ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

στη «Δημόσια Διοίκηση»

MPA

Διπλωματική Εργασία

ΨΗΦΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΚΑΙ ΑΣΦΑΛΕΙΑ: ΤΡΟΠΟΙ ΕΞΑΠΑΤΗΣΗΣ ΤΩΝ ΕΛΛΗΝΩΝ ΧΡΗΣΤΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΟΙ ΣΥΝΕΠΕΙΕΣ

ΧΟΥΛΙΑΡΑ ΜΑΡΙΑ- ΕΛΕΝΗ (Α.Μ. 0070)

Επιβλέπων καθηγητής : Δρ. Πανόπουλος Αναστάσιος

Καστοριά

Σεπτέμβριος, 2024

ΕΥΧΑΡΙΣΤΙΕΣ

Με την παρούσα διπλωματική εργασία ολοκληρώνονται οι σπουδές μου στο μεταπτυχιακό πρόγραμμα σπουδών «ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ» του Πανεπιστημίου Δυτικής Μακεδονίας.

Στις σπουδές μου, ήταν καθοριστική η συμβολή των καθηγητών μου στα γνωστικά αντικείμενα που παρακολούθησα, στους οποίους οφείλω να εκφράσω τις ειλικρινείς μου ευχαριστίες για τη συμβολή τους στην ολοκλήρωση των σπουδών μου.

Ιδιαίτερα, επιθυμώ να ευχαριστήσω τον καθηγητή μου και επιβλέποντα την παρούσα διπλωματική εργασία, κ. Αναστάσιο Πανόπουλο, για την επιστημονική και συμβουλευτική καθοδήγηση που μου προσέφερε σε όλα τα στάδια εκπόνησης της εργασίας με τις εύστοχες και πολύ εποικοδομητικές παρατηρήσεις του.

Τέλος, ευχαριστώ θερμά την οικογένειά μου, αφού για ακόμη μια φορά στάθηκε δίπλα μου και σε αυτή την προσπάθειά μου και αποτέλεσε την κινητήριο δύναμη για να ολοκληρωθεί και αυτός ο στόχος που είχα θέσει, αυτός του μεταπτυχιακού.

ΠΕΡΙΛΗΨΗ

Το κυβερνοέγκλημα αποτελεί μια σύγχρονη μορφή εγκλήματος μέσω του διαδικτύου που βρίσκεται σε διαρκή εξέλιξη. Η παρούσα εργασία μελετάει το κυβερνοέγκλημα στην Ελλάδα. Με τη χρήση ενός ερωτηματολογίου που απαντήθηκε από 300 ερωτώμενους, με μεγάλη εκπροσώπηση από την Ελληνική περιφέρεια, τόσο ανδρών όσο και γυναικών και υψηλού μορφωτικού επιπέδου Έλληνες, εξετάζονται διάφορες πτυχές του προβλήματος της παρενόχλησης μέσω διαδικτύου που γίνεται για εγκληματικούς σκοπούς, όπως η συχνότητά του, οι μορφές που λαμβάνει, οι οικονομικές και άλλες αιτίες του, οι στρατηγικές πειθούς των θυμάτων, οι συνέπειες που έχει (οικονομικές, ψυχολογικές, κοινωνικές) και πλήθος άλλων θεμάτων ώστε να διερευνηθεί το κυβερνοέγκλημα σε μεγάλη έκταση, με βάση την άποψη των θυμάτων και όχι των αρχών ή τρίτων που δεν έχουν βρεθεί από την πλευρά του θύματος.

Από την έρευνα αυτή διαπιστώνεται ότι το κυβερνοέγκλημα και η παρενόχληση μέσω διαδικτύου αποτελεί μια σύγχρονη «Λερναία Ύδρα» με πολλά πρόσωπα. Δεκάδες μορφές παρενόχλησης λαμβάνουν χώρα στο σύνολο της ελληνικής περιφέρειας και ο αριθμός των παρενοχλήσεων ανά ερωτώμενο, είναι επίσης μεγάλος. Αν και το ένα-τρίτο του δείγματος δεν φαίνεται να έχει υποστεί κάποια παρενόχληση (ή να το έχει αντιληφθεί), ωστόσο τα υπόλοιπα δύο-τρίτα, δηλαδή δύο στους τρεις Έλληνες με βάση το δείγμα, έχει υποστεί κάποιας μορφής παρενόχληση. Πιο συχνές είναι οι περιπτώσεις με δήθεν κέρδη από λαχνούς και λαχεία, μέσω «ψαρέματος» (phishing), εξαπάτησης σε σχέση με χρηματικά ποσά από την ΑΑΔΕ ή άλλες αρχές ή από δήθεν κληρονομιές. Τα κίνητρα των δραστών είναι κατά μείζονα λόγο οικονομικά, αλλά φαίνεται ότι παρουσιάζονται πως δήθεν θέλουν να προστατέψουν την ασφάλεια και την προστασία της ιδιωτικής ζωής των θυμάτων τους. Δηλαδή, παραβιάζουν ή «εισέρχονται» από την ίδια «είσοδο» την οποία τα θύματα επιθυμούν να μην παραβιαστεί. Επίσης ακολουθούν και την στρατηγική να πείθουν για την «αξιοπιστία» τους. Η χρήση αληθοφανών ιστοσελίδων είναι ευρέως διαδεδομένη. Η συχνότητα της παρενόχλησης είναι πολύ μεγάλη γιατί ένας στους πέντε έχει δεχτεί παρενόχληση συχνά, πολύ συχνά ή καθημερινά.

Κυριότερες αιτίες της παρενόχλησης, είναι η έλλειψη μέσων προφύλαξης και εκπαίδευσης ως καταναλωτών, η υπερέκθεση προσωπικών δεδομένων και οι

τεχνολογικές εξελίξεις. Παρόλα αυτά, οι αιτίες εντοπίζεται ότι είναι πιο σύνθετες και όχι μόνο μια ανά περίπτωση. Επίσης σύμφωνα με το δείγμα, η Ελληνική Αστυνομία και οι Αρχές αποτυγχάνουν στο ρόλο της προστασίας των Ελλήνων πολιτών, αλλά αυτό μπορεί να οφείλεται και στη φύση του προβλήματος που προκαλεί αδυναμία ελέγχου του αγαθού της ασφάλειας. Τα παραπάνω, δημιουργούν την εικόνα ενός πολύ μεγάλου και ακανθώδους προβλήματος για την Ελληνική κοινωνία και οικονομία, η έκταση και η σημασία του οποίου δεν έχουν εκτιμηθεί καλά και χρειάζεται να μελετηθούν ακόμη καλύτερα, ώστε οι πολιτικές να προσαρμοστούν κατά τρόπο συστηματικό και αποτελεσματικό στη φύση του προβλήματος.

Λέξεις κλειδιά: Κυβερνοέγκλημα, Κυβερνοαπάτη, Παρενόχληση μέσω διαδικτύου, Εξαπάτηση, Αιτίες εξαπάτησης, Μορφές εξαπάτησης

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Η μεγάλη διάδοση της χρήσης των υπολογιστών στην εποχή μας έχει επιφέρει ταυτοχρόνως και αύξηση της διαδικτυακής απάτης, έχει αυξήσει κατά πολύ τις περιπτώσεις παρενόχλησης των χρηστών του διαδικτύου και έχει επιφέρει μεγαλύτερη εκμετάλλευσή τους. Η εξαπάτηση αυτή έχει πολλές συνέπειες, όπως οικονομικές, κοινωνικές και άλλες.

Τα ζητήματα ασφάλειας του διαδικτύου ποικίλλουν και έχουν αποτελέσει ξεχωριστό αντικείμενο μελέτης σε πλήθος άρθρων και βιβλίων (Garg and Nilizadeh, 2013; Badawi and Jourdan, 2020; Mabunda, 2018), εξεταζόμενα από διάφορες σκοπιές. Τη βιβλιογραφία απασχολεί ιδιαίτερα η αυξανόμενη συχνότητα του κυβερνοεγκλήματος και της παρενόχλησης, η έκταση που έχει λάβει, οι διάφοροι τρόποι και στρατηγικές πειθούς που χρησιμοποιούνται από τους θύτες για να εκμεταλλευτούν τα θύματα, το πώς και γιατί αντιδρούν τα θύματα, το τί κάνει τα θύματα πιο ευάλωτα, το πώς μπορεί να προληφθεί το πρόβλημα και ποιές πολιτικές μπορούν να το αντιμετωπίσουν, προληπτικά ή κατασταλτικά (Gopal κ.ά., 2022, Cross, 2019, Kshetri, 2013, Bera κ.α., 2023, Grazioli and Jarvenpaa (2014)). Ένα τμήμα της σχετικής αρθρογραφίας και βιβλιογραφίας εστιάζει σε τεχνικά ζητήματα χρήσης του διαδικτύου και ένα στο είδος των προβλημάτων ασφάλειας που παρουσιάζονται (Badawi and Jourdan, 2020). Ένα σκέλος επίσης εστιάζει στις συνέπειες που υπάρχουν για τους καταναλωτές από τη χρήση του διαδικτύου και των εφαρμογών του (Drew and Webster, 2023, EU, 2024, Cross, 2019, Hansen, 2024)

Ωστόσο, όπως επισημαίνουν οι Bartolleti κ.α. (2021) υπάρχει έλλειψη αξιόπιστων δημόσιων δεδομένων σχετικών με την εξαπάτηση και απουσία μιας καλής ταξινόμησης των διαφόρων εξαπατήσεων, γιατί σε πολλές περιπτώσεις μια εξαπάτηση κατηγοριοποιείται σε μια εσφαλμένη κατηγορία. Το πρόβλημα της πρόσβασης σε δεδομένα ιδιωτικού περιεχομένου που αφορούν ένα έγκλημα σε βάρος κάποιου είναι μεγάλο και μόνο σε περιπτώσεις όπου υπάρχουν τέτοια δεδομένα, επειδή συλλέγονται από δευτερογενείς πηγές, μπορεί να γίνει κάποια έρευνα με τη χρήση δεδομένων.

Τα φαινόμενα εξαπάτησης είναι πολλά, αρκετά συχνά και λαμβάνουν διαφορετικές μορφές. Ερωτήσεις που γίνονται τυχαία σε καταναλωτές ή άλλους χρήστες του διαδικτύου όπως: «σας ενδιαφέρει μια μερικής απασχόλησης εργασία;», «θέλετε να

πάρετε ένα δώρο;» «θέλετε να συμμετάσχετε στην αγορά νομισμάτων με σημαντικά κέρδη;» και άλλες πολλές, υποκρύπτουν την εκμετάλλευση του ερωτώμενου-θύματος από τον ερωτώντα-θύτη. Η προσέγγιση των χρηστών γίνεται είτε απευθείας, μέσα από τη χρήση υπολογιστή, είτε πρώτα μέσω τηλεφώνου και στη συνέχεια μέσω υπολογιστή είτε ακόμα και μέσω της χρήσης των κοινωνικών δικτύων (όπως το Instagram, το Facebook, το Tik-Tok, κ.ά.).

Όταν μέσω του διαδικτύου συντελείται μια εγκληματική δραστηριότητα, τότε αυτή αποκαλείται κυβερνοέγκλημα. Το κυβερνοέγκλημα αποτελεί ειδική κατηγορία εγκλήματος τόσο ως προς την μελέτη του όσο και ως προς τον τρόπο αντιμετώπισής του.

Σε σχέση με άλλες μορφές εγκλήματος υπάρχει μια ειδοποιός διαφορά: Για να συμβεί το κυβερνοέγκλημα χρειάζεται οπωσδήποτε μια ενέργεια από πλευράς του καταναλωτή και χρήστη του διαδικτύου. Ενώ, δηλαδή, μια κλοπή μπορεί να γίνει εξωτερικά (σε έναν δρόμο, στην οικεία κτλ) χωρίς ενέργεια από πλευράς θύματος, για να γίνει το κυβερνοέγκλημα, το θύμα που είναι και χρήστης του διαδικτύου χρειάζεται όχι μόνο να ανοίξει τον υπολογιστή του, αλλά και να κάνει και κάποια δεύτερη συμπληρωματική ενέργεια, όπως π.χ. το να επιλέξει να επισκεφτεί μια ιστοσελίδα που του προτείνεται, να ανοίξει ένα ηλεκτρονικό μήνυμα ή κάποιο συνημμένο σε αυτό (κείμενο ή πηγή κτλ). Πολλές φορές μάλιστα, κάνει κάτι αρκετά περισσότερο από αυτό. Η ενέργεια που προηγείται από πλευράς του κυβερνοεγκληματία και έχει ως σκοπό την εκμετάλλευση του χρήστη, αποτελεί μια παρενόχληση που γίνεται με σκοπό την εξαπάτηση. Πρόκειται για παρενόχληση επειδή παρενοχλείται ο χρήστης του διαδικτύου, αλλά και γιατί σκοπός της παρενόχλησης αυτής είναι η εκμετάλλευσή του.

Το κυβερνοέγκλημα λαμβάνει διάφορες μορφές, όπως για παράδειγμα τα εγκλήματα κλοπής ταυτότητας (identify theft), χρησιμοποίησης e-mail τρίτων (email spoofing), τα οικονομικά κυβερνοεγκλήματα, η παρακολούθηση μέσω διαδικτύου (cyberstalking) και άλλα, όπως αυτά που είναι σχετικά με τη διακίνηση ναρκωτικών, τη σωματεμπορία κ.ά. (Batra κ.α., 2020). Τα πρόσωπα που επιδιώκουν να διαπράξουν το κυβερνοέγκλημα είναι επικίνδυνα και αποτελούν τους λεγόμενους κυβερνοεγκληματίες. Υπάρχουν διάφοροι τύποι κυβερνοεγκληματιών, όπως είναι για παράδειγμα οι χάκερς (hackers), οι κράκερς (crackers), οι ακτιβιστές-χάκερς (hacktivists) και χάκερς που στοχεύουν τα κράτη-έθνη (nation-statehackers) (Batra κ.α., 2020).

Τα διάφορα μηνύματα που αποστέλλονται στους χρήστες του διαδικτύου αποκαλούνται στα αγγλικά «spams» και αποτελούν μια παρενόχληση και, ουσιαστικά, την έναρξη μιας διαδικασίας παρενόχλησης σε βάρος του θύματος. Γνωστές μορφές παρενόχλησης με σκοπό την εξαπάτηση είναι το «phishing» («ψάρεμα») μέσω ιστοσελίδων (URLs) και e-mails, τα πυραμιδοειδή σχήματα Πόντζι και διάφορες μορφές κακόβουλων λογισμικών. Επίσης, μια ειδική μορφή κυβερνοεγκλήματος που αναπτύσσεται ραγδαία είναι όσα συνδέονται με τα κρυπτονομίσματα.

Στην κατηγορία των πιο επικίνδυνων περιπτώσεων κυβερνοαπάτης βρίσκονται τα λεγόμενα «επενδυτικά προγράμματα υψηλής απόδοσης» (high yield investment programs - HYIPs) που υπόσχονται πολύ υψηλές αποδόσεις σε άμεσο χρονικό διάστημα (Badawi and Jourdan, 2020). Στην κατηγορία αυτή, εντάσσονται επίσης περιπτώσεις ξεπλύματος μαύρου χρήματος (money laundering), τα κακόβουλα λογισμικά που απειλούν (ransomware), καθώς και περιπτώσεις εξαπάτησης των χρηστών ή καταναλωτών (scams).

Η εξαπάτηση στην Ελλάδα, γίνεται με διάφορους τρόπους, όπως με ανάρτηση ψευδών ειδήσεων σε ψευδείς ιστοσελίδες, που σε ορισμένες περιπτώσεις φαίνεται να έχουν προέλθει από έγκριτες εφημερίδες ή ιστοσελίδες και σε ορισμένες περιπτώσεις συνοδεύονται και από ανάλογο οπτικοακουστικό υλικό (Ο.Τ., 2024). Το κράτος έχει ήδη μεριμνήσει για την οργάνωση πολιτικών αντιμετώπισης, ανάλογων προς τα προβλήματα που παρουσιάζονται (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).Όμως, ερευνητικά έχουν γίνει πολύ λίγα σχετικά με την κατανόηση του προβλήματος, σε σχέση με την παγκόσμια βιβλιογραφία και αυτό είναι πιθανόν έναν κομμάτι του προβλήματος. Παρά τα πολλά άρθρα στον τύπο και τις πολιτικές από το κράτος, από την αναζήτηση που έγινε σε παγκόσμια βάση άρθρων βρέθηκε μόνο μια έρευνα σχετικά με την Ελλάδα και αυτή από το 2011. Η έρευνα των Vlachos κ.α. (2011) είναι πολύ παλιά, δεδομένης της ταχύτατης εξέλιξης στον κλάδο των υπολογιστών και της πολύ μεγάλης εξάπλωσης του κυβερνοεγκλήματος την τελευταία δεκαπενταετία. Η έρευνα αυτή, με τίτλο «Το τοπίο του κυβερνοεγκλήματος στην Ελλάδα» είχε στηριχθεί σε δευτερογενή δεδομένα, που συνέλεγε τότε η ειδική Ομάδα Εργασίας που είχε συσταθεί εκείνη την περίοδο για το κυβερνοέγκλημα.

Επειδή οι χρήστες στη χώρα μας αυξάνονται, ειδικά μετά τον Covid-19 και την έλευση μιας εποχής όπου οι υπηρεσίες του Ελληνικού κράτους ψηφιοποιούνται και οι μεγαλύτερες γενιές (εκτός από τις μικρότερες), μαθαίνουν να χρησιμοποιούν το

διαδίκτυο, τα πιθανά θύματα και ο αριθμός των κρούσεων παρενόχλησης αυξάνεται εκθετικά. Για όλα αυτά τα θύματα τίθεται θέμα προστασίας και ασφάλειας, δηλαδή της κατοχύρωσης ενός δημόσιου αγαθού, απέναντι σε μια καινούργια μορφή απειλής.
Στην παρούσα μεταπτυχιακή εργασία, αφού αναλυθούν και εξεταστούν στη βιβλιογραφία οι έννοιες και οι μορφές του κυβερνοεγκλήματος και της παρενόχλησης που γίνεται μέσω του διαδικτύου, με σκοπό την εξαπάτηση και ορισμένα χαρακτηριστικά της εξαπάτησης αυτής που την κάνουν περισσότερο προσιτή στα θύματα και αφορούν τις στρατηγικές πειθούς και τους τρόπους θυματοποίησης που χρησιμοποιούνται από τους θύτες, θα παρουσιαστούν τα αποτελέσματα της έρευνας που σχεδιάστηκε και χρησιμοποίησε ερωτηματολόγιο που συμπληρώθηκε με τη βοήθεια του GoogleForms και θα σχολιαστούν. Στο τέλος της εργασίας εξάγονται χρήσιμα συμπεράσματα σχετικά με την έρευνα που έγινε.

ΕΡΕΥΝΗΤΙΚΑ ΕΡΩΤΗΜΑΤΑ

Τα τέσσερα κύρια ερευνητικά ερωτήματα που τίθενται είναι τα εξής:

1. Ποιές μορφές λαμβάνει η παρενόχληση με σκοπό την εξαπάτηση του καταναλωτή και χρήστη του διαδικτύου στην Ελλάδα;
2. Ποιές συνέπειες υπάρχουν για τους καταναλωτές και χρήστες του διαδικτύου;
3. Πώς αντιμετωπίζεται και αν επαρκούν οι πολιτικές και τα μέτρα που λαμβάνουν χώρα;
4. Σε ποιά κατάσταση βρίσκεται η Ελλάδα και η Ελληνική περιφέρεια, από πλευράς κυβερνοεγκλήματος και παρενόχλησης και πώς μπορεί να περιγραφεί καλύτερα το πρόβλημα αυτό;

ΣΤΟΧΟΙ / ΣΚΟΠΟΙ

Σκοπός της παρούσας εργασίας, είναι να διερευνηθεί η έκταση και η σημασία των παρενοχλήσεων που αποσκοπούν στην εξαπάτηση των καταναλωτών στην Ελλάδα και οι οποίες αποτελούν τμήμα του κυβερνοεγκλήματος. Συγκεκριμένα, επιχειρείται να κατανοηθεί το πώς χρησιμοποιείται το διαδίκτυο στην Ελλάδα σε βάρος των Ελλήνων χρηστών του (όσων δηλαδή διαμένουν στην Ελλάδα), ως προς την παρενόχληση που γίνεται με σκοπό την εξαπάτηση, με βάση την εμπειρία των ίδιων των χρηστών του.

Γίνεται προσπάθεια να γίνουν κατανοητές οι μορφές που λαμβάνει η παρενόχληση στην Ελλάδα, πώς θυματοποιούνται οι χρήστες του διαδικτύου, ποιές στρατηγικές πειθούς χρησιμοποιούνται για να τους εξαπατήσουν, οι συνέπειες στα θύματα και εξετάζεται επίσης και το πώς αξιολογούν οι ίδιοι οι χρήστες το ρόλο των δημόσιων αρχών για την αντιμετώπιση του αυξανόμενου αυτού τύπου εγκλήματος. Η εργασία αναμένεται να συμβάλλει στην ενημέρωση των επιστημόνων στον κλάδο, για το πρόβλημα της παρενόχλησης μέσω διαδικτύου στην Ελλάδα και τις συνέπειες του.

Για τον σκοπό της έρευνας, επιδιώχθηκε σε αρχικό στάδιο να αντληθούν στοιχεία σε πανελλαδικό επίπεδο, μέσα από την επικοινωνία με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας που ασχολείται με το ηλεκτρονικό έγκλημα και την απάτη. Δυστυχώς, η συγκέντρωση των στοιχείων αυτών δεν κατέστη δυνατή λόγω του προβλήματος της εμπιστευτικότητας των στοιχείων, γιατί -ας μην λησμονούμε- πρόκειται για μια μορφή εγκλήματος και μάλιστα σοβαρή και σε διαρκή εξάπλωση. Για το λόγο αυτό, η έρευνα στράφηκε αναγκαστικά (προκειμένου να χρησιμοποιηθεί και η ανάλογη μέθοδος) στα ίδια τα θύματα, τους Έλληνες χρήστες του διαδικτύου και έγινε μια προσπάθεια δημιουργίας μιας συνολικής εικόνας για το πρόβλημα της παρενόχλησης σε σχέση και με τα παραπάνω ερευνητικά ερωτήματα.

ΔΟΜΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

Η εργασία αποτελείται από τέσσερα κεφάλαια. Μετά την εισαγωγή, στο πρώτο κεφάλαιο αναλύεται η σχετική αρθρογραφία και βιβλιογραφία. Πιο συγκεκριμένα, εξηγείται τί είναι το κυβερνοέγκλημα, περιγράφονται οι διάφορες μορφές που λαμβάνει, τονίζεται η ανάπτυξη που λαμβάνει κατά την τελευταία 30ετία και η συχνότητά του σε άλλες χώρες, οι αιτίες που το προκαλούν, οι συναρτώμενες με τις αιτίες στρατηγικές και τακτικές πειθούς των θυμάτων, με βάση τη διαθέσιμη βιβλιογραφία. Σε αυτό το κεφάλαιο επιδιώκεται να δοθεί και μια εικόνα για το ποιοί είναι οι κυριότεροι τρόποι και μέθοδοι παρενόχλησης των θυμάτων με σκοπό την εξαπάτησή τους.

Επίσης, παρουσιάζονται οι κύριες συνέπειες που έχει η παρενόχληση όταν αυτή επιτυγχάνει τον σκοπό της (οικονομικές, ψυχολογικές, κοινωνικές, ως προς τον άνθρωπο-θύμα αλλά και στο σύνολο). Τέλος, γίνεται μια σύντομη περιγραφή των

πολιτικών για το κυβερνοέγκλημα, με βάση την Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Στο δεύτερο κεφάλαιο, παρουσιάζεται η μεθοδολογία που υιοθετήθηκε για την παρούσα εργασία. Για την επίτευξη του παραπάνω σκοπού και των επιμέρους στόχων, χρησιμοποιήθηκε για την έρευνα αυτή ερωτηματολόγιο που απευθύνθηκε σε μεγάλο αριθμό αποστολέων (όπως ομάδες φοιτητών και εργαζομένων, αστυνομικές υπηρεσίες και άλλων πολιτών), με σκοπό τη διερεύνηση του φαινομένου της παρενόχλησης μέσα από διάφορες πτυχές αλλά και την μελέτη της παροχής του αγαθού της δημόσιας ασφάλειας σε σχέση με αυτό. Η έρευνα είναι ποιοτική και τα ευρήματά της παρουσιάζονται με διαγράμματα-πίτες, ανάλυση σε κλίμακα likert και ανάλυση με ιστογράμματα. Οι περισσότερες από τις ερωτήσεις επιδέχονταν πάνω από μια απάντηση (εφόσον και το φαινόμενο λαμβάνει διάφορες μορφές και τα θύματά του παρενοχλούνται με διαφορετικούς τρόπους) και για αυτό οι μετρήσεις δεν είναι όλες στην κλίμακα της τάξης του 100%. Η μόνη διάκριση που κάνουμε, είναι μεταξύ θυμάτων και μη θυμάτων (όσων δηλαδή δεν δέχτηκαν ποτέ παρενόχληση).

Με τη χρήση ενός ερωτηματολογίου, που συμπληρώθηκε από 300 ερωτώμενους, εξετάζεται ο τρόπος προσέγγισης και παρενόχλησης των Ελλήνων, η συχνότητα του προβλήματος, οι διαφορετικές μορφές εξαπάτησης, η άποψη που είχαν τα θύματα για τις αιτίες του προβλήματος, η αντίδρασή τους κατά την προσπάθεια εξαπάτησής τους, το εάν επικοινώνησαν με την αστυνομία καθώς και οι συνέπειες που αυτές έχουν σε χρήστες και καταναλωτές που εξαπατήθηκαν τελικά (οικονομικές, κοινωνικές, ψυχολογικές, συναισθηματικές κ.ά.). Οι ερωτήσεις είναι είτε κλειστού τύπου είτε ανοικτού τύπου, ώστε να διερευνηθούν καλύτερα οι διάφορες πτυχές και οι τεχνικές εξαπάτησης των χρηστών, πώς γίνεται η προσέγγιση του καταναλωτή και πώς πείθονται τελικά οι καταναλωτές και χρήστες του διαδικτύου κ.ά..

Στην συνέχεια, στο τρίτο κεφάλαιο, εξετάζονται τα αποτελέσματα της έρευνας που διενεργήθηκε και τέλος, στο τέταρτο, παρουσιάζονται τα συμπεράσματα της εργασίας.

ΣΗΜΑΝΤΙΚΟΤΗΤΑ / ΣΗΜΑΣΙΑ ΤΗΣ ΜΕΛΕΤΗΣ

Μέχρι στιγμής δεν έχει ευρεθεί κατά την φάση της αναζήτησης της βιβλιογραφίας, αντίστοιχη έρευνα για την Ελλάδα και αυτό καθιστά την παρούσα εργασία πρωτότυπη.

Η έρευνα των Vlachos κ.α. (2011) που προαναφέρθηκε είναι ήδη παλαιωμένη, γιατί εν τω μεταξύ οι αλλαγές που έχουν συμβεί, τόσο στο διαδίκτυο όσο και στο κυβερνοέγκλημα είναι πολύ μεγάλες. Μια αδυναμία αυτής της έρευνας, είναι ότι αναφέρεται σε στοιχεία για θύματα που έχουν δηλώσει ότι ήταν θύματα (στην Ομάδα Εργασίας του Υπουργείου Οικονομικών και την τότε Γενική Διεύθυνση Ψηφιακού Σχεδιασμού που είχε συστήσει εκείνη την περίοδο την ομάδα DART). Δηλαδή, εξετάζει μόνο όσα θύματα αντιλήφθηκαν, ήθελαν και δήλωσαν το πρόβλημα, και αυτό όπως θα δούμε στην παρούσα μελέτη είναι σε κάποιες περιπτώσεις ένα εσφαλμένο δείγμα του πραγματικά πληττόμενου πληθυσμού. Επίσης, ούτε το Υπουργείο Ψηφιακής Διακυβέρνησης έχει παρουσιάσει πρόσφατα τα πορίσματα κάποιας μελέτης που να διερευνά το πρόβλημα στις διάφορες πτυχές του και πάνω στην οποία να στηρίζονται οι πολιτικές του κράτους. Σημειώνεται ότι μια τέτοια έρευνα δεν βρέθηκε κατά το στάδιο της αναζήτησης της βιβλιογραφίας.

Πρακτικά, η εργασία διαπιστώνει την ύπαρξη ενός προβλήματος της Ελληνικής κοινωνίας σε ανεξέλεγκτη ανάπτυξη, για το οποίο υπάρχει περιορισμένη Ελληνική βιβλιογραφία αλλά -αντίθετα- ιδιαίτερα αναπτυγμένη βιβλιογραφία στα αγγλικά. Ένα πρόβλημα που επισημαίνεται στη διεθνή βιβλιογραφία διερευνάται για την Ελληνική πραγματικότητα, όπου επιχειρείται να συνεισφέρει και στο έργο της πρόληψης και της καταστολής που ήδη επιτελείται από τις Δημόσιες αρχές και την Ελληνική Αστυνομία.

Επίσης, όπως προκύπτει και από τα παραπάνω, η παρούσα εργασία διερευνά το πρόβλημα από την πλευρά των θυμάτων, των οποίων την άποψη επιχειρεί να ανασυρθεί από την αφάνεια στην επιστημονική επιφάνεια. Δηλαδή, ενώ ατομικά τα θύματα αποφεύγουν (όπως θα διαφανεί και στην μελέτη) να δηλώσουν στις αρχές ότι έπεσαν θύματα ή να εμπλέξουν την Αστυνομία και ενώ πολύ λίγες απόπειρες εξαπάτησης αλλά και θύματα καταγράφονται, σε σχέση με τα πραγματικά, η εργασία μπαίνει στα «άδυτα» ενός εγκλήματος, σεβόμενη πάντοτε την ιδιωτικότητα του θύματος, με το να αναδεικνύει το πρόβλημα, τις πτυχές του, την σημασία, τη συχνότητα και την έκταση που αυτό μπορεί να έχει. Κυρίως όμως, η εργασία αυτή, έχει ιδιαίτερο ενδιαφέρον καθώς το κάνει αυτό, εξετάζοντας την πλευρά των ίδιων των θυμάτων, των υποψήφιων θυμάτων και λοιπών χρηστών του διαδικτύου που κατά δήλωσή τους δεν έχουν ποτέ παρενοχληθεί. Και το ποσοστό των τελευταίων

σύμφωνα με τα αποτελέσματα της έρευνας, έχει εξίσου σημασία. Για αυτό εξάλλου στηρίζεται και σε μια ποιοτική μεθοδολογία που χρησιμοποιείται ευρέως σε έρευνες αναγνώρισης της άποψης του κοινού, με την χρήση ερωτηματολογίων και την ανάλυση των απαντήσεων των ερωτώμενων (και την κατανομή αυτών σε συχνότητες) ώστε να διαπιστώσει τι συμβαίνει στην Ελλάδα, στο μέτρο του δυνατού και λαμβάνοντας υπόψη και τις αδυναμίες και περιορισμούς της έρευνας.

Από την αναζήτηση στη βιβλιογραφία δεν βρέθηκε να έχει παρουσιαστεί μια αντίστοιχη μελέτη ή έρευνα σε διεθνές επίπεδο για μια άλλη χώρα, που να διερευνά ταυτόχρονα τις διάφορες μορφές και πτυχές του προβλήματος και αυτό καθιστά την εργασία σημαντική. Η πρωτοτυπία αυτή, της εργασίας αυτής, εξυπηρετείται από τη μέθοδο που έχει επιλεγεί, η οποία όμως στηρίζεται στην σύγχρονη αρθρογραφία.
Ένα ακόμα στοιχείο που σχετίζεται με την σημαντικότητα της εργασίας απορρέει από την εκπροσώπηση της Ελληνικής περιφέρειας στο δείγμα. Εκπροσωπώντας σε μεγαλύτερο βαθμό την περιφέρεια της Ηπείρου και άλλες πλην της Αττικής, η εργασία επιχειρεί να παρουσιάσει μια εικόνα του τί συμβαίνει στην Ελληνική επαρχία σχετικά με την εξεταζόμενη μορφή εγκλήματος. Αυτό, καθιστά την εργασία ενδιαφέρουσα για τη διερεύνηση του προβλήματος στην Ελληνική περιφέρεια και το δείγμα χρήσιμο για περαιτέρω μελέτη και διερεύνηση. Ωστόσο, ο αντίλογος σε αυτήν την άποψη, θα μπορούσε να είναι ότι τα αποτελέσματα της έρευνας δεν αφορούν ολόκληρη την χώρα, παρά ένα συγκεκριμένο δείγμα της με τα συγκεκριμένα χαρακτηριστικά. Σε αυτή την περίπτωση, πάλι παραμένει ενδιαφέρουσα προς σύγκριση με νεότερες εργασίες που μπορεί να παρουσιαστούν για το θέμα αυτό, σε μελλοντικές προσπάθειες καλύτερης μελέτης του προβλήματος.
Τέλος, τα στοιχεία που έχουν συλλεχθεί μπορεί να χρησιμοποιηθούν για περαιτέρω αναλύσεις.

ΚΕΦΑΛΑΙΟ 1ο: ΑΝΑΛΥΣΗ ΤΗΣ ΒΙΒΛΙΟΓΡΑΦΙΑΣ: ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΚΑΙ ΠΑΡΕΝΟΧΛΗΣΗ: ΤΟ ΠΡΟΒΛΗΜΑ, ΟΙ ΣΥΝΕΠΕΙΕΣ ΚΑΙ ΟΙ ΠΟΛΙΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ

1.1. ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΚΑΙ ΕΞΑΠΑΤΗΣΗ

Το κυβερνοέγκλημα είναι το έγκλημα που διεξάγεται μέσω του διαδικτύου, στον λεγόμενο κυβερνοχώρο. Ο κυβερνοχώρος θεωρείται ότι είναι ο εικονικός χώρος που δημιουργείται μέσα από την λειτουργία και ανάπτυξη του διαδικτύου. Το κυβερνοέγκλημα λαμβάνει διάφορες μορφές και έχει ραγδαία και πολυδιάστατη αύξηση κατά τις τελευταίες δεκαετίες που παρακολουθεί την ανάπτυξη και διάδοση του διαδικτύου, σε παγκόσμια κλίμακα.

Η έκταση του φαινομένου είναι τέτοια που οι ειδικοί αναφέρονται σε μια ολόκληρη βιομηχανία κυβερνοεγκλήματος (Kshetri, 2013).

Ωστόσο δεν πρόκειται απλά για ένα έγκλημα, αλλά και πολλά και πολυπλόκαμα που διαρκώς εξελίσσονται και αναβαθμίζονται, παρακολουθώντας την εξέλιξη της τεχνολογίας των υπολογιστών και του διαδικτύου.

