμό ικανοποίησης 5, το 7,9% με βαθμό ικανοποίησης 4, το 12,7% με βαθμό ικανοποίησης 3, το 4,7% με βαθμό ικανοποίησης 2, το 4,7% με βαθμό ικανοποίησης 1 ενώ το 53,1% δεν δίνει απάντηση.



Διάγραμμα 12β:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet ; β.[δεν αισθάνομαι άνετα με το να μην μπορώ να αγγίξω/παρατηρώ κάτι από κοντά πριν το αγγίξω] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

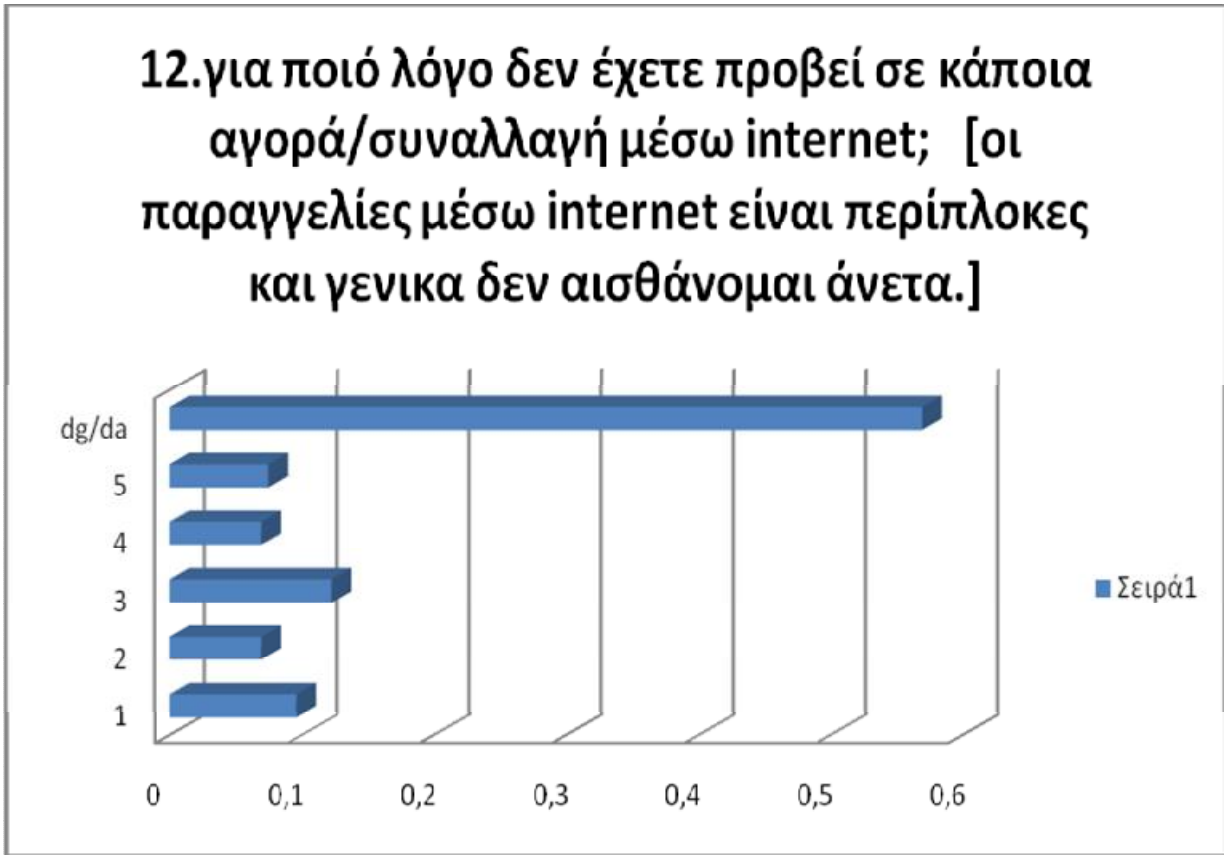
Από τους 188 που απάντησαν το 14,8% δεν αισθάνεται άνετα με το να μην μπορεί να αγγίξει ή να παρατηρήσει από κοντά το προϊόν με βαθμό ικανοποίησης 5, το 10,1% με βαθμό ικανοποίησης 4, το 8,5% με βαθμό ικανοποίησης 3, το 3,7% με βαθμό ικανοποίησης 2, το 5,8% με βαθμό ικανοποίησης 1 ενώ το 56,9% δεν δίνει απάντηση.



Διάγραμμα 12γ:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet ; [τα προϊόντα μπορεί να αργήσουν κατά την αποστολή ή να μην φτάσουν ποτέ] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

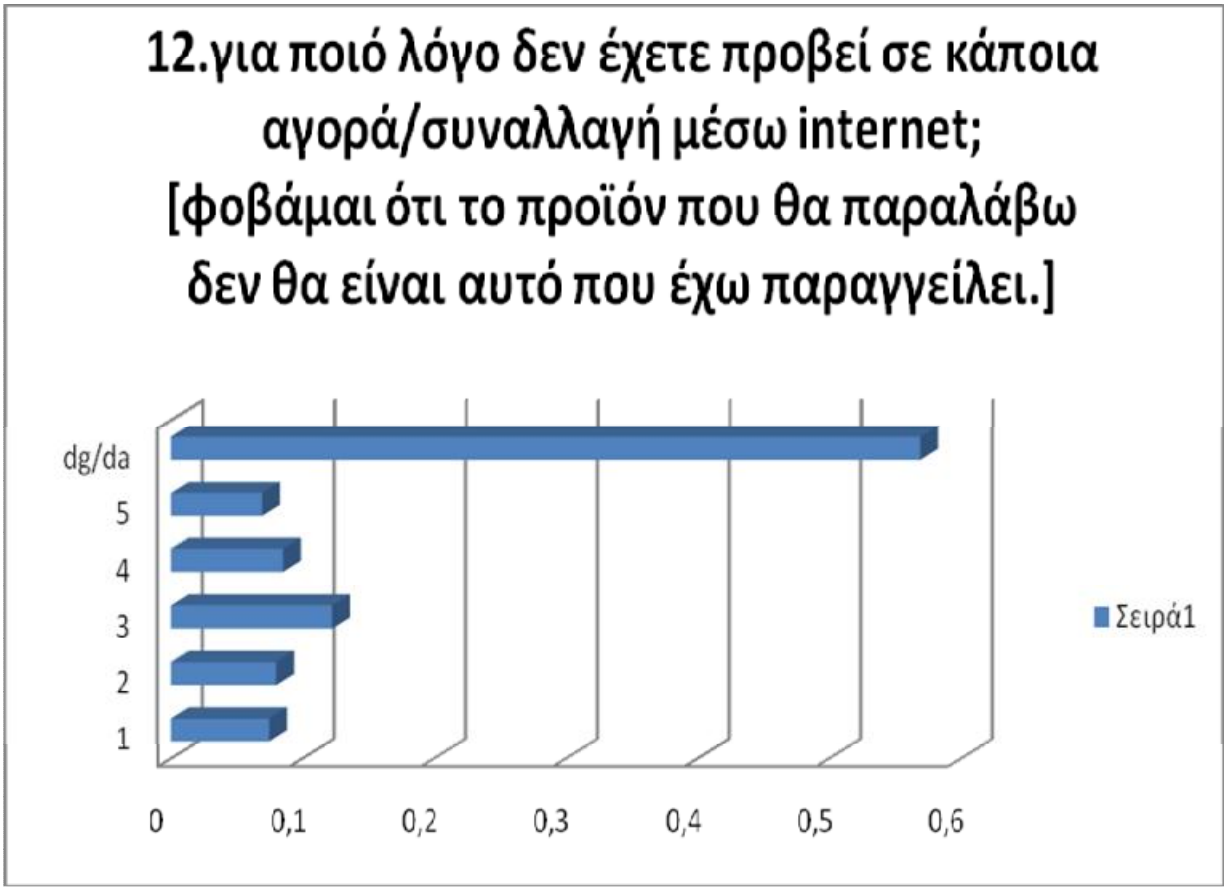
Από τους 188 που απάντησαν το 7,9% ανησυχεί εάν τα προϊόντα αργήσουν κατά την αποστολή ή δεν φτάσουν ποτέ με βαθμό ικανοποίησης 5, το 6,9% με βαθμό ικανοποίησης 4, το 13,8% με βαθμό ικανοποίησης 3, το 9,5% με βαθμό ικανοποίησης 2, το 4,2% με βαθμό ικανοποίησης 1 ενώ το 57,4% δεν δίνει απάντηση.



