ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΤΕΙ ΗΠΕΙΡΟΥ

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Μηχανικών Πληροφορικής ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Μάνου Δήμητρα – ΑΜ:11823

Επιβλέπων καθηγητής: Τσίπουρας Μάρκος

Άρτα, Ιούλιος 2018

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Μηχανικών Πληροφορικής ΤΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Μάνου Δήμητρα - ΑΜ:11823

Επιβλέπων καθηγητής: Τσίπουρας Μάρκος

Άρτα, Ιούλιος 2018

ELECTRONIC CRIME IN SOCIAL MEDIA

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Άρτα, Ιούλιος 2018

ΕΠΙΤΡΟΠΗ ΑΞΟΛΟΓΗΣΗΣ

1. Τσίπουρας Μάρκος
   Καθηγητής

Ο Πρόεδρος του Τμήματος

Στύλιος Χρυσόστομος

Υπογραφή

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα πτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Μάνου Δήμητρα

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις ιδιαίτερες ευχαριστίες μου στον καθηγητή μου κύριο Μάρκο Τσίπουρα που μου εμπιστεύτηκε το παραπάνω θέμα. Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου που είναι πάντα δίπλα μου και με στηρίζει.

ΠΕΡΙΛΗΨΗ

Μεγάλη έξαρση έχει πάρει το ηλεκτρονικό έγκλημα σε πολλές χώρες του κόσμου, τα τελευταία χρόνια. Η εξέλιξη των νέων τεχνολογιών και ειδικά η εξέλιξη στον κόσμο της Πληροφορικής συντέλεσαν στην ανάπτυξή του. Στην παρούσα πτυχιακή πραγματοποιείται μελέτη του φαινομένου και της έκτασης που έχει λάβει αυτό. Πιο συγκεκριμένα αναπτύχθηκε ένα ερωτηματολόγιο που περιλαμβάνει ερωτήσεις που καταγράφουν όσο δημογραφικά στοιχεία όσο και στοιχεία σε σχέση με τις ικανότητες/γνώσεις χρήσης υπολογιστή καθώς και προσωπική εμπειρία σε σχέση με το ηλεκτρονικό έγκλημα. Το ερωτηματολόγιο συμπληρώθηκε από 121 άτομα και η ανάλυση μας οδήγησε σε χρήσιμα συμπεράσματα.

Συγκεκριμένα, στο πρώτο κεφάλαιο γίνεται εισαγωγή στο ηλεκτρονικό έγκλημα και αναλύεται τι είναι ηλεκτρονικό έγκλημα και άλλες βασικές έννοιες του. Στο δεύτερο κεφάλαιο, αναφέρεται θεωρητικά η έρευνα με ερωτηματολόγια καθώς και πώς δημιουργούμε ένα ερωτηματολόγιο. Στο τρίτο κεφάλαιο, εστιάζεται τι πραγματεύεται η εργασία και πως δημιουργήθηκε το ερωτηματολόγιο. Στο τέταρτο κεφάλαιο, γίνεται μια σύντομη περιγραφή της περιγραφικής στατιστικής. Έπειτα, στο πέμπτο κεφάλαιο πραγματοποιείται η ανάλυση των δεδομένων του δείγματος που έχουμε συλλέξει με τη χρήση του προγράμματος SPSS που είναι και ο σκοπός της παρούσας πτυχιακής εργασίας. Τέλος, παρουσιάζονται τα συμπεράσματα της έρευνας έπειτα από την ανάλυση που έχει γίνει, βάση των απαντήσεων που έχουμε πάρει.

Λέξεις κλειδιά: ηλεκτρονικό έγκλημα, SPSS, τεχνολογίες.

ABSTRACT

Electronic crime has taken great expansion in many countries of the world in recent years. The evolution of new technologies and especially the development in the world of Information Technology have contributed to its development. This study examines the phenomenon and the extent to which it has been taken. In particular, a questionnaire was developed that includes questions that record journalistic data as well as information on computer skills/ knowledge and the experience of cybercrime. The questionnaire was completed by 121 people and its analysis led to useful conclusions.

Specifically, the first chapter introduces electronic crime and distinguishes the definition of electronic crime and other key concepts. In the second chapter, the questionnaire survey is theoretically mentioned and how we create a questionnaire. In the third chapter, it focuses on what the work is about and how the questionnaire was created. In the fourth chapter, a brief description of the descriptive statistics is collected using the SPSS program, which is the purpose of this dissertation, is carried out. Finally, the conclusions of the research are presented after the analysis which has been done based on the answers we have received.

Key-words: Electronic crime, SPSS, technologies.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Ο κόσμος των νέων τεχνολογιών και ιδιαίτερα ο κόσμος της πληροφορικής και των ηλεκτρονικών υπολογιστών έχουν εισβάλλει στην ζωή των ανθρώπων και έχουν εξαπλωθεί σε πολλούς τομείς των δραστηριοτήτων τους, από την εκπαίδευση, την επικοινωνία μέχρι και το εμπόριο. Για όλες τις δραστηριότητες που συμβάλλουν στην επικοινωνία και στις συναλλαγές είναι αναγκαία η χρήση του Διαδικτύου. Αυτό φυσικά, είναι καλό διότι διευκολύνει την ζωή πολλών ανθρώπων και μπορούν οποιαδήποτε στιγμή και σε οποιοδήποτε σημείο και αν βρίσκονται να πραγματοποιούν συναλλαγές και να επικοινωνούν με άλλους ανθρώπους που βρίσκονται σε άλλες πόλεις η ακόμη και σε άλλες Ηπείρους.

Από την άλλη πλευρά όμως αυτό συνεπάγεται και με την αύξηση των κινδύνων που μπορεί να κρύβονται μέσα σε έναν υπολογιστή και αντίστοιχα στο διαδίκτυο. Η τεχνολογία εξελίσσεστε έτσι εξελίσσονται και οι γνώσεις των ανθρώπων που διαπράττουν το ηλεκτρονικό έγκλημα. Όπως ένας ηλεκτρονικός εγκληματίας ανακαλύπτει συνεχώς καινούργιους τρόπους να διαπράξει το έγκλημα του σε οποιαδήποτε μορφή κι αν είναι, έτσι και οι αρχές πρέπει να συμβαδίζουν με την τεχνολογία και τα νέα μέσα προκειμένου να προστατεύουν τους πολίτες.

1. Ηλεκτρονικό Έγκλημα

1.1 Ορισμός Ηλεκτρονικού Εγκλήματος

Οι προσπάθειες που έγιναν για να ορισθεί το ηλεκτρονικό έγκλημα ήταν πολλές. Έναν από τους ορισμούς έδωσαν οι Forest και Morrison το 1994 προσδιορίζοντας έτσι το ηλεκτρονικό έγκλημα ως μια εγκληματική πράξη στην οποία το βασικό μέσο για να πραγματοποιηθεί είναι ο ηλεκτρονικός υπολογιστής.[9]

Αναλόγως με τον τρόπο που διαπράττονται χωρίζονται σε δύο κατηγορίες:

Εγκλήματα που γίνονται με τη χρήση Ηλεκτρονικού Υπολογιστή (computer crime):

Αυτά τα εγκλήματα αποτελούνται τις παράνομες δραστηριότητες όπως παράνομη ή μη εξουσιοδοτημένη χρήση προγραμμάτων συνήθως χωρίς τη χρήση του διαδικτύου.

Κυβερνοεγκλήματα (cyber crime):

Πρωταρχικός παράγοντας στα εγκλήματα του κυβερνοχώρου είναι η χρήση του Διαδικτύου. Οι εγκληματίες πραγματοποιούν την τέλεση του εγκλήματος με την βοήθεια του Διαδικτύου και όλων των δυνατοτήτων που τους παρέχει. Η εξέλιξη τεχνολογίας των ηλεκτρονικών υπολογιστών μεγάλωσε το φάσμα των εγκληματικών ενεργειών, οι οποίες απαιτούν μεγάλη εξειδίκευση για την αντιμετώπισή τους.

1.2 Ιστορική αναδρομή του εγκλήματος

Το έγκλημα δεν αρχίζει από την σημερινή εποχή. Είναι κομμάτι της παλαιάς και έχει εξαπλωθεί ραγδαία στην κοινωνία που ζούμε. Δεν έχει σημασία ο χρόνος η το μέρος που βρίσκονται οι άνθρωποι, σημασία έχει πως που κάνουν παραβάσεις στους κανόνες τις κοινωνίας και το αποτέλεσμα αυτού είναι οι ποινές που τους καταλογίζονται.

Στην αρχή της δεκαετίας του ’80 με τον ερχομό του πρωτοκόλλου X.25, οι υπολογιστές της εποχής εκείνης, επικοινωνούσαν μεταξύ τους με τη χρήση του modem και ενός τηλεπικοινωνιακού δικτύου. Σύντομο ήταν το χρονικό διάστημα που έκαναν την εμφάνισή τους οι hackers,οι οποίοι χρησιμοποιώντας τα modem αποκτούσαν πρόσβαση σε άλλους υπολογιστές πέραν τον δικών τους και ανεξάρτητα της απόστασης στην οποία βρισκόταν.

Τα μέτρα ασφαλείας παρουσίαζαν μεγάλη έλλειψη και έτσι το 1983 εμφανίζονται τα πρώτα φαινόμενα hacking που είχαν σαν κύριο σκοπό την παράνομη αντιγραφή

πληροφοριών όπως επίσης και τις ζημιές σε υπολογιστικά συστήματα πανεπιστημίων και πολλών άλλων οργανισμών. Το 1984 ιδρύεται τμήμα δίωξης ηλεκτρονικού εγκλήματος στην New Scotland Yard. Αργότερα, περίπου το 1989 γίνεται η πρώτη προσπάθεια για τη νομική αντιμετώπιση του ηλεκτρονικού εγκλήματος Πανευρωπαϊκά. Τότε υπήρχαν λίγες χώρες που είχαν θεσπίσει τους νόμους οι οποίοι κάλυπταν ένα μικρό μέρος του ηλεκτρονικού εγκλήματος. Μέσα σε αυτές ήταν και η Ελλάδα. Έπειτα από ένα χρόνο ιδρύθηκε το πρώτο κέντρο συντονισμού για την ασφάλεια των υπολογιστικών συστημάτων. Το κέντρο αυτό σήμερα είναι γνωστό ως CERT/CC (Computer Emergency Response Team / Coordination Center). Στην εξάπλωση του Διαδικτύου συμβάλλει και η υπηρεσία www (world wide web), που φιλοξενεί αρχεία, εικόνες και ήχο. Αυτό συνοδεύεται με την άνθιση του πορνογραφικού υλικού, παράνομων σελίδων, πειρατικού λογισμικού και άλλων εγκλημάτων. Μετά τα μέσα της δεκαετίας του ’90 εμφανίζεται στον κόσμο της πληροφορικής ο πρώτος ιός macro – virus, ο οποίος προσβάλει μη εκτελέσιμα αρχεία, γνωστός με το όνομα Melissa.[14]

1.2.1 Μετάβαση στο Ηλεκτρονικό Έγκλημα

Ως γνωστών το έγκλημα είναι κομμάτι της κοινωνίας. Οι μορφές του εξελίσσονται, συνεπώς αυξάνονται και τα μέσα που μπορεί να διαπραχθεί. Στις αρχές του 20^{ου} αιώνα εμφανίστηκαν καινούργιοι τρόποι για την διάπραξη των εγκλημάτων. Το τηλέφωνο άρχισε να χρησιμοποιείται για απάτες και τα μεταφορικά μέσα έκαναν ακόμη πιο εύκολη την διάπραξη της κλοπής και άλλων εγκλημάτων.

Με την ανάπτυξη της τεχνολογίας αναπτύχθηκαν και τα εγκλήματα. Βέβαια υπάρχουν και τα παραδοσιακά εγκλήματα αλλά κυρίαρχο μέρος έχουν πάρει αυτά που οι ηλεκτρονικές συσκευές συντελούν στην ανάπτυξή τους.

Ο σκοτεινός κόσμος του ηλεκτρονικού εγκλήματος πήρε μεγάλη έκταση έπειτα από την εμφάνιση των δικτύων. Τα δίκτυα, άνοιξαν έναν νέο ορίζοντα στον χώρο της πληροφορίας και οι υπολογιστές μπορούν και απομνημονεύουν χρήσιμες πληροφορίες. Αυτό από μόνο του κάνει πιο εύκολη την δραστηριότητα αυτή παρά ποτέ.[1]

1.2.2 Χαρακτηριστικά Ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό έγκλημα ξεχωρίζει από αυτό που γνωρίζαμε ως τώρα. Σαφώς, έχει κάποια ιδιαίτερα χαρακτηριστικά.

- Για να εκτελεστεί χρειάζονται άριστες γνώσεις ηλεκτρονικών μέσων.
- Στον Κυβερνοχώρο το έγκλημα διαπράττεται γρήγορα σε πραγματικό χρόνο. Κάποιες φορές δεν το αντιλαμβάνεται ούτε το θύμα.
- Τα ίχνη που αφήνει είναι ψηφιακά
- Γίνεται σε οποιοδήποτε μέρος και δεν υπάρχει η ανάγκη της μετακίνησης του δράστη. Τα αποτελέσματα μπορεί να είναι παράλληλα και όχι οπωσδήποτε στο ίδιο μέρος.
- Οι εγκληματίες παρουσιάζονται με ψευδή στοιχεία και όχι με την πραγματική τους ταυτότητα.
- Ο αριθμός των θυμάτων του ηλεκτρονικού εγκλήματος είναι πολύ μεγαλύτερος σε σχέση με το παραδοσιακό έγκλημα.
- Η ανακάλυψη του δράστη γίνεται πιο δύσκολη, αλλά όχι ακατόρθωτη.[15]

1.3 Μορφές απειλών

Οι απειλές απέναντι στην ασφάλεια των πληροφοριακών συστημάτων είναι περισσότερες από ποτέ. Όταν ακούμε την λέξη απειλή (threat) σε ένα υπολογιστικό σύστημα σημαίνει ότι μια κατάσταση μπορεί να προκαλέσει ζημιές ή απώλειες.

Μπορούμε να διακρίνουμε τρείς κατηγορίες που μπορούν να περιγράψουν τις μορφές απειλών: τις εξωτερικές, τις εσωτερικές και την Κοινωνική Μηχανική (Social Engineering).[1]

1.3.1 Εξωτερικές απειλές

Οι εξωτερικές απειλές (outside threats) είναι η πιο γνωστή μορφή της επίθεσης. Προέρχεται από τους hackers και τους crackers που δεν ανήκουν στο εσωτερικό του συστήματος. Συνήθης μορφές είναι η μη εξουσιοδοτημένη πρόσβαση δικτύου και η διασπορά κακόβουλου λογισμικού.

- ✓ Hackers

  Στον εξελιγμένο κόσμο των ηλεκτρονικών υπολογιστών ο όρος hacker προέρχεται από τους phreakers, που ίσως είναι από τους πρώτους ηλεκτρονικούς εγκληματίες. Έκαναν την εμφάνισή τους στην ανάπτυξη των τηλεφώνων, δηλαδή πολύ πριν εμφανιστούν οι ηλεκτρονικοί υπολογιστές και κατάφεραν να πραγματοποιούν υπεραστικές κλήσεις χωρίς χρέωση.

  Οι hackers διακρίνονται σε τρείς κατηγορίες.

  - White Hat-Hackers: οι White Hat-Hackers είναι για την καταπολέμηση του ηλεκτρονικού εγκλήματος και των Black Hat-Hackers.
  - Black Hat-Hackers: οι Black Hat-Hackers είναι αυτοί που χρησιμοποιούν τις γνώσεις τους για την εμπλοκή τους στο ηλεκτρονικό έγκλημα. Με την χρήση κώδικα κατασκευάζουν προγράμματα παρακολούθησης και ιούς και εισχωρούν σε δίκτυα και ιστοσελίδες. Το κίνητρό είναι χρηματικό.
  - Grey Hat-Hackers: οι Grey Hat-Hackers είναι αυτοί που παραβιάζουν τον νόμο χωρίς όμως να έχουν κακό σκοπό. Είναι άτομα σε νεαροί ηλικία που δουλεύουν μόνοι τους για την καταπολέμηση των Black Hat-Hackers και των ενεργειών τους.[1]

1.3.2 Εσωτερικές απειλές

Οι εσωτερικές απειλές (inside threats) έχουν να κάνουν με το εσωτερικό του οργανισμού και πιο συγκεκριμένα σχετίζονται με υπαλλήλους που γνωρίζουν τις πολιτικές ασφαλείας του κάθε οργανισμού ή της επιχείρησης.

- ✓ Χρήστες συστημάτων

  Μεγάλος κίνδυνος για την ασφάλεια των συστημάτων είναι ο ίδιος ο χρήστης του συστήματος. Αν γίνει κάποιο λάθος από την χρήση πιθανών να προκληθούν προβλήματα. Τα προβλήματα μπορεί να διακριθούν σε άμεσα ή έμμεσα.

  Άμεσα όταν ο χρήστης ίσως ανοίξει ένα συνημμένο αρχείο από άγνωστο αποστολέα, το οποίο μπορεί να περιέχει κακόβουλο λογισμικό και έμμεσα όταν

διαρρέουν οι κωδικοί πρόσβασης σε άτομα που δεν έχουν το δικαίωμα πρόσβασης σε αυτούς.[1]

1.3.3 Κοινωνική Μηχανική

Η Κοινωνική Μηχανική (Social Engineering) είναι η πιο σοβαρή μορφή επίθεσης. Βασίζεται στην πειθώ και την επιρροή του θύματος , εξασφαλίζοντας την κλοπή προσωπικών πληροφοριών.[1] Οι επιθέσεις Κοινωνικής Μηχανικής μπορεί να προέρχονται είτε από εξωτερικό είτε από εσωτερικό περιβάλλον.

1.4 Μορφές επιθέσεων

1.4.1 Επιθέσεις συμπάθειας (Sympathy Attacks)

Στις επιθέσεις συμπάθειας (Sympathy Attacks) αυτός που επιτίθεται παρουσιάζεται σαν συνάδελφος ή σαν ανώτερο στέλεχος. Ζητά πρόσβαση σε σημαντικές πληροφορίες δίνοντας στον υπάλληλο την αίσθηση πως αν δεν τις αποκαλύψει , θα χάσει την δουλεία του.

1.4.2 Εξατομικευμένες επιθέσεις (Ego Attacks)

Σε αυτήν την περίπτωση ο επιτιθέμενος στηρίζεται στην ματαιοδοξία του θύματος. Συνήθως αναζητά άτομα που προσπαθούν να αποδείξουν στους ανώτερους ότι αξίζουν περισσότερα. Με αυτόν τον τρόπο εμφανίζεται μπροστά τους ως κάποιος ανώτερος, κάνοντάς τον να του δώσει σημαντικές πληροφορίες.

1.4.3 Επιθέσεις εκφοβισμού (Intimidation Attacks)

Όπως αναφέρεται η λέξη, εδώ έχουμε τον εκφοβισμό του θύματος. Ο επιτιθέμενος προσποιείται κάποιο ανώτερο από αυτό που είναι και αν το θύμα αρνηθεί την συνεργασία μαζί του τότε ξεκινούν οι απειλές με πρόφαση πως θα χάσει την δουλειά του ή ότι θα υπάρξουν νομικές διαδικασίες γι αυτό.[1]

1.5 Μορφές Ηλεκτρονικού Εγκλήματος

Για να αναλύσουμε τις βασικότερες μορφές ηλεκτρονικού εγκλήματος τις διακρίνουμε σε δύο κατηγορίες:

i. Τα γνήσια εγκλήματα, δηλαδή τα εγκλήματα που υπήρχαν πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του Διαδικτύου
ii. Τα ηλεκτρονικά εγκλήματα, που δημιουργήθηκαν με την εμφάνιση των ηλεκτρονικών μέσων ,αλλά κάποια από αυτά υπήρχαν και το Διαδίκτυο συντέλεσε στην αύξησή τους.

1.5.1 Επιθέσεις Άρνησης Εξυπηρέτησης

Οι επιθέσεις αυτές αποσκοπούν στην μη εξυπηρέτηση άλλων υπολογιστών, και στοχεύουν κυρίως:

- Στην αδυναμία της σύνδεσης δύο η περισσότερων σημείων, που σημαίνει αδυναμία πρόσβασης σε συγκεκριμένες υπηρεσίες.
- Στην παρεμπόδιση της μετάδοσης δεδομένων δικτύου
- Στην αλλοίωση ποιότητας υπηρεσίας, που παρέχεται σε έναν χρήστη.

1.5.2 Κακόβουλο λογισμικό

Ο κακόβουλος κώδικας (malicious code) είναι ένα από τα διαδεδομένα εγκλήματα στο Διαδίκτυο. Είναι κώδικας που δημιουργείται από τους κακόβουλους χρήστες προκειμένου να προκαλέσει ζημιές σε ηλεκτρονικούς υπολογιστές , να υποκλέψει δεδομένα ή ακόμη και να τα διαγράψει.

Ο κακόβουλος κώδικας διακρίνεται σε τρείς βασικές κατηγορίες.