Τα κυβερνοεγκλήματα διαφέρουν ως προς τα κίνητρα των κακοποιών που τα προκαλούν, την έκταση των ζημιών που προκαλούνται, την επίδραση που έχουν στο διεθνές εμπόριο και την διεθνή αντίδραση που προκαλείται (Dimitrov κ.ά., 2023). Ο Kshetri (2013) επισημαίνει ότι ενώ στη Ρωσία και την Ανατολική Ευρώπη το κίνητρο για το κυβερνοέγκλημα είναι κύρια οικονομικό, στην Κίνα οι κυβερνοεγκληματίες αποβλέπουν πιο συχνά στην αναζήτηση πρόσβασης σε θέματα πνευματικής ιδιοκτησίας και εμπορικών μυστικών.

Το κυβερνοέγκλημα διακρίνεται ανάλογα και με αυτόν που το προκαλεί. Ένα κυβερνοέγκλημα μπορεί να προκαλείται είτε από ιδιώτες είτε από οργανώσεις ή οργανωμένες εγκληματικές ομάδες. Τέλος, υπάρχουν και περιπτώσεις όπου προκαλείται και από κυβερνητικά γραφεία, σε χώρες με μικρή δημοκρατική νομιμοποίηση (Kshetri, 2013).

Ως προς τον στόχο που έχει και τα θύματά του, το κυβερνοέγκλημα διακρίνεται σε αυτό που αφορά τους ιδιώτες, τις επιχειρήσεις και τις κυβερνήσεις (Kshetri, 2013).

Όπως επισημαίνουν οι Meikle and Cross (2024) η εξαπάτηση δεν είναι ένα καινούργιο έγκλημα αλλά έχει μακριές ιστορικές ρίζες. Ως εξαπάτηση, μπορεί να θεωρηθεί το ξεγέλασμα με σκοπό τα χρήματα (Meikle and Cross, 2024).

Ωστόσο, οι CISSPCISA and Sutcliffe (2008) αναφέροντας τα ευρήματα μιας αναφοράς της Symantec Corp. σημειώνουν κάτι πολύ ενδιαφέρον: ότι έχει πλέον δημιουργηθεί μια ολόκληρη παράνομη «αγορά», για παράδειγμα ως προς την παράνομη εύρεση και πώληση πληροφοριών, η οποία και λειτουργεί με όρους αγοράς γιατί μειώνονται οι τιμές των παρεχόμενων πληροφοριών όσο αυξάνεται η παροχή των πληροφοριών. Ως συνέπεια και αυτού, οι κυβερνοεγκληματίες έχουν αρχίσει και συνεργάζονται μεταξύ τους (CISSPCISA and Sutcliffe, 2008). Δηλαδή, τέτοια είναι η έκταση του κυβερνοεγκλήματος σήμερα, που θα μπορούσε να αναφερθεί κανείς σε μια ολόκληρη οικονομική δραστηριότητα που επηρεάζει με την λειτουργία της και τους πολλούς παράνομους τρόπους της, τις υπόλοιπες οικονομικές και κοινωνικές δραστηριότητες.

1.1.1 Ορισμοί

Όπως αναφέρουν οι Gordon και Ford (2006) ακόμα και για τα ζητήματα του ορισμού του κυβερνοεγκλήματος υπάρχει διαφορετική εικόνα ανάμεσα στους χρήστες του διαδικτύου, τους ακαδημαϊκούς και τους ειδικούς σε θέματα ασφάλειας στο διαδίκτυο. Πολλές απόπειρες έχουν γίνει για να οριστεί το κυβερνοέγκλημα. Το Συμβούλιο της Ευρώπης χρησιμοποιεί τον όρο «κυβερνοέγκλημα» για να αναφερθεί σε εγκληματική δραστηριότητα εναντίων δεδομένων, περιεχόμενου και πνευματικών δικαιωμάτων καθώς και σχετική με την παιδική πορνογραφία (Gordon και Ford, 2006). Το Συμβούλιο της Ευρώπης έχει υπογράψει ειδική σύμβαση για το κυβερνοέγκλημα (“Convention on Cybercrime”) που αποτελεί την πρώτη διεθνή σύμβαση για την καταπολέμηση του εγκλήματος που προκαλείται μέσω του διαδικτύου και των δικτύων των υπολογιστών. Ωστόσο, ο όρος κατά άλλους, συμπεριλαμβάνει την εξαπάτηση (fraud), την πρόσβαση χωρίς άδεια σε προσωπικά αρχεία και φωτογραφίες, την παιδική πορνογραφία που προωθείται μέσω του διαδικτύου και την κυβερνο-παρακολούθηση ενός θύματος (Zeviar-Geese, όπως αναφέρεται στο Gordon και Ford, 2006).

Σύμφωνα με την επίσημη ιστοσελίδα του FBI των Ηνωμένων Πολιτειών, το κυβερνοέγκλημα είναι «κακόβουλη διαδικτυακή δραστηριότητα που απειλεί την ασφάλεια του κοινού και την εθνική και οικονομική ασφάλεια» (FBI, 2024).

Το Ευρωπαϊκό Κοινοβούλιο καταγράφει ως κυβερνοέγκλημα την πράξη χρησιμοποίησης τεχνολογιών πληροφόρησης με σκοπό τη διαιώνιση ή τη

διευκόλυνση του εγκλήματος (EU, 2024). Διακρίνει σε δυο κατηγορίες κυβερνοεγκλημάτων: τα εξαρτώμενα από το διαδίκτυο (cyber-dependent) και όσα διευκολύνονται από το διαδίκτυο (cyber-enabled). Η πρώτη κατηγορία αφορά όλα τα εγκλήματα που γίνονται με τη χρήση του υπολογιστή, δικτύων υπολογιστών ή άλλες μορφές Τεχνολογιών Πληροφορίας και Επικοινωνιών (Information and Communication Technology). Σε αυτή την περίπτωση κατατάσσονται το χάκινγκ και το κακόβουλο λογισμικό. Στη δεύτερη κατηγορία κατατάσσονται τα παραδοσιακά εγκλήματα που διευκολύνονται με τη χρήση του υπολογιστή και των τεχνολογιών πληροφορικής, τα οποία έχουν αυξηθεί σε κλίμακα, όπως η εξαπάτηση, το «ψάρεμα» (phishing), η πειρατεία και η πλαστογραφία (EU, 2024).

Με έναν ευρύ ορισμό κυβερνοέγκλημα μπορεί να θεωρηθεί οποιασδήποτε μορφής έγκλημα ή άλλη εγκληματική δραστηριότητα που λαμβάνει χώρα μέσω του διαδικτύου.

Σε αυτό συμπεριλαμβάνονται και οι ευρέως διαδεδομένες απειλές των ιών (viruses) και των «σκουληκιών» (worms) που απειλούν τη λειτουργία του υπολογιστή ή μετατρέπουν ένα υπολογιστή σε ζόμπι.

Οι Gordon και Ford, 2006 διακρίνουν δύο τύπους κυβερνοεγκλήματος. Τα χαρακτηριστικά του Τύπου Ι είναι ότι πρόκειται συνήθως για ένα μόνο γεγονός από την πλευρά του θύματος, διευκολύνεται από τη χρήση ενός προγράμματος, όπως ιό κ.ά. και μπορεί να διευκολύνεται και από στοιχεία τρωτότητας των υπολογιστών των χρηστών. Παραδείγματα αυτού του τύπου περιλαμβάνουν το «ψάρεμα» (“phishing”), την κλοπή ή χρήση προσωπικών δεδομένων ή υπηρεσιών από χάκερς συμπεριλαμβανομένης και της ταυτότητας και την εξαπάτηση σε σχέση με την τράπεζα του ιδιώτη και τις εμπορικές του συναλλαγές μέσω διαδικτύου. Αντίθετα το κυβερνοέγκλημα Τύπου ΙΙ, περιλαμβάνει την παρακολούθηση στο διαδίκτυο ενός συγκεκριμένου χρήστη (cyberstalking), την παρενόχλησή του (harassment), την χρήση ή κακοποίηση παιδιών, τον εκβιασμό, την εκμετάλλευση του χρήστη σχετικά με το χρηματιστήριο και χρηματιστηριακές συναλλαγές, σύνθετη εταιρική κατασκοπεία ή ακόμα και τρομοκρατικές ενέργειες (Gordon και Ford, 2006).

Όπως αναφέρουν οι Gordon και Ford (2006) στην περίπτωση του Τύπου Ι, ένας χρήστης αποφασίζει να εισέλθει στο διαδίκτυο για την πραγματοποίηση κάποιας ενέργειας (για παράδειγμα να διαβάσει το e-mail του ή να επισκεφτεί έναν ιστότοπο) και ακολούθως κάνει κάποια ενέργεια που επιτρέπει την εκδήλωση της εγκληματικής πράξης (για παράδειγμα επισκέπτεται μια άλλη ιστοσελίδα που του έχει προταθεί ή

διαβάζει ένα συνημμένο σε κείμενο που του έχει σταλεί), παρέχοντας έτσι μια ενημέρωση σε κάποιον τρίτο σχετικά με τον υπολογιστή του, τα προσωπικά του στοιχεία ή άλλα δεδομένα που τον αφορούν. Στη συνέχεια, η πληροφορία αυτή χρησιμοποιείται σε βάρος του ενώ ο χρήστης αντιλαμβάνεται αργότερα ότι αυτό συμβαίνει. Για αυτό, σε αυτής της μορφής κυβερνοεγκλήματος είναι σημαντικό να προστατεύονται τα προσωπικά στοιχεία και δεδομένα του χρήστη.

Στην περίπτωση του Τύπου ΙΙ, το κυβερνόεγκλημα είναι πιο σύνθετο ως προς τον τρόπο που λαμβάνει χώρα. Στο έγκλημα αυτό χρησιμοποιούνται συνήθως μέθοδοι άμεσης επικοινωνίας μέσω μηνυμάτων (instantmessaging) (Gordon και Ford, 2006). Στο ενδεικτικό παράδειγμα των Gordon και Ford, 2006, ο χρήστης αναζητάει μια πληροφορία για ένα εξειδικευμένο ζήτημα και αποφασίζει να εισέλθει σε ένα σχετικό φόρουμ επικοινωνίας και συζήτησης. Εκεί ανταλλάσσει σειρά μηνυμάτων με άλλους χρήστες του φόρουμ, ώσπου αποφασίζει να ανταλλάξει στοιχεία επικοινωνίας με έναν άλλο χρήστη του φόρουμ ώστε να συζητήσουν περισσότερο επί του θέματος. Το στάδιο αυτό είναι στάδιο δημιουργίας εμπιστοσύνης, κατά τη διάρκεια του οποίου ένας εγκληματίας προσεγγίζει το θύμα από την θύρα της εμπιστοσύνης, μέχρι να το βρει ευάλωτο και να εκμεταλλευτεί την εμπιστοσύνη του την κατάλληλη στιγμή. Αυτό μπορεί για παράδειγμα να γίνει ζητώντας από τον χρήστη να του παρέχει πρόσβαση σε στοιχεία του τραπεζικού του λογαριασμού, σε προσωπικά δεδομένα, σε κωδικούς ανάληψης από την τράπεζα και πλήθος άλλων.

1.1.2. Αιτίες

Η κυριότερη αιτία και κοινός άξονας κάθε μορφής κυβερνοεγκλήματος είναι ο προσπορισμός εσόδων από τα θύματα. Τα έσοδα αυτά είναι παράνομα επειδή αποτελούν προϊόν υποκλοπής και εξαπάτησης αλλά επίσης επειδή δεν δηλώνονται φορολογικά και αποτελούν και διαφυγόν εισόδημα για μια οικονομία.

Στην εργασία τους οι Vahdati και Yasini (2015) επισημάνουν αρχικά ότι το κυβερνοέγκλημα δεν προκαλείται μόνο από την απληστία, αλλά ότι η φτώχεια και η ανάγκη συμπλήρωσης ενός πενιχρού εισοδήματος συγκαταλέγεται ανάμεσα στους παράγοντας εκείνους που συντελούν σε αυτό. Στη συνέχεια, εξετάζουν ιδιαίτερα ποιοι παράγοντες προκαλούν και οδηγούν όσους είναι εργαζόμενοι σε μια οργάνωση να συμμετάσχουν -οι ίδιοι- σε πράξεις κυβερνοεγκλήματος. Τους παράγοντες αυτούς τους διακρίνουν σε δυο μεγάλες κατηγορίες: i) σε ατομικούς και οργανωσιακούς

παράγοντες που συμπεριλαμβάνουν την οργανωτική δομή μιας οργάνωσης, την σχέση μεταξύ προσωπικότητας και εργασίας, τις διαμάχες μεταξύ εργαζομένων και οργάνωσης, τα συστήματα αξιολόγησης εργαζομένων, την παρακολούθηση και τον έλεγχο των εργαζομένων και ii) τους περιβαλλοντικούς και εξωτερικούς παράγοντες που περιλαμβάνουν υφιστάμενους κανόνες και ρυθμίσεις, οικονομικούς και πολιτικούς παράγοντες, τις υποδομές και την κουλτούρα.

Οι CISSPCISA and Sutcliffe (2008) αφού πρώτα εξηγήσουν ότι το διαδίκτυο ενισχύει την ιδιωτικότητα, την εμπιστευτικότητα και την μη ιχνηλασιμότητα των χρηστών του, τονίζουν ότι μέσα σε αυτό μπορούν να αναζητηθούν και να ευρεθούν αόρατοι στόχοι, όπως οι σχετικοί με τις ανθρώπινες ταυτότητες και την ανθρώπινη γνώση που αποτελούν το αντικείμενο του διεθνούς εγκλήματος.

Οι Albrecht κ.ά. (2018) θεωρούν ότι τα κύρια αίτια για την εξαπάτηση στον χώρο των επιχειρήσεων είναι τρία: Α) η αντιλαμβανόμενη πίεση που θεωρεί κάποιος ότι του ασκείται όταν έχει ανάγκες σε χρήματα αλλά και μη χρηματοδοτική πίεση (όπως για παράδειγμα η απογοήτευση από τη δουλειά ή η θέληση να νικήσει κανείς το σύστημα). Β) η αντιλαμβανόμενη ευκαιρία και Γ) η εκλογίκευση της εξαπάτησης ως κάτι σωστό και λογικό.

Ο Oates (2006) εξηγεί ότι η εξαπάτηση διευκολύνεται από την τεχνολογία και την έλλειψη ασφάλειας, την ανωνυμία των χρηστών-θυτών, την ιδιωτικότητα των θυτών, και την παγκοσμιοποίηση.

Οι Kulibay κ.ά. (2023) αναφέρονται στην ικανότητα ταυτοποίησης μια παρενόχλησης (scam identification ability) και με βάση την έρευνα που διεξήγαγαν στην Κένυα βρήκαν ότι ένα πολύ μικρό ποσοστό (μόλις 12%) ταυτοποίησε σωστά όλες τις παρενοχλήσεις που υπέστη υπό μορφή μηνύματος ενώ διαπίστωσαν ότι κατά μέσο όρο το 74% των ατόμων ταυτοποιούν σωστά ένα μήνυμα παρενόχλησης και το 64% ένα μήνυμα μη παρενόχλησης. Αυτό το στοιχείο είναι ενδεικτικό της έλλειψης πλήρους ικανότητας ταυτοποίησης μιας παρενόχλησης.

1.1.3. Μορφές εξαπάτησης

Εξετάζοντας την περίπτωση της Κίνας, ο Kshetri (2013) διακρίνει το κυβερνοέγκλημα ως προς τους διαφορετικούς του τύπους, την κλίμακα, τα κίνητρα, και τους στόχους του. Η κύρια διάκριση που προτείνει είναι αυτή μεταξύ του αρπακτικού κυβερνοεγκλήματος (predatory crime) και του εγκλήματος που στηρίζεται στην αγορά

(market-based). Στην πρώτη περίπτωση, το κυβερνοέγκλημα προκαλείται με τη χρήση υπολογιστών ή δικτύων υπολογιστών ως κύριων μέσων.

Οι Gordon and Ford κατηγοριοποιούν το κυβερνοέγκλημα σε αδρές γραμμές ανάμεσα στον Τύπο Ι που έχει τεχνολογικά στοιχεία και στον Τύπο ΙΙ που έχει κυρίως ανθρώπινα στοιχεία. Στην πρώτη περίπτωση τα κυβερνοεγκλήματα προκαλούνται λόγω της χρήσης της τεχνολογίας ενώ στην δεύτερη συνδέονται με συμπεριφορές και στάσεις των ατόμων, την κοινωνική τους δραστηριότητα και τη χρήση των κοινωνικών μέσων και δικτύων. Η δεύτερη περίπτωση εξαπλώνεται σε πολλές χώρες και, όπως αναφέρει ο Kshetri (2013) ευνοείται η εξάπλωσή της από την άγνοια που υπάρχει από νέους χρήστες για τα εγκλήματα και τη χρήση των υπολογιστών.

Το κυβερνοέγκλημα διακρίνεται επίσης σε ευκαιριακό και στοχευμένο (Kshetri, 2013).

Οι Vahdati και Yasini (2015), εξετάζοντας τους παράγοντες που έχουν επηρεάσει τη διάδοση του κυβερνοεγκλήματος στο Ιράν, αφού αναφέρουν ότι προέρχεται από διαφορετικές τάξεις επαγγελματιών και όχι αποκλειστικά από φτωχούς, κατηγοριοποιούν το κυβερνοέγκλημα που γίνεται με τη χρήση υπολογιστών σε: i) σχήματα εξαπάτησης μέσω της προκαταβολής χρηματικού αντιτίμου έναντι (όπου τα θύματα προκαταβάλουν ποσά έναντι της παροχής κάποιας υποσχόμενης υπηρεσίας), ii) επιχειρηματικά και εργασιακά σχήματα (όπου τα θύματα αναζητούν εργασία και επισκέπτονται ειδικά διαμορφωμένες ιστοσελίδες που αποσπούν σημαντικά προσωπικά τους δεδομένα), iii) εξαπάτηση με χρήση πιστωτικών/χρεωστικών καρτών χωρίς έγκριση από τα θύματα (credit/ debitcardfraud), iv) κλοπή στοιχείων ταυτότητας (identitytheft), v) σχήματα/πυραμίδες Ponzi, vi) το «ψάρεμα» (phishing) ή η πλαστογράφηση (όπου οι θύτες προσποιούνται ότι είναι κάποιοι άλλοι για να αποσπάσουν χρήματα),vii) η μη εγκεκριμένη πρόσβαση (παραβίαση της ηλεκτρονικής ασφάλειας του θύματος), viii) τα κακόβουλα λογισμικά ή ιοί και viv) η υπέρ-χρήση υπολογιστών στο χώρο εργασίας για άλλους σκοπούς (cyberslacking).

Οι Dimitrov κ.ά. (2023) διακρίνουν σε: i) διακίνηση διαδικτυακού πορνογραφικού υλικού, συμπεριλαμβανομένης της παιδοφιλίας, ii) παραβίαση της ηλεκτρονικής αλληλογραφίας, iii) παραβίασης δικαιωμάτων πνευματικής ιδιοκτησίας, iv) διαδικτυακή εξαπάτηση και v) έγκλημα υπολογιστών.

Το υφιστάμενο εκτός διαδικτύου έγκλημα, χρησιμοποιεί το διαδίκτυο για την εξάπλωσή του, όπως για παράδειγμα αυτό συμβαίνει με την παράνομη εμπορία όπλων ή τη διακίνηση ναρκωτικών ουσιών. Για πολλούς συγγραφείς σε θέματα

κυβερνοεγκλήματος αυτό αποτελεί μια μορφή κυβερνοεγκλήματος (π.χ. Chung κ.ά., 2006). Αυτή η μορφή κυβερνοεγκλήματος αποτελεί μια ξεχωριστή κατηγορία (που δεν εξετάζεται στην παρούσα εργασία). Μια άλλη μορφή (που επίσης δεν εξετάζεται) είναι η κυβερνο-πειρατεία, δηλαδή η αντιγραφή λογισμικού και αρχείων μέσω διαδικτύου. Τέλος, η δημιουργία και διάδοση ιών και κακόβουλων λογισμικών που επιτίθενται στον υπολογιστή ιδιωτών ή εταιρειών είναι μια μορφή εγκλήματος (Chung κ.ά., 2006).

Σημειώνεται ότι η Επιτροπή των ΗΠΑ, FEDERAL TRADE COMMISSION, όπως αναφέρεται στην μελέτη των Bera κ.ά.(2023), κατηγοριοποιεί τα μηνύματα παρενόχλησης των πολιτών στις ΗΠΑ στις ακόλουθες κατηγορίες: μηνύματα για επιχειρήσεις/επενδυτικές ευκαιρίες, για χρηματοδότηση, για προϊόντα/υπηρεσίες, για ενήλικες που επιθυμούν ρομαντικές γνωριμίες, για θέματα υπολογιστών/διαδικτύου, σχετικά με την υγεία, με θέματα αναψυχής/ταξιδιού και με θέματα εκπαίδευσης.

1.1.3.1. Εξαπάτηση σχετικά με τα κρυπτονομίσματα

Μια από τις κύριες μορφές που λαμβάνει το κυβερνοέγκλημα είναι η εξαπάτηση μέσω προσπαθειών που γίνονται να πωληθούν στους χρήστες του διαδικτύου κρυπτονομίσματα, να γίνουν σχετικές με κρυπτονομίσματα συναλλαγές ή ακόμα και να εξαπατηθούν τελείως με την ψεύτικη αγορά δήθεν κρυπτονομισμάτων.

Το κύριο γνώρισμα των κρυπτονομισμάτων είναι ότι παρακάμπτουν το τραπεζικό σύστημα και παρέχουν ευκαιρίες γρήγορου και άμεσου πλουτισμού. Αυτές παρακινούν πολλούς καταναλωτές, στο μέτρο που οι αποδόσεις από το κλασσικό τραπεζικό σύστημα παραμένουν χαμηλές. Μέσω των κρυπτονομισμάτων δημιουργείται μια σχέση ελεύθερης συνεργασίας μεταξύ των επενδυτών ή υποψήφιων επενδυτών και των εταιρειών που παρέχουν τη δυνατότητα για αυτές τις επενδύσεις. Σε αυτή τη σχέση παρεισφρέουν τρίτοι που εκμεταλλεύονται την πλήρη απουσία ελέγχων από κάποιο πιστωτικό ίδρυμα για τις πράξεις συναλλαγής και εξαπατούν τους καταναλωτές-θύματα με διάφορους τρόπους.

Μια περίπτωση διαδεδομένης εξαπάτησης είναι το BGS (Bitcoin Generator Scam). Στο BGS προσφέρεται δήθεν στους χρήστες-θύματα του διαδικτύου η δυνατότητα αγοράς κρυπτονομισμάτων Bitcoin (που αποτελούν το πιο γνωστό και με τις μεγαλύτερες αποδόσεις κρυπτονόμισμα που έγινε γνωστό από το 2009 και έπειτα) με αντάλλαγμα ένα μικρό ποσό που προαπαιτείται για την λεγόμενη «εξόρυξη» του

κρυπτονομίσματος αυτού (Badawi κ.ά, 2022). Το Bitcoin στηρίζει την ανωνυμία του χρήστη και παρέχει ασφάλεια στη δημιουργία μιας σειράς από ηλεκτρονικές διευθύνσεις που δημιουργούνται για κάθε διαφορετικό χρήστη (Badawi κ.ά, 2022). Κατά αυτόν τον τρόπο, ένας χρήστης δεν γνωρίζει ποιος είναι ο άλλος. Αυτός όμως ο τρόπος προστασίας της ασφάλειας του χρήστη, λειτουργεί και αντίστροφα γιατί δεν μπορεί να γνωρίζει με σιγουριά ένας τελικός αγοραστής ενός Bitcoin, σε μια συναλλαγή, αν τελικά του παρέχεται το κρυπτονόμισμα αυτό μέσα από την συναλλαγή αυτή ή επιχειρείται κάποια μορφή εξαπάτησης. Χρειάζεται για τον σκοπό αυτό, η διαμεσολάβηση ενός έγκυρου και επίσημου πωλητή.

Μια άλλη παράνομη δραστηριότητα συναφής με τις συναλλαγές κρυπτονομισμάτων είναι η προσπάθεια να χακαριστούν οι συναλλαγές σε κρυπτονομίσματα, ειδικά οι μεγάλες σε έκταση. Όπως αναφέρεται στο Xia κ.ά. (2020) μόνο το 2017 και τα πρώτα τρία-τέταρτα του 2018, χάθηκαν 882 εκατ. δολάρια από χάκερς που έκαναν επιθέσεις σε συναλλαγές που έγιναν με κρυπτονομίσματα. Οι Xia κ.ά. (2020) τονίζουν ότι το οικοσύστημα των κρυπτονομισμάτων είναι μεγάλο και διάχυτο και οι θύτες στοχεύουν σε κάθε του πτυχή προκειμένου να βρουν θύματα.

1.1.3.2. Εξαπάτηση μέσω ηλεκτρονικών μηνυμάτων παρενόχλησης

Ηλεκτρονικά μηνύματα παρενόχλησης (γνωστά και ως spams) αποστέλλονται σχεδόν καθημερινά σε χρήστες του διαδικτύου που διαθέτουν λογαριασμό ηλεκτρονικού ταχυδρομείου. Συνήθως ο αποστολέας ενός τέτοιου μηνύματος το συνοδεύει με ένα συνημμένο, στο οποίο χρειάζεται να πατήσει ο παραλήπτης, το οποίο μεταφέρει τον παραλήπτη σε άλλη ιστοσελίδα με κακόβουλο λογισμικό ή περιεχόμενο (Manarash κ.ά., 2015).

Οι Manarash κ.ά. (2015) διακρίνουν τις τέσσερις ακόλουθες κατηγορίες παραγόντων για τους οποίους ένας χρήστης του διαδικτύου ανοίγει ένα e-mail που είναι spam: τεχνολογικούς, κοινωνικούς, οικονομικούς και θρησκευτικούς, έπειτα από δείγμα 600 φοιτητών από την Ιορδανία, οι οποίοι απάντησαν στο ερώτημα ποιοι παράγοντες επηρέασαν την απόφασή τους να επισκεφτούν μια ιστοσελίδα η οποία βρίσκονταν συνημμένη στο ηλεκτρονικό μήνυμα που στάλθηκε.

Ο Dunham (2007) αναφέρει ότι αυτή η μορφή εξαπάτησης είναι συχνή γιατί στέλνονται καθημερινά εκατομμύρια μηνύματα σε αποδέκτες και το πολύ μικρό ποσοστό απάντησης σε αυτά αρκεί για να πολλαπλασιάσει τα έσοδα των θυτών.

1.1.3.3. Σχήματα ή πυραμίδες πόντζι (Ponzi)

Στην περίπτωση αυτής της μορφής κυβερνοεγκλήματος, χρησιμοποιείται το διαδίκτυο και η τηλεφωνική επικοινωνία ώστε να ανευρεθούν «επενδυτές» στο σχήμα Ponzi. Οι «επενδυτές» αυτοί καλούνται να επενδύσουν στην εταιρεία και λαμβάνουν αποδόσεις μόνο αν φέρουν νέους επενδυτές (από αυτούς) (Vahdati και Yasini, 2015). Πρόκειται για μια μορφή εξαπάτησης, γιατί δεν υπάρχει αρχικό κεφάλαιο και ο ανώτερος ιεραρχικά στην πυραμίδα δεν έχει ουσιαστικά καμία υποχρέωση έναντι του κατώτερών του.

1.1.3.4. Εξαπάτηση σχετικά με (ρομαντικές) γνωριμίες και επαφές

Η περίπτωση αυτή κυβερνοεγκλήματος είναι αρκετά διαδεδομένη και εξακολουθεί να εξαπλώνεται. Με τα θύματα διαρκώς να αυξάνονται στις ΗΠΑ, το Ηνωμένο Βασίλειο, την Ιαπωνία, την Ισπανία και τη Γερμανία, ένα ολόκληρο δίκτυο εξαπάτησης έχει τεθεί σε λειτουργία που θεωρείται ότι προέρχεται από τις δυτικές αφρικανικές χώρες (Anesa, 2020).

Σε αυτή τη μορφή εξαπάτησης, προσφέρεται η υπόσχεση γνωριμίας ή παρέχεται η δυνατότητα γνωριμίας για ρομαντικούς και ερωτικούς σκοπούς. Ο θύτης προσποιείται ότι θέλει να δημιουργήσει μια αληθινή σχέση με το θύμα και επιχειρεί να τη δημιουργήσει όσο το δυνατόν πιο γρήγορα (Meitle and Cross, 2024).

Οι Meitle and Cross (2024), εξετάζοντας τη διάδοση της μορφής αυτής εγκλήματος στην Αυστραλία, επισημαίνουν ότι συντελείται σε ορισμένα στάδια, τα οποία και διακρίνουν ως εξής:

Στάδιο 1: Κίνητρο για να βρεθεί ο ιδανικός σύντροφος

Στάδιο 2: Παρουσίαση ενός ιδεατού προφίλ συντρόφου

Στάδιο 3:Ανάπτυξη ενός ειδυλλίου, μιας σχέσης ή της προοπτικής μια σχέσης γάμου

Στάδιο 4: Το κεντρί (ή η πρώτη απαίτηση για χρήματα)

Στάδιο 5: Συνέχιση της εξαπάτησης (διαδοχικά αιτήματα για χρήματα)

Στάδιο 6:Σεξουαλική εκμετάλλευση (που δεν συμβαίνει σε όλες τις περιπτώσεις)

Στάδιο 7:Επανα-θυματοποίηση (με την ανάλογη πράξη των θυτών προς τα ίδια θύματα με άλλο προφίλ ή μορφή, ώστε να εξακολουθήσουν να εκμεταλλεύονται την αδυναμία τους) (Meitle and Cross, 2024). Αντίστοιχα είναι και τα στάδια (6 πλην αυτού της σεξουαλικής εκμετάλλευσης) που παρουσιάζει η Anesa (2020). Δηλαδή, υπάρχει γενικά η αναγνώριση μιας διαδικασίας και ενός συγκεκριμένου τρόπου προσέγγισης του θύματος.

Κύριο γνώρισμα, αυτής της μορφής εξαπάτησης, είναι η δημιουργία σχέσης εμπιστοσύνης που αποσκοπεί στο χειρισμό του θύματος. Η προσπάθεια του θύτη είναι να γίνει πειστικός στο θύμα και η πειθώς του αυτή προκαλείται με ψεύτικα προφίλ που είναι αρεστά στους καταναλωτές-θύματα, με ψεύτικες φωτογραφίες, βίντεο αλλά και τα στοιχεία μιας αληθοφανούς επικοινωνίας, κατά την οποία ο χρήστης πείθεται ότι υπάρχει πραγματικά το πρόσωπο με το οποίο επικοινωνεί μέσω του διαδικτύου (Meitle and Cross, 2024). Αυτό το παιχνίδι αληθοφάνειας-ψεύδους έχει πολλές πτυχές και απαιτεί έναν ενεργό θύτη. Στις περισσότερες των περιπτώσεων συνοδεύεται από ψυχολογικές συνέπειες και το αίσθημα της απογοήτευσης για τα θύματα.

Έχει αποδειχθεί, με άλλες μελέτες, ότι το συναίσθημα αυτό της απογοήτευσης είναι ανεξάρτητο από το αν το θύμα έχασε τελικά χρήματα ή όχι (Lazarus κ.ά., 2023). Οι Lazarus κ.ά. (2023) παρουσίασαν (σε έναν περιεκτικό πίνακα) μια σειρά από ενδιαφέροντα συμπεράσματα μελετών σχετικών με αυτή τη μορφή παρενόχλησης. Ανάμεσα σε άλλα, σημειώνεται ότι οι κυβερνοεγκληματίες χρησιμοποιούν ένα μεγάλο εύρος πολύ ισχυρών ψυχολογικών μηχανισμών για να αποσπάσουν τον ηθικό και ψυχολογικό έλεγχο του θύματος, ότι ο συγκεκριμένος τύπος παρενόχλησης έχει πολύ μεγαλύτερη συναισθηματική επίπτωση πάνω στο θύμα σε σχέση με άλλους, ότι τα θύματα είναι σε μεγάλο βαθμό μορφωμένα και όχι απαραίτητα αμόρφωτα, ότι αφορούν και παντρεμένους και ότι τα θύματα τείνουν να παραγνωρίζουν τις αποδείξεις για την παράνομη πράξη των θυτών γιατί εισέρχονται τα ίδια στο επίκεντρο του συναισθηματικού ενδιαφέροντος (κάποιου τρίτου) και αυτό τα καθιστά ιδιαίτερα ευάλωτα και αδύναμα να αποδεχτούν ότι δεν ισχύει η ρομαντική σχέση που έχει δημιουργηθεί.

1.1.3.5. Παρενόχληση μέσω e-mail

Ένα συχνό κυβερνοέγκλημα είναι η παρενόχληση μέσω e-mail, μέσω της οποίας αναζητούνται θύματα που θα μπορούν να γίνουν αντικείμενο εκμετάλλευσης. Τα θύματα δέχονται ένα e-mail που μπορεί να τους ενημερώνει για κάποιο κέρδος που αποκόμισαν, για τη δυνατότητα να τους παρασχεθεί ένα δάνειο, για μια ευκαιρία εύκολου πλουτισμού (με απλή μεταβίβαση χρημάτων, υπό ορισμένες προϋποθέσεις) κ.ά.

Στην πραγματικότητα, η περίπτωση αυτή εξαπάτησης μέσω e-mail λαμβάνει πολλές μορφές και τα σενάρια που παρουσιάζονται στα θύματα εξαπάτησης αφορούν (δήθεν): i) θύματα κυβερνήσεων, ii) μια εύπορη κυρία που κάνει αγαθοεργίες, iii) την συντριβή μιας τράπεζας χωρίς να υπάρχουν συγγενείς για μεταφορά των καταθέσεων, iv) του διεφθαρμένου κυβερνητικού στελέχους, v) του τίμιου κλέφτη και vi) των θυμάτων εμφυλίου πολέμου. (Glickman, 2005 όπως αναφέρεται στο Genc κ.ά., 2021)

Σε αυτή την περίπτωση, τα θύματα μπορούν να προσπεράσουν το e-mail και να μην του δώσουν σημασία, αλλά αν ανταποκριθούν μπορεί να εμπλακούν σε μια διαδικασία που μπορεί να είναι πολύ χρονοβόρα και να τους κοστίσει.

Το φαινόμενο παρουσιάζεται συχνά σε ομάδες για τις οποίες ανευρίσκονται πιο εύκολα τα e-mails, όπως για παράδειγμα στα φοιτητικά κοινά. Οι Manasrah κ.ά. (2015) μελέτησαν την εμφάνισή του στους φοιτητές διαφορετικών σπουδών από τρία διαφορετικά πανεπιστήμια της Ιορδανίας, με τη χρήση ερωτηματολογίων. 100 από αυτά τα ερωτηματολόγια μοιράστηκαν σε φοιτητές σε θέματα τεχνολογίας πληροφορικής, με ποσοστό απάντησης πάνω από 85%.

