ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Μεταπτυχιακή Διπλωματική Εργασία με θέμα:

Διαδικτυακό έγκλημα: Επίπεδο ενημέρωσης του κοινού, πρόληψη και αντιμετώπισή του.

Χριστίνα Γ. Θωμοπούλου

Επιβλέπων: Νικόλαος Φαρμάκης

Αναπληρωτής Καθηγητής Α.Π.Θ.

Θεσσαλονίκη, Σεπτέμβριος 2015

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Μεταπτυχιακή Διπλωματική Εργασία με θέμα:

Διαδικτυακό έγκλημα: Επίπεδο ενημέρωσης του κοινού, πρόληψη και αντιμετώπισή του.

Χριστίνα Γ. Θωμοπούλου

Εγκρίθηκε από την Τριμελή Εξεταστική Επιτροπή την……. 2015:

(*Υπογραφή*)	(*Υπογραφή*)	(*Υπογραφή*)
……..	……..	……..
Φαρμάκης Ν.	Αντωνίου Ι.	Μπράτσας Χ.
Αναπλ. Καθηγητής Α.Π.Θ.	Καθηγητής Α.Π.Θ.	ΕΔΙΠ Α.Π.Θ.

Θεσσαλονίκη, Σεπτέμβριος 2015

(Υπογραφή)

…….

Copyright © Χριστίνα Θωμοπούλου, 2015
Πτυχιούχος Μαθηματικός Α.Π.Θ.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.
Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης.

Στην οικογένειά μου

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον Αναπληρωτή Καθηγητή κ. Φαρμάκη Νικόλαο που ανέλαβε την επίβλεψη της παρούσας εργασίας, για την εμπιστοσύνη που έδειξε στο πρόσωπό μου, για την συνεργασία του και τις πολύτιμες συμβουλές του καθ' όλη τη διάρκεια της εκπόνησης της παρούσας διπλωματικής εργασίας.

Οφείλω επίσης, να ευχαριστήσω όλα τα άτομα που πήραν μέρος στην έρευνα, διότι χωρίς αυτούς θα ήταν αδύνατη η διεξαγωγή αυτής της έρευνας.

Θα ήθελα τέλος, να ευχαριστήσω από τα βάθη της καρδιάς μου την οικογένειά μου για την συμπαράσταση, την ενθάρρυνση και την πολύπλευρη στήριξή τους κατά την διάρκεια των σπουδών μου.

ΠΕΡΙΛΗΨΗ

Το διαδίκτυο στις μέρες μας γνωρίζει μεγάλη άνθηση. Αναπτύχθηκε και συνεχίζει να αναπτύσσεται με πρωτοφανή ταχύτητα τόσο ως προς τον αριθμό των δικτύων και των χρηστών, όσο και ως προς το μεγάλο φάσμα των εφαρμογών του. Πέρα όμως από την πληθώρα των πλεονεκτημάτων του έχει επιφέρει και μια σειρά από εγκλήματα τα οποία οριοθετούνται από δυο βασικά στοιχεία: τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο. Τα διαδικτυακά εγκλήματα με τις διάφορες μορφές τους προκαλούν τεράστιες ζημιές και κινδύνους τόσο στα υπολογιστικά συστήματα όσο και στα προσωπικά δεδομένα. Γι' αυτό το λόγο, η ενημέρωση του κοινού είναι ο σημαντικότερος παράγοντας έτσι ώστε να γνωρίζουν τους κινδύνους που τους απειλούν και να λαμβάνουν τα κατάλληλα μέτρα προστασίας απέναντι στο διαδικτυακό έγκλημα. Ωστόσο, εκτός από την ενημέρωση του κοινού υπάρχουν και άλλοι παράγοντες οι οποίοι είναι απαραίτητοι για την εξάλειψη αυτού του φαινομένου. Η εργασία στηρίχτηκε σε δειγματοληπτική έρευνα με ερωτηματολόγια η οποία πραγματοποιήθηκε ηλεκτρονικά σε Έλληνες χρήστες του διαδικτύου όλων των ηλικιών. Βασικός στόχος της παρούσας έρευνας είναι πρώτον, να αποτυπώσουμε τις απόψεις των χρηστών του διαδικτύου όσον αφορά την ενημέρωσή τους σχετικά με τους κινδύνους των διαφόρων μορφών του διαδικτυακού εγκλήματος και δεύτερον, να διαπιστώσουμε αν τόσο ο χρήστης κάθε ηλικίας όσο και οι γονείς λαμβάνουν μέτρα για να προστατευτούν από τη σύγχρονη αυτή μορφή εγκληματικότητας εφόσον, η αποτελεσματικότερη αντιμετώπιση του προβλήματος είναι η ίδια η πρόληψή του. Από την έρευνα αυτή συνάγονται ουσιαστικά συμπεράσματα για το φαινόμενο του διαδικτυακού εγκλήματος.

Λέξεις Κλειδιά: Διαδίκτυο, έγκλημα, διαδικτυακό έγκλημα, πρόληψη, αντιμετώπιση, δειγματοληπτική έρευνα

ABSTRACT

Nowadays Internet usage is booming. The internet developed and continues to grow at an unprecedented speed in regard to the number of networks and users, as well as to the wide range of its applications. Despite its many advantages it has given birth to a series of crimes which are defined by two basic elements: computers and the internet. Online crimes of various forms cause enormous damages and hide many dangers to both computer systems and to personal data. For this reason, public awareness is an important factor, as the users must learn of the potential dangers that lurk and take appropriate protective measures against online crime. Informing the public of potential danger does not eliminate online crime; there are many factors that are necessary in order to reduce it. This work was based on a sample survey with questionnaires carried out electronically on Greek Internet users of all ages. The main objective of this research is to firstly capture the opinions of internet users and inform them about various forms of Internet crime, and secondly to see if users of all ages and especially parents take steps to protect themselves and their children against modern type of criminality as the most effective treatment of the problem is prevention. The survey reached significant conclusions about the phenomenon of Internet crime.

Keywords: Internet, Crime, Internet crime, prevention, treatment, survey

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΧΑΡΙΣΤΙΕΣ……7

ΠΕΡΙΛΗΨΗ……...9

ABSTRACT……11

ΠΕΡΙΕΧΟΜΕΝΑ…….....13

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ…….....15

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ……..17

ΕΙΣΑΓΩΓΗ…….……21

ΚΕΦΑΛΑΙΟ 1ο

1.1 Ορισμός του Διαδικτύου…….....23

1.2 Ορισμός του εγκλήματος…….……..23

1.3 Ποια είναι η έννοια του Διαδικτυακού εγκλήματος……..24

ΚΕΦΑΛΑΙΟ 2ο

ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ – ΠΡΟΛΗΨΗ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

2.1 Διαδικτυακά εγκλήματα……25

2.1.1 Phishing και Pharming (Ηλεκτρονικό ψάρεμα)……...25

2.1.2 Spamming (Ανεπιθύμητη αλληλογραφία)……...26

2.1.3 Απάτες μέσω διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.)…….27

2.1.4 Παιδική πορνογραφία……..29

2.1.5 Cracking και Hacking……..31

2.1.6 Διακίνηση-Πειρατεία λογισμικού……32

2.1.7 Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων……..32

2.1.8 Cyberbullying (Διαδικτυακός εκφοβισμός)……33

2.1.9 Κακόβουλο λογισμικό (Ιοί, σκουλήκια, δούρειοι ίπποι)……34

2.1.10 Διαδικτυακή τρομοκρατία……..35

2.2 Μέτρα πρόληψης και αντιμετώπισης του Διαδικτυακού εγκλήματος……...36

ΚΕΦΑΛΑΙΟ 3ο

Η ΕΡΕΥΝΑ ΚΑΙ Η ΣΤΑΤΙΣΤΙΚΗ ΑΝΑΛΥΣΗ

3.1 Δειγματοληπτική έρευνα: Πως πραγματοποιήθηκε ……..39

3.2 Παρουσίαση αποτελεσμάτων δειγματοληπτικής έρευνας…….39

ΚΕΦΑΛΑΙΟ 4ο

ΕΛΕΓΧΟΣ ΑΝΕΞΑΡΤΗΣΙΑΣ

4.1 Πίνακες Συνάφειας και Έλεγχος Υποθέσεων…….67

4.2 Παρουσίαση αποτελεσμάτων από την δοκιμασία X^2 ……..……..68

ΚΕΦΑΛΑΙΟ 5ο

5.1 Μελέτη Κατανομών……...99

5.1.1 Συνάρτηση πυκνότητας πιθανότητας της συμμετρικής κατανομής……99

5.1.2 Συνάρτηση πυκνότητας πιθανότητας της φθίνουσας κατανομής……..100

5.1.3 Συνάρτηση πυκνότητας πιθανότητας της αύξουσας κατανομής……...100

5.2 Παρουσίαση αποτελεσμάτων……..101

ΣΥΜΠΕΡΑΣΜΑΤΑ…….119

ΠΑΡΑΡΤΗΜΑ……..121

ΒΙΒΛΙΟΓΡΑΦΙΑ……..129

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 3.1: *Ερώτηση 1*……...40

Πίνακας 3.2: *Ερώτηση 2*……...41

Πίνακας 3.3: *Ερώτηση 3*……...42

Πίνακας 3.4: *Ερώτηση 4*……...43

Πίνακας 3.5: *Ερώτηση 5*……...43

Πίνακας 3.6: *Ερώτηση 6*……...44

Πίνακας 3.7: *Ερώτηση 7(Phishing και Pharming)*……..46

Πίνακας 3.8: *Ερώτηση 7(Spamming)*……...47

Πίνακας 3.9: *Ερώτηση 7(Απάτες μέσω Διαδικτύου)*……47

Πίνακας 3.10: *Ερώτηση 7(Παιδική πορνογραφία)*……...48

Πίνακας 3.11: *Ερώτηση 7(Cracking και Hacking)*……..49

Πίνακας 3.12: *Ερώτηση 7(Διακίνηση-Πειρατεία λογισμικού)*……..50

Πίνακας 3.13: *Ερώτηση 7(Διακίνηση ναρκωτικών)*……51

Πίνακας 3.14: *Ερώτηση 7(Cyberbullying)*……...52

Πίνακας 3.15: *Ερώτηση 7(Κακόβουλο λογισμικό)*……...53

Πίνακας 3.16: *Ερώτηση 7(Διαδικτυακή τρομοκρατία)*……54

Πίνακας 3.17: *Ερώτηση 8*……55

Πίνακας 3.18: *Ερώτηση 9*……57

Πίνακας 3.19: *Ερώτηση 10*……...57

Πίνακας 3.20: *Ερώτηση 11*……...58

Πίνακας 3.21: *Ερώτηση 12*……...59

Πίνακας 3.22: *Ερώτηση 13*……...60

Πίνακας 3.23: *Ερώτηση 14*……...61

Πίνακας 3.24: *Ερώτηση 15*……...62

Πίνακας 3.25: *Ερώτηση 16*……...63

Πίνακας 3.26: *Ερώτηση 17*……...64

Πίνακας 4.1: *Πίνακας Συνάφειας Συσχέτισης Φύλο-Phishing και Pharming*…….69

Πίνακας 4.2: *Πίνακας Συνάφειας Συσχέτισης Ηλικία-Phishing και Pharming*……...85

Πίνακας 4.3: *Συγκεντρωτικός πίνακας συσχετίσεων*……96

Πίνακας 5.1: *Δεδομένα του δείγματος (Phishing και Pharming-Άνδρας)*……..101

Πίνακας 5.2: *Δεδομένα του δείγματος (Phishing και Pharming-Γυναίκα)*…….102

Πίνακας 5.3: *Δεδομένα του δείγματος (Spamming-Άνδρας)*……..104

Πίνακας 5.4: *Δεδομένα του δείγματος (Spamming-Γυναίκα)*…….105

Πίνακας 5.5: *Δεδομένα του δείγματος (Απάτες μέσω Διαδικτύου-Γυναίκα)*……...106

Πίνακας 5.6: *Δεδομένα του δείγματος (Παιδική πορνογραφία-Άνδρας)*…….107

Πίνακας 5.7: *Δεδομένα του δείγματος (Παιδική πορνογραφία-Γυναίκα)*……...108

Πίνακας 5.8: *Δεδομένα του δείγματος (Διακίνηση / Πειρατεία λογισμικού-Άνδρας)*……..110

Πίνακας 5.9: *Δεδομένα του δείγματος (Διακίνηση / Πειρατεία λογισμικού -Γυναίκα)*……...111

Πίνακας 5.10: *Δεδομένα του δείγματος (Cyberbullying-Άνδρας)*……..112

Πίνακας 5.11: *Δεδομένα του δείγματος (Κακόβουλο λογισμικό-Άνδρας)*……..113

Πίνακας 5.12: *Δεδομένα του δείγματος (Κακόβουλο λογισμικό-Γυναίκα)*…….114

Πίνακας 5.13: *Δεδομένα του δείγματος (Διαδικτυακή τρομοκρατία-Γυναίκα)*……...116

Πίνακας 5.14: *Συγκεντρωτικός πίνακας κατανομών*……..117

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

Διάγραμμα 3.1: *Ερώτηση 1*……..40

Διάγραμμα 3.2: *Ερώτηση 2*……..41

Διάγραμμα 3.3: *Ερώτηση 3*……..42

Διάγραμμα 3.4: *Ερώτηση 4*……..43

Διάγραμμα 3.5: *Ερώτηση 5*……..44

Διάγραμμα 3.6: *Ερώτηση 6*……..45

Διάγραμμα 3.7: *Ερώτηση 7(Phishing και Pharming)*……46

Διάγραμμα 3.8: *Ερώτηση 7(Spamming)*……..47

Διάγραμμα 3.9: *Ερώτηση 7(Απάτες μέσω Διαδικτύου)*……48

Διάγραμμα 3.10: *Ερώτηση 7(Παιδική πορνογραφία)*……...49

Διάγραμμα 3.11: *Ερώτηση 7(Cracking και Hacking)*……..50

Διάγραμμα 3.12: *Ερώτηση 7(Διακίνηση-Πειρατεία λογισμικού)*……51

Διάγραμμα 3.13: *Ερώτηση 7(Διακίνηση ναρκωτικών)*……52

Διάγραμμα 3.14: *Ερώτηση 7(Cyberbullying)*……..53

Διάγραμμα 3.15: *Ερώτηση 7(Κακόβουλο λογισμικό)*……..54

Διάγραμμα 3.16: *Ερώτηση 7(Διαδικτυακή τρομοκρατία)*……55

Διάγραμμα 3.17: *Ερώτηση 8*……56

Διάγραμμα 3.18: *Ερώτηση 9*……57

Διάγραμμα 3.19: *Ερώτηση 10*……..58

Διάγραμμα 3.20: *Ερώτηση 11*……..59

Διάγραμμα 3.21: *Ερώτηση 12*……..60

Διάγραμμα 3.22: *Ερώτηση 13*……..61

Διάγραμμα 3.23: *Ερώτηση 14*……..62

Διάγραμμα 3.24: *Ερώτηση 15 και Ερώτηση 16*……...63

Διάγραμμα 3.25: *Ερώτηση 17*……..64

Διάγραμμα 3.26: *Ερώτηση 18*……..65

Διάγραμμα 3.27: *Ερώτηση 19*……..65

Διάγραμμα 3.28: *Ερώτηση 20*……..66

Διάγραμμα 4.1: *Ποσοστιαία κατανομή: Φύλο-Phishing και Pharming*……..70

Διάγραμμα 4.2: *Ποσοστιαία κατανομή: Φύλο-Spamming*……...71

Διάγραμμα 4.3: *Ποσοστιαία κατανομή: Φύλο-Απάτες μέσω Διαδικτύου*……72

Διάγραμμα 4.4: *Ποσοστιαία κατανομή: Φύλο-Παιδική πορνογραφία*……73

Διάγραμμα 4.5: *Ποσοστιαία κατανομή: Φύλο-Cracking και Hacking*……74

Διάγραμμα 4.6: *Ποσοστιαία κατανομή: Φύλο-Διακίνηση/Πειρατεία λογισμικού*……75

Διάγραμμα 4.7: *Ποσοστιαία κατανομή: Φύλο-Διακίνηση ναρκωτικών*……...76

Διάγραμμα 4.8: *Ποσοστιαία κατανομή: Φύλο-Cyberbullying*……77

Διάγραμμα 4.9: *Ποσοστιαία κατανομή: Φύλο-Κακόβουλο λογισμικό*……78

Διάγραμμα 4.10: *Ποσοστιαία κατανομή: Φύλο-Διαδικτυακή τρομοκρατία*……79

Διάγραμμα 4.11: *Ποσοστιαία κατανομή: Φύλο-Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακού εγκλήματος;*……80

Διάγραμμα 4.12: *Ποσοστιαία κατανομή: Φύλο-Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος;*……...81

Διάγραμμα 4.13: *Ποσοστιαία κατανομή: Φύλο-Κατά την πλοήγησή σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις;*……...82

Διάγραμμα 4.14: *Ποσοστιαία κατανομή: Φύλο-Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο;*……..83

Διάγραμμα 4.15: *Ποσοστιαία κατανομή: Φύλο-Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα;*……84

Διάγραμμα 5.1: *Συχνότητες παρατηρήσεων ανά κλάση (Phishing και Pharming-Άνδρας)*...102

Διάγραμμα 5.2: *Συχνότητες παρατηρήσεων ανά κλάση (Phishing και Pharming-Γυναίκα)*..103

Διάγραμμα 5.3: *Συχνότητες παρατηρήσεων ανά κλάση (Spamming-Άνδρας)*……...104

Διάγραμμα 5.4: *Συχνότητες παρατηρήσεων ανά κλάση (Spamming-Γυναίκα)*……..106

Διάγραμμα 5.5: *Συχνότητες παρατηρήσεων ανά κλάση (Απάτες μέσω Διαδικτύου-Γυναίκα)*107

Διάγραμμα 5.6: *Συχνότητες παρατηρήσεων ανά κλάση (Παιδική πορνογραφία-Άνδρας)*…..108

Διάγραμμα 5.7: *Συχνότητες παρατηρήσεων ανά κλάση (Παιδική πορνογραφία-Γυναίκα)*....109

Διάγραμμα 5.8: *Συχνότητες παρατηρήσεων ανά κλάση (Διακίνηση/ Πειρατεία λογισμικού-Άνδρας)*……110

Διάγραμμα 5.9: *Συχνότητες παρατηρήσεων ανά κλάση (Διακίνηση/ Πειρατεία λογισμικού-Γυναίκα)*……..111

Διάγραμμα 5.10: *Συχνότητες παρατηρήσεων ανά κλάση (Cyberbullying-Άνδρας)*……113

Διάγραμμα 5.11: *Συχνότητες παρατηρήσεων ανά κλάση (Κακόβουλο λογισμικό-Άνδρας)*...114

Διάγραμμα 5.12: *Συχνότητες παρατηρήσεων ανά κλάση (Κακόβουλο λογισμικό-Γυναίκα)*...115

Διάγραμμα 5.13: *Συχνότητες παρατηρήσεων ανά κλάση (Διαδικτυακή τρομοκρατία-Γυναίκα)*……..116

ΕΙΣΑΓΩΓΗ

Το ραγδαίως αναπτυσσόμενο φαινόμενο του διαδικτυακού εγκλήματος και οι μορφές με τις οποίες εμφανίζεται επηρεάζουν τόσο το χρήστη όσο και το ίδιο το διαδίκτυο. Είναι ένα μεγάλο και σοβαρό πρόβλημα που έχει λάβει ανεξέλεγκτες διαστάσεις τα τελευταία χρόνια με σκοπό τη θυματοποίηση και εκμετάλλευση πολιτών, επιχειρήσεων ακόμη και κυβερνητικών υπηρεσιών. Κίνητρο για την συγκεκριμένη εργασία αποτέλεσε ο τεράστιος αριθμός των εγκλημάτων και των αντικοινωνικών συμπεριφορών που διαπράττονται μέσω διαδικτύου στις μέρες μας. Η μελέτη που παρουσιάζεται στη συνέχεια αποτελείται από δυο μέρη. Το πρώτο μέρος περιλαμβάνει τη θεωρητική προσέγγιση του θέματος ενώ το δεύτερο μέρος την πρακτική προσέγγιση, δηλαδή την έρευνα.

Στο πρώτο κεφάλαιο παρουσιάζονται στην αρχή οι έννοιες του διαδικτύου και του εγκλήματος και στην συνέχεια ο ορισμός του φαινομένου που δημιουργούν οι δυο αυτές έννοιες, δηλαδή του διαδικτυακού εγκλήματος.

Στη συνέχεια της θεωρητικής προσέγγισης ακολουθεί το δεύτερο κεφάλαιο. Στο συγκεκριμένο κεφάλαιο περιγράφονται αναλυτικά οι κύριες μορφές του διαδικτυακού εγκλήματος καθώς και τα μέτρα πρόληψης και αντιμετώπισης που πρέπει να ληφθούν ώστε οι χρήστες να αποφεύγουν να γίνονται θύματα αυτής της νέας μορφής εγκληματικότητας.

Το πρακτικό μέρος της εργασίας παρουσιάζεται στα τρία τελευταία κεφάλαια. Συγκεκριμένα, στο τρίτο κεφάλαιο παρουσιάζεται όλη η μεθοδολογία της δειγματοληπτικής έρευνας. Παραθέτονται η διαδικασία πραγματοποίησης της έρευνας καθώς και η στατιστική ανάλυση των δεδομένων. Το ερωτηματολόγιο που χρησιμοποιήθηκε για την έρευνα περιλαμβάνει ερωτήσεις σχετικά με τα δημογραφικά χαρακτηριστικά, την ενημέρωση των χρηστών όσον αφορά την κάθε μορφή διαδικτυακού εγκλήματος, τα μέτρα πρόληψης και αντιμετώπισης αυτού του φαινομένου, ερωτήσεις που αφορούν την ασφάλεια που αισθάνονται κατά την πλοήγησή τους στο διαδίκτυο καθώς και ερωτήσεις σχετικά με την πιο συχνή μορφή διαδικτυακού εγκλήματος και το ποσοστό των Ελλήνων που έχουν πέσει θύμα αυτής της μορφής εγκληματικότητας.

Στο τέταρτο κεφάλαιο παρουσιάζονται αναλυτικά ορισμένοι πίνακες συνάφειας όπως επίσης και η ανάλυση συσχετίσεων διαφόρων παραμέτρων του προβλήματος ώστε να έχουμε καλύτερη εικόνα αιτίου – αιτιατού.

Στο πέμπτο κεφάλαιο και τελευταίο κομμάτι του πρακτικού μέρους μελετούμε κατανομές συνεχών μεταβλητών που περιγράφονται από συμμετρική, αύξουσα και φθίνουσα συνάρτηση πυκνότητας πιθανότητας. Και στη συνέχεια πραγματοποιούμε έλεγχο καλής προσαρμογής X^2 για τα δεδομένα του δείγματος.

Στο τέλος της εργασίας παραθέτουμε τα κύρια συμπεράσματα που προέκυψαν, το παράρτημα το οποίο αποτελείται από το ερωτηματολόγιο που χρησιμοποιήσαμε για την έρευνα καθώς και την βιβλιογραφία μαζί με τις ηλεκτρονικές πηγές.

ΚΕΦΑΛΑΙΟ 1ο

1.1 Ορισμός του Διαδικτύου

Το Διαδίκτυο το οποίο προέρχεται από τις λέξεις Διασύνδεση Δικτύων είναι ένα παγκόσμιο δίκτυο συνδεδεμένων υπολογιστών που χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο, δηλαδή κοινούς κανόνες επικοινωνίας. Αποτέλεσμα αυτής της σύνδεσης είναι η δυνατότητα που δίνει στον χρήστη για αναζήτηση πληροφοριών, για επικοινωνία, για αγορές και για ψυχαγωγία. Η χρήση του διαδικτύου μπορεί να έχει ακαδημαϊκό, δημόσιο, ιδιωτικό, επιχειρηματικό ή κυβερνητικό χαρακτήρα.

Το Διαδίκτυο έκανε τα πρώτα του βήματα τη δεκαετία του ΄60, όταν η κυβέρνηση των Ηνωμένων Πολιτειών Αμερικής ανέθεσε σε ερευνητές του στρατού το καθήκον της δημιουργίας ενός αποκεντρωμένου επικοινωνιακού δικτύου το οποίο θα μπορούσε να επιβιώσει σε οποιαδήποτε επίθεση, δηλαδή η επικοινωνία ανάμεσα στους κόμβους να μην σταματούσε μετά από κάποια επίθεση. Κανείς όμως τότε δεν μπορούσε να φανταστεί την τεχνολογική εξέλιξη και την επίδρασή του 50 χρόνια μετά. Το διαδίκτυο έχει συμβάλει στη διαμόρφωση του φαινομένου της παγκοσμιοποίησης όπου τα σύνορα έχουν καταργηθεί, οι αποστάσεις έχουν εκμηδενιστεί και ο χρόνος έχει λάβει μια εντελώς διαφορετική διάσταση. Παρέχει στους χρήστες νέες και ασύλληπτες δυνατότητες, είτε ως μέσα επικοινωνίας, ψυχαγωγίας και ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης ή διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων[1]. Με λίγα λόγια, τα τελευταία χρόνια το διαδίκτυο άλλαξε δραστικά τις ζωές μας.

1.2 Ορισμός του εγκλήματος

Παρατηρούμε ότι γύρω από το έγκλημα δεν υπάρχει ένας κοινός ορισμός.

- Για τους Sutherland και Cressey (1970) «έγκλημα είναι η συμπεριφορά που παραβιάζει τον ποινικό νόμο».
- Σύμφωνα με τον ποινικό κώδικα «έγκλημα είναι πράξη άδικος και καταλογιστή εις τον πράξοντα, τιμωρούμενη υπό του νόμου».

Το πρόβλημα της εγκληματικότητας υπάρχει σε όλες τις κοινωνίες, δηλαδή αποτελεί αναπόσπαστο κομμάτι κάθε κοινωνίας. Ωστόσο εκείνο που αλλάζει είναι η μορφή του. Ουσιαστικά, τα απαραίτητα στοιχεία του εγκλήματος είναι το κοινωνικό αγαθό, η προσβολή και η αντίδραση στην προσβολή τα οποία αποτελούν έναν κύκλο ο οποίος δεν μπορεί να διασπαστεί. Το φαινόμενο της εγκληματικότητας πέρα από τα απαραίτητα στοιχεία του έχει και κάποια χαρακτηριστικά όπως είναι η παγκοσμιότητα και η διαχρονικότητα. Παρόλο τις

[1] Γιάννης Ελαφρός, Το διαδίκτυο αλλάζει άρδην τη ζωή μας, Εφημερίδα ΄΄Η Καθημερινή΄΄ -12.03.06, σελ 31

διαφορετικές κοινωνικοπολιτικές και ηθικές τάσεις κάθε τόπου και χρόνου, το κοινωνικό αυτό φαινόμενο εμφανίζεται σε όλες τις χώρες. Ιδιαίτερο ενδιαφέρον παρουσιάζει η διαχρονικότητα του στο πέρασμα των αιώνων. Τέλος, αυτό που παρατηρούμε είναι η μεγάλη αύξησή του και η εμφάνιση νέων μορφών εγκληματικότητας όπως είναι το διαδικτυακό έγκλημα.

1.3 Ποια είναι η έννοια του Διαδικτυακού εγκλήματος

Η τεράστια ανάπτυξη και εξάπλωση του διαδικτύου σε πολλούς τομείς της καθημερινότητάς μας εκτός από τα θετικά του στοιχεία πρόσφερε και μια σειρά από αρνητικά στοιχεία. Ένα από αυτά είναι η διάπραξη ενός ευρέως φάσματος εγκλημάτων δηλαδή η δυνατότητα που παρέχει για την διάπραξη μιας νέας σειράς εγκληματικών δραστηριοτήτων. Η εγκληματικότητα στον κυβερνοχώρο είναι πολύ πιο ανεπτυγμένη από όσο φαντάζονται οι άνθρωποι και έχει χτυπήσει την ανθρωπότητα με απίστευτη σοβαρότητα. Τα τελευταία χρόνια έπληξε εκατομμύρια ανθρώπους σε όλον τον κόσμο.

Με τον όρο διαδικτυακό έγκλημα εννοούμε το είδος εγκλήματος το οποίο διαπράττεται στο διαδίκτυο ή μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται μέσα στο διαδίκτυο, ή τέλος κάθε εγκληματική πράξη που εμπλέκεται και το διαδίκτυο.[2] Το διαδικτυακό έγκλημα είναι ένας γενικός όρος που αναφέρεται σε όλες τις εγκληματικές δραστηριότητες που γίνονται με τη χρήση του διαδικτύου. Μια σημαντική διαφορά που το διακρίνει από το «συμβατικό» έγκλημα είναι ότι διαπράττεται σε διαφορετικό περιβάλλον. Ωστόσο, το διαδικτυακό έγκλημα παρουσιάζει μια σειρά από χαρακτηριστικά γνωρίσματα. Αρχικά, είναι γρήγορο και εύκολο στην διάπραξή του και δεν απαιτούνται ειδικές γνώσεις προγραμματισμού. Στην συνέχεια, το διαδικτυακό έγκλημα μπορεί να διαπράττεται από οποιοδήποτε σημείο σε βάρος οποιουδήποτε χρήστη όπου και να βρίσκεται και έτσι δίνει την δυνατότητα στον δράστη να διατηρεί την ανωνυμία του. Συνεπώς, απαιτούνται μέτρα πρόληψης για τον έλεγχο του διαδικτυακού εγκλήματος και εξειδικευμένες γνώσεις από την πλευρά της Αστυνομίας/Δίωξης ηλεκτρονικού εγκλήματος για την αντιμετώπιση αυτού του είδους εγκλήματος.

[2] Ζάννη Αν. (2005). *Το διαδικτυακό έγκλημα*. Αντ. Ν. Σακκούλας, Αθήνα, σελ.62

ΚΕΦΑΛΑΙΟ 2ο

ΜΟΡΦΕΣ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1 Διαδικτυακά εγκλήματα

Όπως προαναφέραμε ως Διαδικτυακό έγκλημα εννοούμε οποιοδήποτε έγκλημα το οποίο τελείται μέσω Διαδικτύου. Ωστόσο, οι μορφές του ποικίλουν και με τη συνεχή ανάπτυξη του Διαδικτύου πολλαπλασιάζονται και εμφανίζονται νέες εγκληματικές απειλές. Οι κύριες μορφές του Διαδικτυακού εγκλήματος είναι:

- Phishing και Pharming (Ηλεκτρονικό ψάρεμα)
- Spamming (Ανεπιθύμητη αλληλογραφία)
- Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.)
- Παιδική πορνογραφία
- Cracking και Hacking
- Διακίνηση-Πειρατεία λογισμικού
- Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων
- Cyberbullying (Διαδικτυακός εκφοβισμός)
- Κακόβουλο λογισμικό (Ιοί, σκουλήκια, δούρειοι ίπποι)
- Διαδικτυακή τρομοκρατία

2.1.1 Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")

Phishing

Το phishing είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Είναι μια μορφή εγκλήματος με την οποία ο "θύτης" υποδύεται μια αξιόπιστη οντότητα, ο οποίος καταχρώμενος την ελλιπή προστασία των ηλεκτρονικών εργαλείων και την έλλειψη γνώσεων και προσοχής του θύματος προσπαθεί να αποσπάσει προσωπικά δεδομένα από το θύμα, όπως κωδικοί πρόσβασης, αριθμό πιστωτικής κάρτας, ονόματα χρηστών, αριθμό τραπεζικού λογαριασμού, ταυτότητα, διαβατήριο, αριθμό φορολογικού μητρώου, κ.λ.π. Στη συνέχεια χρεώνουν την πιστωτική κάρτα ή αδειάζουν το τραπεζικό λογαριασμό μεταφέροντας τα χρήματα σε λογαριασμούς τρίτων προσώπων στο εξωτερικό.

Τις περισσότερες φορές ο **τρόπος δράσης** εκτελείται από πλαστογραφημένο e-mail με παραπλανητικό περιεχόμενο. Ο δράστης στέλνει ένα e-mail στο οποίο συστήνεται ως ένα αξιόπιστο πρόσωπο μιας εταιρείας ή ενός οργανισμού και ζητά από το θύμα κάποιες πληροφορίες.

Τα εργαλεία αυτής της μορφής εγκληματικότητας συνήθως είναι αποπλανητικοί σύνδεσμοι (link manipulation), αναδυόμενα παράθυρα (pop-up windows), πολλαπλές

καρτέλες (tab nabbing) , δούρειοι ίπποι ή ακόμα και ψεύτικα δημόσια δίκτυα. Το πιο συνηθισμένο εργαλείο είναι ο αποπλανητικός σύνδεσμος. Το ανυποψίαστο θύμα θα επιλέξει το σύνδεσμο, ο οποίος θα τον οδηγήσει σε μια τοποθεσία-αντίγραφο της πραγματικής, όπου θα υποκλαπούν τα προσωπικά του στοιχεία.

Pharming

Το pharming είναι μια μορφή εγκληματικής επίθεσης παρόμοια με το phishing αλλά πιο επικίνδυνη. Ο σκοπός αυτής της μορφής διαδικτυακού εγκλήματος είναι ο ίδιος με τον σκοπό του phishing. Ο δράστης προσπαθεί να αποκτήσει τα προσωπικά δεδομένα του χρήστη-θύματος με ενέργειες εξαπάτησης. Ο τρόπος όμως που προσπαθεί να εξαπατήσει τους χρήστες από τεχνική άποψη είναι διαφορετικός.

Χρησιμοποιούν και επεμβαίνουν σε ένα ειδικό πρόγραμμα ,το λεγόμενο Σύστημα Ονομάτων Χώρου (DNS). Εξαιτίας κάποιων κενών ασφαλείας του συστήματος επεμβαίνουν στο σύστημα και διεισδύουν στον υπολογιστή του χρήστη. Έτσι, ακόμη και όταν ο χρήστης πληκτρολογεί σωστά την διεύθυνση μιας ιστοσελίδας οδηγείται σε πλαστές ιστοσελίδες. Θεωρώντας ότι βρίσκεται σε ασφαλή χώρο πληκτρολογεί το όνομα χρήστη, τον κωδικό πρόσβασης και άλλα προσωπικά του στοιχεία με αποτέλεσμα να τα «παραδίδει» στην ιστοσελίδα του δράστη. Στην περίπτωση δε που ο χρήστης πληκτρολογήσει την διεύθυνση π.χ. της υπηρεσίας Ηλεκτρονικής Τραπεζικής, η προσπάθεια του να πραγματοποιήσει τις συναλλαγές καταλήγει στη μεταφορά των χρημάτων του στους δράστες.

Έρευνα της Kaspersky Lab και της B2B International ανέδειξε ότι σχεδόν οι μισοί από τους Ευρωπαίους συμμετέχοντες αντιμετώπισαν online απειλές που αφορούσαν απόπειρες κλοπής χρημάτων. Ωστόσο, ακόμα και οι ψηφιακές επιθέσεις που δε σχετίζονται με χρήματα, ενδέχεται να οδηγήσουν σε απρόβλεπτα έξοδα. Οι ψηφιακοί εγκληματίες αποκτούν πολύτιμα δεδομένα από τους χρήστες με διάφορους μεθόδους. Ανάμεσα στις πολλές τεχνικές που χρησιμοποιούν για να συλλέξουν τις εν λόγω πληροφορίες είναι και οι ιστοσελίδες phishing, οι οποίες μιμούνται επίσημες ιστοσελίδες.