- Ιούς (viruses): είναι κακόβουλα προγράμματα στους υπολογιστές τα οποία εξαπλώνονται μολύνοντας τον υπολογιστή χωρίς την άδεια του χρήστη. Μπορεί να διαδοθεί και σε άλλους υπολογιστές μέσω του διαδικτύου. Η μεταφορά του είναι εφικτή να γίνει με οποιοδήποτε αποθηκευτικό μέσο όπως με μία δισκέτα ένα usb, cd ή dvd.[12]

- Σκουλήκια (worms): τα σκουλήκια μοιάζουν με τους ιούς. Η διαφορά τους είναι ότι αυτά πολλαπλασιάζονται χωρίς να κάνει κάτι ο χρήστης. Στην πρώτη τους μορφή διαγράφουν αρχεία και έπειτα δημιουργούν αντίγραφά τους και τα στέλνουν στους ηλεκτρονικούς υπολογιστές των θυμάτων.

  Το πιο διάσημο σκουλήκι είναι το ILOVEYOU το οποίο έφτανε στον υπολογιστή των θυμάτων με τη μορφή ενός e-mail και θέμα I LOVE YOU και ένα συνημμένο αρχείο LOVE-LETTER-FOR-YOU.txt.vps. Όταν ο χρήστης το άνοιγε διέγραφε αρχεία και πολλαπλασιάζονταν χρησιμοποιώντας τη μέθοδο Melissa την οποία θα αναλύσουμε στην συνέχεια.[3]

- Δούρειοι Ίπποι (Trojan horses): οι Δούρειοι Ίπποι είναι προγράμματα που οι λειτουργίες τους δεν είναι εύκολο να εντοπιστούν από το χρήστη. Με τη χρήση του Δούρειου Ίππου αυτός που επιτίθεται πετυχαίνει την απόκτηση απομακρυσμένου ελέγχου στον υπολογιστή του θύματος και συλλέγει τους κωδικούς πρόσβασης καθώς και αριθμούς πιστωτικών καρτών.

  Οι Δούρειοι Ίπποι δεν λειτουργούν σαν τους άλλους ιούς , δεν περιμένουν δηλαδή να συμβεί κάτι για να κάνουν την επίθεσή τους. Κάνουν τη ζημιά αμέσως μόλις ο χρήστης τρέξει το πρόγραμμα στο οποίο περιέχονται. Πλέον οι χρήστες είναι ενημερωμένοι έτσι ώστε να μην εμπιστεύονται μη εμπορικά λογισμικά. Αντίθετα, κάποιες φορές καταφέρνουν και κρύβονται τόσο καλά ξεγελώντας έτσι μέχρι και τους πιο έμπειρους χρήστες, εισβάλλοντας στο λογισμικό χωρίς τα δικαιώματα πρόσβασης των χρηστών.[2][3]

1.5.3 Ανεπιθύμητη Αλληλογραφία (spamming)

Η χρήση οποιουδήποτε ηλεκτρονικού μέσου για την αποστολή ανεπιθύμητων μηνυμάτων ονομάζεται spamming. Ένα spam μήνυμα μπορεί να σταλεί με e-mail και κύριος σκοπός του είναι η προώθηση μιας εταιρίας.

Μέσα από το διαδίκτυο πολλές είναι οι επιχειρήσεις που χρησιμοποιούν τέτοιες μεθόδους για την καλύτερη διαφήμιση και προώθηση των προϊόντων τους. Έτσι λοιπόν οι

spammers παίρνουν τις διευθύνσεις από τις εταιρίες ή χρησιμοποιούν λογισμικό που έχει την δυνατότητα να σαρώνει όλο το διαδίκτυο και να συλλέγει όλες τις διευθύνσεις.

Βέβαια, ας τονίσουμε ότι ένα spam δεν είναι ιός, αλλά μειώνει σημαντικά την λειτουργικότητα του Internet. Επίσης, καθημερινά μάχονται για επιβίωση και το ποσοστό των μηνυμάτων που μπορούν να στείλουν είναι πολύ μεγάλο. Από αυτά τα μηνύματα που στέλνουν συνεχώς, ελπίζουν να πάρουν απαντήσεις έστω κι από ένα ελάχιστο ποσοστό. Ο λόγος που ωθεί τους παραλήπτες των μηνυμάτων αυτών να απαντήσουν είναι είτε γιατί είναι άνθρωποι μπερδεμένοι είτε αδύναμοι και ευκολόπιστοι.[3]

1.5.4 Phishing και Pharming

Οι επιθέσεις τύπου phishing είναι μία απάτη η οποία χρησιμοποιείται πολύ από τους hackers που παγιδεύει τους ανθρώπους για να παραχωρούν προσωπικά δεδομένα. Ο πιο γνωστός τρόπος είναι μέσω του Ηλεκτρονικού Ταχυδρομείου. Τα θύματα λαμβάνουν μήνυμα ότι είναι μια υποτιθέμενη τράπεζα ή και ένα κοινωνικό δίκτυο (socials). Η σελίδα στην αρχή φαίνεται νόμιμη αλλά αν ο χρήστης πατήσει πάνω σε αυτή και την ανοίξει, τότε ήδη έχει πέσει θύμα απάτης.[15]

Μία παραλλαγή των επιθέσεων phishing είναι οι επιθέσεις pharming και ο σκοπός είναι ο ίδιος, η απόσπαση προσωπικών δεδομένων. Η μόνη τους διαφορά βρίσκεται στην τεχνική.[1]

1.5.5 Πειρατεία λογισμικού

Ο όρος πειρατεία λογισμικού αναφέρεται στην κλοπή προγραμμάτων λογισμικού με παράνομη αντιγραφή και παράνομη διανομή πλαστών αντιγραμμένων προϊόντων. Πολλοί χρήστες αποκτούν λογισμικό με κάποιο παράνομο τρόπο[16] Το λογισμικό μπορεί να διακινηθεί μέσω του Διαδικτύου και πιο συγκεκριμένα με e-mails και chat[1]

1.6 Διαδικτυακή απάτη

Η απάτη είναι ένα από τα πιο συνηθισμένα εγκλήματα σε όλο τον κόσμο. Με την ανάπτυξη όμως του Διαδικτύου αυξήθηκε ραγδαία το ποσοστό με το οποίο διαπράττεται.

Ολοένα και περισσότεροι άνθρωποι καθημερινά αρχίζουν και χρησιμοποιούν το Διαδίκτυο, χωρίς να είναι ενημερωμένη για την ασφάλεια του Διαδικτύου.

Η διαδικτυακή απάτη μπορεί να πάρει ποικίλες μορφές, και να θεωρηθεί η αποθήκευση δεδομένων που σχετίζονται με πρόσωπα επιχειρήσεις και οργανισμούς, η διάδοση πληροφορίας, η παράνομη διακίνηση και εμπορία ανθρώπων, η παιδική πορνογραφία, και η εξαπάτηση μέσω των σελίδων κοινωνικής δικτύωσης (social media).[1]

1.6.1 Απάτη με πιστωτικές κάρτες

Με την ανάπτυξη της τεχνολογίας αναπτύχθηκαν και τα συστήματα που σχετίζονται με αυτή. Τα τελευταία χρόνια είναι διαδεδομένη η χρήση των πιστωτικών καρτών για αγορές με κύριο μέσο πραγματοποίησης τους το Διαδίκτυο. Όλο αυτό έχει ανοίξει ένα καινούργιο δρόμο στα εγκλήματα. Είναι πολύ εύκολο κάποιος να εξαπατηθεί για τον κύριο λόγο πως δεν υπάρχει ουσιαστική επαφή μεταξύ του πωλητή και του πελάτη.

Χαρακτηριστικό παράδειγμα ο πελάτης που βρίσκει ένα ηλεκτρονικό μαγαζί στο Διαδίκτυο δίνει την παραγγελία του αφού έχει καταβάλλει πρώτα τα χρήματα για την αξία του προϊόντος και φυσικά το προϊόν δεν φτάνει ποτέ στα χέρια του.

Η απάτη με τις πιστωτικές δεν σταματά μόνο στις ηλεκτρονικές συναλλαγές. Μία άλλη μορφή απάτης με πιστωτικές είναι μέσω τηλεφώνου. Επιτήδειοι τηλεφωνούν σε κατόχους πιστωτικών καρτών υποστηρίζοντας πως είναι υπάλληλοι εταιριών πείθοντας τους να τους κάνουν γνωστούς τους κωδικούς των καρτών να την αποκατάσταση υποτιθέμενων βλαβών.[1]

1.6.2 Απάτη με e-mail

Γνωστή είναι και η απάτη με το ηλεκτρονικό ταχυδρομείο. Είναι πολύ συχνό φαινόμενο στο οποίο οι hackers ανακαλύπτουν συνεχώς καινούργιους τρόπους για να εξαπατήσουν τους χρήστες, χρησιμοποιώντας τα μηνύματα ηλεκτρονικού ταχυδρομείου. Κύριο μέλημα τους είναι η απόσπαση μικρών αλλά και μεγαλύτερων χρηματικών ποσών. Η τεχνική που χρησιμοποιούνε μοιάζει με το phishing. Ο τρόπος που προσπαθούν να προσεγγίσουν τα θύματα είναι διαφορετικός σε κάθε περίπτωση. Παράδειγμα ενός τέτοιου μηνύματος είναι η καταβολή ενός συγκεκριμένου ποσού σε κάποιο λογαριασμό και ο υποτιθέμενος διπλασιασμός που ποτέ δεν γίνεται.[1]

1.6.3 Διακίνηση πορνογραφικού υλικού

Σαν πορνογραφικό υλικό ορίζεται η αναπαράσταση κάθε πραγματικής και μη πραγματικής σεξουαλικής πράξης που προκαλεί διέγερση. Πιο συγκεκριμένα, το πορνογραφικό υλικό διακρίνεται σε σκληρό και ελαφριάς μορφής. Στην πρώτη περίπτωση, το θύμα εμφανίζεται να παίρνει μέρος σε πραγματικές ή εικονικές σεξουαλικές πράξεις μόνος του ή με άλλα άτομα και απεικονίζοντας χυδαία μέρη του σώματός του.

Η δεύτερη περίπτωση είναι πιο ελαφριά καθώς, απεικονίζεται σε απλές εικόνες ερωτικής φύσεως με ή χωρίς ρούχα. Και στις δύο περιπτώσεις η διακίνηση γίνεται παράνομα με τη βοήθεια του Διαδικτύου και την μορφή βίντεο ή εικόνας.[20]

1.6.4 Ξέπλυμα χρήματος (money laundering)

Με το ξέπλυμα χρήματος χαρακτηρίζεται η κάλυψη των χρημάτων από παράνομες δραστηριότητες. Απαρτίζεται από τρία στάδια. Το πρώτο στάδιο περιλαμβάνει την μετατροπή των παράνομων χρημάτων έτσι ώστε να μην μπορεί να γίνει αντιληπτή από τις αρχές. Το δεύτερο στάδιο γίνεται χρήση πολλών οικονομικών συναλλαγών για να κρύψουν τα χρήματα, και στο τρίτο στάδιο ολοκληρώνεται η μετατροπή της παρανομίας για να έχει την μορφή νόμιμου εισοδήματος. Η ανωνυμία του Διαδικτύου βοηθά στο ξέπλυμα χρήματος.

1.6.5 Απάτη στην κινητή τηλεφωνία

Ένα βήμα μετά την σταθερή τηλεφωνία πραγματοποίησαν τα κινητά τηλέφωνα, τα οποία στη αρχή ήταν απλά η εξέλιξη των σταθερών τηλεφώνων. Έπειτα από καιρό με την εξέλιξη της τεχνολογίας η δημιουργία αυτή έκανε και ένα βήμα παραπάνω, προσθέτοντας στις συσκευές αυτές και από μια καινούργια υπηρεσία. Η μεγάλη αλλαγή έγινε με την χρήση του Διαδικτύου. Οι περισσότερες κινητές συσκευές εξελίχτηκαν σε ένα μικρό υπολογιστή υιοθετώντας από τους κανονικούς ηλεκτρονικούς υπολογιστές πολλές αδυναμίες. Τα δεδομένα των κινητών μπορούν να ελεγχθούν από μακριά μέσω των υπηρεσιών που είναι εγκατεστημένες σε κάθε τηλέφωνο σύγχρονης τεχνολογίας. Οι

hacker μπορούν να εισβάλλουν στο λογισμικό και να υποκλέψουν συνομιλίες, φωτογραφίες και προσωπικά δεδομένα.[9]

1.6.6 Trafficking

Ο όρος ‘’Trafficking’’ είναι ο διεθνής όρος της παράνομης εμπορίας ανθρώπων. Είναι ένα καθαρό έγκλημα καθώς παραβιάζει σχεδόν όλα τα ανθρώπινα δικαιώματα. Πολλοί είναι οι τρόποι που διαπράττεται. Αρχικά ξεκίνησε με την εξαναγκαστική μετακίνηση αδύναμων ανθρώπων σε άλλες χώρες για μια καλύτερη ζωή, με σκοπό την εκμετάλλευση τους.[17]

Ο δράστης ή οι δράστες που συνήθως είναι συμμορίες κερδίζουν πολλά χρήματα εκδίδοντας τα θύματα με διάφορες τεχνικές. Στην πορεία με τη χρήση του Διαδικτύου η παραπλάνηση γίνεται ακόμα πιο εύκολη, με θύματα αυτή τη φορά και μικρά παιδιά.

Μορφές ‘’Trafficking’’:

- Σεξουαλική εκμετάλλευση: οι δράστες παραπλανούν τα θύματα τους, που σε αυτήν την περίπτωση είναι γυναίκες και συνήθως άλλης εθνικότητας με διάφορους τρόπους. Η σύγχρονη τεχνική τους είναι να ψαρεύει τα θύματά τους από τα μέσα κοινωνικής δικτύωσης παριστάνοντας κάποιον άλλο και το διακινεί σε σεξουαλικές πράξεις με ή χωρίς χρηματικό συνάλλαγμα. Υπάρχουν περιπτώσεις θυμάτων που είναι καταδικασμένες σε σκοτεινά δωμάτια να περιμένουν τις εντολές, αλλά αυτό δεν συμβαίνει πάντα.
- Εμπορία ανηλίκων: οι δράστες διακινούν ανήλικα παιδιά ανεξαρτήτου φίλου και ηλικίας και τα εκδίδει είτε στην σεξουαλική είτε στην εργασιακή εκμετάλλευση, αλλά και στην απόσπαση των οργάνων τους σε άλλες χώρες με χρηματικό αντάλλαγμα.
- Εργασιακή εκμετάλλευση: οι σπείρες εκδίδουν στην δουλεία παιδιά και ενήλικες, με διάφορες απειλές και πολλές φορές με βία για να κερδίζουν χρήματα.[18]

1.7 Ασφάλεια στο Διαδίκτυο

Ο κόσμος των ηλεκτρονικών υπολογιστών έχει γίνει πλέον κομμάτι της καθημερινότητας των ανθρώπων σε πολλούς κλάδους όπως για παράδειγμα στην εκπαίδευση, στο εμπόριο, στην επικοινωνία και στην ψυχαγωγία. Για τον λόγο αυτό οι χρήστες θα πρέπει να ενημερώνονται τακτικά για τα μέτρα ασφαλείας που πρέπει να λαμβάνουν κατά την

περιήγησή τους στο Διαδίκτυο και περισσότερο απ όλους οι χρήστες που έχουν συχνή επικοινωνία μέσω των προγραμμάτων κοινωνικής δικτύωσης (facebook, instagram, twitter, msn) και άλλα.[18]

Βέβαια με την έξαρση του ηλεκτρονικού εγκλήματος κανένας υπολογιστής δεν είναι ασφαλής.

Παρακάτω αναφέρονται κάποια μέτρα για την πρόληψη και την καλύτερη ασφάλεια των χρηστών στο Διαδίκτυο.

- Κωδικοί πρόσβασης: οι κωδικοί πρόσβασης είναι προσωπικοί για τον χρήστη του κάθε συστήματος, δεν μοιράζονται σε τρίτους και συνήθως δεν πρέπει να επιλέγουμε κωδικούς που περιέχου προσωπικά στοιχεία όπως την ημερομηνία γέννησης ή τον αριθμό του τηλεφώνου.
- Ασφάλεια από ιούς: μεγάλο είναι το φαινόμενο δημιουργίας ιών στα υπολογιστικά συστήματα. Για να αντιμετωπιστεί ένας ιός είναι απαραίτητη η χρήση ενός (antivirus). Η δουλειά που κάνει ένα antivirus είναι να εντοπίσει τον ιό, να ανιχνεύσει την ταυτότητα του προκειμένου να εκτιμηθεί η ζημιά που έχει κάνει και τέλος ανάλογα με το μέγεθος της ζημιάς, να διορθώσει το μολυσμένο αρχείο ή να το σβήσει.[4]
- Η ασφάλεια στο ηλεκτρονικό ταχυδρομείο: για την αποφυγή των επιθέσεων που γίνονται καθημερινά στο ηλεκτρονικό ταχυδρομείο είναι απαραίτητη η λήψη ενός antivirus για τον έλεγχο των μηνυμάτων που εισέρχονται και εξέρχονται, προκειμένου να αναγνωριστεί η ταυτότητα του αποστολέα και του παραλήπτη. Όπως είναι γνωστό η ασφάλεια στο ηλεκτρονικό ταχυδρομείο είναι ελάχιστη. Γι αυτό λοιπόν δεν καταχωρούμε ποτέ προσωπικά δεδομένα και δεν μοιράζουμε κωδικούς πρόσβασης, κωδικούς πιστωτικών καρτών και άλλες ευαίσθητες πληροφορίες.[4]
- Η ασφάλεια στις ηλεκτρονικές συναλλαγές: ένα μεγάλο ποσοστό ανθρώπων προτιμούν να πραγματοποιούν ηλεκτρονικές συναλλαγές. Σαφώς, είναι προφανές πως η πληρωμή των προϊόντων γίνεται με πιστωτικές κάρτες , επιταγές και με μηχανήματα αυτόματης μεταφοράς χρημάτων. Αυτό αυξάνει τους κινδύνους των επιθέσεων. Είναι βασική η προστασία των δεδομένων, γι αυτό το λόγο έχουν δημιουργηθεί πρωτόκολλα επικοινωνίας που προστατεύουν τα δεδομένα. Επίσης, ο ενδιαφερόμενος αγοραστής πρέπει πρώτα να ελέγχει την επιχείρηση και πιο συγκεκριμένα την εμπιστευτικότητα της και την ταυτότητα της. Σε πολλές

περιπτώσεις ο αγοραστής καταβάλλει μεγάλα χρηματικά ποσά για να αγοράσει κάτι αλλά ποτέ δεν το λαμβάνει η λαμβάνει κάτι άλλο από αυτό που βλέπει σε μια φωτογραφία. Αυτό γίνεται γιατί οι εγκληματίες δημιουργούν εικονικά ηλεκτρονικά καταστήματα αλλά πίσω από την εικόνα ενός ηλεκτρονικού υπολογιστή δεν υπάρχει τίποτα.[4]

2. Έρευνα με ερωτηματολόγια

Το ερωτηματολόγιο είναι η μέθοδος καταγραφής και επεξεργασίας των δεδομένων, βάση της οποίας, μπορούμε να πραγματοποιήσουμε μια επιστημονική ή μη επιστημονική έρευνα. Είναι ένα έντυπο με μια σειρά ερωτήσεων στο οποίο οι ερωτώμενοι καλούνται να απαντήσουν προκειμένου να ολοκληρωθεί η έρευνα. Η μέθοδος με την οποία συλλέγουμε τα δεδομένα, δηλαδή το πρακτικό μέρος πρέπει να συνδέεται με το θεωρητικό μέρος της έρευνας.[19]

Η μέθοδος ερωτηματολογίου είναι το μέσο με το οποίο επικοινωνεί ο ερευνητής με τον ερωτώμενο. Είτε έμμεσα είτε άμεσα. Ανάλογα με τον τύπο της έρευνας που θέλουμε να πραγματοποιήσουμε μπορούμε να υλοποιήσουμε το ερωτηματολόγιο ως εξής:

- Με τη χρήση του διαδικτύου
- Με την χρήση ταχυδρομείου
- Με την χρήση τηλεφώνου
- Με συνέντευξη

Ο τρόπος επιλογής του ερωτηματολογίου εξαρτάται από:

- Την αξιοπιστία των απαντήσεων που θα δοθούν
- Το εύρος του δείγματος
- Τον χρόνο που απαιτείται
- Τη χρηματοδότηση της έρευνας
- Το μέγεθος του ερωτηματολογίου, που συνήθως συνίσταται σε συνέντευξη.[17]

Πλεονεκτήματα ερωτηματολογίων:

- Υπάρχει δυνατότητα αποστολής σε πολλούς ανθρώπους
- Ευκολία στη δημιουργία και τη διακίνηση τους
- Δεν έχουν μεγάλο κόστος
- Δεν απαιτούν πολύ χρόνο για να δημιουργηθούν
- Η ανάλυση του δείγματος είναι τυποποιημένη
- Δεν υπάρχει άμεση επικοινωνία του ερωτώμενου και του ερευνητή

Μειονεκτήματα ερωτηματολογίων:

- Δεν υπάρχει δυνατότητα επεξήγησης του ερευνητή στις ερωτήσεις ανοιχτού τύπου

- Ο ερευνητής καθορίζει τον τρόπο που θα απαντήσει ο ερωτώμενος.[17]

2.1 Δημιουργία ερωτηματολογίου

Το ερωτηματολόγιο είναι ένα από τα συνηθέστερα εργαλεία που μας βοηθούν σε μια έρευνα. Με τον καθορισμό των ερωτήσεων βοηθούν τον ερευνητή στην καλύτερη διεξαγωγή της έρευνας. Για την καλύτερη και πιο επιτυχής έρευνα πρέπει να περιέχει τα ακόλουθα χαρακτηριστικά:

i. Πληρότητα
ii. Συνοχή
iii. Σαφήνεια
iv. Δομή
v. Σύνοψη περιγραφής ερωτήσεων ελέγχου
vi. Συντομία
vii. Βασικές οδηγίες συμπλήρωσης
viii. Να επιδέχεται κωδικογραφική και μηχανογραφική επεξεργασία

Η πληρότητα αναφέρεται στην κάλυψη όλων των πτυχών του χαρακτηριστικού που ερευνάται ενώ ήδη έχει γίνει αναφορά.

