ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
ΤΟ ΕΜΠΟΡΙΟ ΤΗΣ ΑΝΘΡΩΠΙΝΗΣ ΖΩΗΣ ΣΤΗΝ ΨΗΦΙΑΚΗ ΚΟΙΝΩΝΙΑ

ΑΝΤΩΝΙΑ ΦΩΤΟΠΟΥΛΟΥ Α.Μ. 3152

Επιβλέπων Καθηγητής : Ασημακόπουλος Γεώργιος

ΠΑΤΡΑ 2023

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Πάτρα, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία. Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος. Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία της φοιτήτριας ΑΝΤΩΝΙΑΣ ΦΩΤΟΠΟΥΛΟΥ που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας /δημιουργός εκχωρεί στο Πανεπιστήμιο Πελοποννήσου, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ’ οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας /δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία πραγματοποιήθηκε στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου . Αρχικά, χρωστάω ένα μεγάλο ευχαριστώ στον καθηγητή μου, κ. Γεώργιο Ασημακόπουλο, που μου έδωσε τη δυνατότητα να μπορέσω να πραγματοποιήσω τη συγκεκριμένη πτυχιακή εργασία καθώς και για τη στήριξη του όλο αυτό τον καιρό. Επίσης θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στους γονείς και την αδερφή μου για την πολύτιμη υποστήριξή και καθοδήγηση κατά την εκπόνηση της πτυχιακής μου εργασίας. Η ενθάρρυνση, η οξυδερκής ανατροφοδότηση και η ακλόνητη πίστη στις ικανότητές μου με βοήθησαν να παραμείνω συγκεντρωμένη σε όλη τη διάρκεια του ακαδημαϊκού ταξιδιού. Αναγνωρίζω τις θυσίες που έκαναν οι γονείς μου, οι οποίοι μου παρείχαν τους απαραίτητους πόρους, συναισθηματική υποστήριξη και ενθάρρυνση για να επιδιώξω τους ακαδημαϊκούς μου στόχους. Η καθοδήγηση και η τεχνογνωσία των καθηγητών μου συνέβαλαν καθοριστικά στη διαμόρφωση των ερευνητικών μου δεξιοτήτων, της ικανότητας κριτικής σκέψης και της συνολικής ακαδημαϊκής μου ανάπτυξης. Είμαι πραγματικά ευγνώμων για τη συνεισφορά τους και περήφανη που τους είχα ως πρότυπα και υποστηρικτές μου.

ABSTRACT

The advent of social media, the dark web, cryptography, and online games has transformed the way people communicate and interact with each other. While social media platforms offer a plethora of benefits, they can also be a breeding ground for fake news and victimization of vulnerable people, especially children and teenagers. Cyber bulling, online death games, grooming and sextortion are some of the criminal activities one encounters on the Internet. The dark web, on the other hand, is a murky and unregulated corner of the internet where illegal activities such as drug trafficking, human trafficking, and money laundering take place. Cryptography, which can be used for secure communication, also has its fair share of misuse in criminal activities. It must be understood that while technological advancements come with great benefits, it is important to be aware of their potential dangers and use them responsibly.

ΠΕΡΙΛΗΨΗ

Η έλευση των μέσων κοινωνικής δικτύωσης, του σκοτεινού ιστού, της κρυπτογραφίας και των διαδικτυακών παιχνιδιών έχει αλλάξει τον τρόπο με τον οποίο οι άνθρωποι επικοινωνούν και αλληλεπιδρούν μεταξύ τους. Ενώ οι πλατφόρμες Μέσων Κοινωνικής Δικτύωσης προσφέρουν μια πληθώρα πλεονεκτημάτων, μπορούν επίσης να αποτελέσουν πρόσφορο έδαφος για ψεύτικες ειδήσεις και θυματοποίηση ευάλωτων ατόμων κυρίως παιδιών και εφήβων. Cyber bulling, διαδικτυακά παιχνίδια θανάτου, grooming και sextortion είναι μερικές από τις εγκληματικές ενέργειες που συναντά κανείς στο διαδίκτυο. Ο σκοτεινός ιστός, από την άλλη πλευρά, είναι μια θολή και άναρχη γωνιά του Διαδικτύου όπου λαμβάνουν χώρα παράνομες δραστηριότητες όπως η διακίνηση ναρκωτικών, η εμπορία ανθρώπων και το ξέπλυμα χρήματος. Η κρυπτογραφία, η οποία μπορεί να χρησιμοποιηθεί για ασφαλή επικοινωνία, έχει επίσης μερίδιο κακής χρήσης της σε εγκληματικές δραστηριότητες. Πρέπει να γίνει κατανοητό ότι ενώ οι τεχνολογικές εξελίξεις συνοδεύονται από μεγάλα οφέλη, είναι σημαντική η συνεχής ενημέρωση για πιθανούς κινδύνους και υπεύθυνη χρήση.

ΚΕΦΑΛΑΙΟ 1ο : ΨΗΦΙΑΚΑ ΜΕΣΑ

❖ 1.1 Διαδίκτυο (Internet)

Το Διαδίκτυο αναμφίβολα είναι ένα από τα σπουδαιότερα κομμάτια εξέλιξης και τεχνολογικής προόδου σε ολόκληρο τον πλανήτη και είναι άρρηκτα συνδεδεμένο με τα ψηφιακά μέσα. Με την ανακάλυψη του παρουσιάστηκε στον κόσμο ολόκληρο ένα ευρύ φάσμα από άγνωστες τεχνολογικές προσθήκες που μέχρι τότε κανείς δεν είχε φανταστεί πως θα υπάρξουν. Πιο συγκεκριμένα, το Διαδίκτυο είναι μία παγκόσμια συλλογή από εκατομμύρια δίκτυα τα οποία διαφέρουν σε μέγεθος και έχουν ποικίλες μορφές, είναι διασυνδεδεμένα μεταξύ τους μέσω ενός καθορισμένου συνόλου από κανόνες που ονομάζονται πρωτόκολλα επικοινωνίας. Το καθένα από τα δίκτυα μπορεί και ασκεί δική του πολιτική οργάνωσης ανάλογα με τις απαιτήσεις και τη χρήση. Ένα σύνολο από διασυνδεδεμένες συσκευές ουσιαστικά δημιουργούν το Διαδίκτυο, οι οποίες επικοινωνούν μεταξύ τους σε παγκόσμια κλίμακα. Με αυτόν τον τρόπο επιτρέπεται η ανταλλαγή δεδομένων μεταξύ οποιωνδήποτε διασυνδεδεμένων συσκευών. Οι συσκευές αυτές είναι σε όλους μας γνωστές αφού καλύπτουν τις πιο πολλές μας καθημερινές ανάγκες, όπως οι προσωπικοί μας υπολογιστές (PCs & Laptops), τα έξυπνα κινητά τηλέφωνα (smartphones) και τα tablets. Επίσης υπάρχουν και εξυπηρετητές (servers) οι οποίοι καλύπτουν κρατικές ανάγκες και ανάγκες εταιριών. Το Διαδίκτυο και οι συσκευές που το ακολούθησαν είναι αναμφίβολα αναπόσπαστο κομμάτι της καθημερινής ζωής για πολλούς ανθρώπους γιατί πάνω σε αυτό έχουν στηριχθεί αμέτρητες δραστηριότητες που αφορούν την επικοινωνία, την εργασία, την εκπαίδευση, την ιατρική, τις δημόσιες υπηρεσίες , την ενημέρωση, την ψυχαγωγία και ότι έχει να κάνει με τη διευκόλυνση της ζωής στην εποχή αυτή. Γνωρίζουμε πως η κοινωνία έχει αναπτύξει ένα μεγάλο μέρος της λειτουργικότητάς της λόγω της προσθήκης της ψηφιακής κοινωνίας. Μέσα από τις συσκευές ανοίγεται ένας ψηφιακός κόσμος γεμάτος δυνατότητες. Έτσι, το Διαδίκτυο έχει γίνει συνώνυμο με την αναπτυσσόμενη ψηφιακή τεχνολογία και οι πληροφορίες που διακινούνται σε αυτό είναι υπεράριθμες. Είναι κατανοητό πως δεν υπάρχει κανένας άμεσος έλεγχος των πληροφοριών που κατακλύζουν το Διαδίκτυο από κάποιο φορέα. Θα δούμε παρακάτω τι θετικές ή αρνητικές συνέπειες επέφερε στις ζωές μας αυτή η ελευθερία κινήσεων μέσα στην ψηφιακή κοινωνία. Σίγουρα η κοινωνία δεν έχει αντιληφθεί ακόμα το εύρος της επίδρασης του Διαδικτύου και θα χρειαστούν ακόμα κάποια χρόνια για να υπάρχει μια ξεκάθαρη σύγκριση με τον παρελθόν. Η ραγδαία εξέλιξη της τεχνολογίας δεν έχει αφήσει

περιθώρια σύγκρισης γιατί η προσαρμοστικότητα του περιβάλλοντος γίνεται αυτόματα ελεγχόμενη και καταργούνται τα εμπόδια του χρόνου και του χώρου.

Τέλος, ο ψηφιακός κόσμος του Διαδικτύου διακατέχεται από δικούς του νόμους οι οποίοι χρειάστηκαν να θεσπιστούν για να καθορίζουν τη σωστή συμπεριφορά των ανθρώπων κα της κοινωνίας ολόκληρης απέναντι σε όλα τα μέλη που το απαρτίζουν. Θα διακρίνουμε και στα επόμενα κεφάλαια, ότι οι νόμοι και ο ορισμός της σωστής συμπεριφοράς μέσα στην ψηφιακή κοινωνία δεν είχαν γερά θεμέλια. Όπως και στην πραγματική ζωή υπάρχουν εγκλήματα έτσι και στον ψηφιακό κόσμο πολλοί προσπάθησαν και κατάφεραν να φέρουν και να εδρεύσουν αθέμιτες συμπεριφορές, οι οποίες παραβιάζουν το δίκαιο, προσβάλλουν και καταπατούν την έννοια της προσωπικής ζωής.

❖ 1.1.1 Ιστορική Αναδρομή

Για να φτάσουμε στο σήμερα και να θεωρούμε το Διαδίκτυο ένα κομμάτι της καθημερινότητας, υπάρχουν πολλά στάδια ιστορίας για το πως ξεκίνησε σαν ιδέα, ποιος ήταν ο αρχικός του σκοπός και πως μέσα από τα χρόνια άρχισε να διαδίδεται ταχύτατα από χώρα σε χώρα και από ήπειρο σε ήπειρο. Το Διαδίκτυο σε καμία περίπτωση δεν ξεκίνησε για να παρέχει υπηρεσίες στους απλούς πολίτες, έτσι η μορφή που είχε τότε και οι δυνατότητες του δεν μοιάζουν με αυτές του σήμερα.

Η ιστορία ξεκινά όταν μέχρι τα μέσα της δεκαετίας του 1950, οι ΗΠΑ θεωρούσαν ότι ήταν εξαιρετικά ανώτεροι τεχνολογικά από τον μεγαλύτερο εκείνης της εποχής εχθρό τους, την Σοβιετική Ένωση. Η άποψή τους διαψεύστηκε στις 4 Οκτωβρίου 1957 όταν οι Σοβιετικοί εκτόξευσαν στο διάστημα τον Sputnik 1 και τον έθεσαν σε τροχιά Γης ως ένα τεχνητό δορυφόρο της. Όταν το 1961 οι Σοβιετικοί με το πρόγραμμα Vostok-1 έστειλαν τον πρώτο άνθρωπο στο διάστημα προκάλεσαν μεγάλη ανησυχία στους Αμερικανούς που θεώρησαν πως ήταν ευάλωτοι σε μια πιθανή επίθεση με πυρηνικά όπλα από το διάστημα. Συνέπεια αυτών των γεγονότων ήταν στις ΗΠΑ να δημιουργηθούν, να ενισχυθούν και να αυξηθούν τα στρατιωτικά προγράμματα. Έτσι ξεκίνησε ένα στρατιωτικό πρόγραμμα, με σκοπό τη δημιουργία ενός επικοινωνιακού δικτύου, που θα έδινε τη δυνατότητα σε στρατιωτικούς να έχουν απρόσκοπτη και συνεχή επικοινωνία μεταξύ τους σε περίπτωση πυρηνικού πολέμου. Ο σχεδιασμός και η κατασκευή αυτού του προγράμματος θα ήταν τέτοιος ώστε αν ένα κομμάτι του καταστρεφόταν, οι πληροφορίες θα έφταναν στο δέκτη μέσω κάποιου άλλου δρόμου αποφεύγοντας το

κατεστραμμένο τμήμα. Το δίκτυο που κατασκευάστηκε, εδραιώθηκε με την ονομασία ARPANET (Advanced Research Project Agency NETwork) και επί της ουσίας ήταν ο πρώτος πυλώνας για την ανάπτυξη του σημερινού Διαδικτύου. Το πρόγραμμα ξεκίνησε το 1961 και ολοκληρώθηκε το 1969 με χρηματοδότηση από το Υπουργείο Άμυνας των ΗΠΑ. Η αρχική του μορφή έφερε μια νέα τεχνολογία εκείνη την εποχή, την μεταγωγή πακέτων (packet switching), όπου τα δεδομένα για να μεταδοθούν διαιρούνται σε πακέτα με αποτέλεσμα πολλοί χρήστες να μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή.

Επόμενος σταθμός για την βελτίωση του Διαδικτύου ήταν το 1973, όπου ένα νέο ερευνητικό πρόγραμμα έκανε την εμφάνισή του με τίτλο Intermeeting Project (Πρόγραμμα Διαδικτύωσης). Σκοπός ήταν να δημιουργήσει ένα κοινό πρωτόκολλο μεταξύ των δικτύων. Με την έρευνα αυτή ήρθε στην επιφάνεια μια νέα τεχνική το Internet Protocol IP (Πρωτόκολλο Διαδικτύωσης). Τα δίκτυα που χρησιμοποιούν το κοινό αυτό πρωτόκολλο μπορούν να συνδέονται και να ανταλλάσσουν δεδομένα μεταξύ τους σχηματίζοντας ένα Διαδίκτυο. Από το 1974 κατασκευάστηκε και προστέθηκε ακόμα ένα πρωτόκολλο που είναι υπεύθυνο για τον έλεγχο της μετάδοσης των δεδομένων με την ονομασία Transmission Control Protocol TCP (Πρωτόκολλο Ελέγχου Μετάδοσης) από τον Vinton Serf. Δόθηκε έτσι η δυνατότητα να συνδέονται στο ARPANET τριτοβάθμια ιδρύματα και ερευνητικά κέντρα. Το 1984 αναπτυχθήκαν οι κανόνες ονοματοδοσίας DNS (Domain Name System), οι οποίοι ορίζαν ότι κάθε υπολογιστής που θα συνδέεται στο δίκτυο θα παίρνει ένα μοναδικό όνομα και θα μπορεί να τακτοποιηθεί ξεχωριστά. Ένα χρόνο νωρίτερα το 1983 ουσιαστικά παύει ο στρατός να εμπλέκεται σε όλο το δίκτυο ARPANET και διαχωρίζεται ένα τμήμα αυτού που το κρατούν για αποκλειστική χρήση με την ονομασία MILNET (MILitart NETwork). Παρατηρούμε πως η τότε εικόνα του Διαδικτύου αρχίζει να αποκτά κάποια σημάδια ότι αυτό που αρχικά κατασκευάστηκε για ένα και μοναδικό στρατιωτικό σκοπό πλέον αποκτά άλλη ουσία. Εξελίσσετε με καινούργιες τεχνικές και πλησιάζει το σήμερα. Μετά τον διαχωρισμό, το 1985 το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ πήρε υπό την ευθύνη του το δίκτυο ARPANET μετονομάζοντάς το σε NSFNET, αποκτώντας νέες υπηρεσίες ενώ οι πληροφορίες μεταδίδονταν ταχύτερα. Κατά συνέπεια το δίκτυο επεκτάθηκε και σε άλλες πανεπιστημιακές και επιστημονικές κοινότητες ανά τον κόσμο, όπου με την συμμετοχή τους επέκτειναν το NSFNET και δημιουργήσαν δικά τους τοπικά δίκτυα. Είχε ως αποτέλεσμα ακόμα περισσότεροι χρήστες να συνδεθούν σε παγκόσμια κλίμακα. Φτάνουμε στο 1987 όπου η ευθύνη για την λειτουργία του NSFNET περνά σε έναν μη κερδοσκοπικό οργανισμό από πανεπιστήμια των ΗΠΑ το Merit Network Inc. και το δίκτυο παρουσιάζεται σε όλους με την ονομασία Internet

(Διαδίκτυο). Το ενδιαφέρον επεκτάθηκε σε ολόκληρο τον πλανήτη και εξαπλώθηκε με ιλιγγιώδη ταχύτητα χαρίζοντας απλόχερα ανύπαρκτες για την εποχή δυνατότητες.

Το 1993 παρουσιάστηκε με την ονομασία Παγκόσμιος Ιστός (World Wide Web) και τον Απρίλιο του 1995 μετρούσε περισσότερο από 1 εκατομμύριο διασυνδεδεμένους υπολογιστές και παραπάνω από 45 εκατομμύρια χρήστες ανά τον κόσμο. Πρωτοεμφανίζονται τα εμπορικά δίκτυα όπου οποιοσδήποτε πολίτης ενδιαφερόταν να συνδεθεί μπορούσε να το κάνει με μικρό κόστος, μέσω των κοινών τότε τηλεφωνικών γραμμών, αρκεί να διέθετε έναν υπολογιστή και μια συσκευή διασύνδεσης. Κανείς δεν είχε προβλέψει πως από ένα στρατιωτικό πρόγραμμα για την ενίσχυση των ΗΠΑ απέναντι στον εχθρό εκείνης της εποχής, θα κατέληγε μέσα από τεχνολογικά βήματα ανά περιόδους, σε μια απλή χρήση από εκπαιδευτικά ιδρύματα και επιστημονικές κοινότητες και θα εκτοξευόταν σε ένα παγκόσμιο φαινόμενο.

❖ 1.1.2 Παγκόσμιος Ιστός (World Wide Web)

Ένα λάθος που κάνουν πολύ συχνά σχεδόν όλοι είναι πως θεωρούν την έννοια Διαδίκτυο και Παγκόσμιος Ιστός (World Wide Web) δυο ίδιες έννοιες, κάτι που φυσικά δεν ισχύει. Ιστορικά και μόνο αυτές τις δυο έννοιες και τεχνολογίες τις χωρίζουν περίπου 28 χρόνια.

Συγκεκριμένα, *«Παγκόσμιος Ιστός είναι μια τεράστια συλλογή από ψηφιακά έγγραφα (τις ιστοσελίδες) , που βρίσκονται αποθηκευμένα σε υπολογιστές του Διαδικτύου. Το Διαδίκτυο αντίθετα είναι ένα παγκόσμιο δίκτυο υπολογιστών συνδεδεμένων μεταξύ τους»* (http://ebooks.edu.gr/ebooks/v/html/8547/2759/Pliroforiki_A-B-G-Gymnasiou_html-empl/indexA_4_2.html).

Η αρχή της ιδέας και του έργου για τον παγκόσμιο ιστό έγινε από τον Berners-Lee (Sir Timothy John Berners-Lee) το 1989, επικεφαλή μιας επιστημονικής ομάδας στο CERN (Ευρωπαϊκό Εργαστήριο Σωματικής Φυσικής) και τον Robert Cailliau την επόμενη χρονιά. Σκοπός της ερευνητικής ομάδας ήταν η διευκόλυνση ανταλλαγής πληροφοριών μεταξύ ερευνητών και η αρχειοθέτηση των μελετών που εκπονούσαν. Για αυτό τον σκοπό κατασκεύασαν μια σειρά από πρωτοκολλά επικοινωνίας, τα οποία έδιναν την δυνατότητα να μεταφέρονται και να παρουσιάζονται πληροφορίες από έναν υπολογιστή που ήταν συνδεδεμένος στο Διαδίκτυο σε έναν άλλον. Φτάνουμε στις 30 Απριλίου του 1993 με το εργαστήριο του CERN να παρουσιάζει τη δεύτερη σημαντικότερη υπηρεσία, που προσφέρθηκε

στις παροχές του Διαδικτύου, με τον πολίτη / χρήστη να έχει πρόσβαση μέσω του προσωπικού του υπολογιστή.

Οι πληροφορίες στον Παγκόσμιο Ιστό είναι οργανωμένες με τη μορφή ιστοσελίδων (web pages). Το σύνολο των ιστοσελίδων, φωτογραφιών, εικόνων, βίντεο και άλλων ψηφιακών στοιχείων οι οποίες αλληλοσυνδέονται με τη βοήθεια των υπερσυνδέσμων (hyperlinks) αποτελούν τον ιστοχώρο (web site). Κατά βάση για τη δημιουργία ιστοσελίδων και περιεχομένου στον Παγκόσμιο Ιστό χρησιμοποιείτε η γλώσσα σήμανσης HTML. Η περιήγηση στο διαδίκτυο γίνεται με τη χρήση προγραμμάτων ανάγνωσης ιστοσελίδων γνωστά ως φυλλομετρητές (browsers). Από τους πιο διαδεδομένους φυλλομετρητές είναι το Google Chrome, το Microsoft Edge, το Mozilla Firefox, Opera, Netscape Navigator κ.ά.. Ο χρήστης πληκτρολογώντας κάποια λέξη-κλειδί, του εμφανίζεται στην οθόνη μια λίστα με διευθύνσεις ιστοσελίδων.