Επίσης σύμφωνα με πρόσφατη ανακοίνωσή της τον Ιανουάριο του 2015, η Ελληνική Αστυνομία εφιστούσε την προσοχή στους πολίτες, μετά τον εντοπισμό κυκλώματος, τα μέλη του οποίου προσπαθούσαν, μέσω e-mails, να κλέψουν προσωπικά οικονομικά δεδομένα. Τα μέλη του κυκλώματος, με τα μηνύματα αυτά, που φαινόταν να έχουν σταλεί από οργανισμό υπηρεσιών πληρωμής, προέτρεπαν τους παραλήπτες να επιβεβαιώσουν προσωπικά τους στοιχεία (αριθμό πιστωτικής κάρτας, ταυτότητα, διαβατήριο, Α.Φ.Μ., κ.λ.π.).

2.1.2 Spamming(Ανεπιθύμητη αλληλογραφία)

Το spam ξεκίνησε ως κάτι άκακο και διασκεδαστικό αλλά κατέληξε να είναι ένα από τα μεγαλύτερα προβλήματα του διαδικτύου. Με τον όρο spamming ή αλλιώς ανεπιθύμητη

αλληλογραφία ορίζεται η μαζική αποστολή μεγάλου αριθμού ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Τα μηνύματα spam κυρίως χρησιμοποιούνται για την αποστολή διαφημιστικών μηνυμάτων. Χρησιμοποιούνται όμως και για την αποστολή μηνυμάτων τα οποία χαρακτηρίζονται ως ενοχλητικά. Μεγάλη ποσότητα μηνυμάτων κατακλύζουν το ηλεκτρονικό ταχυδρομείο διαφημίζοντας διάφορα προϊόντα ή υπηρεσίες, χωρίς να το έχει ζητήσει ο χρήστης. Η ανεπιθύμητη αλληλογραφία εκτός από ενοχλητική μπορεί να είναι συγχρόνως και προσβλητική, απατηλή ακόμα και επικίνδυνου περιεχομένου. Αυτού του είδους τα μηνύματα μπορούν να χρησιμοποιηθούν ως ένα εργαλείο για την διαφήμιση πλαστών προϊόντων και υπηρεσιών ακόμη και πορνογραφικού περιεχομένου. Ένας ακόμη σκοπός είναι η μόλυνση του υπολογιστή με ιούς ή επικίνδυνων λογισμικών. Μεγάλη έκταση επίσης έχει πάρει το spam τύπου phishing το οποίο έχει ως βασικό σκοπό να παραπλανεί τους χρήστες και να υποκλέπτει προσωπικά τους δεδομένα με απώτερο σκοπό να αποσπούν χρήματα.

Το χαμηλό κόστος και η άμεση αποστολή οδηγεί τις εταιρείες σε όλο τον κόσμο να χρησιμοποιούν όλο και περισσότερο αυτή τη μέθοδο για να διαφημίζουν τα προϊόντα τους και τις υπηρεσίες τους. Έτσι, υπερφορτώνουν τον διακομιστή με αποτέλεσμα να δημιουργούν προβλήματα μέχρι και στους Παρόχους Υπηρεσιών Διαδικτύου. Τα τελευταία χρόνια ο αριθμός των μηνυμάτων spam που λαμβάνουν οι χρήστες αυξάνεται με γοργό ρυθμό.

2.1.3 Απάτες μέσω Διαδικτύου (πιστωτικές κάρτες, διαδικτυακός τζόγος κ.λ.π.)

Το διαδίκτυο είναι πλέον το όπλο των σύγχρονων εγκλημάτων. Μέσω του διαδικτύου επιτυγχάνονται εύκολα οι παράνομες δραστηριότητες δηλαδή γρήγορο κέρδος. Στο σύνολο αυτών των σύγχρονων εγκλημάτων ανήκουν και οι απάτες μέσω Διαδικτύου όπως είναι οι απάτες με πιστωτικές κάρτες και ο διαδικτυακός τζόγος.

Πιστωτικές κάρτες

Η μεγάλη χρήση των πιστωτικών καρτών στο Διαδίκτυο οδήγησε στην ευκολότερη διάπραξη των εγκλημάτων. Αυτό οφείλεται πρώτον, στην τεράστια καθημερινή χρήση των πιστωτικών καρτών και δεύτερον στην μη αυτοπρόσωπη παρουσία του αγοραστή και στην άγνωστη ταυτότητα του υποψήφιου απατεώνα. Στις ηλεκτρονικές συναλλαγές ο κάτοχος της κάρτας δεν είναι παρών και έτσι ο πωλητής δεν μπορεί να ελέγξει την υπογραφή του κατόχου.

Οι απάτες με πιστωτικές κάρτες μέσω Διαδικτύου πραγματοποιούνται με διάφορους τρόπους. Ο πιο απλός τρόπος απάτης είναι η κλοπή της κάρτας. Εκτός από την αγορά μέσω Διαδικτύου, αριθμών πιστωτικών καρτών που έχουν υποκλαπεί υπάρχουν και οι παρακάτω μορφές απάτης:

- Η κλωνοποίηση ιστότοπου.
  Με αυτόν τον τρόπο ο απατεώνας δημιουργεί εικονική ιστοσελίδα ενός πραγματικού καταστήματος έτσι ώστε να παραπλανήσει τους χρήστες οι οποίοι νομίζουν ότι είναι η πραγματική ιστοσελίδα και να αποσπάσει τα στοιχεία και τον αριθμό των πιστωτικών καρτών.
- Η δημιουργία ιστοσελίδων με ψεύτικες υπηρεσίες ή προϊόντα.
  Στην περίπτωση αυτή ο υποψήφιος απατεώνας δημιουργεί μια πλασματική ιστοσελίδα με ψεύτικες υπηρεσίες ή προϊόντα κάνοντας τους χρήστες να πιστέψουν ότι πρόκειται για κάποιο κατάστημα στο οποίο μπορούν να πραγματοποιήσουν τις αγορές τους με αποτέλεσμα ο απατεώνας να συγκεντρώνει αριθμούς πιστωτικών καρτών.
- Τα προγράμματα δημιουργίας αριθμών πιστωτικών καρτών.
  Υπάρχουν εφαρμογές λογισμικού τα οποία με τη χρήση διάφορων αλγορίθμων δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών οι οποίοι χρησιμοποιούνται ήδη.
- Κλοπή πληροφοριών πιστωτικών καρτών.
  Αυτός ο τρόπος πραγματοποιείται κατά την διάρκεια μια νόμιμης συναλλαγής. Ο απατεώνας κλέβει τις πληροφορίες των πιστωτικών καρτών με διάφορους παράνομους τρόπους.

Η χρήση των σύγχρονων τεχνολογιών δεν απαιτεί ιδιαίτερες γνώσεις και δεξιότητες για να διαπράξει κάποιος το έγκλημα μέσω πιστωτικών καρτών ωστόσο αν ο χρήστης είναι προσεκτικός και δεν βρίσκεται σε πλήρη άγνοια όσον αφορά τους κινδύνους της ασφάλειας μπορεί να αντιμετωπίσει τέτοιου είδους προβλήματα.

Διαδικτυακός τζόγος

Τζόγος είναι ένα κοινωνικό φαινόμενο το οποίο δεν μπορεί να περάσει απαρατήρητο. Με την λέξη τζόγος εννοούμε το ποντάρισμα ή το στοίχημα πάνω σε κάτι που πιστεύουμε ότι θα κερδίσει και εμείς φυσικά θα έχουμε κέρδος. Ο διαδικτυακός τζόγος είναι τυχερά παιχνίδια που προσφέρονται από το Διαδίκτυο. Στην Ελλάδα κατά κύριο λόγο χωρίζεται σε 3 μέρη:

- Στο online καζίνο
- Στο διαδικτυακό στοίχημα
- Στο online πόκερ

Ο διαδικτυακός τζόγος γνώρισε ιδιαίτερη άνθιση με την εξάπλωση του Διαδικτύου. Μπορεί να πραγματοποιηθεί είτε σε ειδικά κατασκευασμένες ιστοσελίδες είτε μέσα από ανεπιθύμητα μηνύματα(spamming) τα οποία προσκαλούν τους χρήστες να παίξουν διάφορα τυχερά παιχνίδια μέσω του διαδικτύου. Υπάρχουν χιλιάδες ιστοσελίδες που προσφέρουν online τυχερά παιχνίδια. Το ειδικό θέμα όμως με τα online τυχερά παιχνίδια είναι ότι σε πολλές χώρες είναι νόμιμα ενώ σε κάποιες άλλες όχι και έτσι, από νομική άποψη οι ιδιοκτήτες των ιστοσελίδων αυτών είναι ασφαλείς στην πατρίδα τους. Το διαδίκτυο εφόσον είναι ανεξάντλητη πηγή ενδιαφέροντος οδηγεί τους χρήστες σε αυτού του είδους το φαινόμενο. Τα προβλήματα όμως που μπορεί να προκαλέσει είναι πολλά. Το βασικό

πρόβλημα του διαδικτυακού τζόγου είναι η απώλεια χρημάτων είτε δίνοντας τα στοιχεία πιστωτικών καρτών είτε με προπληρωμένες κάρτες. Επιπλέον, ο διαδικτυακός τζόγος μπορεί να οδηγήσει και στον εθισμό δημιουργώντας στον χρήστη κατάθλιψη και διάφορα άλλα προβλήματα υγείας. Το φαινόμενο εθισμού στα τυχερά παιχνίδια αποκτά δραματικές διαστάσεις στους νέους καθώς παρατηρούμε τεράστια αύξηση των ποσοστών εθισμένων νέων στα τυχερά παιχνίδια τα τελευταία χρόνια στη χώρα μας. Γι' αυτό το λόγο οι γονείς πρέπει να πάρουν μέτρα προστασίας έτσι ώστε να βοηθήσουν τα παιδιά τους να αποφύγουν τον διαδικτυακό τζόγο.

2.1.4 Παιδική πορνογραφία

Η διαδικτυακή πορνογραφία πιστεύεται ότι είναι μια από τις μεγαλύτερες επιχειρήσεις στο Διαδίκτυο σήμερα. Τα εκατομμύρια από τις πορνογραφικές ιστοσελίδες που ευδοκιμούν στο διαδίκτυο είναι μια μαρτυρία για αυτό. Ωστόσο, το φαινόμενο της πορνογραφίας ανηλίκων έχει λάβει ανεξέλεγκτες διαστάσεις τα τελευταία χρόνια προκαλώντας ιδιαίτερη ανησυχία στις διωκτικές αρχές. Στατιστικές μελέτες έχουν δείξει ότι η παιδική πορνογραφία είναι μια από τις πιο συχνές μορφές του διαδικτυακού εγκλήματος. Είναι επικερδής εγκληματική απειλή καθώς διαθέτει υπερεθνικό χαρακτήρα. Το ίδιο το διαδίκτυο καθιστά δυνατή την ταυτόχρονη διάχυση πληροφοριών σε περισσότερους ανθρώπους παγκοσμίως.

Τι είναι παιδική πορνογραφία; Η παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες.

Η παιδική πορνογραφία έχει τις εξής μορφές:

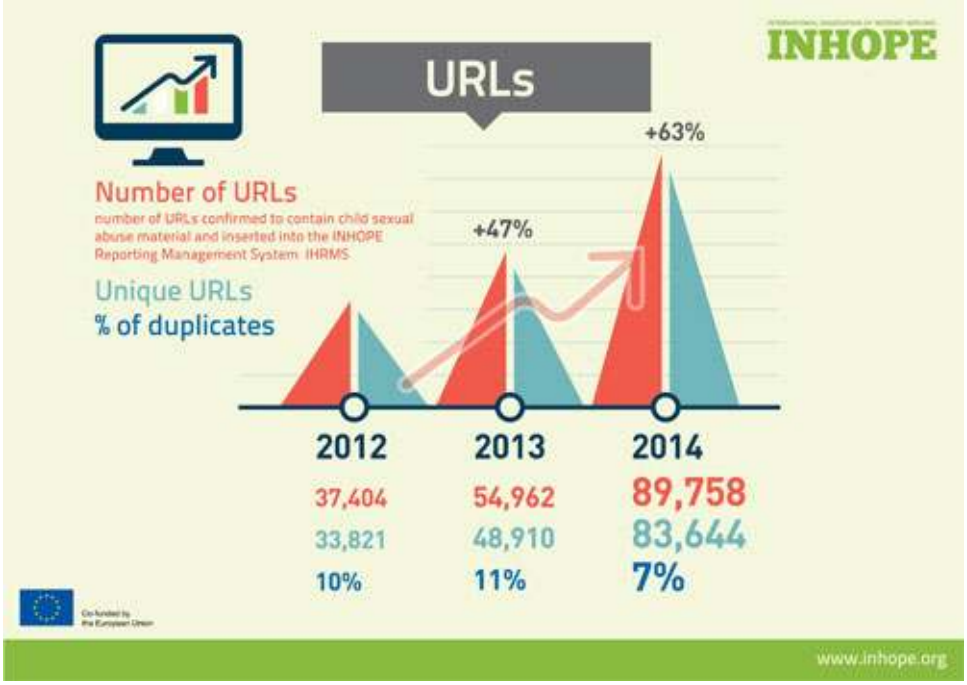
- Ένας ανήλικος που συμμετέχει σε πράξεις με σαφή σεξουαλικό χαρακτήρα συμπεριλαμβανομένης της άσεμνης επίδειξης των γεννητικών οργάνων.
- Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Το συγκεκριμένο έγκλημα είναι διαθέσιμο με διαφορετικούς τρόπους, όπως με φωτογραφίες, βίντεο, κινούμενα σχέδια, spam e-mail και συνδέεται με την παραγωγή, την κατοχή, την διανομή ή την μετάδοση δια μέσω ηλεκτρονικού υπολογιστή. Το υλικό το οποίο διακινείται μέσω του Διαδικτύου μπορεί ο καθένας να το «κατεβάσει» χωρίς να αποκαλύψει την ταυτότητα του. Συνεπώς, έχουμε δυο εκφάνσεις της παιδικής πορνογραφίας στο διαδίκτυο:

- Τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και

- Την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

Σύμφωνα με τα επίσημα στοιχεία για το 2014 που δημοσίευσε τον Απρίλιο του 2015 ο INHOPE, ο Διεθνής Σύνδεσμος Ανοικτών Γραμμών για το παράνομο περιεχόμενο του Ίντερνετ παρατηρούμε ότι για μοναδικά URLs με παιδική πορνογραφία έλαβε και διαχειρίστηκε 83.644 καταγγελίες ενώ την προηγούμενη χρονιά έλαβε 48.910 και το 2012 έλαβε 33.821 καταγγελίες.



Πηγή:INHOPE

Όσον αφορά την Ελλάδα σύμφωνα με τα στατιστικά στοιχεία που παρουσίασε η SafeLine η μοναδική Ανοικτή Γραμμή Καταγγελιών στην Ελλάδα για παράνομο περιεχόμενο στο Διαδίκτυο και από το 2003 το επίσημο μέλος της Ελλάδας στον INHOPE παρατηρούμε ότι ο συνολικός αριθμός καταγγελιών που έλαβε για το 2014 ήταν 3435. Ιδιαίτερα αξιοπρόσεκτο είναι ότι παρόλο που το μεγαλύτερο ποσοστό αφορούσε την παραβίαση προσωπικών δεδομένων (35%) ,η αμέσως επόμενη κατηγορία ήταν οι ιστοσελίδες που περιείχαν παιδική πορνογραφία με ποσοστό 20% , περίπου 10 ποσοστιαίες μονάδες αυξημένο συγκριτικά με το προηγούμενο έτος.[3]

[3] SafeLine.gr

2.1.5 Cracking και Hacking

Στις μέρες μας, η ασφάλεια των πληροφοριακών συστημάτων δέχεται πάρα πολλές απειλές. Οι απειλές μπορούν να προέρχονται από διάφορες μορφές επιθέσεων. Μέσα σε αυτές τις απειλές ανήκει και η πιο συνηθισμένη μορφή επιθέσεων, το λεγόμενο "hacking".

Με τον όρο "hacking" εννοούμε την πράξη εισβολής σε ένα δίκτυο υπολογιστών δηλαδή την χωρίς δικαίωμα είσοδο σε συστήματα υπολογιστών. Οι "χάκερς" διεισδύοντας σε ένα σύστημα υπολογιστών έχουν ως σκοπό την ηθική ικανοποίηση που θα τους προσφέρει η επιτυχία. Προσπαθούν με κάθε τρόπο να ανακαλύψουν τα κενά που παρουσιάζουν αυτά τα συστήματα και τις κρυφές λειτουργίες τους. Οι "χάκερς" είναι άτομα με πολλές γνώσεις προγραμματισμού και με αυτόν τον τρόπο μπορούν να λύνουν διάφορα προβλήματα και να βελτιώνουν εφαρμογές. Ωστόσο, το "hacking" θεωρείται παράνομο εξαιτίας της ελεύθερης πρόσβασης των πληροφοριών που απαιτεί.

Οι ιδιότητες "hacking" και "cracking" δεν αποκλείεται να βρεθούν σε ένα πρόσωπο αλλά με μια σημαντική διάκριση. Ως "crackers" χαρακτηρίζονται τα άτομα που εισβάλουν σε ένα δίκτυο υπολογιστών έχοντας κακή πρόθεση. Τα συγκεκριμένα άτομα έχουν σκοπό την υποκλοπή και την οποιαδήποτε άλλη επιβλαβή ενέργεια. Εισβάλλοντας σε ξένους υπολογιστές χωρίς δικαίωμα προκαλούν διάφορες ζημιές. Οι ζημιές που μπορούν να προκαλέσουν είναι οι εξής:

- Δημιουργία ιών
- Παραβίαση κωδικών ασφαλείας
- Υποκλοπή ταυτότητας και άλλων εμπιστευτικών πληροφοριών ή χρημάτων από τραπεζικούς λογαριασμούς ή πιστωτικές κάρτες
- Καταστροφή ή και αλλοίωση διάφορων ιστοσελίδων
- Τα θύματα να γίνουν εν αγνοία τους δέκτες εκβιασμών, αποστολείς μηνυμάτων spam ή να φιλοξενούν παράνομους servers

Εκτός από τα παραπάνω προβλήματα που προξενούν στα θύματα τους οι "crackers" φέρουν και κοινωνικές, οικονομικές, πολιτικές και επιχειρησιακές συνέπειες. Σύμφωνα με ανακοίνωση της Δίωξης ηλεκτρονικού εγκλήματος τον Απρίλιο του 2015, κάποιοι "επιτήδειοι" άρχισαν να διεισδύουν στην ηλεκτρονική αλληλογραφία μικρών και μεγάλων ελληνικών εταιρειών αποσπώντας μεγάλα χρηματικά ποσά με αποτέλεσμα να δημιουργούν μεγάλα οικονομικά προβλήματα.

2.1.6 Διακίνηση-Πειρατεία λογισμικού

Το λογισμικό το οποίο είναι μια συλλογή από προγράμματα υπολογιστών, διαδικασίες και οδηγίες χρήσης που εκτελούν ορισμένες εργασίες σε ένα υπολογιστικό σύστημα κατέχει μια από τις σημαντικότερες θέσεις της σύγχρονης πληροφορικής. Πάρα πολλές εφαρμογές του διαδικτύου καθημερινά στηρίζονται στο λογισμικό. Έτσι και η λειτουργία του διαδικτύου

βασίζεται στο λογισμικό και το καθιστά ένα από τα πιο σημαντικά και πολύτιμα εργαλεία της σύγχρονης τεχνολογίας. Πάρα πολύ σημαντικό ρόλο παίζει και στο κομμάτι των επιχειρήσεων οι οποίες με τη χρήση λογισμικών γίνονται περισσότερο αποτελεσματικές.

Η Διακίνηση-Πειρατεία λογισμικού ανήκει στα εγκλήματα πνευματικής ιδιοκτησίας. Αυτή η μορφή εγκλήματος υπήρχε και πριν εμφανιστεί το διαδίκτυο αλλά γινόταν με άλλους τρόπους. Όμως, η τεράστια εξάπλωση του διαδικτύου έφερε πολλές αλλαγές στη διακίνηση και πειρατεία του λογισμικού. Με τον όρο πειρατεία λογισμικού εννοούμε την παράνομη αναπαραγωγή και χρήση προγραμμάτων που έχουν δημιουργήσει προγραμματιστές, παραβιάζοντας το νόμο και τα δικαιώματα πνευματικής ιδιοκτησίας των δημιουργών λογισμικού. Οι παραβάτες αυτοί ονομάζονται "πειρατές".

Η αναπαραγωγή και η διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή εξαιτίας του διαδικτύου είναι ιδιαίτερα εύκολη. Το λογισμικό μπορεί να διακινηθεί με πολλούς τρόπους. Τέτοιοι τρόποι είναι οι εξής:

- Μέσω ψεύτικων ιστοσελίδων
- Μέσω ταξινομημένων διαφημίσεων
- Μέσω ηλεκτρονικού ταχυδρομείου (e-mail)
- Μέσω chat
- Μέσω εφαρμογών ανταλλαγής αρχείων (pear to pear)

Παρόλο που οι εταιρείες παραγωγής λογισμικών παίρνουν τα κατάλληλα τεχνολογικά μέτρα υπάρχουν άτομα είτε με ειδικές γνώσεις προγραμματισμού (crackers) είτε παίρνοντας ένα έτοιμο λογισμικό το οποίο διατίθεται ελεύθερο στο διαδίκτυο και αντιγράφουν το λογισμικό. Ωστόσο το πλαστό λογισμικό δηλαδή η αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρείες μπορεί να επιφέρει τεράστια προβλήματα στον υπολογιστή του χρήστη. Η πλαστογράφηση γνήσιων προϊόντων μπορεί να είναι ένα ελαττωματικό και επικίνδυνο αντίγραφο του πρωτοτύπου και συνεπώς, μπορεί να βλάψει σοβαρά τον υπολογιστή και να υπονομεύσει την ασφάλειά του. Τέλος, σύμφωνα με το νόμο, η πράξη της παράνομης εκμετάλλευσης πνευματικής ιδιοκτησίας θεωρείται άδικη πράξη και τιμωρείται αυστηρά.

2.1.7 Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων

Η Διακίνηση ναρκωτικών μέσω Διαδικτύου και άλλων επικίνδυνων πραγμάτων όπως είναι τα όπλα αποτελεί ένα πολύ σοβαρό φαινόμενο και ένα από τα πιο επικίνδυνα διαδικτυακά εγκλήματα. Είναι ένα από τα πιο περίπλοκα φαινόμενα της εποχής μας και σε γενικές γραμμές έχει αυξητικές τάσεις, καθώς πρόκειται για νέα εγκληματική συμπεριφορά.

Εξαιτίας του λεγόμενου «Deep Web», δηλαδή, ιστοσελίδων που διατηρούν την ανωνυμία των χρηστών και δεν ανακαλύπτονται από τις μηχανές αναζήτησης, διακινούνται και διατίθενται προς πώληση όπλα και μεγάλες ποσότητες ναρκωτικών από έναν συνεχώς αυξανόμενο αριθμό ιστότοπων. Αυτό το τεράστιο παρεμπόριο ναρκωτικών μέσω

συγκεκριμένων ιστοσελίδων είναι εύκολο προσβάσιμο ακόμη και από ερασιτέχνες χρήστες, δηλαδή μπορεί να αγοράσει κανείς όπλα και ναρκωτικά από την «μαύρη αγορά» με σχετική ευκολία. Για την πρόσβαση στους συγκεκριμένους ιστότοπους χρειάζεται να έχεις τη σωστή διεύθυνση και το απαραίτητο λογισμικό, δηλαδή, ένα κρυπτογραφημένο λογισμικό το οποίο έχει στόχο να καταστήσει εφικτή την ανώνυμη περιήγηση στο διαδίκτυο. Ακόμη και οι συναλλαγές γίνονται μέσω του διαδικτυακού νομίσματος (bitcoin) χωρίς την χρήση πιστωτικών καρτών ή τη μεσολάβηση τραπεζών. Με τον τρόπο αυτό επιτυγχάνεται η ανωνυμία των μελών και το έργο των διωκτικών αρχών γίνεται ακόμη πιο δύσκολο. Στην ουσία πρόκειται για κρυπτογραφημένα δίκτυα του κυβερνοχώρου που χρησιμοποιούν οι εγκληματίες για να διαπράξουν τις παράνομες ενέργειές τους. Έτσι, εξαιτίας της ολοένα αυξανόμενης χρήσης του «Deep Web», το διαδίκτυο εξελίσσεται ως μια αναπτυσσόμενη αγορά ναρκωτικών ουσιών και έτσι οδηγούμαστε στην έξαρση του φαινομένου της διακίνησης ναρκωτικών και άλλων επικίνδυνων πραγμάτων.

2.1.8 Cyberbullying (Διαδικτυακός εκφοβισμός)

Στις μέρες μας το cyberbullying αποτελεί ένα πολύ διαδεδομένο πρόβλημα και είναι μια αυξανόμενη απειλή για τα παιδιά και τους νέους. Η σημερινή σύγχρονη τεχνολογία βοήθησε ώστε ο διαδικτυακός εκφοβισμός να γίνει ευκολότερος. Το βασικό πρόβλημα είναι ότι τα εργαλεία επικοινωνίας έχουν εξελιχθεί σημαντικά τις τελευταίες δεκαετίες. Συνεπώς, το φαινόμενο του διαδικτυακού εκφοβισμού απασχολεί ιδιαίτερα τους ερευνητές καθώς γνωρίζει έξαρση τον τελευταίο καιρό παγκοσμίως αλλά και στην χώρα μας.

Με τον όρο cyberbullying (διαδικτυακό εκφοβισμό) περιγράφεται μια εγκληματική συμπεριφορά μέσω Διαδικτύου με την οποία ο θύτης εκφοβίζει, απειλεί, εκβιάζει ή παρενοχλεί τα θύματά του τα οποία είναι είτε παιδιά είτε έφηβοι. Το διαδικτυακό εκφοβισμό μπορούμε να τον διακρίνουμε σε δυο κατηγορίες:

- Στην άμεση παρενόχληση, δηλαδή η επίθεση γίνεται απευθείας στο θύμα μέσω μηνυμάτων.
- Στην έμμεση παρενόχληση, δηλαδή το μήνυμα δεν στέλνεται απευθείας στο θύμα.[4]

Η μεγάλη ανάπτυξη του Διαδικτύου και οι τεράστιες δυνατότητες που προσφέρει βοήθησαν έτσι ώστε το cyberbullying να πάρει πάρα πολλές μορφές. Μπορεί να εμφανιστεί είτε σε μορφή κειμένου μέσω e-mail, άμεσων μηνυμάτων ή δωματίων επικοινωνίας (chat), είτε δημοσιεύοντας φωτογραφίες ή ψευδά γεγονότα στα μέσα κοινωνικής δικτύωσης, σε ιστολόγια (blogs) ή άλλες ιστοσελίδες. Οι λόγοι που οι νέοι οδηγούνται σε αυτού του είδους την συμπεριφορά είναι διάφοροι. Κάποιοι από τους οποίους μπορεί να είναι είτε για εκδίκηση, για επίλυση προσωπικών διαφορών, εξαιτίας θυμού και απόγνωσης, είτε ως μορφή ψυχαγωγίας για να ικανοποιήσουν προσωπικές τους ανάγκες. Ωστόσο, η παρενόχληση στον

[4] Βλαχόπουλος Κ. (2007). *Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση*. Νομική Βιβλιοθήκη, Αθήνα, σελ.72

κυβερνοχώρο μπορεί να επιφέρει πολλές σοβαρές και απρόβλεπτες συνέπειες σε ένα νέο. Αρχικά, μπορεί να τον οδηγήσει σε αποχή από το σχολείο του και σε μείωση των σχολικών του επιδόσεων. Στη συνέχεια, μπορεί να τον οδηγήσει στην κοινωνική απομόνωση και στην περιθωριοποίηση από άλλα άτομα, δηλαδή στην μείωση των επιδόσεών του στις κοινωνικές του ικανότητες. Τέλος, ο διαδικτυακός εκφοβισμός έχει τη δυνατότητα να επιφέρει επιπτώσεις και στην ψυχική του υγεία. Μπορεί να τον κάνει να αισθάνεται ένοχος ή να εκτελεί πράξεις αντίθετες από τον χαρακτήρα του ενώ ταυτόχρονα η κατάθλιψη και η αυτοκτονία είναι μια από τις σημαντικότερες συνέπειες αυτής της μορφής εγκλήματος.

Το φαινόμενο του διαδικτυακού εκφοβισμού στην Ελλάδα.

Σύμφωνα με την έρευνα EUNETADB για το 2013 που διεξήγαγε και συντόνισε η Ελληνική Μονάδα Εφηβικής Υγείας του Νοσοκομείου Παίδων Αγλαΐα Κυριακού η Ελλάδα κατέχει την δεύτερη θέση στο διαδικτυακό εκφοβισμό ανάμεσα στην Ευρώπη με ποσοστό 26.8%. Δηλαδή παραπάνω από ένας στους τέσσερις Έλληνες έφηβοι έχουν πέσει θύμα διαδικτυακού εκφοβισμού (cyberbullying).

2.1.9 Κακόβουλο λογισμικό (Ιοί, σκουλήκια, δούρειοι ίπποι)

Το κακόβουλο λογισμικό είναι το πιο διαδεδομένο διαδικτυακό έγκλημα στην Ελλάδα και αποτελεί ένα πολύ σημαντικό πρόβλημα για την ασφάλεια των υπολογιστικών συστημάτων. Το κακόβουλο λογισμικό είναι ένα λογισμικό το οποίο ο εγκληματίας το δημιουργεί έχοντας σκοπό να βλάψει τον υπολογιστή. Στόχος του είναι:

- Να δημιουργήσει πρόβλημα στη λειτουργία του υπολογιστικού συστήματος.
- Να διαγράψει, κλέψει ή να αλλοιώσει πληροφορίες και δεδομένα από το υπολογιστικό σύστημα.
- Να καταρρεύσει ολόκληρο το σύστημα.

Ο επιτιθέμενος προσπαθεί να εξαπλώσει και να μεταδώσει το κακόβουλο λογισμικό είτε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), είτε μέσω “επισφαλών” ιστοσελίδων. Σύμφωνα με τον Sinrod (2000) το κακόβουλο λογισμικό διακρίνεται σε τρία είδη:

- Ιούς (Viruses)
- Σκουλήκια (Worms)
- Δούρειοι ίπποι (Trojan horses)

Ιοί (Viruses)

Ο ιός είναι ο πιο γνωστός αλλά και ο πιο συνηθισμένος τρόπος διάδοσης κακόβουλου λογισμικού διότι η μετάδοση και η εξάπλωσή του γίνεται πολύ εύκολα και γρήγορα. Ουσιαστικά είναι ένα πρόγραμμα, δηλαδή μια σειρά από εντολές οι οποίες εκτελούν κάποιες ενέργειες μέσα σε έναν υπολογιστή. Για την εκτέλεση αυτών των κακόβουλων ενεργειών, ο

ιός πρέπει να βρίσκεται σε κατάλληλη θέση δηλαδή μέσα στα ψηφιακά αρχεία και δεδομένα τα οποία είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή. Έτσι, ο χρήστης δεν μπορεί να εντοπίσει το λογισμικό και άθελα του μεταφέρει τον ιό και σε άλλα υπολογιστικά συστήματα προκαλώντας ζημιές.

Σκουλήκια (Worms)

Τα σκουλήκια είναι μια υποκατηγορία των ιών με διαφορετικό τρόπο λειτουργίας. Αρχικά, εισέρχονται στον υπολογιστή μέσω Διαδικτύου και πολλαπλασιάζονται χωρίς κάποια ενέργεια από τον χρήστη και χωρίς να βρίσκονται σε κάποια συγκεκριμένη θέση του υπολογιστικού συστήματος, η οποία είναι και η βασική διαφορά από τους ιούς. Στη συνέχεια, προκαλούνε την ζημιά τους στον υπολογιστή και διαδίδονται μέσω Διαδικτύου και σε άλλα συστήματα.

Δούρειοι ίπποι (Trojan horses)

Ο Δούρειος ίππος είναι ένα κακόβουλο λογισμικό το οποίο προσβάλλει τον υπολογιστή χωρίς να το εντοπίζει ο χρήστης. Συνήθως ένας δούρειος ίππος είναι ένα πρόγραμμα το οποίο εντοπίζεται στο σκληρό δίσκο και περιέχει κάποιες κρυμμένες λειτουργίες. Με αυτές τις κρυμμένες λειτουργίες ο επιτιθέμενος αποκτά τον πλήρη έλεγχο στον υπολογιστή και με αυτό τον τρόπο μπορεί να υποκλέψει προσωπικά δεδομένα και πληροφορίες όπως είναι ο αριθμός πιστωτικών καρτών, κωδικούς πρόσβασης ακόμη και να δημιουργήσει επιθέσεις άρνησης εξυπηρέτησης. Για αυτό το λόγο, η διάδοση του Δούρειου ίππου αποτελεί το πιο επικίνδυνο κακόβουλο λογισμικό.

2.1.10 Διαδικτυακή τρομοκρατία

Η διαδικτυακή τρομοκρατία είναι η τρομοκρατία με κύριο μέσο το Διαδίκτυο. Εξαιτίας της τεράστιας εξάπλωσής του η διαδικτυακή τρομοκρατία παρουσιάζει μεγάλη έξαρση τα τελευταία χρόνια, αποτελεί την πιο επίφοβη απειλή και έχει τραγικά αποτελέσματα. Το Ομοσπονδιακό Γραφείο Ερευνών των Η.Π.Α. (FBI) ορίζει την κυβερνοτρομοκρατία ως την «προσχεδιασμένη, πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι άμαχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες».[5] Ουσιαστικά, η διαδικτυακή τρομοκρατία θεωρείται η προμελετημένη χρήση απειλών στον κυβερνοχώρο, με την πρόθεση να προωθήσει κοινωνικούς, ιδεολογικούς, θρησκευτικούς, πολιτικούς ή παρόμοιους στόχους, ακόμα και να εκφοβίσει οποιοδήποτε πρόσωπο στα πλαίσια της προώθησης των στόχων αυτών. Το Διαδίκτυο χάρη στις ποικίλες λειτουργίες του προσφέρει πάρα πολλά πλεονεκτήματα σε αυτή τη μορφή τρομοκρατίας. Τα οφέλη που προσφέρει είναι:

[5] Βλαχόπουλος Κ. (2007). *Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση*. Νομική Βιβλιοθήκη, Αθήνα, σελ.71

- Διατηρείται η ανωνυμία δηλαδή, καθιστά αδύνατο τον εντοπισμό της τοποθεσίας και των παράνομων ενεργειών.
- Είναι ένα οικονομικό μέσο επικοινωνίας, φθηνότερο από τις άλλες τρομοκρατικές μεθόδους.
- Τα εγκλήματα πληροφοριών μπορούν να διαπραχθούν από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους, δηλαδή, το διαδίκτυο προσφέρει γρηγορότερη προσέγγιση των στόχων επίθεσης.

Στην διαδικτυακή τρομοκρατία εντάσσεται επίσης και η ρατσιστική προπαγάνδα, δηλαδή, προσβάλλει ανθρώπους άλλων θρησκειών, άλλων σεξουαλικών προτιμήσεων ή άλλων πολιτικών σχηματισμών.