Η συνοχή αναφέρεται στην ανάγκη οργανικής σύνδεσης των επιμέρους ερωτημάτων μεταξύ τους. Ερωτήματα που είναι παρόμοια πρέπει να παρουσιάζονται ομαδοποιημένα και να ερωτώνται μαζί, έτσι ώστε ο ερωτώμενος να κατευθύνεται στη σωστή απάντηση.

Η σαφήνεια, δεν αναφέρεται μόνο στο περιεχόμενο των πληροφοριών αλλά και στο άτομο που θα δώσει τις απαντήσεις.

Η δομή του ερωτηματολογίου, αφορά τη σειρά με την οποία θα διατυπωθούν οι ομάδες των ερωτήσεων και αυτό έχει ιδιαίτερη σημασία στην ανταπόκριση του κοινού. Σε ένα ερωτηματολόγιο, προσωπικές ερωτήσεις στις οποίες το κοινό δυσκολεύεται να απαντήσει, δεν τις βάζουμε στην αρχή του ερωτηματολογίου.

Τα ερωτήματα ελέγχου τίθενται για τον έλεγχο της ορθότητας απαντήσεων σε βασικές ερωτήσεις.

Ένα ερωτηματολόγιο πρέπει να είναι σύντομο. Ερωτηματολόγια πολλών σελίδων ή με μεγάλη διατύπωση της κάθε ερώτησης τείνουν να κουράσουν τον ερωτώμενο και υπάρχει περίπτωση να μην ολοκληρωθούν. Για να αυξηθεί ο αριθμός απαντήσεων συνηθίζεται σε ένα ερωτηματολόγιο να υπάρχουν σύντομες οδηγίες για τον τρόπο συμπλήρωσής του. Τέλος, για κάθε ερώτηση του ερωτηματολογίου πρέπει να έχουν προβλεφθεί ειδικοί χώροι σε κάθε απάντηση ανοιχτού τύπου, για την κωδικογράφιση της, προκειμένου να μεταφραστεί η φράση σε μορφή αριθμού για την κατάλληλη επεξεργασίας της σε ηλεκτρονικό υπολογιστή.[7]

2.2 Τύποι ερωτήσεων

Δημιουργώντας ένα ερωτηματολόγιο , ο ερευνητής έχει την επιλογή ανάμεσα σε δύο είδη ερωτήσεων.

- Ερωτήσεις ανοιχτού τύπου
- Ερωτήσεις κλειστού τύπου

Στις ερωτήσεις ανοιχτού τύπου ο ερωτώμενος μπορεί να εκφέρει την γνώμη του χωρίς κανέναν περιορισμό. Αυτού του είδους οι ερωτήσεις είναι αρκετά πρακτικές όταν ο ερευνητής δεν είναι σίγουρος για τις επιλογές απάντησης που μπορεί να θέσει.

Οι ερωτήσεις κλειστού τύπου περιλαμβάνουν:

i. διχοτομικές ερωτήσεις: οι ερωτήσεις αυτές είναι πολύ κατανοητές και επιτρέπουν τον ερωτώμενο να επιλέξει μια από τις δύο επιλογές που δίνονται. Οι επιλογές είναι συνήθως : ΝΑΙ/ΟΧΙ
ii. ερωτήσεις βαθμονόμησης: στις ερωτήσεις αυτές ο ερωτώμενος μπορεί να επιλέξει μία από τις ήδη υπάρχουσες απαντήσεις, που είναι: ΚΑΘΟΛΟΥ/ΕΛΑΧΙΣΤΑ/ΜΕΤΡΙΑ/ΑΡΚΕΤΑ/ΠΟΛΥ.
iii. Ερωτήσεις κατάταξης: σε αυτή την περίπτωση ο ερωτώμενος καλείται να επιλέξει με σειρά προτεραιότητας, ανάλογα με το ποια επιλογή κατά τη γνώμη του είναι πιο σημαντική. Η επιλογή γίνεται 1 για το πρώτο, 2 για το δεύτερο, 3 για το τρίτο, 4…..,5…..
iv. Ερωτήσεις πολλαπλής επιλογής: σε αυτό το σημείο, ο ερωτώμενος έχει τη δυνατότητα να επιλέξει παραπάνω από μία επιλογές.[7]

2.2.1 Σειρά ερωτήσεων

Η σωστή σειρά που θα τοποθετηθούνε οι ερωτήσεις είναι και ο κύριος παράγοντας ενός σωστά δομημένου ερωτηματολογίου.

Συνήθως οι ερωτήσεις που περιέχουν τα στοιχεία ταυτότητας (φύλο, ηλικία) τοποθετούνται στην αρχή. Έπειτα, μπαίνουν οι πιο εύκολες ερωτήσεις προκειμένου να προκαλέσουν το ενδιαφέρον στον ερωτώμενο και ακολουθούν οι δύσκολες ερωτήσεις με σκοπό να είναι δύσκολο να αρνηθεί να απαντήσει. Κλείνοντας, οι ερωτήσεις που σχετίζονται με τι ίδιο θέμα, συμπεριλαμβάνονται όλες μαζί για να μην μπερδεύουν τον ερωτώμενο, αναγκάζοντάς τον να ανατρέχει στις προηγούμενες ερωτήσεις.

2.2.2 Διατύπωση των ερωτήσεων

Πέραν της σειράς, πρέπει να προσέξουμε και την διατύπωση των ερωτήσεων που είναι βασισμένες στους κανόνες της γραμματικής και του συντακτικού. Όλες οι ερωτήσεις

πρέπει να περιέχουν σαφήνεια και να είναι γραμμένες με τέτοιο τρόπο ώστε να είναι κατανοητές από όλο το κοινό. Δεν πρέπει να περιέχουν δύσκολες λέξεις που δεν είναι κατανοητές. Σε περίπτωση που είναι ανάγκη να δοθούν δύσκολες λέξεις πρέπει να δίνεται μία σύντομη επεξήγηση μέσα σε παρένθεση.

Συμπερασματικά, το περιεχόμενο των ερωτήσεων επιβάλλεται να είναι απλό και περιεκτικό.

2.2.3 Κωδικοποίηση των απαντήσεων του ερωτηματολογίου

Με τον όρο «κωδικοποίηση» ενός ερωτηματολογίου καταλήγουμε στη μετατροπή των απαντήσεων σε αριθμούς ή σύμβολα. Αυτό σημαίνει πως χρειάζεται να μετατρέψουμε το ποιοτικό σε ποσοτικό στοιχείο. Η κωδικοποίηση μετατρέπει τα στοιχεία σε τέτοια μορφή έτσι ώστε να είναι έτοιμα για μηχανογραφική επεξεργασία .

2.3 Δειγματοληψία

Ως δειγματοληψία ορίζεται η συγκέντρωση των στατιστικών δεδομένων που διεξάγει ο ερευνητής για την μελέτη ενός φαινομένου. Πριν ξεκινήσει η δειγματοληψία ο ερευνητής , πρέπει να ορίσει με σαφήνεια το σύνολο που έχει θέσει προς μελέτη. Όσο μεγαλύτερο είναι το δείγμα τόσο καλύτερα αποτελέσματα θα έχει.

Σκοπός της δειγματοληψίας είναι, να είναι ο προσδιορισμός των ιδιοτήτων του πληθυσμού μελετώντας τα δείγματα. Εάν το ποσοστό των δειγμάτων που θα πάρουμε είναι ανομοιογενές τότε είναι αναγκαία η συγκέντρωση μεγαλύτερου δείγματος.[7]

3. Το ερωτηματολόγιο και η έρευνα

Στόχος αυτής της έρευνας είναι η μελέτη όσο αφορά το ηλεκτρονικό έγκλημα, και πιο συγκεκριμένα το ηλεκτρονικό έγκλημα στα μέσα κοινωνικής δικτύωσης.

Ως κοινωνική δικτύωση ορίζεται η συμμετοχή των ανθρώπων σε διάφορες ομάδες με σκοπό την επικοινωνία στις ανθρώπινες σχέσεις και την εξέλιξη της χρηματικής συναλλαγής σε ηλεκτρονική συναλλαγή. Τα online κοινωνικά δίκτυα ως διαδικτυακές υπηρεσίες είναι αυτά που δίνουν τη δυνατότητα στους ανθρώπους να δημιουργήσουν προφίλ προκειμένου να εξασφαλίσουν την επικοινωνία τους με άλλες ομάδες. Τα social media είναι η επέκταση των κοινωνικών δικτύων με την μόνη διαφορά ότι αναφέρεται στα εργαλεία μέσω των οποίων γίνεται ο διαμοιρασμός της πληροφορίας στο κοινό. Οι πιο χρησιμοποιημένες εφαρμογές κοινωνικής δικτύωσης που παρέχονται δωρεάν είναι:

- Facebook: είναι μια εφαρμογή κοινωνικής δικτύωσης μέσω της οποίας ο χρήστης δημιουργεί ένα προσωπικό προφίλ και του παρέχει την δυνατότητα να επικοινωνεί και να ανταλλάσει φωτογραφίες, βίντεο και μηνύματα με άλλους χρήστες και ομάδες.
- Instagram: είναι μια εφαρμογή κοινωνικής δικτύωσης που παρέχει την δυνατότητα επεξεργασίας και κοινοποίησης φωτογραφιών στο διαδίκτυο.
- Viber: είναι μια εφαρμογή που δίνει την δυνατότητα για την πραγματοποίηση φωνητικών κλήσεων, γραπτών μηνυμάτων καθώς και κοινοποίησης φωτογραφιών και βίντεο λίγων λεπτών με την βοήθεια του διαδικτύου

Ο λόγος που επιλέχτηκε το ηλεκτρονικό έγκλημα στα μέσα κοινωνικής δικτύωσης ως αντικείμενο της έρευνας είναι γιατί ολοένα και περισσότεροι άνθρωποι όλων των ηλικιών χρησιμοποιούν το διαδίκτυο και κυρίως τιε σελίδες κοινωνικής δικτύωσης έτσι ώστε να εξυπηρετήσουν του σκοπούς τους. Με την διεξαγωγή αυτής της έρευνας θα παρατηρηθεί το πόσο ενημερωμένοι είναι οι χρήστες του διαδικτύου για την σωστή διαχείριση των σελίδων που χρησιμοποιούν αλλά και κατά πόσο γνωρίζουν την πολιτική απορρήτου της κάθε μιας σελίδας από αυτές.

Συχνά, οι χρήστες των σελίδων κοινωνικής δικτύωσης παραβλέπουν τους βασικούς κινδύνους του διαδικτύου και εστιάζουν μόνο στον σκοπό τους και ην διασκέδασή τους, έτσι ώστε να πραγματοποιήσουν την σκέψη τους.

Επίσης, οι ώρες που αφιερώνουν οι χρήστες χρησιμοποιώντας το διαδίκτυο συμβάλλει στην εξαπάτησή τους, καθώς επισκέπτονται διάφορες σελίδες είτε για την ψυχαγωγία είτε για την γνωριμία με άλλα άτομα, παρόλα αυτά δεν είναι λίγοι αυτοί που χρησιμοποιούν το διαδίκτυο για την εργασία και τις ηλεκτρονικές συναλλαγές τους. Τα τελευταία χρόνια, παρατηρείται μεγάλη παραπλάνηση με κύριο εργαλείο τέλεσης τις σελίδες κοινωνικής δικτύωσης. Υπάρχει σημαντική αύξηση στον αριθμών των γυναικών που έχουν πέσει θύματα σωματεμπορίας “trafficking” ιδίως των αλλοδαπών γυναικών που εκδίδονται στην πορνεία παρά την θέληση τους για καλύτερες συνθήκες διαβίωσης. Όμως το αποτέλεσμα

είναι το αντίθετο. Αναγκάζονται να ζούνε σε μη φυσιολογικές συνθήκες και παραμένουν φυλακισμένες σε διάφορα μέρη για να μην μπορούν να βοηθηθούν. Είναι προφανές λοιπόν να σημειωθεί ότι το ηλεκτρονικό έγκλημα εκτός κάποιων εξαιρέσεων έχει ως κύριο αντικείμενο το διαδίκτυο και τις σελίδες κοινωνικής δικτύωσης.

Για την πραγματοποίηση της παρούσας έρευνας προκειμένου να συγκεντρωθεί ένας ικανός αριθμός δειγμάτων, δημιουργήθηκε ένα ερωτηματολόγιο 17 ερωτήσεων, το οποίο συμπληρώθηκε από 121 άτομα άνδρες και γυναίκες.

Οι τύποι των ερωτήσεων που χρησιμοποιήθηκαν είναι όλες κλειστού τύπου και όλο το ερωτηματολόγιο αποτελείται από ερωτήσεις πολλαπλής επιλογής, γραμμικής κλίμακας από το 1 έως το 5 (1= δεν γνωρίζω, 5= πολύ καλά), πλέγμα πολλαπλών επιλογών με κλίμακα από το 1 έως το 5, καθώς και πλαίσια ελέγχου.

Το συγκεκριμένο ερωτηματολόγιο στήθηκε μέσω της εφαρμογής Google Drive. Τα βήματα που ακολουθήθηκαν για την δημιουργία αυτού είναι:

i. Δημιουργία προσωπικού λογαριασμού στο Google Drive
ii. Επιλογή → NEO
iii. Επιλογή → φόρμες Google

Η σειρά που δημιουργήθηκαν οι ερωτήσεις είναι πρώτα οι δημογραφικές (φύλο, ηλικία) και στη συνέχεια οι ερωτήσεις που αφορούν την παρούσα έρευνα.

Τέλος, η διακίνηση του ερωτηματολογίου έγινε με την βοήθεια των μέσων κοινωνικής δικτύωσης και πιο συγκεκριμένα , με την κοινοποίηση μέσω την εφαρμογής facebook, viber και του ηλεκτρονικού ταχυδρομείου. Ο χρόνος διακίνησης του ερωτηματολογίου ώστε να συλλεχθούν οι απαντήσεις ήταν από της 17/12/2017 έως και της 27/3/2018.

4. Περιγραφική Στατιστική

Η λέξη "Στατιστική" αποδίδεται στο γερμανό Gottfried Achewall (1719 – 1772). Προήλθε από τη λέξη status. Ο John Sinclair (1754 – 1835) ήταν ο πρώτος άγγλος συγγραφέας που υιοθετεί αυτόν τον όρο, κάνοντας επισκόπηση της Σκοτίας βασιζόμενος σε στοιχεία κοινωνικών συμβουλίων. Στα τέλη του 18^{ου} αιώνα, η στατιστική περιγράφεται ως ταυτόχρονη οριζόντια και κάθετη ανάπτυξη. Οριζόντια γιατί οι μέθοδοι εξαπλώθηκαν και σε άλλους κλάδους και κάθετοι διότι η αναγνώριση της έννοιας της πιθανότητας άνοιξε έναν νέο ορίζοντα για τη αρχή της στατιστικής συμπερασματολογίας.

Η περιγραφική στατιστική είναι η περιγραφή που βοηθά στην ανάλυση των δεδομένων, έτσι ώστε να προκύψουν μοτίβα για πιο αποτελεσματική παρουσίαση των δεδομένων. Τα περιγραφικά στατιστικά στοιχεία δεν επιτρέπουν την εξαγωγή συμπερασμάτων εκτός από την ανάλυση των δεδομένων ή να καταλήξουμε σε συμπεράσματα.

Οι μεταβλητές που αντιστοιχούν σε μια στατιστική έρευνα απαρτίζονται από ένα αρκετά μεγάλο πλήθος δεδομένων που συλλέγονται. Για να γίνει μια σύντομη παρουσίαση του δείγματος, πρέπει να γίνει μια αρχική εξαγωγή των συμπερασμάτων της έρευνας. Τα στοιχεία αυτά κατανέμονται σε μορφή πίνακα και έπειτα γίνεται χρήση γραφικών και αριθμητικών μεθόδων.

Παρακάτω αναφέρονται οι κυριότεροι τύποι μεταβλητών.

Κατηγορική: (Nominal): η μοναδική σχέση μεταξύ των κατηγοριών είναι η ύπαρξη διαφοράς. Το σύνολο των τιμών αυτών, των μεταβλητών , δεν έχει καμία χρησιμότητα, όπως για παράδειγμα το φύλο ή η οικογενειακή κατάσταση. Σημαντική είναι μόνο η μεταβλητή που μπορεί να πάρει διαφορετικές τιμές.

Διάταξη: (Ordinal): η διάταξη το μόνο που μπορεί να διασφαλίσει, είναι ο προσδιορισμός της κατηγορίας, και όχι της σύγκρισης, δηλαδή "ΚΑΘΟΛΟΥ", " ΕΛΑΧΙΣΤΑ","ΜΕΤΡΙΑ","ΚΑΛΑ","ΠΟΛΥ ΚΑΛΑ".

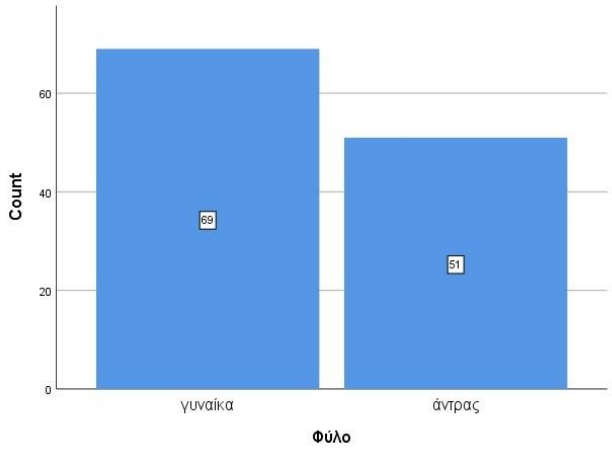
Οι μέθοδοι παρουσίασης των δεδομένων χωρίζονται σε δύο κατηγορίες:

i. Αριθμητικές μέθοδοι (πίνακες συχνοτήτων, μέτρα μεταβλητότητας, μέτρα μορφής).
ii. Γραφικές μέθοδοι (ιστόγραμμα, διάγραμμα διασποράς, ραβδογράμματα, τομεογράμματα, χρονοδιάγραμμα).[5]

4.1 Αποτελέσματα Περιγραφικής Στατιστικής

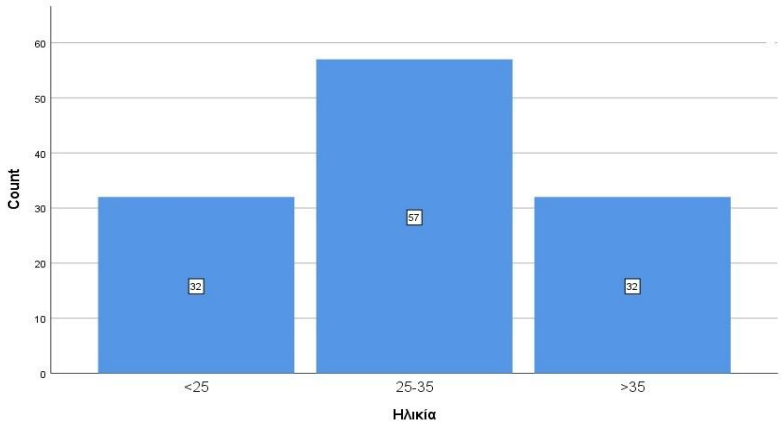
Η ανάλυση των δεδομένων πραγματοποιήθηκε με το πρόγραμμα SPSS 25. Πιο αναλυτικά, επιλέξαμε την καρτέλα Graphs→chart builder. Παρακάτω ακολουθεί η ανάλυση του ερωτηματολογίου τόσο των δημογραφικών όσο και των βασικών ερωτήσεων που

πραγματεύεται η έρευνα μας με σκοπό μιας πιο καθαρής εικόνας των ποσοστών των απαντήσεων και για να γίνει ένας πιο ουσιαστικός διαχωρισμός τους.



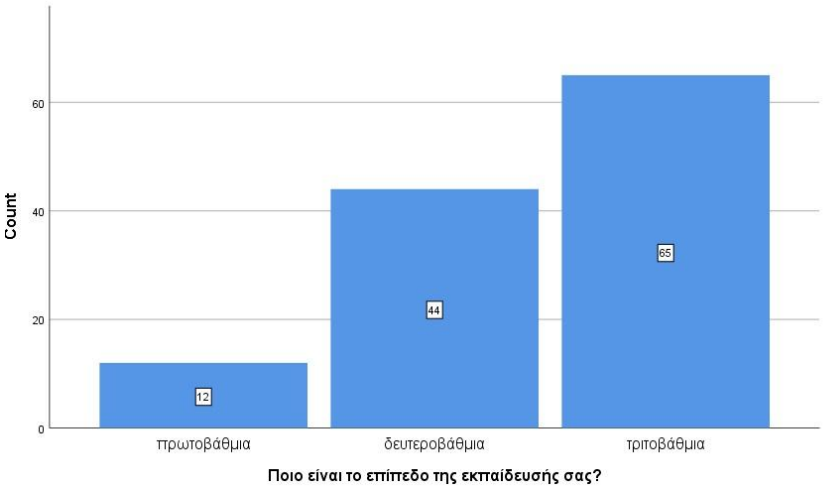
Εικόνα 4.1: Γράφημα αποτελεσμάτων φύλου.