Διάγραμμα 12δ:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet ; [οι παραγγελίες μέσω internet είναι περίπλοκες και γενικά δεν αισθάνομαι άνετα.] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

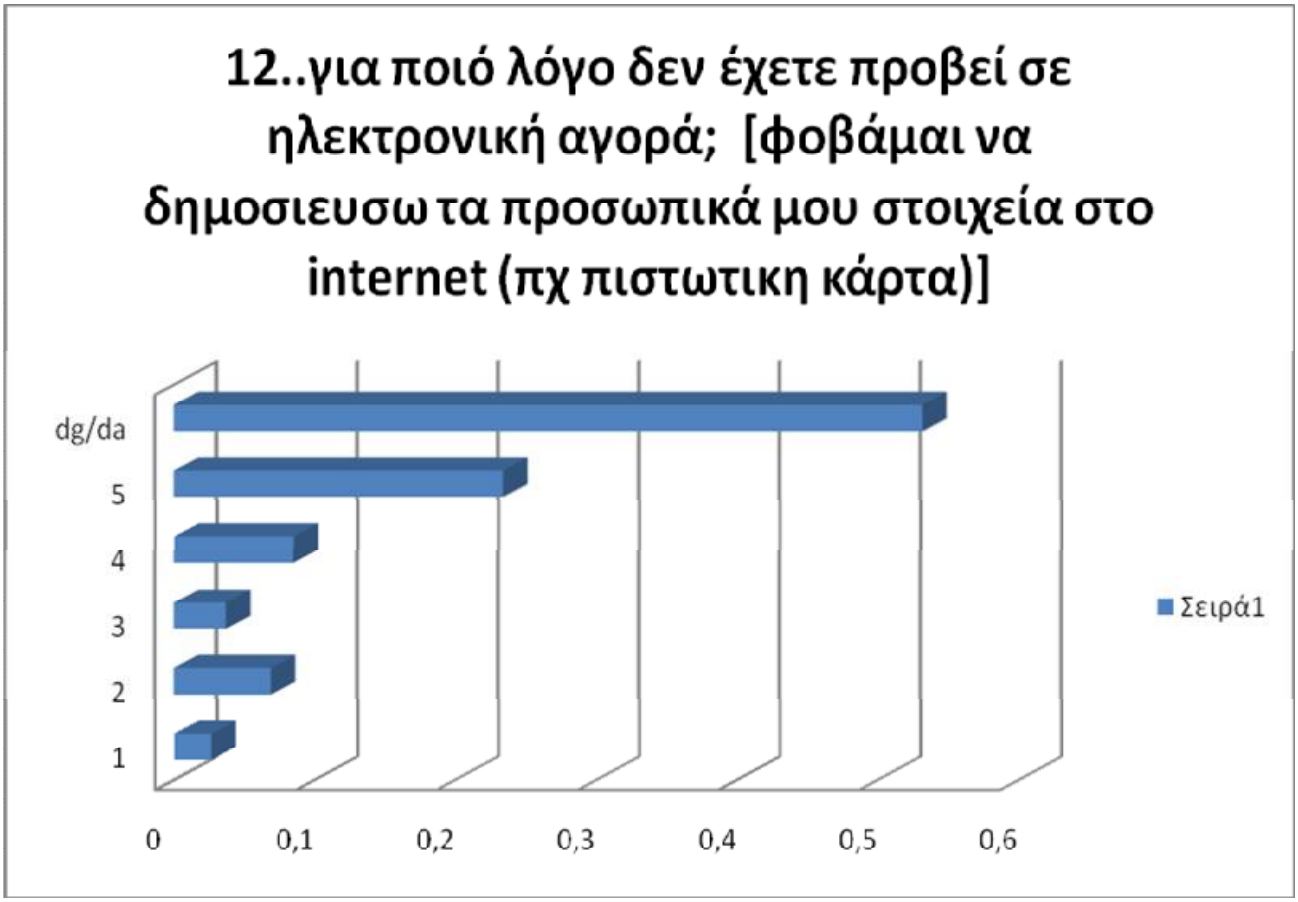
Από τους 188 που απάντησαν το 7,4% θεωρεί ότι οι παραγγελίες μέσω internet είναι περίπλοκες με βαθμό ικανοποίησης 5, το 6,9% με βαθμό ικανοποίησης 4, το 12,2% με βαθμό ικανοποίησης 3, το 6,9% με βαθμό ικανοποίησης 2, το 9,5% με βαθμό ικανοποίησης 1 ενώ το 56,9% δεν δίνει απάντηση.



Διάγραμμα 12ε:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet ; [φοβάμαι ότι το προϊόν που θα παραλάβω δεν θα είναι αυτό που έχω παραγγείλει.] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

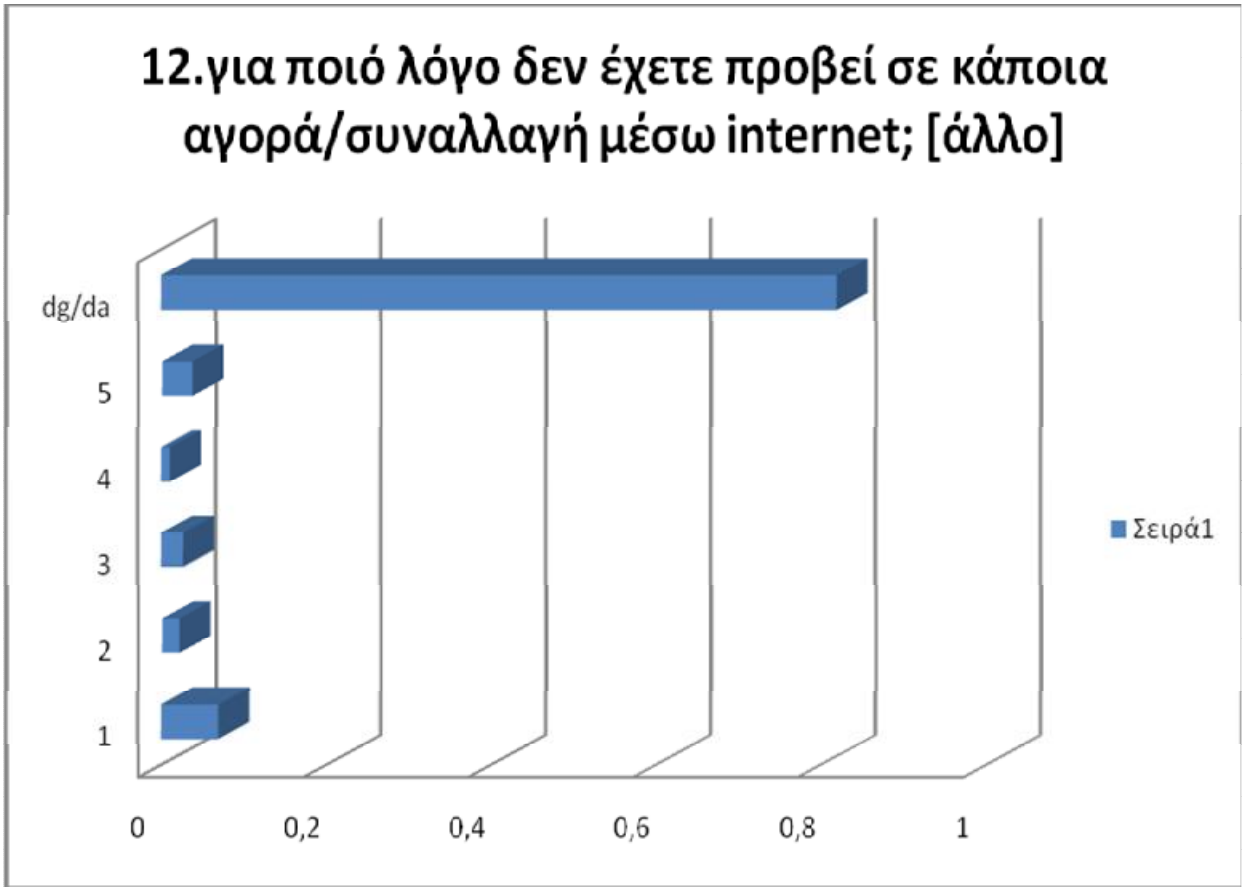
Από τους 188 που απάντησαν το 6,9% φοβάται ότι το προϊόν που παρήγγειλε δεν θα αντιστοιχεί σε αυτό που θα παραλάβει με βαθμό ικανοποίησης 5, το 8,5% με βαθμό ικανοποίησης 4, το 12,2% με βαθμό ικανοποίησης 3, το 7,9% με βαθμό ικανοποίησης 2, το 7,4% με βαθμό ικανοποίησης 1 ενώ το 56,9% δεν δίνει απάντηση.