2.2 Μέτρα πρόληψης και αντιμετώπισης του Διαδικτυακού εγκλήματος

Τα μέτρα πρόληψης και αντιμετώπισης του διαδικτυακού εγκλήματος αποτελούν πρωταρχικό ζήτημα εξαιτίας της ραγδαίας αύξησης του διαδικτυακού εγκλήματος και των κινδύνων που δημιουργεί. Η πρόληψη αποτελεί τη βασική συνιστώσα της ασφάλειας του πληροφοριακού συστήματος και είναι η αποτελεσματικότερη αντιμετώπιση του προβλήματος. Για την αντιμετώπιση των προηγούμενων μορφών διαδικτυακού εγκλήματος κρίνεται απαραίτητη η λήψη συγκεκριμένων μέτρων. Τα κυριότερα μέτρα περιλαμβάνουν:

- Τεχνικά μέτρα ασφαλείας (antivirus, firewall, κ.λ.π.)
- Την κατάλληλη νομοθεσία
- Τις εξειδικευμένες γνώσεις της Αστυνομίας/Δίωξης ηλεκτρονικού εγκλήματος
- Την εκπαίδευση των χρηστών
- Την ευαισθητοποίηση του κοινού

Αρχικά, λέγοντας τεχνικά μέτρα ασφαλείας εννοούμε την χρήση λογισμικού ασφαλείας. Τα πιο διαδεδομένα λογισμικά είναι τα antivirus και τα firewall. Η χρήση των λογισμικών antivirus αντιμετωπίζει τους ιούς. Έχουν την δυνατότητα να δούνε αν το σύστημα έχει μολυνθεί από ιούς και εάν έχει μολυνθεί τότε έχει την δυνατότητα να τους προσδιορίσουν και στην συνέχεια να τους αφαιρέσουν. Στην συνέχεια, με τον όρο firewall εννοούμε ένα εργαλείο λογισμικού το οποίο έχει τη δυνατότητα να φιλτράρει ότι προσπαθεί να εισέλθει ή να εξέλθει από το πληροφοριακό σύστημα και να ξεχωρίσει αν είναι ασφαλές ή όχι. Έτσι, αντιλαμβανόμαστε ότι με την ραγδαία ανάπτυξη του διαδικτυακού εγκλήματος τα εργαλεία αυτά είναι πολύ σπουδαία για την πρόληψη και την αντιμετώπιση αυτού του φαινομένου. Ωστόσο, μόνο τα τεχνολογικά μέτρα προστασίας δεν μπορούν να αποδώσουν το μέγιστο. Έτσι, ο ρόλος των χρηστών είναι πολύ σημαντικός. Χρειάζεται η ενημέρωση, η εκπαίδευση και η ευαισθητοποίησή τους σχετικά με τους κινδύνους του Διαδικτύου έτσι ώστε να αντιμετωπίζουν με κριτική σκέψη οποιαδήποτε κίνησή τους στο Διαδίκτυο όπως για παράδειγμα, είναι η προστασία των κωδικών πρόσβασης, η αποκάλυψη προσωπικών δεδομένων και η προστασία των πιστωτικών καρτών. Πιο συγκεκριμένα, οι γονείς πρέπει να

είναι ιδιαίτερα προσεκτικοί με τα παιδιά τους και να συζητάνε μαζί τους για την ασφάλεια αλλά και για τους κινδύνους που μπορεί να προκαλέσει το Διαδίκτυο. Τέλος, δυο παράγοντες που μπορούν να βοηθήσουν στη μείωση και την αντιμετώπιση του διαδικτυακού εγκλήματος είναι η νομοθεσία και η Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος. Από την μια οι εξειδικευμένες γνώσεις των μελών της Δίωξης ηλεκτρονικού εγκλήματος και από την άλλη οι νόμοι περί του διαδικτυακού εγκλήματος είναι από τους πιο σημαντικούς λόγους για την εξάλειψη αυτής της νέας μορφής εγκληματικότητας.

ΚΕΦΑΛΑΙΟ 3ο

Η ΕΡΕΥΝΑ ΚΑΙ Η ΣΤΑΤΙΣΤΙΚΗ ΑΝΑΛΥΣΗ

3.1 Δειγματοληπτική έρευνα: Πως πραγματοποιήθηκε

Ο βασικός σκοπός της παρούσας μελέτης εστιάζεται στην αποτύπωση των απόψεων των Ελλήνων χρηστών του διαδικτύου σχετικά με την ενημέρωσή τους, την πρόληψη και την αντιμετώπιση όσον αφορά το Διαδικτυακό έγκλημα. Επιλέξαμε ως μέθοδο τη δειγματοληπτική έρευνα μέσω Διαδικτύου με τη χρήση ηλεκτρονικής φόρμας ερωτηματολογίου. Το ερωτηματολόγιο διανεμήθηκε ηλεκτρονικά σε πολλές περιοχές της Ελλάδας και απαντήθηκε από τις ηλικίες 12 και άνω. Η διαδικασία διανομής, συμπλήρωσης και συλλογής διήρκησε από τις 3 έως τις 20 Φεβρουαρίου του 2015. Τα άτομα που συμμετείχαν στην έρευνα ενημερώθηκαν για το σκοπό της και διαβεβαιώθηκαν για το απόρρητο και την ανωνυμία της διαδικασίας. Το δείγμα της έρευνας αποτέλεσαν 326 άτομα. Το ερωτηματολόγιο παρατίθεται στο παράρτημα στο τέλος της εργασίας.

Πριν την διανομή του ερωτηματολογίου έγινε ο έλεγχος αξιοπιστίας όπου πραγματοποιήθηκε πιλοτική έρευνα, δηλαδή συμπλήρωση του ερωτηματολογίου από 10 άτομα έτσι ώστε να διαπιστώσουμε αν οι ερωτήσεις είναι κατανοητές όσον αφορά τη δομή τους, το νόημα και την σαφήνειά τους. Κατά την πιλοτική έρευνα έγιναν βελτιώσεις σε ορισμένες ερωτήσεις του ερωτηματολογίου σε νοηματικό και συντακτικό επίπεδο.

Μετά την ολοκλήρωση της συμπλήρωσης των ερωτηματολογίων ακολούθησε η κωδικοποίηση των απαντήσεων των ερωτηματολογίων και η είσοδος των δεδομένων σε στατιστικό πακέτο. Καταγράφηκαν και προσδιορίστηκαν τα αποτελέσματα της κάθε ερώτησης ξεχωριστά για κάθε άτομο.

Μια σειρά από διεργασίες στατιστικής ανάλυσης εφαρμόστηκαν για την επεξεργασία και ανάλυση των δεδομένων της έρευνας. Χρησιμοποιήθηκε το Στατιστικό πρόγραμμα SPSS Statistics 22 με το 5% επίπεδο σημαντικότητας. Οι στατιστικές αναλύσεις που αφορούσαν τα περιγραφικά χαρακτηριστικά των μεταβλητών, τις συγκρίσεις των κατηγορικών μεταβλητών καθώς και τις συσχετίσεις των μεταβλητών εφαρμόστηκαν στο στατιστικό πακέτο SPSS και στο Excel Microsoft Office 2007.

3.2 Παρουσίαση αποτελεσμάτων δειγματοληπτικής έρευνας

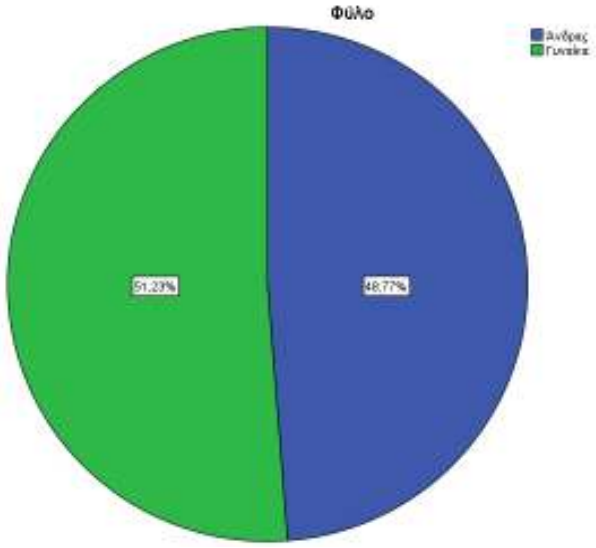
Στο συγκεκριμένο υποκεφάλαιο ακολουθεί η ανάλυση των απαντήσεων που έδωσε το δείγμα στο ερωτηματολόγιο με πίνακες, ραβδογράμματα και πίτες. Αρχικά θα γίνει ανάλυση των ερωτήσεων που αφορούν τα δημογραφικά χαρακτηριστικά του δείγματος και στην συνέχεια θα πραγματοποιηθεί η ανάλυση των υπόλοιπων ερωτήσεων. Για τα αποτελέσματα

που προέκυψαν συνολικά από τη στατιστική ανάλυση και την ερμηνεία τους οφείλουμε να διατυπώσουμε ορισμένες επιφυλάξεις που αφορούν στην πιθανή διαπλοκή του τύπου αίτιο-αιτιατό μεταξύ ορισμένων μεταβλητών.

Συνολικά τα άτομα που συμμετείχαν στην έρευνα και έλαβαν ερωτηματολόγιο είναι 326. Από αυτούς οι 159 (ποσοστό 48.8%) είναι άνδρες και οι 167 (ποσοστό 51.2%) είναι γυναίκες.

Πίνακας 3.1: ***Ερώτηση 1***

Φύλο	**Συχνότητα**	**Ποσοστό**
Άνδρας	159	48.8%
Γυναίκα	167	51.2%
Σύνολο	326	100%



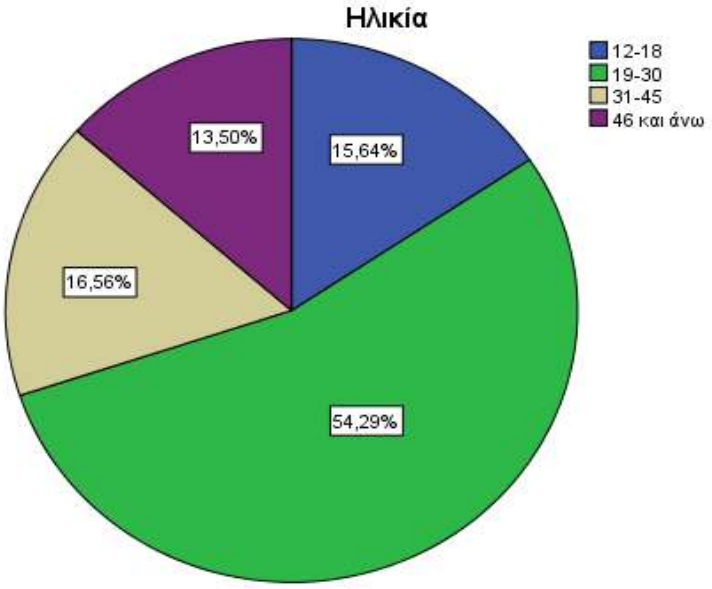
Διάγραμμα 3.1: ***Ερώτηση 1***

Ηλικία

Από το σύνολο του δείγματος, την ηλικιακή ομάδα (12-18 ετών) κατέχουν 51 άτομα (ποσοστό 15.6%), την ηλικιακή ομάδα (19-30 ετών) κατέχουν 177 άτομα (ποσοστό 54.3%), την ηλικιακή ομάδα (31-45 ετών) κατέχουν 54 άτομα (ποσοστό 16.6%) και την ηλικιακή ομάδα άνω των 46 ετών κατέχουν 44 άτομα (ποσοστό 13.5%).

Πίνακας 3.2: ***Ερώτηση 2***

Ηλικία	Συχνότητα	Ποσοστό
12-18	51	15.6%
19-30	177	54.3%
31-45	54	16.6%
46 και άνω	44	13.5%
Σύνολο	326	100%



Διάγραμμα 3.2: ***Ερώτηση 2***

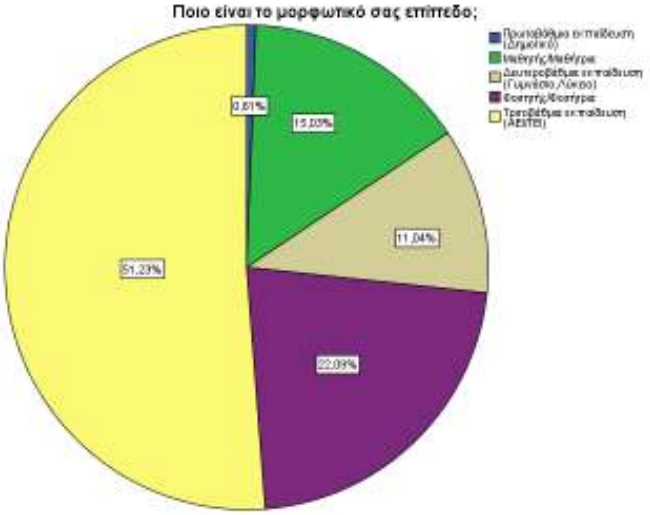
Μορφωτικό επίπεδο

Όσον αφορά το μορφωτικό επίπεδο του δείγματος, 2 άτομα (ποσοστό 0.6%) είναι απόφοιτοι πρωτοβάθμιας εκπαίδευσης, 36 άτομα (ποσοστό 11%) είναι απόφοιτοι δευτεροβάθμιας εκπαίδευσης , 167 άτομα (ποσοστό 51.2%) είναι απόφοιτοι τριτοβάθμιας εκπαίδευσης ενώ 49 άτομα (ποσοστό 15%) είναι μαθητές και 72 άτομα (ποσοστό 22.1%) φοιτητές (ΑΕΙ/ΤΕΙ) χωρίς πτυχίο.

Πίνακας 3.3: ***Ερώτηση 3***

Μορφωτικό επίπεδο	Συχνότητα	Ποσοστό
Πρωτοβάθμια εκπαίδευση(Δημοτικό)	2	0.6%

Μαθητής/Μαθήτρια	49	15%
Δευτεροβάθμια εκπαίδευση(Γυμνάσιο,Λύκειο)	36	11%
Φοιτητής/Φοιτήτρια	72	22.1%
Τριτοβάθμια εκπαίδευση(ΑΕΙ/ΤΕΙ)	167	51.2%
Σύνολο	326	100%



Διάγραμμα 3.3: ***Ερώτηση 3***

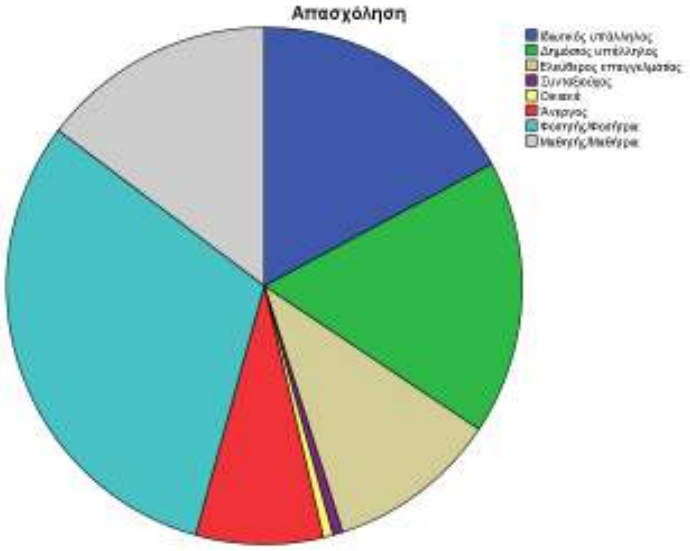
Απασχόληση

Όσον αφορά την απασχόληση των ερωτηθέντων, οι 56 (ποσοστό 17.2%) δήλωσαν ότι είναι ιδιωτικοί υπάλληλοι, οι 56 (ποσοστό 17.2%) δημόσιοι υπάλληλοι, οι 35(ποσοστό 10.7%) ελεύθεροι επαγγελματίες, οι 2 (ποσοστό 0.6%) συνταξιούχοι, οι 2 (ποσοστό 0.6%) ασχολούνται με τα οικιακά, οι 26 (ποσοστό 8%) είναι άνεργοι ενώ οι 101 (ποσοστό 31%) είναι φοιτητές και οι 48 (ποσοστό 14.7%) μαθητές.

Πίνακας 3.4: ***Ερώτηση 4***

Απασχόληση	**Συχνότητα**	**Ποσοστό**
Ιδιωτικός υπάλληλος	56	17.2%
Δημόσιος υπάλληλος	56	17.2%

Ελεύθερος επαγγελματίας	35	10.7%
Συνταξιούχος	2	0.6%
Οικιακά	2	0.6%
Άνεργος	26	8%
Φοιτητής/τρια	101	31%
Μαθητής/τρια	48	14.7%
Σύνολο	326	100%



Διάγραμμα 3.4: ***Ερώτηση 4***

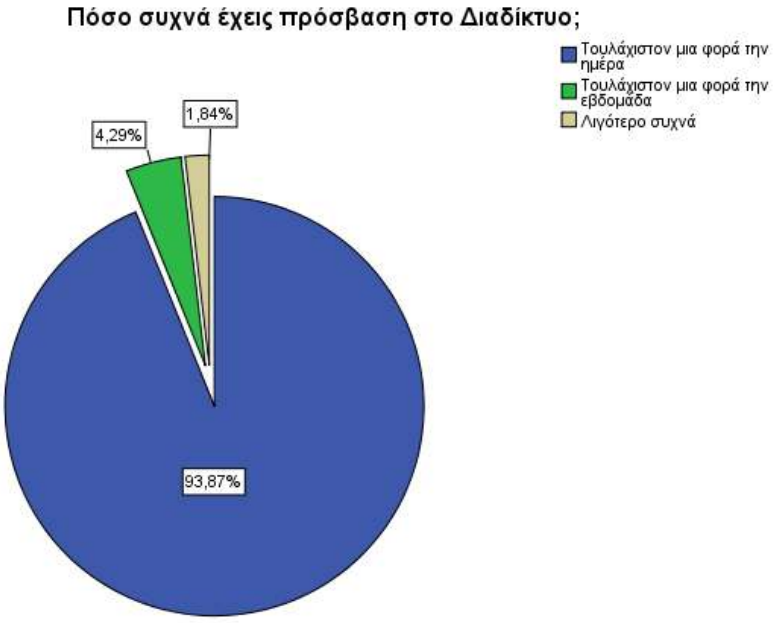
Πόσο συχνά έχεις πρόσβαση στο Διαδίκτυο;

Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα αποτελέσματα της ερώτησης ‘’Πόσο συχνά έχεις πρόσβαση στο Διαδίκτυο;’’.

Οι 306 (ποσοστό 93.9%) από τους 326 απάντησαν ότι έχουν πρόσβαση τουλάχιστον μια φορά την ημέρα, οι 14 (ποσοστό 4.3%) τουλάχιστον μια φορά την εβδομάδα ενώ μόνο οι 6 (ποσοστό 1.8%) έχουν πρόσβαση λιγότερο συχνά.

Πίνακας 3.5: ***Ερώτηση 5***

Πρόσβαση στο Διαδίκτυο	**Συχνότητα**	**Ποσοστό**
Τουλάχιστον μια φορά την ημέρα	306	93.9%
Τουλάχιστον μια φορά την εβδομάδα	14	4.3%
Λιγότερο συχνά	6	1.8%
Σύνολο	326	100%



Διάγραμμα 3.5: ***Ερώτηση 5***

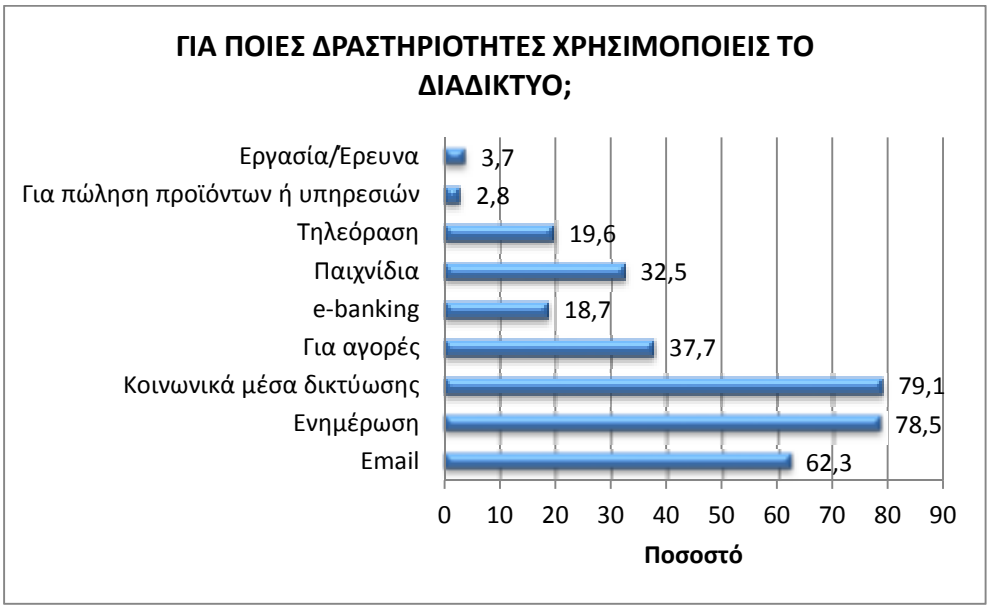
Για ποιες από τις ακόλουθες δραστηριότητες χρησιμοποιείς το Διαδίκτυο;

Στην ερώτηση ‘’Για ποιες από τις ακόλουθες δραστηριότητες χρησιμοποιείς το Διαδίκτυο;’’ οι συχνότητες και τα ποσοστά για την κάθε περίπτωση ξεχωριστά είναι οι ακόλουθες:

Πίνακας 3.6: ***Ερώτηση 6***

Δραστηριότητα	Συχνότητα	Ποσοστό
Email	203	62.3%
Ενημέρωση	256	78.5%
Κοινωνικά μέσα δικτύωσης	258	79.1%
Για αγορές	123	37.7%
e-banking	61	18.7%
Παιχνίδια	106	32.5%
Τηλεόραση	64	19.6%
Για πώληση προϊόντων ή υπηρεσιών	9	2.8%
Εργασία/Ερευνα	12	3.7%

258 ερωτώμενοι (ποσοστό 79.1%) απάντησαν ότι χρησιμοποιούν το Διαδίκτυο για πρόσβαση στα κοινωνικά μέσα δικτύωσης (facebook, twitter, κ.λ.π.), 256 ερωτώμενοι (ποσοστό 78.5%) για ενημέρωση, 203 ερωτώμενοι (ποσοστό 62.3%) για email, 123 ερωτώμενοι (ποσοστό 37.7%) για αγορές μέσω Διαδικτύου, 106 ερωτώμενοι (ποσοστό 32.5%) για να παίζουν παιχνίδια, 64 ερωτώμενοι (ποσοστό 19.6%) για να παρακολουθούν τηλεόραση, 61 ερωτώμενοι (ποσοστό 18.7%) για τραπεζικές και χρηματιστηριακές συναλλαγές(e-banking) ενώ μόνο 9 ερωτώμενοι (ποσοστό 2.8%) απάντησαν ότι το χρησιμοποιούν για πώληση προϊόντων ή υπηρεσιών. Τέλος, 12 ερωτώμενοι (ποσοστό 3.7%) απάντησαν ότι το χρησιμοποιούν για άλλες δραστηριότητες όπως είναι η εργασία/έρευνα.



Διάγραμμα 3.6: ***Ερώτηση 6***

Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος;

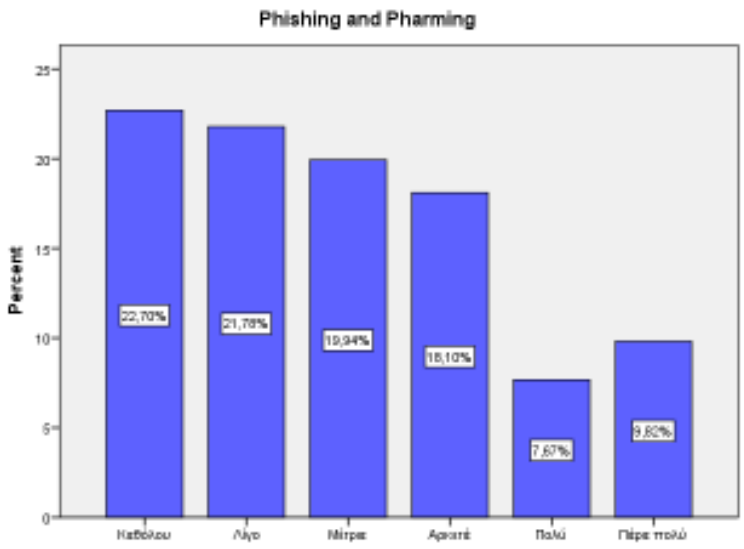
<u>Phishing και Pharming (Ηλεκτρονικό ψάρεμα)</u>

Όσον αφορά το Phishing και Pharming οι απαντήσεις σχετικά με την ενημέρωσή τους κυμαίνονται ως εξής:

Οι 74 (ποσοστό 22.7%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 71 (ποσοστό 21.8%) αισθάνονται λίγο ενημερωμένοι, οι 65 (ποσοστό 19.9%) μέτρια, οι 59 (ποσοστό 18.1%) αρκετά, οι 25 (ποσοστό 7.7%) πολύ και οι 32 (ποσοστό 9.8%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.7: ***Ερώτηση 7(Phishing και Pharming)***

Phishing και Pharming	Συχνότητα	Ποσοστό
Καθόλου	74	22.7%
Λίγο	71	21.8%
Μέτρια	65	19.9%
Αρκετά	59	18.1%
Πολύ	25	7.7%
Πάρα πολύ	32	9.8%
Σύνολο	326	100%



Διάγραμμα 3.7: ***Ερώτηση 7(Phishing και Pharming)***

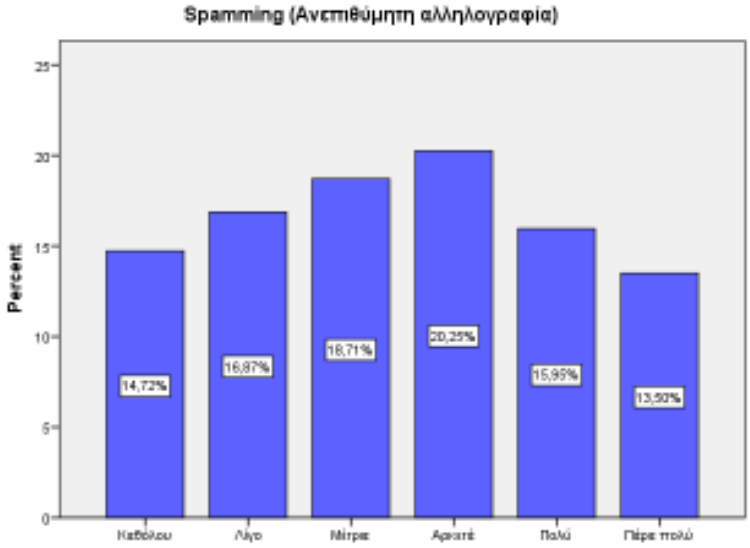
Spamming (Ανεπιθύμητη αλληλογραφία)

Όσον αφορά το Spamming, οι 48 (ποσοστό 14.7%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 55 (ποσοστό 16.9%) αισθάνονται λίγο ενημερωμένοι, οι 61 (ποσοστό 18.7%) μέτρια, οι 66 (ποσοστό 20.2%) αρκετά, οι 52 (ποσοστό 16%) πολύ και οι 44 (ποσοστό 13.5%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.8: ***Ερώτηση 7(Spamming)***

Spamming	Συχνότητα	Ποσοστό
Καθόλου	48	14.7%
Λίγο	55	16.9%
Μέτρια	61	18.7%
Αρκετά	66	20.2%
Πολύ	52	16%

Πάρα πολύ	44	13.5%
Σύνολο	326	100%



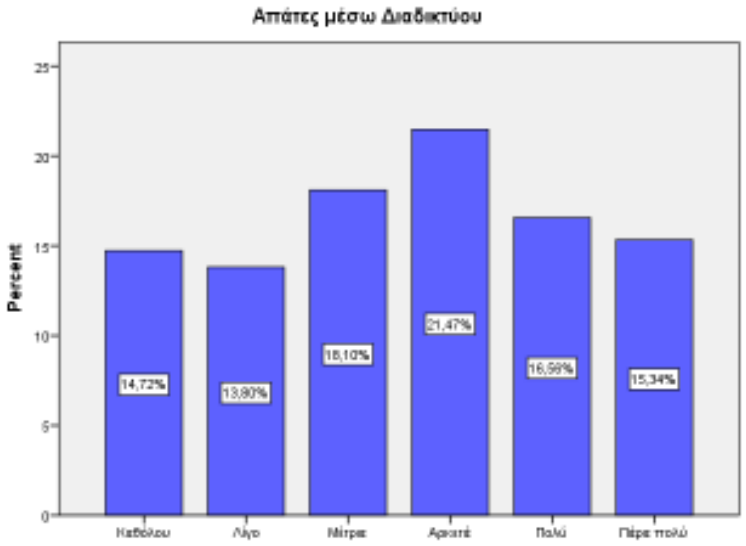
Διάγραμμα 3.8: ***Ερώτηση 7(Spamming)***

<u>Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.)</u>

Όσον αφορά τις Απάτες μέσω Διαδικτύου, οι 48 (ποσοστό 14.7%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 45 (ποσοστό 13.8%) αισθάνονται λίγο ενημερωμένοι, οι 59 (ποσοστό 18.1%) μέτρια, οι 70 (ποσοστό 21.5%) αρκετά, οι 54 (ποσοστό 16.6%) πολύ και οι 50 (ποσοστό 15.3%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.9: ***Ερώτηση 7(Απάτες μέσω Διαδικτύου)***

Απάτες μέσω Διαδικτύου	**Συχνότητα**	**Ποσοστό**
Καθόλου	48	14.7%
Λίγο	45	13.8%
Μέτρια	59	18.1%
Αρκετά	70	21.5%
Πολύ	54	16.6%
Πάρα πολύ	50	15.3%
Σύνολο	326	100%



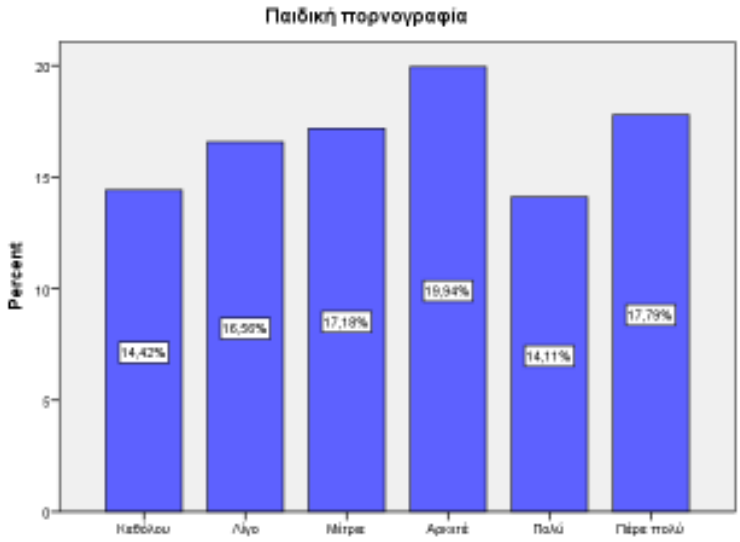
Διάγραμμα 3.9: ***Ερώτηση 7(Απάτες μέσω Διαδικτύου)***

Παιδική πορνογραφία

Όσον αφορά την Παιδική πορνογραφία, οι 47 (ποσοστό 14.4%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 54 (ποσοστό 16.6%) αισθάνονται λίγο ενημερωμένοι, οι 56 (ποσοστό 17.2%) μέτρια, οι 65 (ποσοστό 19.9%) αρκετά, οι 46 (ποσοστό 14.1%) πολύ και οι 58 (ποσοστό 17.8%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.10: ***Ερώτηση 7(Παιδική πορνογραφία)***

Παιδική πορνογραφία	Συχνότητα	Ποσοστό
Καθόλου	47	14.4%
Λίγο	54	16.6%
Μέτρια	56	17.2%
Αρκετά	65	19.9%
Πολύ	46	14.1%
Πάρα πολύ	58	17.8%
Σύνολο	326	100%



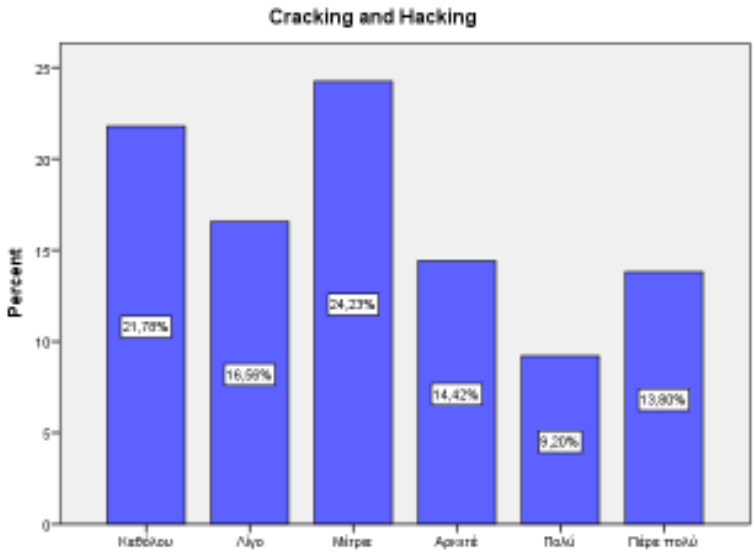
Διάγραμμα 3.10: ***Ερώτηση 7(Παιδική πορνογραφία)***

Cracking και Hacking

Όσον αφορά το Cracking και Hacking, οι 71 (ποσοστό 21.8%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 54 (ποσοστό 16.6%) αισθάνονται λίγο ενημερωμένοι, οι 79 (ποσοστό 24.2%) μέτρια, οι 47 (ποσοστό 14.4%) αρκετά, οι 30 (ποσοστό 9.2%) πολύ και οι 45 (ποσοστό 13.8%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.11: ***Ερώτηση 7(Cracking και Hacking)***

Cracking και Hacking	Συχνότητα	Ποσοστό
Καθόλου	71	21.8%
Λίγο	54	16.6%
Μέτρια	79	24.2%
Αρκετά	47	14.4%
Πολύ	30	9.2%
Πάρα πολύ	45	13.8%
Σύνολο	326	100%



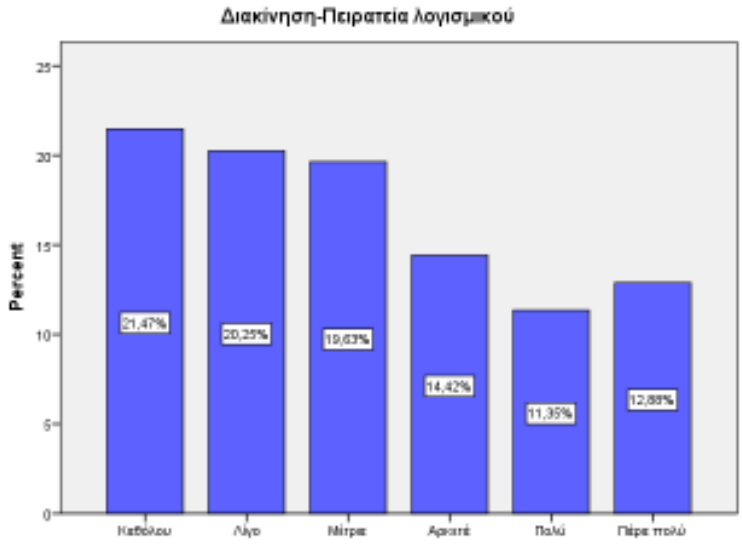
Διάγραμμα 3.11: ***Ερώτηση 7(Cracking και Hacking)***