Ο άνθρωπος κατάφερε να διασυνδεθεί μέσα σε αυτόν τον ψηφιακό κόσμο με την πάροδο του χρόνου καθώς η χρήση του άλλοτε στρατιωτικού προγράμματος εξελίχθηκε, δίνοντας τη δυνατότητα στον απλό χρήστη, εύκολα να εξερευνήσει και να ανακαλύψει ότι για εκείνον πριν λίγο ήταν άγνωστο. Μέσα από τη διασύνδεση με άλλους χρήστες και με τη χρήση του Παγκόσμιου Ιστού κατάφερε μέσα σε λίγα δευτερόλεπτα να βρίσκεται μπροστά σε ότι αναζητεί χωρίς περιορισμούς. Όλοι πλέον έχουν την ευχέρεια να αναζητήσουν πληροφορίες, να επικοινωνήσουν με άτομα σε όλο τον πλανήτη, να αγοράσουν προϊόντα, να ψυχαγωγηθούν, να μοιραστούν σε αυτό φωτογραφίες, βίντεο, σκέψεις και απόψεις από την καθημερινότητά τους.

Όπως και στη κοινωνία υπάρχει η ελευθερία αλλά και το έγκλημα, η καταπάτηση της ανθρώπινης ζωής και η κερδοσκοπία έτσι και σε αυτή την ψηφιακή κοινωνία η απεριόριστη και απόλυτη ελευθερία που δόθηκε σε όλους τους χρήστες, έχει αφήσει χώρο να δημιουργηθεί το ηλεκτρονικό έγκλημα και ένα ευρύ φάσμα από παραβατικές συμπεριφορές.

Εικόνα 1.1 : Μηχανές Αναζήτησης στον Παγκόσμιο Ιστό

❖ 1.2 Dark Web

Στην αντίπερα όχθη του World Wide Web υπάρχει ένας ολόκληρος κόσμος λίγο πιο σκοτεινός όπως προδίδει και το όνομά του, ευρέως γνωστός ως Σκοτεινό Διαδίκτυο (Dark Web). Βέβαια κάπου εδώ πρέπει να αναφερθεί ότι το Dark Web αποτελεί απλά μια υποκατηγορία του Deep Web, στο οποίο υπάγονται όλες οι Ιστοσελίδες που δε θα βρεις ποτέ στις τυπικές μηχανές αναζήτησης όπως Google και Bing και δεν θα μπορέσεις να επισκεφθείς από συμβατικούς Browser όπως Mozilla Firefox, Google Chrome κ.α. Συγκεκριμένα δεν είναι λίγες οι φορές που έχουμε δει να παρομοιάζεται με ένα παγόβουνο, με κορυφή το World Wide Web, μέση το Deep Web και βάση το Dark Web.

Εικόνα 1.2 : Παγόβουνο για την Κατανόηση των Επιπέδων του Διαδικτύου

❖ 1.2.1 Ιστορία και Silk Road

Οι ρίζες του Dark Web προέρχονται από το ομοσπονδιακό κράτος των ΗΠΑ στην απαρχή του ARPANET (Advanced Research Projects Agency Network) την δεκαετία του ’60. Η πρώτη παράνομη δράση έλαβε μέρος το 1970 από μαθητές του Stanford University που έκαναν χρήση λογαριασμών ARPANET στο εργαστήριο Τεχνητής Νοημοσύνης, με σκοπό τη διακίνηση ναρκωτικών ουσιών και συγκεκριμένα μαριχουάνας σε ομόλογούς τους στο MIT (Massachusetts Institute of Technology).

Το περιεχόμενο του Σκοτεινού Ιστού δεν είναι δυνατόν να ευρετηριαστεί από τις μηχανές αναζήτησης, καθώς το περίπλοκο σύστημά του καθιστά ακατόρθωτη την αναπαραγωγή διαδρομής και την αποκρυπτογράφηση πληροφοριών ανά τα επίπεδα, λόγω του υψηλού επιπέδου κρυπτογράφησης. Οι Ιστότοποι δεν είναι σε θέση να προσδιορίσουν τη γεωγραφική τοποθεσία και τη διεύθυνση IP, με αποτέλεσμα η επικοινωνία μεταξύ των χρηστών και η ανταλλαγή εμπιστευτικών δεδομένων να εφαρμόζεται με πλήρη εχεμύθεια και ασφάλεια. Για να καταφέρει ο χρήστης να το προσπελάσει θα πρέπει να διαθέτει έναν ειδικά διαμορφωμένο Browser όπως τον Tor. Ο Tor είναι η πύλη που προσφέρει την πρόσβαση στο κρυμμένο δίκτυο (hidden web). Αναλυτικότερα είναι ένας μηχανισμός δρομολόγησης που σχεδιάστηκε για τη διατήρηση της ανωνυμίας του χρήστη εξαφανίζοντας τα ίχνη του στο Διαδίκτυο, αποκρύπτοντας πληροφορίες αναγνώρισης όπως τοποθεσία, ταυτότητα και συνεπώς το λόγο χρήσης για τον οποίο θέλησε να συνδεθεί στον συγκεκριμένο Browser.

Πολλοί θα αναρωτηθούν αν έχει το Σκοτεινό Διαδίκτυο καλή πλευρά. Η απάντηση είναι βεβαίως θετική και θα απαντηθεί σύντομα το γιατί. Το Dark Web ή Darknet όπως και το ευρύ Διαδίκτυο από μόνο του δεν καθίσταται επικίνδυνο αν δεν χρησιμοποιηθεί με απερισκεψία. Το Σκοτεινό Διαδίκτυο έχει αποτελέσει καταφύγιο έχοντας χρησιμοποιηθεί για νόμιμους σκοπούς ενάντια στη διαφθορά, την καταπίεση και την ανάγκη για απρόσκοπτη ενημέρωση των πολιτών. Άτομα σε χώρες με αυστηρά καθεστώτα όπου η λογοκρισία συναντάται παντού και η τροφοδοσία πληροφορίων οδηγεί το λιγότερο σε φυλάκιση, έχουν τη δυνατότητα είτε να λάβουν είτε να παρέχουν πληροφορίες στον έξω κόσμο. Απαραίτητο πλέον εργαλείο συντελεί για δημοσιογράφους και μυστικούς πράκτορες της αστυνομίας, αφού η αλληλεπίδραση με εγκληματικά στοιχεία λαμβάνει χώρα αβίαστα μέσω των κοινοτήτων που έχουν δημιουργηθεί.

Χαρακτηριστικό παράδειγμα αποτελεί η εξιχνίαση και κατάργηση διαδικτυακής μαύρης αγοράς, με κύριο χαρακτηριστικό της πλατφόρμας τη διακίνηση και πώληση ναρκωτικών ουσιών. Γνωστή με το όνομα Silk Road παρείχε αγαθά και υπηρεσίες σε περισσότερους από 100.000 αγοραστές. Οι χρήστες μπορούσαν να παραγγείλουν από τους εμπόρους οποιαδήποτε παράνομη ναρκωτική ουσία επιθυμούσαν και να την παραλάβουν άφοβα στα σπίτια τους μέσω της Ταχυδρομικής Υπηρεσίας. Οι εν λόγω συναλλαγές πραγματοποιήθηκαν με bitcoins (κρυπτονομίσματα-κεφ.4) για μεγαλύτερη ασφάλεια και ανωνυμία. Η δράση της έλαβε τέλος τον Οκτώβριο του 2013 με το Ομοσπονδιακό γραφείο ερευνών (FBI) να κατεβάζει την ιστοσελίδα και να προχωράει στη σύλληψη του Ross Ulbricht ιδρυτή του Ιστότοπου «Dread

Pirate Roberts», στον οποίου προσάφθηκαν εφτά κατηγορίες συμπεριλαμβανομένης της κατηγορίας για ξέπλυμα βρώμικου χρήματος.

Ο Σκοτεινός Ιστός όμως συχνά εμπλέκεται σε φρικτά εγκλήματα όπως κλοπή και κοινοποίηση προσωπικού περιεχομένου, κακοποίηση ανήλικων παιδιών, πληρωμένες δολοφονίες, διακίνηση παιδικής πορνογραφίας, εμπόριο λευκής σαρκός, διακίνηση όπλων και πολλών άλλων αποτρόπαιων πράξεων. Στη δημοσιότητα έχουν έρθει πολλές μαρτυρίες ανθρώπων που συνδέθηκαν σε ιστοσελίδες στον Σκοτεινό Ιστό. Εντύπωση προκαλεί η ιστορία ενός 14χρονου χάκερ, ο οποίος συνδεόταν στο Dark Web με στόχο την εξερεύνηση καινούριων και ασυνήθιστων σελίδων και όχι για να αγγίξει την πιο σκοτεινή του πλευρά. Όπως εξομολογείται το μεγαλύτερο μέρος των sites είναι αρκετά βαρετά και δίχως να σου δημιουργούν ιδιαίτερο ενδιαφέρον, αφού μπορείς να βρεις από sites γνωριμιών μέχρι forum εξιχνίασης διάφορων γνωστών συνομωσιών. Ακολουθώντας κάποιες περίεργες Ιστοσελίδες βρέθηκε μπροστά σε ένα site που λεγόταν αρπαγές γονιών. Ο σχεδιασμός της ήταν αρκετά απλός και έμοιαζε με σελίδα tumblr. Έχοντας την περιέργεια να μάθει περισσότερα και διαβάζοντας τα περιεχόμενα, ανακάλυψε μια λίστα με λέξεις και αριθμούς μαζί με κάποια link για το ebay που οδηγούσαν σε σελίδες που πουλούσαν έπιπλα Αυτή 37,στο ebay καναπές 14.356 $. Αυτός 28, στο ebay κρεβάτι 11.467$ και η λίστα συνέχιζε. Ψάχνοντας λίγο παραπάνω παρατήρησε κάποιες ακολουθίες αριθμών που του εξίταραν το ενδιαφέρον. Όντας χάκερ και γνωρίζοντας από κρυπτογραφημένα μηνύματα αναρωτήθηκε αν αυτό που βρισκόταν μπροστά του ήταν κάποιου είδους κώδικας και με την βοήθεια μιας εφαρμογής αποκρυπτογράφησης του εμφάνισε ένα κείμενο που έλεγε:" Καλώς ήρθατε στο site αρπαγές γονιών. Χρειάζεστε μια μητέρα ή έναν πατέρα; Δεν είστε ευχαριστημένοι με αυτό που έχετε; Ε τότε ήρθατε στο σωστό μέρος! Ακολουθήστε ΑΥΤΗ για μια νέα μητέρα ή ΑΥΤΟΣ για έναν νέο πατέρα . Μόλις η πληρωμή φτάσει σε εμάς μέσω ebay θα παραλάβετε έναν νέο γονιό". Επιπλέον υπήρχε και ένα μήνυμα όπου έλεγε ότι παρέχετε και εγγύηση, ποιοτικός έλεγχος καθώς και chip παρακολούθησης κάνοντας αδύνατη την απόδραση. Ο 14χρονος αν και υποψιασμένος ότι υπάρχει περίπτωση να είναι απάτη και έπειτα από πολύωρη σκέψη, κατευθύνθηκε στο δωμάτιο της μητέρας του την ώρα που κοιμόταν και πήρε την πιστωτική της κάρτα. Η κινητήριος δύναμη ήταν η απόκτηση ενός πατέρα αφού ο ίδιος δεν είχε τη δυνατότητα ποτέ να έχει μια πατρική φιγούρα δίπλα του. Σκεπτόμενος λοιπόν ότι όταν η μητέρα του θα αντίκριζε τον καινούριο πατέρα θα τον ερωτευόταν και θα δημιουργούσαν όλοι μαζί την οικογένεια που αυτός πάντα ονειρευόταν, δίχως περεταίρω σκέψη πληκτρολόγησε τα στοιχεία της κάρτας και προχώρησε σε πληρωμή του πιο φθηνού «μπαμπά» που βρήκε έναντι 3.000$. Οι επόμενες βδομάδες που ακολούθησαν

βρήκαν τη μητέρα του να τσακώνεται με το ebay για μια μυστηριώδη αγορά που η ίδια δεν είχε κάνει και τον ίδιο φοβισμένο και μόνο στην ιδέα της ανακάλυψης του μυστικού του. Έπειτα από έναν μήνα και με τη σκέψη ότι ήταν ένα ακόμα παιδί που είχε εξαπατηθεί και ενώ ένα ακόμα βράδυ τον έβρισκε μπροστά από την οθόνη του υπολογιστή του, άκουσε ένα παράθυρο να σπάει και βήματα στη σκάλα. Αρπάζοντας το ρόπαλο του baseball την στιγμή που ο εισβολέας άνοιξε την πόρτα του βρέθηκε αντιμέτωπος με κάτι που ποτέ δεν είχε φανταστεί. Ένας μαυροφορεμένος άντρας τον ρώτησε αν ήταν αυτός που είχε παραγγείλει έναν μπαμπά και με γρήγορες κινήσεις κατευθύνθηκε προς το μέρος του αγοριού. Ο 14χρονος πάλεψε με όλη του τη δύναμη, αλλά όπως καταλαβαίνουμε δεν ήταν εύκολο να αμυνθεί απέναντι σε έναν ενήλικο άντρα. Ευτυχώς για το νεαρό αγόρι την πάλη άκουσε η μητέρα του η οποία έτρεξε να βοηθήσει το γιό της. Αφού ακινητοποίησαν τον άντρα, ο 14χρονος αποκάλυψε όλη την αλήθεια στη μητέρα του αλλά και στην αστυνομία. Το site όχι μόνο δεν προσέφερε γονείς αλλά πλήρωναν τα θύματα την αρπαγή τους. Δυστυχώς οι δράστες δεν πιάστηκαν αφού η αστυνομία δεν είχε περεταίρω στοιχεία και το site την επόμενη μέρα είχε κατέβει. Ο έφηβος αποκαλύπτει ότι μετά από τον τρόμο που πέρασε δεν ξανασυνδέθηκε στο Dark Web. Φυσικά η παραπάνω ιστορία δεν είναι η μοναδική περίπτωση που ο Σκοτεινός Ιστός αποδείχτηκε ιδιαίτερα επικίνδυνος. Στα παρακάτω κεφάλαια θα εντρυφήσουμε λίγο περισσότερο στις επικίνδυνες και ανατριχιαστικές ομολογουμένως πλευρές του Διαδικτύου.

❖ 1.3 Μέσα Κοινωνικής Δικτύωσης (Social Media)

Εικόνα 1.3 : Κοινωνική Δικτύωση (Social Networking)

Η τεχνολογική ανάπτυξη του Διαδικτύου από τα μέσα του 20ού αιώνα επηρέασε καταλυτικά τις επερχόμενες γενιές. Ειδικότερα, τον 21ο αιώνα, με την άνοδο των Μέσων Κοινωνικής Δικτύωσης (Social Media) όλο και περισσότερες κοινωνικές και ηλικιακές ομάδες έχουν συνδεθεί και προστεθεί σε αυτά τα νέα για την εποχή μέσα, δημιουργώντας μία

παγκοσμιοποιημένη κοινωνία. Σύμφωνα με τον οδηγό ορθής χρήσης μέσων κοινωνικής δικτύωσης του Γενικού Επιτελείου Εθνικής Άμυνας, *«Ο όρος "Κοινωνικά Δίκτυα-Social Media" αναφέρεται στις διαδικτυακές (online) τεχνολογίες και πρακτικές, που χρησιμοποιούνται για διαμοιρασμό περιεχομένου, γνώμης και πληροφοριών, την προαγωγή του διαλόγου και την οικοδόμηση σχέσεων. Τα μέσα αυτά χρησιμοποιούν μία ποικιλία από διαφορετικές μορφές, συμπεριλαμβανομένων του κειμένου, των εικόνων, του ήχου και του βίντεο»*. Ο χρήστης διαδικτύου με μια απλή περιήγηση στον παγκόσμιο ιστό μπορεί να ανακαλύψει τις ηλεκτρονικές πλατφόρμες κοινωνικής δικτύωσης. Τα μέσα κοινωνικής δικτύωσης δίνουν τη δυνατότητα στον χρήστη με μια εγγραφή να δημιουργήσει το δικό του προσωπικό προφίλ και μέσα από αυτό να εκφραστεί ,να επικοινωνήσει και να αλληλεπιδράσει με άλλους χρήστες.

Η ιδέα των μέσων κοινωνικής δικτύωσης βασίστηκε στην σύνδεση των ανθρώπων μέσω των διευθύνσεων ηλεκτρονικού ταχυδρομείου. Τη δεκαετία του '80 εμφανίζονται οι πρώτες διαδικτυακές κοινότητες με τη μορφή δωματίων επικοινωνίας (chatrooms). Το 1995 ο Randy Conrads δημιουργεί το Classmates με στόχο την επικοινωνία μεταξύ παλιών συμμαθητών. Δύο χρόνια μετά κάνει την εμφάνιση του το SixDegrees, η πρώτη εφαρμογή που συνδυάζει δημιουργία προφίλ, ανταλλαγή μηνυμάτων και εύρεση ατόμων με κοινά ενδιαφέροντα.

Εικόνα 1.4 : Λογότυπα SixDegrees.com & Classmates.com

Μέχρι το 2003 παρουσιάζονται τα blogs (διαδικτυακά ημερολόγια), LinkedIn (ιστόχωρος επαγγελματικής κοινωνικής δικτύωσης) καθώς και το Skype (εφαρμογή που προσφέρει κλήσεις σε όλο τον κόσμο, δυνατότητα αποστολής SMS και αρχείων και φυσικά τη δυνατότητα βιντεοκλήσης). Στις 4 Φεβρουαρίου του 2004 ο Mark Zuckerberg ιδρύει μια από τις δημοφιλέστερες σελίδες κοινωνικής δικτύωσης το Facebook. Στα πρώτα βήματά του δικαίωμα συμμετοχής είχαν μόνο φοιτητές του Χάρβαρντ, όπου σπούδαζε και ο ιδρυτής και αργότερα επεκτάθηκε σε κοινότητες αμερικανικών κολλεγίων. Το 2006 έγινε η απελευθέρωση του από αυτό το πρότυπο και δόθηκε πρόσβαση σε κάθε χρήστη στον πλανήτη άνω των 13 ετών.

Για την δημιουργία ενός προφίλ γίνεται εγγραφή στην πλατφόρμα με τον χρήστη να μπορεί να αποκαλύπτει πληροφορίες και ενδιαφέροντα για τον εαυτό του, φωτογραφίες και βίντεο από την καθημερινή του ζωή, τα συναισθήματα και τη διάθεση του καθώς επίσης και να κοινοποιεί την τοποθεσία του. Αριθμεί περίπου από τα τέλη του 2022 3,7 δισεκατομμύρια μηνιαίους ενεργούς χρήστες παγκοσμίως. Το Messenger προγραμματίστηκε και αναπτύχθηκε από τον ίδιο όμιλο της Facebook.Inc και αρχικά ξεκίνησε Facebook Chat το 2008, δίνοντας τη δυνατότητα στους χρήστες να ανταλλάσσουν εντός της πλατφόρμας του Facebook μηνύματα με τους διαδικτυακούς τους φίλους. Τον Αύγουστο του 2011 κυκλοφόρησε για πρώτη φορά ξεχωριστή και αυτόνομη εφαρμογή Messenger και η δυνατότητα για ξεχωριστό προφίλ. Η εφαρμογή αυτή φτιάχτηκε για Smartphones με λειτουργικό iOS και Android και έδωσε την δυνατότητα ανταλλαγής μηνυμάτων, πολυμέσων, stickers, φωνητικών μηνυμάτων, την πραγματοποίηση βιντεοκλήσεων και τη δημιουργία ομαδικών συνομιλίων με πολλά άτομα. Την ίδια δεκαετία ακολούθησαν πλατφόρμες κοινωνικής δικτύωσης με μεγάλη απήχηση στο κοινό με πιο γνωστές το Instagram, Snapchat και Tik Tok.

❖ 1.3.1 Βασικά Χαρακτηριστικά , Δυνατότητες & Κανόνες της Κοινότητας

Με τη συνεχή αύξηση ενεργών χρηστών στα Μέσα Κοινωνικής Δικτύωσης επήλθε επανάσταση στον τρόπο επικοινωνίας και αλληλεπίδρασης των ανθρώπων.