Το 57.9% του πληθυσμού που απάντησαν ήταν γυναίκες και το 42,1% άντρες.



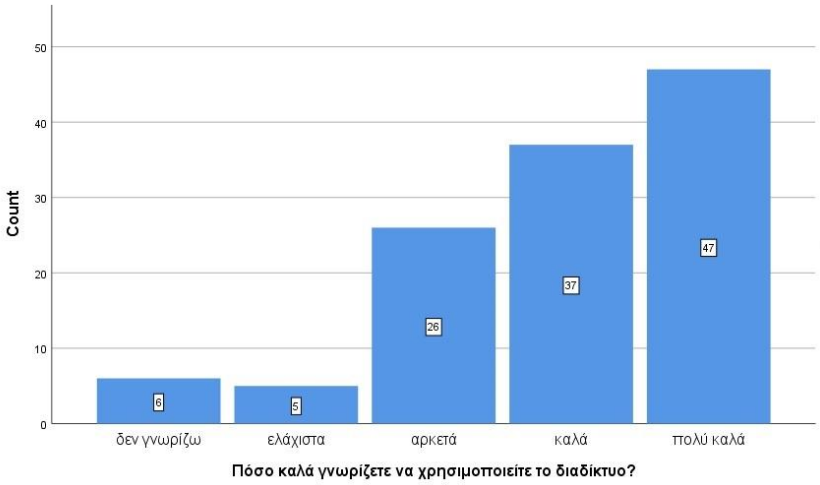
Εικόνα 4.2: Γράφημα αποτελεσμάτων ηλικίας.

Το 26,4% των ατόμων ήταν μικρότεροι των 25 ετών, το 47,1% μεταξύ 25 και 35 ετών και το υπόλοιπο 26,4% μεγαλύτεροι των 35.



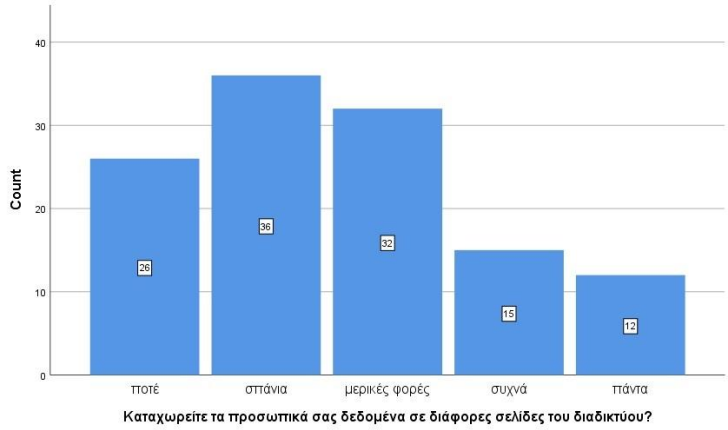
Εικόνα 4.3: Γράφημα αποτελεσμάτων εκπαίδευσης.

Έπειτα, στο επίπεδο της εκπαίδευσης το 9% του πληθυσμού έχει τελειώσει την πρωτοβάθμια εκπαίδευση, το 36,3% την δευτεροβάθμια και το 53,7% τελείωσε την τριτοβάθμια εκπαίδευση.



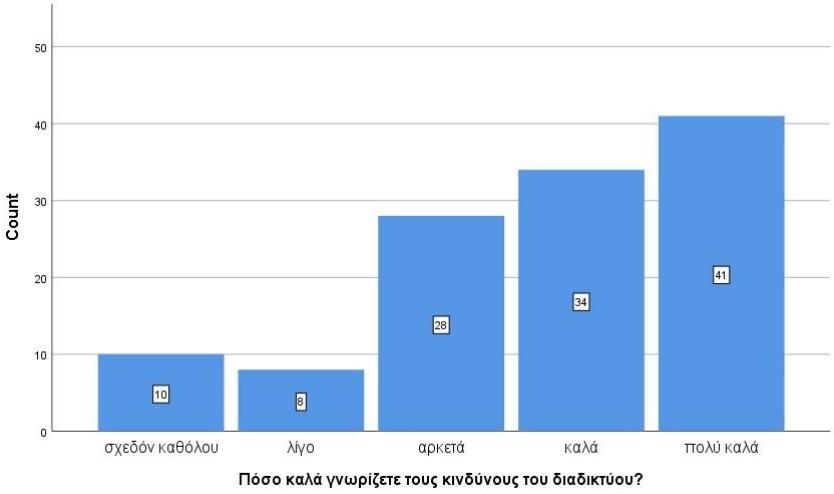
Εικόνα 4.4: Γράφημα αποτελεσμάτων γνώσης χρήσης του διαδικτύου.

Το 4,9% του πληθυσμού δεν γνωρίζουν να χρησιμοποιούνε το διαδίκτυο, το 4,1% γνωρίζει ελάχιστα, το 21,4% γνωρίζει αρκετά, το 30,5% γνωρίζει καλά και το 38,8% γνωρίζει πολύ καλά.



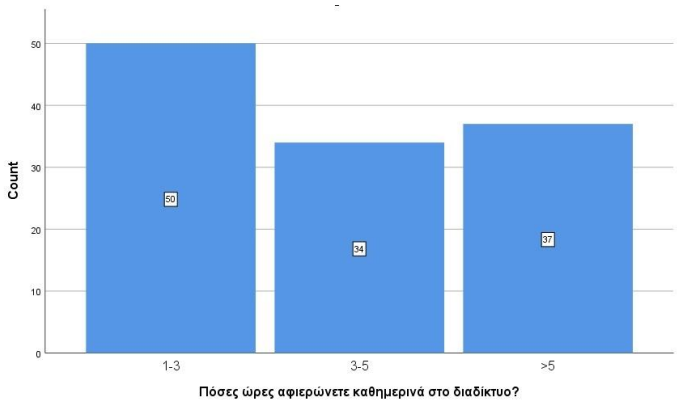
Εικόνα 4.5: Γράφημα αποτελεσμάτων των προσωπικών δεδομένων.

Στη συνέχεια, το 21,4% δεν καταχωρεί ποτέ τα προσωπικά του δεδομένα σε σελίδες του διαδικτύου. Το 29,7% τα καταχωρεί σπάνια, το 26,4% μερικές φορές, το 12,3% συχνά και μόλις 9.9% τα καταχωρεί πάντα.



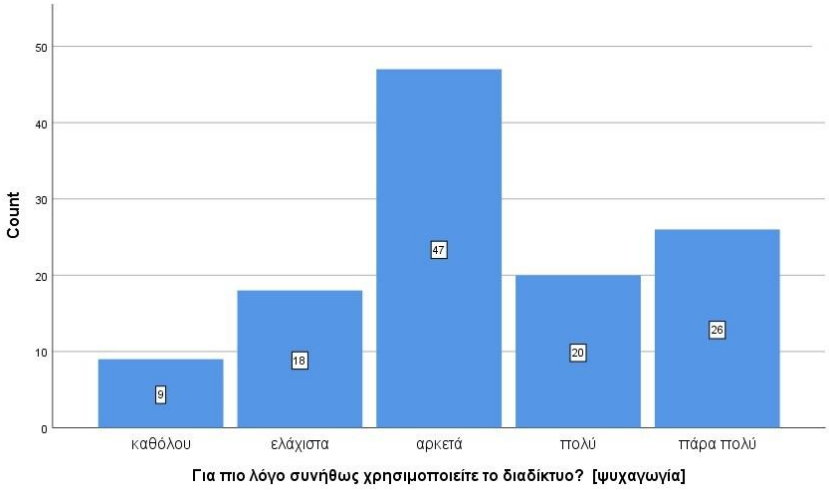
Εικόνα 4.6: Γράφημα αποτελεσμάτων των κινδύνων του διαδικτύου.

Το 8,2% του πληθυσμού δεν γνωρίζει σχεδόν καθόλου τους κινδύνους του διαδικτύου, το 6,6% τους γνωρίζει λίγο, το 23,1% αρκετά, το 28% καλά και το 33,8% τους γνωρίζει πολύ καλά.



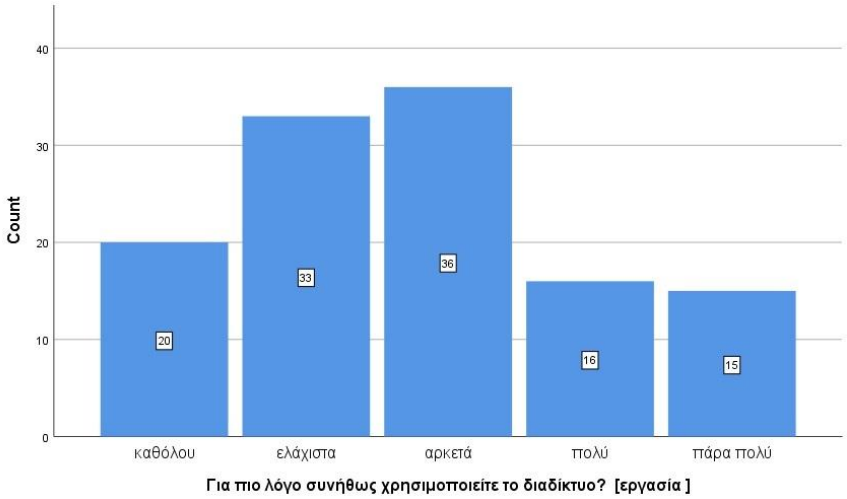
Εικόνα 4.7: Γράφημα αποτελεσμάτων των ωρών στο διαδίκτυο.

Το 41,3% αφιερώνουν καθημερινά για την χρήση τους στο διαδίκτυο από 1 έως 3 ώρες, το 28% από 3 έως 5 και το 30,5% περισσότερες από 5 ώρες .



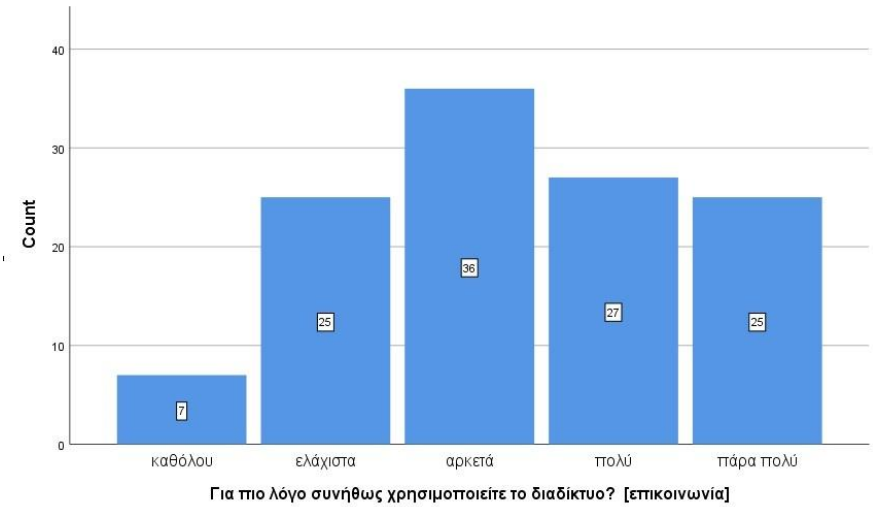
Εικόνα 4.8: Γράφημα αποτελεσμάτων χρήσης διαδικτύου για ψυχαγωγία.

Όσον αφορά τη χρήση του διαδικτύου για ψυχαγωγία, το 7,4% δεν το χρησιμοποιεί καθόλου, το 14,8% το χρησιμοποιεί ελάχιστα, το 38,8% αρκετά, το 16,5% το χρησιμοποιεί πιο πολύ και το 21,4% το χρησιμοποιεί πάρα πολύ.



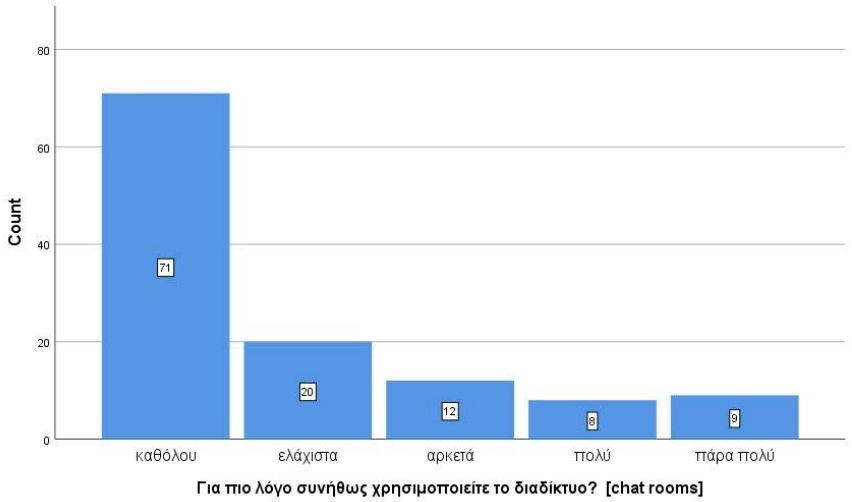
Εικόνα 4.9: Γράφημα αποτελεσμάτων χρήσης του διαδικτύου για εργασία.

Το ποσοστό που χρησιμοποιεί το διαδίκτυο για εργασία είναι 16,5% εκείνοι που δεν το χρησιμοποιούνε καθόλου, 27,2% εκείνοι που το χρησιμοποιούνε ελάχιστα, 29,7% αρκετά, 13,2% πολύ και 12,3% πάρα πολύ.



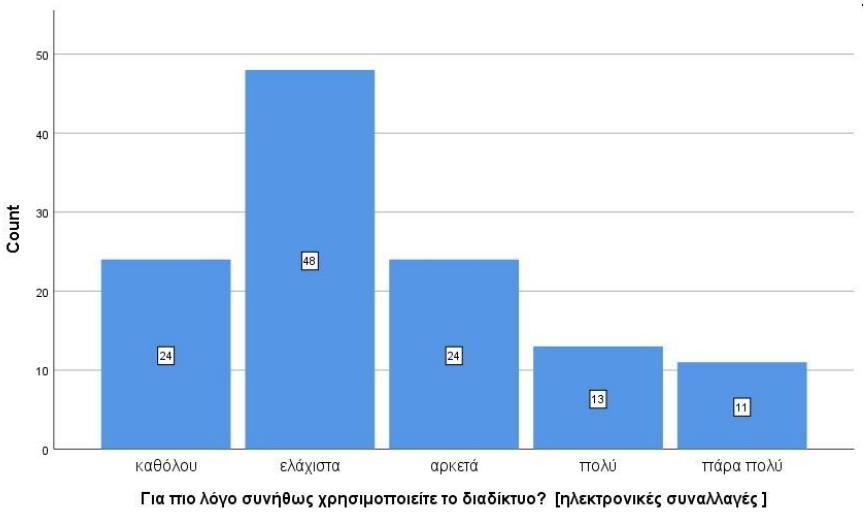
Εικόνα 4.10: Γράφημα αποτελεσμάτων χρήσης του διαδικτύου για επικοινωνία.

Για την επικοινωνία, το 5,7% δεν χρησιμοποιεί το διαδίκτυο σχεδόν καθόλου, το 20,6% το χρησιμοποιεί ελάχιστα, το 29,7% αρκετά, το 22,3% πολύ και το 20,6% πάρα πολύ.



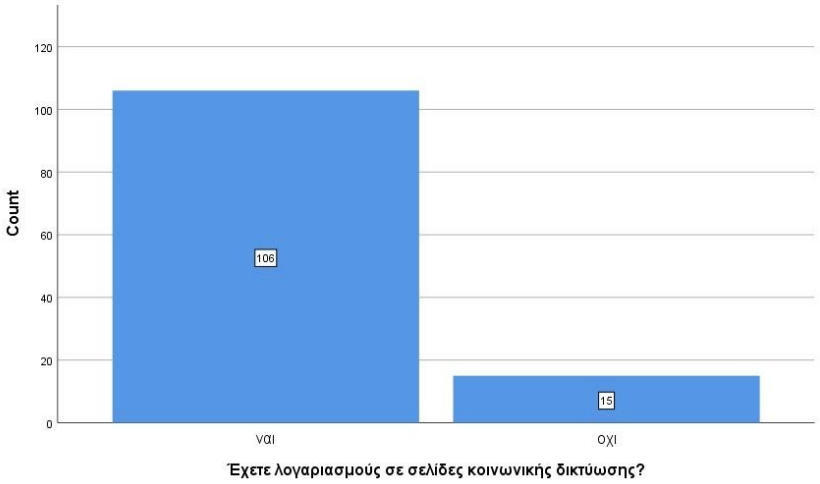
Εικόνα 4.11: Γράφημα αποτελεσμάτων χρήσης του διαδικτύου για chat rooms.

Επίσης, το 58.6% δεν χρησιμοποιούν καθόλου το διαδίκτυο για chat rooms, το 16,5% κάνουν ελάχιστη χρήση του, το 9,9% αρκετή, το 6,6% πολύ και το 7,4% πάρα πολύ.



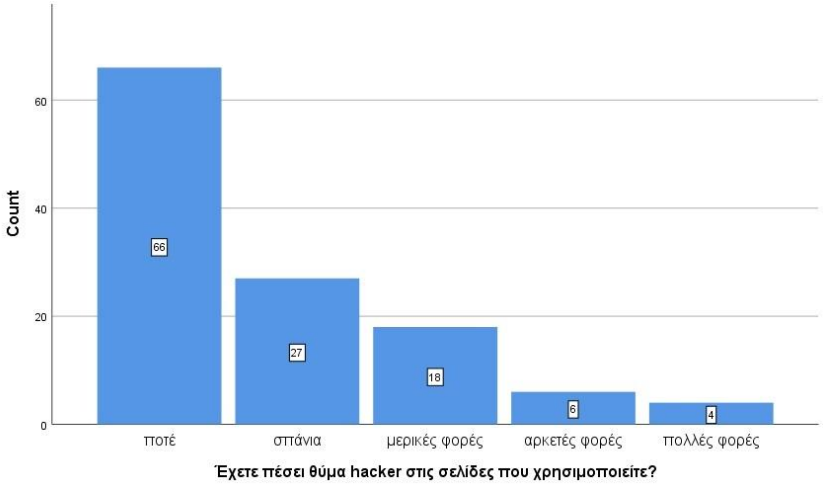
Εικόνα 4.12: Γράφημα αποτελεσμάτων χρήση του διαδικτύου για ηλεκτρονικές συναλλαγές.

Το 19,8% του πληθυσμού δεν πραγματοποιεί καθόλου ηλεκτρονικές συναλλαγές μέσω διαδικτύου, το 39,6% ελάχιστα, το 19,8% αρκετά, το 10,7% πολύ και τέλος, το 9% πάρα πολύ.



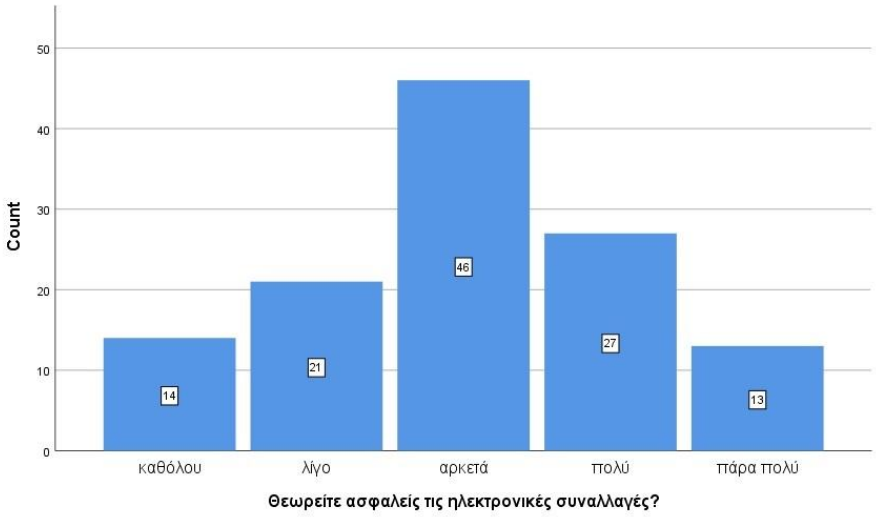
Εικόνα 4.13: Γράφημα αποτελεσμάτων των σελίδων κοινωνικής δικτύωσης.

Το 87,6% του πληθυσμού έχει λογαριασμούς σε σελίδες κοινωνικής δικτύωσης και το 12,3% πως δεν έχει.