Διακίνηση-Πειρατεία λογισμικού

Όσον αφορά την Διακίνηση-Πειρατεία λογισμικού, οι 70 (ποσοστό 21.5%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 66 (ποσοστό 20.2%) αισθάνονται λίγο ενημερωμένοι, οι 64 (ποσοστό 19.6%) μέτρια, οι 47 (ποσοστό 14.4%) αρκετά, οι 37 (ποσοστό 11.3%) πολύ και οι 42 (ποσοστό 12.9%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.12: ***Ερώτηση 7(Διακίνηση-Πειρατεία λογισμικού)***

Διακίνηση/Πειρατεία λογισμικού	**Συχνότητα**	**Ποσοστό**
Καθόλου	70	21.5%
Λίγο	66	20.2%
Μέτρια	64	19.6%
Αρκετά	47	14.4%
Πολύ	37	11.3%
Πάρα πολύ	42	12.9%
Σύνολο	326	100%



Διάγραμμα 3.12: ***Ερώτηση 7 (Διακίνηση-Πειρατεία λογισμικού)***

<u>Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων</u>

Όσον αφορά την Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, οι 102 (ποσοστό 31.3%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 62 (ποσοστό 19%) αισθάνονται λίγο ενημερωμένοι, οι 65 (ποσοστό 19.9%) μέτρια, οι 46 (ποσοστό 14.1%) αρκετά, οι 22 (ποσοστό 6.7%) πολύ και οι 29 (ποσοστό 8.9%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.13: ***Ερώτηση 7 (Διακίνηση ναρκωτικών)***

Διακίνηση ναρκωτικών	**Συχνότητα**	**Ποσοστό**
Καθόλου	102	31.3%
Λίγο	62	19%
Μέτρια	65	19.9%
Αρκετά	46	14.1%
Πολύ	22	6.7%
Πάρα πολύ	29	8.9%
Σύνολο	326	100%

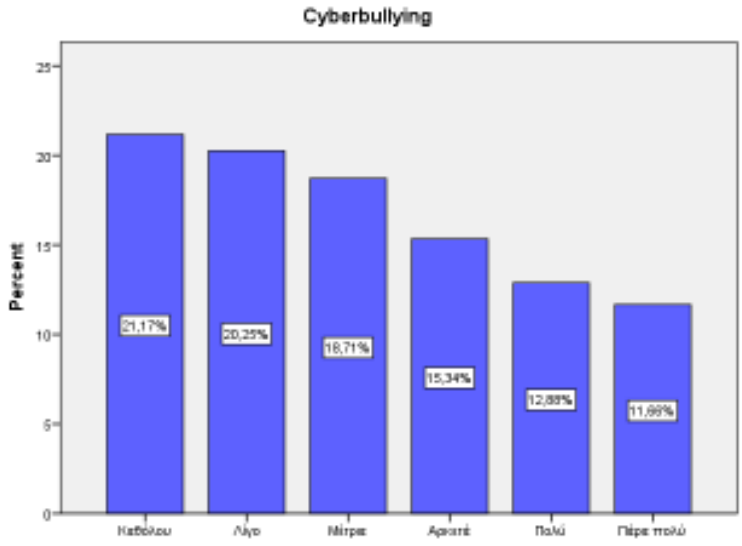
Διάγραμμα 3.13: ***Ερώτηση 7 (Διακίνηση ναρκωτικών)***

Cyberbullying (Διαδικτυακός εκφοβισμός)

Όσον αφορά το Cyberbullying, οι 69 (ποσοστό 21.2%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 66 (ποσοστό 20.2%) αισθάνονται λίγο ενημερωμένοι, οι 61 (ποσοστό 18.7%) μέτρια, οι 50 (ποσοστό 15.3%) αρκετά, οι 42 (ποσοστό 12.9%) πολύ και οι 38 (ποσοστό 11.7%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.14: ***Ερώτηση 7 (Cyberbullying)***

Cyberbullying	Συχνότητα	Ποσοστό
Καθόλου	69	21.2%
Λίγο	66	20.2%
Μέτρια	61	18.7%
Αρκετά	50	15.3%
Πολύ	42	12.9%
Πάρα πολύ	38	11.7%
Σύνολο	326	100%



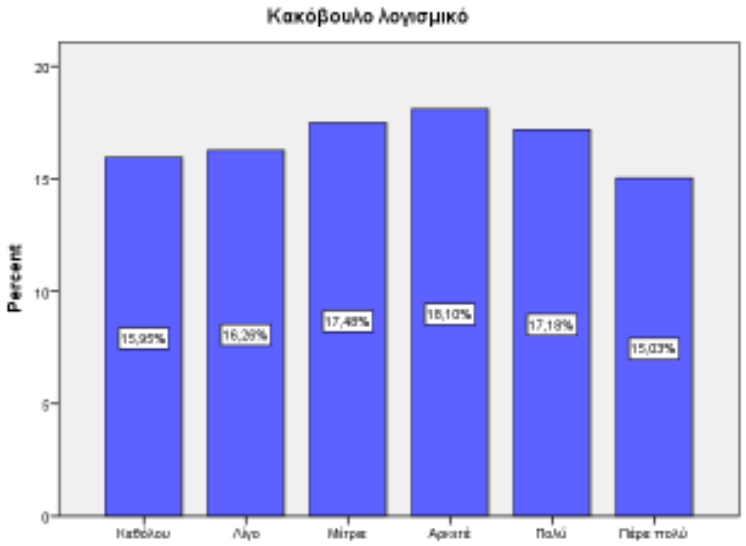
Διάγραμμα 3.14: ***Ερώτηση 7 (Cyberbullying)***

<u>Κακόβουλο λογισμικό (Ιοί, σκουλήκια, δούρειοι ίπποι)</u>

Όσον αφορά το Κακόβουλο λογισμικό, οι 52 (ποσοστό 16%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 53 (ποσοστό 16.3%) αισθάνονται λίγο ενημερωμένοι, οι 57 (ποσοστό 17.5%) μέτρια, οι 59 (ποσοστό 18.1%) αρκετά, οι 56 (ποσοστό 17.2%) πολύ και οι 49 (ποσοστό 15%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.15: ***Ερώτηση 7 (Κακόβουλο λογισμικό)***

Κακόβουλο λογισμικό	**Συχνότητα**	**Ποσοστό**
Καθόλου	52	16%
Λίγο	53	16.3%
Μέτρια	57	17.5%
Αρκετά	59	18.1%
Πολύ	56	17.2%
Πάρα πολύ	49	15%
Σύνολο	326	100%



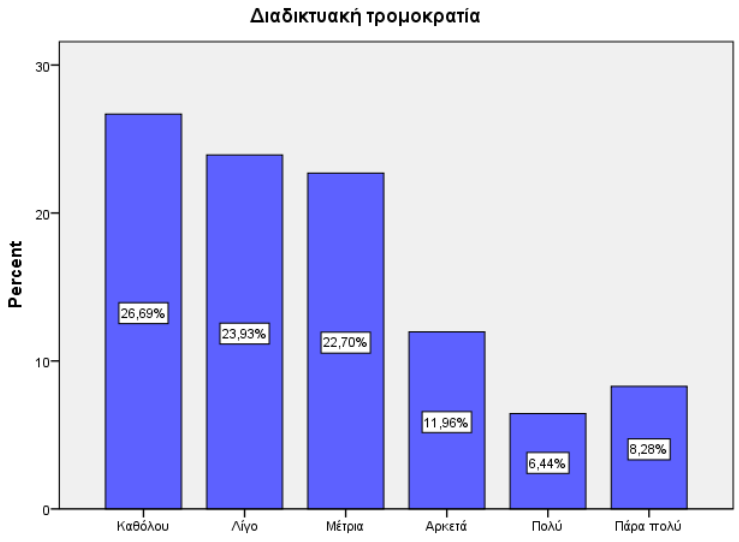
Διάγραμμα 3.15: ***Ερώτηση 7 (Κακόβουλο λογισμικό)***

Διαδικτυακή τρομοκρατία

Όσον αφορά την Διαδικτυακή τρομοκρατία, οι 87 (ποσοστό 26.7%) δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής διαδικτυακού εγκλήματος, οι 78 (ποσοστό 23.9%) αισθάνονται λίγο ενημερωμένοι, οι 74 (ποσοστό 22.7%) μέτρια, οι 39 (ποσοστό 12%) αρκετά, οι 21 (ποσοστό 6.4%) πολύ και οι 27 (ποσοστό 8.3%) αισθάνονται πάρα πολύ ενημερωμένοι.

Πίνακας 3.16: ***Ερώτηση 7 (Διαδικτυακή τρομοκρατία)***

Διαδικτυακή τρομοκρατία	**Συχνότητα**	**Ποσοστό**
Καθόλου	87	26.7%
Λίγο	78	23.9%
Μέτρια	74	22.7%
Αρκετά	39	12%
Πολύ	21	6.4%
Πάρα πολύ	27	8.3%
Σύνολο	326	100%



Διάγραμμα 3.16: ***Ερώτηση 7 (Διαδικτυακή τρομοκρατία)***

Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;

Στην ερώτηση ‘’Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;’’ οι 93(ποσοστό 28.5%) απάντησαν το Κακόβουλο λογισμικό, οι 54(ποσοστό 16.6%) το Spamming, οι 50(ποσοστό 15.3%) την Παιδική πορνογραφία, οι 36(ποσοστό 11%) τις Απάτες μέσω Διαδικτύου, οι 26 (ποσοστό 8%) το Cracking και Hacking, οι 24(ποσοστό 7.4%) το Phishing και Pharming, οι 24(ποσοστό 7.4%) την Διακίνηση-Πειρατεία λογισμικού, οι 12(ποσοστό 3.7%) το Cyberbullying, οι 4(ποσοστό 1.2%) τη Διαδικτυακή τρομοκρατία , μόνο 1(ποσοστό 0.3%) την Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων ενώ 2 άτομα (ποσοστό 0.6%) δεν ξέρουν ποια είναι η πιο συχνή μορφή του διαδικτυακού εγκλήματος.

Παρατηρούμε ότι η πιο συχνή μορφή είναι το Κακόβουλο λογισμικό ενώ η λιγότερο συχνή η Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων.

Πίνακας 3.17: ***Ερώτηση 8***

Μορφές	Συχνότητα	Ποσοστό
Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")	24	7.4%
Spamming(Ανεπιθύμητη αλληλογραφία)	54	16.6%
Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος, Πιστωτικές κάρτες, κ.λ.π.)	36	11%
Παιδική πορνογραφία	50	15.3%
Cracking και Hacking	26	8%

Διακίνηση-Πειρατεία λογισμικού	24	7.4
Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων	1	0.3%
Cyberbullying(Διαδικτυακός εκφοβισμός)	12	3.7%
Κακόβουλο λογισμικό (Ιοί, σκουλήκια, δούρειοι ίπποι)	93	28.5%
Διαδικτυακή τρομοκρατία	4	1.2%
Δεν ξέρω	2	0.6%
Σύνολο	326	100%

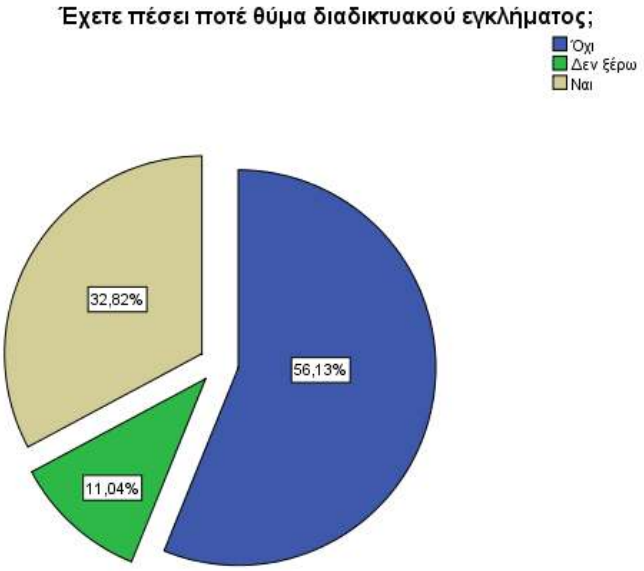
Διάγραμμα 3.17: ***Ερώτηση 8***

Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος;

Στην ερώτηση αν έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος το 56.1% απάντησε ότι δεν έχει πέσει ποτέ θύμα διαδικτυακού εγκλήματος ,το 32.8% δήλωσε ότι έχει πέσει θύμα, ενώ ιδιαίτερο ενδιαφέρον παρατηρείται στο ποσοστό των ανθρώπων που δεν ξέρουν αν έχουν πέσει ποτέ θύμα διαδικτυακού εγκλήματος που αγγίζει το 11%. Το συγκεκριμένο ποσοστό δηλώνει άγνοια για το αν έχει πέσει ποτέ θύμα διαδικτυακού εγκλήματος. Το σύνολο αυτών των ανθρώπων μπορεί να έχουν πέσει θύμα και να μην το έχουν καταλάβει.

Πίνακας 3.18: ***Ερώτηση 9***

Έχετε πέσει θύμα;	Συχνότητα	Ποσοστό
Ναι	107	32.8%
Όχι	183	56.1%
Δεν ξέρω	36	11%
Σύνολο	326	100%



Διάγραμμα 3.18: ***Ερώτηση 9***

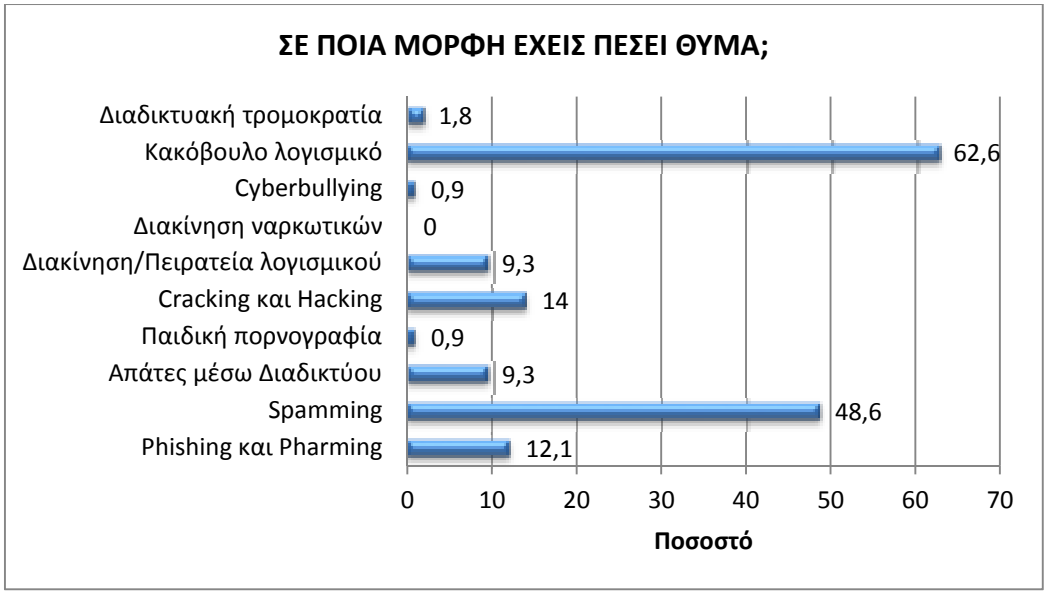
Αν ναι, σε ποια μορφή;

Από αυτούς που έχουν πέσει θύμα διαδικτυακού εγκλήματος, το 62.6% έχει πέσει στην μορφή Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι), το 48.6% στο Spamming(Ανεπιθύμητη αλληλογραφία), το 14% στο Cracking και Hacking, το 12.1% στο Phishing και Pharming, το 9.3% στις Απάτες μέσω Διαδικτύου, το 9.3% στη Διακίνηση-Πειρατεία λογισμικού, το 1.8% στην Διαδικτυακή τρομοκρατία, το 0.9% στην Παιδική πορνογραφία, το 0.9% στο Cyberbullying (Διαδικτυακός εκφοβισμός) ενώ κανένας δεν έχει πέσει θύμα στην Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων.

Πίνακας 3.19: ***Ερώτηση 10***

Μορφές	Ποσοστό
Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")	12.1%
Spamming(Ανεπιθύμητη αλληλογραφία)	48.6%
Απάτες μέσω Διαδικτύου(Διαδικτυακός	9.3%

τζόγος, Πιστωτικές κάρτες,κλπ)	
Παιδική πορνογραφία	0.9%
Cracking και Hacking	14%
Διακίνηση-Πειρατεία λογισμικού	9.3%
Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων	0%
Cyberbullying(Διαδικτυακός εκφοβισμός)	0.9%
Κακόβουλο λογισμικό (Ιοί,σκουλήκια,δούρειοι ίπποι)	62.6%
Διαδικτυακή τρομοκρατία	1.8%



Διάγραμμα 3.19: ***Ερώτηση 10***

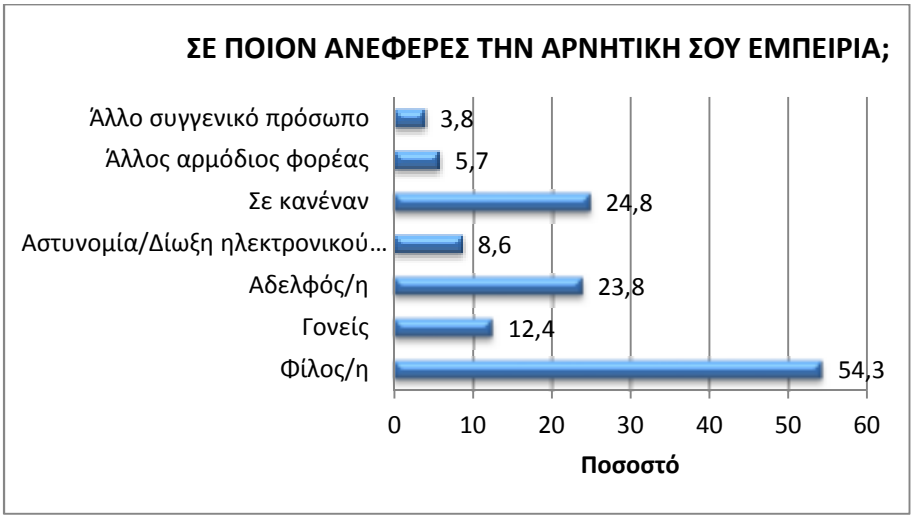
Αν έχεις πέσει θύμα διαδικτυακού εγκλήματος σε ποιον ανέφερες την αρνητική σου εμπειρία;

Από αυτούς που έχουν πέσει θύμα, οι 57(53.2%) το ανέφεραν σε κάποιον φίλο, οι 26(24.2%) δεν το ανέφεραν σε κανέναν, οι 25(23.3%) το ανέφεραν στον αδελφό/ή τους, οι 13(12.1%) στους γονείς, οι 9(8.4%) στην Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος ενώ οι 6(5.6%) το ανέφεραν σε κάποιον άλλο αρμόδιο φορέα και οι 4(3.7%) σε άλλο συγγενικό πρόσωπο.

Πίνακας 3.20: ***Ερώτηση 11***

Σε ποιον το ανέφερες;	**Συχνότητα**	**Ποσοστό**
Φίλος/η	57	53.2%
Γονείς	13	12.1%

Αδελφός/η	25	23.3%
Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος	9	8.4%
Σε κανέναν	26	24.2%
Άλλος αρμόδιος φορέας	6	5.6%
Άλλο συγγενικό πρόσωπο	4	3.7%



Διάγραμμα 3.20: ***Ερώτηση 11***

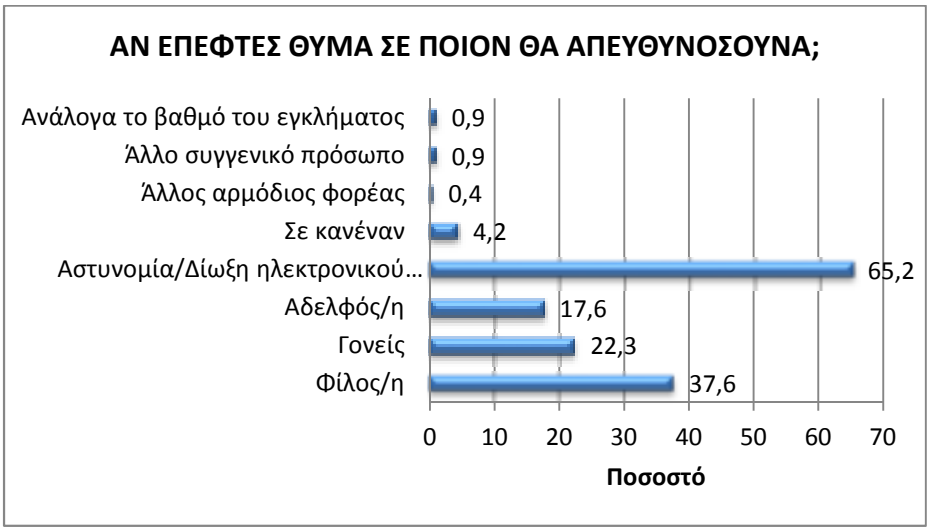
Αν δεν έχεις πέσει θύμα διαδικτυακού εγκλήματος ,τότε αν έπεφτες που θα απευθυνόσουνα;

Όσοι δεν έχουν πέσει θύμα απάτης δήλωσαν ότι αν έπεφταν, το 65.2% θα απευθυνόταν στην Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος, το 37.6% σε κάποιον φίλο, το 22.3% στους γονείς, το 17.6% στον αδελφό/ή, το 4.2% σε κανέναν, το 0.9% σε άλλο συγγενικό πρόσωπο, το 0.4% σε άλλον αρμόδιο φορέα ενώ το 0.9% απάντησε ανάλογα το βαθμό του εγκλήματος.

Πίνακας 3.21: ***Ερώτηση 12***

Σε ποιον θα απευθυνόσουνα;	**Συχνότητα**	**Ποσοστό**
Φίλος/η	79	37.6%
Γονείς	47	22.3%
Αδελφός/η	37	17.6%
Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος	137	65.2%
Σε κανέναν	9	4.2%
Άλλος αρμόδιος φορέας	1	0.4%

Άλλο συγγενικό πρόσωπο	2	0.9%
Ανάλογα το βαθμό του εγκλήματος	2	0.9%



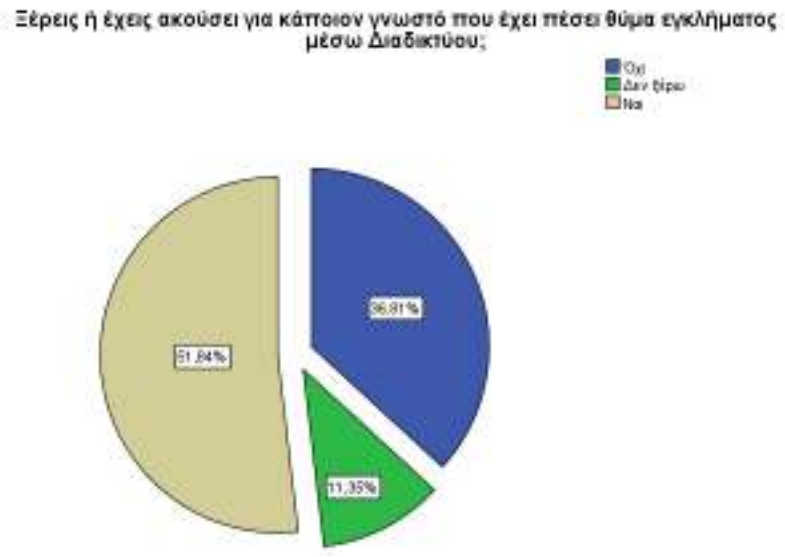
Διάγραμμα 3.21: ***Ερώτηση 12***

Ξέρεις ή έχεις ακούσει για κάποιον γνωστό που έχει πέσει θύμα εγκλήματος μέσω Διαδικτύου;

Στην ερώτηση αν γνωρίζουν ή αν έχουν ακούσει για κάποιον που να έχει πέσει θύμα απάτης, το 51.8% απάντησε ‘’Ναι’’, το 36.8% ‘’Όχι‘’ ενώ το 11.3% απάντησε ότι δεν ξέρει.

Πίνακας 3.22: ***Ερώτηση 13***

Ξέρεις κάποιον που έχει πέσει θύμα;	**Συχνότητα**	**Ποσοστό**
Ναι	169	51.8%
Όχι	120	36.8%
Δεν ξέρω	37	11.3%
Σύνολο	326	100%



Διάγραμμα 3.22: ***Ερώτηση 13***

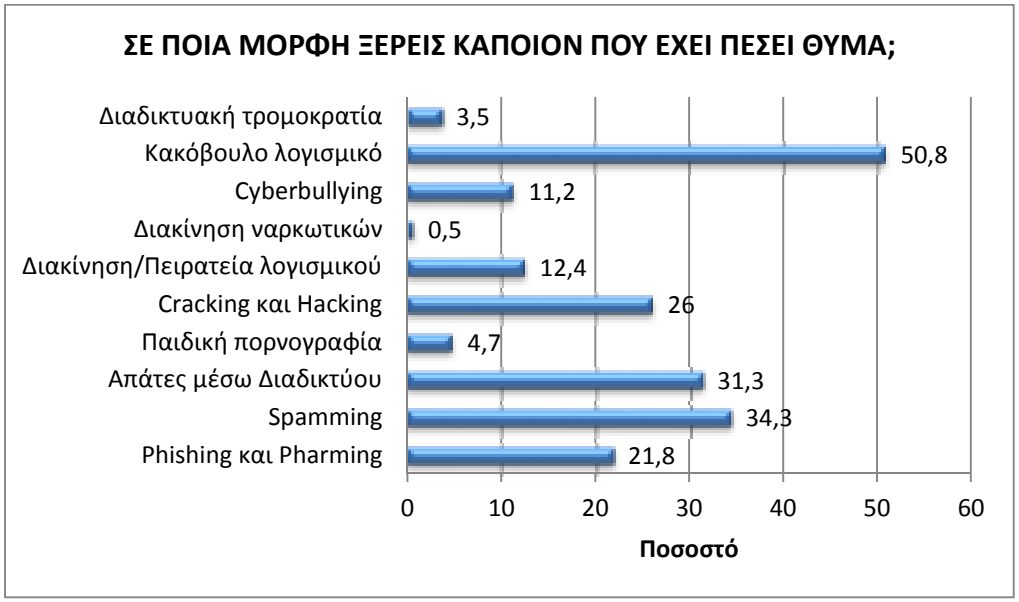
Αν ναι, σε ποια μορφή;

Από αυτούς που ξέρουν κάποιον που έχει πέσει θύμα, το 50.8% απαντάει στο Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι), το 34.3% στο Spamming(Ανεπιθύμητη αλληλογραφία), το 31.3% στις Απάτες μέσω Διαδικτύου, το 26% στο Cracking και Hacking, το 21.8% στο Phishing και Pharming, το 12.4% στην Διακίνηση-Πειρατεία λογισμικού, το 11.2% στο Cyberbullying (Διαδικτυακός εκφοβισμός), το 4.7% στην Παιδική πορνογραφία, το 3.5% στην Διαδικτυακή τρομοκρατία και το 0.5% στην Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων.

Πίνακας 3.23: ***Ερώτηση 14***

Μορφές	**Συχνότητα**	**Ποσοστό**
Phishing και Pharming	37	21.8%
Spamming	58	34.3%
Απάτες μέσω Διαδικτύου	53	31.3%
Παιδική πορνογραφία	8	4.7%
Cracking και Hacking	44	26%
Διακίνηση-Πειρατεία λογισμικού	21	12.4%

Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων	1	0.5%
Cyberbullying(Διαδικτυακός εκφοβισμός)	19	11.2%
Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι)	86	50.8%
Διαδικτυακή τρομοκρατία	6	3.5%



Διάγραμμα 3.23: ***Ερώτηση 14***

Κατά την πλοήγηση σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις;

Όσον αφορά το πόσο αισθάνονται ότι κινδυνεύουν, οι 31(9.5%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 102(31.3%) λίγο, οι 107(32.8%) μέτρια, οι 69(21.2%) αρκετά, οι 14(4.3%) πολύ και οι 3(0.9%) πάρα πολύ.

Πίνακας 3.24: ***Ερώτηση 15***

Πόσο αισθάνεσαι ότι κινδυνεύεις;	**Συχνότητα**	**Ποσοστό**
Καθόλου	31	9.5%
Λίγο	102	31.3%
Μέτρια	107	32.8%

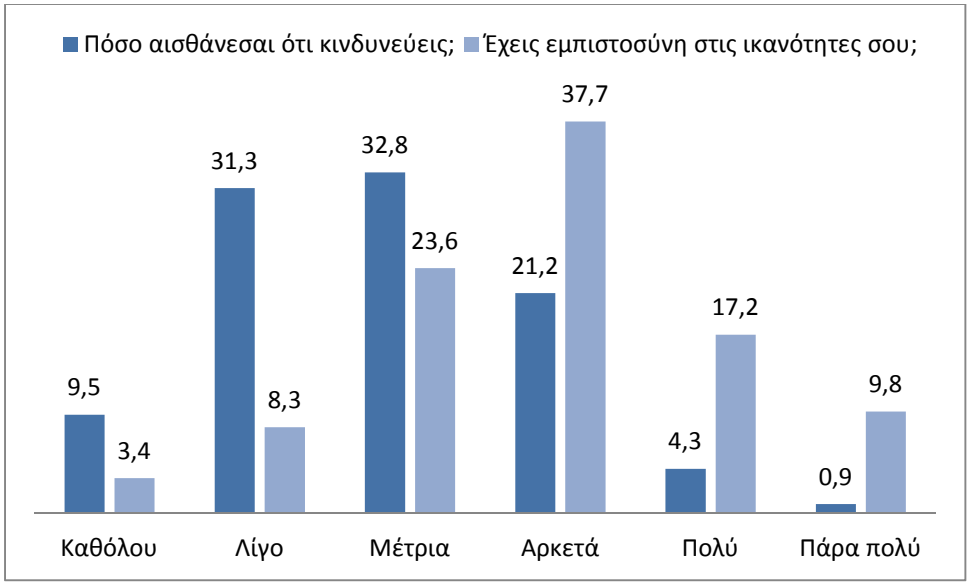
Αρκετά	69	21.2%
Πολύ	14	4.3%
Πάρα πολύ	3	0.9%
Σύνολο	326	100%

Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο;

Όσον αφορά την εμπιστοσύνη που δείχνουν στις ικανότητές τους, οι 11(3.4%) δεν έχουν καθόλου, οι 27(8.3%) λίγο, οι 77(23.6%) μέτρια, οι 123(37.7%) αρκετά, οι 56(17.2%) πολύ και οι 32(9.8%) πάρα πολύ.

Πίνακας 3.25: ***Ερώτηση 16***

Έχεις εμπιστοσύνη στις ικανότητές σου;	**Συχνότητα**	**Ποσοστό**
Καθόλου	11	3.4%
Λίγο	27	8.3%
Μέτρια	77	23.6%
Αρκετά	123	37.7%
Πολύ	56	17.2%
Πάρα πολύ	32	9.8%
Σύνολο	326	100%



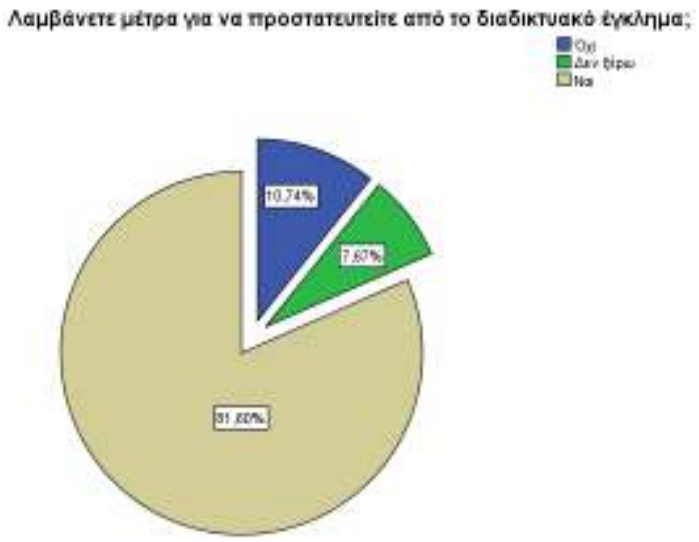
Διάγραμμα 3.24: ***Ερώτηση 15 και Ερώτηση 16***

Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα;

Από το σύνολο του δείγματος, οι 266(81.6%) απάντησαν ότι λαμβάνουν μέτρα προστασίας για το διαδικτυακό έγκλημα, οι 35(10.7%) απάντησαν ότι δεν λαμβάνουν ενώ οι 25(7.7%) δεν ξέρουν αν λαμβάνουν μέτρα προστασίας.

Πίνακας 3.26: ***Ερώτηση 17***

Λαμβάνετε μέτρα προστασίας;	**Συχνότητα**	**Ποσοστό**
Ναι	266	81.6%
Όχι	35	10.7%
Δεν ξέρω	25	7.7%
Σύνολο	326	100%



Διάγραμμα 3.25: ***Ερώτηση 17***

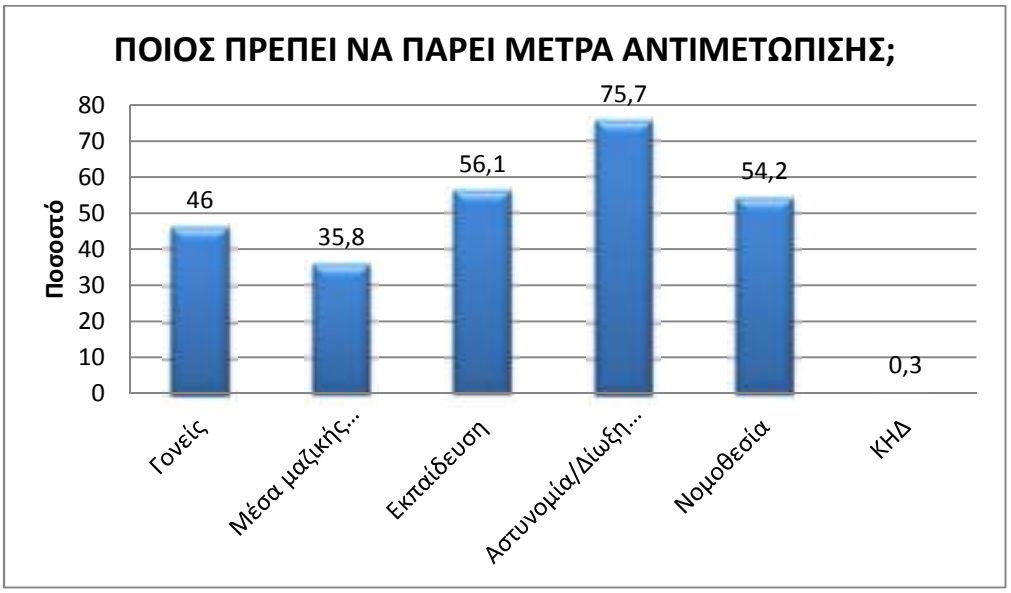
Αν ναι, τι μέτρα;

Από αυτούς που λαμβάνουν μέτρα προστασίας από το διαδικτυακό έγκλημα, το 89.4% λαμβάνει τεχνολογική προστασία, το 63.1% λαμβάνει προστασία των κωδικών πρόσβασης, το 59.7% δεν αποκαλύπτει προσωπικά δεδομένα ενώ το 34.5% διαβάζει πάντα τους όρους χρήσης πριν κάνει εγγραφή.