- Χαρακτηριστικά Μέσων Κοινωνικής Δικτύωσης

Σύμφωνα με τον Anthony Mayfield (2008) τα Μέσα Κοινωνικής Δικτύωσης παρουσιάζουν τα εξής χαρακτηριστικά:

- Συμμετοχή (Participation): Ενθαρρύνουν την συμμετοχική προσφορά των χρηστών παρέχοντάς τους την ευκαιρία να παραθέτουν σχόλια σε δημοσιεύσεις και να εκφράζουν την άποψή τους ενώ ταυτόχρονα έχουν την δυνατότητα να διαβάζουν τα σχόλια άλλων χρηστών.
- Διαφάνεια (Openness): Οι περισσότερες υπηρεσίες και πλατφόρμες είναι ανοιχτές, προσβάσιμες και εύκολα διαθέσιμες για ανατροφοδότηση, συμμετοχή και εύρεση υλικού ενθαρρύνοντας κατά αυτό τον τρόπο καθημερινά περισσοτέρους χρήστες να δημιουργήσουν ένα προφίλ .

- Συνομιλία (Conversation): Λειτουργούν αμφίδρομα δίνοντας την ικανότητα στους χρήστες να έχουν την ταυτότητα του δέκτη αλλά και του πομπού σε ένα μήνυμα, σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης όπου η μετάδοση περιεχομένου λειτουργεί μονόδρομα.
- Κοινότητα (Community): Επιτρέπουν να σχηματίζονται κοινότητες γρήγορα και να επικοινωνούν αποτελεσματικά. Οι κοινότητες μοιράζονται κοινά ενδιαφέροντα, όπως η αγάπη για τη φωτογραφία, ένα πολιτικό ζήτημα ή μία αγαπημένη τηλεοπτική εκπομπή.
- Συνδεσιμότητα (Connectedness): Τα περισσότερα είδη μέσων κοινωνικής δικτύωσης αναπτύσσουν τη συνδεσιμότητά τους, χρησιμοποιώντας συνδέσμους προς άλλους ιστότοπους, πόρους και άτομα.

Δυνατότητες Μέσων Κοινωνικής Δικτύωσης

Τα Μέσα Κοινωνικής Δικτύωσης έχουν φέρει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι συνδέονται, μοιράζονται και αλληλεπιδρούν με τον κόσμο. Αποτελούν σημαντικό εργαλείο προσωπικής και επαγγελματικής επικοινωνίας με τις δυνατότητές τους να εξελίσσονται διαρκώς.

Μια από τις κύριες δυνατότητες των Μέσων Κοινωνικής Δικτύωσης είναι η επικοινωνία. Επιτρέπει στους ανθρώπους να συνδέονται με τους φίλους, την οικογένεια και τους συναδέλφους τους που είναι γεωγραφικά διασκορπισμένοι σε πραγματικό χρόνο, παρέχοντάς τους μια εξαιρετική ευκαιρία να ανταλλάσσουν πληροφορίες, να μοιράζονται ιδέες, απόψεις και να συνεργάζονται εξ αποστάσεως.

Μια άλλη βασική δυνατότητά τους είναι η δικτύωση για επαγγελματική ανάπτυξη. Παρέχουν την ευκαιρία σε εργαζόμενους για εύρεση νέων θέσεων εργασίας και σε επιχειρηματίες να προωθήσουν προϊόντα και υπηρεσίες σε ευρύ φάσμα πελατών.

Χαρακτηριστική δυνατότητα των Μέσων Κοινωνικής Δικτύωσης είναι και η δυνατότητα πρόσβασης και ανταλλαγής πληροφοριών γρήγορα και αποτελεσματικά για εκπαιδευτικούς ή ψυχαγωγικούς σκοπούς Με το πάτημα ενός κουμπιού, τα άτομα αποκτούν πρόσβαση σε πληθώρα δεδομένων για οποιοδήποτε θέμα φανταστούν από επιστημονικά άρθρα και εκπαιδευτικά βίντεο μέχρι μουσική, ταινίες και παιχνίδια. Αυτές οι πληροφορίες μπορούν να βοηθήσουν στην προσωπική ανάπτυξη, βοηθώντας τους ανθρώπους να μάθουν νέες δεξιότητες και να διευρύνουν τη βάση γνώσεων τους.

Τέλος, τα Μέσα Κοινωνικής Δικτύωσης έχουν σημαντικό αντίκτυπο στην πολιτική και κοινωνική αλλαγή. Οι πλατφόρμες Μέσων Κοινωνικής Δικτύωσης έχουν διαδραματίσει σημαντικό ρολό στη διαμόρφωση της κοινής γνώμης και στη διάδοση πληροφοριών σχετικά με την κοινωνική αδικία και τις ανθρωπιστικές κρίσεις παγκοσμίως. Οι χρήστες έχουν επίσης χρησιμοποιήσει αυτές τις πλατφόρμες για να οργανώσουν κοινωνικά κινήματα και διαμαρτυρίες κατά της αστυνομικής βίας, της κλιματικής αλλαγής και άλλων κρίσιμων ζητημάτων.

- Κανόνες στην Ψηφιακή Κοινωνία

Η ψηφιακή κοινωνία είναι μια μορφή κοινωνίας όπου οι άνθρωποι είναι συνυφασμένοι με την τεχνολογία. Είναι μια κοινωνία που έχει θέσει τους δικούς της κανόνες και κανονισμούς για τα μέλη της, οι οποίοι δεν περιορίζονται μόνο σε άτομα, αλλά και σε ομάδες και οργανισμούς που δραστηριοποιούνται στον ψηφιακό κόσμο.

Ένας από τους πιο σημαντικούς κανόνες στην ψηφιακή κοινωνία είναι η ασφάλεια. Είναι σημαντικό να διατηρούνται ασφαλή τα δεδομένα και οι πληροφορίες. Ο ψηφιακός κόσμος είναι γεμάτος με πιθανές απειλές, όπως κακόβουλο λογισμικό, ιούς και χάκερ. Τα μέτρα κυβερνοασφάλειας πρέπει να ληφθούν σοβαρά υπόψη για να διασφαλιστεί ότι τα ευαίσθητα δεδομένα και οι πληροφορίες διατηρούνται απόρρητα και εμπιστευτικά. Για παράδειγμα, οι κωδικοί πρόσβασης πρέπει να ενημερώνονται τακτικά και θα πρέπει να χρησιμοποιείται έλεγχος ταυτότητας δύο παραγόντων όπου είναι δυνατόν. Σημαντική πτυχή της ασφάλειας αποτελεί η προσωπική ευθύνη των χρηστών σχετικά με την ανάρτηση και αποστολή ευαίσθητου προσωπικού περιεχομένου .

Ένας άλλος ουσιαστικός κανόνας στην ψηφιακή κοινωνία είναι η ιδιωτικότητα. Είναι σημαντικό να σέβεται ο ένας το απόρρητο του άλλου στον ψηφιακό κόσμο όπως και στον φυσικό. Οι άνθρωποι πρέπει να σέβονται τις πολιτικές απορρήτου διαφορετικών πλατφορμών και ιστότοπων. Τα προσωπικά στοιχεία δεν πρέπει να κοινοποιούνται χωρίς συγκατάθεση. Το Διαδίκτυο είναι ένα απίστευτα ισχυρό εργαλείο, αλλά μπορεί επίσης να αποτελέσει πηγή κινδύνου για τα άτομα εάν τεθεί σε κίνδυνο το απόρρητό τους.

Εξίσου σημαντικό κανόνα αποτελεί η κοινωνική ευθύνη. Αυτός ο κανόνας ισχύει για διαφορετικές πτυχές της ψηφιακής κοινωνίας όπως τα Μέσα Κοινωνικής Δικτύωσης, η ψηφιακή επικοινωνία και η δημιουργία διαδικτυακού περιεχομένου. Οι άνθρωποι πρέπει πάντα να εξετάζουν τον αντίκτυπο των πράξεων , των λόγων και των μηνυμάτων τους στον ψηφιακό

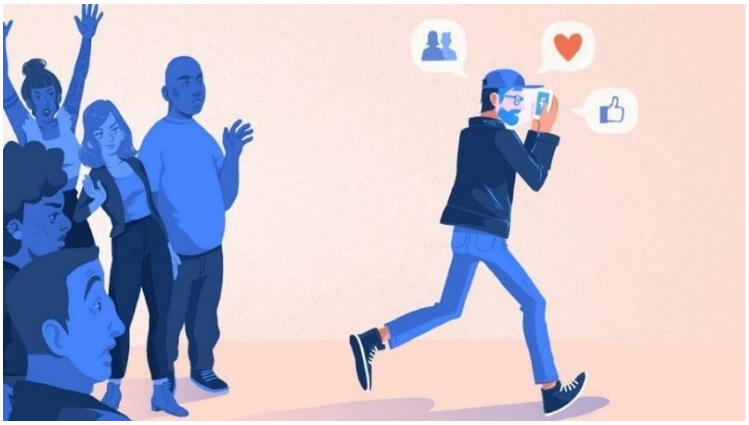
κόσμο. Τα άτομα και οι οργανισμοί πρέπει να αναλαμβάνουν την ευθύνη για τις πράξεις τους και να διασφαλίζον ότι δεν βλάπτουν άλλους ούτε συμπεριφέρονται ανάρμοστα.

Ένας από τους πιο συζητημένους κανόνες στον ψηφιακό κόσμο είναι ο κώδικας δεοντολογικής συμπεριφοράς στο διαδίκτυο (netiquette), δηλαδή το σύνολο των κανόνων που ορίζουν την αποδεκτή συμπεριφορά μεταξύ δύο ή περισσότερων χρηστών του Διαδικτύου κατά την ηλεκτρονική τους επικοινωνία. *Ο Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο στοχεύει στην καθιέρωση συμβάσεων ευγένειας και αλληλοσεβασμού, καθώς και στην πιο αποδοτική αλληλεπίδραση μεταξύ των χρηστών. Ο χαρακτήρας των κανόνων που τον απαρτίζουν είναι εθιμοτυπικός και κατά συνέπεια η μη υπακοή σε αυτούς δεν επιφέρει νομικές κυρώσεις (Wikipedia).*

Η απουσία της φυσικής παρουσίας έχει πάψει να αποτελεί εμπόδιο στην ανάπτυξη ανθρωπίνων σχέσεων στον ψηφιακό κόσμο. Οι άνθρωποι αλληλεπιδρούν στο Διαδίκτυο όπως και στην πραγματική ζωή, ανταλλάσσουν απόψεις και πληροφορίες, εργάζονται, μορφώνονται, κάνουν αγοροπωλησίες , διασκεδάζουν, δημιουργούν φιλίες, ερωτεύονται και βοηθούν ή εξαπατούν ο ένας τον άλλον.

❖ 1.4 Προσφορά των Ψηφιακών Μέσων για την Υλοποίηση των Εγκλημάτων

Το Διαδίκτυο και τα ψηφιακά μέσα πλέον κατέχουν σπουδαίο ρόλο στη σύγχρονη καθημερινότητα και αποτελούν αναπόσπαστο κομμάτι των χρηστών τους. Το Internet και τα Μέσα Κοινωνικής Δικτύωσης όπως Facebook, Instagram, Twitter, Tik Tok και πολλές άλλες ψηφιακές πλατφόρμες έχουν εισβάλλει στη ζωή των ανθρώπων και έχουν αλλάξει όχι μόνο τον τρόπο με το οποίον ο κόσμος επικοινωνεί, μαθαίνει, εργάζεται αλλά και ζει.



Εικόνα 1.5 : Η Φιλία στον Πραγματικό Κόσμο και στο Ψηφιακό Κόσμο

Τα μεγαλύτερα πλεονεκτήματα που τα κάνουν αρεστά είναι η ταχύτητα και η προσβασιμότητα ανά πάσα στιγμή. Η ευκολία με την οποία διεκπεραιώνονται υποχρεώσεις και δραστηριότητες καθώς και ο τεράστιος όγκος πληροφορίας που διατίθεται, τα καθιστούν αυτόνομο αγαθό και υπέρτατη ανάγκη. Ωστόσο ο ψηφιακός κόσμος έχει αποτελέσει τη βάση για πολλά ηλεκτρονικά εγκλήματα.

❖ 1.4.1 Κατηγορίες Ηλεκτρονικών Εγκλημάτων

Βασική προϋπόθεση για το ηλεκτρονικό έγκλημα είναι η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων όπως Η/Υ, tablet, κινητό τηλέφωνο,notepad κλπ.

Κυρίαρχο ρόλο διαδραματίζει ο υπολογιστής ο οποίος μπορεί να είναι απλά ένα βοηθητικό μέσο για την επίθεση ή ακόμα και αυτός που θα τελέσει την εγκληματική ενέργεια. Το 1994 οι Forester και Morrison όρισαν το Ηλεκτρονικό έγκλημα (Computer Crime) σαν «*μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσή της*». Πολλοί είναι οι ορισμοί που του έχουν προσδοθεί κατά καιρούς καθώς δεν είναι εύκολο να αποδοθεί η ερμηνεία του με ακρίβεια λόγω της ποικιλομορφίας του. Εξαιτίας αυτής της συνθήκης υπάρχουν κατηγορίες εγκλημάτων όπου η καθεμία νομοθετείται και διώκεται ποινικά με βάση τα χαρακτηριστικά της. Συνοψίζοντας κάποια από τα βασικά χαρακτηριστικά του εγκλήματος μέσω Διαδικτύου καταλήγουμε στα εξής:

- Απουσία ιχνών με τη συμβατική σημασία (δακτυλικά αποτυπώματα, δείγμα DNA κλπ.).
- Μη αναγκαία φυσική παρουσία του δράστη στον τόπο του εγκλήματος.
- Ταχύτητα και ευκολία με την οποία διεξάγεται.
- Επέκταση της επελθούσας ζημίας καθώς ο δράστης μπορεί να δράσει σε πολύ μικρό χρονικό διάστημα σε πολλά μέρη ή και κράτη.
- Συνήθης είναι η ανάγκη του δράστη για υψηλού επιπέδου εξειδικευμένων γνώσεων προγραμματισμού με σκοπό τη διεκπεραίωση της παράνομης πράξης.

Οι βασικές μορφές του Ηλεκτρονικού Εγκλήματος κατηγοριοποιούνται ως εξής:

- Στα εγκλήματα που τελούνται σε περιβάλλον ηλεκτρονικών υπολογιστών. Ένα παράδειγμα είναι η δημοσίευση προσωπικού και ευαίσθητου περιεχομένου χωρίς τη

συγκατάθεση του εν λόγω προσώπου με σκοπό τη διαπόμπευσή του. Σε αυτή την περίπτωση το Διαδίκτυο αποτελεί το μέσο διάπραξης του εγκλήματος.

- Στα εγκλήματα που τελούνται χωρίς τη βοήθεια του Διαδικτύου όπως είναι η παράνομη αντιγραφή λογισμικού ή το free app download μέσω torrent.
- Σε εγκλήματα που η ύπαρξη του Διαδικτύου είναι αναγκαία, όπως είναι αυτό της διάχυσης των λεγόμενων «ιών».

Στην Ελλάδα ο διαχωρισμός των ηλεκτρονικών εγκλημάτων γίνεται με βάση αυτά που τελούνται μέσω των Η/Υ και σε αυτά που τελούνται με Η/Υ μέσω Διαδικτύου. Συγκεκριμένα, έγκλημα με χρήση υπολογιστή στην χώρα μας διαπράχτηκε για πρώτη φορά στις αρχές της δεκαετίας του ’90, όταν πλαστογράφοι δημιούργησαν πλαστά χαρτονομίσματα σε δραχμές με τη χρήση εξελιγμένων υπολογιστών και σαρωτών (scanner). Αργότερα ακολούθησε και το πρώτο έγκλημα με χρήση υπολογιστή και Διαδικτύου. Ο δράστης ήταν ένας νεαρός άνδρας όπου με τη λήξη της σχέσης που διατηρούσε με τη σύντροφό του, για να την εκδικηθεί δημιούργησε μια σελίδα γνωριμιών όπου της κατασκεύασε ένα ερωτικό προφίλ αναρτώντας εκεί όλα της τα προσωπικά στοιχεία. Αυτό είχε ως αποτέλεσμα η κοπέλα να δεχθεί πολλές κλήσεις και επισκέψεις στην οικία της από αγνώστους που είχαν σκοπό να την γνωρίσουν από κοντά.

Οι πιο γνωστές μορφές εγκληματικής δραστηριότητας που αναπτύσσονται μέσω διαδικτύου είναι:

- Παιδική πορνογραφία
- Εγκλήματα περί τα ήθη
- Απάτες μέσω Διαδικτύου - Πιστωτικές κάρτες - Εγκλήματα κυβερνοεμπορίου
- Cracking και Hacking
- Διακίνηση/πειρατεία λογισμικού
- Διακίνηση ναρκωτικών και όπλων
- Παραβίαση προσωπικών δεδομένων
- Cyberbullying

❖ 1.4.2 Κίνδυνοι από την Κοινωνική Δικτύωση

Εικόνα 1.6 : Κίνδυνοι στα Social Media

Οι δυνατότητες και οι ευκαιρίες που δίνονται μέσω των social media είναι απεριόριστες, ωστόσο μαζί με τη δύναμή τους έχουν επέλθει και σωρεία κινδύνων. Τα Μέσα Κοινωνικής Δικτύωσης αποτελούν φθηνό μέσο για επικοινωνία, όμως πολλές φορές πετυχημένες πλατφόρμες έχουν υπάρξει κύριος παράγοντας για τη διάπραξη εγκλημάτων γνωστών και ως e-crimes. Οι περισσότεροι χρήστες των social media καθημερινά εκτίθενται σε κινδύνους που δεν μπορούν να αντιληφθούν, κάποιοι εκ των οποίων είναι:

- Λόγω της πολύωρης καθημερινής χρήσης του διαδικτύου και των μέσων κοινωνικής δικτύωσης, ολοένα και περισσότερο παρατηρούμε ότι ο εθισμός στο Διαδίκτυο αποτελεί συχνό φαινόμενο, το οποίο επεκτείνεται σε ευρύ ηλικιακό φάσμα. Τα αποτελέσματα αυτού του είδους εθισμού δεν είναι καθόλου ευκαταφρόνητα αφού έχουν άμεση επίδραση στη ζωή των χρηστών. Συγκεκριμένα, οι εθισμένοι χρήστες παρουσιάζουν βίαιες και αντιδραστικές συμπεριφορές στην περίπτωση προσπάθειας μείωσης του χρόνου παραμονής τους στο Διαδίκτυο, απομόνωση από το φιλικό και οικογενειακό περιβάλλον τους, απότομη πτώση της απόδοσής τους σε σχολικές ή εργασιακές υποχρεώσεις καθώς και αποδιοργάνωση σε επίπεδο καθημερινών διεργασιών.
- Υπερβολική έκθεση των προσωπικών δεδομένων από τους ίδιους τους χρήστες μέσω δημοσίευσης φωτογραφιών, βίντεο ακόμα και της ακριβής τοποθεσίας στην οποία βρίσκονται. Έτσι κάνοντας ορατή την προσωπική τους ζωή σε όλους καταργείται η ιδιωτικότητά τους και βάζουν ακόμα και τη ζωή τους σε κίνδυνο. Όπως αναφέρει ο Εμμανουήλ Σφακιανάκης σε μια από τις ομιλίες του είναι χαρακτηριστικό το παράδειγμα μιας έφηβης κοπέλας, η οποία στο προσωπικό της προφίλ στο Facebook

κοινοποίησε την τοποθεσία διασκέδασής της κάνοντας εύκολη την αρπαγή της από τους απαγωγείς της.

- Γνωστό και ως cyberbulling ο διαδικτυακός εκφοβισμός συμβαίνει από κακόβουλους χρήστες που παρενοχλούν ένα άτομο στο Διαδίκτυο ή στα Μέσα Κοινωνικής Δικτύωσης. Η παρενόχληση αυτή μπορεί να γίνεται σε τακτά ή άτακτα χρονικά διαστήματα μέσω οποιασδήποτε πράξης εκφοβισμού, επιθετικότητας, τρομοκρατικής ή αυταρχικής συμπεριφοράς. Ο διαδικτυακός εκφοβισμός περιλαμβάνει καταστάσεις όπως η αποστολή ανήθικων μηνυμάτων, ο αποκλεισμός ατόμων από εφαρμογές συνομιλίων, hacking λογαριασμού, δημοσίευση ευαίσθητου προσωπικού περιεχομένου ή προσβλητικών φημών, απειλές με σκοπό την απολαβή μεγάλων χρηματικών ποσών κ.α.
- Απάτες ηλεκτρονικού ψαρέματος ή αλλιώς Phising είναι οι προσπάθειες απατεώνων να εξαπατήσουν τους χρήστες να δώσουν προσωπικά τους στοιχεία. Η επικοινωνία μπορεί να πραγματοποιηθεί μέσω email, κοινωνικών μέσων, κλήσης ή μηνύματος στο κινητό τηλέφωνο, προσποιούμενοι είτε μια νόμιμη επιχείρηση είτε έναν κρατικό φορέα ζητώντας την επιβεβαίωση προσωπικών στοιχείων μέσω μια ηλεκτρονικής φόρμας ή ενός link. Τα μηνύματα ηλεκτρονικού ψαρέματος έχουν σχεδιαστεί για να φαίνονται γνήσια και συχνά αντιγράφουν τη μορφή του οργανισμού ή της εταιρίας που προσποιούνται έτσι ώστε να είναι δύσκολη η αναγνώριση της απάτης από τους χρήστες.