Το πρόβλημα της εξαπάτησης μέσω e-mail ή σε πρώτο στάδιο μέσω τηλεφώνου (και αργότερα, σε δεύτερο στάδιο, με τη χρήση του υπολογιστή) είναι ευρέως διαδομένο σε λιγότερο αναπτυγμένες χώρες. Οι Kubilay κ.ά. (2023) εξετάζουν στην Κένυα αν οι Κενυάτες έχουν την ικανότητα να αναγνωρίζουν τις περιπτώσεις εξαπάτησης μέσω τηλεφώνου και βρίσκουν ότι απλές συμβουλές και πρακτικές εκπαίδευσης του κοινού που θεωρούνται χρήσιμες για την αναγνώριση των παρενοχλήσεων αυτών και τη διάκρισή τους από αυθεντικά μηνύματα (όπως τον έλεγχο από που προέρχονται τα μηνύματα, την συμβουλή να αποφεύγεται να πατήσει ο χρήστης σε έναν συνημμένο ή έναν σύνδεσμο κ.ά.) δεν φαίνεται να είναι αποτελεσματικές.

Τα παραδείγματα εξαπάτησης μέσω e-mail είναι πάρα πολλά και οφείλονται και στην ευκολία που υπάρχει να εξαπατηθούν ορισμένα ειδικά κοινά καταναλωτών. Ενδεικτικό είναι το παράδειγμα μιας καθολικής εκκλησίας του Αγίου Αμβροσίου στο Οχάιο των ΗΠΑ, όπου κάποιο μέλος της εκκλησίας πείστηκε μέσω ενός e-mail να αλλάξει τα στοιχεία αποστολής εμβασμάτων από την εκκλησία σε μια καινούρια διεύθυνση της εταιρείας που είχε αναλάβει την ανακαίνισή της, χάνοντας συνολικά 1,75 εκατομμύρια δολάρια (Computer Fraud and Security, 2019).

1.1.3.5.1. Η Νιγηριανή απάτη

Η εξαπάτηση που είναι γνωστή ως «Νιγηριανή απάτη» αφορά την αποστολή e-mails μέσω των οποίων ζητείται η χρήση ενός τραπεζικού λογαριασμού από τον παραλήπτη του e-mail για την κατάθεση σημαντικών ποσών, με αντάλλαγμα για τον παραλήπτη ενός ποσοστού επί του μεγάλου ποσού που θα κατατεθεί και το οποίο συνήθως αναγράφεται στο e-mail. Η εξαπάτηση αυτή είναι ευρέως διαδεδομένη παγκοσμίως και έχει πάνω από 40 χρόνια διάρκεια (Computer Fraud and Security, αγνώστου έτους).

Παλαιότερα, αυτή η περίπτωση ήταν γνωστή ως η εξαπάτηση του Νιγηριανού πρίγκιπα ή του Ισπανού φυλακισμένου (Genc κ.ά., 2021). Μετά τη δημιουργία μιας σύνδεσης με το θύμα επιδιώκεται η απόκτηση χρημάτων για την κάλυψη εξόδων αποστολής, εξόδων συναλλαγής, για δωροδοκία ή άλλους σκοπούς (Genc κ.ά., 2021)

1.1.3.6.Εξαπάτηση μέσω ψεύτικων ιστοσελίδων

Μια ευρέως διαδεδομένη μορφή κυβερνοεγκλήματος και εξαπάτησης στο διαδίκτυο είναι και η δημιουργία ψεύτικων ιστοσελίδων φτιαγμένων ειδικά για την προσέλκυση επισκεπτών-θυμάτων, των οποίων στη συνέχεια θα γίνει η εκμετάλλευση. Ο Cohen (2019) αναφέρει ότι μια πολύ διαδεδομένη τέτοια περίπτωση αφορά την προβολή υποτιθέμενου φιλανθρωπικού έργου και δραστηριότητας μέσω του διαδικτύου. Στις ιστοσελίδες αυτές, παρουσιάζονται συνήθως εικόνες από παιδιά που πεθαίνουν από πείνα, σκοτώνονται από βόμβες ή νάρκες, γυναίκες ή παιδιά που διαβιούν σε ερείπια κ.ά. (Cohen, 2019). Πρόκειται συνήθως για ψηφιοποιημένες εικόνες που δεν μπορούν να ιδωθούν ολόκληρες και ο επισκέπτης της ιστοσελίδας χρειάζεται να «πατήσει» πάνω σε αυτές, μεταβαίνοντας έτσι στην ιστοσελίδα. Οι ιστοσελίδες αυτές είναι συνήθως αναγνωρίσιμες (π.χ. islam.tv) και διαφημίζονται και σε άλλες ιστοσελίδες, με σκοπό την κατάθεση χρημάτων για τον φιλανθρωπικό σκοπό που παρουσιάζεται. Εξάλλου σε αρκετές περιπτώσεις το ψεύτικό αυτό φιλανθρωπικό έργο παρουσιάζεται ότι συνδέεται με μια συγκεκριμένη θρησκεία και θρησκευτικούς σκοπούς (Cohen, 2019).

Αυτή η μορφή εξαπάτησης μπορεί να αποκαλυφθεί μετά από παράπονα των καταναλωτών ή με ανάλυση του περιεχομένου της ιστοσελίδας. Ωστόσο υπάρχουν και περισσότερο τεχνικοί τρόποι αποκάλυψης της, που συνδέονται με δομικά γνωρίσματα κάθε ιστοσελίδας (Gopal κ.ά., 2022).

1.1.3.7. Εξαπάτηση σχετική με κληρονομιές

Σε αυτή τη μορφή εξαπάτησης, τα θύματα ενημερώνονται ότι έχουν κληρονομήσει αξιόλογα περιουσιακά στοιχεία από το εξωτερικό (Cross, 2019). Επιδίωξη των θυτών είναι να έρθουν σε επαφή με αυτούς, εντυπωσιασμένα από τα ποσά που αναγράφονται και τα περιουσιακά στοιχεία που δήθεν κληρονομούν.

1.1.3.8. Εξαπάτηση σχετική με λαχνούς ή λαχεία

Σε αυτή τη μορφή εξαπάτησης, τα θύματα ενημερώνονται ότι έχουν κερδίσει ένα λαχείο με μεγάλα κέρδη και τους ζητείται να συμμετάσχουν σε έναν τρόπο λήψης των κερδών τους (Cross, 2019).

1.1.3.9. Εξαπάτηση σχετικά με θέματα υγείας

Η εξαπάτηση για θέματα υγείας με τη χρήση του διαδικτύου είναι αρκετά διαδομένη παγκοσμίως (Garrett κ.ά., 2019A και Garrett κ.ά., 2019B). Το κύριο γνώρισμά του είναι ότι απευθύνεται σε ανθρώπους που βρίσκονται σε ανάγκη, ιατρικής φύσης, γεγονός που καθιστά τα θύματα αρκετά ευάλωτα (Garrett κ.ά., 2019A). Οι Garrett κ.ά. (2019B) εξετάζουν το φαινόμενο της μορφής αυτής εξαπάτησης στον Καναδά και την συνδέουν με την πειθώ που ασκείται στα θέματα και την ανάγκη των θυμάτων για κοινωνική συναλλαγή.

Οι Zhu κ.ά. (2023) αναφέρουν ότι την περίοδο του COVID-19 έγιναν προσπάθειες εξαπάτησης στην Κίνα στις οποίες οι θύτες παρουσιάζονταν ως κυβερνητικοί υπάλληλοι που διέθεταν ειδικές υπηρεσίες κατά της πανδημίας στους πολίτες μέσω e-mail.

1.2. ΤΡΟΠΟΙ ΚΑΙ ΤΑΚΤΙΚΕΣ ΤΩΝ ΘΥΤΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙΑ ΤΗΝ ΕΞΑΠΑΤΗΣΗΤΩΝ ΘΥΜΑΤΩΝ

Σε σχέση με άλλες μορφές εγκλήματος, το κυβερνοέγκλημα προϋποθέτει τη χρήση ενός υπολογιστή, καθώς επίσης και στις περισσότερες των περιπτώσεων, μια πρώτη ενέργεια από πλευράς χρήστη του διαδικτύου.

Οι μελετητές συμφωνούν ότι υπάρχουν διάφορες τακτικές εξαπάτησης των θυμάτων και ότι πολλές από αυτές είναι ψυχολογικές (Bera κ.ά., 2023). Ο ψυχολογικός σχεδιασμός μιας επίθεσης παρενόχλησης ενός υποψήφιου θύματος, θεωρείται πολύ βασικός σε όλη αυτή την επιχείρηση εκμετάλλευσης των θυμάτων που καταβάλλεται

από τους θύτες και μεθοδικά οργανωμένος (Bera κ.ά., 2023). Οι μελετητές Bera κ.ά., (2023) διακρίνουν σε διάφορες ψυχολογικές τακτικές. Ορισμένες από αυτές αποσκοπούν στο να αφυπνίσουν τα συναισθήματα των θυμάτων μέσα από τον φόβο ή την απειλή, την απληστία, την δημιουργία της αντίληψης ότι υπάρχει άμεση αναγκαιότητα για την ανάληψη δράσης ή ότι υπάρχει σημαντική έλλειψη, ότι θα χαθεί μια σημαντική ευκαιρία, ότι θα φανεί ο αλτρουισμός (του θύματος αν απαντήσει στο μήνυμα) ή ότι θα κερδίσει κάτι σημαντικό ή θα ικανοποιήσει κάποια λαγνεία του. Για παράδειγμα στέλνεται (ψεύτικο) μήνυμα στο θύμα ότι τελειώνει η δυνατότητα αποθήκευσης των μηνυμάτων και θα πρέπει άμεσα να λάβει δράση, πατώντας πάνω σε κάποιο κουμπί (Bera κ.α., 2023). Σε όλες αυτές τις περιπτώσεις επιχειρείται η δημιουργία ενός ισχυρού συναισθήματος που θα επιφέρει και την απάντηση, επικοινωνία ή οποιαδήποτε γενικότερα ενέργεια που αποτελεί αλληλεπίδραση από την πλευρά του θύματος.

Σε άλλες πάλι περιπτώσεις επιχειρείται από τους θύτες να προσεγγίσουν τα θύματα μέσα από μηνύματα που αφορούν προσωπικά τον άμεσα ενδιαφερόμενο (στο κινητό του, το τάμπλετ ή τον υπολογιστή του) και δημιουργούν την εντύπωση ότι έχουν φτιαχτεί για να απευθυνθούν ειδικά προς τον ενδιαφερόμενο (Bera κ.α., 2023). Το απρόσωπο ύφος ενός μηνύματος χρησιμοποιείται όταν πρόκειται για (ψευδές) μήνυμα που απευθύνεται από κάποια δημόσια αρχή (Bera κ.α., 2023). Οι τρόποι προσέγγισης των χρηστών του διαδικτύου φαίνεται ότι είναι καλά μελετημένοι, ανάλογα με τον παραλήπτη των μηνυμάτων ή/και τον υποτιθέμενο αποστολέα.

Οι Grazioli and Jarvenpaa (2014) μελέτησαν τις τακτικές εξαπάτησης των θυμάτων, μελετώντας διαθέσιμα αρχεία, χρησιμοποιώντας ανάλυση περιεχομένου και δημιουργώντας μια βάση 201 περιπτώσεων από το διαδίκτυο. Οι συγγραφείς αυτής της μελέτης χρησιμοποιούν τον όρο εξαπάτηση (στα αγγλικά «deception») για να αναφερθούν στην θυματοποίηση των καταναλωτών και θεωρούν ότι ένας κύριος λόγος αυτής της απογοήτευσης είναι οι περιορισμένες και μη αντιπροσωπευτικές πληροφορίες που παρέχονται στα θύματα. Εξηγούν ότι το διαδίκτυο είναι ένα περιβάλλον συναλλαγών που στηρίζεται σε μια νοητική αναπαράσταση, που γίνεται στο μυαλό των ανθρώπων και η ύπαρξη αυτής της αναπαράστασης είναι προϋπόθεση για να ξεγελαστεί ένα θύμα. Αρκεί ο θύτης να δημιουργήσει ένα περιβάλλον που να φαίνεται ως αληθοφανές στον χρήστη που θα το χρησιμοποιήσει (Grazioli and Jarvenpaa, 2014, σελ. 96). Οι συγγραφείς επισημαίνουν ότι σύμφωνα με τη θεωρία της εξαπάτησης, υπάρχουν οι ακόλουθοι τρόποι εξαπάτησης: i) το

«μασκάρεμα» (masking) που προκύπτει όταν αποκρύπτονται ή εξαφανίζονται κρίσιμες πληροφορίες για ένα προϊόν κοινωνικής συναλλαγής, οι οποίες παράγουν εσφαλμένες παραδοχές, ii) το «ζάλισμα» (dazzling) όταν οι πληροφορίες παρέχονται αλλά είναι δύσκολο να τις καταλάβει ο χρήστης μιας ιστοσελίδας ή μιας υπηρεσίας ή είναι δύσκολα προσβάσιμες, iii) το δόλωμα (decoying) που προκύπτει όταν αποσπάται η προσοχή του θύματος από αυτό που πραγματικά συμβαίνει στην συναλλαγή, iv) η μίμηση (mimicking) όταν αντιγράφεται κάτι που συμβαίνει σε ένα άλλο περισσότερο γνωστό προϊόν ή συναλλαγή, v) η εφεύρεση (inventing) όταν ανακαλύπτεται εξολοκλήρου ένα προϊόν ή μια συναλλαγή χωρίς να υπάρχει καθόλου, vi) η δημιουργία καινούργιας ετικέτας για ένα προϊόν που προκύπτει όταν ένα προϊόν πλασάρεται με διαφορετικό τρόπο από αυτό που είναι (π.χ. ως μια χρηματοδοτική «ευκαιρία» ενώ πρόκειται για εξαπάτηση) και το vii) διπλό-παιχνίδι, όταν πείθεται το θύμα ότι το ίδιο το θύμα τελικά εκμεταλλεύεται τον θύτη που τον προσέγγισε (για παράδειγμα e-mails που δήθεν στάλθηκαν εσωτερικά μέσα σε μια επιχείρηση και παρέχουν εμπιστευτική πληροφορία εύκολα και άμεσα εκμεταλλεύσιμη).

1.3. ΕΝΑ ΣΥΓΧΡΟΝΟ ΠΡΟΒΛΗΜΑ ΜΕ ΜΕΓΑΛΕΣ ΔΙΑΣΤΑΣΕΙΣ

Το κυβερνοέγκλημα διαδίδεται παγκοσμίως με ταχύτατους ρυθμούς. Δηλαδή η συχνότητά του φαίνεται να αυξάνει. Σύμφωνα με την International Society που εκδίδει το Cyber Incident and Breach Trends Report, μόλις το 2018 έλαβαν χώρα 2 εκατομμύρια κυβερνο-επεισόδια (Olmstead, 2019). Οι Gopal κ.ά. (2022) αναφέρουν ότι ο τζίρος του κυβερνοεγκλήματος ανέρχεται σε 1,5 τρισεκατομμύριο δολάρια Η.Π.Α. ετησίως και ότι 860 εκατομμύρια εξ αυτών (δηλαδή περίπου το 57%) συνδέονται με τη λειτουργία παράνομων διαδικτυακών αγορών.

Σε ορισμένες περιοχές του πλανήτη, η εξάπλωση του κυβερνοεγκλήματος είναι πολύ μεγαλύτερη από άλλες. Έχει παρατηρηθεί ότι υπάρχει εξάπλωση του κυβερνοεγκλήματος σε χώρες με χαμηλά εισοδήματα, στις οποίες αυξάνεται ραγδαία ο αριθμός χρηστών του διαδικτύου και βελτιώνονται οι υποδομές. Παρόλα αυτά τα περισσότερα κυβερνοεγκλήματα καταγράφονται ακόμα και σήμερα στις ΗΠΑ.

Στις ΗΠΑ χάθηκαν 1.4 δις δολάρια το 2017 και στο Ηνωμένο Βασίλειο, μέχρι τα τέλη Ιούνιου του 2018 παρατηρήθηκαν 3,3 εκατομμύρια εξαπατήσεις σε σχεδόν 2,8 εκατ. θύματα (Cross, 2019).

Παράδειγμα ραγδαίας αύξησης του κυβερνοεγκλήματος αποτελεί η Κίνα, η οποία αποτελεί πλέον τον 2^{ο} μεγαλύτερο παραγωγό κυβερνοεγκλήματος παγκοσμίως. Ο Kshetri (2013) αναφέρει ότι το 2011 στην Κίνα 217 εκατομμύρια χρήστες του διαδικτύου (45% δηλαδή του πληθυσμού των χρηστών) είχαν δεχτεί επίθεση από ιούς, 121 εκατομμύρια χακαρίστηκαν ή παραβιάστηκαν οι κωδικοί τους και 8% έγιναν θύματα των scammers. Το 2009 η Κίνα ήταν 2^{η} μεταξύ των χωρών από τις οποίες προέρχονται οι κυβερνοεπιθέσεις, ενώ το 70% των παγκόσμιων κακόβουλων ιστοτόπων είχαν καταγραφεί στην Κίνα και αποσκοπούσαν σε εγχώριες επιχειρήσεις (Kshetri, 2013).

Υπάρχουν πολλές περιπτώσεις χωρών με μεγάλα προβλήματα κυβερνοεγκλήματος και εξαπάτησης. Πέραν της Νιγηρίας, από την οποία προέρχεται και η Νιγηριανή απάτη, η πλειοψηφία των πολιτών στην Κένυα (56%) έχουν δεχτεί παρενόχληση μέσω τηλεφώνου και θεωρείται ότι δυνάμει ολόκληρος ο πληθυσμός βρίσκεται εκτεθειμένος στην εξαπάτηση μέσω διαδικτύου, παρά τις πολιτικές και την νομοθεσία του κράτους της Κένυας για την αντιμετώπιση του κυβερνοεγκλήματος (Kulibay κ.ά., 2023).

Οι Badawi κ.ά (2022) διαπίστωσαν πολύ εκτεταμένη διάδοση του κυβερνοεγκλήματος σχετικά με τα κρυπτονομίσματα. Σε έρευνα που διεξήγαγαν από τον Νοέμβριο του 2019 έως το Φεβρουάριου του 2021, διαπίστωσαν ότι υπήρχαν πάνω από 8 εκατομμύρια ηλεκτρονικές διευθύνσεις εξαπάτησης σχετικές με τα κρυπτονομίσματα που, συνολικά, ελέγχονταν από πάνω από 1000 domains, και τα οποία έλαβαν συνολικά περίπου 8,7 εκατομμύρια δολάρια, με μέσο ποσό ανά χρήση περίπου 50 ευρώ.

Οι Meitle and Cross (2024) αναφέρουν ότι στην Αυστραλία το 2022 χάθηκαν 220 εκατομμύρια αυστραλιανά δολάρια μόνο από την εξαπάτηση για ρομαντικές γνωριμίες, ενώ το 2017 το ποσό αυτό ανέρχονταν σε 47 εκατομμύρια δολάρια. Επίσης, αναφέρουν ότι οι οικονομικές συνέπειες της συγκεκριμένης μορφής εγκλήματος υποεκτιμούνται γιατί τα θύματα δεν δηλώνουν την εξαπάτησή τους. Αυτό συμβαίνει για πολλούς λόγους: επειδή τα θύματα δεν θεωρούν την εξαπάτηση αυτή ίδια με τα υπόλοιπα εγκλήματα, για λόγους εχεμύθειας ή λόγω του στίγματος που δημιουργείται (Meitle and Cross, 2024). Ζητήματα όπως η συμπεριφορά της Αστυνομίας, η προηγούμενη εμπειρία που υπάρχει ως θύμα, πιθανή γνωριμία με το δράστη-θύτη, η σοβαρότητα της εξαπάτησης, η πιθανότητα αποζημίωσης τελικά και ο χρόνος και η προσπάθεια που χρειάζεται για την αναφορά του κυβερνοεγκληματος

επηρεάζουν την καταγραφή τους (Taylor, 2003, όπως αναφέρεται στο Meitle and Cross, 2024, σελ. 3). Η Anesa (2020) αναφέρει ότι στις ΗΠΑ από το 2015 ως το 2018 αυξήθηκαν κατά 150% οι αναφορές που έγιναν στο Δίκτυο Consumer Sentinel Network για εξαπάτηση σε σχέση με ρομαντικές γνωριμίες ενώ, την ίδια περίοδο η απώλεια χρημάτων εκτοξεύτηκε από 33 εκατομμύρια δολάρια σε 143 εκατομμύρια.
Τέλος, για την συγκεκριμένη μορφή κυβερνοεγκλήματος, στις ΗΠΑ το $1,3 από τα $8,8 εκατομμύρια δολάρια που απέσπασαν οι διάφορες μορφές εξαπάτησης, οφείλονταν σε αυτήν την μορφή εξαπάτησης (Drew και Webster, 2023).

1.4. ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΟΥ ΠΡΟΒΛΗΜΑΤΟΣ

Οι συνέπειες των κυβερνοεγκλημάτων είναι πολλές και εκτείνονται σε ένα μεγάλο φάσμα (EU, 2024).
Υπάρχουν διάφοροι τρόποι κάποιος να διακρίνει και να μελετήσει τις συνέπειες του προβλήματος. Μπορεί να γίνει διάκριση ως προς τα γνωρίσματα των θυμάτων. Για παράδειγμα, στη βιβλιογραφία αναφέρεται ότι η ηλικία είναι ένα κριτήριο για εξαπάτηση σε σχέση με ρομαντικές γνωριμίες (Drew and Webster, 2023). Άρα το κριτήριο της ηλικίας των θυμάτων γίνεται να χρησιμοποιηθεί για τη διάκριση των συνεπειών του προβλήματος.
Ένας άλλος κύριος τρόπος να τις διακρίνουμε, είναι να εστιάσουμε σε συνέπειες για το ίδιο το άτομο όπως ψυχολογικές, οικονομικές, κοινωνικές κτλ. και σε συνέπειες συνολικά για την οικονομία, την κοινωνία κτλ.

1.4.1. Ως προς τους χρήστες του διαδικτύου

1.4.1.1. Οικονομικές συνέπειες για τους χρήστες

Οι κυριότερες ίσως συνέπειες του κυβερνοεγκλήματος για τα θύματα είναι οι οικονομικές. Υπάρχουν, ήδη, πολλά εκατομμύρια ανθρώπων παγκοσμίως που επειδή έγιναν στόχοι των κυβερνοεγκληματιών έχασαν χρηματικά ποσά, περιουσιακά στοιχεία, σπίτια τόσο μέσω της διάπραξης του κυβερνοεγκλήματος όσο και αργότερα, εμπλεκόμενοι στις σχέσεις με τους εγκληματίες. Θα μπορούσε κανείς να δώσει αμέτρητα σχετικά παραδείγματα αλλά τα αθροιστικά στοιχεία είναι αρκετά: Σύμφωνα με το Global Risks Report του Παγκόσμιου Οικονομικού Φόρουμ για το 2023, το κόστος από το κυβερνοέγκλημα ενδέχεται να φτάσει τα 10,5 τρις δολάρια ΗΠΑ το

2025.Η Ευρωπαϊκή Επιτροπή είχε εκτιμήσει για το 2019 το κόστος αυτό στα 5,5 τρις (EU, 2024).

1.4.1.2. Ψυχολογικές συνέπειες

Οι ψυχολογικές συνέπειες για τα θύματα από την διαδικτυακή εξαπάτηση είναι πολλές. Τα θύματα αναφέρουν εκτός από θυμό, την αγωνία, την σύγχυση, την κατάθλιψη, την αϋπνία, σε κάποιες περιπτώσεις μέχρι και τάσεις αυτοκτονίας (Cross κ.ά., 2016, όπως αναφέρεται στο Hansen, 2024). Ο τρόπος που οι θύτες τα έχουν μεταχειριστεί είναι χειριστικός, και έχει δημιουργήσει ήδη πολλά αρνητικά συναισθήματα. Σε αυτά, προστίθεται η μεγάλη ψυχολογική απογοήτευση που δημιουργεί η αποκάλυψη μιας απάτης και ότι αποτελούσαν θύμα εξαπάτησης.

Ο Cross (2019, σελ. 121) αναφέρει επίσης ότι τα θύματα της εξαπάτησης μέσω διαδικτύου νιώθουν μεγάλη απογοήτευση από τον έλεγχο που τους γίνεται από την αστυνομία και τις απαντήσεις που χρειάζεται να δώσουν σε αυτήν και ότι στην πράξη αντιμετωπίζουν συμπληρωματικό τραύμα από τον τρόπο που γίνεται η μεταχείριση της υπόθεσής τους από την αστυνομία.

1.4.1.3. Ως προς την κοινωνία και τον άνθρωπο -θύμα

Τα θύματα του κυβερνοεγκλήματος υπόκεινται σε μια σειρά από αρνητικά στερεότυπα, τον στιγματισμό και την κατηγορία της ίδιας της κοινωνίας, της οικογένειας και του περίγυρού τους (Meikle and Cross, 2024, Hansen, 2024). Η έκταση του στιγματισμού είναι μεγάλη και θεωρείται και βασικός λόγος για τον οποίο τα θύματα δεν επικοινωνούν το πρόβλημά τους σε άλλους χρήστες.

Το αποτέλεσμα του στιγματισμού και της κατηγορίας του θύματος, είναι να θεωρούν τους εαυτούς τους ως ανόητους και ένοχους και να έχουν ενοχικά σύνδρομα (Hansen, 2024).

1.4.2. Ως προς την οικονομία (εθνική, τοπική και άλλη)

Οι Manasrah κ.ά.. (2015, σελ. 3) αναφέρουν ότι οι εκτιμώμενες παγκόσμιες οικονομικές συνέπειες της παρενόχλησης μέσω e-mail, ανέρχονταν σε 25 δις δολάρια ΗΠΑ και οι κυριότερες οικονομικές συνέπειες οφείλονται στον χρόνο που χρειάζεται να βρει και να διαγράψει κανείς τα σχετικά μηνύματα παρενόχλησης που λαμβάνει.

Πρόσφατα υπολογίστηκε από την εταιρεία Pricefox ότι το κόστος των κυβερνοεπιθέσεων είναι της τάξης των 10 τρισεκατομμυρίων δολαρίων για το έτος 2023. Άρα πρόκειται για μια ιδιαίτερα κερδοφόρα δραστηριότητα για τους κυβερνοεγκληματίες (Ναυτεμπορική, 2023).

1.4.3. Ως προς την κοινωνία

Η κοινωνία της οποίας τα μέλη υφίστανται ψυχολογικές, οικονομικές και άλλες συνέπειες και των οποίων δεν διασφαλίζεται το αίσθημα της σιγουριάς και της δημόσιας ασφάλειας, είναι κοινωνίες φόβου και μίσους. Όπως αυτό ισχύει για κάθε μορφής έγκλημα, ισχύει και για το κυβερνοέγκλημα.

Μια κοινωνία, μπορεί να δεχτεί ισχυρό πλήγμα λόγω της μεγάλης ανάπτυξης του κυβερνοεγκλήματος και του αριθμού των θυμάτων, αν για παράδειγμα χάσει κάποια μέλη της που μπορεί να καταναλώνουν και να δαπανούν σε μικρές τοπικές κοινωνίες (και δεν θα μπορούν να το κάνουν πλέον αν χάσουν μεγάλα χρηματικά ποσά).

1.5. Η ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ ΣΤΗΝ ΕΛΛΑΔΑ ΚΑΙ ΤΟ ΕΞΩΤΕΡΙΚΟ: ΔΙΑΘΕΣΙΜΕΣ ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΕΡΓΑΛΕΙΑ

Οι τρόποι αντιμετώπισης του κυβερνοεγκλήματος μπορούν να διακριθούν σε νομικούς, τεχνολογικούς, οργανωσιακούς (Chung κ.ά., 2006).

Νομικά, το κυβερνοέγκλημα καταπολεμάται μέσω της δημιουργίας νόμων και του κατάλληλου νομικού πλαισίου.

Τεχνολογικά, αντιμετωπίζεται μέσω της ενδυνάμωσης της τεχνολογικής προστασίας με τεχνολογικά μέσα ασφάλειας και προστασίας αλλά και της εξιχνίασης, πρόληψης και καταστολής μέσω της κατάλληλης τεχνολογίας.

Οργανωσιακά, το κυβερνοέγκλημα αντιμετωπίζεται μέσω της δημιουργίας κατάλληλων οργανωτικών υποδομών και οργανισμών ή της ανάθεσης ειδικού χαρτοφυλακίου για την κυβερνο-προστασία στο ή στα Υπουργεία εκείνα που ασχολούνται με την προστασία του πολίτη (Chung κ.ά.., 2006).

1.5.1. Πολιτικές ενάντια στο κυβερνοέγκλημα εκτός Ελλάδας

Είναι παγκόσμιο πρόβλημα η αδυναμία των αστυνομικών αρχών να αντιμετωπίσουν το κυβερνοέγκλημα και ο κακός εξοπλισμός τους τροχοπέδη για την αντιμετώπισή

του (Cross, 2019). Σε μια έρευνα που διεξήγαγε το Αυστραλιανό δίκτυο Cybercime Online Reporting Network (ACORN) διαπιστώθηκε ότι τα τρία-τέταρτα των Αυστραλών ήταν δυσαρεστημένοι από το αποτέλεσμα που είχαν οι αναφορές κυβερνοεγκλήματος που έκαναν (Cross, 2019) .

Οι πολιτικές για την αντιμετώπιση της εξαπάτησης μέσω διαδικτύου και του κυβερνοεγκλήματος μπορούν να διακριθούν σε κρατικές και σε πολιτικές μεταξύ κρατών (Chung κ.ά., 2006). Τόσο οι χώρες των G8 όσο και το Συμβούλιο της Ευρώπης έχουν υιοθετήσει μια στρατηγική για την αποτροπή και μείωση του (Chung κ.ά., 2006).

Επίσης στην καταπολέμηση του κυβερνοεγκλήματος εμπλέκονται και άλλοι φορείς. Κυριότεροι, ανάμεσα σε αυτούς είναι οι τράπεζες και τα χρηματοπιστωτικά ιδρύματα, τα οποία αναλαμβάνουν και το ρόλο της προστασίας των χρημάτων των πελατών τους.

Ο ρόλος τους είναι κομβικός σε θέματα όπως η εξαπάτηση με κρυπτονομίσματα. Στην Αυστραλία (Nataraj-Hansen, 2024) έχει δημιουργηθεί ένα Δίκτυο σε θέματα Δικαίου και Εξαπάτησης (Fraud Justice Network) στο οποίο εμπλέκεται οποιαδήποτε αρχή διερευνά, κάνει αναφορά, μετράει, αναλύει την εξαπάτηση μέσω διαδικτύου και υποστηρίζει τα θύματα. Τέτοιες αρχές, είναι η Αυστραλιανή Επιτροπή Καταναλωτών και Ανταγωνισμού, η Αυστραλιανή Επιτροπή Υπηρεσίας Πληροφοριών για το έγκλημα (Criminal Intelligence Commission), διάφορα όργανα της ομοσπονδιακής κυβέρνησης της Αυστραλίας, επιχειρήσεις χρηματοδότησης, όπως και επιχειρήσεις που παρέχουν υπηρεσίες διαδικτυακών ραντεβού κ.ά. Το έργο της ενημέρωσης των χρηστών του διαδικτύου και της πρόληψης είναι συλλογικό και προκύπτει μέσα από την συνεργασία όλων αυτών των φορέων που επίσης εργάζονται και αυτόνομα για την πρόληψη ή/και την καταστολή του κυβερνοεγκλήματος (Nataraj-Hansen, 2024).

Ένα αντίστοιχο δίκτυο (με την ίδια επωνυμία) έχει δημιουργηθεί μεταξύ Λονδίνου και Τορόντο (Cross, 2019).

Οι υπερασπιστές από κυβερνοεπιθέσεις ενδιαφέρονται για την προστασία των περιουσιακών στοιχείων των θυμάτων, την φήμης τους και την προστασία από μελλοντικές κυβερνοεπιθέσεις. Τα εργαλεία που έχουν στη διάθεσή τους και χρησιμοποιούν οι υπερασπιστές των θυμάτων είναι ηλεκτρονικές διευθύνσεις για την ανταλλαγή ενημέρωσης και πληροφοριών, ειδικό λογισμικό προστασίας, εργαλεία διαχείρισης των δικτύων και παρακολούθησης, εργαλεία κρυπτογράφησης καθώς και εργαλεία εγκληματολογικής έρευνας (Arief και Adzmi, 2015).

Η εκπαίδευση των θυμάτων έτσι ώστε να αντιλαμβάνονται καλύτερα μια εξαπάτηση που επιχειρείται μέσω διαδικτύου, είναι μια από τις πολιτικές που χρησιμοποιούνται από ορισμένες χώρες για την αντιμετώπιση της εξαπάτησης αυτής και του κυβερνοεγκλήματος. Ωστόσο έχουν διατυπωθεί και επιφυλάξεις κατά πόσο μπορεί να είναι επιτυχής τελικά μια τέτοιας μορφής εκπαίδευση (Kulibay κ.ά., 2023).

Σε ότι αφορά τα κρυπτονομισματα, ιδιαίτερα, αξίζει να αναφερθεί ότι υπάρχει ένα επίπεδο αυτό-οργάνωσης της κοινότητας των χρηστών του Blockchain, όπως αναφέρουν οι Xia κ.ά. (2020). Μέσα από τη δημιουργία βάσεων, ανοικτών σε πρόσβαση στο κοινό για συγκεκριμένα κρυπτονομίσματα (π.χ. η βάση EtheriumscamDB για το κρυπτονόμισμα Etherium), επιχειρείται να καταστούν γνωστές οι ψεύτικες ιστοσελίδες και οι τρόποι εξαπάτησης σχετικά με τα κρυπτονομίσματα αυτά στο ευρύ κοινό που θέλει να προβεί στην αγοροπωλησία τους (Xiaκ.ά., 2020). Δηλαδή, επιτυγχάνεται σε ένα βαθμό, η αυτό-οργάνωση σε θέματα ασφάλειας που αφορά μελλοντικούς πιθανούς χρήστες του διαδικτύου σχετικά με ένα κρυπτονόμισμα.

1.5.2. Πώς καταπολεμάται το κυβερνοέγκλημα στην Ελλάδα

Στην Ελλάδα, οι τρόποι αντιμετώπισης του κυβερνοεγκλήματος εστιάζουν στο ρόλο και τις αρμοδιότητες της Ελληνικής Αστυνομίας και του Ελληνικού Υπουργείου Προστασίας του Πολίτη. Σε αυτό το Υπουργείο, έχει συσταθεί ειδική Διεύθυνση Δίωξης του Ηλεκτρονικού Εγκλήματος που μελετάει τις περιπτώσεις κυβερνοεγκλήματος στην Ελλάδα και τις αντιμετωπίζει, αναπτύσσοντας κοινές δράσεις με τις υπηρεσίες ασφαλείας άλλων χωρών (Δράκος, 2022).