Διάγραμμα 12στ:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε ηλεκτρονική αγορά; [φοβάμαι να δημοσιεύσω τα προσωπικά μου στοιχεία στο internet (πχ πιστωτική κάρτα)] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

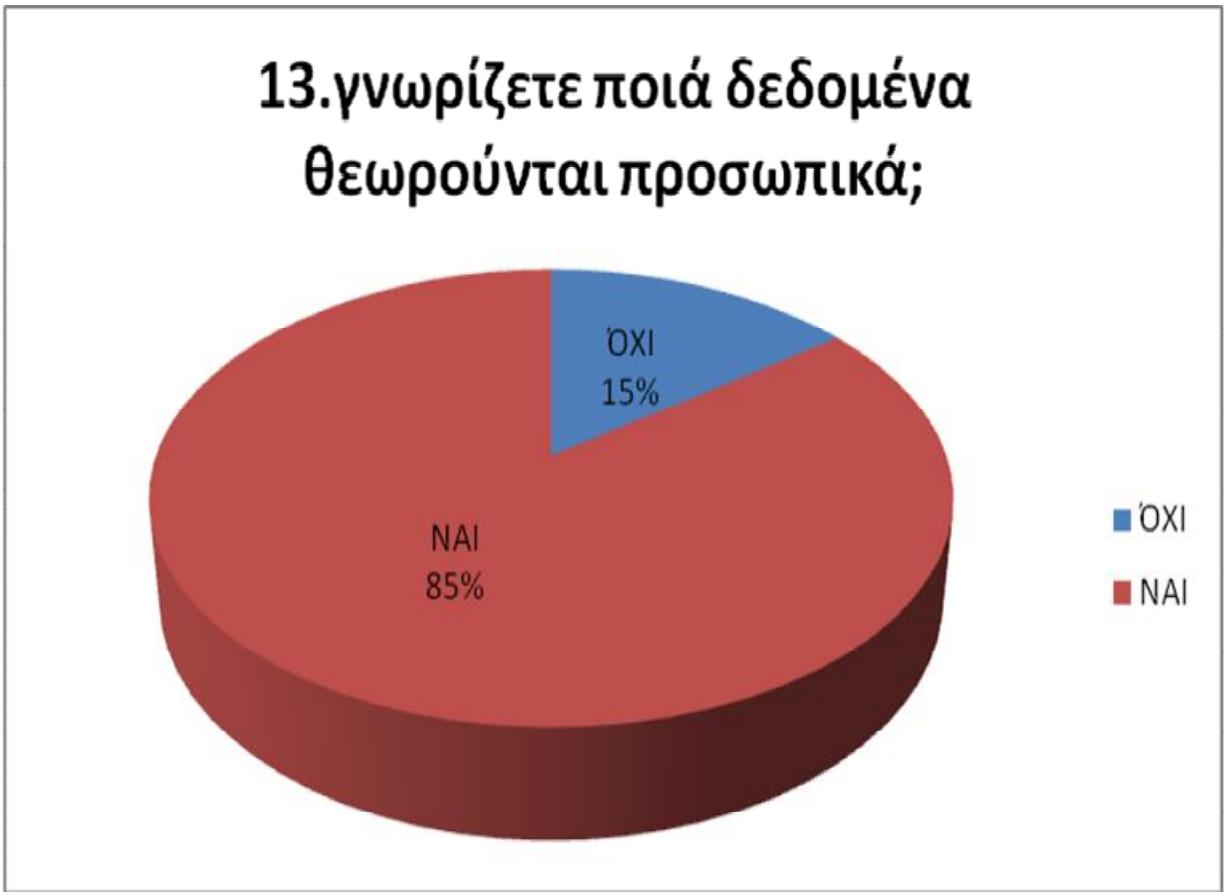
Από τους 188 που απάντησαν το 23,4% φοβάται να δημοσιεύσει τα προσωπικά του στοιχεία στο internet με βαθμό ικανοποίησης 5, το 8,5% με βαθμό ικανοποίησης 4, το 3,7% με βαθμό ικανοποίησης 3, το 6,9% με βαθμό ικανοποίησης 2, το 2,6% με βαθμό ικανοποίησης 1 ενώ το 53,1% δεν δίνει απάντηση.



Διάγραμμα 12ζ:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 12 η οποία είναι: για ποιό λόγο δεν έχετε προβεί σε κάποια αγορά/συναλλαγή μέσω internet ; [άλλο] (όπου βαθμός ικανοποίησης 1 ελάχιστο, όπου 5 μέγιστο.)

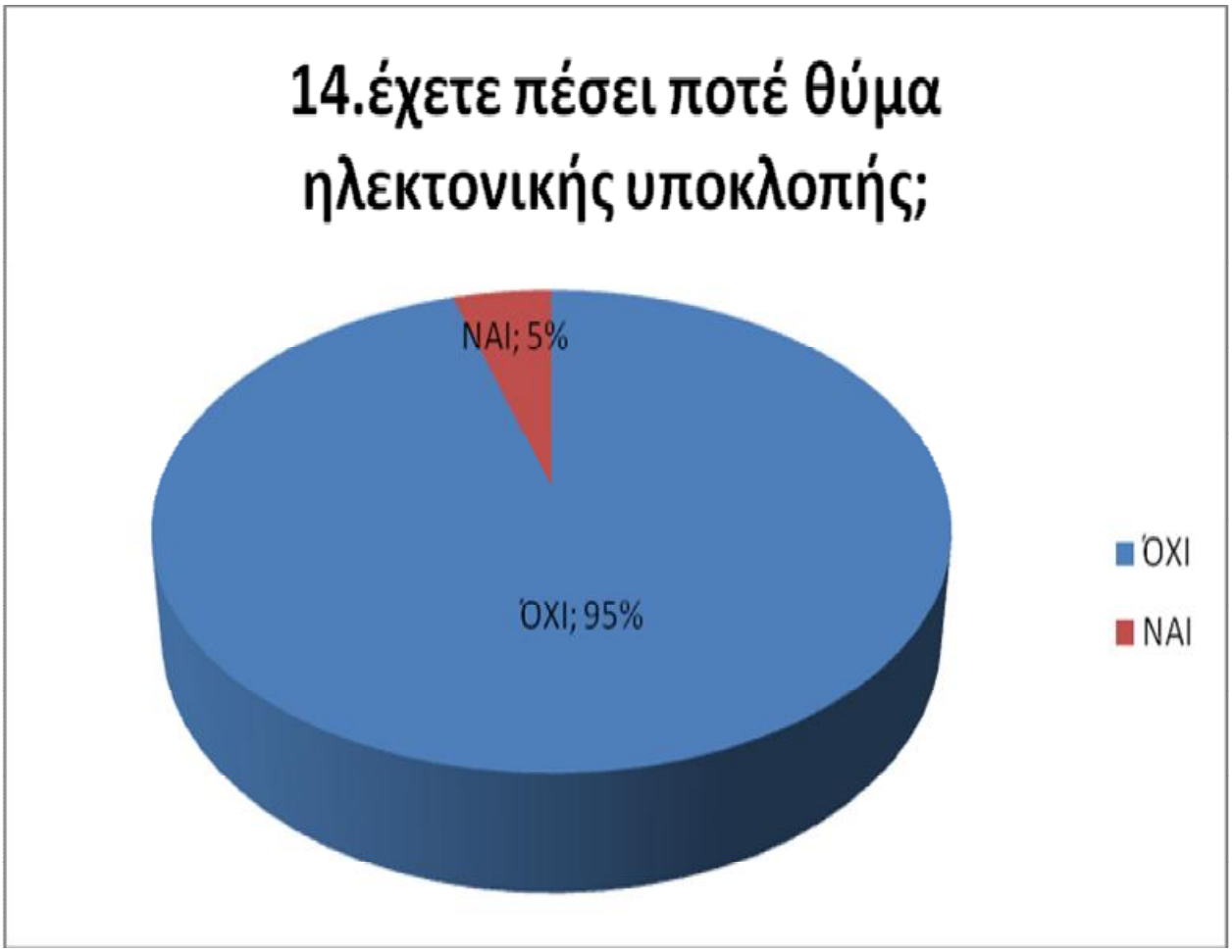
Από τους 188 που απάντησαν το 3,7% φοβάται διάφορους άλλους λόγους με βαθμό ικανοποίησης 5, το 1% με βαθμό ικανοποίησης 4, το 2,6% με βαθμό ικανοποίησης 3, το 2,1% με βαθμό ικανοποίησης 2, το 6,9% με βαθμό ικανοποίησης 1 ενώ το 81,9% δεν δίνει απάντηση.