Συμπερασματικά για να μεγιστοποιηθούν τα οφέλη της ψηφιακής κοινωνίας, ελαχιστοποιώντας παράλληλα τους κινδύνους , τα άτομα πρέπει να είναι προσεκτικά στη χρήση της τεχνολογίας με υπεύθυνο και ισορροπημένο τρόπο , επιτυγχάνοντας μια υγιή ισορροπία μεταξύ παραγωγικότητας και ελεύθερου χρόνου και δίνοντας προτεραιότητα στο απόρρητο και την ασφάλειά τους στο Διαδίκτυο.

Το άσεμνο περιεχόμενο στο Διαδίκτυο έχει γίνει ένα καυτό θέμα τα τελευταία χρόνια. Αναφέρεται σε κάθε μορφή ακατάλληλου ή προσβλητικού υλικού που μπορεί να βρεθεί στο Διαδίκτυο, από πορνογραφία και βίαιο περιεχόμενο έως ρητορική μίσους και διαδικτυακό εκφοβισμό. Αν και το Διαδίκτυο είναι ένα πολύτιμο εργαλείο επικοινωνίας, εκπαίδευσης και ψυχαγωγίας, μπορεί επίσης να είναι μια επικίνδυνη πλατφόρμα για νεαρά και ευάλωτα άτομα που εκτίθενται σε ρητό και επιβλαβές υλικό που μπορεί να επηρεάσει αρνητικά την ψυχική και συναισθηματική τους υγεία.

ΚΕΦΑΛΑΙΟ 2ο : Η ΕΠΙΚΙΝΔΥΝΟΤΗΤΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

❖ 2.1 Παράνομες Ιστοσελίδες

Οι παράνομοι ιστότοποι (illegal websites) είναι πλατφόρμες στο Διαδίκτυο που λειτουργούν εκτός νόμου. Το περιεχόμενό τους αποτελεί σοβαρή απειλή για τους χρήστες τους Διαδικτύου και την κοινωνία γενικότερα. Αυτοί οι ιστότοποι διανέμουν και εμφανίζουν περιεχόμενο που είτε είναι απαγορευμένο είτε πολύ ευαίσθητο για να κυκλοφορεί στον ψηφιακό κόσμο. Μπορούν να χρησιμοποιηθούν για μια ποικιλία παράνομων δραστηριοτήτων, όπως η ροή περιεχομένου που προστατεύεται από πνευματικά δικαιώματα, ο τζόγος, η διακίνηση ναρκωτικών, η τρομοκρατία και η διευκόλυνση της εμπορίας ανθρώπων κ.α.

- Ιστότοποι Πειρατικού Περιεχομένου: Χρησιμοποιούνται για την κλοπή και την παράνομη διανομή υλικού που προστατεύεται από πνευματικά δικαιώματα. Με την έλευση του Διαδικτύου έχει γίνει εύκολο για τους ανθρώπους, να έχουν πρόσβαση σε πειρατικό περιεχόμενο όπως ταινίες, μουσική , παιχνίδια, βιβλία και λογισμικό. Συχνά διαθέτουν ανώνυμους χειριστές οι οποίοι προσελκύουν χρήστες με την υπόσχεση παροχής δωρεάν περιεχομένου. Οι ιστότοποι αυτοί δεν είναι μόνο επιβλαβείς καθώς εκθέτουν τους χρήστες σε κακόβουλο λογισμικό αλλά και γιατί στερούν από τους δημιουργούς του περιεχομένου τα νόμιμα κέρδη τους.
- Ιστότοποι Διακίνησης Παράνομων Υπηρεσιών και Προϊόντων: Το Διαδίκτυο έχει μετατραπεί σε πρόσφορο έδαφος για παράνομες δραστηριότητες, με αμέτρητους ιστότοπους να διακινούν παράνομες υπηρεσίες και προϊόντα με το πάτημα ενός κουμπιού. Από ναρκωτικά, όπλα και τζόγο μέχρι πλαστά έγγραφα ταυτοποίησης, κλεμμένους αριθμούς πιστωτικών καρτών και ενοικίαση πληρωμένων δολοφόνων, αυτοί οι ιστότοποι απευθύνονται σε άτομα που επιδιώκουν να προμηθευτούν παράνομα αγαθά και υπηρεσίες χωρίς τον κίνδυνο εντοπισμού.
- Ιστότοποι Phishing και Κακόβουλου Λογισμικού: Το ηλεκτρονικό ψάρεμα και το παράνομο κακόβουλο λογισμικό είναι δύο από τις πιο επικίνδυνες απειλές στον κυβερνοχώρο που υπάρχουν σήμερα. Το ηλεκτρονικό ψάρεμα (phishing) είναι μια τεχνική που εξαπατά αθώα άτομα μέσω δόλιων ιστότοπων και μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να είναι νόμιμα. Μόλις το άτομο πέσει θύμα

της απάτης, ο χάκερ μπορεί να έχει πρόσβαση στις προσωπικές του πληροφορίες, όπως στοιχεία πιστωτικής κάρτας, κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα. Το παράνομο κακόβουλο λογισμικό, από την άλλη πλευρά, είναι ένας ιός που μολύνει συσκευές και κλέβει πληροφορίες όπως προσωπικά αρχεία και στοιχεία σύνδεσης.

- Διανομή Ακατάλληλου Περιεχομένου: Αναφέρεται στην πράξη διάδοσης ή κοινής χρήσης περιεχομένου που κρίνεται ακατάλληλο ή προσβλητικό για ορισμένους θεατές. Αυτό μπορεί ενδεικτικά να περιλαμβάνει υλικό που είναι ρητά σεξουαλικό, βίαιο, εισάγει διακρίσεις ή προωθεί παράνομες δραστηριότητες. Το ακατάλληλο περιεχόμενο μπορεί να διανεμηθεί εκούσια ή ακούσια και σε ορισμένες περιπτώσεις, μπορεί να συγκαλυφθεί ή να κρυφτεί μέσα σε πιο αθώο περιεχόμενο. Η διανομή ακατάλληλου περιεχομένου μπορεί να είναι επιβλαβής, ειδικά σε ευάλωτες ομάδες όπως τα παιδιά.

❖ 2.2 Δωμάτια Συνομιλίας (Chat Rooms)

Στη σημερινή ψηφιακή εποχή, τα δωμάτια συνομιλίας έχουν γίνει ένας ολοένα και πιο δημοφιλής τρόπος για τους ανθρώπους να συνδέονται και να επικοινωνούν στο Διαδίκτυο. Το chat room είναι ένας διαδικτυακός χώρος όπου χρήστες από διαφορετικές χώρες και πολιτισμικά υπόβαθρα, μπορούν να συμμετέχουν σε συνομιλίες σε πραγματικό χρόνο μεταξύ τους χρησιμοποιώντας μηνύματα κειμένου. Συνήθως, οι αίθουσες συνομιλίας επικεντρώνονται σε ένα συγκεκριμένο θέμα όπως η πολιτική, ο αθλητισμός ή οι σχέσεις.

Τα δωμάτια συνομιλίας προσφέρουν μια σειρά από οφέλη για τους χρήστες. Πρώτα και κύρια, παρέχουν μια αίσθηση κοινότητας και κοινωνικής σύνδεσης σε έναν κόσμο όπου πολλοί άνθρωποι αισθάνονται αποκομμένοι και απομονωμένοι. Οι αίθουσες συνομιλίας μπορούν να είναι ένας πολύ καλός τρόπος για τους ανθρώπους να συναντήσουν άλλους που μοιράζονται τα ενδιαφέροντα, τα χόμπι ή τις πεποιθήσεις τους και να συμμετάσχουν σε ζωηρές συζητήσεις και σε συζητήσεις για σημαντικά θέματα.

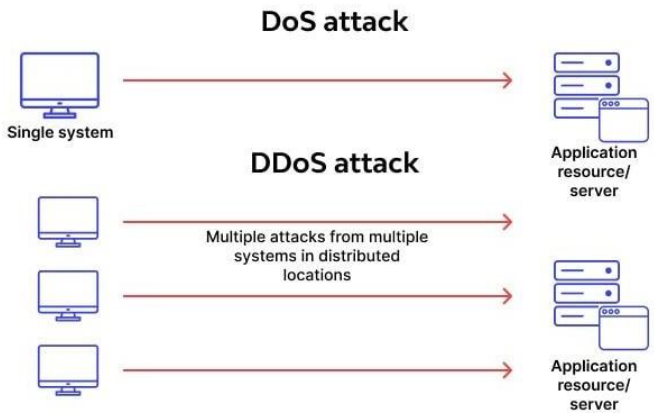
Ένα άλλο πλεονέκτημα των δωματίων συνομιλίας είναι ότι επιτρέπουν στους χρήστες να επικοινωνούν ανώνυμα. Πολλοί άνθρωποι αισθάνονται άνετα να εκφραστούν στο διαδίκτυο παρά προσωπικά και η ανωνυμία που παρέχεται από τα δωμάτια συνομιλίας, μπορεί να διευκολύνει τους χρήστες να ανοίξουν και να μοιραστούν τις σκέψεις και τα συναισθήματά τους. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η ανωνυμία στα δωμάτια συνομιλίας μπορεί

επίσης να οδηγήσει σε αρνητική συμπεριφορά όπως τρολάρισμα, εκφοβισμό, παρενόχληση και σεξουαλική κακοποίηση.

❖ 2.3 Μέθοδοι Επιθέσεων Δικτύων

Οι επιθέσεις δικτύου και οι απειλές για την ασφάλεια του δικτύου είναι ένα διαχρονικό πρόβλημα που επηρεάζει την ακεραιότητα μεμονωμένων συστημάτων αλλά και οργανισμών. Αυτές οι απειλές μπορεί να εμφανιστούν με διάφορες μορφές όπως άρνηση παροχής υπηρεσιών (DoS) , επιθέσεις SQL , δούρειους ίππους κ.α. Όλες αυτές οι απειλές μπορούν να προκαλέσουν σημαντικές απώλειες όσον αφορά τα δεδομένα, τον οικονομικό αντίκτυπο και τη φήμη. Οι απειλές για την ασφάλεια του δικτύου μπορούν να αποφευχθούν διασφαλίζοντας ένα ισχυρό αμυντικό σύστημα που περιλαμβάνει εξελιγμένα μέτρα ασφάλειας όπως τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών, κρυπτογράφηση και λογισμικό προστασίας από ιούς. Επιπλέον, οι τακτικές αξιολογήσεις ασφαλείας δικτύου και μια ενημερωμένη πολιτική ασφαλείας μπορούν να διασφαλίσουν ότι τα δίκτυα παραμένουν προστατευμένα.

❖ 2.3.1 Denial of Service (DoS)



Εικόνα 2.1 : Διαφορά DoS & DDoS επίθεσης

Η επίθεση άρνησης υπηρεσίας (DoS attack) είναι μια επίθεση στον κυβερνοχώρο που στοχεύει στη διακοπή της κανονικής λειτουργίας ενός δικτύου, ενός συστήματος υπολογιστή ή ενός ιστότοπου πλημμυρίζοντάς το με υπερβολική κίνηση ή δεδομένα. Αυτό έχει ως αποτέλεσμα το στοχευμένο σύστημα να κατακλύζεται και να μην μπορεί να ανταποκριθεί σε νόμιμα αιτήματα,

με αποτέλεσμα την απώλεια της υπηρεσίας σε νόμιμους χρήστες. Οι επιθέσεις DoS μπορούν να πραγματοποιηθούν από έναν μόνο εισβολέα, αλλά οι επιθέσεις DDoS (Distributed Denial of Service) περιλαμβάνουν πολλούς εισβολείς που χρησιμοποιούν botnets (δίκτυα μολυσμένων υπολογιστών). Για να αντιμετωπιστεί μια επίθεση DoS, είναι σημαντικό να προσδιοριστεί πρώτα η πηγή της επίθεσης και να εφαρμοστεί σύστημα φιλτραρίσματος για την απόκλιση της επίθεσης. Αυτό μπορεί να γίνει με τη διαμόρφωση των τειχών προστασίας και των συστημάτων πρόληψης εισβολής για την αποτροπή της κακόβουλης κυκλοφορίας να φτάσει στον στόχο. Είναι επίσης σημαντικό να υπάρχει συνεχής παρακολούθηση στην κυκλοφορία του δικτύου και τα αρχεία καταγραφής του συστήματος για την ανίχνευση οποιασδήποτε ασυνήθιστης δραστηριότητας καθώς και η ύπαρξη ενός εφεδρικού συστήματος όπου μπορεί να επιτρέψει τη γρήγορη ανάκτηση δεδομένων σε περίπτωση επίθεσης.

❖ 2.3.2 Κακόβουλο Λογισμικό (Malware)

Εικόνα 2.2 : Κακόβουλο Λογισμικό

Το malware, ένας συντομευμένος όρος για το malicious software (κακόβουλο λογισμικό), είναι ένας τύπος λογισμικού που έχει σχεδιαστεί για να βλάπτει τις υπολογιστικές συσκευές, να κλέβει ή να καταστρέφει δεδομένα και να διακόπτει τις κανονικές λειτουργίες του υπολογιστή. Περιλαμβάνει διάφορους τύπους κακόβουλων προγραμμάτων όπως:

- Ιούς (virus): Ένας ιός υπολογιστή είναι ένα πρόγραμμα που εξαπλώνεται μολύνοντας αρχεία ή περιοχές του συστήματος του σκληρού δίσκου ενός υπολογιστή ή δρομολογητή δικτύου και στη συνέχεια δημιουργεί αντίγραφα του εαυτού του. Ορισμένοι ιοί είναι αβλαβείς ενώ άλλοι μπορεί να καταστρέψουν αρχεία δεδομένων.

- Σκουλήκια (worms): Τα σκουλήκια είναι αυτόνομα κακόβουλα προγράμματα που μπορούν να αυτοαναπαρχθούν και να διαδοθούν ανεξάρτητα μόλις παραβιάσουν το σύστημα.
- Δούρειους Ίππους (Trojans): Οι δούρειοι ίπποι κρύβουν μέσα τους κακόβουλο κώδικα, ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του Διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δεν μεταδίδονται μολύνοντας αρχεία.
- Rootkit: Τα rootkit είναι κακόβουλα προγράμματα που παρέχουν σε εισβολείς Internet απεριόριστη πρόσβαση σε ένα σύστημα, ενώ αποκρύπτουν την παρουσία τους. Τα rootkit, ύστερα από την πρόσβασή τους σε ένα σύστημα (εκμεταλλευόμενα συνήθως ένα κενό ασφαλείας), χρησιμοποιούν λειτουργίες του λειτουργικού συστήματος για να αποφύγουν τον εντοπισμό τους από το λογισμικό Antivirus (αποκρύπτουν διεργασίες, αρχεία και δεδομένα του μητρώου των Windows). Για αυτόν το λόγο, είναι σχεδόν αδύνατη η ανίχνευσή τους χρησιμοποιώντας συνηθισμένες τεχνικές ελέγχου.

Το κακόβουλο λογισμικό μπορεί να διανεμηθεί μέσω διαφόρων καναλιών, όπως ηλεκτρονικά μηνύματα, παραβιασμένοι ιστότοποι, Μέσα Κοινωνικής Δικτύωσης, δίκτυα κοινής χρήσης αρχείων και λήψεις μολυσμένου λογισμικού. Μόλις μπει μέσα σε μια συσκευή το κακόβουλο λογισμικό μπορεί να προκαλέσει διάφορες μορφές ζημιάς, όπως σφάλματα συστήματος, παραβιάσεις δεδομένων, κλοπή ταυτότητας και οικονομική απάτη. Το κακόβουλο λογισμικό είναι συνήθως σχεδιασμένο για να λειτουργεί κρυφά και να παραμένει απαρατήρητο για όσο το δυνατόν περισσότερο, καθιστώντας το ακόμη πιο επικίνδυνο. Η πρόληψη επιθέσεων κακόβουλου λογισμικού απαιτεί μια πολυεπίπεδη προσέγγιση, συμπεριλαμβανομένης και της διατήρησης ενημερωμένου λογισμικού προστασίας από ιούς, αποφυγή κλικ σε ύποπτους συνδέσμους ή λήψη ύποπτων αρχείων, τακτική ενημέρωση λογισμικού και λειτουργικών συστημάτων καθώς επίσης και δημιουργία αντιγράφων ασφαλείας.

❖ 2.3.3 Επιθέσεις με Κωδικό Ασφαλείας (Password Attacks)

Εικόνα 2.3 : Επίθεση με Κωδικό Ασφαλείας

Οι επιθέσεις με κωδικό πρόσβασης γίνονται όλο και πιο συχνές καθώς οι άνθρωποι συνεχίζουν να βασίζονται στην τεχνολογία στην καθημερινή τους ζωή. Αυτές οι επιθέσεις μπορούν να λάβουν πολλές μορφές, από επιθέσεις ωμής βίας που χρησιμοποιούν αλγόριθμους για να μαντέψουν τους κωδικούς πρόσβασης έως επιθέσεις κοινωνικής μηχανικής που εξαπατούν τους ανθρώπους να εγκαταλείψουν τους κωδικούς πρόσβασής τους. Μια κοινή μορφή επίθεσης με κωδικό πρόσβασης είναι η επίθεση λεξικού, η οποία χρησιμοποιεί μια προκαθορισμένη λίστα κοινών λέξεων και φράσεων για να μαντέψει έναν κωδικό πρόσβασης. Αυτοί οι τύποι επιθέσεων είναι συχνά επιτυχείς επειδή πολλοί άνθρωποι χρησιμοποιούν εύκολα «μαντέψιμους» κωδικούς πρόσβασης.

Για την προστασία από επιθέσεις κωδικών πρόσβασης, είναι σημαντικό ο χρήστης να χρησιμοποιεί σύνθετους κωδικούς πρόσβασης που είναι δύσκολο να μαντέψουν οι χάκερς. Ένας ισχυρός κωδικός πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες και να περιλαμβάνει συνδυασμό γραμμάτων, αριθμών και συμβόλων. Επιπλέον, είναι σημαντικό να χρησιμοποιούνται διαφορετικοί κωδικοί πρόσβασης για διαφορετικούς λογαριασμούς, έτσι ώστε εάν ένας κωδικός πρόσβασης παραβιαστεί, οι άλλοι λογαριασμοί να παραμείνουν ασφαλείς.

❖ 2.3.4 SQL Injection

Εικόνα 2.4 : SQL Injection

Το SQL Injection είναι ένας τύπος ευπάθειας ασφάλειας που μπορεί να αξιοποιηθεί από εισβολείς για την πρόσβαση και τροποποίηση ευαίσθητων πληροφοριών που είναι αποθηκευμένες σε βάσεις δεδομένων. Η διαδικασία συνήθως περιλαμβάνει την εισαγωγή κακόβουλου κώδικα σε πεδία εισόδου σε έναν ιστότοπο ή μια εφαρμογή, η οποία στη συνέχεια εκτελεί εντολές στη βάση δεδομένων. Ο εισβολέας μπορεί στη συνέχεια να έχει πρόσβαση στα περιεχόμενα της βάσης δεδομένων, να τα τροποποιήσει ή να τα διαγράψει εντελώς .

Οι συνέπειες μια επιτυχημένης επίθεσης SQL Injection μπορεί να είναι σοβαρές, με αυτές να κυμαίνονται από κλοπή ευαίσθητων δεδομένων όπως προσωπικό φωτογραφικό υλικό και αριθμοί πιστωτικών καρτών έως και την καταστροφή ολόκληρων βάσεων δεδομένων. Οι επιθέσεις SQL Injection αποτελούν σοβαρή ανησυχία για επιχειρήσεις και οργανισμούς όλων των μεγεθών και είναι απαραίτητο να ληφθούν μέτρα για την αποτροπή τους. Αυτό μπορεί να περιλαμβάνει τη διασφάλιση της κωδικοποίησης όλων των εφαρμογών και των ιστότοπων με γνώμονα την ασφάλεια, τον τακτικό έλεγχο για τρωτά σημεία και τη χρήση εργαλείων και τεχνικών για τον εντοπισμό και την πρόληψη επιθέσεων SQL Injection προτού πραγματοποιηθούν.

ΚΕΦΑΛΑΙΟ 3ο : ΠΑΙΔΙΚΗ ΕΚΜΕΤΑΛΛΕΥΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

❖ 3.1 Εισαγωγή

Εικόνα 3.1 : παιδική εκμετάλλευση στο διαδίκτυο

Η αμεσότητα, η ταχύτητα αλλά και ο όγκος πληροφοριών που προσφέρεται από το Διαδίκτυο αποτελεί πόλο έλξης τόσο για τους ενήλικες όσο και για τους ανήλικους χρήστες. Η κατασκευή του Διαδικτύου είναι δομημένη για να έλκει τα παιδιά. Το γεγονός ότι με το πάτημα ενός κουμπιού μπορούν να επισκεφθούν τόσα ελκυστικά πράγματα και να επικοινωνούν με φίλους τους, ικανοποιεί το φυσιολογικό για την ηλικία τους αυθορμητισμό, την περιέργεια και την ανάγκη τους για άμεση ανταπόκριση. Με την απότομη και συνεχή εξέλιξη της τεχνολογίας είναι φανερό πως ο μέσος όρος των παιδιών που είναι ενεργοί χρήστες σε πολύ μικρή ηλικία αυξάνεται με ταχύτατους ρυθμούς, γεγονός που μόνο ανησυχία μπορεί να προκαλέσει.