Επίσης, κύριος είναι ο ρόλος και του Υπουργείου Ψηφιακής Διακυβέρνησης. Το Υπουργείο αυτό έχει προετοιμάσει ειδική Εθνική Στρατηγική για την Κυβερνοασφάλεια για την περίοδο 2020-2025. Στο κείμενο της στρατηγικής αυτής, παρουσιάζονται τα διάφορα κυβερνοεγκλήματα που παρουσιάζονται στην Ελλάδα και των οποίων επιδιώκεται η καταστολή και πρόληψη (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Επίσης, με βάση την Εθνική Στρατηγική για την Κυβερνοασφάλεια, η αντιμετώπιση του κυβερνοεγκλήματος στη χώρα μας γίνεται από ενέργειες και δράσεις της Γενικής Διεύθυνσης Κυβερνοασφάλειας (την Εθνική Αρχή Κυβερνοασφάλειας), την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων- Εθνικό C.E.R.T. (που υπάγεται στην

ΕΥΠ), τη Διεύθυνση Κυβερνοάμυνας του Υπουργείου Εθνικής Άμυνας, τη Δίωξη Ηλεκτρονικού Εγκλήματος (που υπάγεται στην ΕΛΑΣ) και ορισμένες εθνικές αρχές που είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η Εθνική Αρχή Τηλεπικοινωνιών και Ταχυδρομείων, η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών καθώς και το Κέντρο Μελετών Ασφάλειας. Όλες αυτές οι Υπηρεσίες δρουν μεμονωμένα αλλά και σε συνεργασία. Παρόλα αυτά, δεν θα μπορούσαμε να μιλήσουμε για ένα Δίκτυο, υπό την έννοια που το είδαμε να λειτουργεί σε άλλες χώρες, όπως η Αυστραλία.

Κατά καιρούς, έχουν λάβει χώρα στην Ελλάδα διάφορες πρωτοβουλίες για την προστασία από το κυβερνοέγκλημα. Μια ενδεικτική είναι αυτή του Υπουργείου Οικονομικών που συνέστησε την D.A.R.T. (Digital Awareness and Response to Threats), μια ειδική ομάδα για την ψηφιακή ασφάλεια (Vlachos κ.ά., 2011). Η D.A.R.T. λειτούργησε από τον Μάρτιο του 2007 ως το Σεπτέμβριο του 2010 με σκοπό να αυξήσει την ενημέρωση του κοινού για το κυβερνοέγκλημα και να κατευθύνει τα ερωτήματα των χρηστών προς την καλύτερη υπηρεσία (Vlachos κ.ά., 2011). Η ομάδα συνέβαλε στην προώθηση των στρατηγικών συνεργασιών γύρω από το θέμα του κυβερνοεγκλήματος στην Ελλάδα (Vlachos κ.ά., 2011).

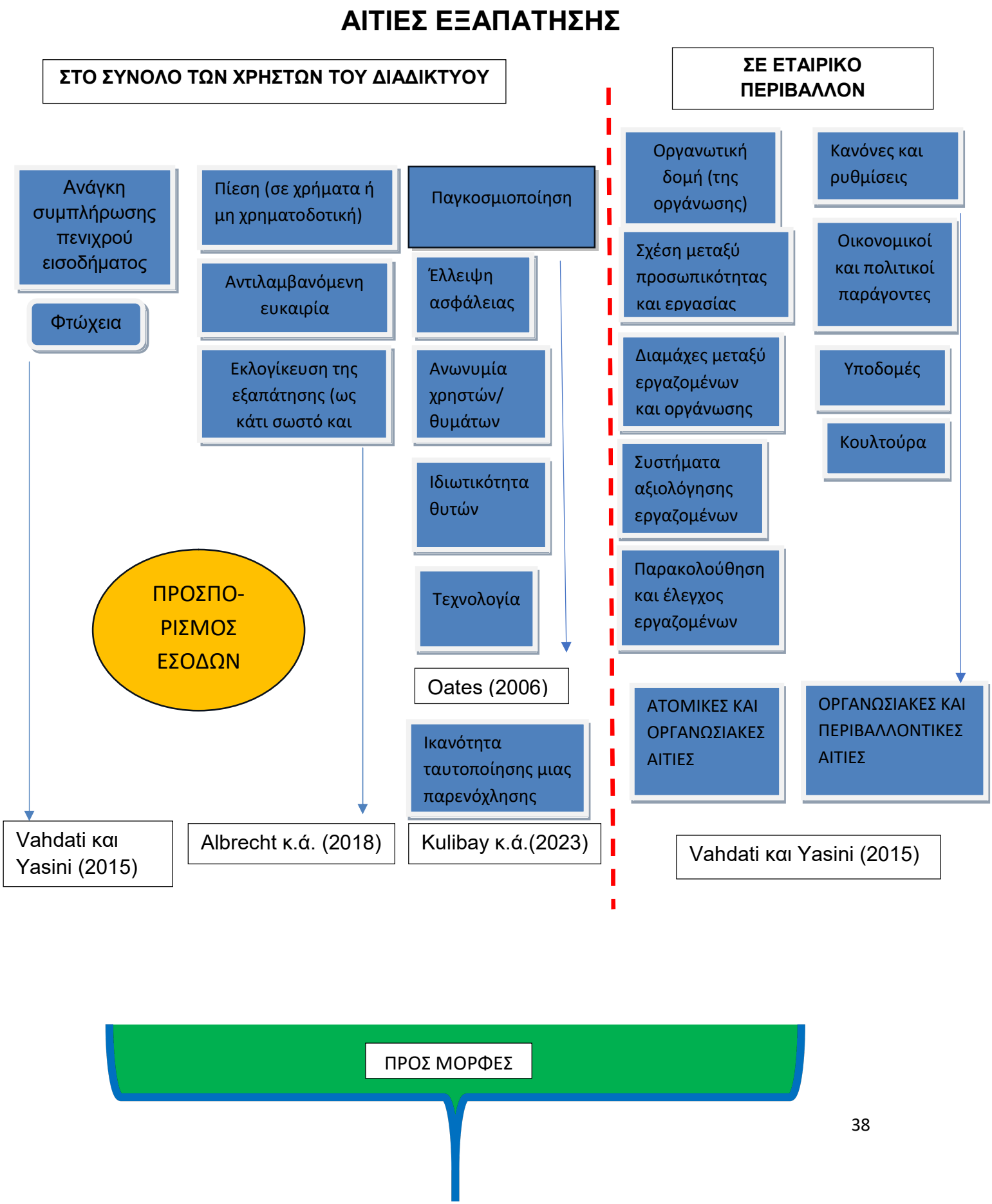
Στην μελέτη τους για το κυβερνοέγκλημα στην Ελλάδα, οι Vlachos κ.ά. (2011) ανάλυσαν τις 1189 περιπτώσεις αναφορών και παραπόνων στην Ελλάδα που χειρίστηκε η D.A.R.T.. Οι μισές από τις περιπτώσεις που εξέτασαν (49.6%), αφορούσαν προσπάθεια χρηματοδοτικής εξαπάτησης και 14.8% αφορούσαν παραβίαση προσωπικών δεδομένων.

1.6. ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ: ΈΝΑ ΣΥΝΘΕΤΟ ΠΡΟΒΛΗΜΑ

Από τα παραπάνω, αντλείται το συμπέρασμα, ότι το κυβερνοέγκλημα προκαλείται από διάφορες αιτίες, ότι υπάρχουν πολλές μορφές παρενόχλησης των υποψήφιων θυμάτων και ότι δύναται να επιφέρει πολλές και διαφορετικές συνέπειες.

Η παραπάνω συσχέτιση μεταξύ αιτιών, μορφών και συνεπειών θα μπορούσε επιγραμματικά να αναπαρασταθεί με το ακόλουθο διάγραμμα που τονίζει ότι υπάρχουν διάφορες αιτίες, μέσα από τις οποίες παράγονται διάφορες μορφές κυβερνοεγκλήματος και επιφέρουν διάφορες συνέπειες:

Πίνακας 1: Αιτίες, μορφές, τακτικές εξαπάτησης και συνέπειες του κυβερνοεγκλήματος



ΜΟΡΦΕΣ ΕΞΑΠΑΤΗΣΗΣ

Εξαπάτηση με κρυπτονομίσματα

Badawiκ.ά (2022), Xia κ.ά. (2020)

Ηλεκτρονικά μηνύματα παρενόχλησης (spams)

Manarash κ.ά. (2015), Dunham (2007)

Σχήματα ή πυραμίδες Ponzi

Vahdati και Yasini (2015)

Ρομαντικές γνωριμίες ή επαφές

Vahdati και Yasini (2015)

Παρενόχληση μέσω email

Manasrahκ.ά. (2015), Glickman (2005), Genc κ.ά. (2021), Kubilay κ.ά. (2023), Computer Fraud and Security, 2019

Νιγηριανή απάτη

Genc κ.ά. (2021), Computer Fraud and Security (αγν.έτους)

Ψεύτικες ιστοσελίδες

Cohen (2019), Gopal κ.ά. (2022)

Εξαπάτηση σχετικά με κληρονομιές

Cross (2019)

Εξαπάτηση σχετικά με λαχνούς ή λαχεία

Cross (2019)

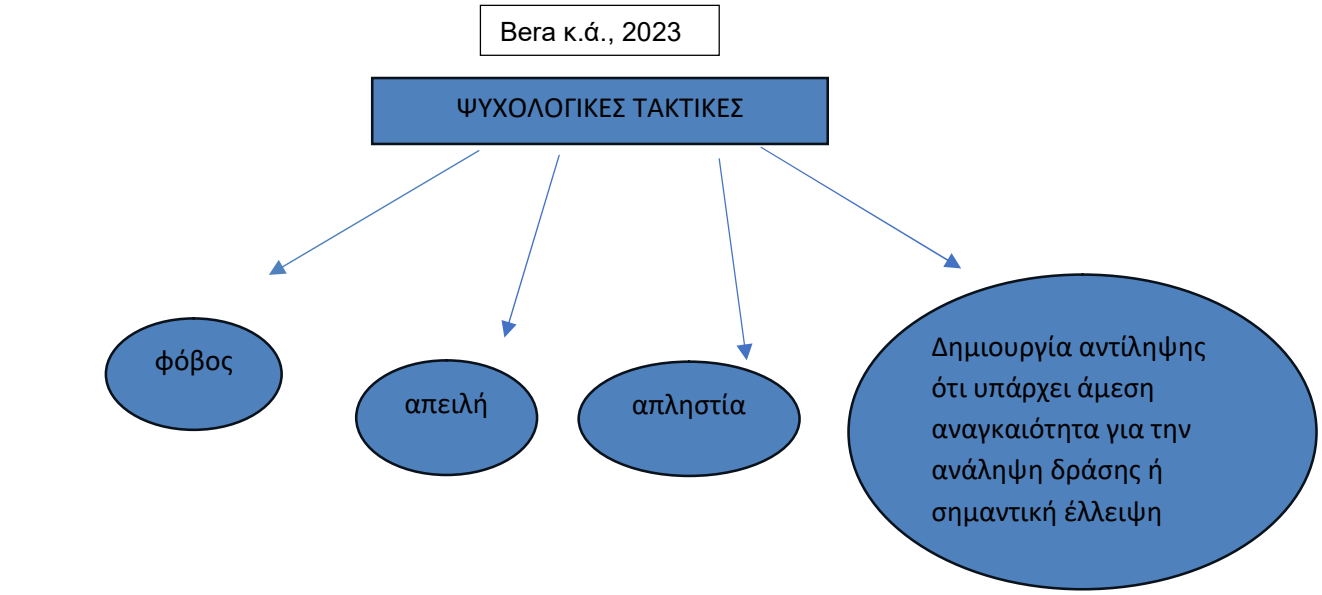
Εξαπάτηση σε θέματα υγείας

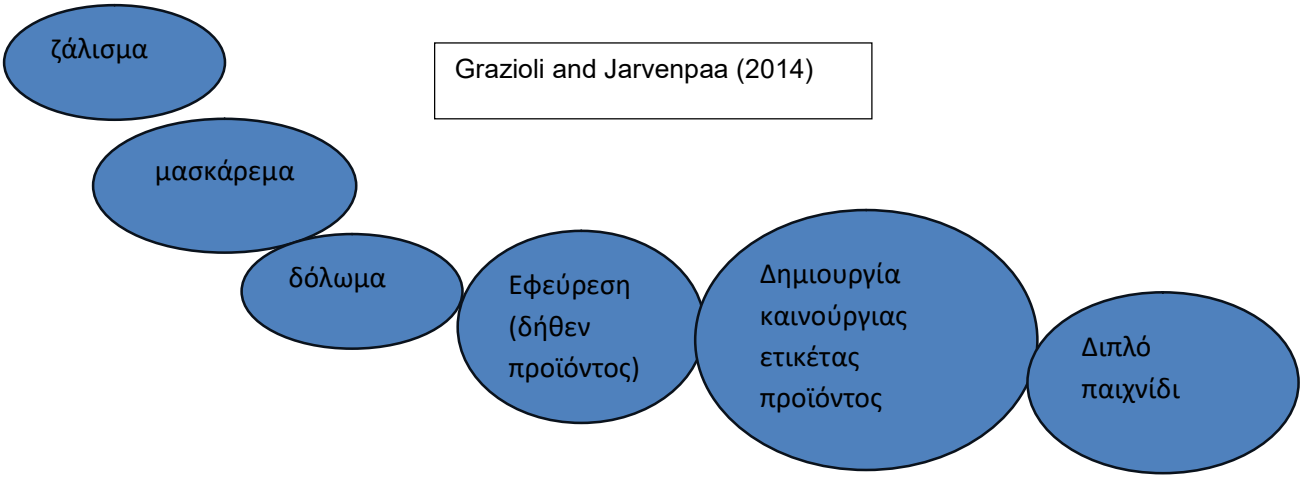
Garrett κ.ά. (2019^{A}), Garrett κ.ά. (2019B)

Κακόβουλα λογισμικά ή ιοί

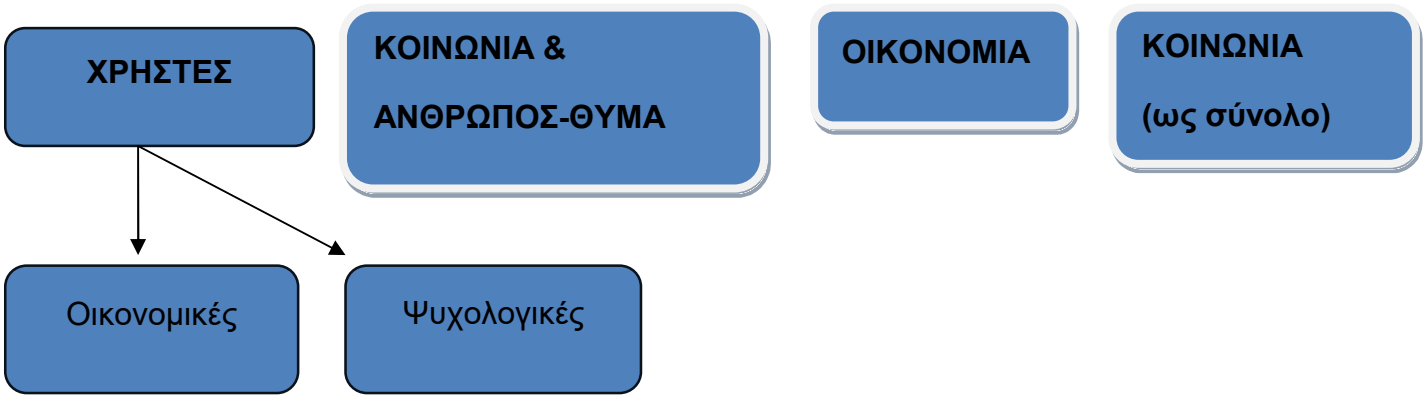
Vahdati και Yasini (2015)

ΤΡΟΠΟΙ ΚΑΙ ΤΑΚΤΙΚΕΣ ΕΞΑΠΑΤΗΣΗΣ





ΣΥΝΕΠΕΙΕΣ



Αν το διάγραμμα συνδεθεί με τις πολιτικές, φαίνεται ότι η αντιμετώπιση του κυβερνοεγκλήματος, μέσα από τις ασκούμενες πολιτικές μπορεί να οφείλεται στις συνέπειες που το προκαλούν, στις πολλές μορφές που λαμβάνει αλλά το ουσιαστικότερο όλων είναι να αντιμετωπίζει τις αιτίες που το προκαλούν, γιατί λόγω των αιτιών αυτών θα εξακολουθεί να λαμβάνει διάφορες μορφές και να επιφέρει τις ίδιες ή και χειρότερες συνέπειες.

Το συμπέρασμα αυτό, έχει ενδιαφέρον και για τις ασκηθείσες πολιτικές, γιατί μπορεί οι αιτίες για τις οποίες παρουσιάζεται το κυβερνοέγκλημα, να είναι αιτίες για τις οποίες δεν αντιμετωπίζεται ορθά και χρειάζεται ένας άλλος συνδυασμός μέσων πολιτικής ή πολιτικών. Για παράδειγμα, στην Ελλάδα δεν υπάρχει η συνεργασία μεταξύ φορέων υπό τη μορφή ενός δικτύου που προαναφέρθηκε ότι υφίσταται στην περίπτωση της Αυστραλίας και λειτουργεί προστατευτικά για τους πολίτες.

Συνεπώς, ταυτόχρονα με τη διερεύνηση των αιτιών του προβλήματος χρειάζεται και η διερεύνηση των αιτιών για τις οποίες οι πολιτικές δεν επιφέρουν καλά αποτελέσματα.

ΚΕΦΑΛΑΙΟ 2ο: ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

Στο παρόν κεφάλαιο, λαμβάνοντας υπόψη την προηγούμενη ανάλυση της βιβλιογραφίας (που σημειώνεται ότι στηρίχθηκε σε άρθρα της ABSqualitylist), παρουσιάζεται η μεθοδολογία της έρευνας που ακολουθήθηκε.

Έχοντας προηγουμένως αναλύσει, στη βιβλιογραφία, ότι το κυβερνοέγκλημα λαμβάνει διάφορες μορφές και έχει αρκετές αιτίες και διαφορετικές συνέπειες ανάλογα με την μορφή που λαμβάνει, το ερευνητικό ερώτημα που τέθηκε (και το συνολικό ερευνητικό εγχείρημα που πραγματοποιήθηκε), εστίασε σε μια προσπάθεια διερεύνησης του κυβερνοεγκλήματος μέσα από τις πολλές πτυχές που αυτό έχει, μέσα από τη χρήση ενός ερωτηματολογίου.

Η -κατά το δυνατόν- ολιστική αυτή προσπάθεια εστίασε στην μελέτη των αιτιών του κυβερνοεγκλήματος, των μορφών παρενόχλησης που είναι περισσότερο διαδεδομένες στην Ελλάδα και των συνεπειών του. Εξετάστηκε όμως και πλήθος άλλων σημείων, όπως η συχνότητα του κυβερνογκλήματος, οι στρατηγικές πειθούς, η αρχική αντίδραση των υποψήφιων θυμάτων κ.ά., ώστε να δοθεί μια συνολική εικόνα για το τι είναι το κυβερνοέγκλημα, πώς λαμβάνει χώρα στην Ελλάδα και γιατί. Επίσης αξιολογήθηκαν οι σημερινοί τρόποι αντιμετώπισής του κυβερνοεγκλήματος από τις αρχές και τη Δημόσια Διοίκηση και η επάρκεια που αυτές έχουν στο πρόσωπο των πολιτών. Σκοπός, ήταν οι πολίτες να δηλώσουν εάν θεωρούν ικανοποιητικούς τους τρόπους αντιμετώπισης του κυβερνοεγκλήματος και σε ποιό βαθμό και αν γίνεται να καταστούν περισσότερο αποτελεσματικοί.

Μεθοδολογικά, αρχικά επιδιώχθηκε να αναζητηθούν στοιχεία από τις δευτερογενείς πηγές μέσω της επικοινωνίας με την Ελληνική Αστυνομία. Ωστόσο, δεν κατέστη δυνατόν να βρεθεί συγκεκριμένη βάση δεδομένων, ανάλογη με αυτήν που υπήρχε παλαιότερα και είχε χρησιμοποιηθεί από την έρευνα των Vlachos κ.α. (2011).Το πρόβλημα της παραβίασης του απορρήτου και της ιδιωτικότητας τέθηκε από τις αρχές όσο και από την συνομιλία με ειδικούς ερευνητές επί του ζητήματος. Για το λόγο αυτό, προτιμήθηκε η συλλογή πρωτογενών δεδομένων, παρά τις πιθανές αδυναμίες που παρουσιάζει σύμφωνα και με τη βιβλιογραφία, δηλαδή την χρονική καθυστέρηση στην συλλογή των δεδομένων αλλά και το κύριο πρόβλημα μεροληψίας της δειγματοληψίας που μπορεί να εμφανιστεί ανάλογα με την μέθοδο δειγματοληψίας που επιλέγεται.

Λόγω τόσο του θέματος όσο και της δειγματοληψίας, επιλέχθηκε η χρήση της ποιοτικής έρευνας, στην οποία, όπως αναφέρουν η Ίσαρη και Πουρκός (2015, σελ. 28), βασίζονται οι κοινωνικές επιστήμες για την ανάλυση ενός φαινομένου. Σε αντίθεση με την ποσοτική μέθοδο που είναι εξηγητική ή εμπειρική ή ακόμα και νομοθετική, η ποιοτική μέθοδος και έρευνα είναι περισσότερο περιγραφική και χρησιμεύει στην περιγραφή, ερμηνεία και συνεπώς και την κατανόηση καταστάσεων. Σε αυτές επιχειρείται καλύτερα η καταγραφή και ανάλυση σύνθετων φαινομένων.(Ίσαρη και Πούρκος, 2015, σελ. 40). Άρα επιτυγχάνει να γίνει περισσότερο ερμηνευτική (Ίσαρη και Πούρκος, 2015, σελ. 28).

Όπως αναφέρουν οι Χαλικιάς κ.ά. (2015), οι δειγματοληψίες είναι χρήσιμες στην μελέτη φαινομένων και ζητημάτων που αφορούν ένα μεγάλο πληθυσμό, όπως είναι ο πληθυσμός μιας ολόκληρης χώρας καθώς και ότι παρουσιάζουν πλεονέκτημα έναντι άλλων ερευνών. Στα πλεονεκτήματά τους συγκαταλέγονται αυτά της εύκολης επεξεργασίας συμπερασμάτων όταν επιλέγονται κλειστές ερωτήσεις. Επίσης ένα σημαντικό πλεονέκτημα της έρευνας αυτής είναι ότι δεν παρουσιάζει πολλά δεοντολογικά προβλήματα, γιατί ο ερευνητής δεν αποκρύπτει τον ρόλο του από τον ερωτώμενο. Ο τελευταίος, μπορεί να αποφασίσει και να απαντήσει στις ερωτήσεις που του γίνονται ανεπηρέαστος. Στα μειονεκτήματά τους οι Χαλικιάς κ.ά., (2015) αναφέρουν ότι η ορθή διεξαγωγή τους απαιτεί πολύ χρόνο και χρήμα..

Υπάρχουν διάφορα είδη δειγματοληψίας στην ποιοτική έρευνα (Ίσαρη και Πούρκος, 2015, Χαλικιάς κ.ά., 2015). Στην παρούσα εργασία, το είδος της δειγματοληψίας που προτιμήθηκε υπαγορεύτηκε και από τις συνθήκες της έρευνας και την χρονική πίεση που υφίσταται για την έρευνα στα πλαίσια μιας πανεπιστημιακής εργασίας. Επιχειρήθηκε, ωστόσο, να γίνει διασπορά του δείγματος μεταξύ πολλών και διαφορετικών φορέων αλλά και προσώπων, ούτως ώστε να προσεγγίσει πολλά και διαφορετικά κοινά και να είναι εν τέλει αντιπροσωπευτικό και αξιόπιστο κατά το μέγιστο δυνατό τρόπο.

Η κύρια μέθοδος της δειγματοληψίας που χρησιμοποιήθηκε είναι της χιονοστιβάδας, δηλαδή, δόθηκε το ερωτηματολόγιο σε ανθρώπους-κλειδιά που το προώθησαν σε μεγάλο αριθμό πληθυσμού, με το αίτημα και εκείνοι να το απαντήσουν να το προωθήσουν σε άλλους. Αυτό έγινε, για να εξασφαλισθεί ότι θα καλυφθεί ολόκληρη η Ελληνική επικράτεια και περιοχές αλλά και τύποι θυμάτων για τα οποία δεν θα ανευρίσκονταν απαντήσεις.

Ένα μεγάλο πρόβλημα της έρευνας όμως, ήταν ότι δεν εξασφαλίζονταν εκ προοιμίου η πανελλαδική σύνθεση του δείγματος μόνο με τη διανομή κατ' αυτόν τον τρόπο. Έτσι, επιλέχθηκαν επιπλέον φορείς, στα μέλη των οποίων στάλθηκε το ερωτηματολόγιο και προέρχονταν από διαφορετικές περιοχές της Ελλάδας. Έτσι, προτιμήθηκε σκόπιμα η δειγματοληψία να εστιάζει σε ένα δείγμα που αντιπροσωπεύει μεγαλύτερο τμήμα της Ελληνικής περιφέρειας σε σχέση με την Αττική. Δηλαδή η δειγματοληψία έγινε και σκόπιμη παράλληλα. Αυτό, επετεύχθη με την αποστολή των ερωτηματολογίων σε φορείς και πρόσωπα, μεταξύ άλλων, από τη νησιωτική Ελλάδα, την περιφέρεια της Πελοποννήσου και της Στερεάς Ελλάδας και Θεσσαλίας, περιοχές που πιθανότατα 'υστερούσαν' με μια πρόχειρη αρχική εκτίμηση. Στη σκόπιμη δειγματοληψία, επιλέγονται σκοπίμως κάποιες συγκεκριμένες περιπτώσεις επιτυχίας ή αποτυχίας ή ασυνήθιστες, προκειμένου να μελετηθούν καλύτερα (Ίσαρη και Προύσκος, 2015).

Όπως προειπώθηκε, η εργασία στηρίχθηκε στη δημιουργία ενός ερωτηματολογίου που θα επέτρεπε τη διερεύνηση του κυβερνο-εγκλήματος στην Ελλάδα, της ιδίας αντίληψης που έχουν οι Έλληνες για αυτό, για τη διάδοσή και τις μορφές που ήδη έχει λάβει στη χώρα μας, τις συνέπειες που προκαλεί, τις αιτίες που το προκαλούν και την αντίληψη που υπάρχει στους Έλληνες πολίτες για τις πολιτικές και τους τρόπους αντιμετώπισής του. Αντί δηλαδή να γίνει καταγραφή από δευτερογενείς πηγές ή μια ανάλυση με ερωτήσεις των ειδικών, προτιμήθηκε να διερευνηθεί η άποψη των πολιτών και όσων έχουν πέσει θύματα του κυβερνοεγκλήματος σε πρώτο βαθμό. Επειδή ένα έγκλημα προϋποθέτει την ύπαρξη θύτη και θύματος, ενώ όσοι το προλαμβάνουν, το καταστέλλουν ή το δικάζουν αποτελούν τρίτους στη σχέση αυτή, θεωρήθηκε πιο σημαντικό να κατανοήσει κανείς το έγκλημα από την πλευρά του θύματος, παρά από την πλευρά ενός εξωτερικού τρίτου προσώπου ή αρχής που λειτουργεί εκ των υστέρων ή προληπτικά. Τα θύματα ενός εγκλήματος είναι κύρια πρόσωπα και φορείς της εγκληματικής πράξης και μπορούν να ερμηνεύσουν πιο καλά ένα έγκλημα και μια πράξη παρενόχλησης, να κατανοήσουν πράγματα όπως τις αιτίες του και να καταγράψουν τις συνέπειες του για αυτούς ή ακόμα και για τους άλλους (οικογένεια, κοινωνία, κτλ).

Γνώμονας για την προετοιμασία και κατάλληλη επεξεργασία του ερωτηματολογίου, μετά την μελέτη της βιβλιογραφίας, ήταν η κατανόηση του προβλήματος της ανάπτυξης του κυβερνοεγκλήματος και της έκθεσης των Ελλήνων πολιτών σε αυτό, εξετάζοντας το μέσα από τις διάφορες μορφές που λαμβάνει και τους διαφορετικούς

τρόπους που χρησιμοποιούνται ώστε να προσεγγίζονται οι Έλληνες χρήστες του διαδικτύου.

Το ερωτηματολόγιο που δημιουργήθηκε, αποτελούνταν από συνολικά 18 ερωτήσεις, εκ των οποίων οι τέσσερεις πρώτες ήταν ερωτήσεις δημογραφικού περιεχομένου για την κατανόηση του προφίλ των χρηστών. Στη συνέχεια, ακολουθούσαν ερωτήσεις διερεύνησης του προβλήματος, με εστίαση στις μορφές που λαμβάνει, τις αιτίες, την συχνότητα και τις συνέπειές του και μετά εξετάστηκε αν οι πολιτικές που ασκούνται κρίνονται ικανοποιητικές και σε ποιο βαθμό.

Οι ερωτήσεις που δημιουργήθηκαν ήταν άλλοτε με κλειστό αριθμό συγκεκριμένων απαντήσεων (κλειστού τύπου) και άλλοτε με την επιλογή να σημειώσει ο ερωτώμενος στην επιλογή «άλλο» κάτι διαφορετικό σε σχέση με τις προσφερόμενες απαντήσεις (ανοικτού τύπου),

Αφού προετοιμάστηκαν οι κατάλληλες ερωτήσεις, χρησιμοποιήθηκε το εργαλείο-πλατφόρμα της GoogleForms για να δημιουργηθεί το ερωτηματολόγιο.

Στη συνέχεια, το ερωτηματολόγιο μοιράστηκε σε περιορισμένο αριθμό χρηστών ώστε να βελτιωθεί η δομή, το περιεχόμενο και η σαφής διατύπωση των ερωτήσεών του. Αυτό επαναλήφθηκε δυο φορές, προκειμένου να εξασφαλισθεί η μέγιστη δυνατή ακρίβεια στις απαντήσεις που θα δίνονταν.

Το ερωτηματολόγιο απευθύνθηκε σε ομάδες πολιτών, διαδικτυακά γκρουπ φοιτητών, τυχαίους χρήστες, εργαζόμενους σε διάφορους κλάδους σε ιδιωτικό και δημόσιο τομέα, συνδικαλιστικά σώματα καθώς και αρκετούς ελεύθερους επαγγελματίες.

Στην αρχή του ερωτηματολογίου τοποθετήθηκε ένα σχετικό ενημερωτικό κείμενο για τον σκοπό της έρευνας που σημείωνε ότι πρόκειται για μεταπτυχιακή εργασία του Πανεπιστημίου Δυτικής Μακεδονίας.

Συνολικά, το ερωτηματολόγιο απαντήθηκε από 300 άτομα, όλα κατά την θερινή περίοδο του 2024. Συγκεκριμένα το δείγμα απαντήθηκε σχεδόν σε ένα 24ωρο, στις αρχές Αυγούστου. Το πολύ σύντομο αυτό χρονικό διάστημα είναι ενδεικτικό του μεγάλου ενδιαφέροντος για το θέμα, όπως διαφαίνεται και από τις απαντήσεις των ερωτώμενων στην ανάλυση που ακολουθεί.

Το μέγεθος του δείγματος (300 απαντήσεις) θεωρήθηκε πολύ μεγάλο ώστε να επιστρέψει την άντληση χρήσιμων συμπερασμάτων σχετικά με τις απαντήσεις που δόθηκαν.

Στο **Παράρτημα Α΄** παρατίθεται το ερωτηματολόγιο όπως ακριβώς χρησιμοποιήθηκε.

Μια από τις κύριες δυσκολίες στην σύνταξη του ερωτηματολογίου ήταν να εξετάσει τον τρόπο μέσω του οποίου θα γίνονταν ο συγκερασμός των απαντήσεων τόσο αυτών που έχουν δεχθεί κυβερνοεπίθεση ή/και έπεσαν θύματα αυτής, όσο και αυτών που δεν έχουν δεχθεί. Στην αρχή εξετάστηκε το ενδεχόμενο να αποκλειστούν όσοι δεν είχαν δεχθεί κάποια παρενόχληση από την συνέχιση του ερωτηματολογίου. Ωστόσο, αυτό κρίθηκε μη σκόπιμο, λόγω του ότι όλοι οι ερωτώμενοι σε ένα τέτοιο ερωτηματολόγιο μπορεί να έχουν διαμορφωμένη άποψη για θέματα όπως τις πολιτικές που υιοθετούνται από το κράτος, αξιολογώντας τον ρόλο, την ευθύνη και την συγκεκριμένη λειτουργία της Δημόσιας Διοίκησης ως προς την αντιμετώπιση του ζητήματος, ανεξάρτητα αν έχουν υποστεί οι ίδιοι μια παρενόχληση.

Προτιμήθηκε το ερωτηματολόγιο να μην στερεί τη δυνατότητα απάντησης από τη δεύτερη κατηγορία ερωτώμενων (όσων δεν έχουν υποστεί οι ίδιοι παρενόχληση), αναδεικνύοντας ταυτόχρονα και το ποσοστό του δείγματος που έχει υποστεί το πρόβλημα του κυβερνοεγκλήματος στην Ελλάδα. Αυτή είναι μια κύρια διαφορά της έρευνας αυτής, σε σχέση με την έρευνα των Vlachos κ.α. (2011). Έγινε επίσης κατανοητό, ότι οι πολλαπλές απαντήσεις δεν ενοχλούν στην απεικόνιση του προβλήματος και των διάφορων εξεταζόμενων πτυχών του, αλλά μπορούν μάλιστα να αναδείξουν μια ποικιλομορφία σχετικών απαντήσεων, που να βοηθήσει την καλύτερη διερεύνηση και μελέτη του.

Δεν μπορεί να απαντηθεί το ερώτημα αν και κατά πόσο οι περισσότεροι ερωτώμενοι που απάντησαν το ερωτηματολόγιο επέλεξαν να το κάνουν επειδή ήταν ήδη θύματα. Σίγουρα αναμένεται, να επιδιώκεται από τα ίδια τα θύματα να δώσουν απάντηση -και άμεσα- σε ένα ερωτηματολόγιο που απευθύνεται σε θύματα ενός εγκλήματος. Εφόσον έχουν πέσει θύματα και πιστεύουν ότι γνωρίζουν τις απαντήσεις (ενώ παράλληλα συντρέχει και το στοιχείο της ανωνυμίας μιας πανεπιστημιακής έρευνας) θα θεωρούν ότι θα μπορέσουν να απαντήσουν ή ακόμα και ότι πρέπει να απαντήσουν, γιατί έτσι μπορεί να συμβάλλουν και στην επίλυση του προβλήματος.

Για να γίνει όμως πιο σαφές τι θεωρούν τα ίδια τα θύματα, οι απαντήσεις που δόθηκαν για ορισμένες ειδικά ερωτήσεις, αναλύθηκαν αφαιρώντας προηγουμένως τις απαντήσεις όσων δήλωναν ότι δεν έχουν πέσει ήδη θύμα κάποιας μορφής παρενόχλησης μέσω διαδικτύου και εξετάζοντας μόνο τις υπόλοιπες απαντήσεις.