Διάγραμμα 3.26: ***Ερώτηση 18***

Ποιος πιστεύετε ότι πρέπει να πάρει μέτρα αντιμετώπισης για το διαδικτυακό έγκλημα;

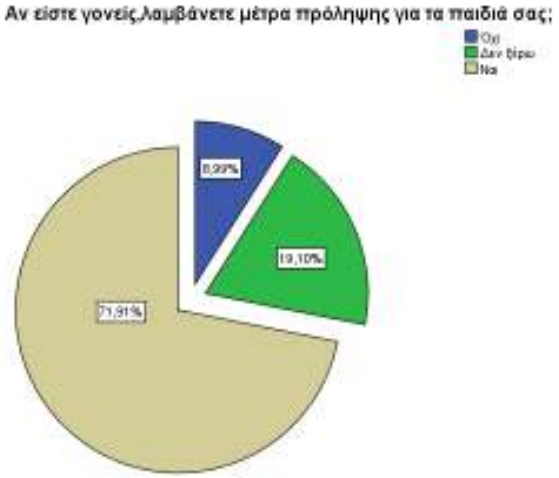
Από το σύνολο των ερωτηθέντων, οι 247(75.7%) πιστεύουν ότι η Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος πρέπει να πάρει μέτρα αντιμετώπισης για το διαδικτυακό έγκλημα, οι 183(56.1%) η εκπαίδευση, οι 177(54.2%) η νομοθεσία, οι 150(46%) οι γονείς, οι 117(35.8%) τα ΜΜΕ και 1 άτομο(0.3%) πιστεύει ότι το ΚΗΔ πρέπει να λάβει μέτρα αντιμετώπισης.



Διάγραμμα 3.27: ***Ερώτηση 19***

Αν είστε γονείς, λαμβάνετε μέτρα πρόληψης για τα παιδιά σας;

Από το σύνολο των γονιών το 71.9% λαμβάνει μέτρα, το 19.1% δεν λαμβάνει μέτρα ενώ το 9% δεν ξέρει αν λαμβάνει μέτρα προστασίας για τα παιδιά τους.



Διάγραμμα 3.28: ***Ερώτηση 20***

ΚΕΦΑΛΑΙΟ 4ο

ΕΛΕΓΧΟΣ ΑΝΕΞΑΡΤΗΣΙΑΣ

4.1 Πίνακες Συνάφειας και Έλεγχοι Υποθέσεων

Ο πίνακας συνάφειας ο οποίος είναι ένας διδιάστατος ή πολυδιάστατος πίνακας αποτελείται από γραμμές και στήλες που ορίζονται από τις κατηγορίες των δυο μεταβλητών και εκφράζει την συνάφεια δυο ή περισσοτέρων μεταβλητών. Είναι ιδιαίτερα χρήσιμος όταν έχουμε ονομαστικές μεταβλητές και θέλουμε να ελέγξουμε αν είναι συσχετισμένες. Μας δίνει μια συνοπτική περιγραφή της κοινής κατανομής των δυο ποιοτικών μεταβλητών. Συνεπώς, στην επόμενη ενότητα βλέπουμε ορισμένους πίνακες συνάφειας μεταξύ ορισμένων μεταβλητών της έρευνας.

Στις περιπτώσεις των στατιστικών ελέγχων σημαντικότητας η παρατηρούμενη στάθμη σημαντικότητας (p-value) υπολογίστηκε με τη δοκιμασία X^2 του Pearson (Pearson's chi-squared test) και όπου αυτό δεν ήταν δυνατόν με το ακριβές τεστ του Monte Carlo (exact Monte-Carlo test) σε διάστημα εμπιστοσύνης 95% και 10000 επαναλήψεις. Με το ακριβές τεστ του Monte-Carlo ενισχύεται η εγκυρότητα των συμπερασμάτων σε περίπτωση που δεν ικανοποιούνται οι προϋποθέσεις εφαρμογής του ελέγχου X^2 του Pearson. Η μέθοδος Monte Carlo είναι μια κατηγορία υπολογιστικών αλγορίθμων που στηρίζονται σε επαναλαμβανόμενες τυχαίες δειγματοληψίες για τον υπολογισμό των αποτελεσμάτων τους. Επιτρέπει την εκτίμηση ακριβούς επιπέδου σημαντικότητας χωρίς να βασίζεται σε συμπεράσματα ασυμπτωτικών μεθόδων.

Για τον στατιστικό έλεγχο ανεξαρτησίας X^2 είναι απαραίτητος ο προσδιορισμός των αναμενόμενων συχνοτήτων έτσι ώστε να εξετάσουμε αν υπάρχει διαφορά μεταξύ των πραγματικών και των αναμενόμενων συχνοτήτων. Οι αναμενόμενες συχνότητες αναφέρονται στις συχνότητες που ο ερευνητής θα διαπίστωνε εάν ίσχυε η μηδενική υπόθεση (τα χαρακτηριστικά είναι ανεξάρτητα). Ο έλεγχος ανεξαρτησίας X^2 χρησιμοποιείται για την ανάλυση ποιοτικών μεταβλητών και οι προϋποθέσεις εφαρμογής του είναι:

- Οι παρατηρήσεις πρέπει να είναι ανεξάρτητες.
- Οι μεταβλητές πρέπει να είναι ποιοτικές.
- Θα πρέπει το πολύ το 20% των κελιών του πίνακα να έχει αναμενόμενη συχνότητα κάτω από 5.
- Η μικρότερη αναμενόμενη συχνότητα να είναι μεγαλύτερη ή ίση της μονάδας.

Ο τύπος υπολογισμού του ελέγχου X^2 είναι:

$$X^2=\sum_{i,j}\frac{(n_{ij}-\theta_{ij})^2}{\theta_{ij}}$$

όπου:

n_{ij}: η παρατηρούμενη συχνότητα στο κελί (i,j)

θ_{ij}: η αναμενόμενη συχνότητα στο κελί (i,j)

Ο έλεγχος υποθέσεων περιλαμβάνει την μηδενική υπόθεση H0 και την εναλλακτική υπόθεση H1 όπου:

H0: Τα χαρακτηριστικά X και Y του δείγματος κατανέμονται ανεξάρτητα στον πληθυσμό.

H1: Τα χαρακτηριστικά X και Y του δείγματος δεν κατανέμονται ανεξάρτητα στον πληθυσμό.

4.2 Παρουσίαση αποτελεσμάτων από την έλεγχο ανεξαρτησίας X^2.

Στο σημείο αυτό θα παρουσιαστούν ορισμένοι πίνακες συνάφειας και μια σειρά από ζεύγη μεταβλητών τα οποία ελέγχθηκαν ως προς την συσχέτισή τους. Στο τέλος αυτού του κεφαλαίου υπάρχει ένας πίνακας ο οποίος έχει συγκεντρωμένα όλα τα αποτελέσματα της παρουσίασης από την δοκιμασία X^2.

Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος;

Στην συγκεκριμένη ερώτηση, θέλουμε να εξερευνήσουμε τη σχέση φύλου και απαντήσεων για την κάθε μορφή διαδικτυακού εγκλήματος ξεχωριστά.

Φύλο-Phishing και Pharming

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Phishing και Pharming, από το σύνολο των ανδρών οι 31(19.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 27(17%) αισθάνονται λίγο ενημερωμένοι, οι 28(17.6%) μέτρια, οι 34(21.4%) αρκετά, οι 16(10.1%) πολύ και οι 23(14.5%) πάρα πολύ. Από το σύνολο των γυναικών οι 43(25.7%) δεν αισθάνονται καθόλου ενημερωμένες, οι 44(26.3%) αισθάνονται λίγο, οι 37(22.2%) μέτρια, οι 25(15%) αρκετά, οι 9(5.4%) πολύ και οι 9(5.4%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

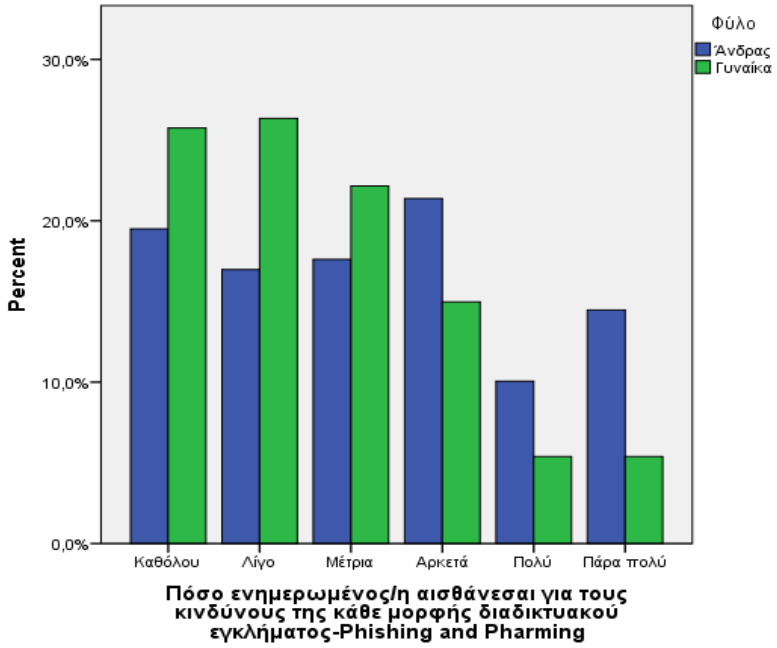
Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Phishing και Pharming και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για

τους κινδύνους της μορφής Phishing και Pharming, δηλαδή να διαφέρουν οι απόψεις και των δυο φύλων (X^2=16.534, df=5, p=0.005).

Πίνακας 4.1: *Πίνακας Συνάφειας Συσχέτισης Φύλου-Phishing και Pharming*

Phishing_Pharming1 * Φύλο Crosstabulation

			Φύλο		
			Άνδρας	Γυναίκα	Total
	Καθόλου	Count	31	43	74
		Expected Count	36,1	37,9	74,0
		% of Total	9,5%	13,2%	22,7%
	Λίγο	Count	27	44	71
		Expected Count	34,6	36,4	71,0
		% of Total	8,3%	13,5%	21,8%
	Μέτρια	Count	28	37	65
		Expected Count	31,7	33,3	65,0
		% of Total	8,6%	11,3%	19,9%
	Αρκετά	Count	34	25	59
		Expected Count	28,8	30,2	59,0
		% of Total	10,4%	7,7%	18,1%
	Πολύ	Count	16	9	25
		Expected Count	12,2	12,8	25,0
		% of Total	4,9%	2,8%	7,7%
	Πάρα πολύ	Count	23	9	32
		Expected Count	15,6	16,4	32,0
		% of Total	7,1%	2,8%	9,8%
Total		Count	159	167	326
		Expected Count	159,0	167,0	326,0
		% of Total	48,8%	51,2%	100,0%



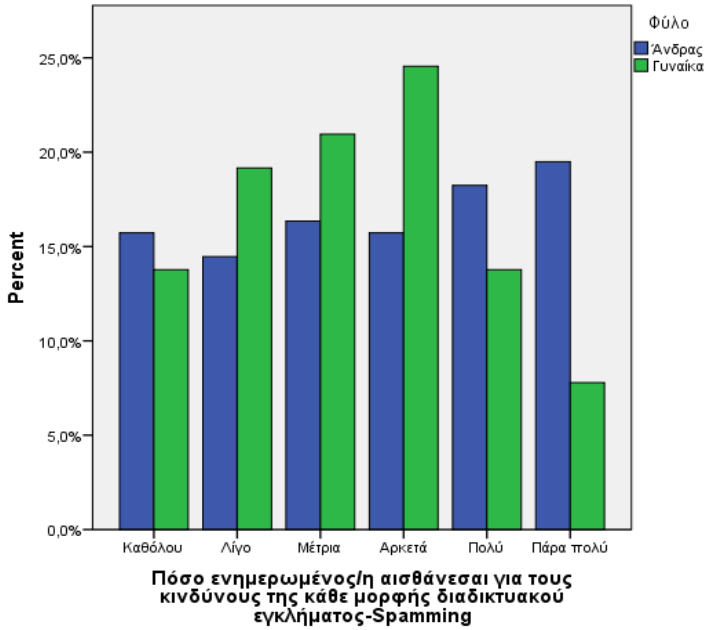
Διάγραμμα 4.1: *Ποσοστιαία κατανομή: Φύλο-Phishing και Pharming*

Φύλο-Spamming(Ανεπιθύμητη αλληλογραφία)

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία), από το σύνολο των ανδρών οι 25(15.7%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 23(14.5%) αισθάνονται λίγο ενημερωμένοι, οι 26(16.4%) μέτρια, οι 25(15.7%) αρκετά, οι 29(18.2%) πολύ και οι 31(19.5%) πάρα πολύ. Από το σύνολο των γυναικών οι 23(13.8%) δεν αισθάνονται καθόλου ενημερωμένες, οι 32(19.2%) αισθάνονται λίγο, οι 35(21%) μέτρια, οι 41(24.6%) αρκετά, οι 23(13.8%) πολύ και οι 13(7.8%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία) (X^2=14.631, df=5, p=0.012). Φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



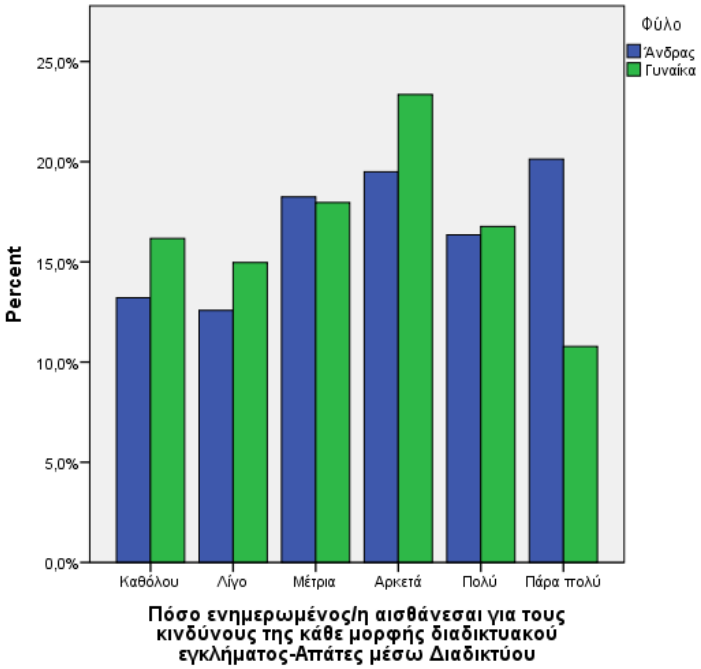
Διάγραμμα 4.2: *Ποσοστιαία κατανομή: Φύλο-Spamming*

Φύλο-Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.)

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.), από το σύνολο των ανδρών οι 21(13.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 20(12.6%) αισθάνονται λίγο ενημερωμένοι, οι 29(18.2%) μέτρια, οι 31(19.5%) αρκετά, οι 26(16.4%) πολύ και οι 32(20.1%) πάρα πολύ. Από το σύνολο των γυναικών οι 27(16.2%) δεν αισθάνονται καθόλου ενημερωμένες, οι 25(15.0%) αισθάνονται λίγο, οι 30(18%) μέτρια, οι 39(23.4%) αρκετά, οι 28(16.8%) πολύ και οι 18(10.8%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.) (X^2=6.038, df=5, p=0.303). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



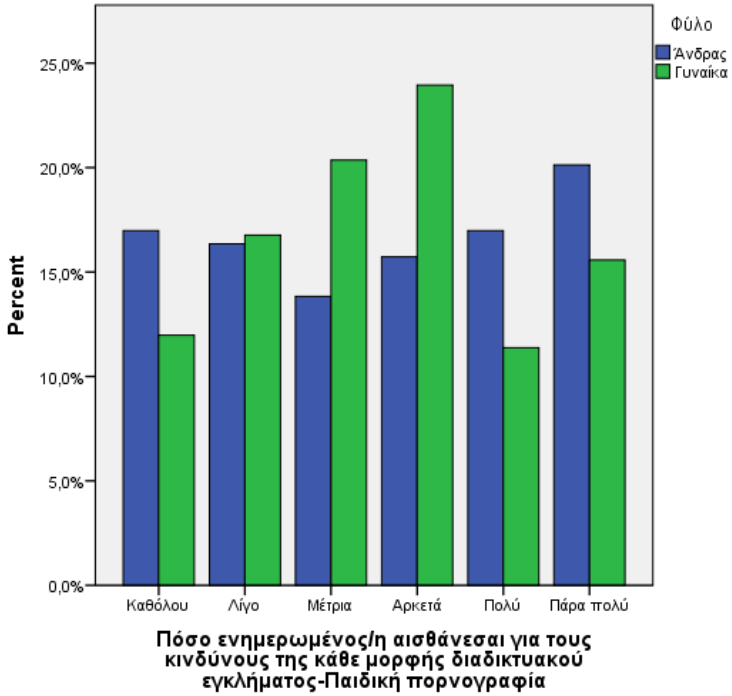
Διάγραμμα 4.3: *Ποσοστιαία κατανομή: Φύλο-Απάτες μέσω Διαδικτύου*

Φύλο-Παιδική πορνογραφία

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Παιδική πορνογραφία, από το σύνολο των ανδρών οι 27(17.0%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 26(16.4%) αισθάνονται λίγο ενημερωμένοι, οι 22(13.8%) μέτρια, οι 25(15.7%) αρκετά, οι 27(17.0%) πολύ και οι 32(20.1%) πάρα πολύ. Από το σύνολο των γυναικών οι 20(12.0%) δεν αισθάνονται καθόλου ενημερωμένες, οι 28(16.8%) αισθάνονται λίγο, οι 34(20.4%) μέτρια, οι 40(24.0%) αρκετά, οι 19(11.4%) πολύ και οι 26(15.6%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Παιδική πορνογραφία και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Παιδική πορνογραφία (X^2=8.971, df=5, p=0.110). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



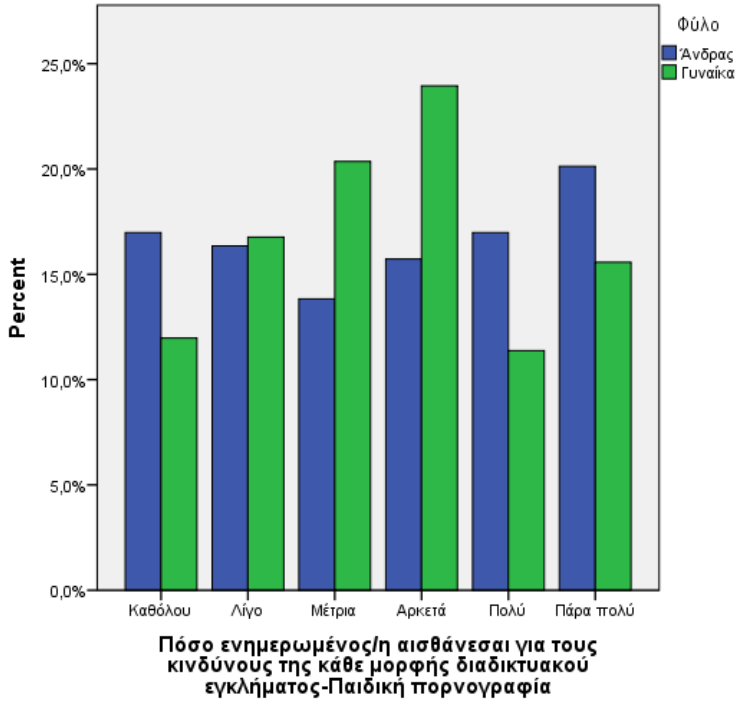
Διάγραμμα 4.4: *Ποσοστιαία κατανομή: Φύλο-Παιδική πορνογραφία*

Φύλο-Cracking και Hacking

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Cracking και Hacking, από το σύνολο των ανδρών οι 34(21.4%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 24(15.1%) αισθάνονται λίγο ενημερωμένοι, οι 40(25.2%) μέτρια, οι 20(12.6%) αρκετά, οι 16(10.1%) πολύ και οι 25(15.7%) πάρα πολύ. Από το σύνολο των γυναικών οι 37(22.2%) δεν αισθάνονται καθόλου ενημερωμένες, οι 30(18.0%) αισθάνονται λίγο, οι 39(23.4%) μέτρια, οι 27(16.2%) αρκετά, οι 14(8.4%) πολύ και οι 20(12.0%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Cracking και Hacking και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Cracking και Hacking (X^2=2.343, df=5, p=0.8). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



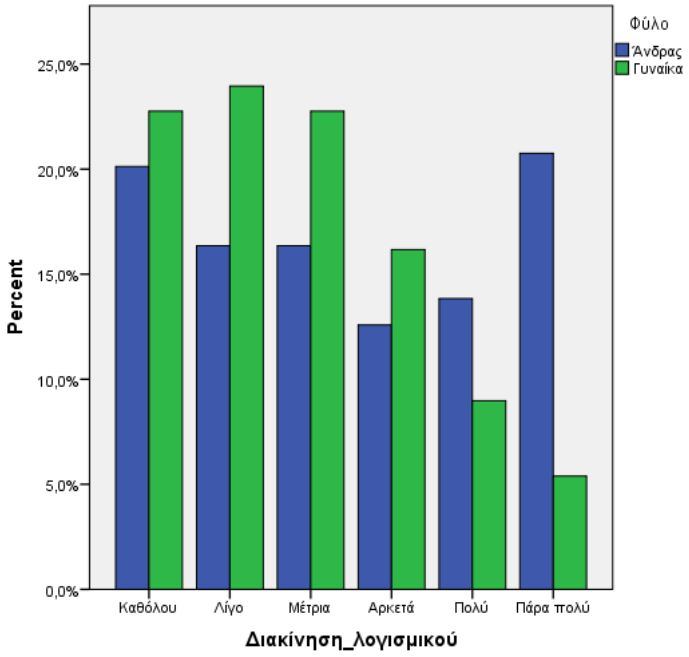
Διάγραμμα 4.5: *Ποσοστιαία κατανομή: Φύλο-Cracking και Hacking*

Φύλο-Διακίνηση/Πειρατεία λογισμικού

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού, από το σύνολο των ανδρών οι 32(20.1%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 26(16.4%) αισθάνονται λίγο ενημερωμένοι, οι 26(16.4%) μέτρια, οι 20(12.6%) αρκετά, οι 22(13.8%) πολύ και οι 33(20.8%) πάρα πολύ. Από το σύνολο των γυναικών οι 38(22.8%) δεν αισθάνονται καθόλου ενημερωμένες, οι 40(24.0%) αισθάνονται λίγο, οι 38(22.8%) μέτρια, οι 27(16.2%) αρκετά, οι 15(9.0%) πολύ και οι 9(5.4%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού (X^2=21.632, df=5, p=0.001). Φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



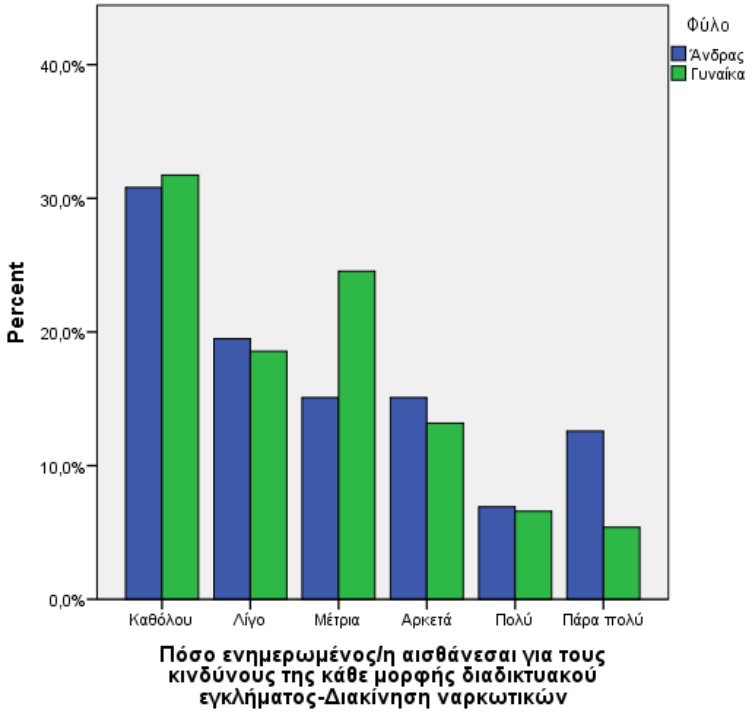
Διάγραμμα 4.6: *Ποσοστιαία κατανομή: Φύλο-Διακίνηση/Πειρατεία λογισμικού*

Φύλο-Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, από το σύνολο των ανδρών οι 49(30.8%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 31(19.5%) αισθάνονται λίγο ενημερωμένοι, οι 24(15.1%) μέτρια, οι 24(15.1%) αρκετά, οι 11(6.9%) πολύ και οι 20(12.6%) πάρα πολύ. Από το σύνολο των γυναικών οι 53(31.7%) δεν αισθάνονται καθόλου ενημερωμένες, οι 31(18.6%) αισθάνονται λίγο, οι 41(24.6%) μέτρια, οι 22(13.2%) αρκετά, οι 11(6.6%) πολύ και οι 9(5.4%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων (X^2=8.671, df=5, p=0.123). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



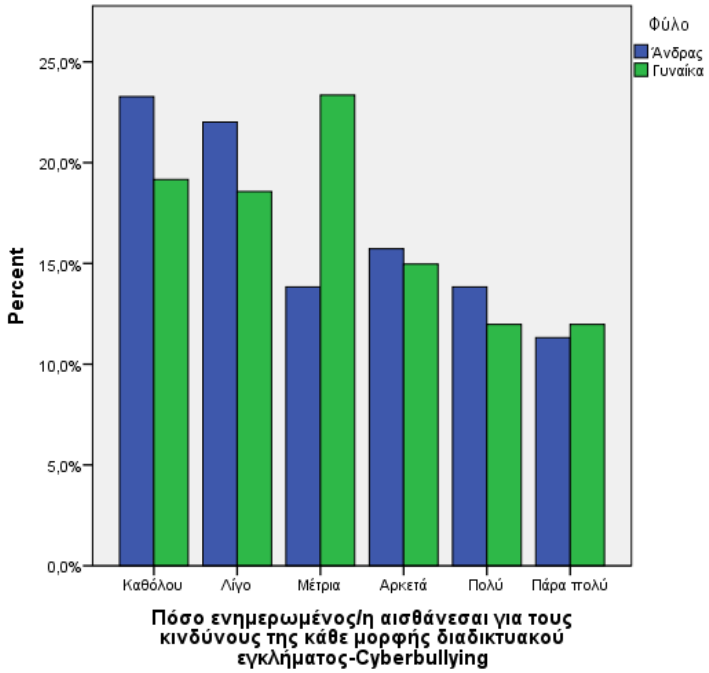
Διάγραμμα 4.7: *Ποσοστιαία κατανομή: Φύλο-Διακίνηση ναρκωτικών*

Φύλο-Cyberbullying(Διαδικτυακός εκφοβισμός)

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Cyberbullying(Διαδικτυακός εκφοβισμός), από το σύνολο των ανδρών οι 37(23.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 35(22.0%) αισθάνονται λίγο ενημερωμένοι, οι 22(13.8%) μέτρια, οι 25(15.7%) αρκετά, οι 22(13.8%) πολύ και οι 18(11.3%) πάρα πολύ. Από το σύνολο των γυναικών οι 32(19.2%) δεν αισθάνονται καθόλου ενημερωμένες, οι 31(18.6%) αισθάνονται λίγο, οι 39(23.4%) μέτρια, οι 25(15.0%) αρκετά, οι 20(12.0%) πολύ και οι 20(12.0%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Cyberbullying(Διαδικτυακός εκφοβισμός) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Cyberbullying(Διαδικτυακός εκφοβισμός) (X^2=5.350, df=5, p=0.375). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



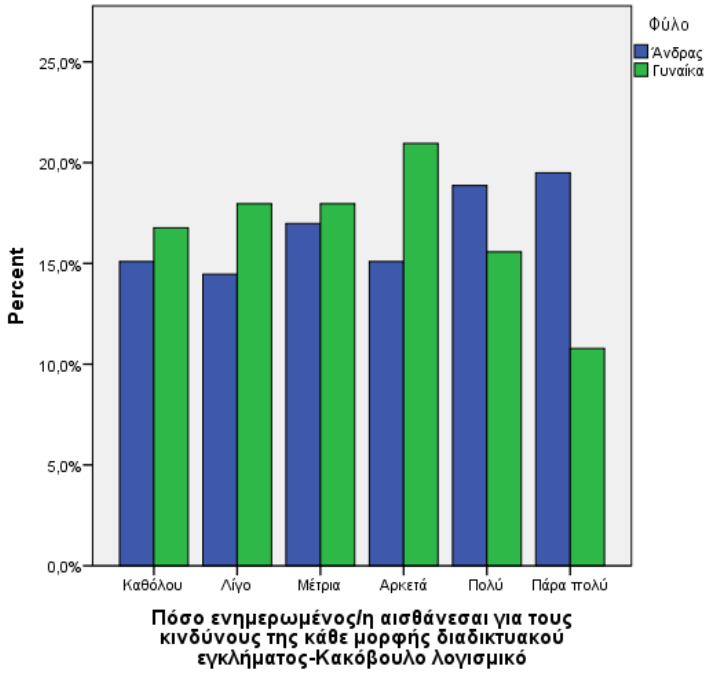
Διάγραμμα 4.8: *Ποσοστιαία κατανομή: Φύλο-Cyberbullying*

<u>Φύλο-Κακόβουλο λογισμικό(Ιοί, σκουλήκια,δούρειοι ίπποι)</u>

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι), από το σύνολο των ανδρών οι 24(15.1%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 23(14.5%) αισθάνονται λίγο ενημερωμένοι, οι 27(17.0%) μέτρια, οι 24(15.1%) αρκετά, οι 30(18.9%) πολύ και οι 31(19.5%) πάρα πολύ. Από το σύνολο των γυναικών οι 28(16.8%) δεν αισθάνονται καθόλου ενημερωμένες, οι 30(18.0%) αισθάνονται λίγο, οι 30(18.0%) μέτρια, οι 35(21.0%) αρκετά, οι 26(15.6%) πολύ και οι 18(10.8%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι) (X^2=6.984, df=5, p=0.222). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



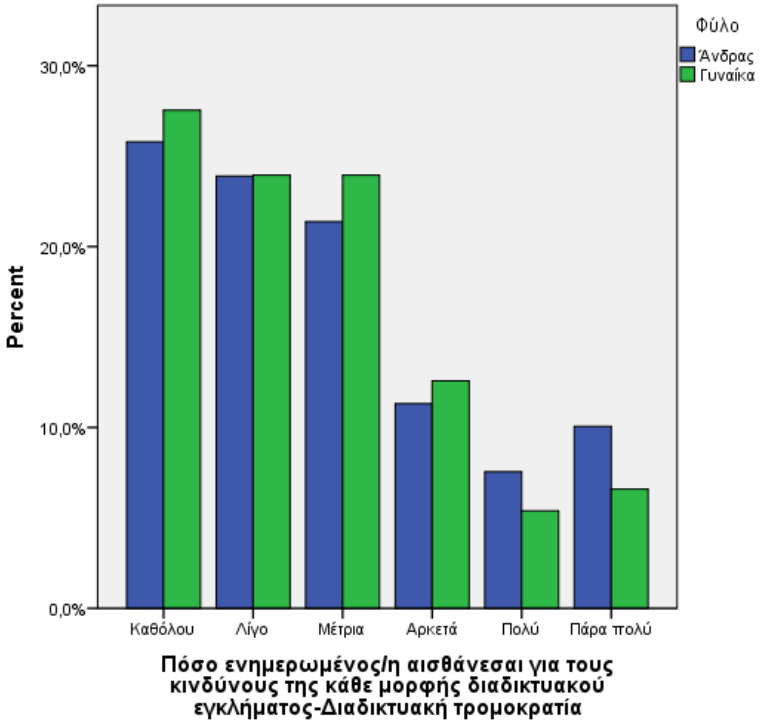
Διάγραμμα 4.9: *Ποσοστιαία κατανομή: Φύλο-Κακόβουλο λογισμικό*

Φύλο-Διαδικτυακή τρομοκρατία

Όσον αφορά το φύλο σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία, από το σύνολο των ανδρών οι 41(25.8%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 38(23.9%) αισθάνονται λίγο ενημερωμένοι, οι 34(21.4%) μέτρια, οι 18(11.3%) αρκετά, οι 12(7.5%) πολύ και οι 16(10.1%) πάρα πολύ. Από το σύνολο των γυναικών οι 46(27.5%) δεν αισθάνονται καθόλου ενημερωμένες, οι 40(24.0%) αισθάνονται λίγο, οι 40(24.0%) μέτρια, οι 21(12.6%) αρκετά, οι 9(5.4%) πολύ και οι 11(6.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και ενημέρωσης για τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία (X^2=2.215, df=5, p=0.819). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



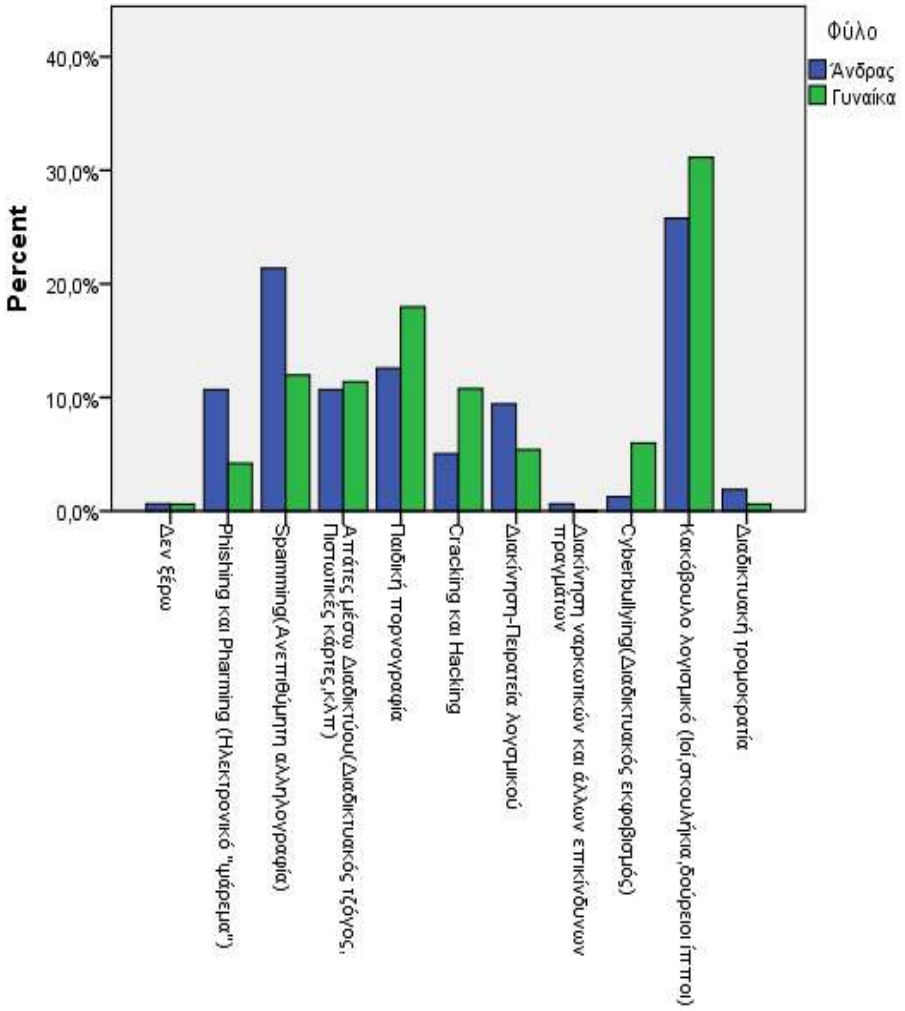
Διάγραμμα 4.10: *Ποσοστιαία κατανομή: Φύλο-Διαδικτυακή τρομοκρατία*

Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;

Όσον αφορά το φύλο με το ποια πιστεύουν ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας, από το σύνολο των ανδρών οι 17(10.7%) πιστεύουν ότι είναι το Phishing και Pharming, οι 34(21.4%) το Spamming, οι 17(10.7%) οι Απάτες μέσω Διαδικτύου, οι 20(12.6%) η Παιδική πορνογραφία, οι 8(5%) το Cracking και Hacking, οι 15(9.4%) η Διακίνηση-Πειρατεία λογισμικού, 1(0.6%) η Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, οι 2(1.3%) το Cyberbullying, οι 41(25.8%) το Κακόβουλο λογισμικό, οι 3(1.9%) η Διαδικτυακή τρομοκρατία ενώ 1(0.6%) δεν ξέρει ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας. Από το σύνολο των γυναικών, οι 7(4.2%) πιστεύουν ότι είναι το Phishing και Pharming, οι 20(12%) το Spamming, οι 19(11.4%) οι Απάτες μέσω Διαδικτύου, οι 30(18%) η Παιδική πορνογραφία, οι 10.8(5%) το Cracking και Hacking, οι 9(5.4%) η Διακίνηση-Πειρατεία λογισμικού, 0(0%) η Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, οι 10(6%) το Cyberbullying, οι 52(31.1%) το Κακόβουλο λογισμικό, 1(0.6%) η Διαδικτυακή τρομοκρατία ενώ 1(0.6%) δεν ξέρει ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και απόψεων σχετικά με το ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας (p=0.004). Φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



Διάγραμμα 4.11: *Ποσοστιαία κατανομή: Φύλο-Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακού εγκλήματος*

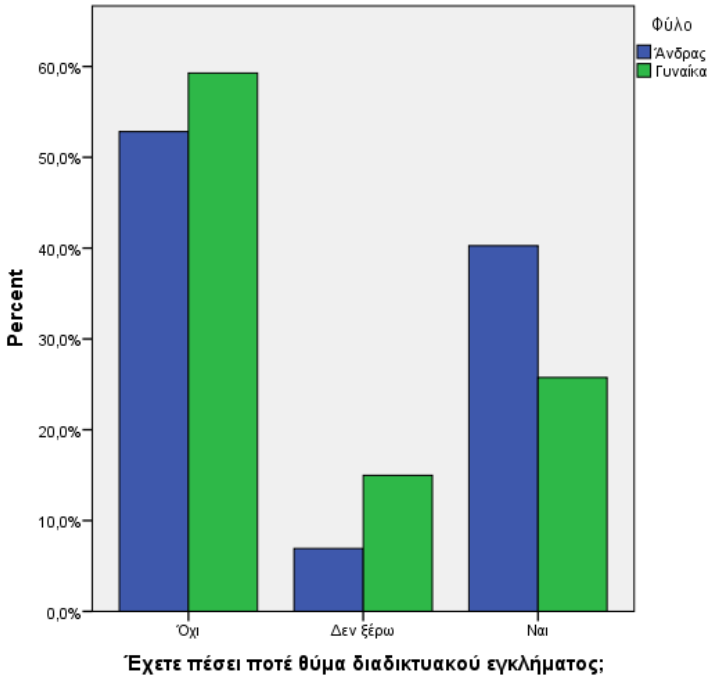
Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος;

Στην σύγκριση του φύλου με το αν έχουν πέσει θύμα διαδικτυακού εγκλήματος παρατηρούμε ότι όσον αφορά το σύνολο των ανδρών, οι 84(52.8%) δεν έχουν πέσει θύμα, οι 64(40.3%) έχουν πέσει ενώ οι 11(6.9%) δεν ξέρουν αν έχουν πέσει θύμα διαδικτυακού εγκλήματος. Όσον αφορά το σύνολο των γυναικών, οι 99(59.3%) δεν έχουν πέσει θύμα, οι 43(25.7%) έχουν πέσει θύμα ενώ οι 25(15.0%) δεν ξέρουν αν έχουν πέσει θύμα διαδικτυακού εγκλήματος.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι απαντήσεις των ανδρών και των γυναικών σχετικά με το αν έχουν πέσει θύμα ή όχι δεν διαφέρουν σημαντικά και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και των απαντήσεων σχετικά με το αν έχουν

πέσει θύμα απάτης ή όχι, δηλαδή οι απαντήσεις και των δυο φύλων διαφέρουν (X^2=10.606, df=2, p=0.005).