Διάγραμμα 13:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 13 η οποία είναι: γνωρίζετε ποιά δεδομένα θεωρούνται προσωπικά;

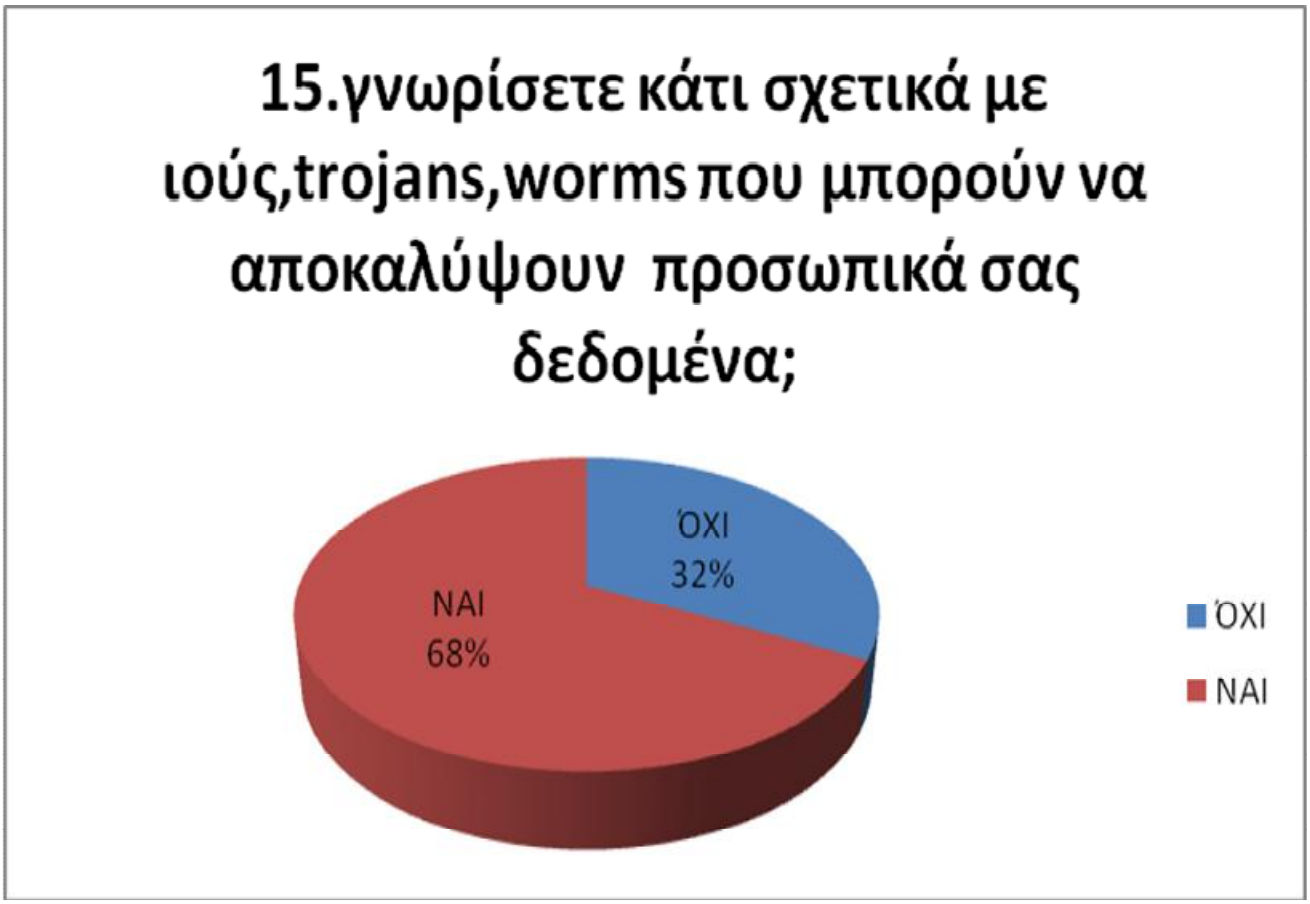
Από τους 188 που απάντησαν το 14,8% δεν γνωρίζει ποια δεδομένα είναι προσωπικά ενώ το 85,1% απάντησε ότι γνωρίζει.



Διάγραμμα 14:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 14 η οποία είναι: έχετε πέσει ποτέ θύμα ηλεκτρονικής υποκλοπής;

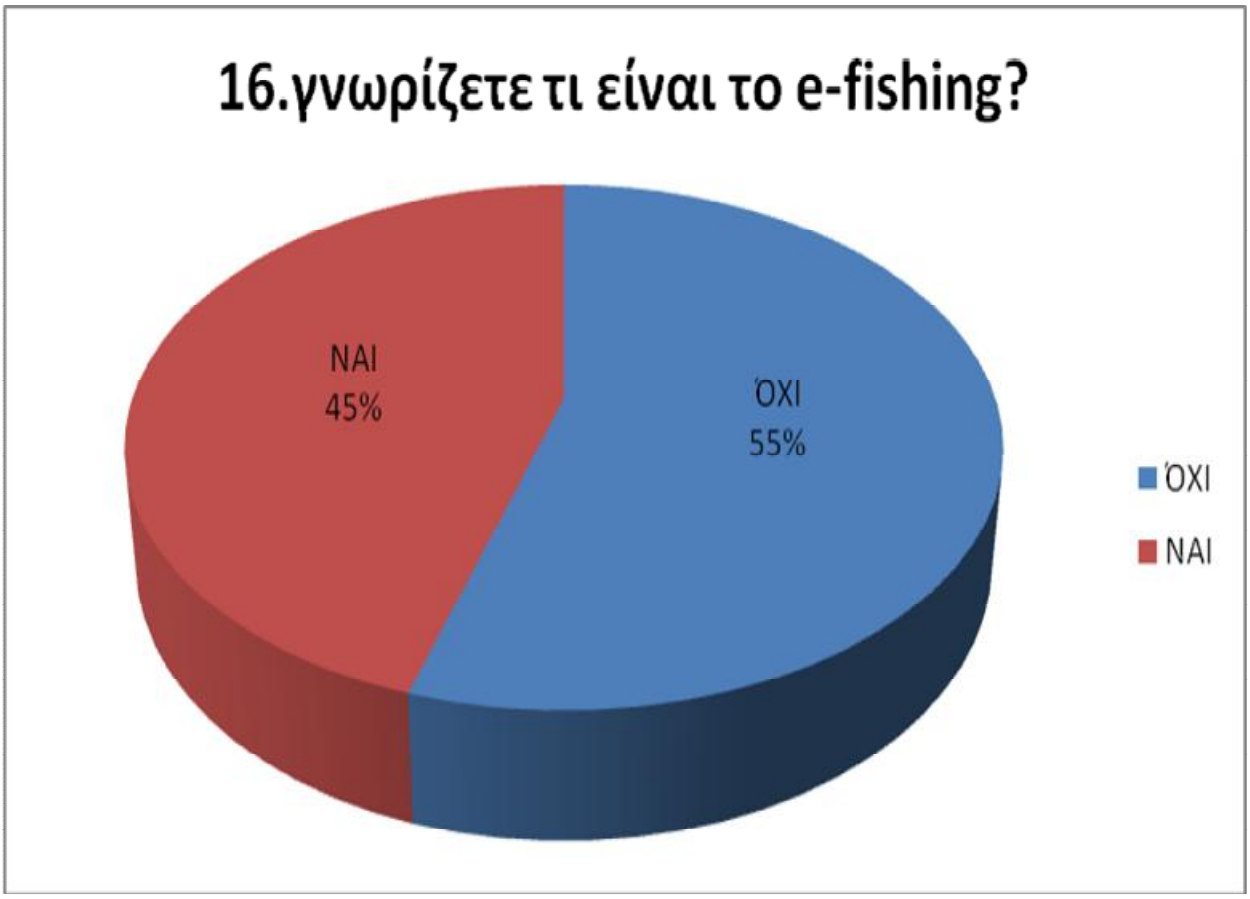
Από τους 188 που απάντησαν το 95,2% δεν έχει πέσει θύμα υποκλοπής ενώ το 4,7% έχει.