Για την καλύτερη και πιο ενημερωμένη απάντηση των ερωτήσεων ακολουθήθηκε η εξής στρατηγική. Παρουσιάστηκε σιγά-σιγά το φαινόμενο, μέσα από τις πολλές πτυχές που έχει και τις απαντήσεις που δόθηκαν για τις ερωτήσεις που το

διερευνούσαν (ως προς τις αιτίες, τη συχνότητα, τις δυσκολίες αντιμετώπισης κτλ) ώστε σιγά – σιγά οι ερωτώμενοι να αντιληφθούν τις διαστάσεις (ή να τις φέρουν απλώς στη μνήμη τους) και έτσι να απαντήσουν με μεγαλύτερη πληρότητα και επάρκεια τις ερωτήσεις που αφορούσαν τον ρόλο της Δημόσιας Διοίκησης και την προστασία των πολιτών από τις παρενοχλήσεις. Για το λόγο αυτό, εξάλλου, δεν τέθηκε το ερώτημα για το αν απευθύνθηκαν οι ίδιοι στην Αστυνομία για την αντιμετώπιση της παρενόχλησης που υπέστησαν μαζί με τα ερωτήματα για τον ρόλο της Αστυνομίας, τον πραγματικό και τον δυνητικό.

Στα ερωτήματα για τη Δημόσια Διοίκηση και την Αστυνομία ρωτήθηκαν οι ερωτώμενοι όχι μόνο για τον πραγματικό ρόλο που έχουν και καταφέρνουν να επιτύχουν οι αρχές αλλά και για τον δυνητικό τους ρόλο.

Η εγκυρότητα του δείγματος, συνδέεται με την αντιπροσώπευση του πληθυσμού, αλλά επίσης και με την δυνατότητα διερεύνησης και καλύτερης περιγραφής του προβλήματος του κυβερνοεγκλήματος, το οποίο για παράδειγμα μπορεί να αφορά περισσότερο την Ελληνική περιφέρεια. Επειδή στο δείγμα εκπροσωπείται ολόκληρη η Ελλάδα, υπάρχει ένα βασικό στοιχείο εγκυρότητας. Όμως, αν και η μεγάλη εκπροσώπηση της περιφέρειας Ηπείρου και της Μακεδονίας σε σχέση με την Αττική θα μπορούσε να θεωρεί ότι θέτει ζήτημα εγκυρότητας και τα ευρήματα της έρευνας αυτής να ήταν διαφορετικά για το σύνολο της επικράτειας, όπως θα δούμε και στη συνέχεια, η έρευνα φέρνει στο φως τη διάσταση του προβλήματος και στην Ελληνική περιφέρεια. Ως προς την αντιπροσώπευση πολλών και διαφορετικών ομάδων, το δείγμα έχει ληφθεί από πολλές πηγές και το αναμενόμενο είναι να αντιπροσωπεύει τυχαία πολλές ομάδες. Οπωσδήποτε δεν αποτελεί προϊόν απλής τυχαίας δειγματοληψίας, αλλά η δειγματοληψία με τον τρόπο που έγινε ο διαμοιρασμός του ερωτηματολογίου, εν τέλει, μπορεί να θεωρηθεί τυχαία λόγω και της διασποράς του δείγματος.

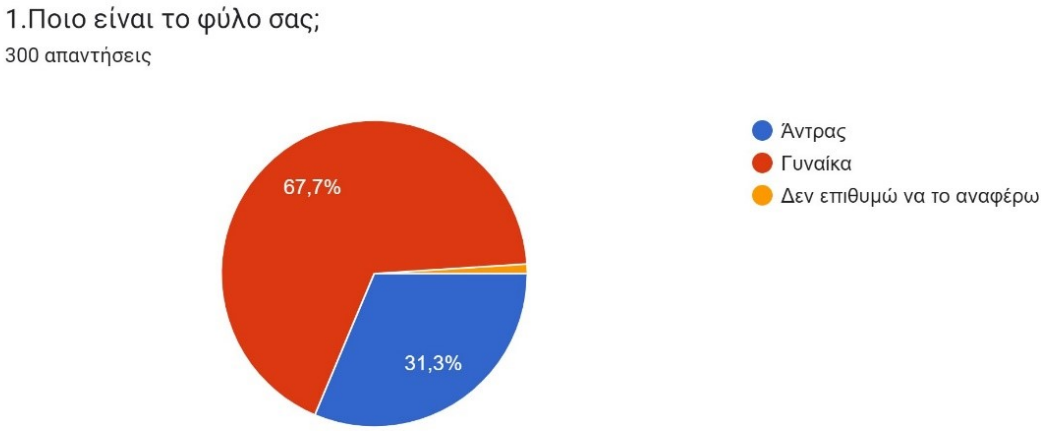
Τέλος, σε ότι αφορά την αξιοπιστία της έρευνας, αυτή συνδέεται με την επιλογή της ποιοτικής μεθόδου για την περιγραφή και ανάλυση ενός σύνθετου προβλήματος για την Ελλάδα (σε αντίθεση με την επιλογή ποσοτικών μεθόδων), τουλάχιστον σε ότι αφορά τον αρχικό της σχεδιασμό. Σε αυτό συντελεί και η προσπάθεια που έγινε για να επιτευχθεί το ταίριασμα των ερωτημάτων της έρευνας με τη θεωρία.

ΚΕΦΑΛΑΙΟ 3ο: ΑΝΑΛΥΣΗ ΑΠΑΝΤΗΣΕΩΝ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

3.1. ΔΗΜΟΓΡΑΦΙΚΑ ΣΤΟΙΧΕΙΑ ΔΕΙΓΜΑΤΟΣ

Οι ερωτηθέντες που απάντησαν το ερωτηματολόγιο ήταν κατά 67,7% γυναίκες και κατά 31,3% άντρες. Δηλαδή η αναλογία γυναικών προς άντρες ήταν 2 προς 1, πράγμα που υποδηλώνει μεγαλύτερο ενδιαφέρον από το γυναικείο κοινό να απαντήσει στις ερωτήσεις, δεδομένου ότι δεν υπήρχε για τους παραλήπτες κάποιο στοιχείο που να υποδήλωνε την μεγαλύτερη εκπροσώπηση του γυναικείου φύλου άλλα μάλλον το αντίθετο ίσχυε.

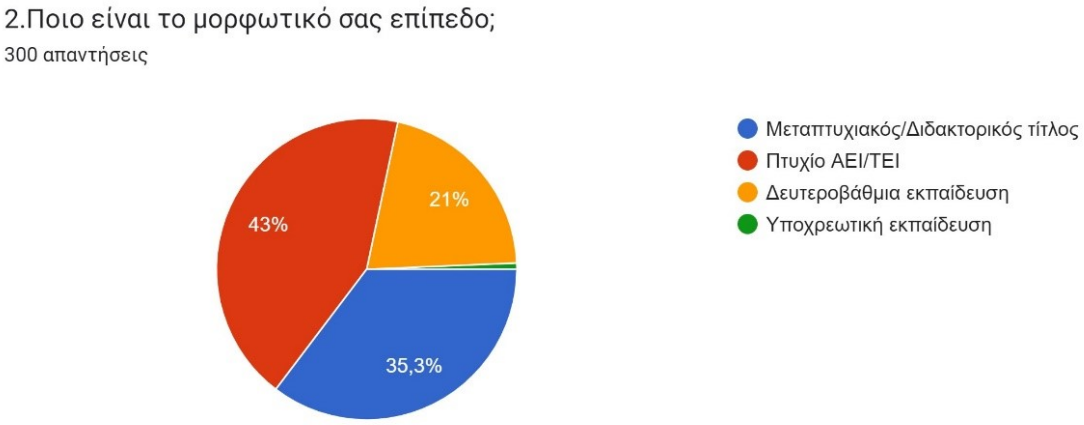
Ερώτηση-Διάγραμμα 1



Το μορφωτικό επίπεδο όσων απάντησαν φαίνεται αρκετά υψηλό. Το 43% δήλωσε ότι διαθέτει πτυχίο ΑΕΙ/ΤΕΙ ενώ περίπου το ένα-τρίτο (ποσοστό 35,3%) έχει μεταπτυχιακό ή διδακτορικό τίτλο. Συνολικά δηλαδή πάνω από τα δύο τρίτα (αθροιστικά 78,3%) διαθέτουν ανώτατη ή ανώτερη εκπαίδευση, σε τριτοβάθμιο επίπεδο. Το επίπεδο αυτό είναι πολύ υψηλό για το δείγμα. Ένα ποσοστό 21% διαθέτει δευτεροβάθμια εκπαίδευση ενώ η υποχρεωτική εκπαίδευση ένα ποσοστό κάτω του 1%. Αυτή η υποεκπροσώπηση της υποχρεωτικής εκπαίδευσης μπορεί να οφείλεται και στην περιορισμένη χρήση του διαδικτύου από άτομα χαμηλότερου μορφωτικού επιπέδου ή στην περιορισμένη συμμετοχή όσων έχουν τελειώσει την υποχρεωτική εκπαίδευση σε έρευνες γενικότερα και σε αντίστοιχες έρευνες ειδικότερα. Η εκπροσώπηση ενός υψηλού μορφωτικού επιπέδου στο δείγμα αρμόζει

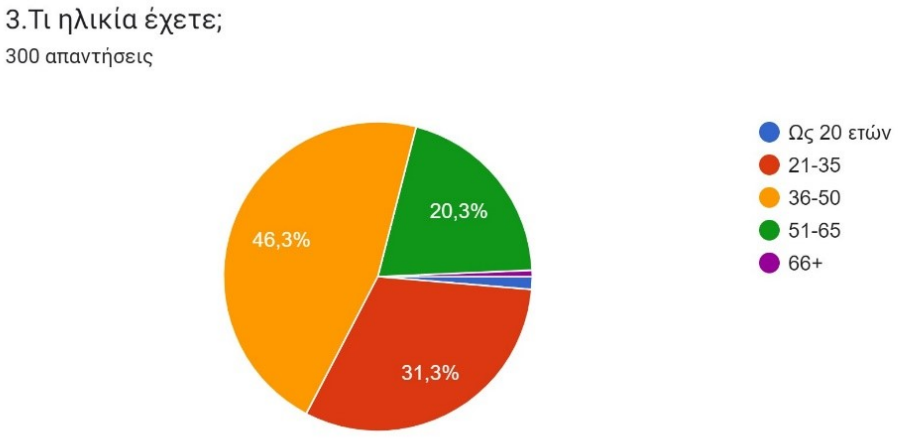
με την εικόνα που παρουσιάζεται στη χώρα μας, όπου το επίπεδο μόρφωσης είναι υψηλό.

Ερώτηση-Διάγραμμα 2



Ηλικιακά το δείγμα κατανέμεται περισσότερο μεταξύ των ηλικιών 20 και 65, δηλαδή σε ηλικίες εργάσιμου βίου (σε ποσοστό σχεδόν 98%). Το μεγαλύτερο του τμήμα είναι ηλικίας μεταξύ 36 και 50 χρονών (46,3%). Σε ηλικίες μεταξύ 21-35 χρονών αντιστοιχεί ποσοστό 31,3%. Δηλαδή πάνω από τα δυο τρίτα (77,6%) είναι μεταξύ 21 και 50 χρονών. Ένα 20,3% προέρχεται από ηλικίες μεταξύ 51 και 65 ετών. Δηλαδή ακριβώς τα δυο τρίτα του δείγματος προέρχονται από ηλικίες μεταξύ 36-65 ετών.

Ερώτηση-Διάγραμμα 3



Το δείγμα προέρχεται από ολόκληρη την Ελλάδα, έτσι όπως παρουσιάζεται στο Διάγραμμα 4. Παρουσιάζει ενδιαφέρον το μεγάλο ποσοστό ερωτώμενων που έχουν μόνιμη κατοικία στην Ήπειρο (31%) ενώ εξίσου υψηλό είναι και το ποσοστό που διαμένουν μόνιμα στην Μακεδονία και Θράκη (24.7%). Η Αττική αντιπροσωπεύεται με μόλις 22,7%, πράγμα που υποδηλώνει ότι το δείγμα αφορά γεωγραφικά την περιφέρεια και ειδικά την παραμεθόρια περιφέρεια της Ελλάδας όχι την Αττική (που συγκεντρώνει από μόνη της το 40% του Ελληνικού πληθυσμού). Αυτό είναι σημαντικό γιατί τα αποτελέσματά αντανακλούν σε όσα συμβαίνουν στην Ελληνική περιφέρεια και όχι αποκλειστικά στο μεγάλο αστικό κέντρο της Αττικής. Δηλαδή σε σχέση με μια άλλη έρευνα, η παρούσα έχει ενδιαφέρον γιατί δείχνει τι συμβαίνει στην Ελληνική περιφέρεια, με έμφαση στην Ήπειρο και την Κεντρική Μακεδονία και Θράκη.

Ερώτηση-Διάγραμμα 4

3.2. ΕΡΩΤΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΣΤΗΝ ΕΛΛΑΔΑ

3.2.1. Συχνότητα και σημασία του προβλήματος έκθεσης στο κυβερνόεγκλημα στην Ελλάδα

Η πρώτη ερώτηση σχετικά με το αν οι ερωτώμενοι έχουν δεχτεί κάποια κακόβουλη «επίθεση» ή άλλη ενέργεια παρενόχλησης που να αντιλήφθηκαν ότι αποσκοπούσε στη θυματοποίησή τους ήταν ερώτηση ανοικτή σε αριθμό απαντήσεων.

Το ένα-τρίτο σχεδόν του δείγματος (ποσοστό 34%) απάντησε ότι δεν έχει δεχτεί κάποια κακόβουλη επίθεση ή άλλη ενέργεια παρενόχλησης. Το ποσοστό αυτό επαναλαμβάνεται και άρα επιβεβαιώνεται και μέσα από επόμενες ερωτήσεις. Συνεπώς οι ερωτήσεις που απαντώνται από άτομα που έχουν δεχτεί ήδη κάποια κακόβουλη επίθεση ή άλλη παρενόχληση μέσω διαδικτύου αφορούν το 66% του δείγματος.

Όπως φαίνεται και στο Διάγραμμα 5 που ακολουθεί, λίγο περισσότερο από το ένα-τρίτο του δείγματος έχει δεχτεί παρενόχληση ή κακόβουλη επίθεση στο e-mail του (37,7%). Αυτό είναι ένα πολύ υψηλό ποσοστό. Δεδομένου ότι, όπως προαναφέρθηκε, το ένα τρίτο του δείγματος δεν έχει καν δεχτεί κάποια κακόβουλη «επίθεση» ή άλλου τύπου παρενόχληση, αποτελεί ένα πολύ υψηλό ποσοστό ανάμεσα σε αυτούς που δέχτηκαν τέτοια «επίθεση» ή παρενόχληση, περίπου τους μισούς. Φαίνεται δηλαδή ότι το e-mail είναι μια «ευάλωτη θύρα» που παραβιάζεται εύκολα η πρόσβαση σε αυτό και χρησιμοποιείται από τους θύτες για τους σκοπούς της εκμετάλλευσης του θύματος.

Είναι επίσης μεγάλο το ποσοστό (31,7%) πως αναφέρουν ένα άλλο κοινωνικό μέσο δικτύωσης που χρησιμοποιεί ως το κύριο μέσο, δια μέσω του οποίου έχουν δεχτεί κυβερνοεπίθεση. Δηλαδή φαίνεται ότι η χρήση των κοινωνικών δικτύων γίνεται αντικείμενο εκμετάλλευσης από επιτήδειους που αναζητούν θύματα εκμετάλλευσης σε ένα αρκετά μεγάλο βαθμό. Τέλος είναι πάλι αρκετά μεγάλο το ποσοστό που αναφέρει ότι έχει δεχτεί τέτοια επίθεση μέσω του τηλεφώνου (28%). Δηλαδή είναι και το τηλέφωνο ένας σημαντικός τρόπος μέσω του οποίου αναζητούνται θύματα.

Μόλις 9% (27 απαντήσεις) αναφέρει ότι έχει δεχτεί «επίθεση» ή παρενόχληση από ιστοσελίδα που διαθέτει ή επισκέφτηκε.

Τέλος, στην επιλογή «άλλο» παρατίθενται και άλλοι λόγοι, όπως μια περίπτωση «επίθεσης» σε πιστωτική κάρτα, δύο περιπτώσεις στο υπηρεσιακό e-mail (ενώ έχουν ήδη απαντήσει στο προσωπικό e-mail), 1 μέσω sms και 2 περιπτώσεις δεν συμπλήρωσαν κάτι άλλο πιο συγκεκριμένο.

Από τα παραπάνω φαίνεται αρχικά ότι πρόκειται για ένα πολύ μεγάλο πρόβλημα της Ελληνικής κοινωνίας και οικονομίας, γιατί αφορά στα δύο της τρίτα και προφανώς και ειδικότερα για την Ελληνική περιφέρεια, αφού, όπως προαναφέρθηκε, το δείγμα έχει αναλογικά μεγάλη εκπροσώπηση από τις περιφέρειες της Ηπείρου και της Μακεδονίας και Θράκης. Επίσης, φαίνεται ότι τα τρία μέσα που αναφέρονται και στη βιβλιογραφία, το e-mail, τα κοινωνικά δίκτυα και το τηλέφωνο, αποτελούν κύρια μέσα

δια μέσω των οποίων αναζητούνται θύματα ενώ σε μικρότερο βαθμό είναι η ύπαρξη ιστοσελίδων. Δηλαδή φαίνεται ότι η θυματοποίηση είναι μια ενεργητική διαδικασία από πλευράς θύτη, με αναζήτηση των θυμάτων και την επιδίωξη για επικοινωνία μαζί τους.

Ερώτηση-Διάγραμμα 5

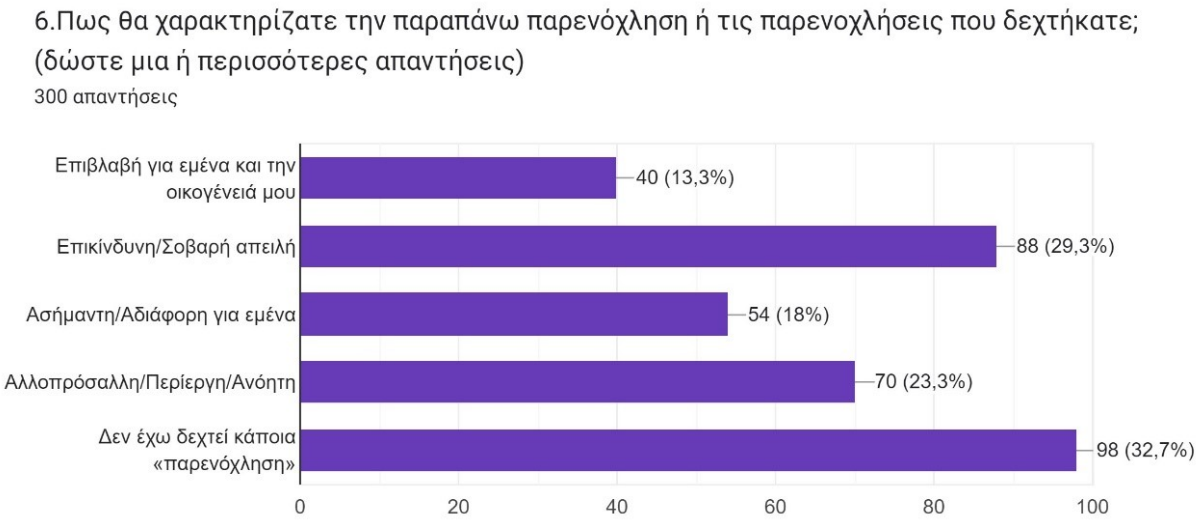
3.2.2. Η σοβαρότητα - επικινδυνότητα των περιπτώσεων κυβερνοεγκλήματος στην Ελλάδα

Παρά το γεγονός ότι η παρενόχληση φαίνεται ιδιαίτερα συχνή, στην ερώτηση πως θα χαρακτηρίζατε την παρενόχληση (ή τις παρενοχλήσεις) που δεχτήκατε, οι ερωτώμενοι απάντησαν κατά 29,3% ως επικίνδυνη ή σοβαρή απειλή και κατά ένα επίσης μεγάλο ποσοστό (23,3%) ως αλλοπρόσαλλη, περίεργη ή/και ανόητη. Μικρότερο ποσοστό τη θεώρησε επιβλαβή για αυτούς και την οικογένειά τους (13,3%) και επίσης ένα 18% απάντησε ότι τους ήταν αδιάφορη και ασήμαντη για αυτούς.

Αν αθροιστούν όμως οι απαντήσεις όσων τη θεώρησαν επικίνδυνη ή σοβαρή απειλή και αυτών που τη θεώρησαν επιβλαβή για αυτούς και την οικογένειά τους το ποσοστό είναι πολύ μεγάλο, 37% (για ορισμένες απαντήσεις έχουν δοθεί και οι δυο απαντήσεις ταυτόχρονα). Αν μάλιστα αφαιρεθούν οι περιπτώσεις όσων απάντησαν ότι δεν έχουν δεχτεί επίθεση και το παραπάνω ποσοστό (για τις δυο αυτές απαντήσεις) υπολογιστεί με βάση το υπόλοιπο ποσοστό, τότε προσεγγίζει το 55%. Αυτά φανερώνουν ότι οι «επιθέσεις» και «παρενοχλήσεις» κρίνονται από τους

χρήστες σοβαρές υποθέσεις, με χαρακτήρα επικίνδυνο και επιβλαβή, σε καμία περίπτωση αμελητέες.

Ερώτηση-Διάγραμμα 6



3.2.3. Η πρόσληψη του κυβερνοεγκλήματος από τα θύματα κατά την περίοδο έκθεσής τους σε αυτό

Εξετάζοντας πως θεώρησαν την παρενόχληση την στιγμή που τη δέχτηκαν, οι μισοί σχεδόν ερωτώμενοι δήλωσαν ότι την απέφυγαν. Αν λάβουμε υπόψη το ένα τρίτο σχεδόν που δήλωσε ότι δεν δέχτηκε παρενόχληση, τότε το παραπάνω ποσοστό αυξάνεται, εξετάζοντας δηλαδή μεμονωμένα μόνο όσους δέχθηκαν παρενόχληση.

Ένα ποσοστό 14,7% δήλωσε ότι την απέφυγε μετά από λίγο και ποσοστό 7,3% ότι δεν αντιλήφθηκε τίποτε αλλά το κατάλαβε εκ των υστέρων. Αντίθετα ήταν μικρός ο αριθμός εκείνων που φαίνεται ότι πείστηκαν. Ένα ποσοστό 2% δήλωσε ότι πείστηκε αλλά δεν το εκμεταλλεύτηκαν ενώ ένα μεγαλύτερο ποσοστό 4% δήλωσε ότι έπεσε θύμα και το εκμεταλλεύτηκαν.

Από την ερώτηση δηλαδή φαίνεται ότι το 6% των ερωτώμενων πείστηκε από μια παρενόχληση και το ποσοστό όσων πείστηκαν τελικά και τους εκμεταλλεύτηκαν φαίνεται εκ πρώτης όψεως να είναι μικρό. Αθροιστικά όμως σε όσους έχουν δεχτεί κάποια παρενόχληση φαίνεται ότι ένα ποσοστό 10% έχει πειστεί και αυτό δεν είναι καθόλου μικρό. Αντίθετα πρόκειται για ένα αρκετά υψηλό ποσοστό.

Ερώτηση-Διάγραμμα 7

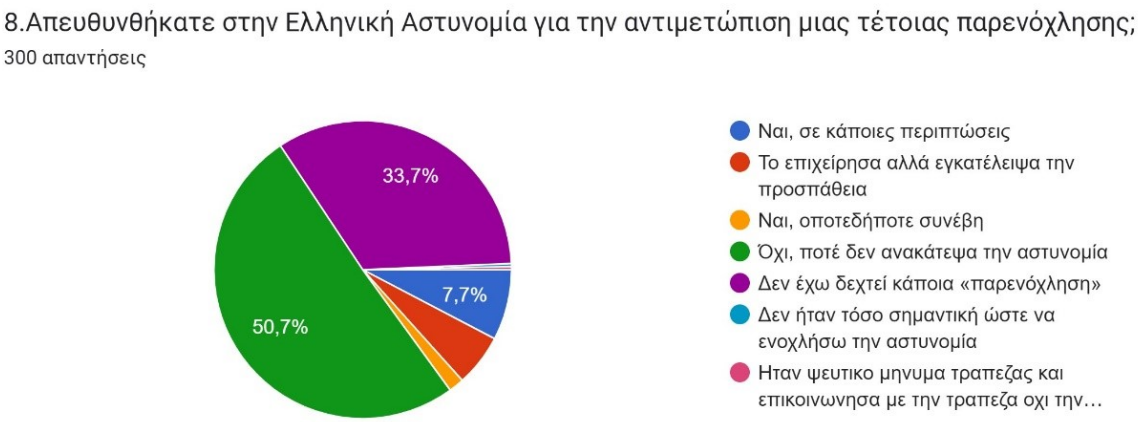
3.2.4. Σχετικά με την εμπλοκή των αστυνομικών αρχών από τα θύματα

Ως προς την εμπλοκή της αστυνομίας, σε ποσοστό 50,7% οι ερωτώμενοι απάντησαν ότι δεν ανακάτεψαν ποτέ στην αστυνομία. Αυτό είναι μεγάλο ποσοστό, δεδομένων των απαντήσεων στην ερώτηση 6 που έδειχναν ότι πρόκειται για περιπτώσεις σοβαρές, με χαρακτήρα επικίνδυνο.

Μόλις 7,7% δήλωσαν ότι το έκαναν σε κάποιες περιπτώσεις, ποσοστό που γίνεται λίγο υψηλότερο του 10,5% όταν δεν λαμβάνονται υπόψη όσοι δεν υπέστησαν καμία παρενόχληση, δηλαδή λίγοι περισσότεροι από ένας στους δέκα.

Αν συγκριθεί το ποσοστό αυτό με την απάντηση στην ερώτηση 6 όπου ένα 60% (δηλαδή έξι στους δέκα) θεώρησαν ότι πρόκειται για σοβαρή απειλή, τότε προκύπτει ότι η εμπλοκή των αστυνομικών αρχών δεν αντιστοιχεί με την σοβαρότητα των περιπτώσεων παρενόχλησης και κυβερνοεγκλήματος.

Ερώτηση-Διάγραμμα 8



3.2.5. Κατηγορίες και τρόποι εξαπάτησης του κυβερνοεγκλήματος

Σε ότι αφορά την κρίσιμη ερώτηση τι ακριβώς σας συνέβη, οι απαντήσεις είναι διασκορπισμένες ανάμεσα σε περισσότερες διαθέσιμες επιλογές.

Στην ερώτηση αυτή φαίνεται ότι το ποσοστό όσων δήλωσαν ότι δεν έχουν δεχτεί κάποια παρενόχληση ελαττώνεται σε 25%, δηλαδή μόλις σε 75 από 100.Αυτό μπορεί να οφείλεται στην μεγαλύτερη διερεύνηση του προβλήματος που γίνεται μέσα από τη μεγάλη (προτεινόμενη) γκάμα των απαντήσεων. Αιτιολογώντας την διαφορά αυτή σε σχέση με πριν, αξίζει να θυμηθούμε τα αποτελέσματα της έρευνας των Kulibay κ.ά. (2023) για την Κένυα (που αναφέρονται στο κεφάλαιο 1) και οι οποίοι διαπίστωσαν ότι ένα ποσοστό 74% ταυτοποιεί σωστά ένα μήνυμα παρενόχλησης και ένα ποσοστό 66% ένα μήνυμα που δεν περιλαμβάνει παρενόχληση. Δηλαδή ότι η ικανότητα ταυτοποίησης μιας παρενόχλησης διαφέρει από άτομο σε άτομο.

Πρακτικά το παραπάνω ποσοστό σημαίνει ότι ένα ποσοστό περίπου 5% στο σύνολο των ερωτηθέντων διαπιστώνει -κατά τη διάρκεια του ερωτηματολογίου- ότι έχει δεχτεί κάποιας μορφής παρενόχληση και διαλέγει κάποια από τις αναφερόμενες στην ερώτηση.

Συνολικά δόθηκαν 607 απαντήσεις (σε σύνολο 300 ερωτώμενων), πράγμα που δηλώνει ότι κατά μέσο όρο δόθηκαν 2 απαντήσεις. Αν αφαιρεθούν οι 75 απαντήσεις (που αντιστοιχούσαν στο ποσοστό 25%), τότε κατά μέσο όρο δίνονται 2,36 κατηγορίες παρενόχλησης. Το υψηλό αυτό νούμερο υποδηλώνει ότι κάθε χρήστης έχει δεχτεί πάνω από δυο παρενοχλήσεις (κατά μέσο όρο) και άρα προφανώς πρόκειται για ένα φαινόμενο σε μεγάλη έκταση.

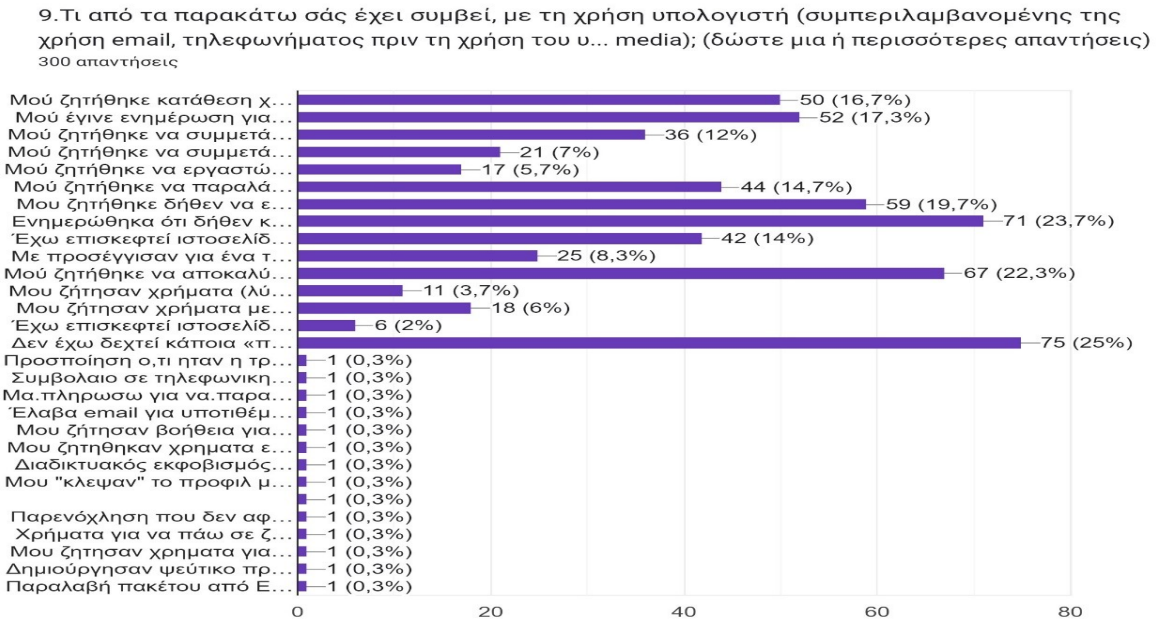
Από την ανάλυση των αποτελεσμάτων φαίνεται ότι ένα ποσοστό 23,7% έτυχε θύμα παρενόχλησης σε σχέση με λαχνούς και λαχεία (απάντησε «Ενημερώθηκα ότι δήθεν κέρδισα κάποιον λαχνό ή λαχείο και θα χρειαστεί να παραλάβω τα χρήματα που κέρδισα»), ποσοστό που μετατρέπεται σε 31,7%, δηλαδή προσεγγίζει το ένα-τρίτο του δείγματος. Γίνεται δηλαδή μεγάλη προσπάθεια εκμετάλλευσης των τυχερών παιχνιδιών και της ανταπόκρισης του κόσμου σε αυτά.

Επίσης σημαντικό είναι το ποσοστό 22,3% (67 απαντήσεις συνολικά) σε βάρος του οποίου έγινε προσπάθεια «ψαρέματος» (phishing), δηλαδή του ζητήθηκε να αποκαλύψει τα προσωπικά του δεδομένα και πληροφορίες που το αφορούν. Το ποσοστό αυτό αυξάνει σε σχεδόν 30% (29,8%) όταν δεν εξετάζονται όσοι δήλωσαν δεν έχουν δεχτεί κάποια παρενόχληση.

Σχεδόν στο ένα-πέμπτο του δείγματος (19,7%) ζητήθηκε δήθεν να επιστρέψει χρήματα, να καταβάλει φόρο, να διευθετήσει χρηματικά υπόλοιπα σε σχέση με δημόσια υπηρεσία (ΑΑΔΕ ή άλλη), το οποίο μετατρέπεται σε άνω του ενός-τετάρτου (26,1%) όταν αφαιρούνται οι περιπτώσεις όσων δεν υπέστησαν παρενόχληση.

Αυξημένη πολύ είναι η συχνότητα σε άλλες τρεις τουλάχιστον επιλογές απαντήσεων που είχαν δοθεί. Μετατρεπόμενες σε ποσοστά χωρίς όσους δεν δέχτηκαν παρενόχληση, οι απαντήσεις αυτές προσεγγίζουν ή ξεπερνούν το ένα-πέμπτο του δείγματος. Πιο συγκεκριμένα απαντήθηκε ότι «Μού έγινε ενημέρωση για την απόκτηση εύκολων χρημάτων λειτουργώντας ως διαμεσολαβητής για κάποιον άλλο» σε ποσοστό 23,1%, ότι «Μού ζητήθηκε κατάθεση χρημάτων σε λογαριασμό στο εξωτερικό, με χρηματικό αντάλλαγμα» σε ποσοστό 22,2% και ότι «Μού ζητήθηκε να παραλάβω κληρονομιά που δήθεν κληρονόμησα» σε ποσοστό 19,6%.

Ερώτηση-Διάγραμμα9Α



Στην απάντηση «άλλο» δόθηκαν όλες οι παρακάτω διαφορετικές περιπτώσεις απαντήσεων (όλες από μια απάντηση). Ορισμένες βέβαια από αυτές θα μπορούσαν να ενταχθούν στις παραπάνω κατηγορίες. Πάντως οι διαφορετικές απαντήσεις που δίνονται στην κατηγορία «άλλο» είναι συνολικά 14 και αθροιζόμενες στις ήδη 14 που εξετάστηκαν μέσα από το ερωτηματολόγιο γιατί αναγράφονταν στη βιβλιογραφία δίνουν συνολικά 28 διαφορετικές απαντήσεις. Δηλαδή ο τρόπος εξαπάτησης φαίνεται να είναι πράγματι μια σύγχρονη Λερναία Ύδρα, με πολλά κεφάλια.

Αν λάβουμε υπόψη ότι ορισμένες απαντήσεις στην ερώτηση αυτή εμπεριείχαν πάνω από μια διαφορετική περίπτωση εξαπάτησης, τότε συνολικά υπολογίζονται τουλάχιστον 30 διαφορετικοί τρόποι που χρησιμοποιούνται για την εξαπάτηση. Αν μάλιστα συμπληρωθεί σε αυτές ότι υπάρχουν πολλοί και διαφορετικοί τρόποι με τους οποίους προκαλείται κάθε διαφορετική κατηγορία εξαπάτησης από αυτές που παρουσιάζονται στις απαντήσεις της ερώτησης (ως γενικές κατηγορίες), τότε ο παραπάνω αριθμός δείχνει την ύπαρξη ενός έκρυθμου φαινομένου για την Ελληνική κοινωνία, με έμφαση -όπως προαναφέρθηκε- στην Ελληνική περιφέρεια.