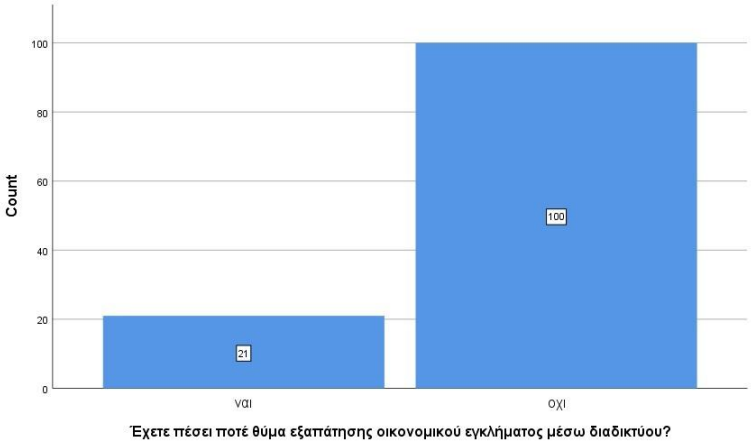
Εικόνα 4.14: Γράφημα αποτελεσμάτων των θυμάτων των σελίδων.

Το 54,5% δεν έχει πέσει θύμα hacker ποτέ, το 22,3% σπάνια, το 14,8% μερικές φορές, το 4,9% αρκετές φορές, και μόλις 3,3% έχει πέσει θύμα πολλές φορές.



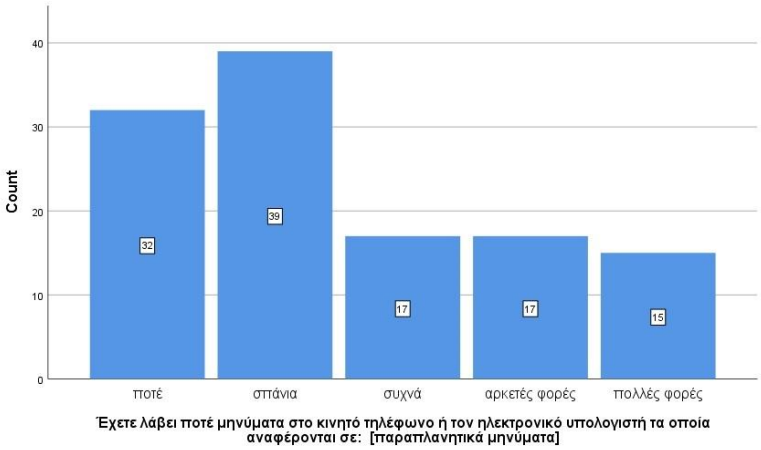
Εικόνα 4.15: Γράφημα αποτελεσμάτων ασφάλειας ηλεκτρονικών συναλλαγών.

Το 11,5% του δείγματος δεν θεωρούν καθόλου ασφαλείς τις ηλεκτρονικές συναλλαγές, το 17,3% τις θεωρούν λιγότερο ασφαλείς, το 38% αρκετά ασφαλείς, το 22,3% πολύ ασφαλείς και το 10,7% πάρα πολύ ασφαλείς.



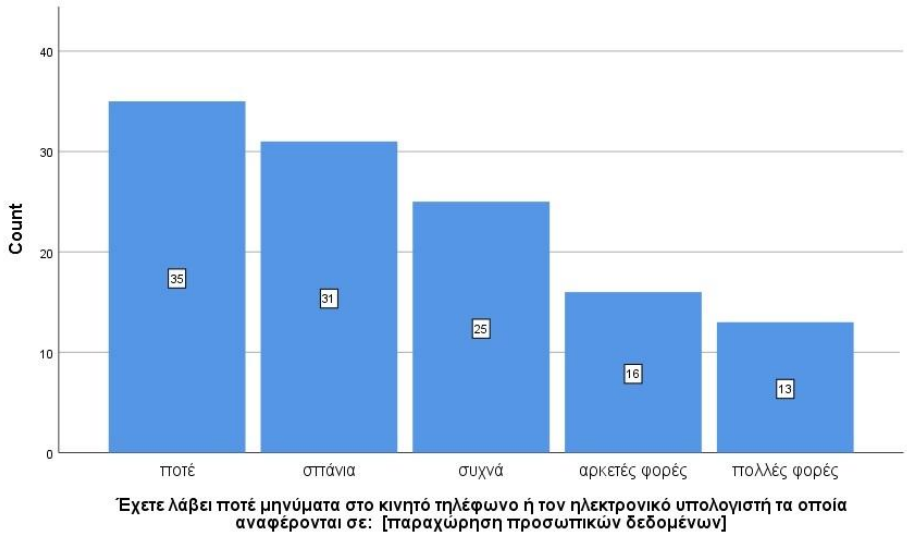
Εικόνα 4.16: Γράφημα αποτελεσμάτων των θυμάτων οικονομικού εγκλήματος.

Το μεγαλύτερο μέρος του δείγματος 82,6% δεν έχει εξαπατηθεί ποτέ οικονομικά μέσω διαδικτύου ενώ το 17,3% έχει εξαπατηθεί.



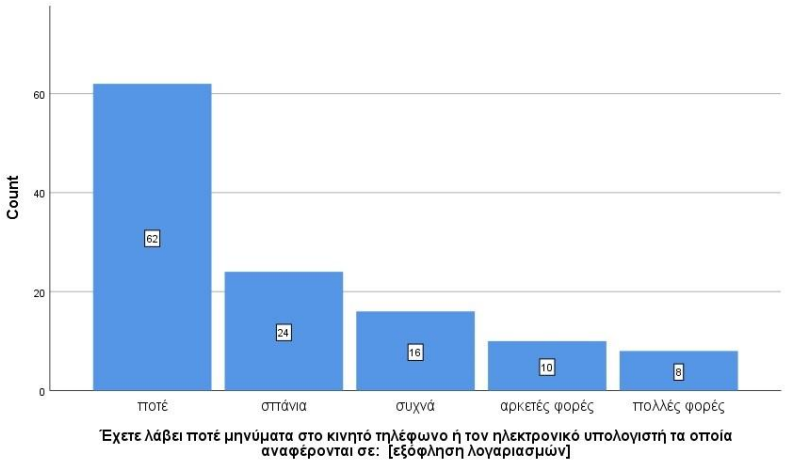
Εικόνα 4.17: Γράφημα αποτελεσμάτων για παραλαβή παραπλανητικών μηνυμάτων.

Το 3226,4% του δείγματος δεν έχει λάβει ποτέ παραπλανητικά μηνύματα, το 32,2% σπάνια έχει λάβει, το 14% λαμβάνει συχνά μηνύματα, το 14% λαμβάνει αρκετές φορές και το 12,3% πολλές φορές.



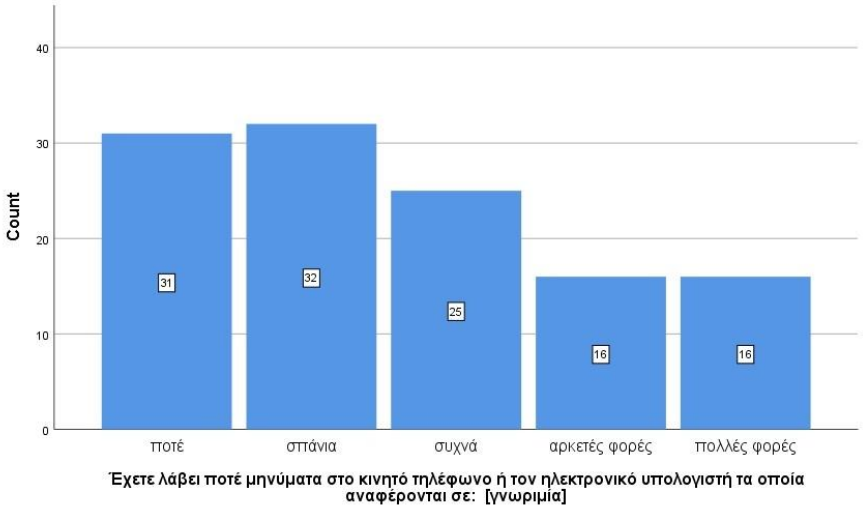
Εικόνα 4.18: Γράφημα αποτελεσμάτων για παραλαβή παραχώρησης προσωπικών δεδομένων.

Το 28,9% του δείγματος δεν έχει λάβει ποτέ μηνύματα παραχώρησης δεδομένων, το 25,6% σπάνια λαμβάνει, το 28,9% συχνά, το 13,2% λαμβάνει αρκετές φορές και το 10,7% πολλές φορές.



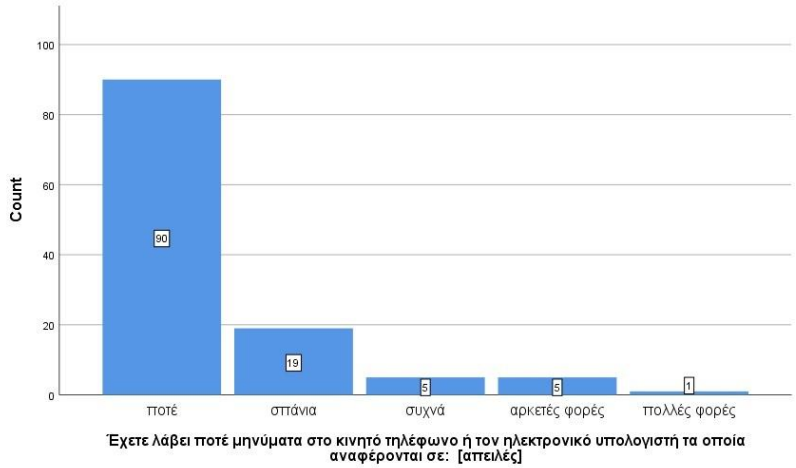
Εικόνα 4.19: Γράφημα αποτελεσμάτων για εξόφληση λογαριασμών.

Το 51,2% δεν έχει λάβει ποτέ μηνύματα όσον αφορά την εξόφληση λογαριασμών, το 19,8% σπάνια λαμβάνει, το 13,2% δέχεται συχνά, το 8,2% έχει πάρει αρκετές φορές και το 6,6% έχει πάρει πολλές φορές.



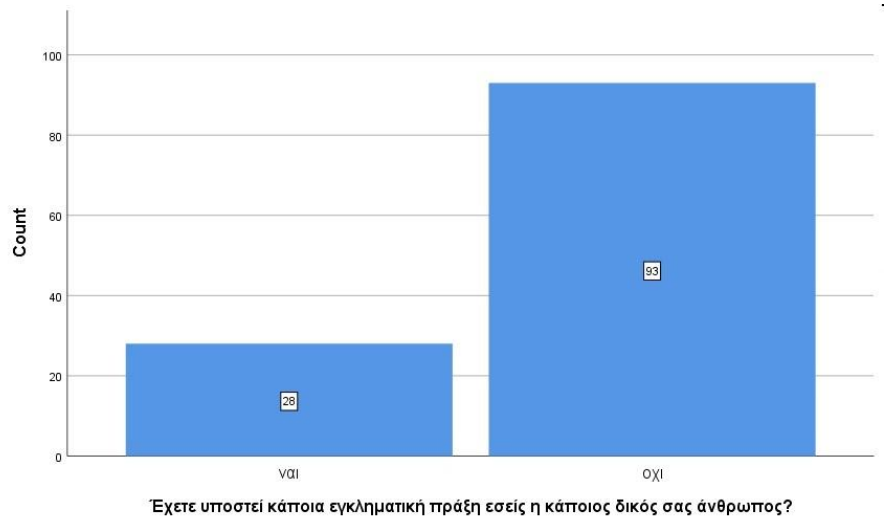
Εικόνα 4.20: Γράφημα αποτελεσμάτων για μηνύματα γνωριμίας.

Στη συνέχεια, σχετικά με την γνωριμία, το 25,6% δεν έχει δεχτεί μηνύματα, το 26,4% σπάνια δέχεται, το 20,6% λαμβάνει συχνά, το 13,2% αρκετές φορές και 13,2%πολλές φορές.



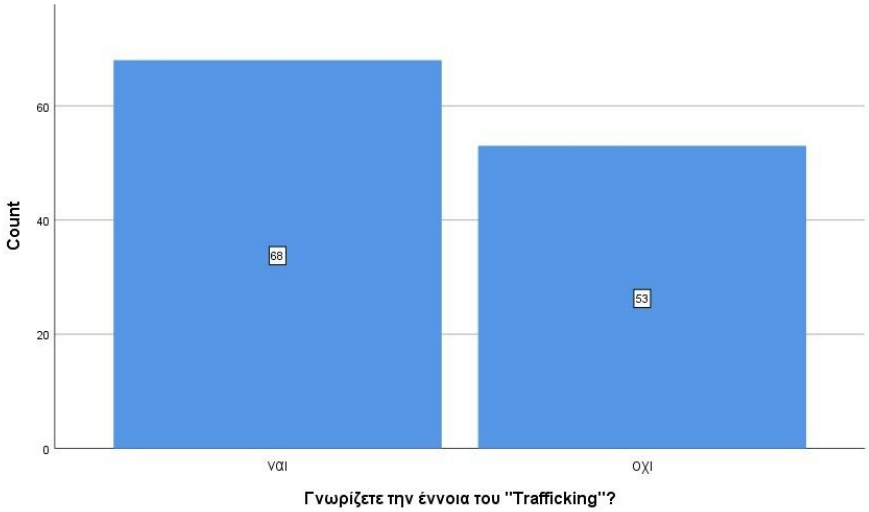
Εικόνα 4.21: Γράφημα αποτελεσμάτων για μηνύματα απειλών.

Το 74,3% δεν έχει λάβει ποτέ απειλές μέσω μηνυμάτων, το 15,7% σπάνια λαμβάνει, το 4,1% λαμβάνει αρκετές φορές και συχνά και μόνο το 1% έχει λάβει πολλές φορές.



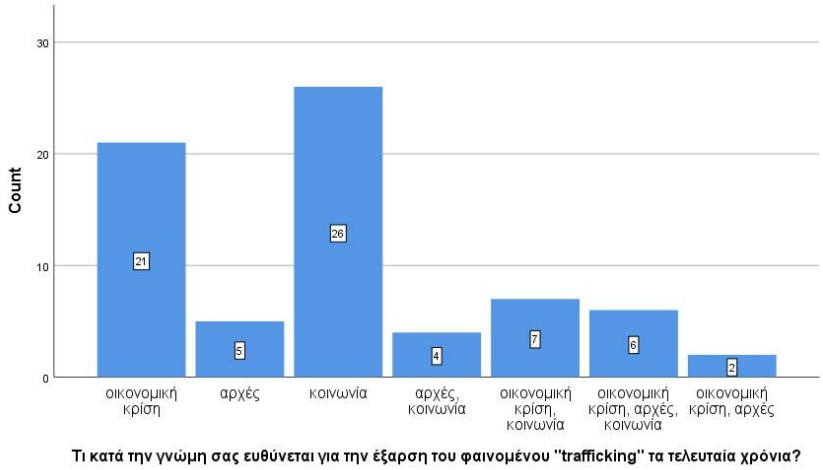
Εικόνα 4.22: Γράφημα αποτελεσμάτων για εγκληματική πράξη.

Το μεγαλύτερο δείγμα 76,8% δεν έχει υποστεί κάποια εγκληματική πράξη και το 23,1% έχει δεχτεί.



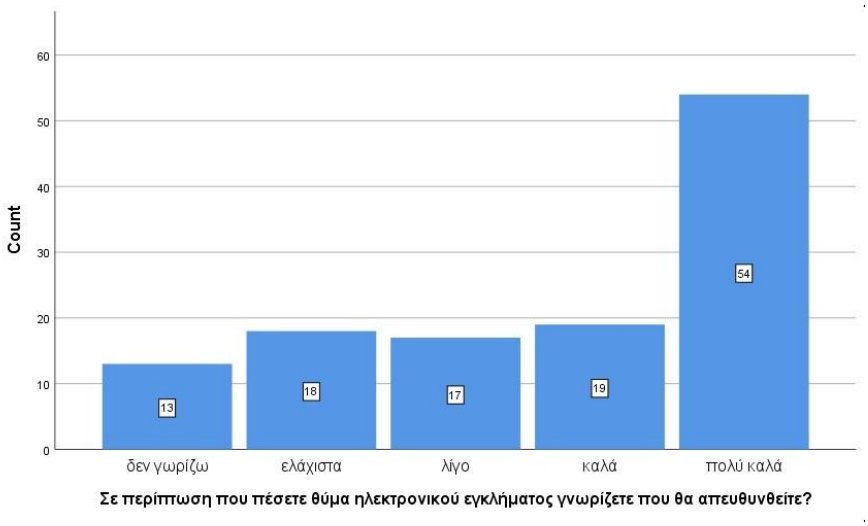
Εικόνα 4.23: Γράφημα αποτελεσμάτων για την έννοια του "trafficking".

Το 56,1% γνωρίζει την έννοια του trafficking, και το 43,8% δεν την γνωρίζει.



Εικόνα 4.24: Γράφημα αποτελεσμάτων για ευθύνες του «trafficking".

Το 17,3% θεωρεί πως το φαινόμενο οφείλεται στην οικονομική κρίση, το 4,1% στις αρχές, το 21,4% στην κοινωνία, το 3,3% στις αρχές και στην κοινωνία, το 5,7% στην οικονομική κρίση και την κοινωνία, το 4,9% στην οικονομική κρίση τις αρχές και την κοινωνία και μόλις ένα 1,6% στην οικονομική κρίση και τις αρχές.



Εικόνα 4.25: Γράφημα αποτελεσμάτων γνώσης σε περίπτωση κατάστασης ηλεκτρονικού εγκλήματος.

Το μεγαλύτερο ποσοστό του δείγματος 44,6% γνωρίζει πολύ καλά που θα απευθυνθεί σε περίπτωση που πέσει θύμα ηλεκτρονικού εγκλήματος, το 10,7% δεν γνωρίζει καθόλου, το 14,8% γνωρίζει ελάχιστα, το 14% λίγο και το 15,7% καλά.

5. Στατιστική Ανάλυση

Αρχικά θα ξεκινήσουμε με μία περιγραφή των ερωτήσεων του ερωτηματολογίου για να δείξουμε ποιες από αυτές θα μας βοηθήσουν στην ανάλυση που θα κάνουμε. Έπειτα, θα ορίσουμε τους άξονες με σκοπό την ομαδοποίηση των ερωτήσεων και θα περιγράψουμε ποιες ερωτήσεις περιέχει ο κάθε άξονας. Στη συνέχεια, θα ακολουθήσει η περιγραφή του δείκτη Cronbach's alpha(εσωτερικής συνοχής), έτσι ώστε να καταλήξουμε στην αξιοπιστία της έρευνας μας, όπως επίσης θα εξετάσουμε την ύπαρξη συσχετισμού μεταξύ των ομάδων με την μέθοδο One- way ANOVA και θα γίνουν οι απαραίτητες αναλύσεις.[9]

5.1 Ερωτήσεις και Άξονες

Στο ερωτηματολόγιο υπήρχαν 25 ερωτήσεις. Από αυτές κρατήσαμε μόνο της ερωτήσεις της κλίμακας Likert που είναι 14. Οι ερωτήσεις περιγράφουν το πρόβλημα πάνω στο οποίο κάνουμε την μελέτη δηλαδή στο ηλεκτρονικό έγκλημα.

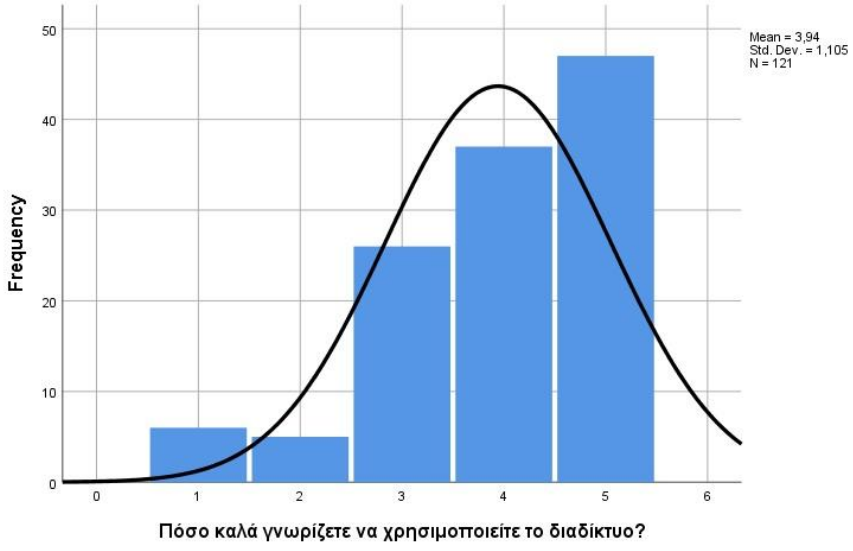
Παρακάτω ακολουθεί ο πίνακας των ερωτήσεων του ερωτηματολογίου που θα χρησιμοποιήσουμε για την ανάλυσή μας.