Η διαδικτυακή παιδική εκμετάλλευση είναι μάστιγα της σύγχρονης κοινωνίας αφού κακόβουλοι χρήστες του διαδικτύου προσελκύουν με διάφορα τεχνάσματα ανήλικα παιδιά με κύριο σκοπό να τα κακοποιήσουν σεξουαλικά ή να τα παρασύρουν σε επικίνδυνα παιχνίδια θάρρους. Παιδιά ηλικίας άνω των 13 χρόνων είναι πιο ευάλωτα και είναι αυτά που κατέχουν το μεγαλύτερο ποσοστό θυματοποίησής τους καθώς αποκτούν μεγαλύτερη εξοικείωση με τους ηλεκτρονικούς υπολογιστές και τις ηλεκτρονικές συσκευές από όπου και τους δίνεται η δυνατότητα πρόσβασης στο Διαδίκτυο. Η πολύωρη χρήση των ηλεκτρονικών υπολογιστών και κινητών τηλεφώνων σε συνδυασμό με την έλλειψη επικοινωνίας με τους γονείς και την άγνοια των γονιών για τους κινδύνους που διατρέχει ένα παιδί αν η έκθεσή του στο διαδίκτυο είναι

ανεξέλεγκτη και χωρίς την απαραίτητη επίβλεψη αποτελεί πρωταρχική αιτία θυματοποίησης του παιδιού. Ο διαδικτυακός δράστης είναι επιδέξιος στο να εντοπίζει ευάλωτα παιδιά και να συλλέγει τις απαραίτητες πληροφορίες, τις οποίες θα εκμεταλλευθεί ως μέσο εκδήλωσης του ενδιαφέροντος του, εκμεταλλευόμενος τα αισθήματα μοναχικότητας και απομόνωσης του παιδιού. Δημιουργεί πλασματικούς χαρακτήρες και προφίλ στα Μέσα Κοινωνικής Δικτύωσης υποδυόμενος άτομο πολύ μικρότερης ηλικίας, διαφορετικού φύλου ή ακόμα και εταιρεία (π.χ. πρακτορείο μοντέλων) προκειμένου να αποκρύψει την πραγματική ταυτότητά του καθώς και άλλα προσωπικά στοιχεία ώστε να διασφαλιστεί η ανωνυμία του σε πιθανή επιπλοκή. Η επικοινωνία αρχικά ξεκινά με ουδέτερο περιεχόμενο με σκοπό να κάμψει τις αντιστάσεις του παιδιού, να κερδίσει την εμπιστοσύνη του και να εξασφαλίσει την ενεργή συμμετοχή του σε «φιλικές» συνομιλίες.

Μέσω της χρήσης του Διαδικτύου, όπου ευνοείται η ανωνυμία και συγκάλυψη της πραγματικής ταυτότητας, ο δράστης κερδίζει σε μικρότερο χρονικό διάστημα την εμπιστοσύνη του θύματος, ενώ ενδέχεται να ανταλλάσσει συνομιλίες με πολλά θύματα ταυτόχρονα. Σε πολλές περιπτώσεις όταν το υποψήφιο θύμα δημιουργήσει συναισθηματικούς δεσμούς με τον δράστη τότε του ζητείται να προχωρήσει σε συνάντηση από κοντά προκειμένου η «σχέση» να προχωρήσει σε επόμενο επίπεδο. Το θύμα πιστεύοντας ότι θα έρθει σε επαφή με έναν άνθρωπο που εμπιστεύεται και αγαπάει προχωράει στη συνάντηση όπου συνειδητοποιεί ότι το άτομο με το οποίο συνομιλούσε και είχε ανταλλάξει προσωπικές συζητήσεις και ενδεχομένως ευαίσθητο φωτογραφικό υλικό δεν είναι το ίδιο πρόσωπο. Εκεί δίνεται η δυνατότητα στο δράστη να κακοποιήσει το παιδί σεξουαλικά είτε να το απειλήσει με τη δημοσίευση του ήδη υπάρχοντος υλικού, εξασφαλίζοντας περισσότερες προσωπικές φωτογραφίες ή βίντεο του θύματος. Η εξασφάλιση της εμπιστοσύνης και της συναίνεσης του θύματος, η καλλιέργεια συναισθηματικών δεσμών αλλά και ο εκφοβισμός υπό την απειλή της δημοσίευσης προσωπικών στιγμών με κύριο σκοπό τον δημόσιο εξευτελισμό του θύματος συχνά αποτελεί ανασταλτικό παράγοντα για την αναφορά και τον εντοπισμό ανάλογης δραστηριότητας στο διαδίκτυο.

❖ 3.2 Διαδικτυακά Παιχνίδια

Τα online παιχνίδια έχουν κατακλύσει το Διαδίκτυο προκαλώντας το ενδιαφέρον σε ολοένα και περισσότερους χρήστες να συμμετάσχουν ώστε να απολαύσουν και αυτοί την online ψυχαγωγία που τους προσφέρετε. Η εξέλιξή τους στα γραφικά, το εικονικό περιβάλλον, η

θεματολογία και η αλληλεπίδρασή με τους χρήστες σε συνδυασμό με το χαμηλό κόστος και την εύκολη προσβασιμότητα έχουν συμβάλλει στο να αποκτήσουν σπουδαία αναγνωρισιμότητα. Ανάμεσα στο θαυμαστό αυτό κόσμο των διαδικτυακών παιχνιδιών βρίσκεται και ένα αγκάθι γνωστό ως «διαδικτυακά παιχνίδια πρόκλησης ή διαδικτυακά παιχνίδια θανάτου».

Τα επικίνδυνα διαδικτυακά «παιχνίδια» που θέτουν σε κίνδυνο τη σωματική ακεραιότητα των χρηστών μονοπωλούν συχνά την επικαιρότητα. Στόχος τους είναι ο αυτοτραυματισμός των χρηστών εκπληρώνοντας προκλήσεις, επισφραγίζοντας την επιτυχή περάτωσή τους στον διαχειριστή/επιμελητή του λογαριασμού που έχει θέσει τις προκλήσεις. Τα θύματα κυρίως είναι ανήλικα παιδιά τα οποία προσεγγίζονται από τον κακόβουλο χρήστη μέσω ενός ψεύτικου προφίλ και ξεκινούν την επικοινωνία δημιουργώντας τρυφερούς δεσμούς. Όταν ο θύτης νιώσει πως χειραγωγεί το θύμα τότε του ζητάει να συμμετάσχει σε ένα παιχνίδι. Οι προκλήσεις που δίνονται έχουν σταδιακή αύξηση επικινδυνότητας, με τελικό στόχο το θάνατο του συμμετέχοντα. Οι περισσότεροι από τους συμμετέχοντες στα επικίνδυνα challenges που λαμβάνουν χώρα στο διαδίκτυο είναι παιδιά, έφηβοι και νεαροί ενήλικες.

Γιατί οι νέοι συμμετέχουν σε επικίνδυνα challenges;

- **Η ανάγκη για προσοχή :** Οι νέοι συχνά θέλουν να ξεχωρίζουν από το πλήθος και οι επικίνδυνες προκλήσεις τους δίνουν έναν τρόπο να τραβήξουν την προσοχή και να γίνουν αρεστοί.
- **Αυθόρμητη ενέργεια:** Οι έφηβοι συχνά έλκονται από επίφοβες προκλήσεις. Κομμάτι του να είσαι νέος είναι ο έλεγχος των ορίων, ο πειραματισμός, η λήψη απερίσκεπτων αποφάσεων και ο μιμητισμός.
- **Αψηφώντας τους ενήλικες:** Οι διαδικτυακές προκλήσεις δύναται να χρησιμοποιηθούν ως μέσο για τους νέους να αντισταθούν στους κανόνες και τις υποδείξεις των γονιών τους ή των ενηλίκων σχετικά με τη ζωή τους.

Πολλά είναι τα παιχνίδια που έχουν έρθει στο φως της δημοσιότητας κατά καιρούς . Κάποια από αυτά παραθέτονται στις επόμενες σελίδες.

❖ 3.2.1 Blue Whale

Εικόνα 3.2 : Blue Whale Suicide Game

Το Blue Whale Challenge δεν είναι μια εφαρμογή που μπορείτε να κατεβάσετε ή ένα παιχνίδι που μπορείτε να εγκαταστήσετε στον υπολογιστή σας. Πραγματοποιείται μόνο μέσω συνομιλιών στα social media. Το παιχνίδι «μπλε φάλαινα» ξεκίνησε στη Ρωσία και την πρώτη του εμφάνιση έκανε το 2016 σε αρκετές χώρες ανά τον κόσμο. Στην Ελλάδα το παιχνίδι πρόκλησης έφτασε ένα χρόνο αργότερα το 2017 θέτοντας σε κίνδυνο την ψυχική και σωματική υγεία πολλών ανήλικων παιδιών και κυρίως αυτών που βρίσκονταν σε εφηβικό στάδιο.

Πίσω από το αρρωστημένο αυτό ηλεκτρονικό παιχνίδι είναι ο 21χρονος Ρώσος Philipp Budeikin, ο οποίος συνελήφθη και κρατήθηκε στη φυλακή Kresty στην Αγία Πετρούπολη και τον Μάιο του 2016 κρίθηκε ένοχος για ηθική αυτουργία σε τουλάχιστον 16 περιπτώσεις έφηβων κοριτσιών που τις προέτρεψε να αυτοκτονήσουν. Ο πρώην μαθητής ψυχολογίας που είχε αποβληθεί από το πανεπιστήμιο, ισχυρίστηκε ότι εφηύρε το παιχνίδι το 2013. Στην ομολογία του δήλωσε ότι πρόθεσή του ήταν να «καθαρίσει» την κοινωνία με το να οδηγεί κάποια άτομα στην αυτοκτονία. Συγκεκριμένα στην ανατριχιαστική συνέντευξη δήλωσε «Ναι, το παραδέχομαι πράγματι αυτό έκανα. Μην ανησυχείτε, θα τα καταλάβετε όλα. Όλοι θα καταλάβουν» σημειώνει και συνεχίζει «πέθαναν ευτυχισμένες. Τους έδωσα αυτό που δεν είχαν στην πραγματική ζωή: ζεστασιά, κατανόηση και επαφή… Υπάρχουν οι άνθρωποι και υπάρχουν και τα βιολογικά απόβλητα. Εκείνοι που δεν αντιπροσωπεύουν καμιά αξία για την κοινωνία. Που προκαλούν ή θα προκαλέσουν μόνο ζημιά στην κοινωνία. Καθάριζα την κοινωνία από τέτοια άτομα. Όλα ξεκίνησαν το 2013 όταν δημιούργησα την online κοινότητα, F57. Είχα αυτή την ιδέα για πέντε χρόνια. Ήταν αναγκαίο να ξεχωρίσω τα φυσιολογικά άτομα από τα βιολογικά σκουπίδια».

Την σκυτάλη ανέλαβαν πολλοί άλλοι διεστραμμένοι χρήστες , οι οποίοι αυτοαποκαλέστηκαν επικεφαλής και εξασφάλισαν τη διαιώνιση της θανάσιμης εφεύρεσής του . Η ονομασία του φαινομένου «μπλε φάλαινα» δόθηκε από το θηλαστικό το οποίο πολλές φορές χάνει τον προσανατολισμό του, απομακρύνεται από το κοπάδι και εξοκείλει στη στεριά όπου πεθαίνει εξαιτίας της έλλειψης οξυγόνου. Όπως οι φάλαινες έτσι και οι διαχειριστές του θανάσιμου παιχνιδιού θέλουν να απομακρύνουν τα παιδιά από την κοινωνία, το οικογενειακό, φιλικό και σχολικό τους περιβάλλον με τελικό σκοπό να τα οδηγήσουν στο θάνατό τους .

Τις οδηγίες λαμβάνουν από άγνωστο άτομο, που έχει χρηστεί "επικεφαλής", προκειμένου να ολοκληρώσουν με επιτυχία μια σειρά άκρως επικίνδυνων για την υγεία τους και τη σωματική τους ακεραιότητα δοκιμασιών. Αρχικά τους ζητείτε να σχεδιάσουν σε ένα χαρτί μια φάλαινα και έπειτα να συνεχίσουν κάνοντας το ίδιο στο χέρι τους χαράζοντάς το με μαχαίρι . Τα αρχικά στάδια είναι αρκετά απλά όπως το ξύπνημα στις 4:30 το πρωί, η παρακολούθηση ταινιών τρόμου ή βίαιων και καταθλιπτικών περιεχομένων στο διαδίκτυο. Κατά τη διάρκεια του τα challenge γίνονται σταδιακά όλο και πιο επικίνδυνα (π.χ. αυτοτραυματισμός, αναρρίχηση σε ψηλά κτίρια κ.λπ.). Το παιχνίδι αυτό έχει πάρει παγκόσμιες διαστάσεις με τις αρχές πολλών χωρών να έχουν εκδώσει ειδοποιήσεις προς γονείς και παιδιά, ενώ πολυάριθμα είναι και τα σχετικά δημοσιεύματα από Μέσα Μαζικής Ενημέρωσης του εξωτερικού, που αναφέρουν πως το φαινόμενο λαμβάνει μεγάλες διαστάσεις και έχει εξαπλωθεί πιθανόν ως αυτοδιαδιδόμενη φάρσα που όμως κόστισε την ζωή σε εκατοντάδες παιδιά.

3.2.2 Jonathan Galindo

Εικόνα 3.3 : Jonathan Galindo

Ο Jonathan Galindo αποτελεί μια νέα εκδοχή του εφιαλτικού παιχνιδιού «Blue Whale», που απευθύνεται σε ευάλωτες παιδικές ψυχές και γνωρίζει ταχύτατη εξάπλωση στο χώρο του διαδικτύου και των social media. Η τρομακτική μάσκα που έχει σπείρει τον φόβο σε πολλούς

εφήβους αλλά και σε γονείς έχει παρομοιαστεί με μορφή σκύλου, ποντικιού ή με την παραμορφωμένη εικόνα ενός παιδικού χαρακτήρα κινούμενων σχεδίων, του Γκούφυ. Η μάσκα δημιουργήθηκε από τον παραγωγό κινηματογραφικών ειδικών εφέ, Samuel Canini το 2012, αλλά έκτοτε φωτογραφίες βασισμένες σε αυτή έχουν χρησιμοποιηθεί για τη δημιουργία του χαρακτήρα Jonathan Galindo. Ο κ. Canini επιβεβαίωσε ότι δεν έχει καμία σχέση με το δυσάρεστο τρόπο που χρησιμοποιείται τώρα η μάσκα.

Πίσω από την ανατριχιαστική φιγούρα σύμφωνα με ειδικούς ψυχολόγους και ανθρώπους της Δίωξης Ηλεκτρονικού Εγκλήματος δεν κρύβεται μόνο ένας χρήστης αλλά πολλά καταθλιπτικά άτομα χωρία αξίες και σεβασμό της ανθρώπινης ύπαρξης. Δημοσιεύματα υποστηρίζουν ότι ο πρώτος λογαριασμός με το όνομα Jonathan Galindo ήταν ένας λογαριασμός στο TikTok με όνομα χρήστη @jonathangalindo54. Αυτός ο λογαριασμός καταχωρήθηκε το φθινόπωρο του 2019 και θεωρείται ότι αυτός αναβίωσε το θανατηφόρο παιχνίδι της «μπλε φάλαινας» . Με την πάροδο του χρόνου κλώνοι του Jonathan κατέκλυσαν το διαδικτυακό κόσμο σε Instagram, Facebook, TikTok, Snapchat, Twitter και γενικότερα τις ευρέως διαδεδομένες ηλεκτρονικές πλατφόρμες κοινωνικής δικτύωσης.

Το παιχνίδι ακολουθεί ακριβώς τα ίδια βήματα και μεθοδολογία του «Blue Whale», όμως θεωρείται πιο ανησυχητικό από τον προκάτοχό του καθώς οι κλώνοι του εν λόγω προφίλ είναι πάρα πολλοί σε όλες τις χώρες και έτσι καθίσταται ακατόρθωτη η σύλληψη των «Jonathan» και ο περιορισμός της φρενίτιδας που έχει προκύψει. Για ασφάλεια οι πλατφόρμες κοινωνικής δικτύωσης όπως το Facebook έχουν αποκρύψει από την αναζήτησή hashtags με την επιγραφή **#Jonathan Galindo** γνωστοποιώντας ότι «παραβαίνουν τους Όρους Χρήσης της Κοινότητας», αναφέρει το Διεθνές Ινστιτούτο για την Κυβερνοασφάλεια.

Ο Ιδρυτής του Ινστιτούτου Διεθνούς Κυβερνοασφάλειας (CSI Institute) και Ειδικός Ερευνητής Ηλεκτρονικών Εγκλημάτων**,** Μανώλης Σφακιανάκης δήλωσε σε μια συνέντευξή του πως το δίκτυο του Jonathan Galindo έχει φτάσει και στην Ελλάδα και προσεγγίζει σε ελληνικά δωμάτια επικοινωνίας (Chat Rooms) παιδιά ηλικίας 8 έως 12 ετών. Εκεί, τους προτρέπει να εκπληρώσουν μερικές προκλήσεις, οι οποίες γίνονται βαθμηδόν όλο και πιο επικίνδυνες για την σωματική ακεραιότητα του παιδιού. Σκοπός του είναι να κατευθύνει όλο και περισσότερα παιδιά στην αυτοκτονία.

❖ 3.2.3 Παιχνίδι Πνιγμού

Εικόνα 3.4 : Chocking game

Το παιχνίδι ασφυξίας γνωστό ως παιχνίδι πνιγμού ή παιχνίδι λιποθυμίας ή από τα αγγλικά ως choking game, αναφέρεται στην σκόπιμη αποκοπή οξυγόνου στον εγκέφαλο με στόχο την πρόκληση προσωρινής απώλειας συνείδησης.

Αναστάτωση δημιούργησαν και επεξηγηματικά βίντεο στο διαδίκτυο τα οποία δείχνουν βήμα-βήμα πώς θα πρέπει να εκτελεστεί το challenge, εκτοξεύοντας τη δημοτικότητά του στο ανήλικο κοινό. Εκατοντάδες άνθρωποι, κυρίως νεαρής ηλικίας, ανεβάζουν στο διαδίκτυο βίντεο που έχουν τραβήξει οι ίδιοι και στα οποία φαίνεται να πνίγουν ή να στραγγαλίζουν τους ίδιους τους εαυτούς τους ή ο ένας τον άλλο, προκειμένου να νιώσουν για μερικά δευτερόλεπτα μια αίσθηση «ευφορίας» προτού λιποθυμήσουν. Αφού ολοκληρώσουν την πρόκληση με ανάρτηση στα μέσα κοινωνικής δικτύωσης προκαλούν άλλα άτομα να προχωρήσουν και αυτά στην πραγματοποίηση του challenge. Σε αυτό το επικίνδυνο παιχνίδι που γρήγορα διαδόθηκε η φήμη του, έχουν συμμετοχή κυρίως έφηβα αγόρια προκειμένου να αποδείξουν ότι είναι κυρίαρχα απέναντι στους συνομηλίκους τους και ικανά να διεξάγουν με επιτυχία ένα τέτοιο παιχνίδι χωρίς να επηρεαστεί η υγεία τους.

Σύμφωνα με το Αμερικανικό Κέντρο Ελέγχου και Πρόληψης Νοσημάτων (ΚΕΠΝ) στα πρώτα τρία λεπτά στραγγαλισμού βασικές λειτουργίες του εγκεφάλου όπως η μνήμη, η ισορροπία και το κεντρικό νευρικό σύστημα παραλύουν. Λίγα δευτερόλεπτα πιο μετά το άτομο πεθαίνει. Για όσους επιζούν, η παρατεταμένη στέρηση του οξυγόνου στον εγκέφαλο είναι γνωστό ότι προκαλεί κώμα, επιληπτικές κρίσεις, διασείσεις και αιμορραγίες στα μάτια. Με βάση τα παραπάνω δεν αποτελεί έκπληξη ότι λόγω του μικρού χρονικού διαστήματος που χρειάζεται για να πεθάνει κάποιος από

ασφυξία διαβάζουμε σε άρθρο στην ιστοσελίδα του αμερικανικού TIME, πως τα περιστατικά θανάτων από το «παιχνίδι πνιγμού» είναι δεκάδες μόνο στις ΗΠΑ. Από το 1995 ως το 2007, είχαν καταγραφεί, σύμφωνα με το TIME και πληροφορίες από το Κέντρο Πρόληψης και Ελέγχου Ασθενειών στις ΗΠΑ, 82 περιπτώσεις παιδιών και εφήβων από 6 ως 19 ετών που έχασαν τη ζωή τους αφού επιχείρησαν να παίξουν το επικίνδυνο αυτό παιχνίδι.