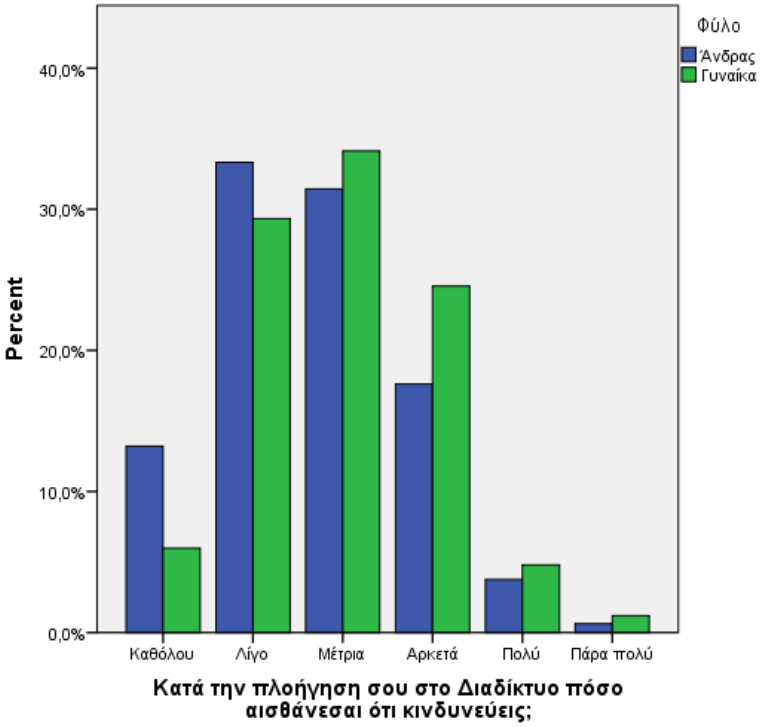
Διάγραμμα 4.12: *Ποσοστιαία κατανομή: Φύλο-Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος*

Κατά την πλοήγησή σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις;

Στην σύγκριση του φύλου με το πόσο αισθάνονται ότι κινδυνεύουν κατά την πλοήγησή τους στο Διαδίκτυο παρατηρούμε ότι όσον αφορά το σύνολο των ανδρών, οι 21(13.2%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 53(33.3%) αισθάνονται λίγο, οι 50(31.4%) μέτρια, οι 28(17.6%) αρκετά, οι 6(3.8%) πολύ ενώ μόνο 1(0.1%) αισθάνεται ότι κινδυνεύει πάρα πολύ. Όσον αφορά το σύνολο των γυναικών, οι 10(6.0%%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 49(29.3%) αισθάνονται λίγο, οι 57(34.1%) μέτρια, οι 41(24.6%) αρκετά, οι 8(4.8%) πολύ ενώ μόνο 2(1.2%) αισθάνονται ότι κινδυνεύουν πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στις απόψεις τους όσον αφορά το πόσο αισθάνονται ότι κινδυνεύουν κατά την πλοήγησή τους στο Διαδίκτυο και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και απόψεων όσον αφορά το πόσο αισθάνονται ότι κινδυνεύουν κατά την πλοήγησή τους στο Διαδίκτυο (X^2=7.394, df=5, p=0.193). Δεν φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



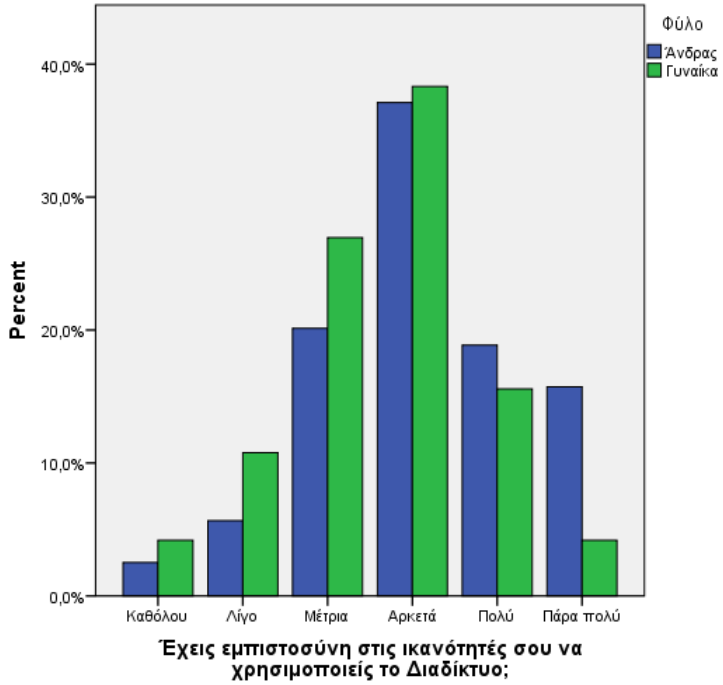
Διάγραμμα 4.13: *Ποσοστιαία κατανομή: Φύλο-Πόσο αισθάνεσαι ότι κινδυνεύεις*

Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο;

Στην σύγκριση του φύλου με το αν έχουν εμπιστοσύνη στις ικανότητές τους να χρησιμοποιούν το Διαδίκτυο παρατηρούμε ότι όσον αφορά το σύνολο των ανδρών, οι 4(2.5%) δεν έχουν καθόλου εμπιστοσύνη στις ικανότητές τους, οι 9(5.7%) έχουν λίγο, οι 32(20.1%) μέτρια, οι 59(37.1%) αρκετά, οι 30(18.9%) πολύ και οι 25(15.7%) έχουν πάρα πολύ εμπιστοσύνη στις ικανότητές τους. Όσον αφορά το σύνολο των γυναικών, οι 7(4.2%) δεν έχουν καθόλου εμπιστοσύνη, οι 18(10.8%) έχουν λίγο, οι 45(26.9%) μέτρια, οι 64(38.3%) αρκετά, οι 26(15.6%) πολύ και οι 7(4.2%) έχουν πάρα πολύ εμπιστοσύνη στις ικανότητές τους να χρησιμοποιούν το Διαδίκτυο.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι άνδρες και γυναίκες δεν διαφέρουν σημαντικά στις απόψεις τους όσον αφορά το πόσο εμπιστοσύνη έχουν στις ικανότητές τους να χρησιμοποιούν το Διαδίκτυο και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και απόψεων όσον αφορά το πόσο εμπιστοσύνη έχουν στις ικανότητές τους να χρησιμοποιούν το Διαδίκτυο (X^2=16.441, df=5, p=0.006). Φαίνεται να διαφέρουν οι απόψεις και των δυο φύλων σημαντικά.



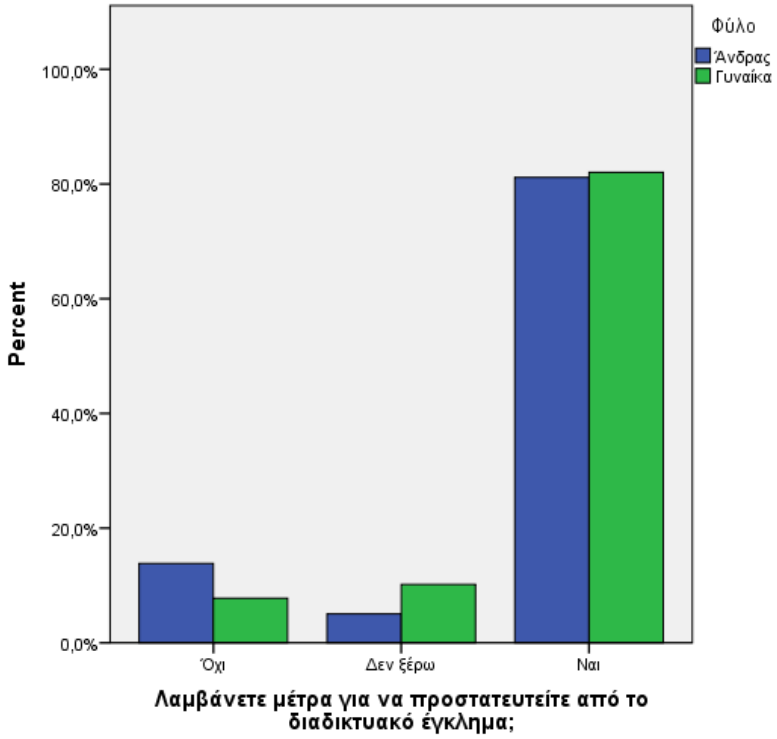
Διάγραμμα 4.14: *Ποσοστιαία κατανομή: Φύλο-Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο;*

Λαμβάνετε μέτρα για να προστατευτείτε από το διαδικτυακό έγκλημα;

Στην σύγκριση του φύλου με το αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα παρατηρούμε ότι όσον αφορά το σύνολο των ανδρών, οι 129(81.1%) λαμβάνουν μέτρα, οι 22(13.8%) δεν λαμβάνουν μέτρα ενώ οι 8(5.0%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα. Όσον αφορά το σύνολο των γυναικών, οι 137(82.0%) λαμβάνουν μέτρα, οι 13(7.8%) δεν λαμβάνουν μέτρα ενώ οι 17(10.2%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι απαντήσεις των ανδρών και των γυναικών σχετικά με το αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα δεν διαφέρουν σημαντικά και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ φύλου και των απαντήσεων σχετικά με το αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα (X^2=10.606, df=2, p=0.061). Δεν φαίνεται να διαφέρουν οι απαντήσεις και των δυο φύλων σημαντικά.



Διάγραμμα 4.15: *Ποσοστιαία κατανομή: Φύλο-Λαμβάνετε μέτρα για να προστατευτείτε από το διαδικτυακό έγκλημα;*

Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος;

Στην συγκεκριμένη ερώτηση, θέλουμε να εξερευνήσουμε τη σχέση ηλικίας των ερωτώμενων και απαντήσεων για την κάθε μορφή διαδικτυακού εγκλήματος ξεχωριστά.

Ηλικία-Phishing και Pharming (Ηλεκτρονικό ψάρεμα)

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Phishing και Pharming (Ηλεκτρονικό ψάρεμα), από το σύνολο των ατόμων ηλικίας 12-18, οι 14(27.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 11(21.6%) αισθάνονται λίγο, οι 12(23.5%) μέτρια, οι 8(15.7%) αρκετά, οι 2(3.9%) πολύ και οι 4(7.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 40(22.6%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 38(21.5%) αισθάνονται λίγο, οι 35(19.8%) μέτρια, οι 33(18.6%) αρκετά, οι 14(7.9%) πολύ και οι 17(9.6%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 12(22.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 17(31.5%) αισθάνονται λίγο, οι 12(22.2%) μέτρια, οι 5(9.3%) αρκετά, οι 3(5.6%) πολύ και οι 5(9.3%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 8(18.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 5(11.4%) αισθάνονται λίγο, οι 6(13.6%) μέτρια, οι 13(29.5%) αρκετά, οι 6(13.6%) πολύ και οι 6(13.6%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Phishing και Pharming και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δε φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Phishing και Pharming (X^2=16.690, df=15, p=0.338). Δεν φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Πίνακας 4.2: Πίνακας Συνάφειας Συσχέτισης *Ηλικία-Phishing και Pharming*

Phishing_Pharming1 * Ηλικία Crosstabulation

			Ηλικία				Total
			12-18	19-30	31-45	46 και άνω	
	Καθόλου	Count	14	40	12	8	74
		Expected Count	11,6	40,2	12,3	10,0	74,0
		% of Total	4,3%	12,3%	3,7%	2,5%	22,7%
	Λίγο	Count	11	38	17	5	71
		Expected Count	11,1	38,5	11,8	9,6	71,0
		% of Total	3,4%	11,7%	5,2%	1,5%	21,8%
	Μέτρια	Count	12	35	12	6	65
		Expected Count	10,2	35,3	10,8	8,8	65,0
		% of Total	3,7%	10,7%	3,7%	1,8%	19,9%
	Αρκετά	Count	8	33	5	13	59
		Expected Count	9,2	32,0	9,8	8,0	59,0
		% of Total	2,5%	10,1%	1,5%	4,0%	18,1%
	Πολύ	Count	2	14	3	6	25
		Expected Count	3,9	13,6	4,1	3,4	25,0
		% of Total	0,6%	4,3%	0,9%	1,8%	7,7%
	Πάρα πολύ	Count	4	17	5	6	32
		Expected Count	5,0	17,4	5,3	4,3	32,0
		% of Total	1,2%	5,2%	1,5%	1,8%	9,8%
Total		Count	51	177	54	44	326
		Expected Count	51,0	177,0	54,0	44,0	326,0
		% of Total	15,6%	54,3%	16,6%	13,5%	100,0%

Ηλικία-Spamming (Ανεπιθύμητη αλληλογραφία)

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία), από το σύνολο των ατόμων ηλικίας 12-18, οι 17(33.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(11.8%) αισθάνονται λίγο, οι 11(21.6%) μέτρια, οι 5(9.8%) αρκετά, οι 6(11.8%) πολύ και οι 6(11.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 18(10.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 29(16.4%) αισθάνονται λίγο, οι 37(20.9%) μέτρια, οι 42(23.7%) αρκετά, οι 27(15.3%) πολύ και οι 24(13.6%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 6(11.1%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 14(25.9%) αισθάνονται λίγο, οι 9(16.7%) μέτρια, οι 9(16.7%) αρκετά, οι 9(16.7%) πολύ και οι 7(13.0%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 7(15.9%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(13.6%) αισθάνονται λίγο, οι 4(9.1%) μέτρια, οι 10(22.7%) αρκετά, οι 10(22.7%) πολύ και οι 7(15.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Spamming (Ανεπιθύμητη αλληλογραφία) (X^2=28.190, df=15, p=0.020). Φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.)

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.), από το σύνολο των ατόμων ηλικίας 12-18, οι 14(27.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 4(7.8%) αισθάνονται λίγο, οι 14(27.5%) μέτρια, οι 10(19.6%) αρκετά, οι 3(5.9%) πολύ και οι 6(11.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 18(10.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 25(14.1%) αισθάνονται λίγο, οι 28(15.8%) μέτρια, οι 44(24.9%) αρκετά, οι 34(19.2%) πολύ και οι 28(15.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 10(18.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 10(18.5%) αισθάνονται λίγο, οι 13(24.1%) μέτρια, οι 6(11.1%) αρκετά, οι 6(11.1%) πολύ και οι 9(16.7%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 6(13.6%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(13.6%) αισθάνονται λίγο, οι 4(9.1%) μέτρια, οι 10(22.7%) αρκετά, οι 11(25.0%) πολύ και οι 7(15.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Απάτες μέσω

Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (Διαδικτυακός τζόγος, πιστωτικές κάρτες, κ.λ.π.) (X^2=28.278, df=15, p=0.020). Φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Παιδική πορνογραφία

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Παιδική πορνογραφία, από το σύνολο των ατόμων ηλικίας 12-18, οι 11(21.6%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 5(9.8%) αισθάνονται λίγο, οι 11(21.6%) μέτρια, οι 11(21.6%) αρκετά, οι 3(5.9%) πολύ και οι 10(19.6%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 19(10.7%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 30(16.9%) αισθάνονται λίγο, οι 30(16.9%) μέτρια, οι 39(20.0%) αρκετά, οι 30(16.9%) πολύ και οι 29(16.4%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 9(16.7%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 11(20.4%) αισθάνονται λίγο, οι 9(16.7%) μέτρια, οι 8(14.8%) αρκετά, οι 5(9.3%) πολύ και οι 12(22.2%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 8(18.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 8(18.2%) αισθάνονται λίγο, οι 6(13.6%) μέτρια, οι 7(15.9%) αρκετά, οι 8(18.2%) πολύ και οι 7(15.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Παιδική πορνογραφία και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Παιδική πορνογραφία (X^2=14.346, df=15, p=0.499). Δεν φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Cracking και Hacking

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Cracking και Hacking, από το σύνολο των ατόμων ηλικίας 12-18, οι 13(25.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 5(9.8%) αισθάνονται λίγο, οι 10(19.6%) μέτρια, οι 9(17.6%) αρκετά, οι 4(7.8%) πολύ και οι 10(19.6%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 28(15.8%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 32(18.6%) αισθάνονται λίγο, οι 45(25.4%) μέτρια, οι 29(16.4%) αρκετά, οι 20(11.3%) πολύ και οι 22(12.4%) πάρα πολύ. Από το σύνολο των

ατόμων ηλικίας 31-45, οι 17(31.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 9(16.7%) αισθάνονται λίγο, οι 15(27.8%) μέτρια, οι 4(7.4%) αρκετά, οι 1(1.9%) πολύ και οι 8(14.8%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 13(29.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 7(15.9%) αισθάνονται λίγο, οι 9(20.5%) μέτρια, οι 5(11.4%) αρκετά, οι 5(11.4%) πολύ και οι 5(11.4%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Cracking και Hacking και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Cracking και Hacking (X^2=18.764, df=15, p=0.225). Δεν φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Διακίνηση-Πειρατεία λογισμικού

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού, από το σύνολο των ατόμων ηλικίας 12-18, οι 17(33.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(11.8%) αισθάνονται λίγο, οι 15(29.4%) μέτρια, οι 6(11.8%) αρκετά, οι 3(5.9%) πολύ και οι 4(7.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 28(15.8%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 34(19.2%) αισθάνονται λίγο, οι 35(19.8%) μέτρια, οι 32(18.1%) αρκετά, οι 26(14.7%) πολύ και οι 22(12.4%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 10(18.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 18(33.3%) αισθάνονται λίγο, οι 9(16.7%) μέτρια, οι 4(7.4%) αρκετά, οι 4(7.4%) πολύ και οι 9(16.7%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 15(34.1%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 8(18.2%) αισθάνονται λίγο, οι 5(11.4%) μέτρια, οι 5(11.4%) αρκετά, οι 4(9.1%) πολύ και οι 7(15.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού (X^2=30.272, df=15, p=0.011). Φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, από το σύνολο των ατόμων ηλικίας 12-18, οι 17(33.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 7(13.7%) αισθάνονται λίγο, οι 12(23.5%) μέτρια, οι 7(13.7%) αρκετά, οι 3(5.9%) πολύ και οι 5(9.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 43(24.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 42(23.7%) αισθάνονται λίγο, οι 38(21.5%) μέτρια, οι 29(16.4%) αρκετά, οι 13(7.3%) πολύ και οι 12(6.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 23(42.6%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 7(13%) αισθάνονται λίγο, οι 11(20.4%) μέτρια, οι 3(5.6%) αρκετά, οι 3(5.6%) πολύ και οι 7(13%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 19(43.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(13.6%) αισθάνονται λίγο, οι 4(9.1%) μέτρια, οι 7(15.9%) αρκετά, οι 3(6.8%) πολύ και οι 5(11.4%) πάρα πολύ.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων (p=0.111). Δεν φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Cyberbullying(Διαδικτυακός εκφοβισμός)

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Cyberbullying (Διαδικτυακός εκφοβισμός), από το σύνολο των ατόμων ηλικίας 12-18, οι 10(19.6%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 1(2.0%) αισθάνονται λίγο, οι 11(21.6%) μέτρια, οι 11(21.6%) αρκετά, οι 9(17.6%) πολύ και οι 9(17.6%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 27(15.3%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 38(21.5%) αισθάνονται λίγο, οι 41(23.2%) μέτρια, οι 26(14.7%) αρκετά, οι 27(15.3%) πολύ και οι 18(10.2%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 19(35.2%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 14(25.9%) αισθάνονται λίγο, οι 7(13.0%) μέτρια, οι 5(9.3%) αρκετά, οι 2(3.7%) πολύ και οι 7(13.0%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 13(29.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 13(29.5%) αισθάνονται λίγο, οι 2(4.5%) μέτρια, οι 8(18.2%) αρκετά, οι 4(9.1%) πολύ και οι 4(9.1%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Cyberbullying(Διαδικτυακός εκφοβισμός) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής

Cyberbullying(Διαδικτυακός εκφοβισμός) (X^2=39.318, df=15, p=0.001). Φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι)

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι), από το σύνολο των ατόμων ηλικίας 12-18, οι 12(23.5%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 5(9.8%) αισθάνονται λίγο, οι 8(15.7%) μέτρια, οι 10(19.6%) αρκετά, οι 8(15.7%) πολύ και οι 8(15.7%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 21(11.9%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 25(14.1%) αισθάνονται λίγο, οι 31(17.5%) μέτρια, οι 38(21.5%) αρκετά, οι 36(20.3%) πολύ και οι 26(14.7%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 9(16.7%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 16(29.6%) αισθάνονται λίγο, οι 10(18.5%) μέτρια, οι 6(11.1%) αρκετά, οι 5(9.3%) πολύ και οι 8(14.8%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 10(22.7%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 7(15.9%) αισθάνονται λίγο, οι 8(18.2%) μέτρια, οι 5(11.4%) αρκετά, οι 7(15.9%) πολύ και οι 7(15.9%) πάρα πολύ.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι ηλικιακές ομάδες της έρευνας δεν διαφέρουν σημαντικά στην ενημέρωσή τους σχετικά με τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι) και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι) (X^2=19.753, df=15, p=0.182). Δεν φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ηλικία-Διαδικτυακή τρομοκρατία

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο ενημερωμένοι αισθάνονται για τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία, από το σύνολο των ατόμων ηλικίας 12-18, οι 16(31.4%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 6(11.8%) αισθάνονται λίγο, οι 11(21.6%) μέτρια, οι 5(9.8%) αρκετά, οι 7(13.7%) πολύ και οι 6(11.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 32(18.1%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 50(28.2%) αισθάνονται λίγο, οι 48(27.1%) μέτρια, οι 26(14.7%) αρκετά, οι 10(5.6%) πολύ και οι 11(6.2%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 21(38.9%) δεν αισθάνονται καθόλου ενημερωμένοι, οι 14(25.9%) αισθάνονται λίγο, οι 9(16.7%) μέτρια, οι 4(7.4%) αρκετά, οι 0(0%) πολύ και οι 6(11.1%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 18(40.9%) δεν αισθάνονται καθόλου

ενημερωμένοι, οι 8(18.2%) αισθάνονται λίγο, οι 6(13.6%) μέτρια, οι 4(9.1%) αρκετά, οι 4(9.1%) πολύ και οι 4(9.1%) πάρα πολύ.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και ενημέρωσης για τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία (p=0.002). Φαίνεται να διαφέρουν οι απόψεις των ατόμων ανάλογα με την ηλικία σημαντικά.

Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;

Στην σύγκριση της ηλικίας με το ποια πιστεύουν ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας, από το σύνολο των ατόμων ηλικίας 12-18, οι 5(9.8%) πιστεύουν ότι είναι το Phishing και Pharming, οι 2(3.9%) το Spamming, οι 2(3.9%) οι Απάτες μέσω Διαδικτύου, οι 7(13.7%) η Παιδική πορνογραφία, οι 9(17.6%) το Cracking και Hacking, οι 3(5.9%) η Διακίνηση-Πειρατεία λογισμικού, οι 7(13.7%) το Cyberbullying, οι 14 (27.5%) το Κακόβουλο λογισμικό, οι 1(2%) η Διαδικτυακή τρομοκρατία ενώ 1(2%) δεν ξέρει ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας. Από το σύνολο των ατόμων ηλικίας 19-30, οι 4(2.3%) πιστεύουν ότι είναι το Phishing και Pharming, οι 26(14.7%) το Spamming, οι 23(13%) οι Απάτες μέσω Διαδικτύου, οι 32(18.1%) η Παιδική πορνογραφία, οι 15(8.5%) το Cracking και Hacking, οι 15(8.5%) η Διακίνηση-Πειρατεία λογισμικού, 1(0.6%) η Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων, οι 4(2.3%) το Cyberbullying, οι 54(30.5%) το Κακόβουλο λογισμικό, οι 2(1.1%) η Διαδικτυακή τρομοκρατία ενώ 1(0.6%) δεν ξέρει ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας. Από το σύνολο των ατόμων ηλικίας 31-45, οι 9(16.7%) πιστεύουν ότι είναι το Phishing και Pharming, οι 13(24.1%) το Spamming, οι 4(7.4%) οι Απάτες μέσω Διαδικτύου, οι 6(11.1%) η Παιδική πορνογραφία, οι 1(1.9%) το Cracking και Hacking, οι 4(7.4%) η Διακίνηση-Πειρατεία λογισμικού, οι 1(1.9%) το Cyberbullying, οι 15(27.8%) το Κακόβουλο λογισμικό και 1(1.9%) η Διαδικτυακή τρομοκρατία .Από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 6(13.6%) πιστεύουν ότι είναι το Phishing και Pharming, οι 13(29.5%) το Spamming, οι 7(15.9%) οι Απάτες μέσω Διαδικτύου, οι 5(11.4%) η Παιδική πορνογραφία, οι 1(2.3%) το Cracking και Hacking, οι 2(4.5%) η Διακίνηση-Πειρατεία λογισμικού και οι 10(22.7%) το Κακόβουλο λογισμικό.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και απόψεων σχετικά με το ποια είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας (p=0.000). Φαίνεται να διαφέρουν οι απόψεις ανάλογα με την ηλικία σημαντικά.

Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος;

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το αν έχουν πέσει ποτέ θύμα διαδικτυακού εγκλήματος, από το σύνολο των ατόμων ηλικίας 12-18, οι 35(68.6%) δεν έχουν πέσει ποτέ θύμα, οι 12(23.5%) έχουν πέσει θύμα ενώ οι 4(7.8%) δεν ξέρουν αν έχουν πέσει θύμα απάτης. Από το σύνολο των ατόμων ηλικίας 19-30, οι 91(51.4%) δεν έχουν πέσει ποτέ θύμα, οι 66(37.3%) έχουν πέσει θύμα ενώ οι 20(11.3%) δεν ξέρουν αν έχουν πέσει θύμα απάτης. Από το σύνολο των ατόμων ηλικίας 31-45, οι 28(51.9%) δεν έχουν πέσει ποτέ θύμα, οι 18(33.3%) έχουν πέσει θύμα ενώ οι 8(14.8%) δεν ξέρουν αν έχουν πέσει θύμα απάτης. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 29(65.9%) δεν έχουν πέσει ποτέ θύμα, οι 11(25.0%) έχουν πέσει θύμα ενώ οι 4(9.1%) δεν ξέρουν αν έχουν πέσει θύμα απάτης.

Στατιστικός έλεγχος X^2 (Pearson's chi-squared test)

Η μηδενική μας υπόθεση είναι ότι οι απαντήσεις των ηλικιακών ομάδων της έρευνας σχετικά με το αν έχουν πέσει θύμα ή όχι δεν διαφέρουν σημαντικά και η εναλλακτική μας είναι ότι διαφέρουν. Με βάση τα αποτελέσματα της διαδικασίας X^2 δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και των απαντήσεων σχετικά με το αν έχουν πέσει θύμα απάτης ή όχι (X^2=7.619, df=6, p=0.267). Δεν φαίνεται να διαφέρουν οι απαντήσεις ανάλογα με την ηλικία σημαντικά.

Κατά την πλοήγησή σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις;

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το πόσο αισθάνονται ότι κινδυνεύουν, από το σύνολο των ατόμων ηλικίας 12-18, οι 6(11.8%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 17(33.3%) αισθάνονται λίγο, οι 13(25.5%) μέτρια, οι 11(21.6%) αρκετά, οι 4(7.8%) πολύ ενώ κανένας δεν αισθάνεται πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, οι 11(6.2%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 54(30.5%) αισθάνονται λίγο, οι 71(40.1%) μέτρια, οι 37(20.9%) αρκετά, οι 4(2.3%) πολύ ενώ κανένας δεν αισθάνεται πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 7(13%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 14(25.9%) αισθάνονται λίγο, οι 14(25.9%) μέτρια, οι 15(27.8%) αρκετά, οι 2(3.7%) πολύ και οι 2(3.7%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 7(15.9%) δεν αισθάνονται καθόλου ότι κινδυνεύουν, οι 17(38.6%) αισθάνονται λίγο, οι 9(20.5%) μέτρια, οι 6(13.6%) αρκετά, οι 4(9.1%) πολύ και οι 1(2.3%) πάρα πολύ.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και απόψεων όσον αφορά το πόσο αισθάνονται ότι κινδυνεύουν κατά την πλοήγησή τους στο Διαδίκτυο (p=0.011). Φαίνεται να διαφέρουν οι απόψεις ανάλογα με την ηλικία σημαντικά.

Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο;

Όσον αφορά την ηλικία των ατόμων του δείγματος σε σχέση με το αν έχουν εμπιστοσύνη στις ικανότητές τους, από το σύνολο των ατόμων ηλικίας 12-18, 1(2%) δεν έχει καθόλου εμπιστοσύνη, οι 6(11.8%) λίγο, οι 15(29.4%) μέτρια, οι 20(39.2%) αρκετά, οι 5(9.8%) πολύ ενώ οι 4(7.8%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 19-30, 1(0.6%) δεν έχει καθόλου εμπιστοσύνη, οι 12(6.8%) λίγο, οι 39(22%) μέτρια, οι 69(39%) αρκετά, οι 38(21.5%) πολύ ενώ οι 18(10.2%) πάρα πολύ. Από το σύνολο των ατόμων ηλικίας 31-45, οι 3(5.6%) δεν έχουν καθόλου εμπιστοσύνη, οι 4(7.4%) λίγο, οι 13(24.1%) μέτρια, οι 21(38.9%) αρκετά, οι 9(16.7%) πολύ ενώ οι 4(7.4%) πάρα πολύ. Τέλος, από το σύνολο των ατόμων ηλικίας 46 και άνω, οι 6(13.6%) δεν έχουν καθόλου εμπιστοσύνη, οι 5(11.4%) λίγο, οι 10(22.7%) μέτρια, οι 13(29.5%) αρκετά, οι 4(9.1%) πολύ ενώ οι 6(13.6%) πάρα πολύ.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και απόψεων όσον αφορά το πόσο εμπιστοσύνη έχουν στις ικανότητές τους να χρησιμοποιούν το Διαδίκτυο (p=0.034). Φαίνεται να διαφέρουν οι απόψεις τους ανάλογα με την ηλικία σημαντικά.

Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα;

Στην σύγκριση της ηλικίας με το αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα παρατηρούμε ότι όσον αφορά το σύνολο των ατόμων ηλικίας 12-18, οι 40(78.4%) λαμβάνουν μέτρα, οι 6(11.8%) δεν λαμβάνουν μέτρα ενώ οι 5(9.8%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα. Όσον αφορά το σύνολο των ατόμων ηλικίας 19-30, οι 151(85.3%) λαμβάνουν μέτρα, οι 15(8.5%) δεν λαμβάνουν μέτρα ενώ οι 11(6.2%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα. Όσον αφορά το σύνολο των ατόμων ηλικίας 31-45, οι 40(74.1%) λαμβάνουν μέτρα, οι 7(13%) δεν λαμβάνουν μέτρα ενώ οι 7(13%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα. Τέλος, όσον αφορά το σύνολο των ατόμων ηλικίας 46 και άνω, οι 35(79.5%) λαμβάνουν μέτρα, οι 7(15.9%) δεν λαμβάνουν μέτρα ενώ οι 2(4.5%) δεν ξέρουν αν λαμβάνουν μέτρα για να προστατευτούν από το διαδικτυακό έγκλημα.