Διάγραμμα 15:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 15 η οποία είναι: γνωρίζετε κάτι σχετικά με ιούς, trojans, worms που μπορούν να αποκαλύψουν προσωπικά σας δεδομένα;

Από τους 188 που απάντησαν το 67,5% γνωρίζει σχετικά με ιούς ενώ το 32,5% δεν γνωρίζει.



Διάγραμμα 16:

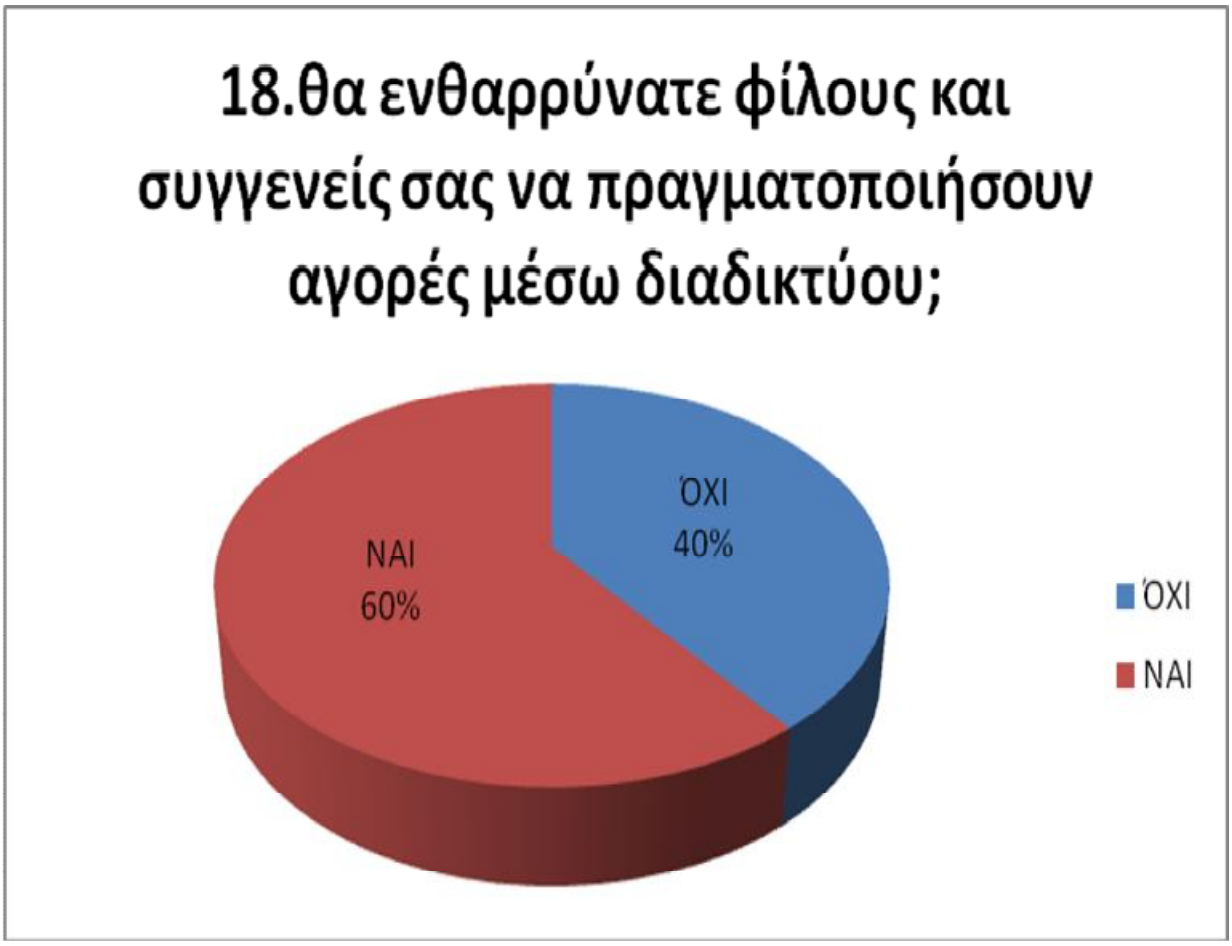
Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 16 η οποία είναι: γνωρίζετε τι είναι το e-fishing ;

Από τους 188 που απάντησαν το 54,7% δεν γνωρίζει τι είναι το e-fishing ενώ το 45,2% γνωρίζει.

Διάγραμμα 17:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 17 η οποία είναι: ποιά από τις παρακάτω ομάδες ατόμων θα συμβουλευόσασταν για αγορές μέσω internet ;

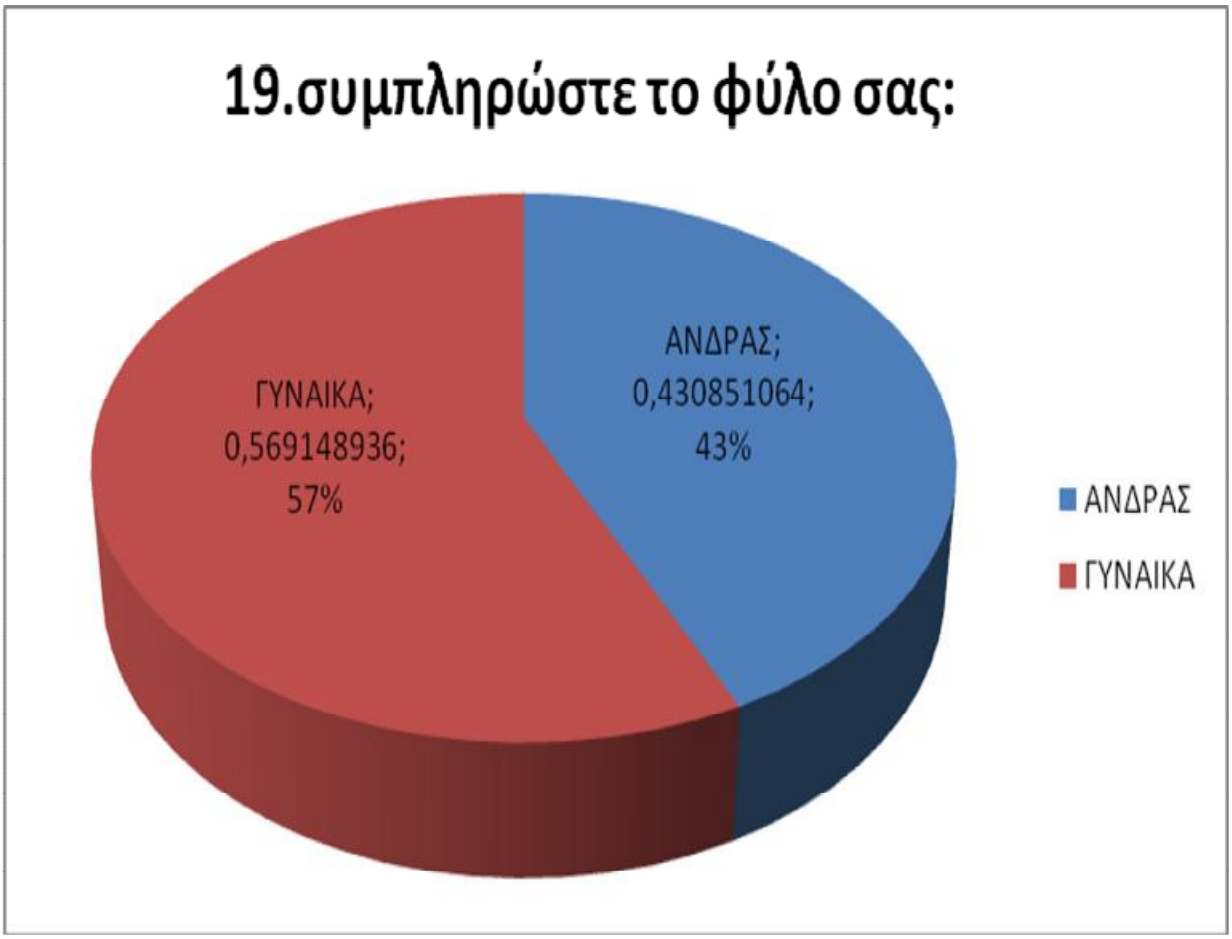
Από τους 188 που απάντησαν το 63% εμπιστεύεται φίλους του, το 29% την οικογένειά του, το 29% ειδικούς , το 20% μέλη φόρουμ, το 19% συναδέλφους του ενώ το 17% αποφασίζει μόνο του.