Γνωστή στην Ελλάδα έγινε και η ιστορία ενός 12χρονου αγοριού στο Λουτράκι μετά το παιχνίδι πνιγμού που επιχείρησε να παίξει με τους συμμαθητές του, χρειάστηκε να διακομιστεί με ασθενοφόρο του ΕΚΑΒ σε νοσοκομείο της Κορίνθου και από εκεί στο νοσοκομείο Παίδων στην Αθήνα. Ευτυχώς η περιπέτεια του νεαρού αγοριού δεν έληξε άδοξα μιας και με τη βοήθεια των γιατρών ξεπέρασε τον κίνδυνο.

❖ 3.2.4 Fire Fairy

Εικόνα 3.5: Fire Fairy Steps

Η «νεράιδα της φωτιάς» ξεκίνησε στην Ρωσία και είχε ως σκοπό να προτρέψει μικρά κοριτσάκια να ανάψουν τους καυστήρες αερίου στις σόμπες του σπιτιού τους και ακολουθώντας κάποια βήματα στο τέλος θα τις μετέτρεπε σε νεράιδες της φωτιάς .Τα βήματα ήταν τα εξής:

Τα μεσάνυχτα όταν όλοι κοιμούνται, σηκωθείτε από το κρεβάτι σας και πηγαίνετε γύρω από το δωμάτιο τρεις φορές και μετά πείτε τα μαγικά λόγια: «Alfey βασίλειο, γλυκές μικρές νεράιδες, δώστε μου τη δύναμη που σας ζητώ». Στη συνέχεια, πηγαίνετε σιωπηλά στην κουζίνα, όπου κανείς δεν θα σας παρατηρήσει γιατί η μαγεία των λέξεων θα εξαφανιστεί. Ενεργοποιήστε τη σόμπα

αερίου και τους τέσσερις καυστήρες. Αλλά μην το ανάβετε. Δεν θέλετε να κάνετε εγκαύματα, έτσι; Μετά πηγαίνετε για ύπνο. Το μαγικό αέριο θα έρθει σε εσάς, θα το αναπνέετε ενώ κοιμάστε και το πρωί, όταν ξυπνήσετε, πείτε: «Ευχαριστώ Alfey, έχω γίνει νεράιδα». Και θα γίνετε μια πραγματική νεράιδα της φωτιάς.

Έμπνευση του παιχνιδιού αποτέλεσε το καρτούν Winx club. Ο Iginio Straffi, διευθύνων σύμβουλος της Rainbow (η εταιρεία που είναι υπεύθυνη για την επωνυμία Winx club) καταδίκασε το επικίνδυνο παιχνίδι και άσκησε ποινική δίωξη έναντι των δημιουργών του παιχνιδιού. Το fire fairy έγινε γνωστό με την υπόθεση της 5χρονης Sofia Ezhova, που υπέστη σοβαρά εγκαύματα σε ολόκληρο το σώμα στην προσπάθειά της να μετατραπεί σε νεράιδα της φωτιάς.

❖ 3.3 Cyber Bulling

Τα τελευταία χρόνια, οι πλατφόρμες μέσων κοινωνικής δικτύωσης έχουν γίνει κοινός τόπος για τα άτομα να συνδέονται και να αλληλεπιδρούν μεταξύ τους. Δυστυχώς, τα μέσα κοινωνικής δικτύωσης προκάλεσαν επίσης ένα νέο είδος εκφοβισμού - τον διαδικτυακό εκφοβισμό. Ο διαδικτυακός εκφοβισμός έχει αναδειχθεί ως σημαντικό και αυξανόμενο κοινωνικό πρόβλημα σε αυτήν την ψηφιακά συνδεδεμένη εποχή. Είναι μια μορφή εκφοβισμού όπου άτομα χρησιμοποιούν το Διαδίκτυο και τις πλατφόρμες μέσων κοινωνικής δικτύωσης για να παρενοχλήσουν, να εκφοβίσουν ή να υποτιμήσουν τους άλλους, ιδιαίτερα σε περιπτώσεις όπου τα άτομα έχουν διαφορετικές απόψεις, πεποιθήσεις ή τρόπο ζωής. Ο διαδικτυακός εκφοβισμός μπορεί να συμβεί με διάφορες μορφές όπως η διάδοση φημών ή ενοχλητικών πληροφοριών, η αποστολή κειμένων ή εικόνων ή η δημιουργία πλαστών προφίλ για τον εξευτελισμό ή το μαρτύριο των ατόμων που στοχοποιούνται.

Μια από τις σημαντικές προκλήσεις του διαδικτυακού εκφοβισμού είναι ότι μπορεί να συμβεί ανά πάσα στιγμή και το θύμα μπορεί να μην γνωρίζει καν ότι συμβαίνει. Ο διαδικτυακός εκφοβισμός μπορεί να συμβεί ανώνυμα ή με ψευδείς ταυτότητες, καθιστώντας δύσκολη την παρακολούθηση και την ανάληψη ευθύνης των δραστών. Επιπλέον, μπορεί να έχει μακροχρόνιες συνέπειες που επηρεάζουν ένα θύμα ακόμη και πέρα από τον ψηφιακό χώρο. Αυτά θα μπορούσαν να περιλαμβάνουν κατάθλιψη, άγχος, αυτοτραυματισμό και σε ακραίες περιπτώσεις, αυτοκτονία.

Σε έρευνα του Pew Research Center που διεξήχθη από τις 14 Απριλίου έως τις 4 Μαΐου 2022 σχεδόν οι μισοί από τους εφήβους στις ΗΠΑ ηλικίας 13 έως 17 ετών (46%) που ρωτήθηκαν αναφέρουν ότι έχουν βιώσει τουλάχιστον μία από τις έξι συμπεριφορές διαδικτυακού εκφοβισμού.

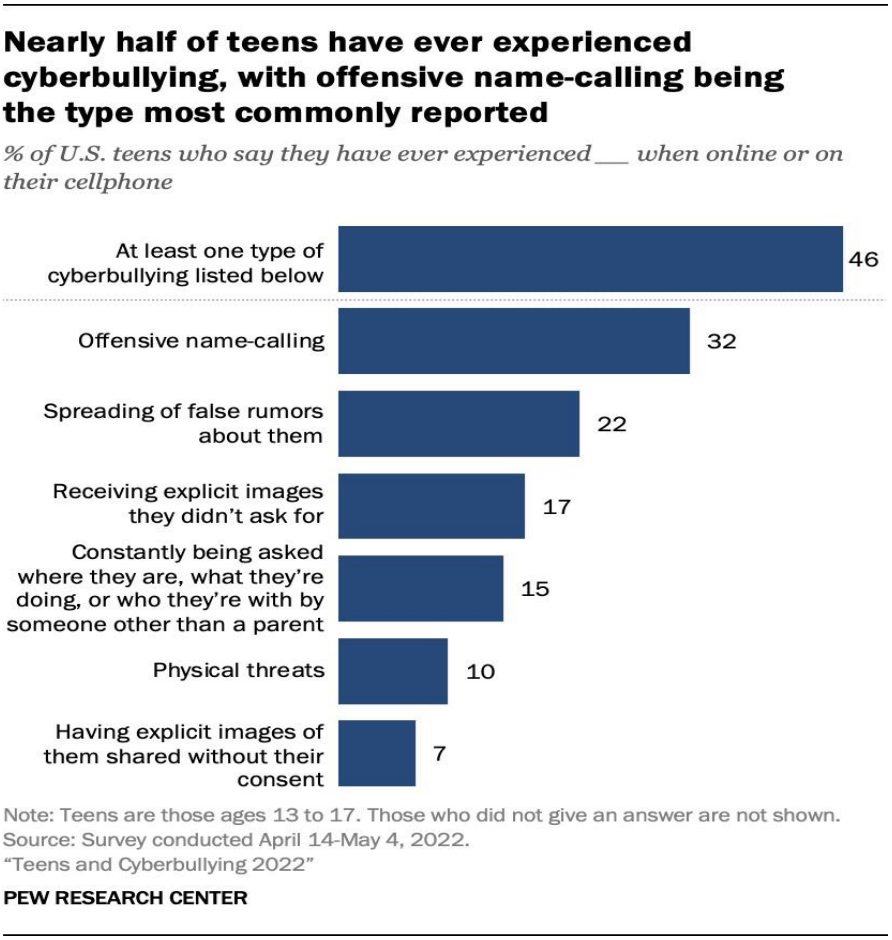
Στη συγκεκριμένη έρευνα χρησιμοποιήθηκαν έξι διακριτές συμπεριφορές:

- Προσβλητικό όνομα
- Διάδοση ψευδών φημών για αυτούς
- Λήψη ακατάλληλων εικόνων που δεν ζήτησαν
- Φυσικές απειλές
- Ερωτήσεις συνεχώς πού είναι, τι κάνουν ή με ποιον είναι από άλλο άτομο εκτός του γονέα
- Κοινή χρήση ακατάλληλων εικόνων τους χωρίς τη συγκατάθεσή τους

Η πιο συχνά αναφερόμενη συμπεριφορά σε αυτήν την έρευνα είναι η χρήση προσβλητικού ονόματος, με το 32% των εφήβων να λένε ότι τους έχουν αποκαλέσει με κάποιο προσβλητικό όνομα ή χαρακτηρισμό στο διαδίκτυο ή στο κινητό τους. Το 22% αναφέρουν ότι είχαν διαδοθεί ψευδείς φήμες σχετικά με αυτούς στο διαδίκτυο και το 17% ότι τους εστάλησαν εικόνες που δεν ζήτησαν. Περίπου το 15% των εφήβων λένε ότι έχουν βιώσει κάποιον άλλο εκτός από έναν γονέα να τους ρωτάει συνεχώς πού είναι, τι κάνουν ή με ποιον είναι, ενώ το 10% ότι έχει απειληθεί σωματικά και το 7% των εφήβων ότι έχουν κοινοποιηθεί εικόνες τους χωρίς τη συγκατάθεσή τους.

Συνολικά, το 28% των εφήβων έχουν βιώσει πολλαπλούς τύπους διαδικτυακού εκφοβισμού.

Στην συγκεκριμένη έρευνα βρέθηκε επίσης ότι η ηλικία και το φύλο σχετίζονται με τις εμπειρίες διαδικτυακού εκφοβισμού των εφήβων, με τα μεγαλύτερα κορίτσια να είναι ιδιαίτερα πιθανό να αντιμετωπίσουν αυτή την κακοποίηση. Επίσης η φυλή, η εθνικότητα και η θρησκεία έπαιξαν σημαντικό ρόλο στη διαδικτυακή στοχοποίηση και κακοποίηση των εφήβων.



Εικόνα 3.6: Έρευνα Pew Research Center

Ενώ ο εκφοβισμός υπήρχε πολύ πριν από το Διαδίκτυο, η άνοδος των τεχνολογικών εξελίξεων και των μέσων κοινωνικής δικτύωσης έδωσε πολύ μεγάλο βήμα σε αυτήν την επιθετική συμπεριφορά και είναι ένα ζήτημα που πρέπει να αντιμετωπιστεί άμεσα και σοβαρά λόγω της σημαντικής επίπτωσης που έχει στη ζωή των θυμάτων.

❖ 3.4 Online Grooming

Online Grooming σύμφωνα με το *Άρθρο 23 της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας εκμετάλλευσης και κακοποίησης, την οποία κύρωσε η χώρα μας με το Ν.3727/2008 (ΦΕΚ Α' 257/18.12.2008)* ορίζεται η διαδικτυακή αποπλάνηση ανηλίκου ή άγρα των παιδιών για γενετήσιους λόγους. Συνοπτικά είναι η προσέλκυση ανηλίκων μέσω της χρήσης της σύγχρονης τεχνολογίας με απώτερο στόχο την τέλεση ασελγών πράξεων ή/και τη συλλογή σχετικού πορνογραφικού υλικού σε βάρος τους, συμπεριφορά η οποία εδράζεται στην προσπάθεια του ενήλικα να αποπλανήσει τον ανήλικο χρήστη του διαδικτύου, δημιουργώντας μια σχέση εμπιστοσύνης, εχεμύθειας και μυστικότητας

όπως αναφέρουν σε άρθρο τους οι Samantha Craven, Sarah Brown και η Elizabeth Gilchrist στο ακαδημαϊκό περιοδικό ¨Journal of Sexual Aggression¨.

Το διαδικτυακό «grooming» συμβαίνει όταν ένας ενήλικας έρχεται σε επαφή μέσω του διαδικτύου με ένα παιδί ή έφηβο προκειμένου να το συναντήσει από κοντά και να το εκμεταλλευτεί. Περιλαμβάνει μια διαδικασία όπου οι groomers κερδίζουν σιγά σιγά την εμπιστοσύνη των θυμάτων τους μέσω φιλικής συνομιλίας και χειριστικών τακτικών σε δημοφιλείς για τα παιδιά και τους εφήβους ιστόχωρους όπως τα κοινωνικά δίκτυα, τα διαδικτυακά παιχνίδια, τα δωμάτια συνομιλίας κ.α. Η πιο συνηθισμένη διαδικασία είναι η εξαπάτηση μέσω ψεύτικου προφίλ δηλώνοντας ψευδή στοιχεία για τον εαυτό τους όπως όνομα, ηλικία, φύλο, ιδιότητα κ.α. Προσπαθούν να δημιουργήσουν μια σχέση άνεσης και εμπιστοσύνης με τους ανήλικους για να μειώσουν τις αναστολές τους με σκοπό να τους κακοποιήσουν σεξουαλικά και πολλές φορές να τους παρασύρουν σε παράνομες επιχειρήσεις όπως η εμπορία παιδιών, η παιδική πορνεία, η διακίνηση σεξ στον κυβερνοχώρο και η παιδική πορνογραφία.

❖ 3.4.1 Παιδική Πορνογραφία

Ο ορισμός της παιδικής πορνογραφίας έχει δοθεί από το Πρόσθετο Πρωτόκολλο στη Σύμβαση του ΟΗΕ για τα δικαιώματα του παιδιού. Σύμφωνα με τον ορισμό αυτό ως παιδική πορνογραφία ορίζεται η οποιαδήποτε αναπαράσταση, με οποιοδήποτε μέσο, παιδιού εμπλεκομένου σε πραγματικές ή εικονικές γενετήσιες δραστηριότητες ή κάθε απεικόνιση των γενετήσιων οργάνων παιδιού για πρωτευόντως σεξουαλικούς σκοπούς. Φυσικά, ο συνηθέστερος τρόπος τέλεσης της παιδικής πορνογραφίας είναι μέσω του διαδικτύου.

Με βάση τη Σύμβαση για το Έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης (Βουδαπέστη, 23.11.2001) η παιδική πορνογραφία περιλαμβάνει πορνογραφικό υλικό που απεικονίζει οπτικά:

- Έναν ανήλικο να εμπλέκεται σε σαφώς σεξουαλική συμπεριφορά.
- Ένα πρόσωπο που φαίνεται ότι είναι ανήλικο να συμμετέχει σε σεξουαλική συμπεριφορά.
- Ρεαλιστικές εικόνες που απεικονίζουν έναν ανήλικο να εμπλέκεται σε σεξουαλική συμπεριφορά .

Η παιδική πορνογραφία είναι μια απεχθής και παράνομη πράξη κατά την οποία παιδιά όλων των ηλικιών, συμπεριλαμβανομένων των βρεφών, κακοποιούνται σεξουαλικά για την ικανοποίηση άλλων. Η χρήση κρυπτογραφημένων εφαρμογών ανταλλαγής μηνυμάτων και ανώνυμων δικτύων, όπως ο σκοτεινός ιστός , έχουν καταστήσει δύσκολο τον εντοπισμό των δραστών κα τη διάσωση θυμάτων. Με την εξέλιξη της τεχνολογίας εμφανίστηκε ένας νέος τύπος σεξουαλικής κακοποίησης σε ζωντανή ροή (live streaming). Σε αυτή την περίπτωση, τα άτομα πληρώνουν για να παρακολουθήσουν ζωντανά την κακοποίηση ενός παιδιού μέσω μιας υπηρεσίας ροής βίντεο. Αυτός ο τύπος κατάχρησης είναι απίστευτα δύσκολο να εντοπιστεί, λόγω της τέλεσής του σε πραγματικό χρόνο και της έλλειψης ψηφιακών αποδεικτικών στοιχείων που μένουν πίσω μετά το έγκλημα.

❖ 3.4.2 Sextortion

Η λέξη sextortion αποτελείται από τις λέξεις sex (σεξ) και extortion (εκβιασμός). Σύμφωνα με την Janis Wolak (Ανώτερη Ερευνήτρια στο Ερευνητικό Κέντρο Εγκλημάτων κατά των Παιδιών και Εργαστήριο Οικογενειακής Έρευνας) το sextortion αναφέρεται στην «*απειλή να εκτεθεί μια σεξουαλική εικόνα για να εξαναγκάσει το θύμα να κάνει κάτι, ακόμα κι αν η έκθεση της εικόνας δεν συμβεί ποτέ στην πραγματικότητα*». Ομοίως, οι Justin Patchin (Καθηγητής Ποινικής Δικαιοσύνης στο Τμήμα Πολιτικών Επιστημών στο Πανεπιστήμιο του Wisconsin-Eau Claire) και ο Sameer Hinduja (Καθηγητής στη Σχολή Εγκληματολογίας και Ποινικής Δικαιοσύνης στο Florida Atlantic University) ορίζουν το sextortion ως «*την επαπειλούμενη διάδοση ξεκάθαρων, οικείων ή ενοχλητικών εικόνων σεξουαλικής φύσης χωρίς συγκατάθεση, συνήθως με σκοπό την απόκτηση πρόσθετων εικόνων, σεξουαλικών πράξεων, χρημάτων ή κάτι άλλο*».

Οι δράστες αυτού του τύπου εγκλήματος συχνά χρησιμοποιούν πλατφόρμες Μέσων Κοινωνικής Δικτύωσης ή ιστότοπους γνωριμιών για να στοχοποιήσουν τα θύματά τους. Πολλοί νέοι, με την πεποίθηση ότι επικοινωνούν με ένα συνομήλικο που ενδιαφέρεται για μια σχέση ή που μπορεί να τους προσφέρει κάτι π.χ. ευκαιρία σταδιοδρομίας στο χώρου του modeling, πείθονται να στείλουν προσωπικές τους φωτογραφίες ή βίντεο. Επίσης οι δράστες μπορούν να χρησιμοποιήσουν κακόβουλο λογισμικό ή μηνύματα ηλεκτρονικού ψαρέματος για να αποκτήσουν πρόσβαση στις συσκευές των στόχων τους. Μόλις έχουν στην κατοχή τους προσωπικό υλικό, μπορούν να το χρησιμοποιήσουν για να εκβιάσουν για σεξουαλικές χάρες, χρήματα ή άλλου είδους υπηρεσίες από τα θύματά τους.

Το sextortion είναι μια ιδιαίτερα επιβλαβής μορφή εγκλήματος στον κυβερνοχώρο, καθώς συχνά περιλαμβάνει την κακοποίηση ευάλωτων ατόμων, όπως τα παιδιά ή οι έφηβοι, με πολλά θύματα να αισθάνονται ντροπή ως αποτέλεσμα των εμπειριών τους. Το sextortion μπορεί να οδηγήσει σε έναν κύκλο κακοποίησης και εκμετάλλευσης, επιφέροντας σημαντική βλάβη στην ψυχική υγεία των θυμάτων.

❖ 3.5 Σημάδια Κακοποίησης & Τρόποι Αντιμετώπισης

Η κακοποίηση και ο διαδικτυακός εκφοβισμός είναι δύο από τα πιο κοινά προβλήματα που αντιμετωπίζουν τα παιδιά και οι ενήλικες στον εικονικό κόσμο. Ως εκ τούτου, είναι σημαντικό για τους γονείς, τους εκπαιδευτικούς και άλλα ενδιαφερόμενα άτομα να συνειδητοποιήσουν τα σημάδια κακοποίησης και διαδικτυακού εκφοβισμού για να αναλάβουν δράση.

Όπως αναφέρουν η Βάνια Φισούν κλινική ψυχολόγος MSc και Υπ. Διδάκτορας Πανεπιστημίου Αθηνών και ο Γεώργιος Φλώρος ψυχίατρος MSc και Υπ. Διδάκτορας στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΑΠΘ) στο βιβλίο “Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κίνδυνου” μερικά από τα σημάδια που χαρακτηρίζονται άκρως ανησυχητικά και υποδηλώνουν ότι το παιδί έχει πέσει θύμα εκφοβισμού ή συμμετέχει σε διαδικτυακά παιχνίδια προκλήσεων είναι τα εξής :

- Εμφανίζεται νευρικό ή αναστατωμένο όταν παρουσιάζεται ένα μήνυμα.
- Το παιδί αιφνίδια διακόπτει την χρήση του υπολογιστή.
- Παρουσιάζει σημάδια κατάθλιψης ή φαίνεται αναστατωμένο μετά τη σύνδεση του στο διαδίκτυο.
- Αποφεύγει συζητήσεις σχετικά με τις ενέργειές του στο διαδίκτυο.
- Χρησιμοποιεί τον υπολογιστή νυχτερινές ώρες.