Μέθοδος Monte Carlo (exact Monte Carlo test)

Με βάση τα αποτελέσματα της μεθόδου Monte Carlo δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση μεταξύ ηλικίας και απαντήσεων όσον αφορά το αν λαμβάνουν μέτρα για να προστατευτούνε από το Διαδικτυακό έγκλημα (p=0.349). Δεν φαίνεται να διαφέρουν οι απαντήσεις τους ανάλογα με την ηλικία σημαντικά.

ΜΟΡΦΩΤΙΚΟ ΕΠΙΠΕΔΟ

Όσον αφορά το Μορφωτικό Επίπεδο, σύμφωνα με τον έλεγχο ανεξαρτησίας X^2 του Pearson και το ακριβές τεστ του Monte Carlo τα ζευγάρια των ερωτήσεων στα οποία φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση είναι:

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Spamming (exact Monte Carlo test, p value=0.004)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (exact Monte Carlo test, p value=0.006)

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Cyberbullying (exact Monte Carlo test, p value=0.007)

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Κακόβουλο λογισμικό (Pearson Chi-Square, p value=0.026)*

Μορφωτικό επίπεδο- Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας; (exact Monte Carlo test, p value=0.000)

Ενώ τα ζευγάρια των ερωτήσεων στα οποία δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση είναι:

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Phishing και Pharming (exact Monte Carlo test, p value=0.47)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Παιδική πορνογραφία (Pearson Chi-Square,p value=0.318)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Cracking και Hacking (exact Monte Carlo test, p value=0.442)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Διακίνηση-Πειρατεία λογισμικού (exact Monte Carlo test, p value=0.140)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων (exact Monte Carlo test, p value=0.795)*

Μορφωτικό επίπεδο- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής *Διαδικτυακή τρομοκρατία (exact Monte Carlo test, p value=0.282)*

Μορφωτικό επίπεδο- Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος; (exact Monte Carlo test, p value=0.063)

Μορφωτικό επίπεδο- Κατά την πλοήγησή σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις; (exact Monte Carlo test, p value=0.801)

Μορφωτικό επίπεδο-Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο; (exact Monte Carlo test, p value=0.331)

Μορφωτικό επίπεδο- Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα; (exact Monte Carlo test, p value=0.659)

ΑΠΑΣΧΟΛΗΣΗ

Όσον αφορά την Απασχόληση, σύμφωνα με το ακριβές τεστ του Monte Carlo τα ζευγάρια των ερωτήσεων στα οποία φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση είναι:

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Spamming (p value=0.035)

Απασχόληση Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής -Cyberbullying (p value=0.000)

Απασχόληση-Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;(p value=0.020)

Ενώ τα ζευγάρια των ερωτήσεων στα οποία δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση είναι:

Απασχόληση-Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Phishing και Pharming (p value=0.158)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Απάτες μέσω Διαδικτύου (p value=0.146)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Παιδική πορνογραφία (p value=0.409)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Cracking και Hacking (p value=0.941)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Διακίνηση-Πειρατεία λογισμικού (p value=0.415)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων (p value=0.384)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Κακόβουλο λογισμικό (p value=0.312)

Απασχόληση- Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Διαδικτυακή τρομοκρατία (p value=0.156)

Απασχόληση-Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος;(p value=0.398)

Απασχόληση-Κατά την πλοήγησή σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις;(p value=0.586)

Απασχόληση-Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο; (p value=0.425)

Απασχόληση-Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα; (p value=0.695)

Πίνακας 4.3: *Συγκεντρωτικός πίνακας συσχετίσεων*

	Φύλο	Ηλικία	Μορφ.επίπεδο	Απασχόληση
Phishing_Pharming	Σ	Α	Α	Α
Spamming	Σ	Σ	Σ	Σ
Απάτες μέσω Διαδικτύου	Α	Σ	Σ	Α
Παιδ.πορνογραφία	Α	Α	Α	Α
Cracking_Hacking	Α	Α	Α	Α
Διακ_Πειρ_λογισμικού	Σ	Σ	Α	Α
Διακ.ναρκωτικών	Α	Α	Α	Α
Cyberbullying	Α	Σ	Σ	Σ
Κακόβουλο λογισμικό	Α	Α	Σ	Α
Διαδ.τρομοκρατία	Α	Σ	Α	Α
Η πιο συχνή μορφή	Σ	Σ	Σ	Σ
Έχετε πέσει θύμα;	Σ	Α	Α	Α
Αισθάνεσαι ότι κινδυνεύεις;	Α	Σ	Α	Α
Εμπιστοσύνη στις ικανότητες σου;	Σ	Σ	Α	Α
Λαμβάνετε μέτρα προστασίας;	Α	Α	Α	Α

Στον παραπάνω πίνακα φαίνονται όλες οι συσχετίσεις που πραγματοποιήσαμε συγκεντρωμένες, όπου με Α συμβολίζονται τα ζεύγη των μεταβλητών στα οποία δεν φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση και με Σ τα ζεύγη των μεταβλητών στα οποία φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση.

Έτσι, συμπεραίνουμε ότι οι ερωτήσεις ‘’Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας;’’ και ‘’Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Spamming(Ανεπιθύμητη αλληλογραφία)’’ είναι στατιστικά συσχετισμένες με το φύλο, την ηλικία, το μορφωτικό επίπεδο και με την απασχόληση ενώ οι ερωτήσεις ‘’Λαμβάνετε μέτρα για να προστατευτείτε από το Διαδικτυακό έγκλημα;’’ και ‘’Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της μορφής Παιδική πορνογραφία, Cracking και Hacking, Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων’’ δεν είναι στατιστικά συσχετισμένες με καμία από τις προηγούμενες μεταβλητές.

ΚΕΦΑΛΑΙΟ 5^{ο}

5.1 Μελέτη Κατανομών

Στο συγκεκριμένο κεφάλαιο θα πραγματοποιήσουμε έλεγχο καλής προσαρμογής μιας συνάρτησης πυκνότητας πιθανότητας (σ.π.π.) η οποία είναι:

i. Συμμετρική
ii. Αύξουσα
iii. Φθίνουσα

ως προς την κατανομή και οι παράμετροί της προσδιορίζονται μέσα από δειγματοληπτικά δεδομένα τα οποία είναι ομαδοποιημένα εντός κλάσεων. Με τον έλεγχο X^2 για καλή προσαρμογή διαπιστώνουμε εάν ένα δείγμα ακολουθεί μια συγκεκριμένη κατανομή πιθανοτήτων. Ο έλεγχος βασίζεται στη διαφορά μεταξύ των παρατηρούμενων συχνοτήτων των τιμών που λαμβάνει η τυχαία μεταβλητή στο δείγμα και των θεωρητικών συχνοτήτων των τιμών που πρέπει να εμφανίζει η τυχαία μεταβλητή εφόσον ακολουθεί την εξεταζόμενη κατανομή πιθανοτήτων.

5.1.1 Συνάρτηση πυκνότητας πιθανότητας της συμμετρικής κατανομής

Έστω μια τυχαία μεταβλητή Χ η οποία ακολουθεί μια συγκεκριμένη σ.π.π. Η συνάρτηση πυκνότητας πιθανότητας της συμμετρικής κατανομής ορίζεται από τον παρακάτω τύπο:

$$f(x)=\begin{cases} h(x-a)^k, & x\epsilon[a,\frac{a+b}{2}] \\ h(b-x)^k, & x\epsilon[\frac{a+b}{2},b] \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases} \quad \text{όπου } \kappa\neq-1 \qquad (5.1)$$

α: το κάτω όριο του πεδίου ορισμού της σ.π.π.

b: το άνω όριο του πεδίου ορισμού της σ.π.π.

Για τον υπολογισμό της σ.π.π. χρειαζόμαστε τις παρακάτω σχέσεις όπου m: προσωρινή δειγματική μέση τιμή, w: πλάτος της κάθε κλάσης και x_i: η κεντρική τιμή της κάθε κλάσης

<u>Μέση τιμή του δείγματος</u>: $\bar{x}=m + w\frac{T_1}{n}$ (5.2)

<u>Διακύμανση του δείγματος:</u> $s^2 = \frac{w^2}{n-1}(T_2 - \frac{T1^2}{n})$ (5.3)

<u>Τυπική απόκλιση του δείγματος</u>: $s = \sqrt{s^2}$ (5.4)

Συντελεστής μεταβλητότητας του δείγματος: $CV = \frac{s}{\bar{x}}$ (5.5)

Η παράμετρος $\lambda = CV^{-2}$ (5.6)

Η παράμετρος $k = \frac{-5+\sqrt{1+8\lambda}}{2}$ (5.7)

Η παράμετρος $h = \frac{(k+1)2^k}{(b-a)^{k+1}}$ όπου $k \neq -1$ (5.8)

5.1.2 Συνάρτηση πυκνότητας πιθανότητας της αύξουσας κατανομής

Έστω μια τυχαία μεταβλητή X η οποία ακολουθεί μια συγκεκριμένη σ.π.π. Η συνάρτηση πυκνότητας πιθανότητας της αύξουσας κατανομής ορίζεται από τον παρακάτω τύπο:

$$f(x)=\begin{cases} h(\frac{x}{b})^k, & x\epsilon[0,b] \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases} \quad \text{όπου } k \neq -1 \qquad (5.9)$$

b: το άνω όριο του πεδίου ορισμού της σ.π.π.

Για τον υπολογισμό της σ.π.π. χρειαζόμαστε τις παρακάτω σχέσεις όπου m: προσωρινή δειγματική μέση τιμή, w: πλάτος της κάθε κλάσης και x_i: η κεντρική τιμή της κάθε κλάσης και τις σχέσεις (5.2)-(5.6) .

$$k = -2+\sqrt{1+\lambda} \qquad (5.10)$$

$$h = \frac{k+1}{b} \qquad (5.11)$$

5.1.3 Συνάρτηση πυκνότητας πιθανότητας της φθίνουσας κατανομής

Έστω μια τυχαία μεταβλητή X η οποία ακολουθεί μια συγκεκριμένη σ.π.π. Η συνάρτηση πυκνότητας πιθανότητας της φθίνουσας κατανομής ορίζεται από τον παρακάτω τύπο:

$$f(x)=\begin{cases} h(1-\frac{x}{b})^k, & x\epsilon[0,b] \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases} \quad \text{όπου } k \neq -1 \qquad (5.12)$$

b: το άνω όριο του πεδίου ορισμού της σ.π.π.

Για τον υπολογισμό της σ.π.π. χρειαζόμαστε τις παρακάτω σχέσεις όπου m: προσωρινή δειγματική μέση τιμή, w: πλάτος της κάθε κλάσης και x_i: η κεντρική τιμή της κάθε κλάσης και τις σχέσεις (5.2)-(5.6) .

$$k = -1 + \frac{2}{\lambda - 1} \quad (5.13)$$

$$h = \frac{k+1}{b} \quad (5.14)$$

5.2 Παρουσίαση αποτελεσμάτων

Στην ερώτηση "Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος;" δοκιμάσαμε για την κάθε μορφή διαδικτυακού εγκλήματος ξεχωριστά αν μια διακριτή κατανομή μπορεί να εκφράσει τα δεδομένα. Δοκιμάσαμε την κατανομή Poisson και δεν απέδωσε. Έτσι, θεωρήσαμε την τυχαία μεταβλητή X συνεχή η οποία παίρνει τις τιμές i=0,1,2,3,4,5 με την έννοια ότι: x=i => x∈[i, i+1).

<u>Phishing και Pharming-Άνδρας</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.79, s^2=2.8018, s=1.67, CV=0.5986, λ=2.7908, k=-0.0851, h=0.1674

Άρα η σ.π.π. ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1674x^{-0.0851}, & x\epsilon[0,3) \\ 0.1674(6-x)^{-0.0851}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.1: ***Δεδομένα του δείγματος (Phishing και Pharming-Άνδρας)***

Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	31	-2	-62	124	29,1	33,02405
[1,2)	1.5	27	-1	-27	27	25,8	28,25581
[2,3)	**2.5**	28	0	0	0	24,6	31,86992
[3,4)	3.5	34	1	34	34	24,6	46,99187
[4,5)	4.5	16	2	32	64	25,8	9,922481
[5,6)	5.5	23	3	69	207	29,1	18,17869
Σύνολα		**159**		**46**	**456**	**159**	168,2428
X^2							**9,242832**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

H_0: Τα δεδομένα ακολουθούν την συμμετρική κατανομή

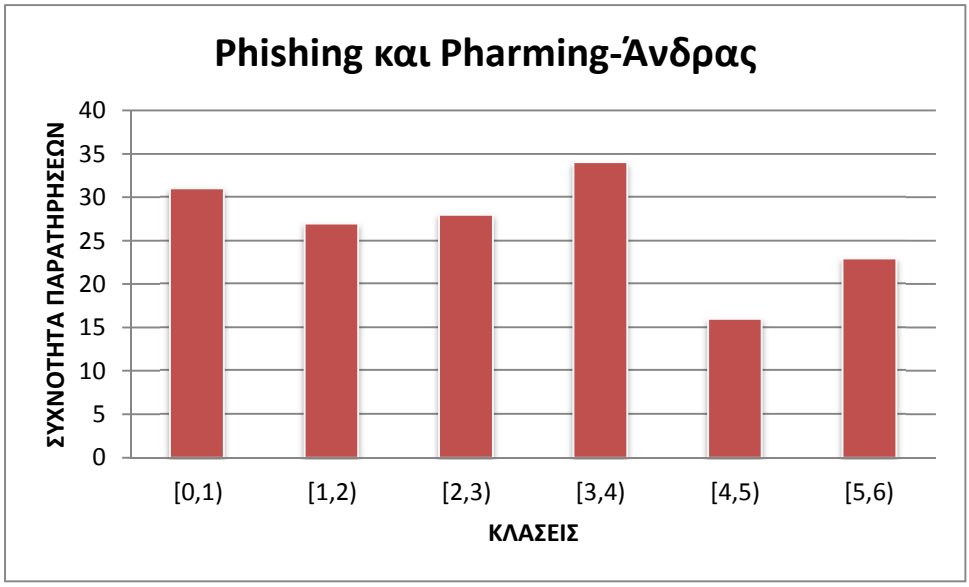
H_1: Τα δεδομένα δεν ακολουθούν την συμμετρική κατανομή

R={ $X^2 > X^2_{k-m-1}$}, όπου $X^2=\sum_{i=1}^{k}\frac{n_i^2}{\theta'_i}-n$

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=9.242832<X^2_{4;0.05}=9,4888$ σε επίπεδο σημαντικότητας 5%.

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.1: ***Συχνότητες παρατηρήσεων ανά κλάση (Phishing και Pharming-Άνδρας)***

Phishing και Pharming-Γυναίκα

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την φθίνουσα κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.1407, s^2=2.0268, s=1.42, CV=0.6636, λ=2.2708, ν=0.5738, h=0.2623

Άρα η σ.π.π. ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.2623(1-\frac{x}{6})^{0.5738}, & x\epsilon[0,6] \\ 0 & ,\alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.2: ***Δεδομένα του δείγματος (Phishing και Pharming-Γυναίκα)***

Κλάσεις	x_i	n_i	$x_i'=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	43	-2	-86	172	41,6	44,44712
[1,2)	1.5	44	-1	-44	44	37,1	52,18329
[2,3)	**2.5**	37	0	0	0	32,1	42,64798
[3,4)	3.5	25	1	25	25	26,5	23,58491

[4,5)	4.5	9	2	18	36	19,7	4,111675
[5,6)	5.5	9	3	27	81	10	8,1
Σύνολα		**167**		**-60**	**358**	**167**	175,075
X^2							**8,07496**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

H_0: Τα δεδομένα ακολουθούν την φθίνουσα κατανομή

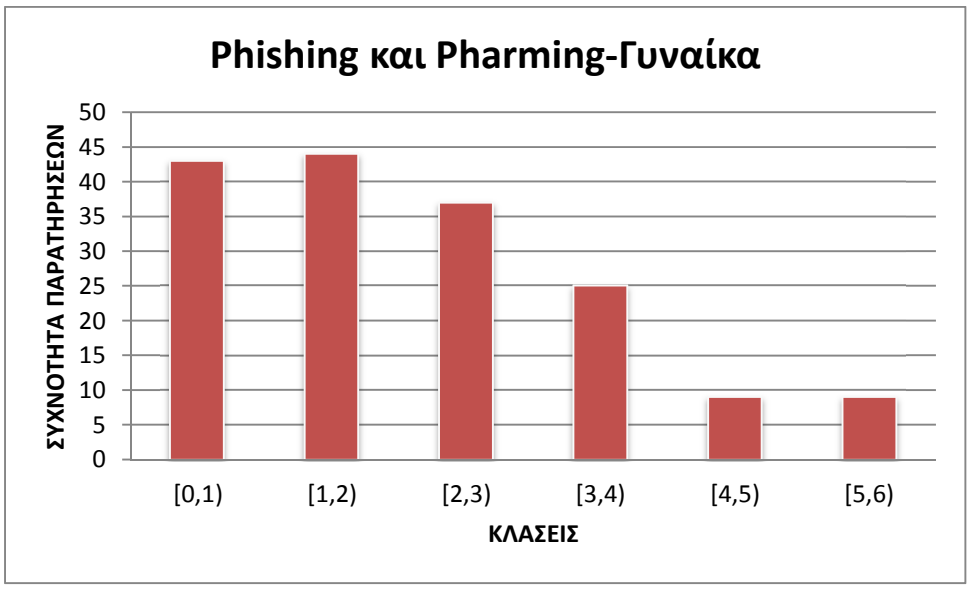
H_1: Τα δεδομένα δεν ακολουθούν την φθίνουσα κατανομή

R={ $X^2 > X^2_{k-m-1}$}, όπου $X^2 = \sum_{i=1}^{k} \frac{n_i^2}{\theta_i} - n$

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2 = 8.07496 < X^2_{4;0.05} = 9,4888$ σε επίπεδο σημαντικότητας 5%.

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την φθίνουσα κατανομή.



Διάγραμμα 5.2: ***Συχνότητες παρατηρήσεων ανά κλάση (Phishing και Pharming-Γυναίκα)***

<u>Spamming-Άνδρας</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την φθίνουσα κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=3.1478, s^2=3.0005, s=1.7322, CV=0.5503, λ=3.3022, ν=0.1181, h=0.1637

Άρα η σ.π.π. ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1637x^{0.1181}, & x\epsilon[0,3) \\ 0.1637(6-x)^{0.1181}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.3: ***Δεδομένα του δείγματος (Spamming-Άνδρας)***

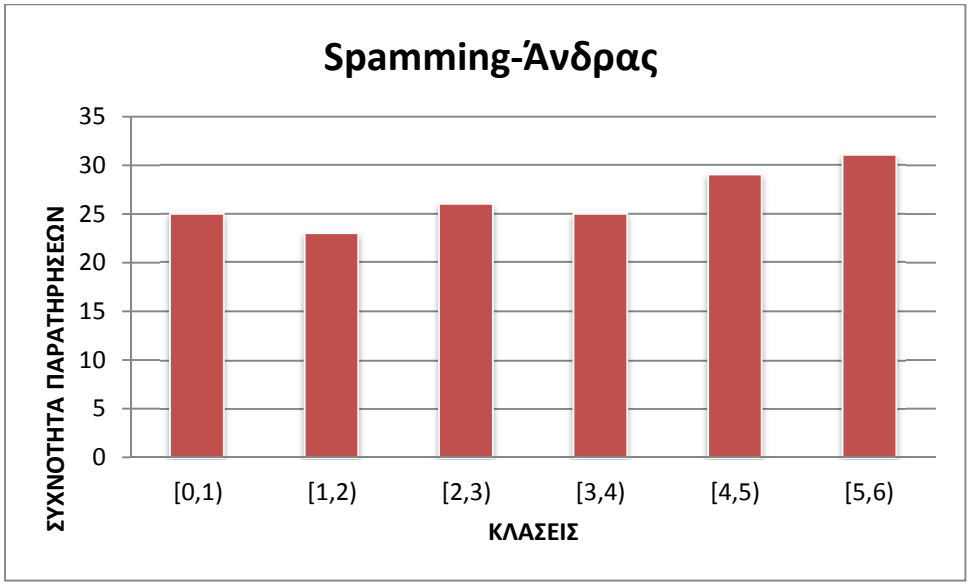
Κλάσεις	x_i	n_i	$x_{i'}=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	25	-2	-50	100	23,3	26,82403
[1,2)	1.5	23	-1	-23	23	27,3	19,37729
[2,3)	**2.5**	26	0	0	0	28,9	23,391
[3,4)	3.5	25	1	25	25	28,9	21,6263
[4,5)	4.5	29	2	58	116	27,3	30,80586
[5,6)	5.5	31	3	93	279	23,3	41,24464
Σύνολα		**159**		**103**	**543**	**159**	163,2691
X^2							**4,269121**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=4.269121<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.3: ***Συχνότητες παρατηρήσεων ανά κλάση (Spamming-Άνδρας)***

<u>Spamming-Γυναίκα</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.7874, s^2=2.1699, s=1.4731, CV=0.5285, λ=3.5802, ν=0.2222, h=0.1596

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1596x^{0.2222}, & x\epsilon[0,3) \\ 0.1596(6-x)^{0.2222}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.4: ***Δεδομένα του δείγματος (Spamming-Γυναίκα)***

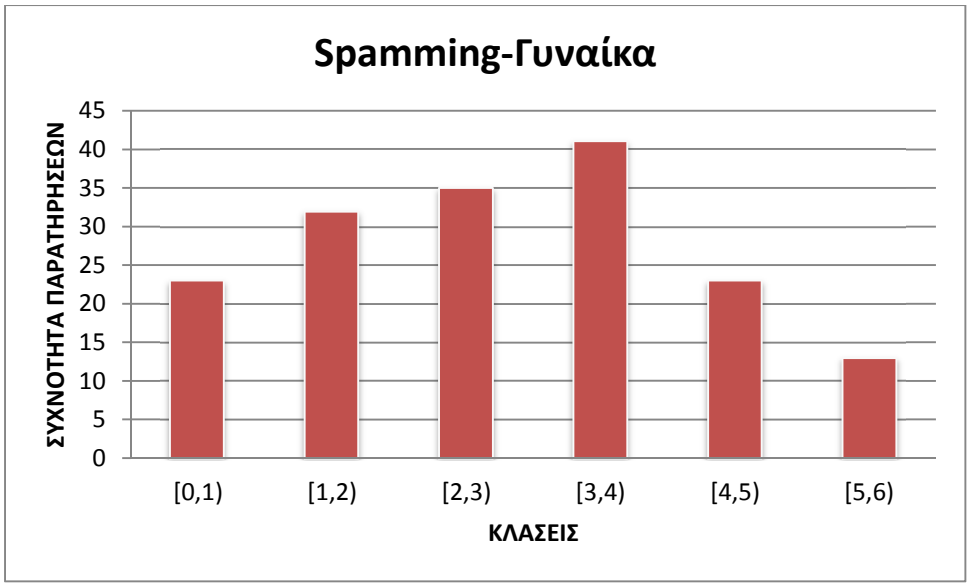
Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	23	-2	-46	92	21,8	24,26606
[1,2)	1.5	32	-1	-32	32	29,1	35,189
[2,3)	**2.5**	35	0	0	0	32,6	37,57669
[3,4)	3.5	41	1	41	41	32,6	51,56442
[4,5)	4.5	23	2	46	92	29,1	18,17869
[5,6)	5.5	13	3	39	117	21,8	7,752294
Σύνολα		**167**		**48**	**374**	**167**	174,5272
X^2							**7,527151**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

X^2=7.527151<$X^2_{4;0.05}$=9,4888

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.4: ***Συχνότητες παρατηρήσεων ανά κλάση (Spamming-Γυναίκα)***

<u>Απάτες μέσω Διαδικτύου-Γυναίκα</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.9192, s^2=2.5100, s=1.5843, CV=0.5427, λ=3.3953, ν=0.1534, h=0.1624

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1624x^{0.1534}, & x\epsilon[0,3) \\ 0.1624(6-x)^{0.1534}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.5: ***Δεδομένα του δείγματος (Απάτες μέσω Διαδικτύου-Γυναίκα)***

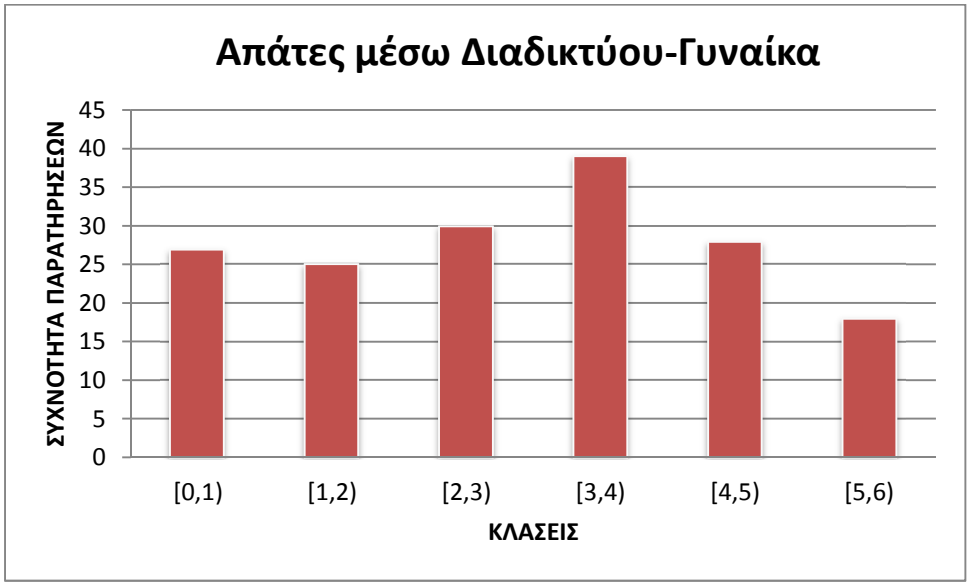
Κλάσεις	x_i	n_i	$x_{i'}=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	27	-2	-54	108	23,5	31,02128
[1,2)	1.5	25	-1	-25	25	28,8	21,70139
[2,3)	**2.5**	30	0	0	0	31,2	28,84615
[3,4)	3.5	39	1	39	39	31,2	48,75
[4,5)	4.5	28	2	56	112	28,8	27,22222
[5,6)	5.5	18	3	54	162	23,5	13,78723
Σύνολα		**167**		**70**	**446**	**167**	171,3283
X^2							**4,328276**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=4.328276<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.5: ***Συχνότητες παρατηρήσεων ανά κλάση (Απάτες μέσω Διαδικτύου-Γυναίκα)***

<u>Παιδική πορνογραφία-Άνδρας</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=3.0975, s^2=3.1534, s=1.7758, CV=0.5733, λ=3.0425, ν=0.0169, h=0.1664

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1664x^{0.0169}, & x\epsilon[0,3) \\ 0.1664(6-x)^{0.0169}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.6: ***Δεδομένα του δείγματος (Παιδική πορνογραφία-Άνδρας)***

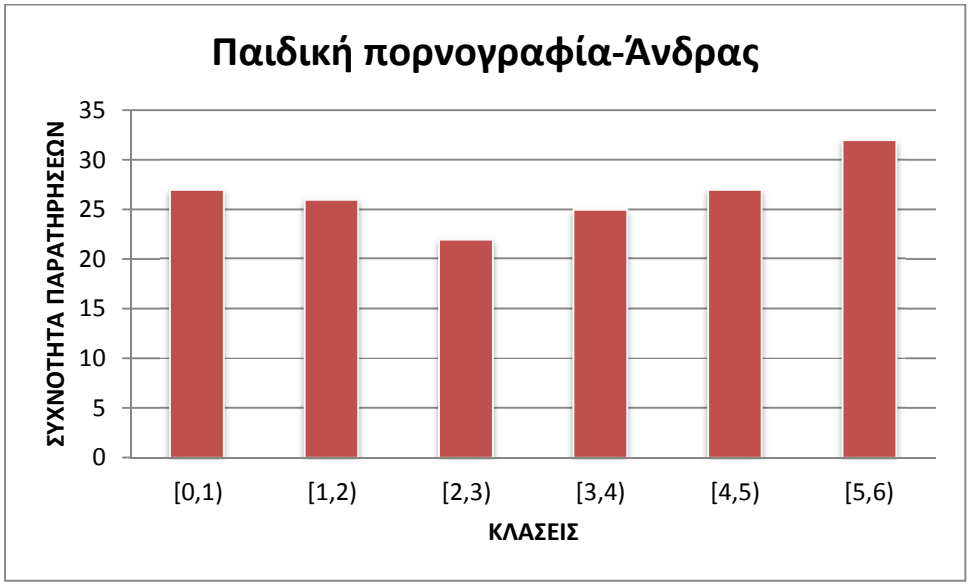
Κλάσεις	x_i	n_i	$x_i'=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	27	-2	-54	108	26	28,03846
[1,2)	1.5	26	-1	-26	26	26,6	25,41353
[2,3)	**2.5**	22	0	0	0	26,9	17,99257
[3,4)	3.5	25	1	25	25	26,9	23,2342
[4,5)	4.5	27	2	54	108	26,6	27,40602
[5,6)	5.5	32	3	96	288	26	39,38462
Σύνολα		**159**		**95**	**555**	**159**	161,4694
X^2							**2,469392**

Έλεγχος Καλής Προσαρμογής X^2

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=2.469392<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.6: ***Συχνότητες παρατηρήσεων ανά κλάση (Παιδική πορνογραφία-Άνδρας)***

<u>Παιδική πορνογραφία-Γυναίκα</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

$m=2.5$,$w=1$, $\bar{x}=3.0269$, $s^2=2.4797$, $s=1.5747$, $CV=0.5202$, $\lambda=3.6954$, $\nu=0.2642$, $h=0.1576$

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1576x^{0.2642}, & x\epsilon[0,3) \\ 0.1576(6-x)^{0.2642}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.7: ***Δεδομένα του δείγματος (Παιδική πορνογραφία-Γυναίκα)***

Κλάσεις	x_i	n_i	$x_i'=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	20	-2	-40	80	20,8	19,23077
[1,2)	1.5	28	-1	-28	28	29,2	26,84932

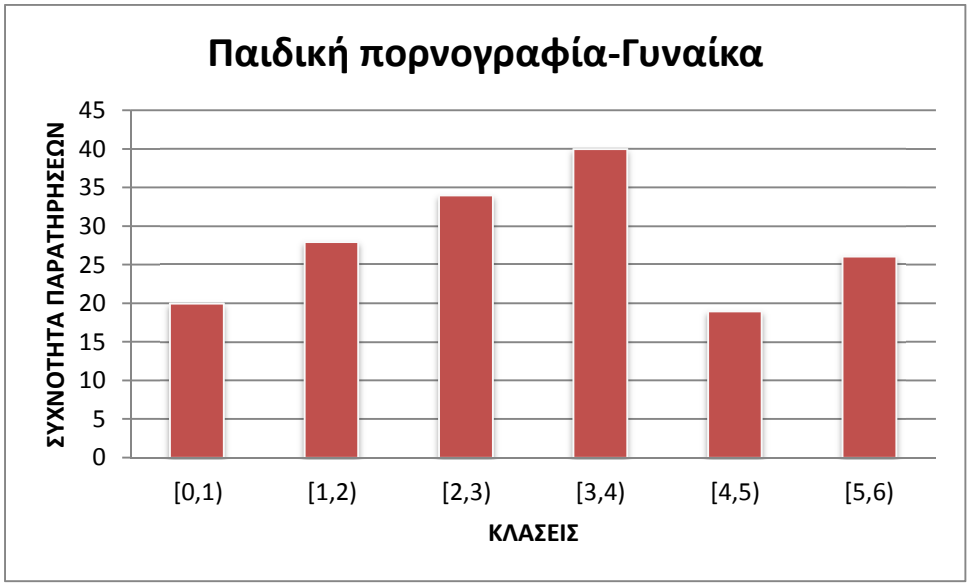
[2,3)	**2.5**	34	0	0	0	33,5	34,50746
[3,4)	3.5	40	1	40	40	33,5	47,76119
[4,5)	4.5	19	2	38	76	29,2	12,36301
[5,6)	5.5	26	3	78	234	20,8	32,5
Σύνολα		**167**		**88**	**458**	**167**	173,2118
X^2							**6,211755**

Έλεγχος Καλής Προσαρμογής X^2

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=6.211755<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.7: ***Συχνότητες παρατηρήσεων ανά κλάση (Παιδική Πορνογραφία-Γυναίκα)***

Διακίνηση/Πειρατεία λογισμικού-Άνδρας

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.9591, s^2=3.3258, s=1.8237, CV=0.6163, λ=2.6328, ν=-0.1515, h=0.1670

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1670x^{-0.1515}, & x\epsilon[0,3) \\ 0.1670(6-x)^{-0.1515}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.8: ***Δεδομένα του δείγματος (Διακίνηση/ Πειρατεία λογισμικού-Άνδρας)***

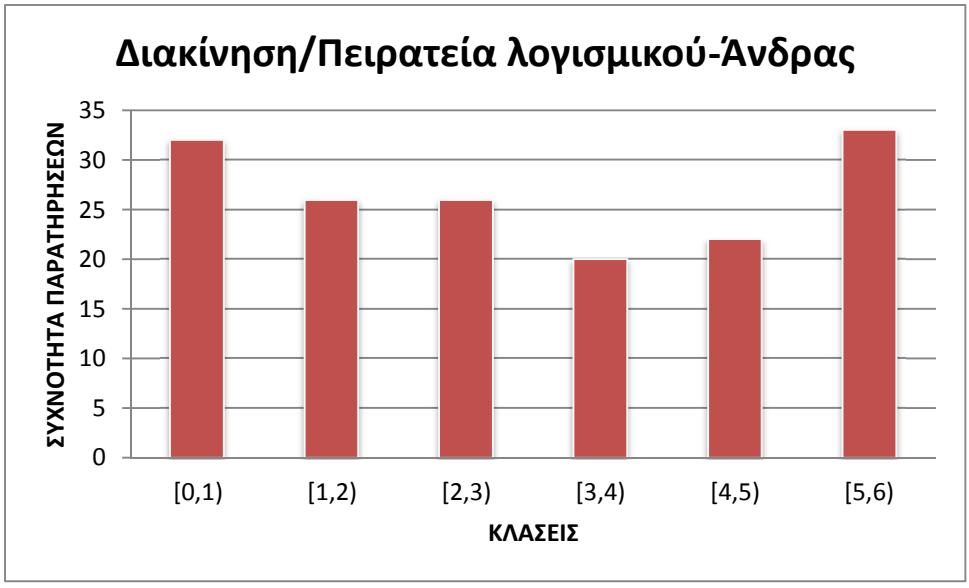
Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	32	-2	-64	128	31,3	32,71565
[1,2)	1.5	26	-1	-26	26	25,1	26,93227
[2,3)	**2.5**	26	0	0	0	23,1	29,26407
[3,4)	3.5	20	1	20	20	23,1	17,31602
[4,5)	4.5	22	2	44	88	25,1	19,28287
[5,6)	5.5	33	3	99	297	31,3	34,79233
Σύνολα		**159**		**73**	**559**	**159**	160,3032
X^2							**1,303213**

Έλεγχος Καλής Προσαρμογής X^2

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=1.303213<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.8: ***Συχνότητες παρατηρήσεων ανά κλάση (Διακίνηση/ Πειρατεία λογισμικού-Άνδρας)***

Διακίνηση/Πειρατεία λογισμικού-Γυναίκα

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την φθίνουσα κατανομή έχουμε:

$m=2.5$,$w=1$, $\bar{x}=2.3084$, $s^2=2.1317$, $s=1.4600$, $CV=0.6325$, $\lambda=2.4996$, $\nu=0.3337$, $h=0.2223$

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.2223(1-\frac{x}{6})^{0.3337}, x\epsilon[0,6] \\ 0 \qquad\qquad\qquad\qquad , \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.9: ***Δεδομένα του δείγματος (Διακίνηση /Πειρατεία λογισμικού-Γυναίκα)***

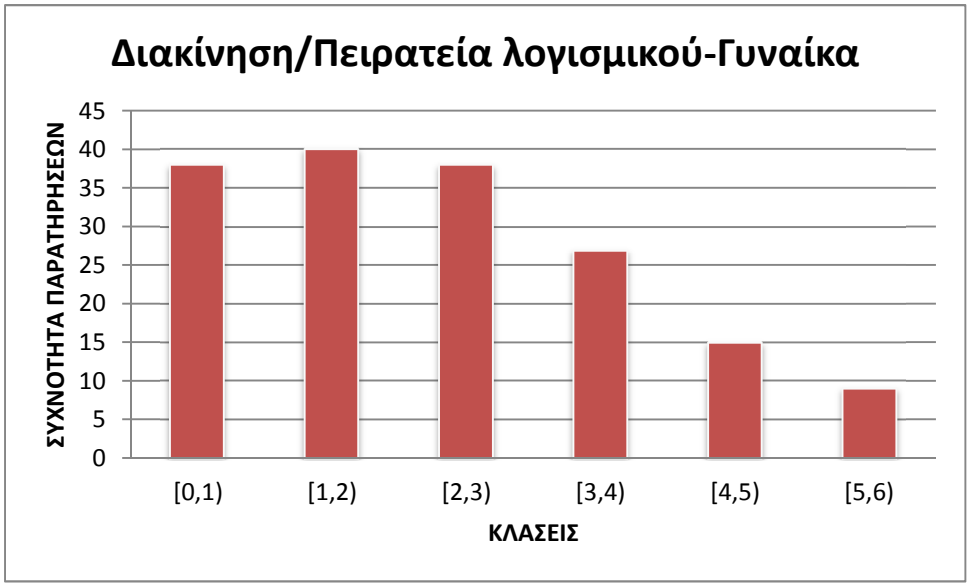
Κλάσεις	x_i	n_i	$x_i'=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	38	-2	-76	152	36	40,11111
[1,2)	1.5	40	-1	-40	40	33,7	47,47774
[2,3)	**2.5**	38	0	0	0	31	46,58065
[3,4)	3.5	27	1	27	27	27,7	26,31769
[4,5)	4.5	15	2	30	60	23,3	9,656652
[5,6)	5.5	9	3	27	81	15,3	5,294118
Σύνολα		**167**		**-32**	**360**	**167**	175,438
X^2							**8,437961**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=8.437961<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την φθίνουσα κατανομή.