Σε αυτό όπως και σε άλλα ερωτηματολόγια φαίνεται ότι παρουσιάζεται μια τάση σε ορισμένους από τους ερωτώμενους να θέλουν να δώσουν και απαντήσεις έξω από τις εξεταζόμενες. Όμως επειδή ακριβώς αυτές οι περιπτώσεις δεν εξετάζονται στην

παρούσα έρευνα, όπως για παράδειγμα η περίπτωση No 12 στον παρακάτω πίνακα («Μου ζήτησαν χρήματα για συγγενή μου που προκάλεσε ατύχημα»), δεν σημαίνει ότι δεν έχουν επίσης μεγάλη εξάπλωση. Το αντίθετο μάλιστα.

Ερώτηση-Διάγραμμα 9Β: Απαντήσεις που δόθηκαν στην απάντηση «άλλο» στην ερώτηση 9

1. Προσποίηση ότι ήταν η τράπεζα και έπρεπε να ελέγξω /επιβεβαιώσω τα στοιχεία μου
2. Συμβόλαιο σε τηλεφωνική εταιρεία
3. Μού έγινε ενημέρωση για την απόκτηση εύκολων χρημάτων λειτουργώντας ως διαμεσολαβητής για κάποιον άλλο
4. Να πληρώσω για να παραλάβω κάποιο δέμα
5. Έλαβα e-mail για υποτιθέμενη παραλαβή από ταχυδρομείο που είχε κάποιο link (Δεν το προχώρησα όμως)
6. Μου ζήτησαν βοήθεια για κάποιο διαγωνισμό και αφού μπλόκαραν το λογαριασμό μου άρχισαν να στέλνουν μηνύματα στις επαφές μου
7. Μου ζητήθηκαν χρήματα ενώ προσποιούνταν φίλη μου μέσω της τράπεζας Πειραιώς με παραλαβή του ποσού από ATM χωρίς χρήση κάρτας.
8. Διαδικτυακός εκφοβισμός με ψεύτικα προφίλ
9. Μου "κλέψαν" το προφίλ μου σε κοινωνικό δίκτυο
10. Παρενόχληση που δεν αφορά όλα τα παραπάνω
11. Χρήματα για να πάω σε ζωολογικό πάρκο δωρεάν. Και καλά διαγωνισμός.
12. Μου ζήτησαν χρήματα για συγγενή μου που προκάλεσε ατύχημα
13. Δημιούργησαν ψεύτικο προφίλ στο Fb με φωτογραφίες μου και έκαναν αιτήματα φιλίας σε φίλους και γνωστούς μου.
14. Παραλαβή πακέτου από ΕΛΤΑ

3.2.6. Πώς παρουσιάζονται ότι είναι οι συχνότερες παρενοχλήσεις;

Η επόμενη ερώτηση αφορούσε το πως παρουσιάζεται η παρενόχληση από τους θύτες. Όπως φάνηκε και στην απάντηση παραπάνω ερώτησης υπάρχουν διάφοροι τύποι παρενόχλησης και μερικές από αυτές είναι συχνότερες. Οι περισσότερες παρενοχλήσεις γίνονται με σκοπό την οικονομική εκμετάλλευση και την άντληση

χρημάτων από τα θύματα. Ωστόσο πέραν αυτής της συχνής περίπτωσης, υπάρχουν και άλλες παρενοχλήσεις που παρουσιάζονται με διάφορους τρόπους.

Στην ερώτηση τι τύπου παρουσιάζονταν ότι ήταν οι συχνότερες παρενοχλήσεις που δέχτηκαν, οι ερωτώμενοι, εκτός ενός ποσοστού 30% που δεν έχει δεχτεί κάποια παρενόχληση, απάντησαν ότι σε ποσοστό επίσης 30% παρουσιάζονταν ότι ήταν σχετικές με την προστασία της ασφάλειας, της προσωπικής ζωής και ιδιωτικότητας. Αυτό το υψηλό ποσοστό καθιστά σαφές ότι σε μεγάλο αριθμό περιπτώσεων επειδή ακριβώς εγείρεται θέμα ασφάλειας και προστασίας της ιδιωτικής ζωής μέσω της λειτουργίας του διαδικτύου ή άλλων μορφών παράνομης δραστηριότητας, οι εγκληματίες που βρίσκονται πίσω από τις επιθέσεις μέσω του διαδικτύου επιχειρούν να το εκμεταλλευτούν αυτό γιατί το γνωρίζουν. Δηλαδή ο θύτης εκμεταλλεύεται την ανησυχία του θύματος.

Ένα ποσοστό 11% δήλωσε ότι συχνότερες παρενοχλήσεις παρουσιάζονταν ότι ήταν σχετικές με υποτιθέμενη παράνομη δραστηριότητα του θύματος. Σε αυτή την περίπτωση επιδιώκεται η μομφή και κατηγορία του ίδιου του θύματος και η πιθανή ενοχοποίησή του. Αθροιστικά με το παραπάνω ποσοστό και εφόσον αφαιρεθούν οι 13 κοινές απαντήσεις, σε ένα μεγάλο ποσοστό που ξεπερνάει το ένα-τρίτο(36,6%) φαίνεται να έχουν παρουσιαστεί ζητήματα κυβερνοεπίθεσης και παρενόχλησης που συνδέεται με κάποιο τρόπο με την ασφάλεια και την προστασία τους.

Αν μάλιστα γίνει η μετατροπή του ποσοστού αυτού σε ποσοστό δίχως τις περιπτώσεις όσων δεν δέχτηκαν κάποια επίθεση, τότε το αναγόμενο ποσοστό είναι 52,4%. Δηλαδή πάνω από μια στις δυο περιπτώσεις δήλωσαν ότι για ένα θέμα που είναι για αυτούς ζήτημα ασφάλειας, οι θύτες το παρουσιάζουν σε μεγάλο βαθμό να συνδέεται με την ίδια τους την ασφάλεια και την προστασία της ασφάλειας τους.

Πρόκειται δηλαδή για μια προσπάθεια συγκάλυψης της ίδιας της φύσης της εξαπάτησης που από μόνη της εγείρει ζήτημα ασφάλειας, ιδιωτικότητας και νομιμότητας.

Σε ότι αφορά τις υπόλοιπες απαντήσεις, ένα ποσοστό 11,7% απάντησε ότι ήταν σχετικές με τον ερωτικό τομέα. Αναγόμενο στο δείγμα των 210 που απάντησαν ότι επιχειρήθηκε να εξαπατηθούν, το 16,7% απάντησε σχετικά με τον ερωτικό τομέα. Δηλαδή περίπου μια στις εφτά περιπτώσεις παρενόχλησης που δεν παρουσιάστηκαν ότι είναι οικονομικού ενδιαφέροντος για τον χρήστη-θύμα ήταν ερωτικού ενδιαφέροντος. Αυτό δείχνει ότι υπάρχει σημαντική εξαπάτηση σε αυτόν τον τομέα επίσης, όπου αναζητείται ένα σημείο τρωτότητας του θύματος.

Ένα ποσοστό 6% των περιπτώσεων απάντησε ότι ήταν σχετικές με κοινωνικές εκδηλώσεις (π.χ. εθελοντισμού) και τον κοινωνικό περίγυρο των ερωτώμενων ένα μικρότερο ποσοστό, 2,7%, των περιπτώσεων απάντησε ότι είναι σχετικές με τη θρησκεία.

Υπάρχει τέλος και ένα αξιοσημείωτο ποσοστό, 25%, που απάντησε ότι οι συχνότερες παρενοχλήσεις που έχει δεχτεί δεν ανήκαν σε κάποια από τις παρατιθέμενες από την ερώτηση κατηγορίες απαντήσεων.

Ερώτηση-Διάγραμμα 10

3.2.7. Συνέπειες των παρενοχλήσεων και του κυβερνοεγκλήματος

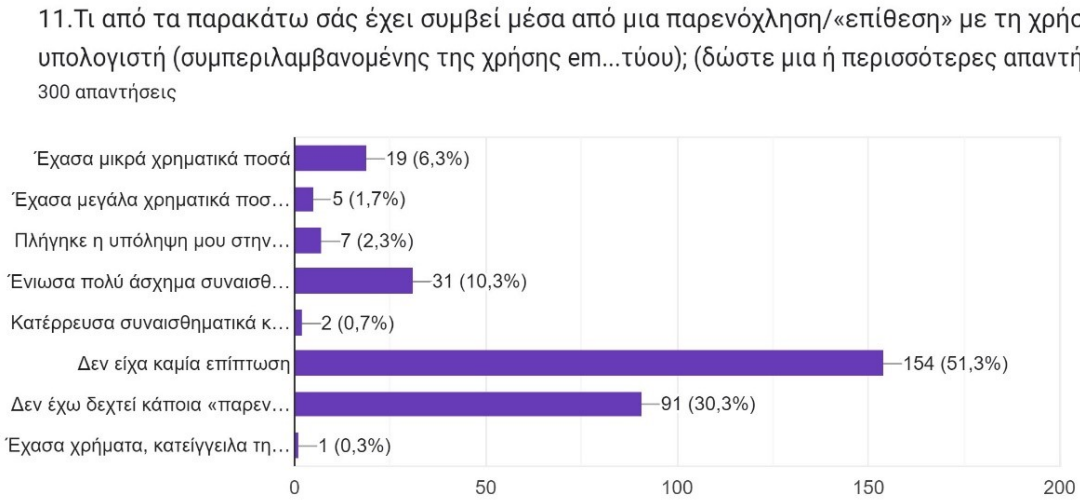
Η επόμενη ερώτηση διερευνούσε τις συνέπειες που είχε για τα θύματα η παρενόχληση που τους είχε συμβεί και το ή τα κυβερνοεγκλήματα με τα οποία ήρθαν αντιμέτωποι.

Πέραν του ποσοστού όσων δεν υπέστησαν παρενόχληση (30,3%), 154 ερωτώμενοι, δηλαδή ένα ποσοστό στο δείγμα που ξεπερνάει τον έναν στους δυο (51,3%) δηλώνει ότι δεν είχε καμία συνέπεια από την παρενόχληση που δέχτηκε. Προφανώς πρόκειται για τις περιπτώσεις των απαντήσεων στην ερώτηση 7 «την απέφυγα αμέσως» που απάντησαν 142 άτομα ή «την απέφυγα μετά από λίγο» που απάντησαν 44 άτομα.

Αν αθροιστούν τα ποσοστά όσων δεν υπέστησαν παρενόχληση και όσων δεν είχαν συνέπειες φαίνεται ότι το φαινόμενο αγγίζει το 81,6% των ερωτώμενων συμπολιτών μας, ποσοστό ιδιαίτερα υψηλό. Αν αφαιρεθεί το ποσοστό όσων δεν υπέστησαν

παρενόχληση, τότε το ποσοστό όσων δεν είχαν καμία συνέπεια αγγίζει το 73,7% ανάμεσα σε όσους δέχθηκαν παρενόχληση στο δείγμα δεν υπέστησαν καμία συνέπεια, ποσοστό ιδιαίτερα υψηλό.

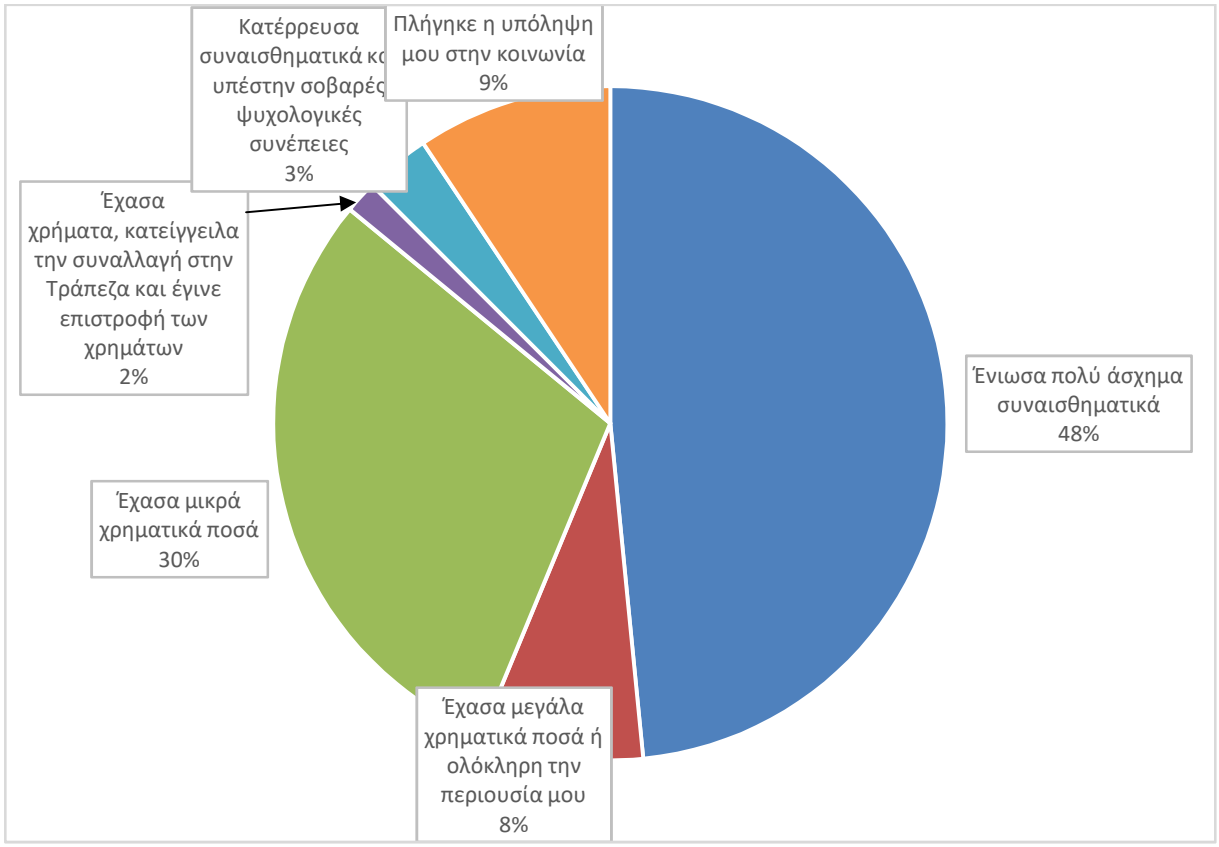
Ερώτηση-Διάγραμμα 11Α



Οφείλουμε να υπενθυμίσουμε το υψηλό μορφωτικό επίπεδο του δείγματος (σε ποσοστό 78,3%) που προφανώς επηρεάζει και την απάντηση αυτή, γιατί οι πιο μορφωμένοι τείνουν να πέφτουν λιγότερο θύματα μιας μορφής εξαπάτησης και αμφισβητούν περισσότερο.

Μολονότι ένα μεγάλο τμήμα του δείγματος δεν υπέστη κάποια συνέπεια, το υπόλοιπο δείγμα που αθροιστικά ανέρχεται στο 18,6% υπέστηκε σοβαρές συνέπειες. Ανακατανέμοντας τα ποσοστά όσων υπέστησαν τις συνέπειες αυτές και αθροίζοντας ανά κατηγορία συνέπειας για το θύμα (μην υπολογίζοντας όμως το ποσοστό για όσους δήλωσαν «Δεν είχα καμία επίδραση» ή «Δεν έχω δεχτεί κάποια παρενόχληση») δημιουργείται το παρακάτω διάγραμμα-πίττα, από το οποίο μαθαίνουμε τα εξής σχετικά με το δείγμα μας.

Ερώτηση-Διάγραμμα 11Β



Τα μισά σχεδόν από τα θύματα ένιωσαν άσχημα συναισθηματικά (48%). Αυτό το πολύ μεγάλο ποσοστό είναι δηλωτικό των ψυχικών συνεπειών που προκαλεί η θυματοποίηση από το κυβερνοέγκλημα και την παρενόχληση. Επίσης, ένα 3% δηλώνει ότι κατέρρευσε συναισθηματικά και υπέστη σοβαρές ψυχολογικές συνέπειες. Αθροιζόμενα τα ποσοστά αυτά φανερώνουν ότι πλέον των μισών θυμάτων υφίστανται ψυχολογικές συνέπειες.

Σε ένα μεγάλο ποσοστό (30%) τα θύματα έχασαν μικρά χρηματικά ποσά αλλά επίσης ένα 8% έχασε μεγάλα χρηματικά ποσά ή ολόκληρη την περιουσία του. Ακόμα ένα ποσοστό 2% (1 άτομο) έχασε χρήματα αλλά κατήγγειλε τη συναλλαγή και έγινε επιστροφή των χρημάτων του από την Τράπεζα. Δηλαδή συνολικά το 40% των θυμάτων έχασε χρηματικά ποσά. Αυτό φανερώνει την κύρια στόχευση των δραστών που είναι η απόσπαση χρηματικών ποσών και η οικονομική εκμετάλλευση.

Τέλος, υπάρχει και ένα ποσοστό 9% που δηλώνει ότι πλήγηκε η υπόληψή του επειδή έπεσε θύμα αυτής της εξαπάτησης μέσω του διαδικτύου και του κυβερνοεγκλήματος.

3.2.8. Τρόποι προσέγγισης θυμάτων και υποψηφίων θυμάτων

Στην ερώτηση με ποιον τρόπο επιχείρησαν να σας παρενοχλήσουν, πέραν από όσους δήλωσαν ότι δεν έχουν δεχτεί κάποια παρενόχληση, απαντώνται οι ακόλουθοι τρόποι. Σε ένα ποσοστό 20,3% υποσχέθηκαν στα θύματα χρήματα, ανταμοιβές ή εύκολο πλουτισμό.

Σε ποσοστό 12,3% απάντησαν τόσο ότι οι θύτες παρουσίασαν τους εαυτούς τους (ή άλλα πρόσωπα) ως επιτυχημένους χάρις την χρήση της υπηρεσίας ή της εργασίας που επιδίωκαν να προσφέρουν όσο και ότι προσπάθησαν να αποκρύψουν κρίσιμες πληροφορίες, να "ζαλίσουν" σκοπίμως τα θύματά τους με βροχή πληροφοριών ή να χρησιμοποιήσουν παραπλανητικές πληροφορίες. Σε ένα ποσοστό 10,3% προσποιήθηκαν συγγενικό, φιλικό ή άλλο πρόσωπο, σε ποσοστό 5,7% προσπάθησαν να πείσουν τα θύματα ότι τελικά εκείνα θα τους εκμεταλλεύονταν αν προέβαιναν στην προτεινόμενη συναλλαγή ενώ σε ένα ποσοστό 8% επιδίωξαν να δημιουργήσουν φιλική σχέση και επικοινωνία με τα θύματά τους ενώ τέλος υποσχέθηκαν επιτυχία στην εύρεση ερωτικού συντρόφου σε ποσοστό μόλις 0,7%.

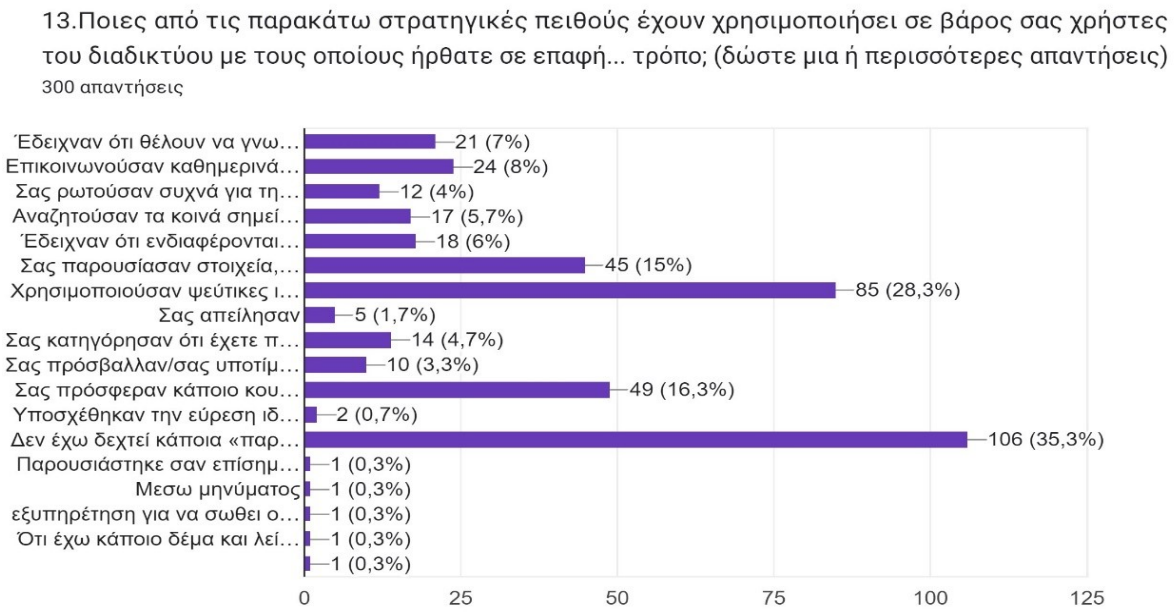
Από τα παραπάνω ποσοστά συμπεραίνουμε ότι χρησιμοποιούνται διαφορετικές τεχνικές και τρόποι προσέγγισης των υποψήφιων θυμάτων και των θυμάτων και ότι τελικά κανένα από αυτά δεν ξεπερνάει το 20,3%. Υπάρχει ωστόσο και ένα ποσοστό 25% που δηλώνει ότι δεν χρησιμοποιήθηκε καμία από τις παραπάνω περιπτώσεις προσέγγισης, χωρίς ωστόσο να καθίσταται δυνατό να προσδιοριστεί ποια άλλη προσέγγιση χρησιμοποιήθηκε, γιατί η δομή του ερωτηματολογίου ήταν τέτοια που δεν δόθηκε η δυνατότητα να προσδιοριστεί ποια άλλη προσέγγιση χρησιμοποιήθηκε πέραν των ήδη εντοπισμένων στην ακαδημαϊκή βιβλιογραφία που μελετήθηκε.

Ερώτηση-Διάγραμμα 12

3.2.9. Στρατηγικές πειθούς των θυτών έναντι των θυμάτων

Σε ότι αφορά τις στρατηγικές πειθούς που χρησιμοποιήθηκαν από τους θύτες, πέραν του 35,3% που απάντησε ότι δεν έχει δεχτεί κάποια παρενόχληση, φαίνεται διαδεδομένη η στρατηγική να δημιουργούν αληθοφανείς ιστοσελίδες που είναι όμως ψεύτικες (σε ποσοστό 28,3%) ενώ σε ένα ποσοστό 16,3% οι θύτες πρόσφεραν στα θύματα κάποιο κουπόνι ή άλλο δώρο. Οι θύτες προσπαθούν επίσης σε ένα μεγάλο ποσοστό (15%) να χτίσουν μια εικόνα αξιοπιστίας και παρουσίασαν στοιχεία, εικόνες ή άλλα τεκμήρια από τη δράση τους που τις καθιστούσαν αξιόπιστες.

Ερώτηση-Διάγραμμα13



Οι απαντήσεις που δόθηκαν στην επιλογή απάντησης «Άλλο» ήταν οι ακόλουθες τέσσερεις:

1. «Παρουσιάστηκε σαν επίσημο e-mail της κυβέρνησης»,
2. «Μέσω μηνύματος»,
3. «Εξυπηρέτηση για να σωθεί ο συγγενής μου» και
4. «Οτι έχω κάποιο δέμα και λείπουν στοιχεία να πατήσω το link»

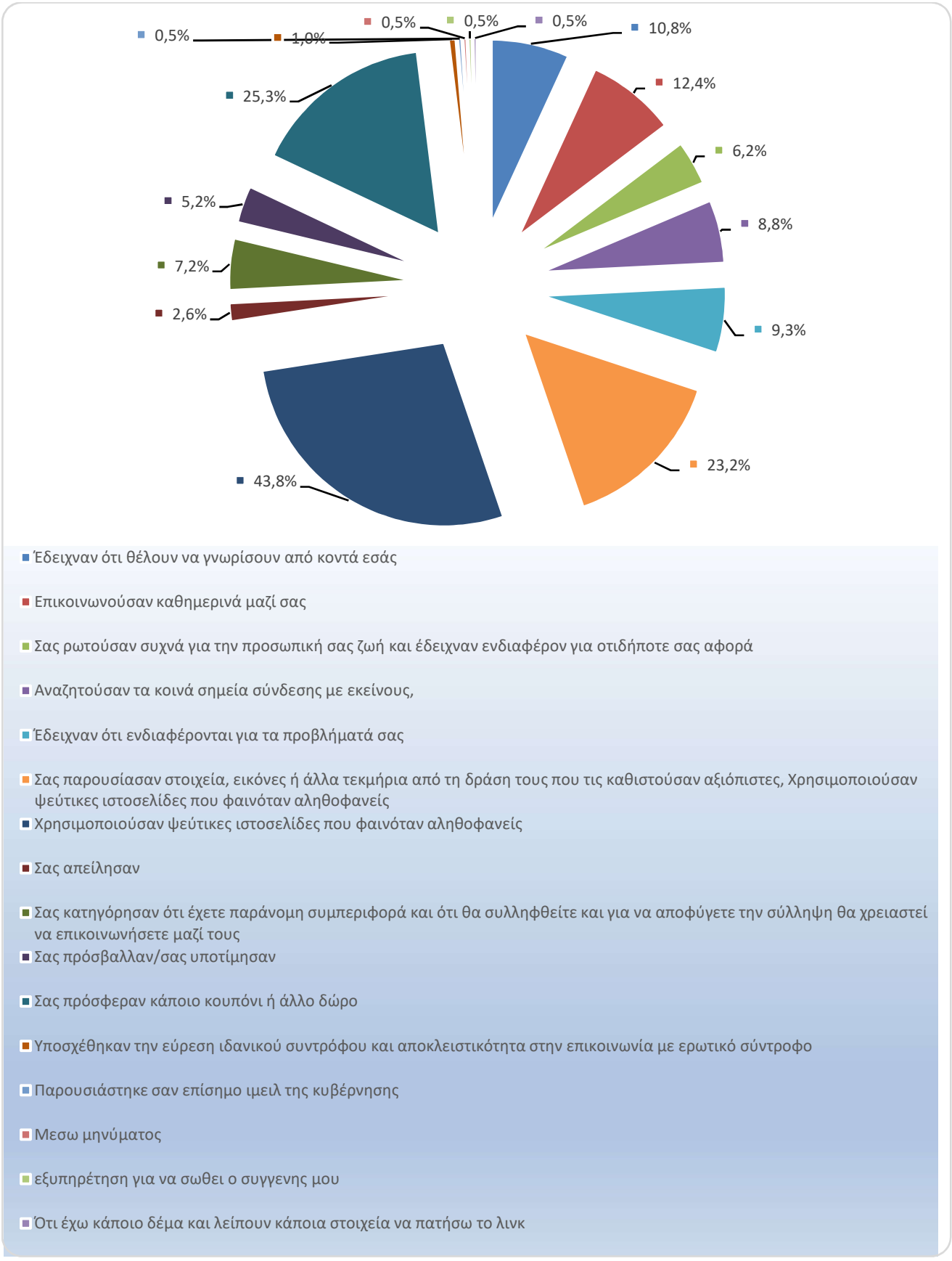
Αφαιρώντας τις περιπτώσεις όσων δεν υπέστησαν κάποια παρενόχληση, παρουσιάζονται τα ποσοστά ανά κατηγορία για όλες τις υπόλοιπες κατηγορίες (συμπεριλαμβανομένου και του «Άλλου»).

Όπως φαίνεται στο παρακάτω διάγραμμα, το ποσοστό χρησιμοποίησης αληθοφανών ιστοσελίδων που ήταν όμως ψεύτικες είναι πολύ υψηλό και προσεγγίζει τις μισές από τις περιπτώσεις θυματοποίησης (43,8%). Δηλαδή πρόκειται για μια πολύ κεντρική στρατηγική που υιοθετείται για το κυβερνοέγκλημα στην Ελλάδα, σύμφωνα με το δείγμα μας.

Επίσης, περίπου στο ένα-τέταρτο των περιπτώσεων που επιχειρήθηκε εξαπάτηση (25,3%) οι θύτες πρόσφεραν στα θύματα κάποιο κουπόνι ή άλλο δώρο. Τέλος, σε ποσοστό λίγο λιγότερο από το ένα-τέταρτο οι θύτες επιχείρησαν να χτίσουν μια εικόνα αξιοπιστίας και παρουσίασαν στοιχεία, εικόνες ή άλλα τεκμήρια από τη δράση τους που τις καθιστούσαν αξιόπιστες. Δηλαδή επιχειρούν να καλύψουν το πρόβλημα της έλλειψης αξιοπιστίας παρουσιάζοντας την εξαπάτηση που επιδιώκουν ως αξιόπιστη.

Άλλα συμπεράσματα σχετικά με τις στρατηγικές είναι ότι οι θύτες σε ποσοστό 12,4% επιδιώκουν την καθημερινή επικοινωνία με τα θύματά τους (σχεδόν σε μια στις εφτά περιπτώσεις που επιχειρήθηκε εξαπάτηση), σε ποσοστό 10,8% έδειχναν ότι θέλουν να γνωρίσουν από κοντά τα θύματα (περίπου 1 στις 10 περιπτώσεις), το 8,8% δηλώνουν ότι αναζητούσαν τα κοινά σημεία σύνδεσης με τα θύματα (περίπου μια στους δώδεκα).

Ερώτηση-Διάγραμμα 13Β



3.2.10. Συχνότητα παρενόχλησης μέσω διαδικτύου

Η συχνότητα της παρενόχλησης είναι επίσης ένα θέμα ουσιαστικό.

Όπως φαίνεται από το διάγραμμα-πίττα που ακολουθεί, το 57,3% του δείγματος έχει δεχτεί σπάνια παρενόχληση από το e-mail, το τηλέφωνο ή μέσω εφαρμογής κοινωνικού δικτύου ενώ το 23% δεν έχει δεχτεί ποτέ παρενόχληση. Συχνά όμως έχει δεχτεί το 17% δηλαδή σχεδόν ένας στους έξι ερωτώμενους. «Πολύ συχνά» απάντησαν 6 (2%) ενώ καθημερινά απάντησαν 2 (0,7%). Αθροιζόμενα τα ποσοστά των τριών τελευταίων περιπτώσεων (συχνά, πολύ συχνά και καθημερινά) δίνουν ένα ποσοστό που προσεγγίζει το 20%, δηλαδή περίπου τον έναν στους πέντε.

Αυτό αποτελεί ένα πολύ ανησυχητικό συμπέρασμα, γιατί δείχνει ότι επιχειρείται η συχνή ή και η πλέον της συχνής προσέγγισης των θυμάτων προκειμένου να επιτευχθεί ο σκοπός της εκμετάλλευσής τους και, προφανώς, κατά τη διάρκεια αυτής της συχνότητας δεν παρεμβάλλεται κάποιος (θεσμικό ή άλλο πρόσωπο) ώστε να διακόψει την επικοινωνία που γίνεται με το σκοπό της εξαπάτησης.

Φαίνεται δηλαδή ότι η συχνότητα της παρενόχλησης εντάσσεται στην στρατηγική των θυτών και ότι δεν συμβαίνει τυχαία αλλά εξυπηρετεί τον σκοπό της εξαπάτησης.

Ερώτηση-Διάγραμμα 14

3.2.11. Αιτίες παρενόχλησης μέσω διαδικτύου όπως κρίνονται από τους ερωτώμενους και τις ανάλογες εμπειρίες τους

Η απάντηση στην ερώτηση γιατί λαμβάνει χώρα η παρενόχληση μέσω διαδικτύου δόθηκε τόσο από εκείνους που υπέστησαν κάποια μορφή παρενόχλησης όσο και από όσους δεν υπέστησαν καμία παρενόχληση. Η δεύτερη κατηγορία δεν επηρεάζει κάπως τα αποτελέσματα της ερώτησης αυτής. Επίσης, όπως και στις προηγούμενες ερωτήσεις, πολλαπλές απαντήσεις μπορούσαν να δοθούν.

Σύμφωνα με τις απαντήσεις που δόθηκαν, το 44,3% (133 απαντήσεις) θεωρεί ότι «αντίθετα με την ανάπτυξη της τεχνολογίας, δεν έχουν αναπτυχθεί τα μέσα προφύλαξης από τέτοιες παρενοχλήσεις», το 43,3% (130 απαντήσεις) θεωρούν ότι «δεν υπάρχει η κατάλληλη εκπαίδευση και γνώση των καταναλωτών για την ασφαλή χρήση του διαδικτύου» και το 41,7% (125 απαντήσεις) θεωρεί ότι «πολλά από τα προσωπικά μας στοιχεία είναι πλέον έκθετα σε πολλούς». Αυτές οι τρεις κατηγορίες, δηλαδή η ανάπτυξη της τεχνολογίας σε αναντιστοιχία με τα μέσα προφύλαξης, η έλλειψη εκπαίδευσης των καταναλωτών για ασφαλή χρήση του διαδικτύου και η υπερ-έκθεση των προσωπικών στοιχείων των καταναλωτών/ χρηστών του διαδικτύου κατατάσσονται ως οι κυριότερες αιτίες για τις παρενοχλήσεις στο διαδίκτυο από τους ερωτώμενους.

Αν και η πρώτη αιτία είναι και θέμα λειτουργίας του ιδιωτικού τομέα και του κλάδου της πληροφορικής, εντούτοις και οι τρεις αυτές αιτίες είναι ζήτημα ασφάλειας των πολιτών και άρα άπτονται των θεμάτων δημόσιας ασφάλειας. Δηλαδή οι ερωτώμενοι συγκλίνουν στην άποψη ότι υπάρχει ένα σοβαρό ζήτημα ασφάλειας και προστασίας της ιδιωτικής ζωής, το οποίο μάλιστα προέρχεται από την πλευρά της πρόληψης.

Παράλληλα με το μεγάλο ποσοστό όσων απάντησαν ότι δεν έχουν αναπτυχθεί τα μέσα προφύλαξης, ένα μεγάλο ποσοστό, το 33, 7% (101 απαντήσεις) δηλώνουν ότι «έχει αναπτυχθεί πολύ η τεχνολογία κατά τα τελευταία χρόνια». Δηλαδή οι ερωτώμενοι αναγνωρίζουν το πρόβλημα έχει τις ρίζες του και στην ανάπτυξη της τεχνολογίας και άρα και της χρησιμοποίησής της από τους θύτες, με σκοπό την εξαπάτηση.

Αυτό εξάλλου προκύπτει και από το ποσοστό περίπου στο 30% (συγκεκριμένα 29,7%, 89 απαντήσεις) που δήλωσε ότι «Έχει εξελιχθεί πολύ η εγκληματική δραστηριότητα».

Ένα ποσοστό 26,7% (80 απαντήσεις) εντοπίζει ότι «υπάρχει μεγάλη δυσκολία στον έλεγχο των περιστατικών» ενώ το 16% (48 απαντήσεις) θεωρεί ότι «Δεν έχει

ανταποκριθεί στο ρόλο της η Ελληνική Αστυνομία και οι δημόσιες αρχές». Αντίστοιχα, το 15% (45 απαντήσεις) δήλωσαν ότι πρόκειται για διεθνικές δραστηριότητες που δυσχεραίνουν την παρέμβαση των αρχών. Αθροιστικά είναι υψηλό το ποσοστό των απαντήσεων που παρουσιάζει τον έλεγχο από τις Αρχές των περιστατικών κυβερνοεγκλήματος ως δύσκολο έργο, λόγω και της διεθνικότητας των περιπτώσεων του.