Το Cyber bulling και το Grooming δρουν διαφορετικά στη ψυχοσύνθεση του παιδιού. Κάποια από τα σημάδια κακοποίησης είναι κοινά και στις δυο αυτές μορφές , ωστόσο αυτά που φανερώνουν ότι ένα παιδί έχει υποστεί σεξουαλική κακοποίηση είναι:

- Σεξουαλική συμπεριφορά ή γνώση σεξουαλικών θεμάτων που δεν συνάδουν με την ηλικία του παιδιού.
- Έντονη και συνεχής ενασχόληση με την περιοχή των γενετικών οργάνων.
- Ντροπή για το σώμα και την αλλαγή ρούχων μπροστά σε άλλους.

- Αδικαιολόγητη ευαισθησία, μώλωπες ή τραυματισμοί στη στοματική ή γενετική περιοχή που δεν αντιστοιχούν σε τυχαίο τραυματισμό.
- Κατοχή αδικαιολόγητων μεγάλων χρηματικών ποσών.

Όλες οι εγκληματικές συμπεριφορές που αναφέρθηκαν σε αυτό το κεφάλαιο έχουν καταστροφικό αντίκτυπο στις ζωές των παιδιών και των εφήβων οδηγώντας τους σε ψυχολογική, συναισθηματική και σωματική βλάβη. Για την καταπολέμηση αυτών των συμπεριφορών στο διαδίκτυο τα άτομα και οι κοινότητες θα πρέπει να συνεργαστούν για να δημιουργήσουν μια κουλτούρα σεβασμού και ενσυναίσθησης στο διαδίκτυο.

Οι εταιρείες τεχνολογίας μπορούν επίσης να διαδραματίσουν κρίσιμο ρόλο στην αντιμετώπιση της διαδικτυακής παιδικής κακοποίησης. Οι πλατφόρμες Μέσων Κοινωνικής Δικτύωσης έχουν την ευθύνη να προωθήσουν ένα ασφαλές και χωρίς αποκλεισμούς διαδικτυακό περιβάλλον. Η εφαρμογή πιο ισχυρών πολιτικών και διαδικασιών που μπορούν να ανιχνεύσουν, να μετριάσουν και να περιορίσουν την ανωνυμία των χρηστών παρέχοντας μηχανισμούς αναφοράς και υποστήριξης για τα θύματα θα μπορούσε να βοηθήσει πολύ.

Οι γονείς και οι εκπαιδευτικοί μπορούν επίσης να συμβάλουν σημαντικά στην καταπολέμηση του διαδικτυακού εκφοβισμού. Η εκπαίδευση των παιδιών και των εφήβων σχετικά με τη διαδικτυακή συμπεριφορά, η διασφάλιση ότι κατανοούν τον αντίκτυπο των λόγων και των πράξεών τους θα τους βοηθήσει πολύ.

Οι γονείς μπορούν να εμπλακούν στις διαδικτυακές δραστηριότητες των παιδιών τους, να παρακολουθούν τη χρήση των Μέσων Κοινωνικής Δικτύωσης και να τους μιλήσουν για την υπεύθυνη διαδικτυακή συμπεριφορά.

Συμπερασματικά, υπάρχει ανάγκη για συλλογική προσπάθεια για την αντιμετώπιση της κακοποίησης και του διαδικτυακού εκφοβισμού. Είναι ένα σύνθετο ζήτημα που απαιτεί συνεργασία από διάφορους φορείς. Αναγνωρίζοντας τη σοβαρότητα του προβλήματος, εκπαιδεύοντας τους νέους και εφαρμόζοντας πιο ισχυρές πολιτικές και διαδικασίες, μπορεί να σημειωθεί πρόοδος στη μείωση της επικράτησης και του αντίκτυπου των παραβατικών συμπεριφορών στο Διαδίκτυο.

ΚΕΦΑΛΑΙΟ 4ο : ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

❖ 4.1 Εισαγωγή στην Κρυπτογραφία

Εικόνα 4.1: Εισαγωγή στην Κρυπτογραφία

Η κρυπτογραφία είναι η επιστήμη η οποία ασχολείται με τη μελέτη ,την ανάπτυξη και χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με τελικό στόχο το αρχικό κείμενο να είναι δυσανάγνωστο ή ευανάγνωστο ανάλογα με τον τελικό παραλήπτη. Στην ιδανική περίπτωση, μόνο εξουσιοδοτημένα μέλη μπορούν να αποκρυπτογραφήσουν ένα κείμενο κρυπτογράφησης σε απλό κείμενο και να αποκτήσουν πρόσβαση στις αρχικές πληροφορίες. Αν ο παραλήπτης του κρυπτοκειμένου γνωρίζει ποιος αλγόριθμος έχει χρησιμοποιηθεί και διαθέτει το κλειδί αποκρυπτογράφησης, τότε μόνο έχει τη δυνατότητα ανάκτησης των δεδομένων. Αντίθετα οι πιθανότητες να κατορθώσει κάποιος, που δεν διαθέτει το κλειδί αποκρυπτογράφησης, να ανακτήσει το πρωτότυπο κείμενο είναι σχεδόν μηδενικές καθώς αντιστοίχως με το «κλειδί» που έχει χρησιμοποιηθεί αλλάζει και η σειρά και τα σύμβολα τα οποία αποτελούν το κρυπτοκείμενο. Για λόγους ασφαλείας τα «κλειδιά» παράγονται από ψευδοτυχαίες γεννήτριες αριθμών ή μέσω αλγορίθμων που μιμούνται τις γεννήτριες ψευδοτυχαίων αριθμών. Κάθε κλειδί διαθέτει το στοιχείο της μοναδικότητας για να εξασφαλίζεται πως κακόβουλοι χρήστες με διάθεση να υποκλέψουν τα μυστικά δεδομένα δεν θα καταφέρουν να προβλέψουν το κλειδί που έχει χρησιμοποιηθεί.

Η κρυπτογραφία παρέχει κάποιες βασικές λειτουργείες:

- **Εμπιστευτικότητα**: Η πληροφορία που θα μεταδοθεί σε περίπτωση που φτάσει σε τρίτους μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη αφού θα είναι ακατανόητο το κείμενο.

- **Ακεραιότητα**: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη.
- **Μη απάρνηση**: Ο παραλήπτης ή ο αποστολέας δεν μπορεί να απαρνηθεί τη μετάδοση ή δημιουργία του κειμένου.
- **Πιστοποίηση:** Ο αποστολέας και ο παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους, την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι παραποιημένες.

❖ 4.1.1 Ιστορία της Κρυπτογραφίας

Εικόνα 4.2: Ιερογλυφικά

Η επιστήμη της κρυπτογραφίας είναι τόσο παλιά όσο και η ανάγκη του κόσμου να κρατήσει ορισμένες πληροφορίες μυστικές. Η ιστορία της κρυπτογραφίας χωρίζεται σε τρείς περιόδους.

- Πρώτη περίοδος κρυπτογραφίας (1900π.Χ. - 1900μ.Χ.)
- Δεύτερη περίοδος κρυπτογραφίας (1900 μ.Χ.-1950 μ.Χ.)
- Τρίτη περίοδος κρυπτογραφίας (1950 μ.Χ. - σήμερα)

Πρώτη περίοδος κρυπτογραφίας (1900π.Χ. - 1900μ.Χ.)

Κατά τη διάρκεια αυτής της περιόδου προόδευσε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές οι πρώιμες κρυπτογραφήσεις δεν προϋπέθεταν ότι ο χρήστης θα διέθετε εξειδικευμένες γνώσεις και πολύπλοκες ηλεκτρονικές συσκευές αλλά βασίζονταν στην ευφυΐα και την ευρηματικότητα.

Το πρώτο ίχνος κρυπτογραφίας κάνει την εμφάνισή του στη Μεσοποταμία και είναι μια σφηνοειδής επιγραφή που απεικονίζει μεθόδους κατασκευής σμάλτων για την αγγειοπλαστική. Στη συνέχεια ακολούθησαν και άλλα συστήματα και συσκευές κρυπτογράφησης που εφευρέθηκαν για στρατιωτική χρήση όπως αύτη της «Σπαρτιατικής Σκυτάλης». Ήταν μια ξύλινη ράβδος γύρω από την οποία ήταν τυλιγμένη μια περγαμηνή που περιείχε το κείμενο γραμμένο σε στήλες και ως «κλειδί» είχε τη διάμετρο της ράβδου.

Εικόνα 4.3: Σπαρτιατική Σκυτάλη

Ωστόσο προκάτοχος στη χρήση αλγόριθμου αντικατάστασης ήταν ο Ιούλιος Καίσαρας. Ο Καίσαρας έγραφε τα μηνύματα που έστελνε στους φίλους του αντικαθιστώντας τα γράμματα του κειμένου με γράμματα που βρίσκονταν τρείς θέσεις μετά στο Λατινικό αλφάβητο. Το σύστημα κρυπτογράφησης του Καίσαρα χρησιμοποιείτε ακόμα στο σύγχρονο πολιτισμό με διάφορες τροποποιήσεις, προκειμένου να καλυφθούν οι ανάγκες ισχυρότερης κρυπτογράφησης και αποκρυπτογράφησης. Ακρογωνιαίο λίθο για την εξέλιξη της κρυπτογραφίας συντέλεσαν οι Άραβες με την επινόηση της κρυπτανάλυσης, η οποία συνδύαζε τη συχνότητα των γραμμάτων κειμένου με τη συχνότητα εμφάνισης στα κείμενα της γλώσσας.

Σπουδαίο επίτευγμα αποτέλεσε και η αποκρυπτογράφηση των ιερογλυφικών από τον Ζαν-Φρανσουά Σαμπολιόν με τη βοήθεια της Στήλης της Ροζέτας, η οποία είναι μια πέτρινη πλάκα από γρανοδιορίτη που προέρχεται από τον ναό του Πτολεμαίου Ε' του Επιφανούς και φέρει μια εγχάρακτη επιγραφή σε δύο γλώσσες (αιγυπτιακή και ελληνική) και τρία συστήματα γραφής (ιερογλυφικά, δημώδη αιγυπτιακή και ελληνική).

Εικόνα 4.4: Στήλη της Ροζέτας

Την περίοδο αυτή στον Ελληνικό χώρο εμφανίζονται οι Γραμμικές γραφές Α και Β. Σημαντικότερο εύρημα της Γραμμικής Α είναι ο δίσκος της Φαιστού που αποτελεί μέχρι και σήμερα ένα άλυτο μυστήριο καθώς ακόμα δεν έχει καταφέρει κανείς να την αποκρυπτογραφήσει.

Εικόνα 4.5: Δίσκος της Φαιστού

Δεύτερη περίοδος κρυπτογραφίας (1900 – 1950μ.Χ.)

Εικόνα 4.6: Μηχανή Κρυπτογράφησης Enigma

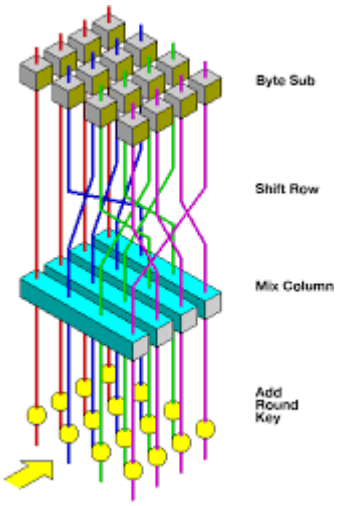
Η δεύτερη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Εξαιτίας των δύο παγκοσμίων πολέμων παρουσιάζεται μεγάλη ανάγκη για μετάδοση πληροφοριών, με αποτέλεσμα την εκρηκτική ανάπτυξη της κρυπτογραφίας μέσα σε μόλις 50 χρόνια. Τα κρυπτοσυστήματα γίνονται πολύπλοκα και αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές».

Στο τέλος του πρώτου παγκοσμίου πολέμου ο Γερμανός Arthur Scherbius εφηύρε της ηλεκτρομηχανικές συσκευές κρυπτογράφησης Enigma. Ο πολωνός μαθηματικός Marian

Rajewski κατάφερε το 1932 να σπάσει τον κώδικα που χρησιμοποιούσε το σύστημα Enigma. Το 1939 οι Γερμανοί προχωρούν σε αλλαγές στο σύστημα τις οποίες αδυνατούν να παρακολουθήσου οι πολωνοί λόγω των ελάχιστων πόρων που διέθεταν έτσι αναγκάζονται να παραχωρήσουν γνώσεις και μηχανές σε Βρετανούς και Γάλλους. Κατά τη διάρκεια του δευτέρου παγκοσμίου πολέμου ο Βρετανός μαθηματικός Alan Turing διαδραματίζει καθοριστικό ρόλο στην υπηρεσία Βρετανικής Αντικατασκοπίας για την αποκρυπτογράφηση του συστήματος Enigma.

Την ίδια περίοδο χώρες που ενεπλάκησαν στο δεύτερο παγκόσμιο πόλεμο δημιούργησαν συστήματα κρυπτογράφησης όπως το Βρετανικό TypeX, το Αμερικάνικο SIGABA , το Ιαπωνικό Purple.

Τρίτη περίοδος κρυπτογραφίας (1950 μ.Χ.– σήμερα)



Εικόνα 4.7: AES Algorithm

Η Τρίτη περίοδος είναι η εποχή της σύγχρονης κρυπτογραφίας. Η μεγάλη εξέλιξη στους κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων συντέλεσαν στην αλματώδη ανάπτυξη της κρυπτογραφίας. Ο Αμερικανός Claude Shannon θεωρείται ο «πατέρας της θεωρίας της πληροφορίας» και ήταν αυτός που με τις εργασίες του από το 1948 έως το 1951 καθιέρωσε μια στέρεα θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση.

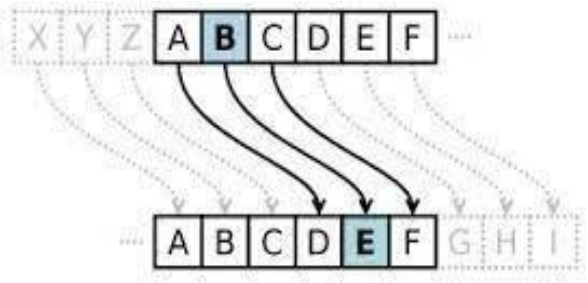
Η κρυπτογραφία μέχρι τη δεκαετία του '70 χρησιμοποιείται κυρίως για πολεμικούς σκοπούς και από μυστικές υπηρεσίες για κυβερνητικές επικοινωνίες όπως την Υπηρεσία Εθνικής Ασφάλειας (National Security Agency, NSA) των ΗΠΑ, αρμόδια για την ασφάλεια των επικοινωνιών. Ωστόσο, αυτό αλλάζει όταν επιχειρήσεις όπως τράπεζες και μεγάλες

οικονομικές οργανώσεις αναγνωρίζουν τις δυνατότητες που τους προσφέρει η κρυπτογραφία για την ασφάλεια των δεδομένων και των επικοινωνιών. Στα μέσα της δεκαετίας του '70, η IBM δημιουργεί τον αλγόριθμο Lucifer, ο οποίος λειτουργεί σε ομάδες bits σταθερού μήκους που ονομάζονται blocks. Το μήκος κλειδιού που χρησιμοποιείται είναι 56 bit καθιστώντας το ανασφαλές για εφαρμογές. Ο Lucifer συνδύασε την κρυπτογράφηση μεταφοράς και αντικατάστασης και οδήγησε σε αυτό που είναι σήμερα γνωστό ως Πρότυπο Κρυπτογράφησης Δεδομένων (DES).

Το 2001, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) επέλεξε το Προηγμένο Πρότυπο Κρυπτογράφησης (AES) για να αντικαταστήσει το DES. Το AES χρησιμοποιεί έναν αλγόριθμο συμμετρικού κλειδιού και είναι ένα υποσύνολο της κρυπτογράφησης μπλοκ Rijandael και χρησιμοποιεί μεγαλύτερα μήκη κλειδιών 128, 192 και 256 bit, με μέγεθος μπλοκ 128 bit.

❖ 4.1.2 Γνωστοί Αλγόριθμοι Κρυπτογράφησης

1. **Αλγόριθμος του Καίσαρα**



Εικόνα 4.8: Caesar algorithm

Ο αλγόριθμος του Καίσαρα αποτελεί έναν από τους πιο γνωστούς τρόπους κρυπτογράφησης κειμένου. Είναι χαρακτηριστικό παράδειγμα μονοαλφαβητικού κρυπτοσυστήματος αντικατάστασης και θεωρείται αναξιόπιστος επειδή είναι τρωτός σε ένα τύπο ανάλυσης που λέγεται ανάλυση συχνότητας. Η κρυπτογράφηση και αποκρυπτογράφηση γίνεται με τη χρήση του ίδιου αλφαβήτου μετατοπισμένου κατά k γράμματα. Έτσι αν κάποιος βρει το κλειδί δηλαδή το k τότε μπορεί εύκολα να «σπάσει» τον αλγόριθμο και να φανερώσει το κρυπτοκείμενο.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Εικόνα 4.9: Πίνακας για το Παράδειγμα του Caesar algorithm

Οπότε, εάν κρυπτογραφούσαμε τη λέξη «ENCRYPTION» με κλειδί ίσο με k=3, τότε το αποτέλεσμα θα ήταν «HQFUBSWLRP» και βλέπετε στη συνέχεια πως εξηγείται αυτό με τις παραπάνω μαθηματικές αναπαραστάσεις για το πρώτο γράμμα της λέξης «ENCRYPTION», το γράμμα E.

k=3 και p=E δηλαδή 4

c = (p+k) mod 26

Άρα c =(4+3) mod 26 => c = 7 mod 26

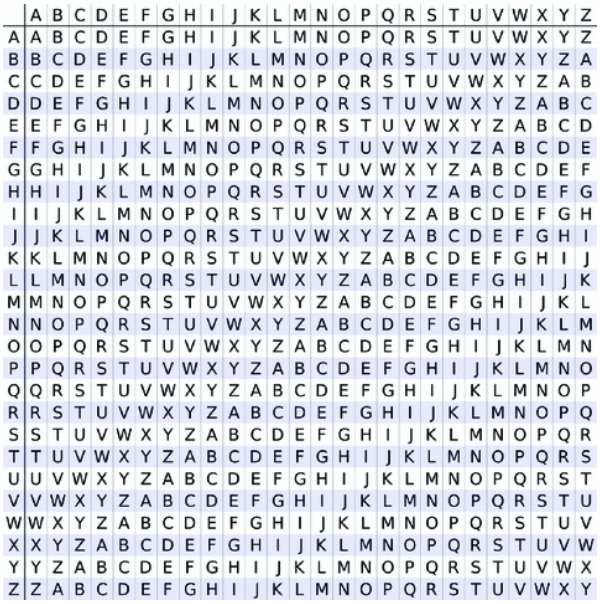
c=7 => c=H

Επομένως το E θα γίνει H

Τα ίδια βήματα θα επαναλάβουμε και για τα επόμενα γράμματα της λέξης που θέλουμε να κρυπτογραφήσουμε.

2. Αλγόριθμος κρυπτογράφησης Vigenère

Ο αλγόριθμος κρυπτογράφησης Vigenère είναι μία μέθοδος κρυπτογράφησης σε αλφαβητικό κείμενο στο οποίο εφαρμόζονται διαφορετικοί αλγόριθμοι καίσαρα με βάση τη θέση των γραμμάτων μιας λέξης ή φράσης κλειδί. Για την κρυπτογράφηση γίνεται χρήση ενός πίνακα του αλφάβητου (Vigenère table) ως πίνακας αντικατάστασης. Αποτελείται από το αλφάβητο, που αναγράφεται σε διαφορετικές γραμμές και στήλες τόσες φορές όσες και τα γράμματα του αλφαβήτου και κάθε αλφάβητο μετατοπίζεται κυκλικά σε σχέση με το προηγούμενο αλφάβητο, ώστε να υπάρχουν όλοι οι πιθανοί αλγόριθμοι κρυπτογράφησης του Καίσαρα. Κατά τη διαδικασία κρυπτογράφησης, χρησιμοποιείται διαφορετικό αλφάβητο σε κάθε ένα από τα γράμματα. Το αλφάβητο που χρησιμοποιείται σε κάθε γράμμα εξαρτάται από μια επαναλαμβανόμενη λέξη-κλειδί.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Εικόνα 4.10: Πίνακας για το Παράδειγμα του Vigenère Algorithm

Εάν το γράμμα του κλειδιού είναι “x” και το γράμμα του plaintext “y”, το αντίστοιχο ciphertext γράμμα είναι αυτό που βρίσκεται στην τομή της γραμμής που ξεκινάει με το “x” και της στήλης με επικεφαλίδα “y”. Δηλαδή θα είναι το “v”

Επειδή το κλειδί πρέπει να είναι τόσο μεγάλο όσο και το plaintext, αυτή η μυστική λέξη συνεχώς επαναλαμβάνεται

plaintext: findthehiddentext (17 χαρακτήρες)

key: encryption

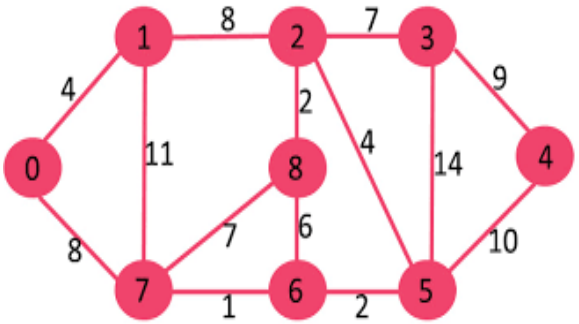
keysystem: encryptionencrypt (17 χαρακτήρες)

ciphertext: jvpurwxpwqhrpkcmm

3. Αλγόριθμος Dijkstra

Ο αλγόριθμος του Dijkstra πήρε το όνομά του από τον Ολλανδό Edsger Wybe Dijkstra. Πρόκειται για έναν αλγόριθμο, ο οποίος διερευνάει και ανιχνεύει τις συντομότερες διαδρομές από κοινή αφετηρία σε έναν γράφο με μη αρνητικά βάρη. Στο παραπάνω σχήμα γράφοι αποτελούν οι ροζ αριθμημένοι κύκλοι και βάρη οι αριθμοί που βρίσκονται στις ενώσεις των γράφων. Ο αλγόριθμος σε κάθε βήμα του επιλέγει την τοπικά βέλτιστη λύση.