Διάγραμμα 18:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 18 η οποία είναι: θα ενθαρρύνατε φίλους και συγγενείς σας να πραγματοποιήσουν αγορές μέσω διαδικτύου;

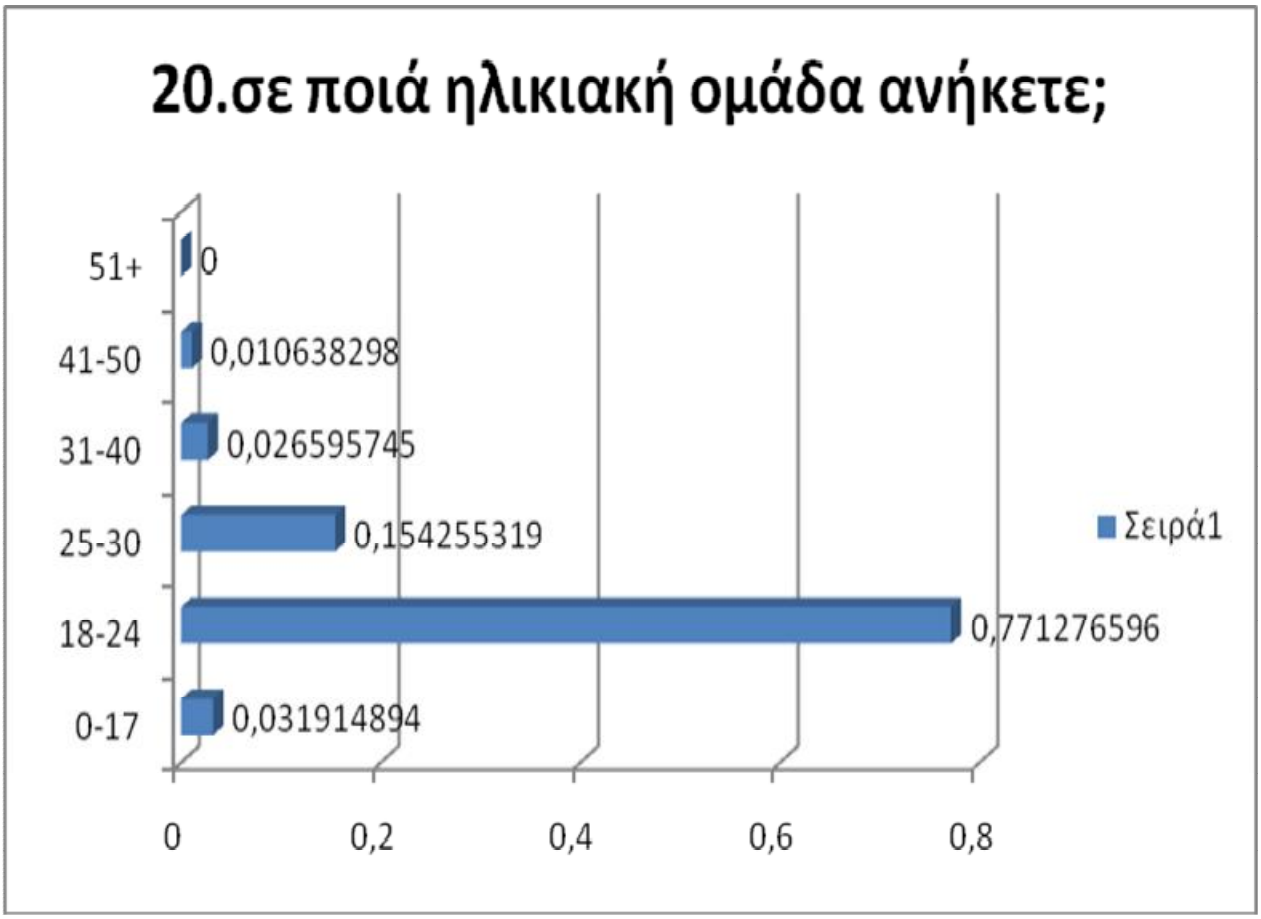
Από τους 188 που απάντησαν το 60% θα ενθάρρυνε τους φίλους του ενώ το 40% όχι.



Διάγραμμα 19:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 19 η οποία είναι: συμπληρώστε το φύλο σας.

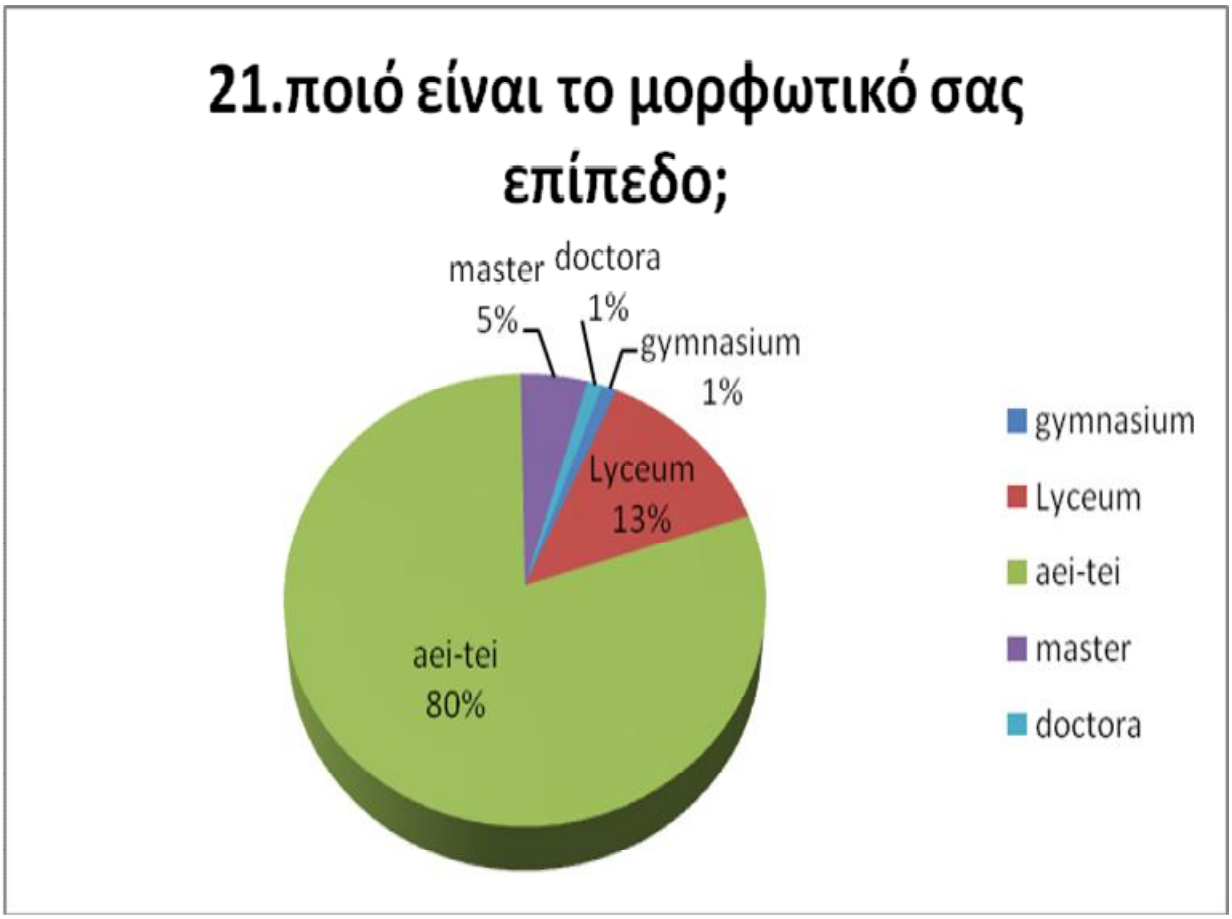
Από τους 188 που απάντησαν το 57% είναι άνδρες ενώ το 43% γυναίκες.