Το 31% (91 απαντήσεις) θεωρεί ως αιτία ότι «υπάρχουν ευκολόπιστα θύματα που ευνοούν τη συνέχιση των παρενοχλήσεων», τοποθετώντας το πρόβλημα και την αναπαραγωγή του από την πλευρά των θυμάτων.

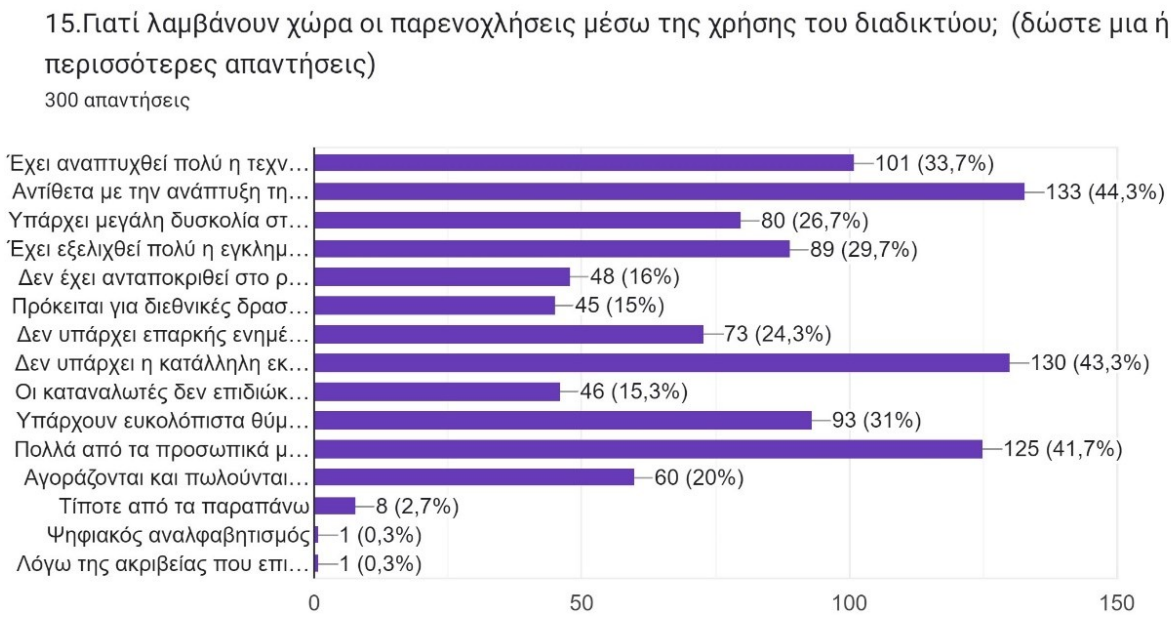
Ωστόσο το 24,3% (74 απαντήσεις) αναγνωρίζει ότι «Δεν υπάρχει επαρκής ενημέρωση των καταναλωτών» και το 15,3% (46 απαντήσεις) θεωρούν ότι «Οι καταναλωτές δεν επιδιώκουν να μοιραστούν τις άσχημες εμπειρίες τους από την παρενόχλησή τους ώστε να γίνουν παραδείγματα προς αποφυγή».

Το 20% (60 απαντήσεις) αναφέρει ως αιτία την αγοροπωλησία προσωπικών στοιχείων και δεδομένων. Αν σε αυτό το ποσοστό προστεθεί και το 41,7% (125 απαντήσεις) που θεωρεί, όπως προαναφέρθηκε, ότι «πολλά από τα προσωπικά μας στοιχεία είναι πλέον έκθετα σε πολλούς», τότε υπάρχει διάχυτη η αντίληψη της διασφάλισης του απόρρητου και της μη χρήσης προσωπικών δεδομένων από τρίτους και της έλλειψης επαρκούς προστασίας των προσωπικών δεδομένων.

«Τίποτε από τα παραπάνω» απάντησε μόλις το 2,7% (8 απαντήσεις).Τα πολύ χαμηλά αυτά ποσοστά δείχνουν ότι οι απαντήσεις που δόθηκαν σε αυτή την ερώτηση κάλυψαν σχεδόν εξολοκλήρου ολόκληρο το φάσμα των απόψεων που είχαν οι ερωτώμενοι και, ανάμεσα σε αυτούς, όσοι υπέστησαν παρενόχληση. Δύο από τους παραπάνω οκτώ σημείωσαν στην απάντηση «Άλλο» τον ψηφιακό αναλφαβητισμό και την ακρίβεια («Λόγω της ακριβείας που επικρατεί, οι άνθρωποι αναζητούν εύκολες λύσεις για να αυξήσουν τα οικονομικά τους με αποτέλεσμα να πείθονται»).

Τα ποσοστά για δώδεκα από τις εξεταζόμενες αιτίες είναι άνω του 15% δηλαδή πολλές από τις εξεταζόμενες αιτίες συγκεντρώνουν αξιοσημείωτο αριθμό απαντήσεων. Επίσης, μεγάλος αριθμός ερωτώμενων απάντησαν περισσότερες από δυο αιτίες. 90 στους 300 έδωσαν ως απάντηση μια και μοναδική αιτία, δηλαδή το 30%. Συνεπώς οι ερωτώμενοι αναγνωρίζουν ότι το πρόβλημα έχει σύνθετες αιτίες και δεν είναι προϊόν μιας μόνο αιτίας. Είναι χαρακτηριστικό ότι μόνο από τους 91 που απάντησαν ότι υπάρχουν ευκολόπιστα θύματα, μόνο 8 σημείωσαν μόνον αυτή ως αιτία.

Ερώτηση-Διάγραμμα 15



3.3 Η ΑΠΟΨΗ ΤΩΝ ΠΟΛΙΤΩΝ ΓΙΑ ΤΙΣ ΥΦΙΣΤΑΜΕΝΕΣ ΠΟΛΙΤΙΚΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥΣ ΑΠΟ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΚΑΙ ΤΗΝ ΠΑΡΕΝΟΧΛΗΣΗ

3.3.1. Σχετικά με τον ρόλο της Ελληνικής Αστυνομίας και του Υπουργείου Προστασίας του Πολίτη

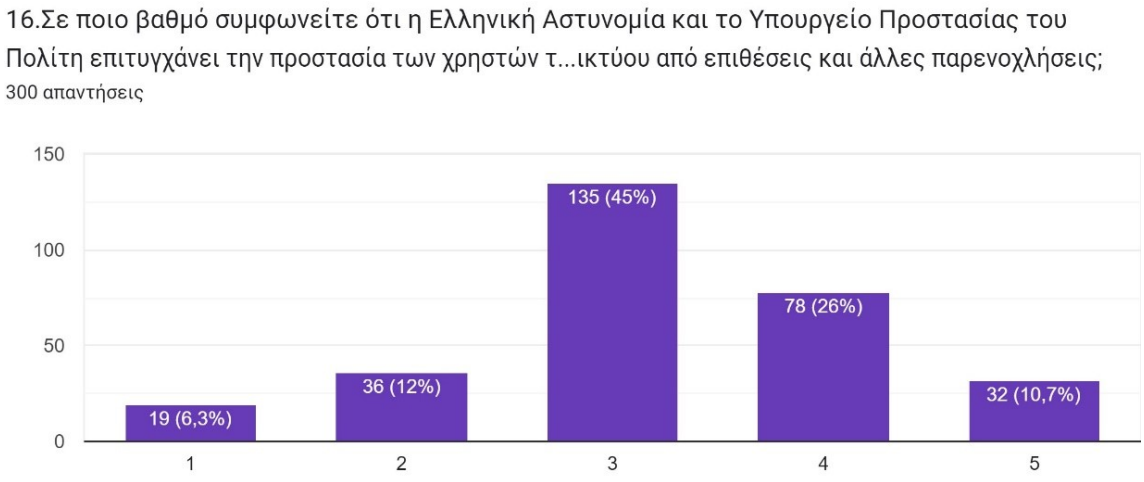
Εξετάζοντας το βαθμό στον οποίο η Ελληνική Αστυνομία και το Υπουργείο Προστασίας του Πολίτη επιτυγχάνουν την προστασία των χρηστών του διαδικτύου από κυβερνοεπιθέσεις και άλλες παρενοχλήσεις, η σχετική ερώτηση χρησιμοποίησε μια κλίμακα Likert για το βαθμό στον οποίο συμφωνούν οι ερωτώμενοι, όπου το 1 αντιστοιχεί σε πλήρη συμφωνία (ότι επιτυγχάνουν την προστασία) και το 5 (την πλήρη διαφωνία). Το 3 σημαίνει την ενδιάμεση άποψη δηλαδή το ούτε συμφωνώ ούτε διαφωνώ, το 2 σημαίνει «συμφωνώ» και το 4 «διαφωνώ». Η απάντηση που δόθηκε από τους ερωτώμενους ήταν μια και μοναδική.

Από τις απαντήσεις γίνεται φανερό ότι η Ελληνική Αστυνομία και το Υπουργείο Προστασίας του Πολίτη, παρά την αποστολή τους για τη διαφύλαξη της δημόσιας τάξης, δεν επιτυγχάνουν τον ρόλο τους να προστατεύουν τους πολίτες που χρησιμοποιούν το διαδίκτυο από το κυβερνοέγκλημα, στις διάφορες μορφές του. Ένα ποσοστό 45% (που προσεγγίζει τους μισούς, 135 απαντήσεις) δήλωσε το 3 ενώ το

26% δήλωσε ότι διαφωνεί (4). Αθροίζοντας τα δυο αυτά ποσοστά στο ποσοστό όσων διαφωνούν απόλυτα (10,7%) προκύπτει ότι συνολικά ένα ποσοστό 81,7% δηλώνει από 3 και άνω, στην κλίμακα Likert. Επίσης ένα ποσοστό 36,7% δηλώνει ότι διαφωνεί ή ότι διαφωνεί απόλυτα. Δηλαδή μπορούμε να πούμε με σιγουριά ότι υπάρχει μια σαφής εκτίμηση από τους πολίτες ότι η Ελληνική Αστυνομία και το Υπουργείο Προστασίας του Πολίτη δεν προστατεύουν τους χρήστες του διαδικτύου από το κυβερνοέγκλημα.

Ωστόσο καλό είναι να σημειώσουμε ότι υπάρχει και ένα ποσοστό που δηλώνει ότι συμφωνεί ή συμφωνεί απόλυτα και ανέρχεται στο 18,3% αθροιστικά. Θεωρώντας ότι οι μισοί από τους ερωτώμενους που απάντησαν 3 μπορεί να συμφωνούν σε έναν βαθμό, τότε υπάρχει και ένα αξιοπρόσεχτο ποσοστό όσων θεωρούν ότι γίνεται μια προσπάθεια για την προστασία του πολίτη από την Ελληνική Αστυνομία και το Υπουργείο Προστασίας του πολίτη. Είναι φανερό ότι η προσπάθεια αυτή όμως χρειάζεται να βελτιωθεί, προκειμένου να αυξηθούν και τα ποσοστά ικανοποίησης των πολιτών από το έργο της Αστυνομίας και η μείωση των περιστατικών παρενόχλησης.

Ερώτηση-Διάγραμμα 16



3.3.2. Δύναται η Δημόσια Διοίκηση και η Ελληνική Αστυνομία να επιτύχει τον συστηματικό περιορισμό των παρενοχλήσεων των χρηστών διαδικτύου;

Έχοντας προηγουμένως εξετάσει σε τι βαθμό οι ερωτώμενοι συμφωνούν με την παρεχόμενη προστασία απέναντι στις παρενοχλήσεις από την Ελληνική Αστυνομία

και το Υπουργείο Προστασίας του Πολίτη, εξετάστηκε περαιτέρω αν μπορούν τελικά τόσο η Ελληνική Αστυνομία όσο και η Δημόσια Διοίκηση ευρύτερα (συμπεριλαμβανομένων και άλλων Υπουργείων και φορέων πλην του Υπουργείου Προστασίας του Πολίτη, όπως για παράδειγμα το Υπουργείο Ψηφιακής Διακυβέρνησης και τα Υπουργεία Παιδείας, Οικονομικών, Ανάπτυξης) μπορούν, ασκώντας τις πολιτικές εκείνες που εστιάζουν στο αγαθό της δημόσιας ασφάλειας, να περιορίσουν συστηματικά τις παρενοχλήσεις των χρηστών του διαδικτύου και συνεπώς και του κυβερνοεγκλήματος .

Εξετάζοντας το Διάγραμμα 17 και συγκρίνοντάς το με το Διάγραμμα 16 διαπιστώνεται μια παρόμοια κατανομή των απαντήσεων στην (κοινή) κλίμακα Likert που εκφράζει τον βαθμό στον οποίο συμφωνούν ή διαφωνούν με την ερώτηση. Το ποσοστό όσων ούτε συμφωνούν ούτε διαφωνούν (ενδιάμεσα στην κλίμακα Likert) είναι 40,3%. Πρόκειται για μια απάντηση που χαρακτηρίζει την άποψη ότι δεν δύναται να τα καταφέρει η Ελληνική Δημόσια Διοίκηση στον ρόλο αυτό.

Ένα ποσοστό 12% (υψηλότερο από την προηγούμενη απάντηση) δήλωσε ότι συμφωνεί απόλυτα και ποσοστό 21% ότι συμφωνεί. Αθροιζόμενα δίνουν 33%, το ένα-τρίτο των απαντήσεων. Είναι δηλαδή εμφανές ότι ένα μεγαλύτερο τμήμα από ότι στην προηγούμενη ερώτηση συμφωνεί ότι μπορεί η συστηματική προστασία των χρηστών του διαδικτύου να επιτευχθεί από τις ενέργειες της Δημόσιας Διοίκησης και της Ελληνικής Αστυνομίας. Ακόμα όμως και αν αθροίσουμε τμήμα του ποσοστού όσων απάντησαν ότι ούτε συμφωνούν ούτε διαφωνούν, τότε και πάλι παραμένει ένα αξιοσημείωτο τμήμα των ερωτώμενων πού διαφωνούν ή διαφωνούν απόλυτα.

Μόνο όμως το 12% των ερωτώμενων συμφωνεί απόλυτα ότι μέσα από τις πολιτικές για το αγαθό της δημόσιας ασφάλειας από την Ελληνική Αστυνομία και Υπουργείο Προστασίας του Πολίτη δύναται να αντιμετωπιστεί το πρόβλημα των παρενοχλήσεων. Το ποσοστό αυτό δείχνει είτε ότι ένα μεγάλο ποσοστό των πολιτών είναι προβληματισμένο ως προς την επάρκεια των πολιτικών και των δυο αυτών φορέων (της Ελληνικής Αστυνομίας και του Υπουργείου Προστασίας του Πολίτη) να αντιμετωπίσουν από μόνοι τους το πρόβλημα είτε ότι είναι προβληματισμένο ως προς τη διάσταση και έκταση του προβλήματος και εκφράζει μέσω της απάντησης αυτής και μια έκδηλη απογοήτευση (με βάση και ανάλογες εμπειρίες των χρηστών που απάντησαν το ερωτηματολόγιο).

Επειδή η ερώτηση δεν διερευνούσε αν η αιτία που δεν συμφωνούν ή συμφωνούν οι ερωτώμενοι συνδέεται με εξωγενείς παράγοντες από τη λειτουργία της Δημόσιας

Διοίκησης (όπως μερικοί από αυτούς έχουν παρουσιαστεί και απαντηθεί στην ερώτηση 15 και αφορούν για παράδειγμα την μεγάλη παγκόσμια ανάπτυξη της τεχνολογίας και του κυβερνοεγκλήματος), δεν μπορεί να γίνει αντιληπτό από τις απαντήσεις στην ερώτηση αυτή αν πρόκειται για την άποψη όσων θεωρούν ότι το Δημόσιο δεν μπορεί να επιλύσει το πρόβλημα ανεξάρτητα από ποιες πολιτικές που θα ασκήσει.

Για τον παραπάνω λόγο εξετάστηκε ξεχωριστά το θέμα των αιτιών, στην αμέσως επόμενη ερώτηση.

Ερώτηση-Διάγραμμα 17

3.3.3. Αιτίες για την μη πλήρη προστασία των χρηστών του διαδικτύου από κυβερνοεπιθέσεις και την παρενόχληση

Σε συνέχεια αυτή της παραπάνω ερώτησης αλλά και προηγούμενων ερωτήσεων που είχαν ήδη δημιουργήσει μια εικόνα στους ερωτώμενους του προβλήματος που λαμβάνει χώρα και στην Ελλάδα (ή υπενθυμίσει για τους πιο πολλούς από αυτούς), επιδιώχθηκε να αντληθεί από το δείγμα η άποψη για τα αίτια της μη πλήρης προστασίας των χρηστών του διαδικτύου από τις κυβερνοεπιθέσεις και την παρενόχληση στην Ελλάδα.

Για να απαντηθεί η ερώτηση αυτή που αφορούσε στις αιτίες παρενόχλησης, δεν ήταν προϋπόθεση ο ερωτώμενος να έχει προηγουμένως υποστεί κάποια παρενόχληση. Όσοι απάντησαν ότι δεν έχουν δεχτεί κάποια παρενόχληση, έδωσαν επίσης απάντηση και σε αυτήν ερώτηση. Δεν συντρέχει κάποιος λόγος που να μας κάνει να

θεωρήσουμε ότι οι απαντήσεις των τελευταίων επηρεάζουν με ιδιαίτερο τρόπο το τελικό αποτέλεσμα και θα έπρεπε να μη ληφθούν υπόψη και να γίνει αναγωγή.

Όπως φαίνεται και στο Διάγραμμα 18 που ακολουθεί, το 44,7% φαίνεται ότι έχει αντιληφθεί ότι «Οι τρόποι παρενόχλησης και κυβερνοεπίθεσης είναι πολλοί και διαρκώς εφευρίσκονται καινούργιοι». Το ποσοστό αυτό είναι ιδιαίτερα υψηλό και προσεγγίζει σχεδόν τον έναν στους δύο ερωτώμενους.

Ένα ποσοστό 33% απάντησαν ότι «Υπάρχει ανάγκη σε εξειδικευμένο προσωπικό σε θέματα κυβερνοασφάλειας», διαπιστώνοντας ότι το ζήτημα της διασφάλισης της προστασίας των θυμάτων και της μείωσης των περιστατικών παρενόχλησης είναι τεχνικό και συνδέεται με το εξειδικευμένο προσωπικό που είναι αναγκαίο για τα θέματα κυβερνοασφάλειας. Επίσης ένα ποσοστό 31,3% απάντησε ότι υπάρχει «Έλλειψη γνώσεων και ανεπάρκεια της δημόσιας διοίκησης για τις απειλές από το διαδίκτυο». Αθροιζόμενες οι απαντήσεις για τις δυο αυτές περιπτώσεις, χωρίς όμως να υπολογίζονται δυο φορές οι απαντήσεις που ήταν κοινές (που περιείχαν δηλαδή και τις δυο απαντήσεις) δίνουν ένα ποσοστό 48,7% (συνολικά 146 απαντήσεις). Αυτό υποδηλώνει ότι περίπου ένας στους δυο θεωρούν το ζήτημα τεχνικό που χρειάζεται να καλυφθεί με γνώσεις και κατάλληλη επάρκεια της Δημόσιας Διοίκησης που σήμερα απουσιάζει.

Το 25,3% απάντησε ότι «το έγκλημα δεν έχει σύνορα». Δηλαδή ένας στους τέσσερις θεωρεί ότι οι διεθνείς ορίζοντες του προβλήματος και το πολυπλόκαμο στο διεθνές στερέωμα επηρεάζουν και τους τρόπους αντιμετώπισης.

Ποσοστό 21% απάντησε ότι «Τα ίδια τα προβλήματα παρενόχλησης και κυβερνοεπίθεσης είναι σύνθετα». Άρα, λίγο περισσότερο από ένας στους πέντε αντιλαμβάνεται ότι πρόκειται για προβλήματα σύνθετα που δεν επιλύονται εύκολα και χρειάζονται ειδικές και συστηματικές πολιτικές.

Ένα ποσοστό 22,7% απάντησε ότι «η δράση των αρχών (αστυνομία, εκπαίδευση, φορείς) δεν είναι προσαρμοσμένη στην εποχή μας», θέτοντας ζήτημα επάρκειας της λειτουργίας της Δημόσιας Διοίκησης ως προς το κυβερνοέγκλημα.

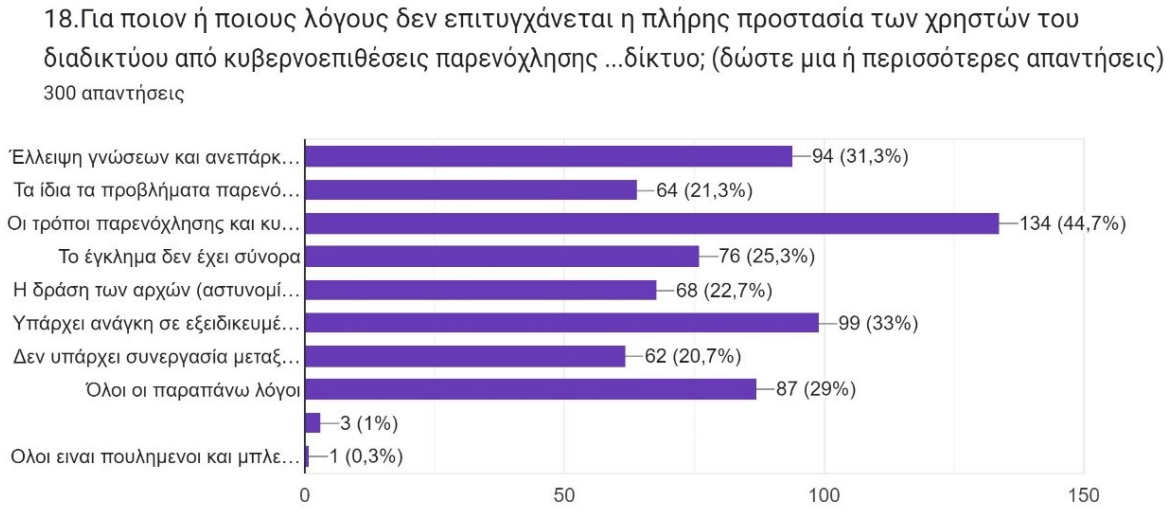
Ποσοστό 20,7% απάντησε ότι «δεν υπάρχει συνεργασία μεταξύ των φορέων που εμπλέκονται στην καταπολέμηση του κυβερνοεγκλήματος». Δηλαδή ένας στους πέντε πάλι αντιλαμβάνεται ότι το κυβερνοέγκλημα καταπολεμάται απαραιτήτως μέσα από την συνεργασία φορέων που εμπλέκονται για την καταπολέμησή του.

Το 29% των ερωτώμενων θεωρεί ότι για όλους τους παραπάνω λόγους δεν επιτυγχάνεται η πλήρης προστασία των θυμάτων κυβερνοεγκλήματος από τους

θύτες. Αυτό είναι ένα σημαντικό ποσοστό που δείχνει ότι οι ερωτώμενοι αξιολογούν ότι το πρόβλημα είναι σύνθετο και η μη επίλυσή του έχει πολλές αιτίες. Σημειώνεται ότι οι 75 από τους 87 που απάντησαν «όλοι οι παραπάνω λόγοι» έδωσαν αποκλειστικά αυτή την απάντηση ενώ οι υπόλοιποι απάντησαν και προηγούμενες απαντήσεις, όχι απαραίτητα όλες. Αυτή είναι μια δυσκολία ενός τέτοιου ερωτήματος, ειδικά όταν η απάντηση «όλοι» βρίσκεται στο τέλος της ερώτησης και ο ερωτώμενος έχει ξεκινήσει να δίνει τις απαντήσεις που (ήδη) κρίνει ως ορθές.

Τέλος υπάρχει και ένα ποσοστό 1% (3 απαντήσεις μόλις) που επέλεξαν να απαντήσουν «άλλο» χωρίς να σημειώσουν τι. Ένας μόνο αναγράφει την άποψη ότι «Όλοι είναι πουλημένοι και μπλεγμένοι εξίσου» που εκφράζει μια αγανάκτηση. Το πολύ χαμηλό αυτό ποσοστό υποδηλώνει ότι ελάχιστοι ερωτώμενοι αναζήτησαν ή βρήκαν κάποια πρόσθετη αιτία σε αυτές που έδινε ήδη η εκφώνηση.

Ερώτηση-Διάγραμμα 18



ΚΕΦΑΛΑΙΟ 4^{ο} : ΣΥΜΠΕΡΑΣΜΑΤΑ

Το κυβερνοέγκλημα είναι μιας μορφής έγκλημα που αναπτύσσεται ραγδαία κατά τις τελευταίες δεκαετίες, παρακολουθώντας τις εξελίξεις της ανάπτυξης του διαδικτύου με το οποίο συνδέεται. Θύματά του, είναι εκατομμύρια χρήστες του διαδικτύου παγκοσμίως ενώ η οικονομική αιμορραγία που αφήνει είναι ήδη της τάξης των τρισεκατομμυρίων ευρώ. Αποτελεί μια ιδιαίτερα προσοδοφόρα εγκληματική δραστηριότητα που τείνει να ξεπεράσει άλλες εγκληματικές δραστηριότητες σε τζίρο και ζημιά για τις εθνικές οικονομίες και τις επιχειρήσεις. Καθώς αναπτύσσεται το διαδίκτυο και τα οφέλη που δημιουργεί στους χρήστες του, αυξάνει -δυστυχώς- σχεδόν παράλληλα και η συχνότητα, οι περιπτώσεις και τα κρούσματα όσων πέφτουν θύμα του κυβερνοεγκλήματος. Συνεπώς, η μελέτη του κυβερνοεγκλήματος αποτελεί καίριας σημασίας ζήτημα στις μέρες μας.

Παρά το γεγονός ότι ασκούνται ήδη κάποιες πολιτικές από το κράτος για την προστασία από το κυβερνοέγκλημα, το έγκλημα αυτό λαμβάνει χώρα στην Ελλάδα με πολύ μεγάλη ανάπτυξη και παρουσία, όπως και στον υπόλοιπο κόσμο. Η ψηφιακή μετάβαση που συντελείται στην Ελληνική κοινωνία και εντάθηκε μετά τον κορωνοϊό βρίσκει πολλούς Έλληνες ευάλωτους και τρωτούς σε διάφορες μορφές παρενόχλησης.

Η παρούσα εργασία μελέτησε το κυβερνοέγκλημα και τις μορφές εξαπάτησης που λαμβάνει στην Ελλάδα, αφού προηγουμένως εξέτασε μια πολύ πλούσια σχετική βιβλιογραφία και αρθρογραφία και επιχείρησε να αντιληφθεί το μέγεθος και την σημασία του και να καταγράψει τις διάφορες πτυχές του που είναι απαραίτητες για την μελέτη. Επίσης, επιχείρησε να καταγράψει όχι μόνο τι έχει συμβεί αλλά και πως, αν έγινε αντιληπτό από τα θύματα κατά τη διάρκεια της ίδιας της κυβερνοεπίθεσης, αν η σοβαρότητα της απειλής έγινε αντιληπτή, το γιατί θυματοποιήθηκαν, γιατί καθυστέρησαν να αντιδράσουν, αν αντέδρασαν ενημερώνοντας την αρχές και την Αστυνομία, τι ένιωσαν ως θύματα και άλλα ερωτήματα περιγραφής του προβλήματος.

Με βάση την αρθρογραφία και βιβλιογραφία γύρω από το κυβερνοέγκλημα, φαίνεται ότι υπάρχουν πολλές και διάφορες αιτίες, αλλά η κυριότερη από αυτές είναι οικονομική αβεβαιότητα και η αποκόμιση εσόδων από την πλευρά του θύτη. Επίσης, φαίνεται ότι οι μορφές που λαμβάνει είναι πολλές, αφού οι χρήστες του διαδικτύου εκτίθενται απευθείας είτε σε ένα δεύτερο στάδιο. Οι συνέπειες του

κυβερνοεγκλήματος τόσο πάνω στα θύματα όσο και για την ίδια την κοινωνία και την οικονομία είναι πολλές και εκτείνονται σε οικονομικές, κοινωνικές, ψυχολογικές κ.ά.

Η έρευνα κατέληξε σε πολλά χρήσιμα συμπεράσματα που αφορούν διάφορες πτυχές και ερωτήματα που εξετάστηκαν γύρω από το κυβερνοέγκλημα στην Ελλάδα. Τα κυριότερα από αυτά αναλύονται παρακάτω.

Μέχρι στιγμής δεν φαίνεται να υπάρχουν αντίστοιχες μελέτες στην Ελλάδα που να έχουν παρουσιάσει μια εικόνα του τι συμβαίνει στην Ελλάδα, έστω και με βάση κάποιο δείγμα, όπως αυτό επιχειρείται στην παρούσα εργασία.

Τα κύρια χαρακτηριστικά του δείγματος που επιλέγει τυχαία είναι ότι αποτελείται σε μεγάλο ποσοστό από ανθρώπους υψηλού μορφωτικού επιπέδου, κατά τα δύο-τρίτα γυναίκες και προέρχεται και από την Ελληνική περιφέρεια, δηλαδή εκπροσωπείται η εικόνα του τι συμβαίνει στην Ελληνική περιφέρεια και όχι απλώς στην Αττική όπου είναι συγκεντρωμένο το μεγαλύτερο τμήμα του Ελληνικού πληθυσμού.

Το ένα-τρίτο σχεδόν του δείγματος (ποσοστό 34%) απάντησε ότι δεν έχει δεχτεί κάποια κακόβουλη επίθεση ή άλλη ενέργεια παρενόχλησης μέσω του διαδικτύου. Αυτό δείχνει ότι ένας στους τρεις δεν δέχεται κάποια μορφής παρενόχληση αλλά δυο στους τρεις δέχονται, ποσοστό πολύ υψηλό.

Το e-mail χρησιμοποιείται από το κυβερνοέγκλημα σε περισσότερο από το ένα-τρίτο του δείγματος, ποσοστό 37,7%. Εξίσου υψηλής πιθανότητας για τη δημιουργία θύματος είναι και τα κοινωνικά δίκτυα, γιατί ένα ποσοστό 31,3% δέχτηκε παρενόχληση μέσω αυτών. Περισσότερο φαίνεται ότι οι θύτες αναζητούν ενεργητικά τα θύματα και επιδιώκουν να τους «χτυπάνε την πόρτα», «οχυρωμένοι» πίσω από την ελευθερία που τους παρέχεται να δρουν ανενόχλητοι στον άναρχο κόσμο του διαδικτύου και την αδυναμία εύρεσής τους. Έτσι δικαιολογείται και το δεύτερο συνθετικό της λέξης «κυβερνο-επίθεση». Από την ενεργητικότητα και επιθετικότητα αυτή που επιδεικνύουν απορρέει ο προβληματισμός και ο διάλογος για το αν πρόκειται για ένα ζήτημα που αφορά τη δημόσια ασφάλεια και αν οι πολίτες βρίσκονται εκτεθειμένοι σε μια διαρκή απειλή.

Οι Έλληνες χρήστες του διαδικτύου θεωρούν επικίνδυνη και σοβαρή απειλή ή επιβλαβή για αυτούς και για την οικογένειά τους σε μεγάλο ποσοστό, που ξεπερνούσε τον έναν στους τρεις ή το 54% αν δεν υπολογιστούν όσοι δεν δέχτηκαν παρενόχληση.

Παρά το γεγονός ότι σχεδόν το μισό δείγμα (47,3%) απέφυγε την παρενόχληση και το ποσοστό όσων την απέφυγαν αμέσως ή πιο μετά είναι υψηλό (άνω του 60%),

ένας στους δέκα (10%) στο δείγμα που δεν περιλαμβάνει όσους δεν δέχτηκαν παρενόχληση πείστηκαν από τους παρενοχλούντες θύτες. Αυτό υποδηλώνει την μεγάλη πειθώ των θυτών, δεδομένου ότι το δείγμα αποτελείται από μορφωμένους κυρίως ανθρώπους.

Παρά το γεγονός ότι απάντησαν σε μεγάλο ποσοστό ότι πρόκειται για σοβαρή περίπτωση με επιβλαβείς επιπτώσεις σε αυτούς και την οικογένειά τους, το 50,7% απάντησε ότι δεν ανακάτεψε την Αστυνομία. Δηλαδή φαίνεται η Αστυνομία δεν εμπλέκεται σε πολλές περιπτώσεις κυβερνοεγκλήματος κατά τη διάρκεια της εξέλιξής του ή για την εξιχνίαση τους. Οι περιπτώσεις αυτές περνάνε απαρατήρητες από την Αστυνομία, που προφανώς θα έχει εικόνα διαφορετική από αυτήν που λαμβάνει τελικά χώρα. Δηλαδή πρόκειται για ένα έγκλημα που επειδή σε πολλές περιπτώσεις δεν καταγράφεται και δεν τίθεται υπόψη των αστυνομικών αρχών, πιθανόν δεν αντιμετωπίζεται κιόλας όπως πρέπει (παρά δηλαδή τον ρόλο και την επιμέλεια της Αστυνομίας να διασφαλίζει την δημόσια ασφάλεια).

Από την ερώτηση για τους τρόπους εξαπάτησης των θυμάτων, δόθηκαν 2,36 μορφές παρενόχλησης ανά ερωτώμενο, αναλογία πολύ υψηλή που υποδηλώνει την μεγάλη εξάπλωση και έκταση του φαινομένου. Η περίπτωση της εξαπάτησης μέσω υποτιθέμενων κερδών από λαχνούς ή λαχεία φαίνεται ότι είναι πολύ διαδεδομένη στην Ελληνική επικράτεια (λιγότερο από ένας στους τρεις στο δείγμα χωρίς όσους δεν έπεσαν θύματα) ενώ αξιοσημείωτο είναι και το ποσοστό του «ψαρέματος» (phishing) (λίγο λιγότερο από το παραπάνω), ενώ η εξαπάτηση σε σχέση με χρηματικά ποσά από δημόσιες υπηρεσίες (ΑΑΔΕ ή άλλες) που χρειάζεται να εκταμιευτούν ξεπέρασε το ένα τέταρτο του αντίστοιχου δείγματος (χωρίς τους μη παρενοχλημένους), ποσοστό που προσέγγισε και η εξαπάτηση με την κατάθεση χρημάτων στο εξωτερικό, με χρηματικό αντάλλαγμα (23,1% στο δείγμα χωρίς τους μη παρενοχλημένους). Στο ένα-πέμπτο αυτού του δείγματος επιχειρήθηκε η εξαπάτηση με τη δήθεν κληρονομιά που παρέλαβαν. Οι παραπάνω φαίνεται να είναι και οι συχνότερες μορφές παρενόχλησης στην Ελλάδα από τους κυβερνο-εγκληματίες και απατεώνες.