	Ερωτήσεις
1.	**Πόσο καλά γνωρίζετε να χρησιμοποιείτε το διαδίκτυο?**
2.	**Καταχωρείτε τα προσωπικά σας δεδομένα σε διάφορες σελίδες του διαδικτύου?**
3.	**Πόσο καλά γνωρίζετε τους κινδύνους του διαδικτύου?**
4.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ψυχαγωγία]**
5.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[εργασία]**
6.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[επικοινωνία]**
7..	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[chat rooms]**
8.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ηλεκτρονικές συναλλαγές]**
9.	**Θεωρείτε ασφαλείς τις ηλεκτρονικές συναλλαγές?**
10.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [**

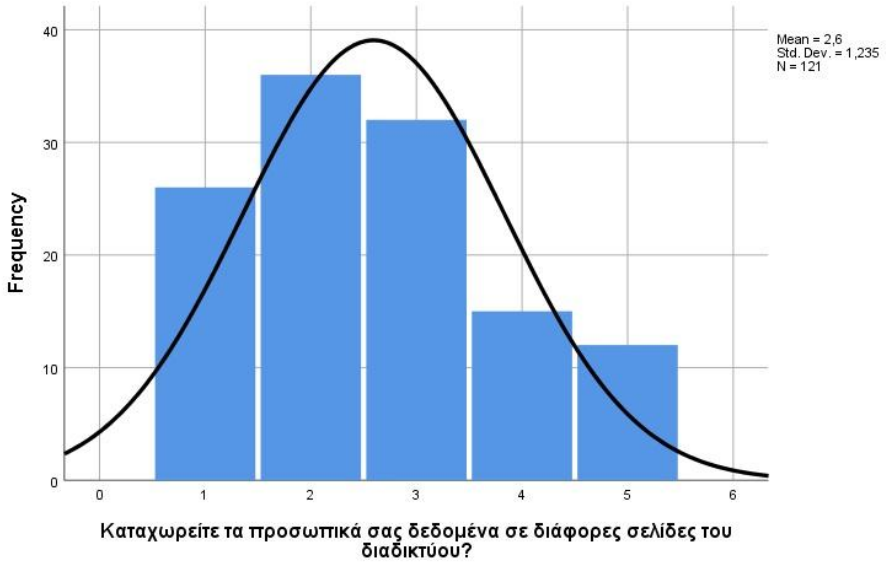
	παραπλανητικά μηνύματα]
11.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [παραχώρηση προσωπικών δεδομένων]**
12.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [εξόφληση λογαριασμών]**
13.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [γνωριμία]**
14.	**Σε περίπτωση που πέσετε θύμα ηλεκτρονικού εγκλήματος?**

Πίνακας 5.1: Πίνακας ερωτήσεων του ερωτηματολογίου.

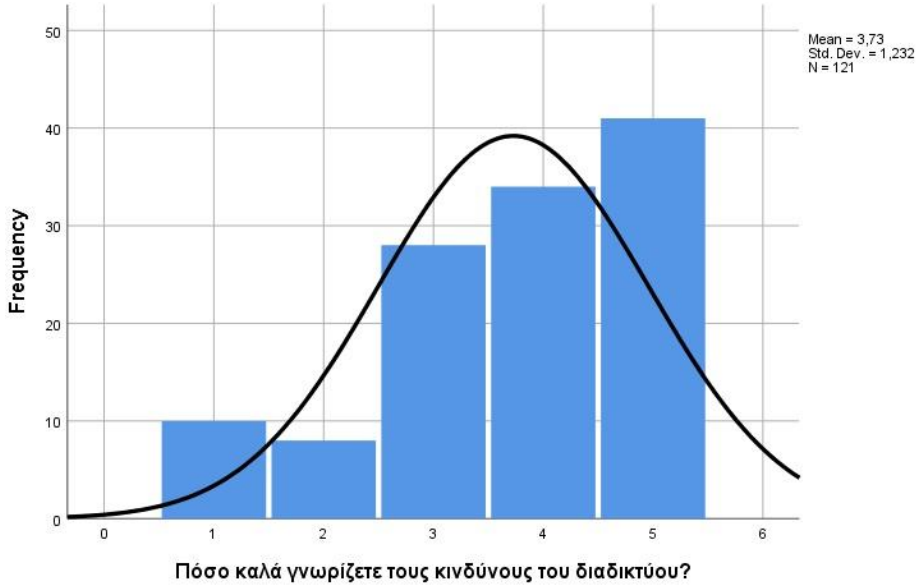
Στη συνέχεια, βλέπουμε τις εικόνες που φανερώνουν το πλήθος των απαντήσεων, την τυπική απόκλιση και τη μέση τιμή των απαντήσεων του ερωτηματολογίου. Το κάθε γράφημα ξεχωριστά μας φανερώνει την συχνότητα εμφάνισης κάθε τιμής της μεταβλητής που έχουμε επιλέξει.



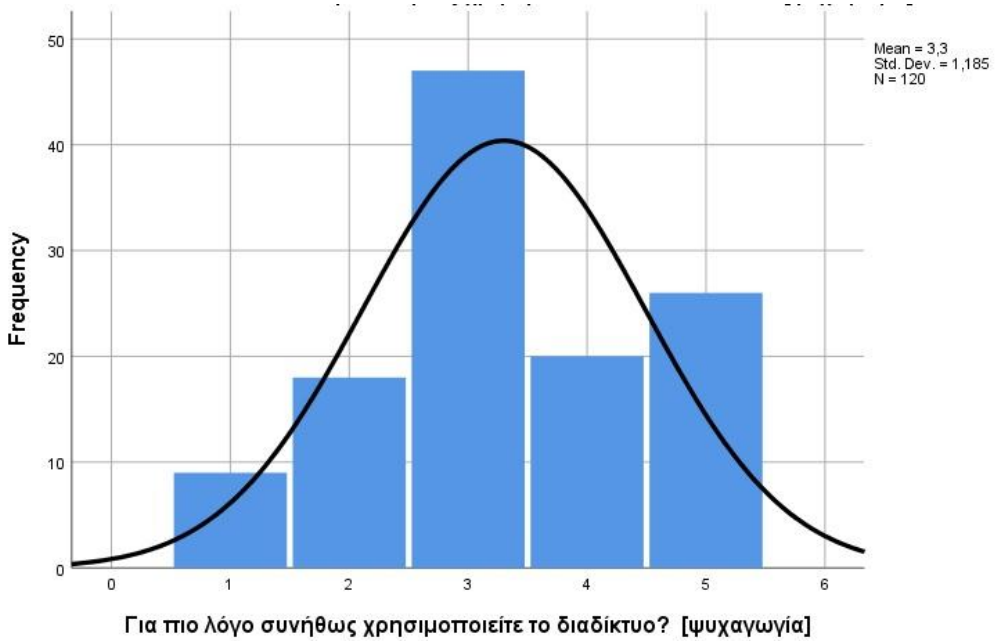
Εικόνα 5.1: Ιστόγραμμα αποτελεσμάτων γνώσης χρήσης του διαδικτύου.



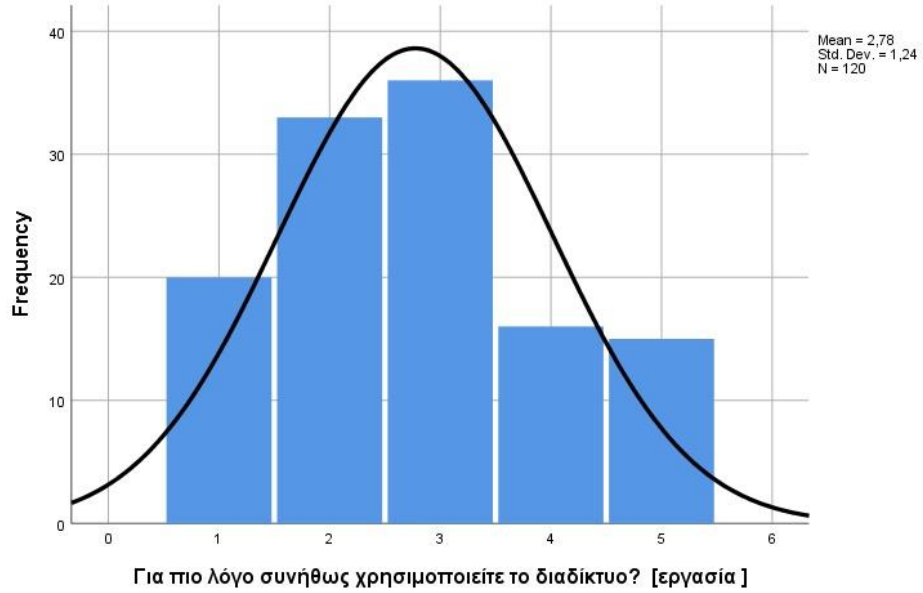
Εικόνα 5.2: Ιστόγραμμα αποτελεσμάτων καταχώρησης προσωπικών δεδομένων.



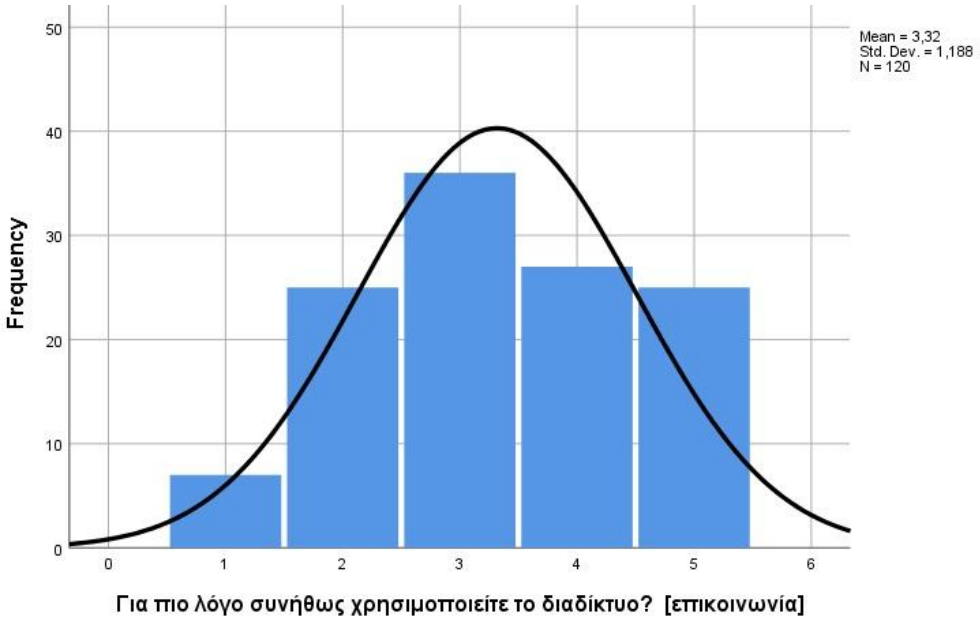
Εικόνα 5.3: Ιστόγραμμα αποτελεσμάτων κινδύνων του διαδικτύου.



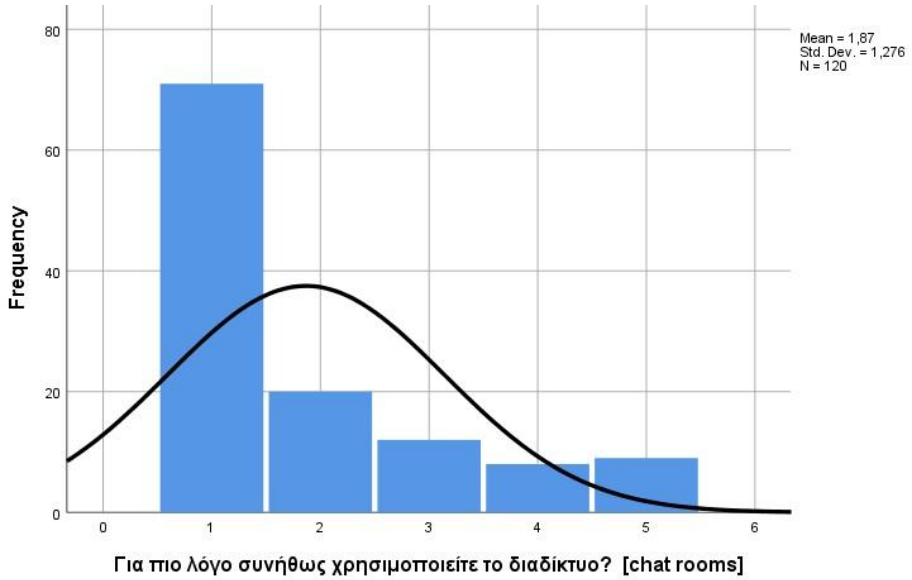
Εικόνα 5.4: Ιστόγραμμα αποτελεσμάτων χρήσης διαδικτύου για ψυχαγωγία.



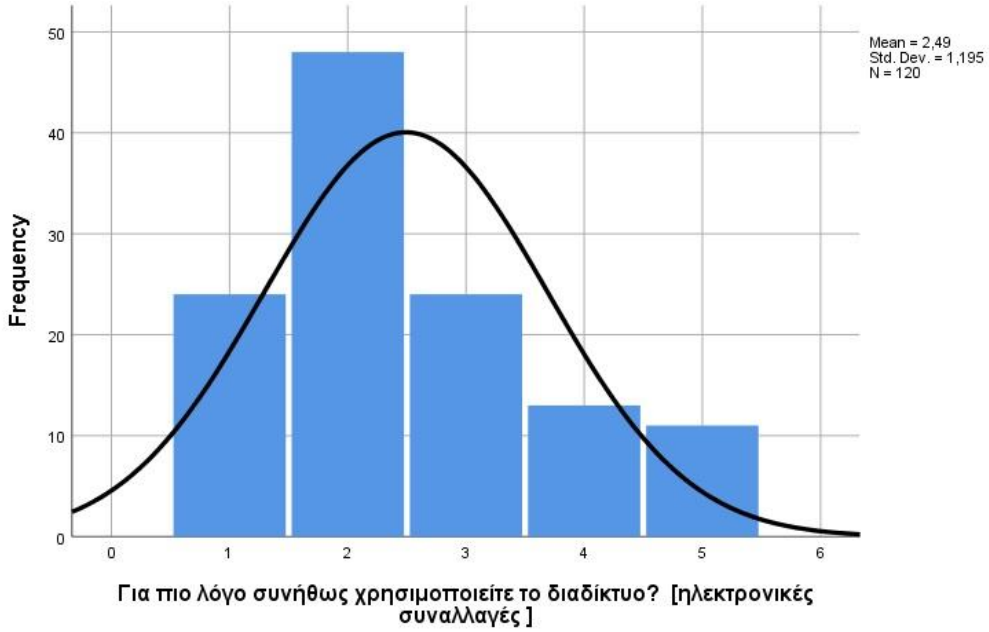
Εικόνα 5.5: Ιστόγραμμα αποτελεσμάτων χρήσης διαδικτύου για εργασία.



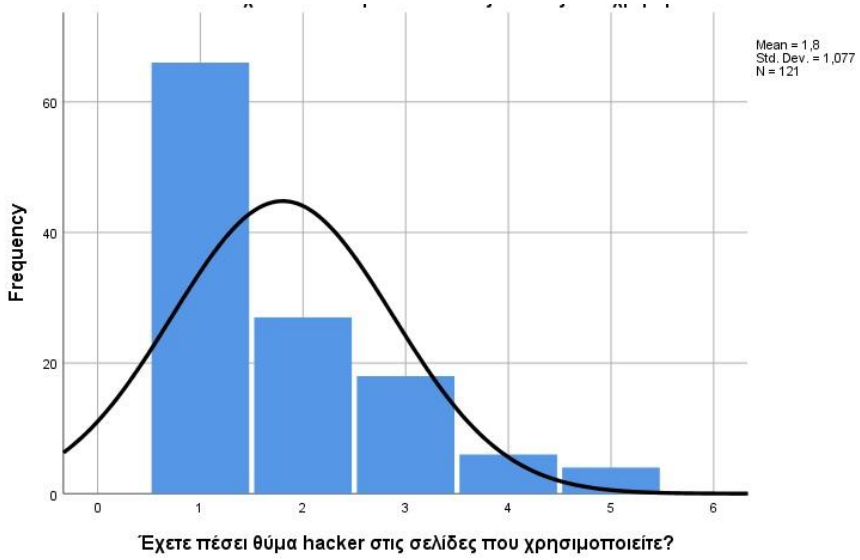
Εικόνα 5.6: Ιστόγραμμα αποτελεσμάτων χρήσης διαδικτύου για επικοινωνία.



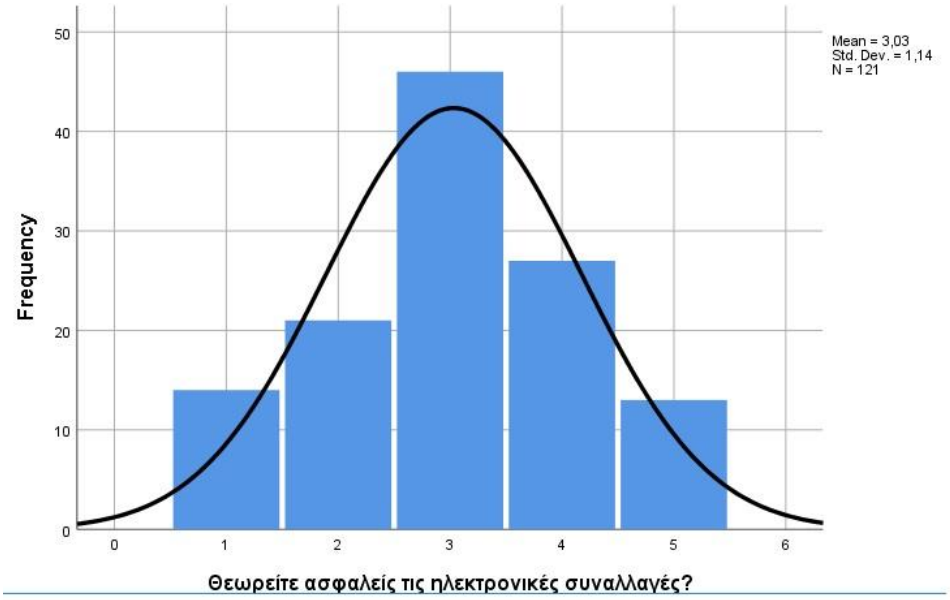
Εικόνα 5.7: Ιστόγραμμα αποτελεσμάτων χρήσης διαδικτύου για chat rooms.



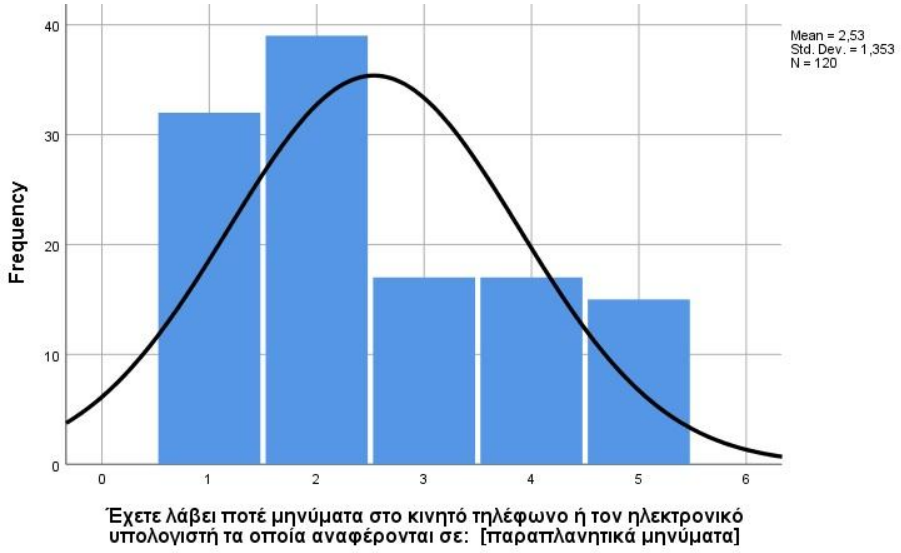
Εικόνα 5.8: Ιστόγραμμα αποτελεσμάτων χρήσης διαδικτύου για ηλεκτρονικές συναλλαγές.



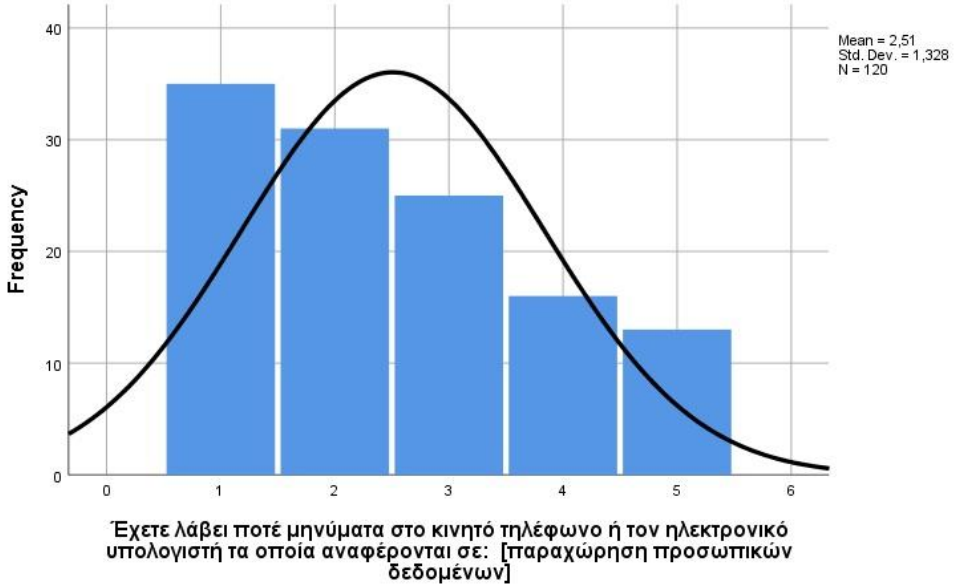
Εικόνα 5.9: Ιστόγραμμα αποτελεσμάτων ερώτησης αν έχετε πέσει θύμα hacker σε σελίδες του διαδικτύου.