Διάγραμμα 5.9: ***Συχνότητες παρατηρήσεων ανά κλάση (Διακίνηση/ Πειρατεία λογισμικού-Γυναίκα)***

Cyberbullying-Άνδρας

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την φθίνουσα κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.5881, s^2=2.8909, s=1.7003, CV=0.6570, λ=2.3167, ν=0.5189, h=0.2532

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.2532(1-\frac{x}{6})^{0.5189}, x\epsilon[0,6] \\ 0 \qquad\qquad\qquad\qquad , \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.10: ***Δεδομένα του δείγματος (Cyberbullying-Άνδρας)***

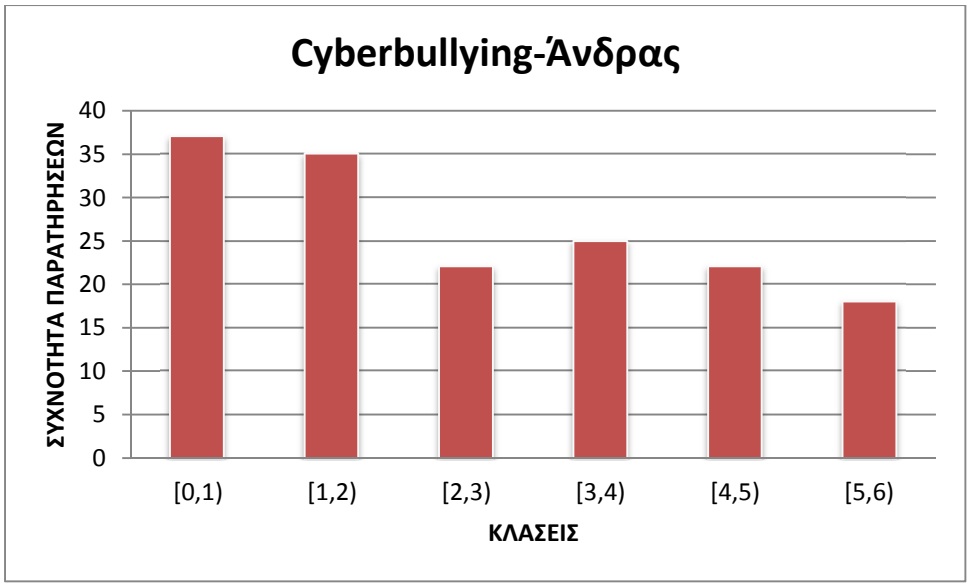
Κλάσεις	x_i	n_i	$x_i'=\frac{x_i-m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i'=n\cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	37	-2	-74	148	38,5	35,55844
[1,2)	1.5	35	-1	-35	35	34,6	35,40462
[2,3)	**2.5**	22	0	0	0	30,4	15,92105
[3,4)	3.5	25	1	25	25	25,5	24,5098
[4,5)	4.5	22	2	44	88	19,5	24,82051
[5,6)	5.5	18	3	54	162	10,5	30,85714
Σύνολα		**159**		**14**	**458**	**159**	167,0716
X^2							**8,071578**

Έλεγχος Καλής Προσαρμογής X^2

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

X^2=8.071578<$X^2_{4;0.05}$=9,4888

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την φθίνουσα κατανομή.



Διάγραμμα 5.10: ***Συχνότητες παρατηρήσεων ανά κλάση (Cyberbullying-Άνδρας)***

<u>Κακόβουλο λογισμικό-Άνδρας</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την αύξουσα κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=3.1666, s^2=2.9831, s=1.7272, CV=0.5454, λ=3.3618, ν=-0.0885, h=0.1814

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1814\left(\frac{x}{6}\right)^{-0.0885}, & x\epsilon[0,6] \\ 0 \quad , & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.11: ***Δεδομένα του δείγματος (Κακόβουλο λογισμικό-Άνδρας)***

Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	24	-2	-48	96	22,6	25,48673
[1,2)	1.5	23	-1	-23	23	25,5	20,7451
[2,3)	**2.5**	27	0	0	0	26,7	27,30337
[3,4)	3.5	24	1	24	24	27,5	20,94545
[4,5)	4.5	30	2	60	120	28,1	32,02847
[5,6)	5.5	31	3	93	279	28,6	33,6014
Σύνολα		**159**		**106**	**542**	**159**	160,1105
X^2							**1,110517**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

H_0: Τα δεδομένα ακολουθούν την αύξουσα κατανομή

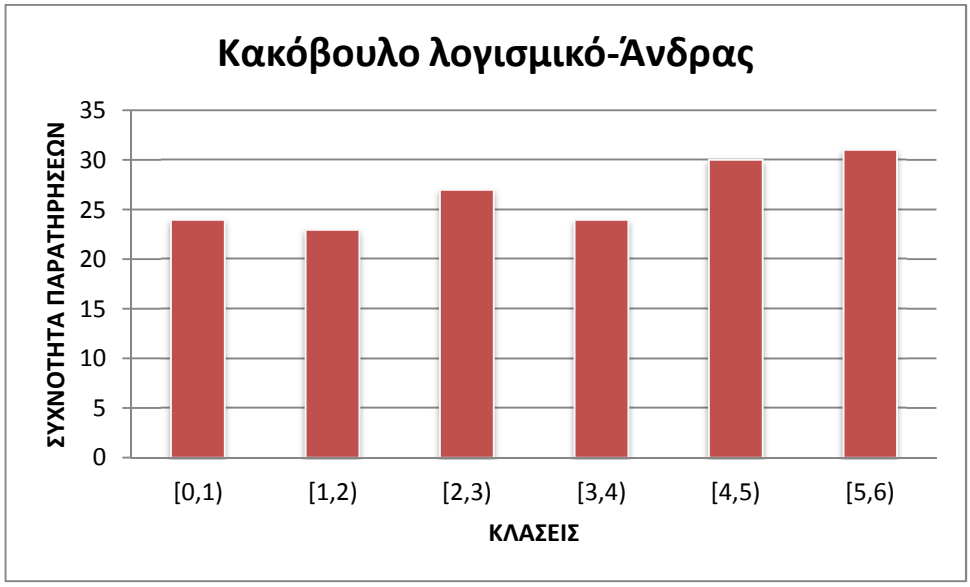
H_1: Τα δεδομένα δεν ακολουθούν την αύξουσα κατανομή

R={ $X^2 > X^2_{k-m-1}$}, όπου $X^2 = \sum_{i=1}^{k} \frac{n_i^2}{\theta_i} - n$

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2 = 1.110517 < X^2_{4;0.05} = 9{,}4888$ σε επίπεδο σημαντικότητας 5%.

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την αύξουσα κατανομή.



Διάγραμμα 5.11: ***Συχνότητες παρατηρήσεων ανά κλάση (Κακόβουλο λογισμικό-Άνδρας)***

<u>Κακόβουλο λογισμικό-Γυναίκα</u>

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την συμμετρική κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.8293, s^2=2.5596, s=1.5999, CV=0.5655, λ=3.1270, ν=0.0503, h=0.1656

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.1656x^{0.0503}, & x\epsilon[0,3) \\ 0.1656(6-x)^{0.0503}, & x\epsilon[3,6) \\ 0, & \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.12: ***Δεδομένα του δείγματος (Κακόβουλο λογισμικό-Γυναίκα)***

Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	28	-2	-56	112	26,3	29,80989

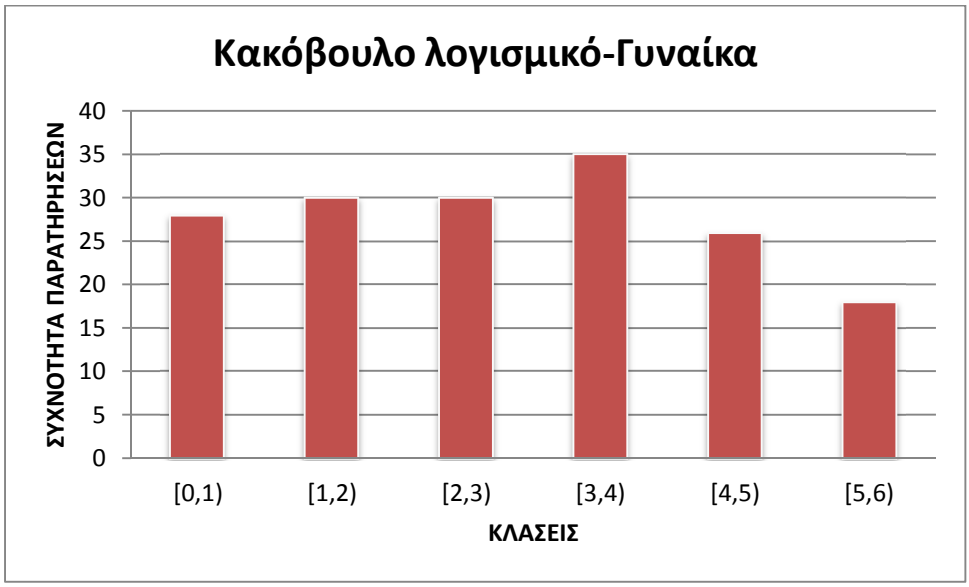
[1,2)	1.5	30	-1	-30	30	28,2	31,91489
[2,3)	**2.5**	30	0	0	0	29	31,03448
[3,4)	3.5	35	1	35	35	29	42,24138
[4,5)	4.5	26	2	52	104	28,2	23,97163
[5,6)	5.5	18	3	54	162	26,3	12,31939
Σύνολα		**167**		**55**	**443**	**167**	171,2917
X^2							**4,291664**

Έλεγχος Καλής Προσαρμογής X^2

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=4.291664<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την συμμετρική κατανομή.



Διάγραμμα 5.12: ***Συχνότητες παρατηρήσεων ανά κλάση (Κακόβουλο λογισμικό-Γυναίκα)***

Διαδικτυακή τρομοκρατία-Γυναίκα

Τα δεδομένα του δείγματος παρουσιάζονται στον παρακάτω πίνακα και σύμφωνα με τις σχέσεις που αφορούν την φθίνουσα κατανομή έχουμε:

m=2.5 ,w=1, $\bar{x}$=2.1407, s^2=2.1593, s=1.4695, CV=0.6865, λ=2.1219, ν=0.7827, h=0.2971

Άρα η σ.π.π ορίζεται από τον τύπο:

$$f(x)=\begin{cases} 0.2971(1-\frac{x}{6})^{0.7827}, x\epsilon[0,6] \\ 0 \qquad\qquad\qquad\qquad , \alpha\lambda\lambda o\acute{\upsilon} \end{cases}$$

Πίνακας 5.13: ***Δεδομένα του δείγματος (Διαδικτυακή τρομοκρατία-Γυναίκα)***

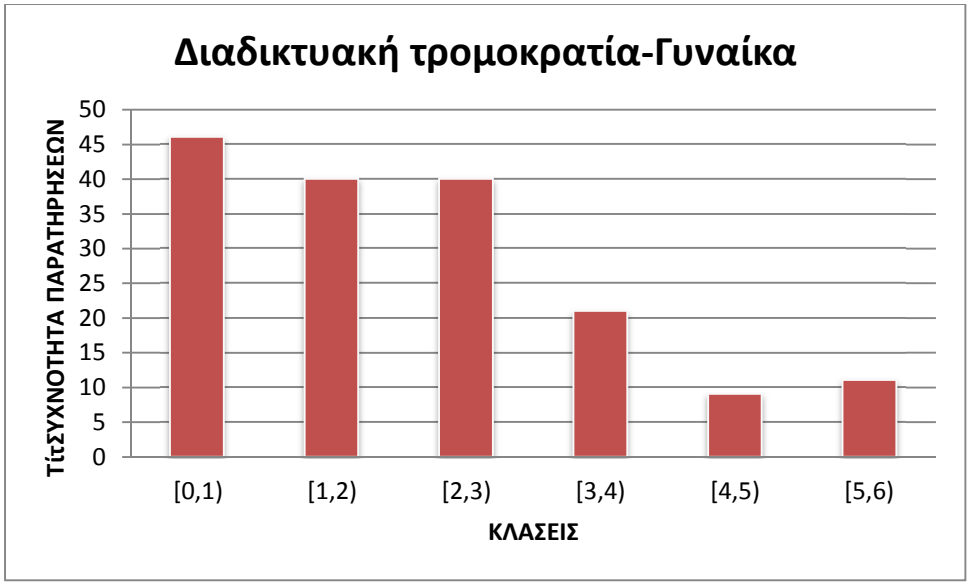
Κλάσεις	x_i	n_i	$x_i' = \frac{x_i - m}{w}$	$n_i \cdot x_i'$	$n_i \cdot x_i'^2$	$\theta_i' = n \cdot p_i$	$\frac{n_i^2}{\theta_i'}$
[0,1)	0.5	46	-2	-92	184	46,3	45,70194
[1,2)	1.5	40	-1	-40	40	39,6	40,40404
[2,3)	**2.5**	40	0	0	0	32,5	49,23077
[3,4)	3.5	21	1	21	21	25	17,64
[4,5)	4.5	9	2	18	36	16,7	4,850299
[5,6)	5.5	11	3	33	99	6,9	17,53623
Σύνολα		**167**		**-60**	**380**	**167**	175,3633
X^2							**8,363285**

<u>Έλεγχος Καλής Προσαρμογής X^2</u>

Σύμφωνα με τα στοιχεία του πίνακα παρατηρούμε ότι:

$X^2=8.363285<X^2_{4;0.05}=9,4888$

Συνεπώς, δεχόμαστε την μηδενική υπόθεση ότι τα δεδομένα ακολουθούν την φθίνουσα κατανομή.



Διάγραμμα 5.13: ***Συχνότητες παρατηρήσεων ανά κλάση (Διαδικτυακή τρομοκρατία-Γυναίκα)***

Όλες οι υπόλοιπες περιπτώσεις δεν ακολουθούν καμία από τις προηγούμενες τρεις κατανομές.

Πίνακας 5.14: ***Συγκεντρωτικός πίνακας κατανομών***

	Άνδρας	**Γυναίκα**
Phishing και Pharming	Συμμετρική κατανομή	Φθίνουσα κατανομή
Spamming	Συμμετρική κατανομή	Συμμετρική κατανομή
Απάτες μέσω διαδικτύου	Δεν ακολουθούν καμία από τις 3 κατανομές	Συμμετρική κατανομή
Παιδική πορνογραφία	Συμμετρική κατανομή	Συμμετρική κατανομή
Cracking και Hacking	Δεν ακολουθούν καμία από τις 3 κατανομές	Δεν ακολουθούν καμία από τις 3 κατανομές
Διακίνηση/Πειρατεία λογισμικού	Συμμετρική κατανομή	Φθίνουσα κατανομή
Διακίνηση ναρκωτικών	Δεν ακολουθούν καμία από τις 3 κατανομές	Δεν ακολουθούν καμία από τις 3 κατανομές
Cyberbullying	Φθίνουσα κατανομή	Δεν ακολουθούν καμία από τις 3 κατανομές
Κακόβουλο λογισμικό	Αύξουσα κατανομή	Συμμετρική κατανομή
Διαδικτυακή τρομοκρατία	Δεν ακολουθούν καμία από τις 3 κατανομές	Φθίνουσα κατανομή

Στον παραπάνω πίνακα φαίνονται συγκεντρωμένα όλα τα αποτελέσματα από την μελέτη κατανομών που πραγματοποιήσαμε στο συγκεκριμένο κεφάλαιο.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Μετά την στατιστική ανάλυση των δεδομένων ακολούθησε η διεξαγωγή συμπερασμάτων όπου παρουσιάζονται στην συνέχεια τα σημαντικότερα:

- Σχεδόν το 94% των Ελλήνων χρηστών έχουν πρόσβαση στο διαδίκτυο τουλάχιστον μια φορά την ημέρα. Το ποσοστό είναι πολύ μεγάλο και δείχνει την ραγδαία εξέλιξη του διαδικτύου αλλά και την τεράστια εξάρτηση του ανθρώπου από το διαδίκτυο.

- Ιδιαίτερο ενδιαφέρον παρουσιάζει το ποσοστό των χρηστών που δεν ξέρουν αν έχουν πέσει θύμα απάτης του διαδικτυακού εγκλήματος το οποίο αγγίζει το 11%. Παρόλο που το ποσοστό των ανδρών που έχει πέσει θύμα είναι σχεδόν το διπλάσιο από το ποσοστό των γυναικών, το ποσοστό των ανδρών που δεν ξέρει αν έχει πέσει θύμα είναι το μισό από το ποσοστό των γυναικών.

- Η διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων είναι η μορφή διαδικτυακού εγκλήματος η οποία κατέχει το μεγαλύτερο ποσοστό (31.3%) σύμφωνα με το οποίο οι χρήστες δεν αισθάνονται καθόλου ενημερωμένοι για τους κινδύνους αυτής της μορφής και συγχρόνως η μορφή η οποία παρουσιάζει το μικρότερο ποσοστό (0.3%) στην ερώτηση ‘’Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακού εγκλήματος;’’.

- Το κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι) είναι η μορφή διαδικτυακού εγκλήματος η οποία κατέχει το μεγαλύτερο ποσοστό (32.2%) στο επίπεδο του πολύ έως πάρα πολύ σχετικά με την ενημέρωσή τους για τους κινδύνους αυτής της μορφής και συγχρόνως η μορφή η οποία παρουσιάζει το μεγαλύτερο ποσοστό (28.5%) στην ερώτηση ‘’Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακού εγκλήματος;’’.

- Επίσης, παρατηρούμε ότι το κακόβουλο λογισμικό είναι η μοναδική μορφή διαδικτυακού εγκλήματος σύμφωνα με την οποία το δείγμα των ανδρών όσον αφορά την ερώτηση ‘’Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος;’’ ακολουθεί αύξουσα κατανομή πιθανοτήτων.

- Η μορφή στην οποία οι χρήστες έχουν πέσει περισσότερο θύμα απάτης είναι το κακόβουλο λογισμικό (ποσοστό 62.6%) και η αμέσως επόμενη είναι το spamming (ποσοστό 48.6%) ενώ η μορφή στην οποία δεν έχει πέσει κανένας θύμα είναι η διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων.

- Σχεδόν το 20% από τους γονείς δεν λαμβάνουν μέτρα πρόληψης για τα παιδιά τους ενώ το 9% δεν ξέρει αν λαμβάνει μέτρα πρόληψης.

- Όσον αφορά τα μέτρα αντιμετώπισης του διαδικτυακού εγκλήματος, το μεγαλύτερο ποσοστό 75.7% πιστεύει ότι η Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος πρέπει να πάρει μέτρα αντιμετώπισης αυτού του φαινομένου. Ωστόσο, μόνο το 8.4% από αυτούς που έχουν πέσει θύμα ανέφεραν την αρνητική τους εμπειρία στην Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος ενώ το 24.2% δεν το ανέφεραν σε κανέναν.

- Το ενδιαφέρον είναι ότι όσον αφορά την αίσθηση κινδύνου και την εμπιστοσύνη που έχουν στις ικανότητές τους κατά την πλοήγηση στο διαδίκτυο, μόνο μεταξύ της ηλικίας φαίνεται να υπάρχει μια στατιστικά σημαντική συσχέτιση. Ενώ μεταξύ φύλου, μορφωτικού επιπέδου και απασχόλησης δεν διαφέρουν οι απόψεις τους σημαντικά.

ΠΑΡΑΡΤΗΜΑ

Ερωτηματολόγιο

Θέμα: “Διαδικτυακό έγκλημα”

Η έρευνα γίνεται στο πλαίσιο της διπλωματικής μου εργασίας για το Πρόγραμμα Μεταπτυχιακών Σπουδών στην Επιστήμη του Διαδικτύου του τμήματος Μαθηματικών του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης και είναι εντελώς ανώνυμη. Οπότε σας παρακαλώ να είστε ειλικρινείς στις απαντήσεις σας. Οι ερωτήσεις με το * είναι υποχρεωτικές για την υποβολή του ερωτηματολογίου.

Σας ευχαριστώ πολύ!

Χριστίνα Θωμοπούλου

* Required

Φύλο *

- ☐ Άνδρας
- ☐ Γυναίκα

Ηλικία *

- ☐ 12-18
- ☐ 19-30
- ☐ 31-45
- ☐ 46 και άνω

Ποιο είναι το μορφωτικό σας επίπεδο; *

Όσοι είναι μαθητές ή φοιτητές να απαντήσουν μια από τις δυο τελευταίες επιλογές αντίστοιχα.

- ☐ Πρωτοβάθμια εκπαίδευση(Δημοτικό)
- ☐ Δευτεροβάθμια εκπαίδευση(Γυμνάσιο, Λύκειο)
- ☐ Τριτοβάθμια εκπαίδευση(ΑΕΙ/ΤΕΙ)
- ☐ Μαθητής/Μαθήτρια
- ☐ Φοιτητής/Φοιτήτρια

Απασχόληση *

- ☐ Ιδιωτικός υπάλληλος

- ☐ Δημόσιος υπάλληλος
- ☐ Ελεύθερος επαγγελματίας
- ☐ Φοιτητής/Φοιτήτρια
- ☐ Μαθητής/Μαθήτρια
- ☐ Οικιακά
- ☐ Συνταξιούχος
- ☐ Άνεργος
- ☐ Other: _____

Πόσο συχνά έχεις πρόσβαση στο Διαδίκτυο; *

- ☐ Τουλάχιστον μια φορά την ημέρα
- ☐ Τουλάχιστον μια φορά την εβδομάδα
- ☐ Λιγότερο συχνά

Για ποιες από τις ακόλουθες δραστηριότητες χρησιμοποιείς το Διαδίκτυο; *

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- ☐ Email
- ☐ Ενημέρωση
- ☐ Κοινωνικά μέσα δικτύωσης(facebook, twitter, κλπ)
- ☐ Για αγορές
- ☐ e-banking(τραπεζικές και χρηματιστηριακές συναλλαγές)
- ☐ Παιχνίδια
- ☐ Τηλεόραση
- ☐ Για πώληση προϊόντων ή υπηρεσιών
- ☐ Other: _____

Πόσο ενημερωμένος/η αισθάνεσαι για τους κινδύνους της κάθε μορφής διαδικτυακού εγκλήματος; *

	Καθόλου	Λίγο	Μέτρια	Αρκετά	Πολύ	Πάρα πολύ
Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")	☐	☐	☐	☐	☐	☐

	Καθόλου	Λίγο	Μέτρια	Αρκετά	Πολύ	Πάρα πολύ
Spamming(Ανεπιθύμητη αλληλογραφία)	☐	☐	☐	☐	☐	☐
Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος,πιστωτικές κάρτες,κλπ)	☐	☐	☐	☐	☐	☐
Παιδική πορνογραφία	☐	☐	☐	☐	☐	☐
Cracking και Hacking	☐	☐	☐	☐	☐	☐
Διακίνηση-Πειρατεία λογισμικού	☐	☐	☐	☐	☐	☐
Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων	☐	☐	☐	☐	☐	☐
Cyberbullying(Διαδικτυακός εκφοβισμός)	☐	☐	☐	☐	☐	☐
Κακόβουλο λογισμικό (Ιοί,σκουλήκια,δούρειοι ίπποι)	☐	☐	☐	☐	☐	☐
Διαδικτυακή τρομοκρατία	☐	☐	☐	☐	☐	☐

Ποια πιστεύετε ότι είναι η πιο συχνή μορφή διαδικτυακής εγκληματικότητας; *

- ☐ Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")
- ☐ Spamming(Ανεπιθύμητη αλληλογραφία)
- ☐ Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος,Πιστωτικές κάρτες,κλπ)
- ☐ Παιδική πορνογραφία
- ☐ Cracking και Hacking
- ☐ Διακίνηση-Πειρατεία λογισμικού
- ☐ Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων
- ☐ Cyberbullying(Διαδικτυακός εκφοβισμός)
- ☐ Κακόβουλο λογισμικό (Ιοί,σκουλήκια,δούρειοι ίπποι)

- [ ] Διαδικτυακή τρομοκρατία
- [ ] Other: _____

Έχετε πέσει ποτέ θύμα διαδικτυακού εγκλήματος; *

- [ ] Ναι
- [ ] Όχι
- [ ] Δεν ξέρω

Αν ναι, σε ποια μορφή;

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- [ ] Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")
- [ ] Spamming(Ανεπιθύμητη αλληλογραφία)
- [ ] Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος, Πιστωτικές κάρτες, κλπ)
- [ ] Παιδική πορνογραφία
- [ ] Cracking και Hacking
- [ ] Διακίνηση-Πειρατεία λογισμικού
- [ ] Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων
- [ ] Cyberbullying(Διαδικτυακός εκφοβισμός)
- [ ] Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι)
- [ ] Διαδικτυακή τρομοκρατία
- [ ] Other: _____

Αν έχεις πέσει θύμα διαδικτυακού εγκλήματος σε ποιον ανέφερες την αρνητική σου εμπειρία;

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- [ ] Φίλος/η
- [ ] Γονείς
- [ ] Αδελφός/η
- [ ] Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος
- [ ] Σε κανέναν
- [ ] Other: _____

Αν δεν έχεις πέσει θύμα διαδικτυακού εγκλήματος, τότε αν έπεφτες που θα απευθυνόσουνα;

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- [ ] Φίλος/η
- [ ] Γονείς
- [ ] Αδελφός/η
- [ ] Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος
- [ ] Σε κανέναν
- [ ] Other: _____

Ξέρεις ή έχεις ακούσει για κάποιον γνωστό που έχει πέσει θύμα εγκλήματος μέσω Διαδικτύου;*

- [ ] Ναι
- [ ] Όχι
- [ ] Δεν ξέρω

Αν ναι, σε ποια μορφή;

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- [ ] Phishing και Pharming (Ηλεκτρονικό "ψάρεμα")
- [ ] Spamming(Ανεπιθύμητη αλληλογραφία)
- [ ] Απάτες μέσω Διαδικτύου(Διαδικτυακός τζόγος, Πιστωτικές κάρτες, κλπ)
- [ ] Παιδική πορνογραφία
- [ ] Cracking και Hacking
- [ ] Διακίνηση-Πειρατεία λογισμικού
- [ ] Διακίνηση ναρκωτικών και άλλων επικίνδυνων πραγμάτων
- [ ] Cyberbullying(Διαδικτυακός εκφοβισμός)
- [ ] Κακόβουλο λογισμικό(Ιοί, σκουλήκια, δούρειοι ίπποι)
- [ ] Διαδικτυακή τρομοκρατία
- [ ] Other: _____

Κατά την πλοήγηση σου στο Διαδίκτυο πόσο αισθάνεσαι ότι κινδυνεύεις; *

- [ ] Καθόλου
- [ ] Λίγο
- [ ] Μέτρια
- [ ] Αρκετά
- [ ] Πολύ
- [ ] Πάρα πολύ

Έχεις εμπιστοσύνη στις ικανότητές σου να χρησιμοποιείς το Διαδίκτυο; *

- ☐ Καθόλου
- ☐ Λίγο
- ☐ Μέτρια
- ☐ Αρκετά
- ☐ Πολύ
- ☐ Πάρα πολύ

Λαμβάνετε μέτρα για να προστατευτείτε από το διαδικτυακό έγκλημα; *

- ☐ Ναι
- ☐ Όχι
- ☐ Δεν ξέρω

Αν ναι, τι μέτρα;

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- ☐ Τεχνολογική προστασία(antvirus,firewall,κλπ)
- ☐ Προστασία των κωδικών πρόσβασης
- ☐ Δεν αποκαλύπτω προσωπικά δεδομένα
- ☐ Διαβάζω πάντα τους όρους χρήσης πριν κάνω εγγραφή
- ☐ Other: _____

Ποιος πιστεύετε ότι πρέπει να πάρει μέτρα αντιμετώπισης για το διαδικτυακό έγκλημα; *

Μπορείτε να επιλέξετε περισσότερες από μια απαντήσεις.

- ☐ Γονείς
- ☐ Μέσα μαζικής ενημέρωσης
- ☐ Εκπαίδευση
- ☐ Αστυνομία/Δίωξη ηλεκτρονικού εγκλήματος
- ☐ Νομοθεσία
- ☐ Other: _____

Αν είστε γονείς, λαμβάνετε μέτρα πρόληψης για τα παιδιά σας;

Σε αυτήν την ερώτηση να απαντήσουν μόνο όσοι είναι γονείς.

- ☐ Ναι
- ☐ Όχι
- ☐ Δεν ξέρω

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική:

Βλαχόπουλος Κ. (2007). *Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση*. Νομική Βιβλιοθήκη, Αθήνα.

Δαφέρμος Β. (2011). *Κοινωνική Στατιστική & Μεθοδολογία Έρευνας με το SPSS*. Εκδόσεις Ζήτη, Θεσσαλονίκη.

Ζάννη Αν. (2005). *Το διαδικτυακό έγκλημα*. Αντ. Ν. Σακκούλας, Αθήνα.

Ίδρυμα Μαραγκοπούλου για τα Δικαιώματα του ανθρώπου & Κιουπής Δ. (2007). *Η παιδική πορνογραφία στο διαδίκτυο*. Νομική βιβλιοθήκη, Αθήνα.

Κολυβά-Μαχαίρα Φ. (1998). *Μαθηματική Στατιστική Τόμος Ι Εκτιμητική*. Εκδόσεις Ζήτη, Θεσσαλονίκη

Κολυβά-Μαχαίρα Φ. & Μπόρα-Σέντα Ε. (1999). *Στατιστική: Θεωρία και Εφαρμογές*. Εκδόσεις Ζήτη, Θεσσαλονίκη

Κριθαράς Ν. Θεόδωρος (2009). *Ποινικό δίκαιο και διαδίκτυο*. Νομική Βιβλιοθήκη, Αθήνα.

Λάζος Γρ. (2001). *Πληροφορική και Έγκλημα*. Νομική Βιβλιοθήκη, Αθήνα.

Λάζος Γρ. (2007). *Κριτική Εγκληματολογία*. Νομική Βιβλιοθήκη, Αθήνα.

Τσαντάς Ν. και Μωυσιάδης Χρ. και Μπαγιάτης Κ. και Χατζηπαντελής Θ. (1999). *Ανάλυση Δεδομένων με τη βοήθεια Στατιστικών πακέτων*. Εκδόσεις Ζήτη, Θεσσαλονίκη.

Φαρμάκης Ν. (2009$^{\alpha}$). *Εισαγωγή στη δειγματοληψία*. Εκδόσεις Χριστοδουλίδη, Θεσσαλονίκη.

Φαρμάκης Ν. (2001). *Στατιστική: Περιληπτική Θεωρία-Ασκήσεις*. Εκδόσεις Χριστοδουλίδη, Θεσσαλονίκη.

Φαρμάκης Ν. (2009$^{\beta}$). *Δημοσκοπήσεις και Δεοντολογία*. Εκδόσεις Χριστοδουλίδη, Θεσσαλονίκη.

Furnell S. & Μηλιώνη Φ. (2006). *Κυβερνοέγκλημα: Καταστρέφοντας την κοινωνία της πληροφορίας*. Παπαζήση, Αθήνα

Ξενόγλωσση:

Farmakis N. (2003). *Estimation of coefficient of variation: Scaling of Symmetric Continuous Distributions*. Statistics in Transition, June 2003 Vol.6, No1, pp 83-96

Farmakis N. (2010). *Coefficient of Variation: Connecting Sampling with some Increasing Distribution Models.*

Farmakis N. (2011) *Coefficient of Variation: Connecting Sampling with some Decreasing Distribution Models*.

Greenwood P.E. & Nikulin M.S. (1996). *A guide to chi-squared testing. Wiley, New York.*

Majid Yar (2006). *Cybercrime and Society*. Thousand Oaks, CA: Sage Publications, London.

Mandras N. (2002). *Lectures on Monte Carlo methods*. American Mathematical Society, Providence, R.I.

Robert C & Casella G. (1999). *Monte Carlo statistical methods*. Springer, New York.

Sheehan B. (1999). *Using e-mail to survey Internet users in the United States: methodology and assessment*. Journal of Computer Mediated Communication.

Yaman Akdeniz (2008). *Internet Child Pornography and the Law*: National and International Responses. Journal of High Technology Law.

Ηλεκτρονικές πηγές:

http://www.pi.ac.cy/InternetSafety/

http://www.astynomia.gr/newsite.php?&lang=

http://www.inhope.org/gns/home.aspx

http://www.safeline.gr/

http://youth-health.gr/

http://www.epapers.gr/