Διάγραμμα 20:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 20 η οποία είναι: σε ποιά ηλικιακή ομάδα ανήκετε;

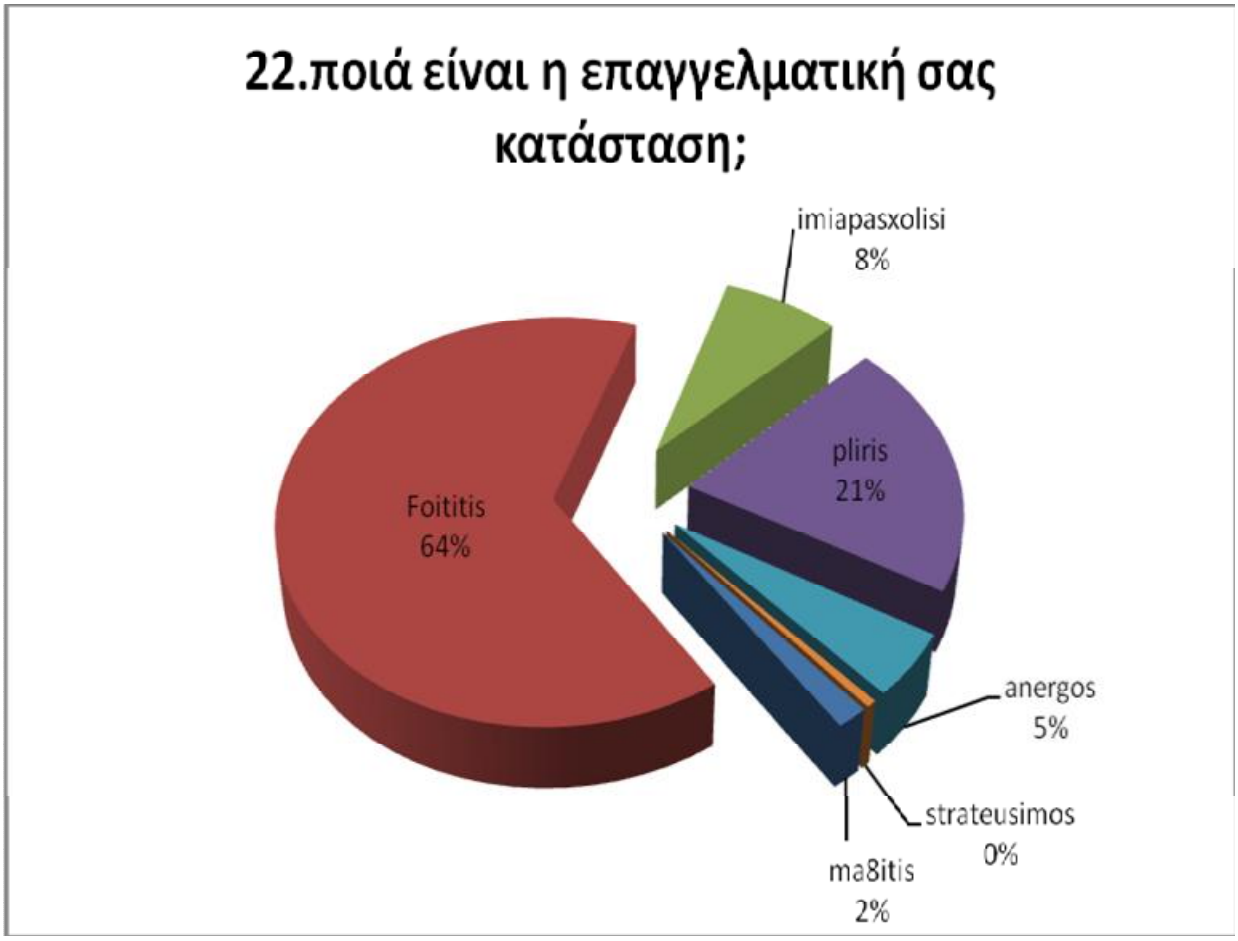
Από τους 188 που απάντησαν το 77% είναι ηλικίας από 18-24 χρονών, το 15,4% είναι 25-30, το 3,2% είναι 0-17, το 2,6% είναι 31-40, το 1% είναι 41-50, και μόλις ένα άτομο είναι 51+.



Διάγραμμα 21:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 21 η οποία είναι: ποιό είναι το μορφωτικό σας επίπεδο;

Από τους 188 που απάντησαν το 79,7% είναι απόφοιτοι ΑΕΙ-ΤΕΙ, το 13,2 έχουν απολυτήριο Λυκείου, το 4,7 είναι κάτοχοι master, το 1% είναι κάτοχοι διδακτορικού ενώ το υπόλοιπο 1% είναι απόφοιτοι Γυμνασίου.



Διάγραμμα 22:

Το διάγραμμα αυτό αντιστοιχεί στην ερώτηση 22 η οποία είναι: ποιά είναι η επαγγελματική σας κατάσταση;

Από τους 188 που απάντησαν το 61,7% είναι φοιτητές, το 19,6 εργάζονται με πλήρη απασχόληση, το 7,4% εργάζονται με ημιαπασχόληση, το 4,7% είναι άνεργοι, το 1,6% είναι μαθητές, 0,5% είναι στρατεύσιμοι.

5. ΣΥΓΚΡΙΣΗ ΕΡΕΥΝΩΝ

Έρευνες εξωτερικού

I. Grazioli St. & Javernpaa S.L (2000)

a. 80 ερωτηματολόγια σε φοιτητές πανεπιστημίου.

b. Στάση απέναντι σε ηλεκτρονικά καταστήματα, εμπιστοσύνη, κίνδυνος, μηχανισμοί ασφαλείας, απάτη.

c. Αγοραστική συμπεριφορά, προθυμία αγοράς μέσω του καταστήματος, στάση απέναντι στο κατάστημα, κίνδυνος, εμπιστοσύνη.

d. Η ασφάλεια & η εγγύηση που παρέχονται από μια ηλεκτρονική συναλλαγή συσχετίζονται σημαντικά με τον αναμενόμενο κίνδυνο, ενώ το μέγεθος & η φήμη συσχετίζονται με την εμπιστοσύνη σε αυτό. Επιπλέον η απάτη δεν έχει άμεση επίδραση στην αγοραστική συμπεριφορά του καταναλωτή ή στην προθυμία να αγοράσει από το συγκεκριμένο κατάστημα. Ωστόσο ο κίνδυνος & η εμπιστοσύνη επηρεάζουν σημαντικά την συμπεριφορά του καταναλωτή απέναντι στο κατάστημα.

e. Η αναμενόμενη εξαπάτηση έχει σημαντική επίδραση στην εμπιστοσύνη και τον αναμενόμενο κίνδυνο και καθορίζει τη σχέση μεταξύ ασφαλείας και κινδύνου, όσο υψηλότερη η αντίληψη της εξαπάτησης τόσο ισχυρότερη είναι η εμπιστοσύνη στους μηχανισμούς καταστολής του κινδύνου.

Συμπέρασμα: Εδώ παρατηρούμε σε μια έρευνα πριν από μια δεκαετία ότι όσο και να αυξηθούν οι ηλεκτρονικές συναλλαγές οι σχέσεις πελάτη-καταστήματος και κινδύνου-εμπιστοσύνης δεν αλλάζουν και βασίζονται πάνω σε σταθερές όπως η φήμη και το μέγεθος του εκάστοτε οργανισμού (καταστήματος, τράπεζας, κτλ).

II. Goldsmith R.E (2001) Η.Π.Α

a. 117 ερωτηματολόγια σε φοιτητές πανεπιστημίου.

b. Χρήση διαδικτύου, έκταση της αγοράς, πιθανότητα πραγματοποίησης μελλοντικής συναλλαγής, φόρτωση μουσικής στον Η/Υ.

c. Πρόθεση για ηλεκτρονική συναλλαγή.

d. Η πρόθεση για ηλεκτρονική συναλλαγή σχετίζεται θετικά με πολλές ώρες χρήσης του διαδικτύου, περισσότερες ηλεκτρονικές συναλλαγές, αυξημένες πιθανότητες για μελλοντική συναλλαγή και χρήση διαδικτύου για αγορά μουσικής.