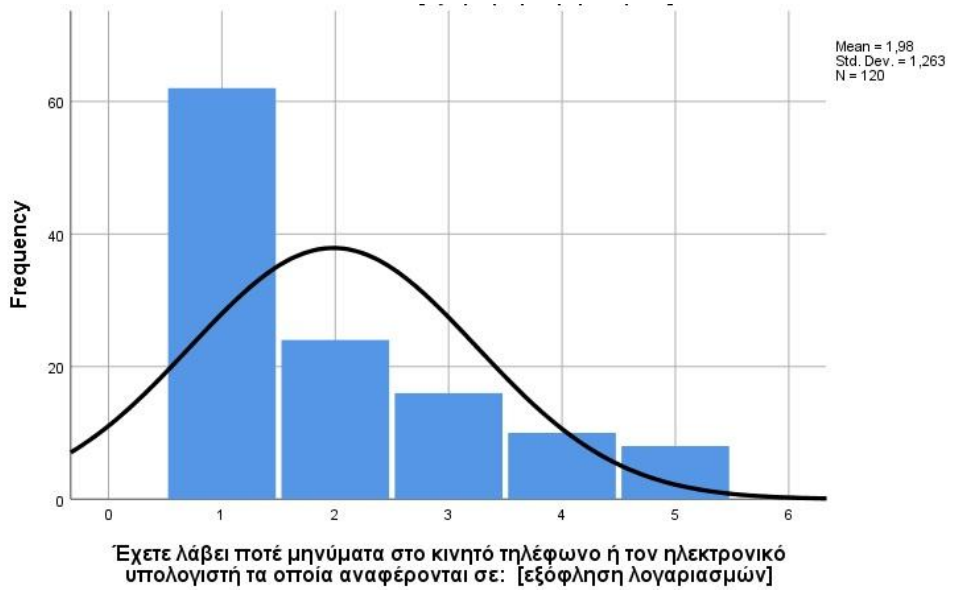
Εικόνα 5.10: Ιστόγραμμα αποτελεσμάτων ασφάλειας ηλεκτρονικών συναλλαγών.



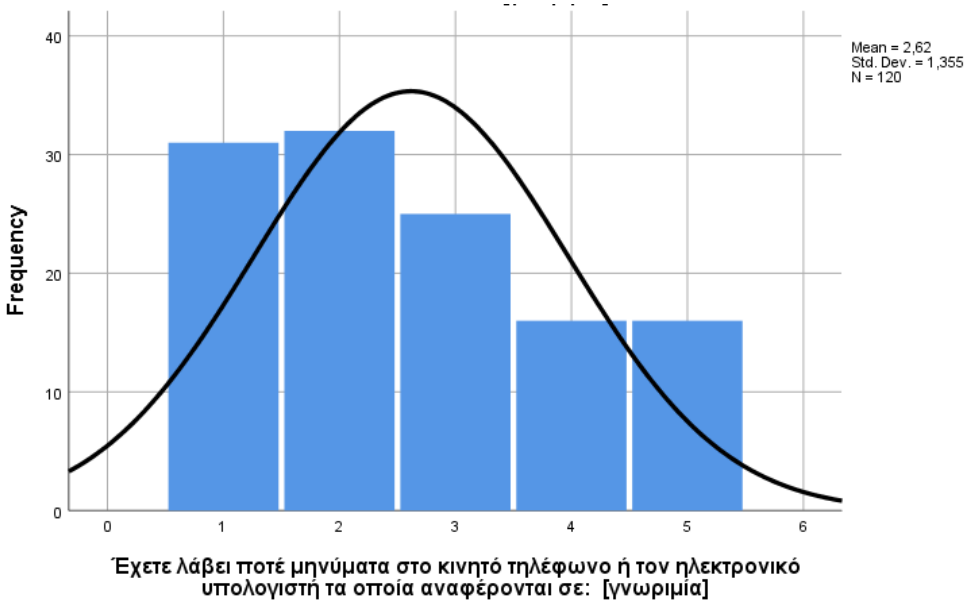
Εικόνα 5.11: Ιστόγραμμα αποτελεσμάτων λήψης παραπλανητικών μηνυμάτων.



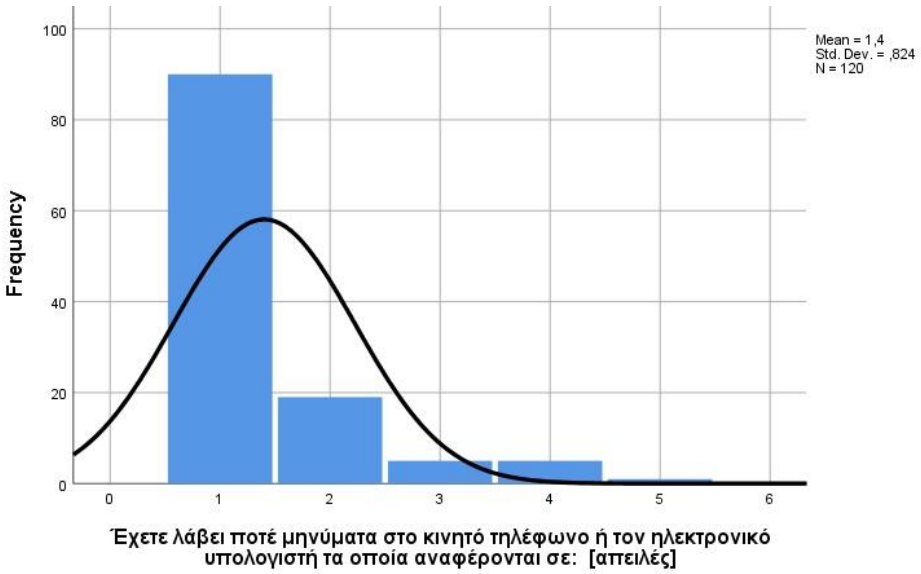
Εικόνα 5.12: Ιστόγραμμα αποτελεσμάτων λήψης μηνυμάτων για παραχώρηση προσωπικών δεδομένων.



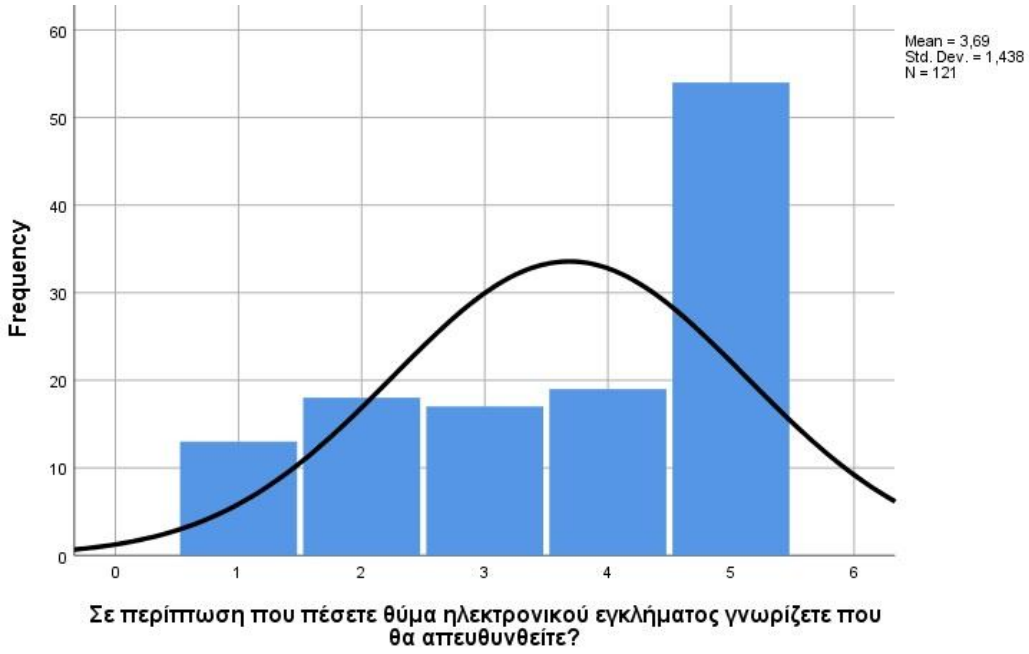
Εικόνα 5.13: Ιστόγραμμα αποτελεσμάτων λήψης μηνυμάτων για εξόφληση λογαριασμών.



Εικόνα 5.14: Ιστόγραμμα αποτελεσμάτων λήψης μηνυμάτων για γνωριμία.



Εικόνα 5.15: Ιστόγραμμα αποτελεσμάτων λήψης μηνυμάτων με απειλές.



Εικόνα 5.16: Ιστόγραμμα αποτελεσμάτων γνώσεων ηλεκτρονικού εγκλήματος.

Στις παραπάνω εικόνες παρατηρούμε πως η μέση τιμή των απαντήσεων που λάβαμε βρίσκεται κάπου στην μέση των απαντήσεων. Η τυπική απόκλιση είναι μεταξύ 1,5 και 4. Αυτό σημαίνει πως οι ακραίες τιμές δεν λαμβάνονται υπόψην.

5.2 Άξονες

Στη συνέχεια, έγινε ομαδοποίηση των ερωτήσεων με αποτέλεσμα να εξάγουμε τους άξονες που στόχος μας είναι η συνολική απεικόνιση του ερωτηματολογίου σε σχέση με βασικά θέματα που σχετίζονται με την έρευνα. . Η δημιουργία τους πραγματοποιήθηκε από το μενού του SPSS και την καρτέλα Transform → Compute Variable ορίζοντας στα κατάλληλα πλαίσια το όνομα του παράγοντα και στη συνέχεια αθροίζοντας τις ερωτήσεις που θέλουμε να περιλαμβάνει.

Οι άξονες που χρησιμοποιήσαμε είναι τρείς.

Άξονας 1: " Χρήση Διαδικτύου", περιέχει τις ερωτήσεις που σχετίζονται με τη χρήση του διαδικτύου και πιο συγκεκριμένα τους λόγους που μπορεί κάποιος να χρησιμοποιεί το διαδίκτυο.

- Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ψυχαγωγία]
- Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[εργασία]
- Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[επικοινωνία]
- Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[chat rooms]
- Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ηλεκτρονικές συναλλαγές]

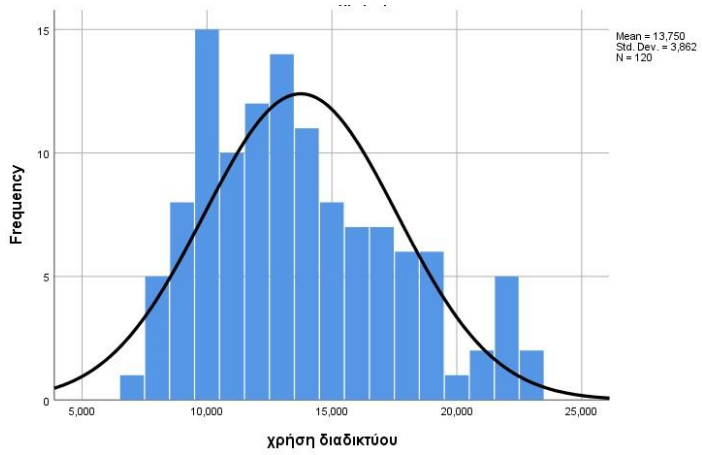
Άξονας 2: " Γνώσεις και σχέση με το Διαδίκτυο", περιέχει τις γνώσεις της χρήσης και τους κινδύνους που μπορεί να κρύβει το διαδίκτυο. Στόχος είναι να δούμε κατά πόσο γνωρίζουν οι άνθρωποι που απάντησαν να χρησιμοποιούν ορθά το διαδίκτυο.

- Πόσο καλά γνωρίζετε να χρησιμοποιείτε το διαδίκτυο?
- Πόσο καλά γνωρίζετε τους κινδύνους του διαδικτύου?
- Σε περίπτωση που πέσετε θύμα ηλεκτρονικού εγκλήματος γνωρίζετε που θα απευθυνθείτε?

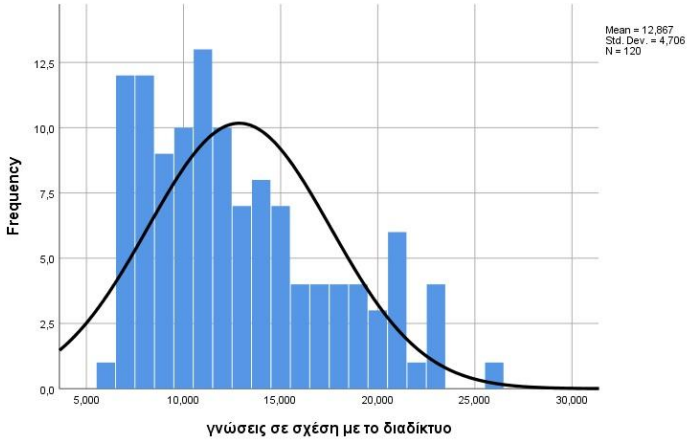
Άξονας 3: " Επικίνδυνες Καταστάσεις", περιέχει τις ερωτήσεις καταστάσεων, και στόχος είναι να παρατηρήσουμε κατά πόσο έχουν βρεθεί αντιμέτωποι με επικίνδυνες καταστάσεις του διαδικτύου.

- Έχετε πέσει ποτέ θύμα οικονομικού εγκλήματος μέσω διαδικτύου?
- Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε παραπλανητικά μηνύματα?
- Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε παραχώρηση προσωπικών δεδομένων?
- Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε εξόφληση λογαριασμών?
- Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε γνωριμία?
- Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε απειλές?

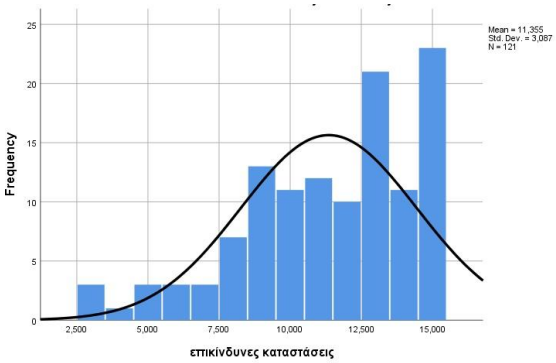
Παρακάτω ακολουθεί η εικόνα του κάθε άξονα ξεχωριστά φανερώνοντας το πλήθος των απαντήσεων, και το άθροισμα της μέσης τιμής και την τυπική απόκλιση όλων των απαντήσεων από τις ερωτήσεις που αποτελούν τους άξονες.



Εικόνα 5.17: Ιστόγραμμα αποτελεσμάτων άξονα για χρήση του διαδικτύου.



Εικόνα 5.18: Ιστόγραμμα αποτελεσμάτων άξονα γνώσεις σε σχέση με το διαδίκτυο.



Εικόνα 5.19: Ιστόγραμμα αποτελεσμάτων άξονα, επικίνδυνων καταστάσεων.

5.3 Παραγοντική Ανάλυση (Factor Analysis)

Μετά την περιγραφική ανάλυση ακολούθησε η παραγοντική ανάλυση (factor analysis) στις 16 μεταβλητές του ερωτηματολογίου της κλίμακας Likert με την μέθοδο ορθογώνιας περιστροφής αξόνων(varimax rotation), η οποία ελαχιστοποιεί τον αριθμό των μεταβλητών που έχουν μεγάλες επιβαρύνσεις. Επιλέξαμε την ορθογώνια περιστροφή αξόνων για να ερμηνεύσουμε πιο εύκολα τους παράγοντές μας. Ορίσαμε ότι οι τιμές πρέπει να είναι ίσες με το 1 και σαν μικρότερη τιμή ορίσαμε το 0,5. Στη συνέχεια εφαρμόστηκε σε δύο επίπεδα. Στο επίπεδο των ερωτήσεων και το επίπεδο των αξόνων.

ΠΙΝΑΚΑΣ ΑΞΙΟΛΟΓΗΣΗΣ FACTOR ANALYSIS	
Τιμή του συντελεστή	**Αξιοπιστία**
<0,5	Μη αποδεκτή αξιοπιστία
0,5-0,6	Μικρή συνοχή
0,6-0,7	Αποδεκτή
0,7-0,9	Καλή
>0,9	Εξαιρετική αξιοπιστία

Πίνακας 5.2: Πίνακας αξιολόγησης factor analysis.

5.3.1 Παραγοντική Ανάλυση Ερωτήσεων

Η παραγοντική ανάλυση μας βοηθά να ομαδοποιήσουμε τις μεταβλητές σε κοινές συνιστώσες. Με άλλα λόγια, μας βοηθά να συνδέσουμε τους παράγοντες με τις μεταβλητές που έχουμε πάρει μετρήσεις. Στόχος της παραγοντικής ανάλυσης είναι να μελετήσουμε μόνο την διακύμανση την οποία έχουν κοινή οι μεταβλητές που θα αναλύσουμε. Παρακάτω ακολουθούν τα αποτελέσματα παραγοντικής ανάλυσης με τη μέθοδο περιστροφή αξόνων.

Στον πίνακα που ακολουθεί παρατηρούμε ότι με την πραγματοποίηση της περιστροφής το ποσοστό διακύμανσης αυξάνεται σε σχέση με το αρχικό. Στην ερώτηση 11 και 15 παρατηρούμε πτώση της διακύμανσης στην περιστροφή.

		Component Matrix a	**Rotated component Matrix** a
1.	**Πόσο καλά γνωρίζεται να χρησιμοποιείτε το διαδίκτυο?**	,649	,791
2.	**Καταχωρείτε τα προσωπικά σας δεδομένα σε διάφορες σελίδες του διαδικτύου?**	,439	,519
3.	**Πόσο καλά γνωρίζεται τους κινδύνους του διαδικτύου?**	,627	,794
4.	**Για ποιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ΨΥΧΑΓΩΓΙΑ]**	,542	,706
5.	**Για ποιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ΕΡΓΑΣΙΑ]**	,519	,523
6.	**Για ποιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ΕΠΙΚΟΙΝΩΝΙΑ]**	,707	,820
7.	**Για ποιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[CHAT ROOMS]**	,425	,680
8.	**Για ποιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ]**	,492	,713
9.	**Έχετε πέσει θύμα hacker στις σελίδες που χρησιμοποιείτε?**	,666	,367
10.	**Θεωρείτε ασφαλείς τις ηλεκτρονικές συναλλαγές?**	,757	,752
11.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα**	,735	,829

	οποία αναφέρονται σε:[ΠΑΡΑΠΛΑΝΗΤΙΚΑ ΜΗΝΥΜΑΤΑ]		
12.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε:[ΠΑΡΑΧΩΡΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ]**	,786	,871
13.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε:[ΕΞΟΦΛΙΣΗ ΛΟΓΑΡΙΑΣΜΩΝ]**	,626	,710
14..	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε:[ΓΝΩΡΙΜΙΑ]**	,663	,748
15.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε:[ΑΠΕΙΛΕΣ]**	,622	,750
16.	**Σε περίπτωση που πέσετε θύμα ηλεκτρονικού εγκλήματος γνωρίζετε που θα απευθυνθείτε?**	,691	,576

Πίνακας 5.3: Αποτελέσματα παραγοντικής ανάλυσης ερωτήσεων με περιστροφή αξόνων.

5.3.2 Παραγοντική Ανάλυση Αξόνων

Αφού πραγματοποιήσαμε την ανάλυση των ερωτήσεων, στη συνέχεια θα αναλύσουμε τους άξονες που δημιουργήσαμε. Στον παρακάτω πίνακα ακολουθούν τα αποτελέσματα της συνολικής διακύμανσης του περιεχομένου που απαρτίζεται ο παράγοντας.

		Component Matrix a	**Rotated component Matrix** a
1.	**Χρήση Διαδικτύου**	,552	,848
2.	**Επικίνδυνες Καταστάσεις**	,879	,930
3.	**Γνώσεις σε σχέση με το διαδίκτυο**	,852	,747

Πίνακας 5.4: Αποτελέσματα παραγοντικής ανάλυσης αξόνων με περιστροφή αξόνων.

5.4 Ανάλυση αξιοπιστίας

Αξιοπιστία (Reliability), είναι ο συσχετισμός μιας μεταβλητής ενός παράγοντα με κάτι υποθετικό που μετρά αυτό που πρέπει να μετρηθεί. Ο δείκτης Cronbach alpha είναι ο πιο διαδεδομένος συντελεστής αξιοπιστίας ο οποίος αναφέρεται στο βαθμό όπου οι ερωτήσεις μετρούν τα ίδιο χαρακτηριστικό και εμφανίζουν μεγάλη συνοχή ή συσχέτιση είτε μεταξύ τους είτε με τι ίδιο το χαρακτηριστικό. Η τιμή του δείκτη αυξάνεται όταν αυξάνονται και οι μεταβλητές. Έτσι μ αυτόν τον τρόπο μπορούμε να καταφέρουμε ένα αποδεκτό επίπεδο του δείκτη. Όταν οι τιμές του δείκτη είναι μεγαλύτερες του 0,7 είναι ικανοποιητικές ενώ όταν είναι μικρότερες του 0.65 δεν είναι ικανοποιητικές.