Παρουσιάζει ιδιαίτερο ενδιαφέρον ότι παρά το γεγονός ότι η ερώτηση έδινε 15 διαφορετικές απαντήσεις και μεγάλο αριθμό επιλογών, οι ερωτώμενοι απάντησαν επίσης πολλές και διαφορετικές απαντήσεις, ανάγοντας τον αριθμό των απαντήσεων σε τουλάχιστον 30 διαφορετικούς μορφές εξαπάτησης που χρησιμοποιούνται από τους θύτες. Από το στοιχείο αυτό, συμπεραίνεται ότι πρόκειται για ένα φαινόμενο που

έχει πολλά ‘πλοκάμια’ και λαμβάνει πολλές και διαφορετικές μορφές (οι οποίες δύσκολα μπορούν να διερευνηθούν μέσα από μια ερώτηση και πιθανόν να χρειάζονται και ειδικότερο ερωτηματολόγιο για την μελέτη τους).

Φαίνεται, επίσης, ότι η δεύτερη πιο διαδεδομένη «θύρα» από την οποία μπαίνουν οι εγκληματίες (μετά τα οικονομικά οφέλη για τα θύματα) είναι αυτή ακριβώς που πρέπει να επιδιώκουν να προσέχουν οι χρήστες: της ασφάλειας, της προστασίας της προσωπικής ζωής και της ιδιωτικότητας. Δηλαδή οι θύτες επιδιώκουν να εκμεταλλευτούν την ανησυχία των θυμάτων για θέματα ασφάλειας για να επιτύχουν ακριβώς το αντίθετο από αυτό που επιθυμούν τα θύματα. Σε πάνω από μια στις δυο περιπτώσεις παρενόχλησης οι θύτες παρουσιάζουν στα θύματα ότι συντρέχει λόγος ασφάλειας και προστασίας τους.

Σε ότι αφορά τις στρατηγικές πειθούς όσων τελικά έπεσαν θύματα, φαίνεται ότι η χρήση αληθοφανών ιστοσελίδων είναι ευρέως διαδομένη (σε ποσοστό 43,8% για όσους δέχθηκαν παρενόχληση στο δείγμα) από τους θύτες καθώς και η πρακτική να δημιουργούν μια εικόνα αξιοπιστίας, με τεκμήρια ή άλλα δήθεν αποδεικτικά στοιχεία. Συχνά χρησιμοποιείται και η παραπλάνηση με κουπόνι ή άλλο δώρο ενώ επιδιώκουν και την συστηματική επικοινωνία με το θύμα, στο οποίο δημιουργούν την προσδοκία ότι θέλουν να γνωρίσουν και από κοντά.

Σε ότι αφορά τη συχνότητα της παρενόχλησης, ένας στους έξι έχει δεχτεί συχνά παρενόχληση και ένας στους πέντε από συχνά και πάνω (πολύ συχνά ή και καθημερινά). Αυτό υποδηλώνει μεγάλη συχνότητα παρενόχλησης, εικόνα που συνάδει και με την προγενέστερη, για τις πολλές και διάφορες μορφές παρενόχλησης.

Ως προς τις αιτίες για τις παρενοχλήσεις στο διαδίκτυο, οι ερωτώμενοι διακρίνουν ως κυριότερες, την ανάπτυξη της τεχνολογίας σε αναντιστοιχία με τα μέσα προφύλαξης, την έλλειψη εκπαίδευσης των καταναλωτών σε θέματα ασφαλούς χρήσης του διαδικτύου και την υπερ-έκθεση των προσωπικών στοιχείων των καταναλωτών/χρηστών του διαδικτύου στην εποχή μας. Οι τρεις αυτές αιτίες υποδηλώνουν την ύπαρξη ενός σοβαρού ζητήματος ασφάλειας για την Ελληνική κοινωνία. Σημαντικό είναι και το ποσοστό των ερωτώμενων που θεωρεί ως αιτίες για την ανάπτυξη του κυβερνοεγκλήματος τις τεχνολογικές εξελίξεις.

Το 31% θεωρεί ότι τα θύματα είναι ευκολόπιστα αλλά από αυτούς μόλις το 0,03% θεωρεί την αιτία ως τη μοναδική. Μόλις το 30% θεωρεί ως αιτία του κυβερνοεγκλήματος μια μόνο αιτία. Οι περισσότερο απαντάνε πάνω από μια αιτία για

το πρόβλημα. Αυτό προκύπτει και από το ότι πολλές από τις αιτίες που εξετάστηκαν εντοπίζονται ως σημαντικές (ποσοστά άνω του 15% λαμβάνουν δώδεκα από τις εξεταζόμενες αιτίες).

Σε ότι αφορά την άποψη των ερωτώμενων αν η Αστυνομία και το Υπουργείο Προστασίας του Πολίτη επιτυγχάνουν τον ρόλο τους να προστατεύουν το κράτος, ένας στους τρεις διαφώνησε ή διαφώνησε απόλυτα και ένας στους δυο είτε διαφωνεί (πολύ ή λίγο) είτε ούτε συμφωνεί ούτε διαφωνεί. Δηλαδή η θέση των ερωτώμενων είναι ότι υπάρχει μια μεγάλη αδυναμία της Αστυνομίας και του Υπουργείου να επιτύχει τον ρόλο της να προστατέψει τους πολίτες από το κυβερνοέγκλημα και απαιτείται σημαντική βελτίωση της όποιας προσπάθειας καταβάλλεται.

Σε ό,τι αφορά, το εάν δύναται η Δημόσια Διοίκηση και η Ελληνική Αστυνομία να αντιμετωπίσει το κυβερνοέγκλημα, ένα ποσοστό 40,5% απαντάει ότι ούτε συμφωνεί ούτε διαφωνεί ενώ ένας στους τρεις απαντάει ότι συμφωνεί απλώς ή πολύ. Δηλαδή υπάρχει μεγάλος αριθμός ερωτώμενων που θεωρεί ότι το πρόβλημα ξεπερνάει τις δυνάμεις της Δημόσιας Διοίκησης και της Ελληνικής Αστυνομίας και προφανώς αυτό δικαιολογεί και την απάντηση στην προηγούμενη ερώτηση.

Διερευνώντας τα αίτια για την μη πλήρη προστασία των χρηστών του διαδικτύου από τις παρενοχλήσεις, οι ερωτώμενοι απάντησαν σε ποσοστό 44,7% ότι οι τρόποι του κυβερνοεγκλήματος είναι πολλοί και διαρκώς εφευρίσκονται νέοι, δηλαδή όπως είχε προκύψει από τις 30 απαντήσεις στην ερώτηση για τις αιτίες ότι πρόκειται για μια «Λερναία Ύδρα». Στο σημείο αυτό φαίνεται η συμβατότητα των απαντήσεων μεταξύ των δυο αυτών ερωτήσεων, πράγμα που δείχνει ότι η ανάλυση σε αυτό το ζήτημα είναι έγκυρη. Σχεδόν ένας στους δυο ερωτώμενους απάντησε ότι το ζήτημα είναι τεχνικό ενώ ένας στους τέσσερις θεωρεί ότι το κυβερνοέγκλημα δεν αντιμετωπίζεται πλήρως γιατί πρόκειται για διεθνικό έγκλημα. Ένας στους τέσσερις αναγνωρίζει ότι πρόκειται για σύνθετης μορφής έγκλημα και πάνω από ένας στους τέσσερις ότι η δράση των αρχών δεν είναι προσαρμοσμένη στην εποχή μας. Τέλος ένας στους τέσσερις αναφέρεται στην έλλειψη της συνεργασίας μεταξύ των φορέων και την ανάγκη να υπάρχει συνεργασία. Στην ερώτηση αυτή, που πολλοί ερωτώμενοι απάντησαν πάνω από έναν λόγους, το 29%, δηλαδή ένα πολύ σημαντικό ποσοστό, ανέφερε όλους τους λόγους που εκτέθηκαν από την εκφώνηση ως σημαντικούς. Μάλιστα 75 από τους 87 που απάντησαν «όλοι οι λόγοι» έδωσαν αποκλειστικά αυτή την απάντηση (χωρίς να την συνδυάσουν και μια ή περισσότερες από τις άλλες απαντήσεις).

Από όλα τα παραπάνω προκύπτει ότι το κυβερνοέγκλημα είναι ένα πολύ μεγάλο σύγχρονο πρόβλημα για τους Έλληνες πολίτες και την ελληνική κοινωνία και οικονομία και ότι οι πολιτικές που γίνονται για την αντιμετώπισή τους χρειάζονται βελτίωση και συστηματική παρακολούθηση ως προς τα αποτελέσματα και την αποτελεσματικότητα που έχουν, γιατί φαίνεται ότι αυτή είναι περιορισμένη. Η καθιέρωση ενός συστηματικού τρόπου μελέτης του, όπως μέσα από ερωτηματολόγια σαν το παρόν, και η μελέτη σε βάθος τόσο του κυβερνοεγκλήματος, όσο και των αιτιών, των μορφών και των συνεπειών του, χρειάζονται για την βελτίωση των πολιτικών αυτών και την συστηματική αντιμετώπιση ενός τόσο σύγχρονου και μόνιμα επικαιροποιημένου προβλήματος που ‘τρέχει’ παράλληλα με την εξέλιξη της τεχνολογίας και ήδη τείνει να κατασπαράξει το αγαθό της δημόσιας ασφάλειας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Anesa, P. (2020) Lovextortion: Persuasion strategies in romance cybercrime, Discourse, Context & Media, 35, 100398

Arief, B. and Adzmi, A.B. (2015) Understanding Cybercrime from its Stakeholder's Perspective, IEEE Security and Privacy, March/April 2015

Awodiran, M.A., Ogundele, A.T., Udosen, J.I. and Anwana, E.O. (2023) Cybercrime consciousness among undergraduate students, 2023 International Conference On Cyber Management And Engineering (CyMaEn)

Badawi, E., Jourdan, G.-V. and Onut, I.-V. (2022) The "Bitcoin Generator" Scam, Blockchain: Research and Applications, 3, 100084

Badawi, E. and G.-V. Jourdan (2020)Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review, IEEE Access, 8 DOI: 10.1109/ACCESS.2020.3034816

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L. and Seruisi, S. (2021) Cryptocurrency Scams: Analysis and Perspectives, IEEE, Access, DOI: 10.1109/ACCESS.2021.3123894

Betra., S., Gupta, M. Singh, J. Srivastava, D. and Aggarwal, I. (2020) An Empirical Study of Cybercrime and its Preventions, 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), DOI:978-1-7281-7132-6/20, IEEE

Bera, D., Ogbanufe, O. and Kim, D.J. (2023) Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions, Decision Support Systems, 171, 113977

Chung, W., Chen, H., Chang, W. Chou, S. (2006) Fighting cybercrime: a review and the Taiwan experience, Decision Support Systems, 41, 669– 682

CISSPCISA and Sutcliffe (2008) An Overview of Transnational Organized CyberCrime, Information Security Journal: A Global Perspective, 17, 87–94

Cohen, F. Internet Fraud: Mythical Online Scams, Compute Fraud and Security, 19
Computer Fraud and Security (2019) Church scammed as FBI warns of FBI major rise in BEC fraud, Computer Fraud and Security, 3-4, May 2019

Computer Fraud and Security (αγν. έτους) Nigerian Fraud — do people fall for this scam— statistics say yes, Computer Fraud and Security, 20

Cross, C. (2019) Is online fraud just fraud? Examining the efficacy of the digital divide, Journal of Criminological Research, Policy and Practice, 50 (20), 120-131

Dimitrov, N., Nozharov, S. and Cenkov, Y. (2023) Economic Typology of Cybercrimes in Bulgaria, 2023 International Scientific Conference on Computer Science (COMSCI), DOI: 10.1109/COMSCI59259.2023.10315844

Drew, J.M. and Webster, J. (2023) The victimology of online fraud: A focus on romance fraud victimisation, Journal of Economic Criminology, 3, 100053

Dunham, K. (2007) Pump and Dump Scams, Information Systems Security,16 (1), 65-71, DOI: 10.1080/10658980601051755

FBI (2024) What we investigate: The Cyber Threat, accessed the 28th of June 2024, from: https://www.fbi.gov/investigate/cyber

European Parliamentary Research Service (2024) Understanding Cybercrime, Briefing EU policies insight, πρόσβαση την 30/6/2024 από το: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Garrett, B., Mallia MPH-E.and Anthony, J. (2019A) Public perceptions of Internet-based health scams, and factors that promote engagement with them, Health Soc Care Community, 27, 672–686.

Garrett, B., Murphy, S., Jamal, S., MacPhee, Reardon, J., Cheung, W., Mallia, E.,and Jackson, C. (2019B) Internet health scams—Developing a taxonomy and risk-of-deception assessment tool, Health Soc Care Community, 27, 226–240

Garg, V. and Nilizadeh, S. (2013) Craigslist Scams and Community Composition: Investigating Online Fraud Victimization, 2013 IEEE Security and Privacy Workshops, DOI: 10.1109/SPW.2013.21

Genc, Y., Kour, H., Arslan, H.T. and Chen, L.-C. (2021) Understanding Nigerian e-mail scams: A computational content analysis approach, Information Security Journal: A Global Perspective, 30 (2), 88-99, DOI:10.1080/19393555.2020.1804647

Gopal, R.D., Hojati, A., Patterson, R.A. (2022) Analysis of third-party request structures to detect fraudulent websites, Decision Support Systems 154, 113698

Gordon, S. and Ford, R. (2006) On the definition and classification of cybercrime, Journal in Computer Virology, 2, 13–2

Grazioli, S. and Jarvenpaa, S.L. (2003) Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence, International Journal of Electronic Commerce, 7 (4), 93-118, DOI:10.1080/10864415.2003.11044283

Hansen, S.N. (2024) “More intelligent, less emotive and more greedy”: Hierarchies of blame in online fraud, International Journal of Law, Crime and Justice 76, 100652

Kshetri, N. (2022) Scams, Frauds and Crimes in the Nonfungible Token Market, Computing’s Economics, D.O.I. 10.1109/MC.2022.3144763

Kshetri, N. (2013) Cybercrime and cyber-security issues associated with China: some economic and institutional considerations, Electron Commer Res, 13, 41–69, DOI 10.1007/s10660-013-9105-4

Kubilay, E., Raiber, E., Spantig, L. Cahl, J, and Kaaria, L. (2023) Can you spot a scam? Measuring and improving scam identification ability, Journal of Development Economics,165, 103147

Lazarus, S., Whittaker, J.M. and McGuire, M.R. (2023) What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021), Journal of Economic Criminology, 2, 100013

Mabunda, S. (2018) Cryptocurrency: The new face of cyber money laundering, 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD): Durban, South Africa http://dx.doi.org/10.1109//ICABCD.2018.8465467

Manasrah,A., Akour, M. and Alsukhni, E. (2015) Toward Improving University Students Awareness of Spam Email and Cybercrime: Case Study of Jordan, IEEE, 1-6

Meikle, W. and Cross, C. (2024) What action should I take?": Help-seeking behaviours of those targeted by romance fraud, Journal of Economic Criminology, 3, 100054

Nataraj-Hansen, S. (2024) More intelligent, less emotive and more greedy: Hierarchies of blame in online fraud, International Journal of Law, Crime and Justice 76, 100652

Oates, B. (2001) Cyber Crime: How Technology Makes It Easy and What to Do About It, Information Systems Security, 9 (6), 1-6, DOI:kk10.1201/1086/43298.9.6.20010102/30989.8

Olmstead, K. (2019) Internet Society's Online Trust Alliance 2018 Cyber Incidents & Breach Trends Report, πρόσβαση την 1/6/2024 από https://www.internetsociety.org/blog/2019/07/internet-societys-online-trust-alliance-2019-cyber-incidents-breach-trends-

report/?gad_source=1&gclid=CjwKCAjwjeuyBhBuEiwAJ3vuoayp2NK5xAnN24DkfsuqiP2b1o8nlDL6B94XalMVMgkVrGQyY0nqNhoCFD8QAvD_BwE

Vahdati, S. and Yasini N. (2015) Factors affecting internet frauds in private sector: A case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran, Computers and Human Behavior, 51, 180–187

Vlachos, V., Minou, M., Asimakopoulos, V. and Toska, A. (2011) The landscape of cybercrime in Greece, 19 (2), 113-123, DOI 10.1108/09685221111143051

Zhang, Y. and Dong, H. (2023)Criminal law regulation of cyber fraud crimes—from the perspective of citizens' personal information protection in the era of edge computing, Journal of Cloud Computing: Advances, Systems and Applications, 12, 64, https://doi.org/10.1186/s13677-023-00437-3

Zhu, Ch., Zhang , Ch., Wang, R., Tian, J., Hu, R. , Zhao, J. , Ke, Y. , Liu, N. (2023) Building of safer urban hubs: Insights from a comparative study on cyber telecom scams and early warning design, Urban Governance 3, 200–210

Xia,P., Wang,H., Zhang,B., Ji,R., Gao,B. , Wu,L., Luo,X., Xu,G. (2020) Characterizing cryptocurrency exchange scams, Computers & Security, 98, 101993

Yin, H.S. and Vatrapu, R. (2017) A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning, in Proc. IEEE Int. Conf. BigData (BigData), Dec (2017), pp. 3690-3699.

Δράκος, Ν. (2022) Ομιλία στο συνέδριο Κυβερνοέγκλημα- Απειλές, Τάσεις και Μελλοντικές προκλήσεις, πρόσβαση την 29η Ιουνίου από https://www.youtube.com/watch?v=JHPxmPyT34&ab_channel=ISACAAthensChapter

Ίσαρη, Φ. και Πούρκος, Μ. (2015) Ποιοτική Μεθοδολογία Έρευνας: Εφαρμογές στην Ψυχολογία και την Εκπαίδευση, Κάλλιπος, πρόσβαση από https://repository.kallipos.gr/bitstream/11419/5826/3/15327_Isari-KOY.pdf

Ναυτεμπορική (2023) Ασύλληπτο το κόστος των κυβερνοεγκλημάτων, ξεπερνά τα 10 τρισ. το 2023, 25/4/2023, πρόσβαση την 19/6/2023 από https://www.naftemporiki.gr/techscience/1464355/asyllipto-to-kostos-ton-kyvernoegklimaton-xeperna-ta-deka-tris-to-2023/

Οικονομικός Ταχυδρόμος (2024) Δίωξη ηλεκτρονικού εγκλήματος: προσοχή στις απάτες με τα κρυπτονομίσματα, πρόσβαση την 28/2/2024 από: https://www.ot.gr/2021/06/28/epikairothta/koinonia/dioksi-ilektronikou-egklimatos-prosoxi-stis-apates-me-ta-kryptonomismata/

Παπαγεωργίου, Ι. (2015) Θεωρία δειγματοληψίας, Κάλλιπος, πρόσβαση από https://repository.kallipos.gr/handle/11419/1296

Υπουργείο Ψηφιακής Διακυβέρνησης (2020) Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, Εθνική Αρχή Κυβερνοασφάλειας, Δεκέμβριος 2020, πρόσβαση την 28/2/2024 από https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

Χαλικιάς, Μ., Μανωλέσσου, Α. και Λάλου, Π. (2015) Μεθοδολογία Έρευνας και Εισαγωγή στην Στατιστική Ανάλυση Δεδομένων με το IBMSPSS Statistics, Εκδόσεις Κάλλιπος, Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα

ΠΑΡΑΡΤΗΜΑ: ΤΟ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Ερωτηματολόγιο

Η δημόσια ασφάλεια είναι μια υπόθεση τόσο δημόσια όσο και ατομική. Στην Ελλάδα, ολοένα και συχνότερα συμβαίνει οι χρήστες του διαδικτύου να θυματοποιούνται μέσω της χρήσης του. Για παράδειγμα δέχονται μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου (e-mails), τηλεφωνήματα (που σε επόμενο στάδιο ζητούν τη χρήση του υπολογιστή) ή μηνύματα μέσω εφαρμογών σε κοινωνικά δίκτυα (όπως το Facebook, το Instagram κ.ά.) από αγνώστους με κακόβουλες προθέσεις που επιδιώκουν συνήθως να τους αποσπάσουν χρηματικά ποσά. Οι ενέργειες αυτές είναι ενοχλητικές και κακόβουλες και αποκαλούνται στη βιβλιογραφία «παρενοχλήσεις». Πρόκειται για μια κατηγορία κυβερνοεγκλήματος.

Με βάση την προσωπική σας εμπειρία απαντήστε στις ερωτήσεις του ακόλουθου ερωτηματολογίου που πραγματοποιείται από το Πανεπιστήμιο Δυτικής Μακεδονίας, στα πλαίσια της μεταπτυχιακής μου εργασίας.

Σας ευχαριστώ εκ των προτέρων για την πολύτιμη βοήθεια και τον χρόνο σας.

Χουλιαρά Μαρία - Ελένη

1.Ποιο είναι το φύλο σας;

- Άντρας
- Γυναίκα
- Δεν επιθυμώ να το αναφέρω

2.Ποιο είναι το μορφωτικό σας επίπεδο;

- Μεταπτυχιακός/Διδακτορικός τίτλος
- Πτυχίο ΑΕΙ/ΤΕΙ
- Δευτεροβάθμια εκπαίδευση
- Υποχρεωτική εκπαίδευση

3.Τι ηλικία έχετε;

- Ως 20 ετών
- 21-35
- 36-50

- 51-65
- 66+

4.Σε ποια περιοχή της Ελλάδας βρίσκεται η μόνιμη κατοικία σας;

- Ήπειρος
- Μακεδονία και Θράκη
- Κεντρική Ελλάδα και Θεσσαλία
- Αττική
- Πελοπόννησος
- Νησιά
- Άλλο:

5.Έχετε δεχθεί κακόβουλη «επίθεση» ή άλλη ενέργεια παρενόχλησης η οποία έχετε αντιληφθεί ότι αποσκοπεί στην θυματοποίησή σας; (δώστε μια ή περισσότερες απαντήσεις)

- Ναι, στο e-mail μου
- Ναι, μέσω τηλεφώνου
- Ναι, από μέσο κοινωνικής δικτύωσης που χρησιμοποιώ
- Ναι, κατά την επίσκεψή μου σε μια ιστοσελίδα ή στην προσωπική ιστοσελίδα που διαθέτω
- Δεν έχω δεχτεί κάποια «παρενόχληση»
- Άλλο:

6.Πως θα χαρακτηρίζατε την παραπάνω παρενόχληση ή τις παρενοχλήσεις που δεχτήκατε; (δώστε μια ή περισσότερες απαντήσεις)

- Επιβλαβή για εμένα και την οικογένειά μου
- Επικίνδυνη/Σοβαρή απειλή
- Ασήμαντη/Αδιάφορη για εμένα
- Αλλοπρόσαλλη/Περίεργη/Ανόητη
- Δεν έχω δεχτεί κάποια «παρενόχληση»
- Άλλο:

7.Την στιγμή που δεχτήκατε μια παρενόχληση πως τη θεωρήσατε; (δώστε μια ή περισσότερες απαντήσεις)

- Δεν αντιλήφθηκα τίποτε αλλά το κατάλαβα εκ των υστέρων
- Την απέφυγα αμέσως
- Την απέφυγα μετά από λίγο
- Με έπεισαν αλλά δεν με εκμεταλλεύτηκαν
- Έπεσα θύμα και με εκμεταλλεύτηκαν
- Δεν έχω δεχτεί κάποια «παρενόχληση»
- Άλλο:

8.Απευθυνθήκατε στην Ελληνική Αστυνομία για την αντιμετώπιση μιας τέτοιας παρενόχλησης;

- Ναι, σε κάποιες περιπτώσεις
- Το επιχείρησα αλλά εγκατέλειψα την προσπάθεια
- Ναι, οποτεδήποτε συνέβη
- Όχι, ποτέ δεν ανακάτεψα την αστυνομία
- Δεν έχω δεχτεί κάποια «παρενόχληση»
- Άλλο:

9.Τι από τα παρακάτω σάς έχει συμβεί, με τη χρήση υπολογιστή (συμπεριλαμβανομένης της χρήσης e-mail, τηλεφωνήματος πριν τη χρήση του υπολογιστή ή της χρήσης ενός μέσου κοινωνικής δικτύωσης- socialmedia); (δώστε μια ή περισσότερες απαντήσεις)

- Μού ζητήθηκε κατάθεση χρημάτων σε λογαριασμό στο εξωτερικό, με χρηματικό αντάλλαγμα
- Μού έγινε ενημέρωση για την απόκτηση εύκολων χρημάτων λειτουργώντας ως διαμεσολαβητής για κάποιον άλλο
- Μού ζητήθηκε να συμμετάσχω σε αγοραπωλησία κρυπτονομισμάτων
- Μού ζητήθηκε να συμμετάσχω σε πυραμίδα κατάθεσης χρημάτων, από την οποία περισσότερο θα επωφελούνταν ο ιεραρχικά ανώτερος (πυραμίδα Ponzi)
- Μού ζητήθηκε να εργαστώ σε εργασία, ξεκινώντας με δική μου δαπάνη
- Μού ζητήθηκε να παραλάβω κληρονομιά που δήθεν κληρονόμησα

- Μου ζητήθηκε δήθεν να επιστρέψω χρήματα, να καταβάλω φόρο, να διευθετήσω χρηματικά υπόλοιπα σε σχέση με δημόσια υπηρεσία (ΑΑΔΕ ή άλλη)
- Ενημερώθηκα ότι δήθεν κέρδισα κάποιον λαχνό ή λαχείο και θα χρειαστεί να παραλάβω τα χρήματα που κέρδισα
- Έχω επισκεφτεί ιστοσελίδα που ήταν ψεύτικη με σκοπό την εκμετάλλευση του καταναλωτή
- Με προσέγγισαν για ένα τελείως ανύπαρκτο προϊόν ή υπηρεσία
- Μού ζητήθηκε να αποκαλύψω προσωπικά δεδομένα μου και πληροφορίες που με αφορούν (phishing)
- Μου ζήτησαν χρήματα (λύτρα) για να απελευθερώσουν τον υπολογιστή μου, ο οποίος είχε προηγουμένως παραβιαστεί με κάποιου είδους ιό ή άλλο κακόβουλο λογισμικό (ransomware)
- Μου ζήτησαν χρήματα με πρόφαση λόγους υγείας (για τα οποία χρειάστηκε να χρησιμοποιήσω τον υπολογιστή)
- Έχω επισκεφτεί ιστοσελίδα για ρομαντικές γνωριμίες που είτε ήταν ψεύτικη είτε επιχείρησαν ψευδώς να τους εξαπατήσουν μέσω αυτής
- Δεν έχω δεχτεί κάποια «παρενόχληση»

10.Εκτός των χρημάτων τι τύπου παρουσιάζονται ότι είναι οι συχνότερες παρενοχλήσεις που έχετε δεχθεί στο διαδίκτυο; (δώστε μια ή περισσότερες απαντήσεις)

- Σχετικές με υποτιθέμενη δική μου παράνομη δραστηριότητα (ή ανάλογα άλλου θύματος)
- Σχετικές με την προστασία της ασφάλειας, της προσωπικής ζωής και ιδιωτικότητας
- Σχετικές με κοινωνικές εκδηλώσεις (π.χ. εθελοντισμού) και τον κοινωνικό μου περίγυρο
- Σχετικές με τον ερωτικό τομέα
- Σχετικές με την θρησκεία (Χριστιανισμός ή άλλη) ή τη γενικότερη ιδεολογία μου
- Κανένα από τα παραπάνω
- Δεν έχω δεχτεί κάποια «παρενόχληση»

- Άλλο:

11.Τι από τα παρακάτω σάς έχει συμβεί μέσα από μια παρενόχληση/«επίθεση» με τη χρήση υπολογιστή(συμπεριλαμβανομένης της χρήσης e-mail, τηλεφώνου ή μέσου κοινωνικού δικτύου); (δώστε μια ή περισσότερες απαντήσεις)

- Έχασα μικρά χρηματικά ποσά
- Έχασα μεγάλα χρηματικά ποσά ή ολόκληρη την περιουσία μου
- Πλήγηκε η υπόληψη μου στην κοινωνία
- Ένιωσα πολύ άσχημα συναισθηματικά
- Κατέρρευσα συναισθηματικά και υπέστην σοβαρές ψυχολογικές συνέπειες
- Δεν είχα καμία επίπτωση
- Δεν έχω δεχτεί κάποια «παρενόχληση»

12.Με ποιον ή ποιους από τους ακόλουθους τρόπους σάς προσέγγισαν προκειμένου να σας εκμεταλλευτούν μέσω μιας κακόβουλης ενέργειας;(δώστε μια ή περισσότερες απαντήσεις)

- Υποσχέθηκαν χρήματα, ανταμοιβές ή εύκολο πλουτισμό
- Υποσχέθηκαν επιτυχία στην πιθανή εύρεση συντρόφου
- Επιδίωξαν να δημιουργήσουν φιλική σχέση και επικοινωνία μαζί σας
- Προσποιήθηκαν ότι είναι συγγενικό, φιλικό πρόσωπο ή κάποιοι άλλοι
- Παρουσίασαν τους εαυτούς τους (ή άλλα πρόσωπα) ως επιτυχημένους χάρις την χρήση της υπηρεσίας ή της εργασίας που επιδίωκαν να σας πρόσφεραν
- Προσπάθησαν να αποκρύψουν κρίσιμες πληροφορίες, να σας "ζαλίσουν" σκοπίμως με βροχή πληροφοριών ή να χρησιμοποιήσουν παραπλανητικές πληροφορίες
- Προσπάθησαν να σας πείσουν ότι τελικά εσείς θα εκμεταλλευτείτε αυτόν ή αυτούς που σας προσέγγισαν αν προβείτε στην προτεινόμενη συναλλαγή
- Κανέναν από τα παραπάνω
- Δεν έχω δεχτεί κάποια «παρενόχληση»
- Άλλο:

13.Ποιες από τις παρακάτω στρατηγικές πειθούς έχουν χρησιμοποιήσει σε βάρος σας χρήστες του διαδικτύου με τους οποίους ήρθατε σε επαφή και επιδίωξαν να σας εκμεταλλευτούν με κάποιο τρόπο; (δώστε μια ή περισσότερες απαντήσεις)

- Έδειχναν ότι θέλουν να γνωρίσουν από κοντά εσάς
- Επικοινωνούσαν καθημερινά μαζί σας
- Σας ρωτούσαν συχνά για την προσωπική σας ζωή και έδειχναν ενδιαφέρον για οτιδήποτε σας αφορά
- Αναζητούσαν τα κοινά σημεία σύνδεσης με εκείνους
- Έδειχναν ότι ενδιαφέρονται για τα προβλήματά σας
- Σας παρουσίασαν στοιχεία, εικόνες ή άλλα τεκμήρια από τη δράση τους που τις καθιστούσαν αξιόπιστες
- Χρησιμοποιούσαν ψεύτικες ιστοσελίδες που φαινόταν αληθοφανείς
- Σας απείλησαν
- Σας κατηγόρησαν ότι έχετε παράνομη συμπεριφορά και ότι θα συλληφθείτε και για να αποφύγετε την σύλληψη θα χρειαστεί να επικοινωνήσετε μαζί τους
- Σας πρόσβαλλαν/σας υποτίμησαν
- Σας πρόσφεραν κάποιο κουπόνι ή άλλο δώρο
- Υποσχέθηκαν την εύρεση ιδανικού συντρόφου και αποκλειστικότητα στην επικοινωνία με ερωτικό σύντροφο
- Δεν έχω δεχτεί κάποια «παρενόχληση»

14.Πόσο συχνά δέχεστε παρενόχληση στο e-mail σας, από το τηλέφωνο ή μέσω εφαρμογής κοινωνικού δικτύου; (μια απάντηση)

- Ποτέ
- Σπάνια
- Συχνά
- Πολύ συχνά
- Καθημερινά
- Άλλο:

15.Γιατί λαμβάνουν χώρα οι παρενοχλήσεις μέσω της χρήσης του διαδικτύου; (δώστε μια ή περισσότερες απαντήσεις)

- Έχει αναπτυχθεί πολύ η τεχνολογία κατά τα τελευταία χρόνια
- Αντίθετα με την ανάπτυξη της τεχνολογίας, δεν έχουν αναπτυχθεί τα μέσα προφύλαξης από τέτοιες παρενοχλήσεις
- Υπάρχει μεγάλη δυσκολία στον έλεγχο των περιστατικών
- Έχει εξελιχθεί πολύ η εγκληματική δραστηριότητα
- Δεν έχει ανταποκριθεί στο ρόλο της η Ελληνική Αστυνομία και οι Δημόσιες Αρχές
- Πρόκειται για διεθνικές δραστηριότητες που δυσχεραίνουν την παρέμβαση των Αρχών
- Δεν υπάρχει επαρκής ενημέρωση των καταναλωτών
- Δεν υπάρχει η κατάλληλη εκπαίδευση και γνώση των καταναλωτών για την ασφαλή χρήση του διαδικτύου
- Οι καταναλωτές δεν επιδιώκουν να μοιραστούν τις άσχημες εμπειρίες τους από την παρενόχλησή τους ώστε να γίνουν παραδείγματα προς αποφυγή
- Υπάρχουν ευκολόπιστα θύματα που ευνοούν τη συνέχιση των παρενοχλήσεων
- Πολλά από τα προσωπικά μας στοιχεία είναι πλέον έκθετα σε πολλούς
- Αγοράζονται και πωλούνται προσωπικά στοιχεία και δεδομένα
- Τίποτε από τα παραπάνω
- Άλλο:

16.Σε ποιο βαθμό συμφωνείτε ότι η Ελληνική Αστυνομία και το Υπουργείο Προστασίας του Πολίτη επιτυγχάνει την προστασία των χρηστών του διαδικτύου από επιθέσεις και άλλες παρενοχλήσεις;

(Συμφωνώ απόλυτα) 1 2 3 4 5 (Διαφωνώ απόλυτα)

17. Μέσα από τις πολιτικές της Δημόσιας Διοίκησης και της Ελληνικής Αστυνομίας που εστιάζουν στην παροχή του αγαθού της δημόσιας ασφάλειας μπορεί να επιτευχθεί ο συστηματικός περιορισμός των παρενοχλήσεων των χρηστών του διαδικτύου;

(Συμφωνώ απόλυτα) 1 2 3 4 5 (Διαφωνώ απόλυτα)

18.Για ποιον ή ποιους λόγους δεν επιτυγχάνεται η πλήρης προστασία των χρηστών του διαδικτύου από κυβερνοεπιθέσεις παρενόχλησης από το διαδίκτυο; (δώστε μια ή περισσότερες απαντήσεις)

- Έλλειψη γνώσεων και ανεπάρκεια της δημόσιας διοίκησης για τις απειλές από το διαδίκτυο
- Τα ίδια τα προβλήματα παρενόχλησης και κυβερνοεπίθεσης είναι σύνθετα
- Οι τρόποι παρενόχλησης και κυβερνοεπίθεσης είναι πολλοί και διαρκώς εφευρίσκονται καινούργιοι
- Το έγκλημα δεν έχει σύνορα
- Η δράση των αρχών (αστυνομία, εκπαίδευση, φορείς) δεν είναι προσαρμοσμένη στην εποχή μας
- Υπάρχει ανάγκη σε εξειδικευμένο προσωπικό σε θέματα κυβερνοασφάλειας
- Δεν υπάρχει συνεργασία μεταξύ των φορέων που εμπλέκονται στην καταπολέμηση του κυβερνοεγκλήματος
- Όλοι οι παραπάνω λόγοι