Συμπέρασμα: Σε αυτή την έρευνα παρατηρούμε άλλον έναν προσδιοριστικό παράγοντα των ηλεκτρονικών συναλλαγών που είναι η εξοικείωση με τους Η/Υ. πράγμα που φαίνεται και στην πρόσφατη έρευνα που πραγματοποιήσαμε. Όσο συχνότερη είναι η χρήση του Η/Υ τόσο πιο θετικά αποτελέσματα εμφανίζονται όσο αφορά την προθυμία πραγματοποίησης μιας ηλεκτρονικής συναλλαγής χωρίς βέβαια αυτό να σημαίνει ότι υπάρχει απαραίτητα ολοκληρωμένη γνώση όσο αφορά το θεωρητικό κομμάτι. Συνεπώς παρατηρείται μια άγνοια κινδύνου.

III. Vijayarathy L.R & Jones J.M (2000) Η.Π.Α

a. 201 ερωτηματολόγια .

b. Αξία προϊόντος, αγοραστική εμπειρία, πληροφορίες προ-παραγγελίας, πληροφορίες επιλογής αποστολής, αξιοπιστία, απτότητα, εμβίωση, ρίσκο καταναλωτή.

c. Στάση απέναντι στην αγορά μέσω ηλεκτρονικού καταλόγου, πρόθεση αγοράς μέσω ηλεκτρονικού καταλόγου.

d. Σύμφωνα με τα αποτελέσματα της έρευνας υπάρχουν ανησυχίες σχετικά με την αξιοπιστία και την φήμη των ηλεκτρονικών καταλόγων με κατώτερους ηλεκτρονικούς καταλόγους όπως αυτοί συγκρίνονται με τους έντυπους, με την έλλειψη ασφάλειας στις ηλεκτρονικές συναλλαγές και μετά τα προσωπικά δεδομένα οι σχεδιαστές ηλεκτρονικών καταλόγων θα πρέπει να λάβουν υπόψη τους το σχεδιασμό και τις πρωταρχικές ανάγκες και επιθυμίες των καταναλωτών-στόχων.

Συμπέρασμα: Εδώ μπορούμε να παρατηρήσουμε το κυριότερο μειονέκτημα που παρατηρείται κυρίως στις ηλεκτρονικές αγορές, οι κατάλογοι των προϊόντων, η βιτρίνα και στη συνέχεια η επαφή με το προϊόν. Χρειάζεται σωστή στάση από πλευράς αισθητικής και λειτουργικότητας καθώς και ανταγωνιστική τιμολόγηση, έτσι ώστε να μπορέσει να εξισορροπηθεί η απουσία επαφής με το προϊόν.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Με βάση τα στοιχεία που παρουσιάζονται στο ερωτηματολόγιο συμπεραίνουμε ότι το μεγαλύτερο ποσοστό εκείνων που απάντησαν, χρησιμοποιούν ηλεκτρονικό υπολογιστή στην καθημερινότητά τους. Επίσης παρατηρούμε ότι η χρήση διαδικτύου είναι πλέον ευρέως διαδεδομένη και ένα μεγάλο ποσοστό έχει πρόσβαση από το σπίτι του μέσω ευρυζωνικής σύνδεσης. Στη συνέχεια παρατηρούμε ότι παρότι σχεδόν το 50% δηλώνουν έμπειροι χρήστες πάνω από το 50% δεν πραγματοποιεί ηλεκτρονικές συναλλαγές . Έτσι προκύπτει ότι οι έλληνες χρήστες του διαδικτύου παραμένουν διστακτικοί όσο αφορά τις ηλεκτρονικές συναλλαγές τους.

Παρόλα αυτά ακόμη και αυτοί που ισχυρίζονται ότι πραγματοποιούν συναλλαγές μέσω διαδικτύου, δεν πραγματοποιούν ηλεκτρονικές αγορές και ακόμα μικρότερο ποσοστό δεν εμπιστεύεται το διαδίκτυο για την εξασφάλιση πληροφοριών. Πράγμα που θα διευκόλυνε σε μεγάλο βαθμό τις καθημερινές συναλλαγές μας.

Βασικός παράγοντας αποτροπής από τις ηλεκτρονικές συναλλαγές είναι ο φόβος για την παραβίαση προσωπικών δεδομένων και πιθανές υποκλοπές. Επιπλέον, στην αποτροπή οδηγεί η νοοτροπία πολλών καταναλωτών που προτιμούν την επαφή με το προϊόν και τον πωλητή, πράγμα που τους οδηγεί στο φυσικό κατάστημα. Οι λόγοι που επικαλούνται ποικίλλουν, μερικοί από αυτούς είναι:

- “Είμαι ευχαριστημένος με το φυσικό κατάστημα, δεν έχω νιώσει την ανάγκη.”

- “Δεν αισθάνομαι άνετα να μην μπορώ να αγγίξω ή να παρατηρήσω το αντικείμενο από κοντά.”

- “Τα προϊόντα μπορεί να αργήσουν κατά την αποστολή ή και να μην φτάσουν ποτέ.”

- “Οι αγορές μέσω διαδικτύου είναι περίπλοκες.”

- “Φοβάμαι ότι το προϊόν που θα παραλάβω δεν θα είναι αυτό που έχω παραγγείλει.” κλπ.

Σε σχετική θεωρητική ερώτηση παρατηρείται ότι μεγάλο ποσοστό έχει γνώση σχετικά με τα προσωπικά δεδομένα, την παραβίασή τους και τους ιούς που απειλούν τα υπολογιστικά συστήματα. Αντιθέτως σχεδόν το 55% των ερωτηθέντων δεν γνωρίζει σχετικά με το e-fishing που αποτελεί βασικό παράγοντα υποκλοπών.

Πλέον η αγορά ενός Η/Υ είναι προσιτή στο ευρύ κοινό καθώς και μια οικιακή σύνδεση στο διαδίκτυο. Επίσης πάρα πολλές εταιρείες δραστηριοποιούνται στο χώρο του ηλεκτρονικού εμπορίου και συμβάλουν στην προσπάθεια ανάπτυξης. Όσο αφορά τις διατραπεζικές συναλλαγές και το θέμα της ασφάλειας έχει παρατηρηθεί μεγάλη πρόοδος από τους τραπεζικούς ομίλους οι οποίοι ενθαρρύνουν τους χρήστες να δοκιμάσουν τις εκάστοτε εφαρμογές τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Γκρίτζαλης Στ.- Κάτσικας Σ.- Γκρίτζαλης Δ. (συλλογικό), *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδ. Νέων Τεχνολογιών, 2004.

[2] Brenton-Hunt, *Ασφάλεια Δικτύων*, Αθήνα 2003. <σελ.331>

[3] Αποστολάκης Ι. - Λουκής Ε. - Χάλαρης Ι., *Ηλεκτρονική Διακυβέρνηση*, κδ. ΙΝ.ΕΠ., Αθήνα 2004. <σελ.11>

[4] W. Stallings, *Cryptography and Network Security*. Old Tappan, NJ:Prentice Hall, 1999.

[5] J. Feghhi, P. Williams and J. Feghhi, *Digital Certificates*. Old Tappan,, NJ:Addison Wesley, 1998

[6] R. Housley, W. Polk, W. Ford, D. Solo, *RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002; http://www.faqs.org/rfcs/rfc3280.html

[7] Mike Schiffman “Network Safety-A Beginner’s Guide”

[8] Γκρίτζαλης Στ.- Κάτσικας Σ.- Γκρίτζαλης Δ. (συλλογικό), *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδ. Νέων Τεχνολογιών, 2004.

[9] Oppliger R.“Authentication Systems for Secure Networks”

[10] William Stallings “Cryptography and Network Security-Principles and Practice”

[11] Bellovin S. and Merritt M. "Limitations of the Kerberos Authentication System"

[12] Γκρίτζαλης Στ.- Κάτσικας Σ.- Γκρίτζαλης Δ. (συλλογικό), *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδ. Νέων Τεχνολογιών, 2004.

[13] Μήτρου, Λίλιαν, «Η αρχή Προστασίας Προσωπικών Δεδομένων», Αθήνα-Κομοτηνή, 1999, Εκδ. Σάκκουλα

[14] www.dpa.gr <*Εφημερίδα Ευρωπαϊκών Κοινοτήτων*>

Χρήσιμα Sites:

http://www.cypher.com.au/crypto_history.htm
http://www.youdzone.com/signature.html
http://en.wikipedia.org/wiki/Digital_signature
http://www.ebusinessforum.gr/index.php?op=modload&modname=Teams&action=teamsviewnewall&pageid=32