Στον παρακάτω πίνακα βλέπουμε την εξήγηση των τιμών του δείκτη Cronbach's alpha για την εκτίμηση της αξιοπιστίας

ΠΙΝΑΚΑΣ ΑΞΙΟΛΟΓΗΣΗΣ CRONBACH'S ALPHA	
Τιμή του συντελεστή	**Αξιοπιστία**
<0,5	Μη αποδεκτή
0,5-0,59	Πτωχή
0,6-0,69	Αμφισβητήσιμη
0,7-0,79	Αποδεκτή
0,8-0,89	Καλή
0,9-0,94	Άριστη

Πίνακας 5.5: Πίνακας αξιολόγησης cronbach's alpha.

5.4.1 Ανάλυση Αξιοπιστίας Ερωτήσεων

Αρχικά έγινε η ανάλυση των ερωτήσεων και βρήκαμε τα παρακάτω αποτελέσματα του πίνακα με τις τιμές αξιοπιστίας που έχουμε αναλύσει. Με την μέθοδο αυτή μετράμε την εσωτερική σταθερότητα ενός τεστ.

Παρατηρούμε ότι η συνάφεια των ερωτήσεων είναι αποδεκτή σε λίγες περιπτώσεις. Στις περισσότερες είναι αμφισβητήσιμη. Αυτό μας οδηγεί στο αποτέλεσμα πως δεν έχουμε πλήρη αξιοπιστία ερωτηματολογίου καθώς και έρευνας.

	Ερωτήσεις	**Cronbach's alpha**
1.	**Πόσο καλά γνωρίζετε να χρησιμοποιείτε το διαδίκτυο?**	,712
2.	**Καταχωρείτε τα προσωπικά σας δεδομένα σε διάφορες σελίδες του διαδικτύου?**	,684
3.	**Πόσο καλά γνωρίζετε τους κινδύνους του διαδικτύου?**	,713
4.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ψυχαγωγία]**	,676
5.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[εργασία]**	,668

6.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[επικοινωνία]**	,696
7.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[chat rooms]**	,678
8.	**Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο?[ηλεκτρονικές συναλλαγές]**	,662
9.	**Θεωρείτε ασφαλείς τις ηλεκτρονικές συναλλαγές?**	,703
10.	**Έχετε πέσει ποτέ θύμα hacker στις σελίδες που χρησιμοποιείτε?**	,687
11.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [παραπλανητικά μηνύματα]**	,646
12.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [παραχώρηση προσωπικών δεδομένων]**	,653
13.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [εξόφληση λογαριασμών]**	,678
14.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [γνωριμία]**	,666
15.	**Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται: [απειλές]**	,691
16.	**Σε περίπτωση που πέσετε θύμα ηλεκτρονικού εγκλήματος γνωρίζετε που θα απευθυνθείτε?**	,724

Πίνακας 5.6: Αποτελέσματα ανάλυσης ερωτηματολογίου με το δείκτη cronbach's alpha.

5.4.2 Ανάλυση Αξιοπιστίας των Αξόνων

Στην συνέχεια , πραγματοποιήθηκε ανάλυση των παραγόντων με τον δείκτη cronbach's alpha και παρατηρούμε πως οι τιμές αξιοπιστίας δεν είναι αποδεκτές διότι για όλους τους παράγοντες οι τιμές του συντελεστή είναι <0,5. Αυτό πιθανόν οφείλεται στο φτωχό αριθμό μεταβλητών που αποτελείται ο κάθε παράγοντας.

	Ερωτήσεις	**Cronbach's alpha**
1.	**Χρήση Διαδικτύου**	-,434
2.	**Επικίνδυνες Καταστάσεις**	,438
3.	**Γνώσεις σε σχέση με το διαδίκτυο**	,186

Πίνακας 5.7: Αποτελέσματα ανάλυσης αξόνων με το δείκτη cronbach's alpha.

5.5 Ανάλυση διακύμανσης κατά ένα παράγοντα (One way ANOVA)

Η ανάλυση (One way ANOVA) είναι η μέθοδος που ανιχνεύει τις διαφορές ανάμεσα στους μέσους του πληθυσμού, με λίγα λόγια μας δείχνει εάν υπάρχει στατιστική διαφορά μεταξύ των ομάδων. Για να αποδειχθεί ότι υπάρχει στατιστική διαφορά των μέσων του πληθυσμού σε σχέση ενός ζεύγους μεταβλητών, η πιθανότητα του ελέγχου πρέπει να είναι μικρότερη (<0,05) δηλαδή (απόρριψη Ho). Αν η πιθανότητα είναι μεγαλύτερη (>0,05) τότε δεχόμαστε τη μηδενική υπόθεση για την ισότητα των μέσων του πληθυσμού.

Παρακάτω, αναλύουμε αν δημιουργείται σημαντική διαφορά των εξαρτημένων μεταβλητών, σε σχέση με τους τρείς ανεξάρτητους παράγοντες οι οποίοι είναι το φύλο, η ηλικία και το επίπεδο εκπαίδευσης.[10]

5.5.1 Φύλο

Ο παρακάτω πίνακας μας δείχνει την ανάλυση της διακύμανσης για το φύλο και τους παράγοντες.

Παράγοντας	**Τιμή F**	**Πιθανότητα**
1.Χρήση Διαδικτύου	2.055	,154
2.Επικίνδυνες Καταστάσεις	**6,142**	**,015**
3.Γνώσεις σε σχέση με το διαδίκτυο	,003	,959

Πίνακας 5.8: Αποτελέσματα διακύμανσης σε σχέση με το φύλο.

Τα αποτελέσματα μας δείχνουν ότι υπάρχει μικρή διαφορά στον τρόπο που αντιμετωπίζουν τον παράγοντα 2 οι γυναίκες και οι άντρες. Αυτό συμβαίνει διότι η τιμή της πιθανότητας είναι μεγαλύτερη του 5%. Για τους υπόλοιπους δύο παράγοντες δηλαδή για τον παράγοντα 1 και 3, οι απαντήσεις μεταξύ ανδρών και γυναικών, δεν διαφέρουν.

5.5.2 Ηλικία

Ο παρακάτω πίνακας μας φανερώνει την ανάλυση της διακύμανσης για την ηλικία και τους παράγοντες.

Παράγοντας	Τιμή F	Πιθανότητα
1.Χρήση Διαδικτύου	**7,387**	**,001**
2. Επικίνδυνες Καταστάσεις	**2.279**	**,107**
3.Γνώσεις σε σχέση με το διαδίκτυο	1,018	,364

Πίνακας 5.9: Αποτελέσματα διακύμανσης σε σχέση με την ηλικία.

Τα αποτελέσματα που έχουμε λάβει, μας φανερώνουν μεγάλη διαφορά στις απαντήσεις σχετικά με την ηλικία για τον παράγοντα 1. Οι απαντήσεις που δόθηκαν σχετικά με τη χρήση του διαδικτύου διαφέρουν ανάλογα με την ηλικία. Για τους παράγοντες 2 και 3 δεν βρέθηκε σημαντική στατιστική διαφορά.

5.5.3 Επίπεδο Εκπαίδευσης

Ο παρακάτω πίνακας μα δείχνει τα αποτελέσματα της ανάλυσης διακύμανσης, όσον αφορά το επίπεδο της εκπαίδευσης και τους παράγοντες.

Παράγοντας	Τιμή F	Πιθανότητα
1.Χρήση Διαδικτύου	1,120	,330
2.Επικίνδυνες Καταστάσεις	2,105	,126
3.Γνώσεις σε σχέση με το διαδίκτυο	**12,354**	**,000**

Πίνακας 5.10: Αποτελέσματα διακύμανσης σε σχέση με το επίπεδο εκπαίδευσης.

Τα αποτελέσματα που λάβαμε δείχνουν πως υπάρχει σημαντική διαφορά στο επίπεδο της εκπαίδευσης σχετικά με τον παράγοντα 3. Οι απαντήσεις που δόθηκαν είναι διαφορετικές στις κατηγορίες αυτές. Για τους παράγοντες 1 και 2 δεν βρέθηκε κάποια σημαντική διαφορά.[10]

6. Συμπεράσματα

Ολοκληρώνοντας, την έρευνα και αφού έχουμε ολοκληρώσει τα απαιτούμενα βήματα για να εξάγουμε τα αποτελέσματα προέκυψαν ορισμένα συμπεράσματα. Από τα αποτελέσματα που έχουμε λάβει στις απαντήσεις του ερωτηματολογίου μπορούμε να διακρίνουμε μια δυσαρέσκεια. Τα συμπεράσματα ολοκληρώθηκαν με την μέθοδο cronbach's alpha και one way Anova με την οποία διακρίνουμε τις διαφορές φύλου(γυναίκα, άντρας), ηλικία(<25, 25-35, >35), επίπεδο εκπαίδευσης(πρωτοβάθμια, δευτεροβάθμια, τριτοβάθμια).

Ας ξεκινήσουμε με την μεταβλητή φύλο. Παρατηρούμε ότι στους 3 παράγοντες που έχουμε δημιουργήσει μόνο στον παράγοντα 2 , δηλαδή στην περίπτωση εξαπάτησης οικονομικού εγκλήματος και στα μηνύματα που λαμβάνουνε (παραπλάνηση, παραχώρηση προσωπικών δεδομένων, εξόφληση λογαριασμών, γνωριμία, απειλές) σημειώνεται μία μικρή διαφορά. Από τα αποτελέσματα της έρευνας φαίνεται ότι οι γυναίκες έχουν λάβει περισσότερα μηνύματα με το περιεχόμενο που αναφέραμε παραπάνω απ ότι οι άντρες, σαφώς και έχουν πέσει θύματα εξαπάτησης οικονομικού εγκλήματος. Στον παράγοντα 1 και 3 δεν υπάρχουν σημαντικές διαφορές απαντήσεων.

Στη συνέχεια για τη μεταβλητή ηλικία βλέπουμε πως υπάρχει διαφορά απόψεων στον παράγοντα 1 ανάλογα με την ηλικία τους μικρότερη των 25, 25-35, και μεγαλύτερη των 25. Πιο συγκεκριμένα, από την ανάλυση του δείγματος οδηγηθήκαμε στα εξής αποτελέσματα: τα άτομα ηλικίας <25 χρησιμοποιούνε το διαδίκτυο περισσότερο για γνωριμία και ηλεκτρονικές συναλλαγές. Από αυτό καταλαβαίνουμε πως είναι πιο εύκολο αυτή η ηλικιακή ομάδα ανθρώπων να βρεθούν σε κάποια επικίνδυνη κατάσταση του σκοτεινού διαδικτύου απ' ότι οι υπόλοιπες δύο ομάδες που το χρησιμοποιούνε για εργασία επικοινωνία και ψυχαγωγία.

Τέλος, στα αποτελέσματα της μεταβλητής του επιπέδου εκπαίδευσης παρατηρούμε σημαντική διαφορά στον παράγοντα 3 που αποτελείται γενικά από τις γνώσεις σχετικά με το διαδίκτυο και ειδικότερα από το πόσο καλά γνωρίζουν τους κινδύνους του διαδικτύου, πόσο καλά γνωρίζουν να χρησιμοποιούνε το διαδίκτυο και αν πέσουν θύμα ηλεκτρονικού εγκλήματος αν γνωρίζουν που θα απευθυνθούνε. Με βάση τα αποτελέσματα της έρευνας, είναι φανερό πως το επίπεδο της εκπαίδευσης των ανθρώπων συμβάλλει αρκετά στο πόσο εύκολο είναι κανείς να βρεθεί σε δύσκολη κατάσταση. Οι απόφοιτοι της πρωτοβάθμιας εκπαίδευσης λόγω το ότι δεν γνωρίζουν να χρησιμοποιούνε καλά το διαδίκτυο, τους κινδύνους του και αν σε περίπτωση βρεθούνε σε μια τέτοια κατάσταση δεν ξέρουν που θα απευθυνθούνε είναι πιο εύκολο να πέσουν θύματα ηλεκτρονικού εγκλήματος. Στην συγκεκριμένη έρευνα οι περισσότεροι έχουν μια μέτρια έως καλή γνώση σχετικά με την χρήση του διαδικτύου. Όσον αφορά τους παράγοντες 1 και 2 δεν υπάρχει διαφορά των απαντήσεων που έχουν δοθεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Κ. Βλαχόπουλος , *ηλεκτρονικό έγκλημα μορφές πρόληψη αντιμετώπιση*, νομική βιβλιοθήκη, 2007
2. R. Mansfield, *Οι Χάκερ Επιτίθενται*, 1η Αμερικανική Έκδοση, 2000
3. J Scambray, S.McClure, G Kurtz., *χάκερ επίθεση και άμυνα*, 2η Αμερικανική Έκδοση,2001,
4. Ν.Αλεξανδρής, Ε.Κιουντούζης, Β.Τραπεζάνογλου, *ασφάλεια πληροφοριών τεχνικά, νομικά και κοινωνικά θέματα*, 1995
5. Η.Θεοδώρου -Αποστολοπούλου, *στατιστική επιχειρήσεων περιγραφική και επαγωγική στατιστική,*1991
6. Ν.Τσάντας, Χ.Μωυσιάδης, Ν.Μπαγιάτης, Θ.Χατζηπαντελής, *ανάλυση δεδομένων με τη βοήθεια στατιστικών πακέτων*, εκδόσεις ζητη,1999
7. Ν.ΚΥΡΙΑΖΗ, *Η κοινωνιολογική έρευνα*, 5η έκδοση, ελληνικά γράμματα,2002
8. Ι.Αποστολάκης, Α. Καστανιά, *Λήψη αποφάσεων με το SPSS/PC*", εκδόσεις Α. Σταμούλης,1994
9. K. Tsianou, M.G. Tsipouras, N. Giannakeas, A. Skamnelos, K.H. Katsanos, A. Tatsioni, E.C. Karvounis, V. Tsianos, A.T. Tzallas, E.V. Tsianos and J. Vlcek, "Beliefs about Medicines Questionnaire (BMQ) for inflammatory bowel disease patients in Greece. Is it useful?", European Journal of Person Centered Healthcare,2016
10. K. Tsianou, N. Giannakeas, M.G. Tsipouras, A. T. Tzallas, A. Skamnelos, J. Bureš, J. Vlchek and E.V. Tsianos, "Accessing patient views about medication in chronic conditions using the Beliefs about Medicine Questionnaire (BMQ): A review study", J Drug Res Dev,2017

ΙΣΤΟΣΕΛΙΔΕΣ

11. Γ.Κούρος, "Ορισμός ηλεκτρονικού εγκλήματος,"[Online]. Διαθέσιμο: http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414 [Ανακτήθηκε: Μάιος,28,2018].
12. "Χαρακτηριστικά ηλεκτρονικού εγκλήματος," [Online]. Διαθέσιμο: https://sites.google.com/site/elektronikoenklema2012/charakteristika-tou-elektronikou [Ανακτήθηκε: Μάιος,28,2018]
13. Μ.-Π. Κάτρη, "Κακόβουλες εισβολές σε δίκτυα," [Online]. Διαθέσιμο: http://katrimaria.gr/?p=436 [Ανακτήθηκε: Μάιος,28,2018].
14. "Ιοί," [Online]. Διαθέσιμο: https://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE [Ανακτήθηκε: Μάιος,28,2018].
15. Σ.Προβατά,"Η έννοια του πορνογραφικού υλικού" , [Online]. Διαθέσιμο: http://www.provataslaw.gr/%CE%B7-%CE%AD%CE%BD%CE%BD%CE%BF%CE%B9%CE%B1-%CF%84%CE%BF%CF%85-

%CF%80%CE%BF%CF%81%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%B9%CE%BA%CE%BF%CF%8D-%CF%85%CE%BB%CE%B9%CE%BA%CE%BF%CF%8D [Ανακτήθηκε: Μάιος,28,2018].

16. " Ιστορική αναδρομή εγκλήματος," [Online]. Διαθέσιμο: https://newtech-pub.com/wp-content/uploads/2013/10/kef-asf.plhr_.pdf [Ανακτήθηκε: Μάιος,28,2018].
17. "Phishing and pharming," [Online]. Διαθέσιμο: https://www.scribd.com/document/376085175/Phishing-and-Pharming [Ανακτήθηκε: Μάιος,28,2018].
18. "Πειρατεία λογισμικού," [Online]. Διαθέσιμο: http://sapounatzanetos.blogspot.com/2012/02/h.html [Ανακτήθηκε: Μάιος,28,2018].
19. Α.Μόσχου," Trafficking", [Online]. Διαθέσιμο: https://frapress.gr/2016/12/trafficking-mia-morfi-doulias-tou-21ou-eona/ [Ανακτήθηκε: Μάιος,28,2018].
20. "Τι είναι το trafficking," [Online]. Διαθέσιμο: https://stoptrafficking.gr/el/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-trafficking [Ανακτήθηκε: Μάιος,28,2018].
21. "Μέθοδος κατάρτισης ερωτηματολογίου," [Online]. Διαθέσιμο: http://eclass.teiion.gr/modules/document/file.php/DSE274/2.%20%CE%9C%CE%AD%CE%B8%CE%BF%CE%B4%CE%BF%CF%82%20%CE%BA%CE%B1%CF%84%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7%CF%82%20%CE%B5%CF%81%CF%89%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%BF%CF%85.doc [Ανακτήθηκε: Μάιος,28,2018].
22. "Πορνογραφικό υλικό," [Online]. Διαθέσιμο: http://www.provataslaw.gr/%CE%B7-%CE%AD%CE%BD%CE%BD%CE%BF%CE%B9%CE%B1-%CF%84%CE%BF%CF%85-%CF%80%CE%BF%CF%81%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%B9%CE%BA%CE%BF%CF%8D-%CF%85%CE%BB%CE%B9%CE%BA%CE%BF%CF%8D [Ανακτήθηκε: Μάιος,28,2018].
23. Α.Μπαλτζής*," παραγοντική ανάλυση*," [Online]. Διαθέσιμο: http://users.auth.gr/baltzis [Ανακτήθηκε: Μάιος,30,2018].

ΠΑΡΑΡΤΗΜΑ

Ηλεκτρονικό έγκλημα στα μέσα κοινωνικής δικτύωσης

Το ερωτηματολόγιο που έχετε στα χέρια σας, έχει συνταχθεί στα πλαίσια της πτυχιακής μου εργασίας στο τμήμα "Μηχανικών Πληροφορικής" και έχει σκοπό να ερευνήσει τις γνώσεις των ανθρώπων στους υπολογιστές και συγκεκριμένα στο ηλεκτρονικό έγκλημα. Παρακαλώ απαντήστε με ειλικρίνεια. Η έρευνα είναι ανώνυμη.

Ευχαριστώ για το χρόνο σας.

Φύλο *

- Γυναίκα
- άντρας

Ηλικία *

- <25
- 25 έως 35
- >35

Ποιο είναι το επίπεδο της εκπαίδευσής σας? *

- πρωτοβάθμια
- δευτεροβάθμια
- τριτοβάθμια

Πόσο καλά γνωρίζετε να χρησιμοποιείτε το διαδίκτυο? *

1 2 3 4 5

Καταχωρείτε τα προσωπικά σας δεδομένα σε διάφορες σελίδες του διαδικτύου? *

1 2 3 4 5

Πόσο καλά γνωρίζετε τους κινδύνους του διαδικτύου? *

1 2 3 4 5

Πόσες ώρες αφιερώνετε καθημερινά στο διαδίκτυο? *

- 1 έως 3
- 3 έως 5
- >5

Για πιο λόγο συνήθως χρησιμοποιείτε το διαδίκτυο? *

	Καθόλου	ελάχιστα	αρκετά	πολύ	πάρα πολύ
ψυχαγωγία					
εργασία					
επικοινωνία					
chat rooms					
ηλεκτρονικές συναλλαγές					

Έχετε λογαριασμούς σε σελίδες κοινωνικής δικτύωσης? *

- ναι
- όχι

Έχετε πέσει θύμα hacker στις σελίδες που χρησιμοποιείτε? *

1 2 3 4 5

Θεωρείτε ασφαλείς τις ηλεκτρονικές συναλλαγές? *

1 2 3 4 5

Έχετε πέσει ποτέ θύμα εξαπάτησης οικονομικού εγκλήματος μέσω διαδικτύου? *

- ναι
- όχι

Έχετε λάβει ποτέ μηνύματα στο κινητό τηλέφωνο ή τον ηλεκτρονικό υπολογιστή τα οποία αναφέρονται σε: *

	Ποτέ	σπάνια	συχνά	αρκετές φορές	πολλές φορές
παραπλανητικά μηνύματα					
παραχώρηση προσωπικών δεδομένων					
εξόφληση λογαριασμών					
γνωριμία					
απειλές					

Έχετε υποστεί κάποια εγκληματική πράξη εσείς η κάποιος δικός σας άνθρωπος? *

- ναι
- όχι

Γνωρίζετε την έννοια του "Trafficking"? *

- ναι
- όχι

Αν απαντήσατε ναι στην προηγούμενη ερώτηση απαντήστε σε αυτή. Τι κατά την γνώμη σας ευθύνεται για την έξαρση του φαινομένου "trafficking" τα τελευταία χρόνια?

- οικονομική κρίση
- αρχές
- κοινωνία

Σε περίπτωση που πέσετε θύμα ηλεκτρονικού εγκλήματος γνωρίζετε που θα απευθυνθείτε? *

1 2 3 4 5