Συγκεκριμένα προσπαθεί να βρει τη διαδρομή που με το πέρας της θα έχει τα λιγότερα βάρη.



Εικόνα 4.11: Σχήμα για το Παράδειγμα του Dijkstra Algorithm

Αν από τον γράφο 0 θέλουμε να πάμε στον γράφο 8 τότε μας δίνονται οι εξής επιλογές στις διαδρομές

Διαδρομή 1 : 0-1-2-8=4+8+2=14

Διαδρομή 2 :0-1-7-8=4+11+7=22

Διαδρομή 3 :0-7-8=8+7=15

Διαδρομή 4 :0-7-6-8=8+1+6=15

Επομένως η διαδρομή που πρέπει να ακολουθήσουμε είναι η πρώτη καθώς έχει τα μικρότερα βάρη και άρα είναι η βέλτιστη.

4. Αλγόριθμος RSA

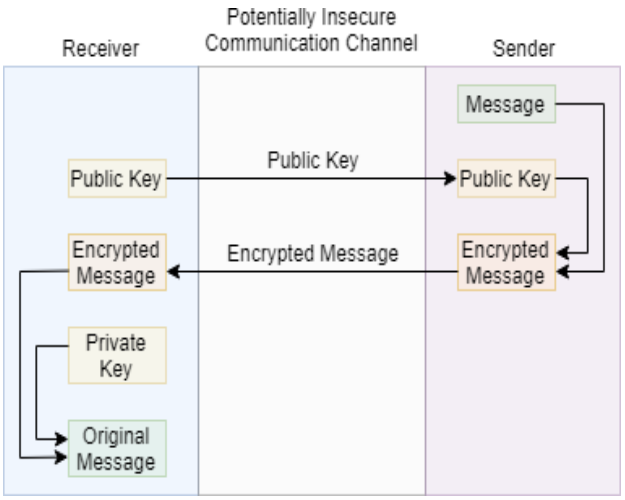
Ο αλγόριθμος RSA είναι ασύμμετρος αλγόριθμος κρυπτογραφίας. Το ασύμμετρο σημαίνει στην πραγματικότητα ότι λειτουργεί σε δύο διαφορετικά κλειδιά, δηλαδή Δημόσιο Κλειδί και Ιδιωτικό Κλειδί**.** Το δημόσιο κλειδί δίνεται σε όλους και το ιδιωτικό κλειδί παραμένει ιδιωτικό. Σημαντικό χαρακτηριστικό του αποτελεί ότι επιτρέπει όχι μόνο την κωδικοποίηση μηνυμάτων αλλά μπορεί επίσης να χρησιμοποιηθεί και ως ψηφιακή υπογραφή**.**

Ένα παράδειγμα ασύμμετρης κρυπτογραφίας:

1. Ένας πελάτης στέλνει το δημόσιο κλειδί του στο διακομιστή και ζητά ορισμένα δεδομένα.
2. Ο διακομιστής κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το δημόσιο κλειδί του πελάτη και στέλνει τα κρυπτογραφημένα δεδομένα.

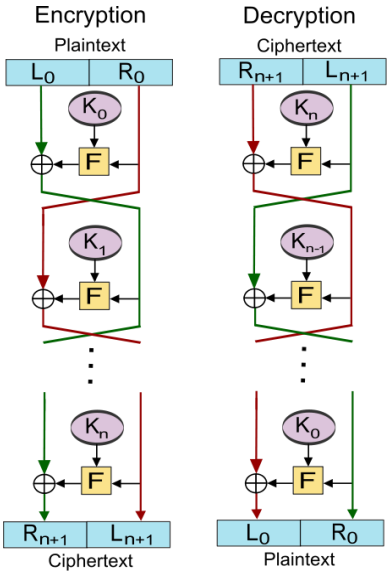
3. Ο πελάτης λαμβάνει αυτά τα δεδομένα και τα αποκρυπτογραφεί.

Δεδομένου ότι αυτό είναι ασύμμετρο, κανένας άλλος εκτός από το πρόγραμμα περιήγησης δεν μπορεί να αποκρυπτογραφήσει τα δεδομένα, ακόμη και αν ένα τρίτο μέρος έχει δημόσιο κλειδί προγράμματος περιήγησης.



Εικόνα 4.12: Σχήμα για την κατανόηση λειτουργείας του RSA Algorithm

5. Αλγόριθμος DES



Εικόνα 4.13: Σχήμα για την κατανόηση λειτουργείας του DES Algorithm

Το πρότυπο κρυπτογράφησης δεδομένων (DES) είναι ένας αλγόριθμος συμμετρικού κλειδιού για την κρυπτογράφηση ψηφιακών δεδομένων. Το αρχικό κείμενο έχει μήκος 64 bit και το κλειδί έχει μήκος 56 bit. Στην πραγματικότητα το αρχικό κλειδί έχει μέγεθος 64 bit, αλλά μόνον τα 56 από αυτά συμμετέχουν στην κρυπτογράφηση, τα υπόλοιπα 8 bit του κλειδιού

χρησιμοποιούνται για αρτιότητα (parity bits). Η δομή του αλγορίθμου DES αποτελεί μια μικρή διαφοροποίηση του δικτύου Feistel. Υπάρχουν 16 γύροι επεξεργασίας. Από το αρχικό κλειδί των 56 bit παράγονται 16 υποκλειδιά, καθένα από τα οποία χρησιμοποιείται σε ένα γύρο. Παίρνει μια σειρά από bit απλού κειμένου (plaintext bits) σταθερού μήκους και την τροποποιεί μέσω μιας σειράς πολύπλοκων ενεργειών σε μια άλλη σειρά bit, το κρυπτοκείμενο (chiphertext) με το ίδιο μήκος. Όταν χρησιμοποιείται για την επικοινωνία, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν το ίδιο μυστικό κλειδί, το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος ή για τη δημιουργία και την επαλήθευση ενός κώδικα ταυτότητας μηνυμάτων. Ο DES μπορεί επίσης να χρησιμοποιηθεί για μεμονωμένους χρήστες κρυπτογράφησης, όπως για την αποθήκευση αρχείων σε ένα σκληρό δίσκο σε κρυπτογραφημένη μορφή.

❖ 4.2 Ιστορία του Bitcoin

Εικόνα 4.14: Bitcoin

Το Bitcoin εφευρέθηκε το 2008 από ένα άγνωστο άτομο ή ομάδα που ονομάζεται Satoshi Nakamoto. Ωστόσο, η προέλευση του κρυπτονομίσματος μπορεί να εντοπιστεί ακόμη πιο πίσω στα τέλη της δεκαετίας του 1990, όταν έγιναν προσπάθειες να δημιουργηθεί ένα ψηφιακό νόμισμα που θα μπορούσε να λειτουργήσει σαν μετρητά. Οι πρώτες ιδέες παρεμποδίστηκαν από προβλήματα διπλής δαπάνης, όπου ένα μόνο ψηφιακό νόμισμα μπορούσε να χρησιμοποιηθεί περισσότερες από μία φορές.

Το Bitcoin ήταν η πρώτη επιτυχημένη προσπάθεια επίλυσης αυτού του προβλήματος, χρησιμοποιώντας ένα αποκεντρωμένο δίκτυο που ονομάζεται blockchain για την αποφυγή διπλών δαπανών. Το Blockchain είναι αρχεία που συνδέονται μεταξύ τους χρησιμοποιώντας

μηχανισμούς κρυπτογραφίας. Είναι σαν μια «αλυσίδα» δεδομένων ανθεκτική σε αλλαγές και τροποποιήσεις που για να εκτελέσει ή να επιβεβαιώσει τις «κινήσεις» των χρηστών της, χρειάζεται υπολογιστική ισχύ και πολλά ανεξάρτητα και αξιόπιστα μέλη τα οποία θα επιβεβαιώσουν τις συναλλαγές. Είναι ένα εργαλείο πολυδιάστατο το οποίο θεωρείται πρωτοποριακό λόγω της ασφάλειας που παρέχει.

Στις πρώτες μέρες, το Bitcoin χρησιμοποιήθηκε κυρίως από λάτρεις της τεχνολογίας και διαδικτυακούς εγκληματίες. Ωστόσο, η χρήση του εξαπλώθηκε γρήγορα και σύντομα έγινε σαφές ότι αυτή η νέα μορφή νομίσματος είχε τη δυνατότητα να φέρει επανάσταση στον κόσμο των οικονομικών. Η πρώτη συναλλαγή σε Bitcoin που πραγματοποιήθηκε στον πραγματικό κόσμο έγινε στις 22 Μάιου 2010 . Ο προγραμματιστής Lazlo Hanyecz, με ανάρτηση του σε ένα φόρουμ προσέφερε 10.000 Bitcoins σε όποιον είτε αγόραζε είτε μαγείρευε δυο πίτσες και τις διένειμε στο σπίτι του. Ένας άλλος χρήστης του φόρουμ δέχτηκε και έτσι πραγματοποιήθηκε η συναλλαγή. Η μέρα έμεινε γνωστή ως «Bitcoin Pizza Day». Η τιμή του Bitcoin εκτινάχθηκε στα ύψη και κατέρρευσε επανειλημμένα, υποκινούμενη από το αυξανόμενο ενδιαφέρον και τις εικασίες γύρω από αυτό. Το 2013 η αξία του Bitcoin ξεπέρασε για λίγο τα 1.000 $ ανά νόμισμα πριν καταρρεύσει ξανά.

Από τότε, το Bitcoin συνέχισε να κερδίζει σε δημοτικότητα, με όλο και περισσότερες επιχειρήσεις να το αποδέχονται ως τρόπο πληρωμής. Η αποκεντρωμένη φύση του το καθιστά επίσης ελκυστικό για όσους θέλουν να παρακάμψουν τα παραδοσιακά τραπεζικά συστήματα, συμπεριλαμβανομένων των ανθρώπων που ζουν σε χώρες με ασταθή νομίσματα ή υψηλό πληθωρισμό. Ενώ υπήρξαν ορισμένες αμφιβολίες και διαφωνίες γύρω από το Bitcoin όσον αφορά τη συσχέτισή του με εγκληματικές δραστηριότητες, παραμένει μια ισχυρή δύναμη στον κόσμο των οικονομικών με μια συναρπαστική ιστορία.

❖ 4.2.1 Χαρακτηριστικά και Λόγοι Προτίμησης Bitcoin

Ένα από τα κυριότερα χαρακτηριστικά που κάνει τα Bitcoin προτιμότερα από τα συμβατικά νομίσματα είναι η ανωνυμία. Όταν πρόκειται για παραδοσιακούς τρόπους πληρωμής, όπως πιστωτικές κάρτες ή τραπεζικά εμβάσματα, συχνά απαιτούνται προσωπικά στοιχεία. Με το Bitcoin, αυτό δεν συμβαίνει, καθώς δεν απαιτούνται προσωπικά στοιχεία κατά την πραγματοποίηση συναλλαγών. Το σύστημα λειτουργεί σε ένα δίκτυο peer-to-peer (ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους

ισοδύναμα) στο οποίο οι ταυτότητες των χρηστών του παραμένουν ανώνυμες. Για να στείλουν ή να λάβουν Bitcoins, οι χρήστες πρέπει πρώτα να δημιουργήσουν ένα πορτοφόλι. Αυτό μπορεί να γίνει είτε με λήψη ενός λογισμικού πορτοφολιού σε υπολογιστή ή κινητό τηλέφωνο είτε με εγγραφή σε μια διαδικτυακή υπηρεσία πορτοφολιού. Κάθε πορτοφόλι έχει μια μοναδική διεύθυνση, η οποία χρησιμοποιείται για την αποστολή και λήψη Bitcoin. Για την αποστολή Bitcoin, οι χρήστες πρέπει απλώς να εισάγουν τη διεύθυνση του παραλήπτη και το ποσό που επιθυμούν να στείλουν. Στη συνέχεια πρέπει να επιβεβαιώσουν τη συναλλαγή εισάγοντας ένα ιδιωτικό κλειδί, το οποίο είναι ένας μυστικός κωδικός που εξουσιοδοτεί τη μεταφορά. Μόλις επιβεβαιωθεί η συναλλαγή, υποβάλλεται σε επεξεργασία από το δίκτυο, επαληθεύεται από εξορύκτες και προστίθεται στο Blockchain. Αυτή η δυνατότητα του Bitcoin είναι ιδιαίτερα χρήσιμη για όσους εκτιμούν το απόρρητό τους και δεν θέλουν οι συναλλαγές τους να παρακολουθούνται.

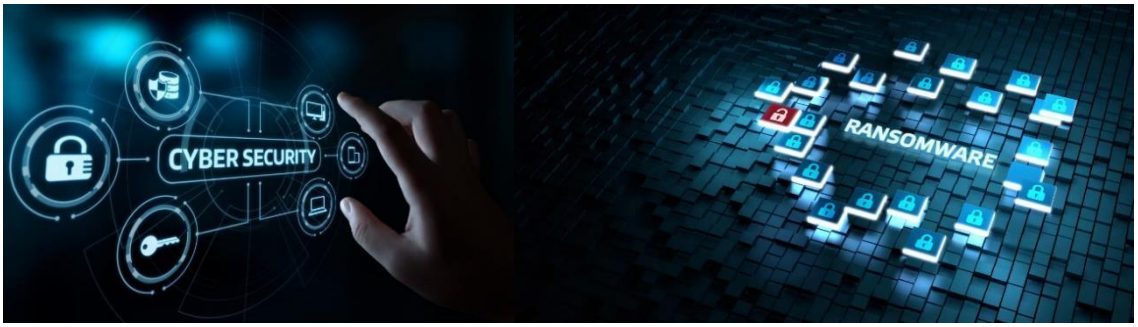
Ένα άλλο χαρακτηριστικό των συναλλαγών με Bitcoins είναι η ταχύτητα. Όλες οι συναλλαγές διεκπεραιώνονται σε λίγα μόλις λεπτά. Επιπλέον αυτές οι συναλλαγές είναι μη αναστρέψιμες, δηλαδή κάθε συναλλαγή που πραγματοποιείται δεν μπορεί να ανακληθεί εκτός και αν ο παραλήπτης επιστρέψει το χρηματικό ποσό.

Τέλος, τα Bitcoin είναι προτιμότερα επειδή προσφέρουν χαμηλές χρεώσεις συναλλαγών σε σύγκριση με τις παραδοσιακές μεθόδους πληρωμής όπου οι χρεώσεις συναλλαγών μπορεί να είναι αρκετά υψηλές και μπορεί να προκαλέσουν καθυστερήσεις ή δυσκολίες κατά την πραγματοποίηση άμεσων συναλλαγών. Με το Bitcoin, τα τέλη που χρεώνονται για συναλλαγές είναι σχετικά χαμηλότερα και συνήθως επεξεργάζονται γρήγορα. Αυτό τα καθιστά μια οικονομικά αποδοτική επιλογή για όσους θέλουν να κάνουν άμεσες πληρωμές χωρίς να ανησυχούν για το υψηλό κόστος που σχετίζεται με τις τραπεζικές προμήθειες.

❖ 4.3 Συμβολή της Κρυπτογραφίας στην Εγκληματικότητα στο Διαδίκτυο

Η κρυπτογραφία, ένα ζωτικό εργαλείο για την ασφάλεια των ψηφιακών επικοινωνιών μέσω κωδικών και κρυπτογράφησης έχει παίξει σημαντικό ρόλο στο έγκλημα στον κυβερνοχώρο. Ένας από τους πιο συνηθισμένους τρόπους χρήσης της κρυπτογραφίας στο διαδικτυακό έγκλημα είναι μέσω της κρυπτογράφησης. Η κρυπτογράφηση χρησιμοποιείται ευρέως σε επιθέσεις Ransomware. Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που

κρυπτογραφεί τα προσωπικά ή επιχειρηματικά δεδομένα ενός χρήστη και απαιτεί πληρωμή (συχνά σε Bitcoin) σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης.



Εικόνα 4.15: Ransmoware

Μια άλλη μορφή κρυπτογραφίας που χρησιμοποιείται όλο και περισσότερο από εγκληματίες του ίντερνετ είναι η στεγανογραφία, μια διαδικασία απόκρυψης ενός μηνύματος σε άλλο μέσο, όπως μια εικόνα ή ένα αρχείο βίντεο. Χρησιμοποιούν στεγανογραφία για να ενσωματώσουν τα μηνύματά τους σε νόμιμα αρχεία , επιτρέποντάς τους την λαθραία επικοινωνία και την αποφυγή του εντοπισμού τους από τις αρχές. Η χρήση της έχει γίνει πιο διαδεδομένη τα τελευταία χρόνια καθώς γίνεται πιο περίπλοκη και δύσκολη η ανίχνευσή της.

Ένας άλλος τρόπος με τον οποίο η κρυπτογραφία συνέβαλε στο έγκλημα στον κυβερνοχώρο είναι μέσω της χρήσης κρυπτονομισμάτων όπως τα Bitcoins (BTC). Τα Bitcoins έχουν χρησιμοποιηθεί για τη νομιμοποίηση εσοδών από παράνομες δραστηριότητες. Οι κακόβουλοι χρήστες μπορούν να μεταφέρουν τα παράνομα κεφάλαιά τους από παραδοσιακό νόμισμα σε bitcoin και στη συνέχεια να το ξαναμετατρέψουν σε νόμισμα fiat (χρήματα που ελέγχονται από τις κυβερνήσεις και τις κεντρικές τράπεζες) για να φαίνονται νόμιμα. Αυτό έχει ως αποτέλεσμα την μετακίνηση υπέρογκων χρηματικών ποσών πέρα από τα διεθνή σύνορα με ελάχιστο έλεγχο.

Επιπλέον όσοι παρανομούν στο χώρο του Διαδικτύου χρησιμοποιούν την κρυπτογραφία για να διαπράττουν εγκλήματα όπως διακίνηση παράνομων αγαθών (ναρκωτικών και όπλων), παιδική πορνογραφία, sextortion κ.α. Οι εγκληματίες χρησιμοποιούν κρυπτογραφημένα μηνύματα μέσω κρυπτογραφημένων υπηρεσιών ανταλλαγής μηνυμάτων όπως το Signal, το Telegram και το Wickr που επιτρέπουν την απρόσκοπτη επικοινωνία χωρίς να αφήνουν κανένα ίχνος. Αυτό καθιστά σχεδόν αδύνατο για τις αρχές να παρακολουθούν την επικοινωνία και τις δραστηριότητές τους, να τους εντοπίσουν και να τους διώξουν.

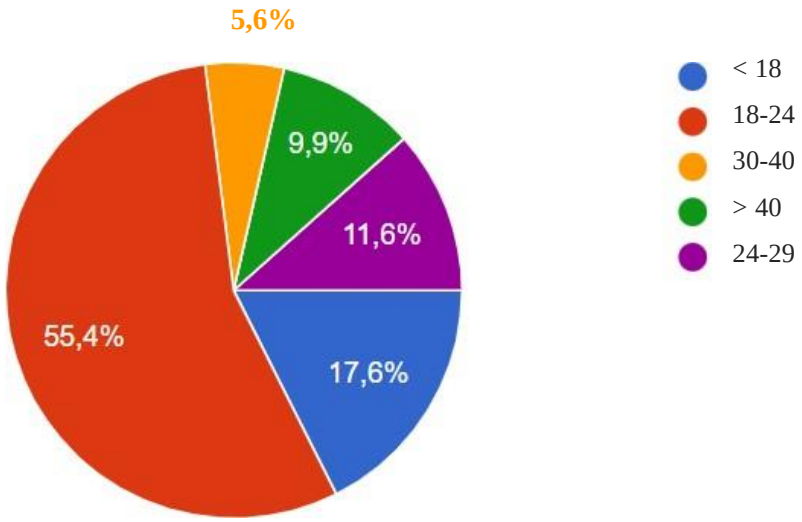
Συμπερασματικά, η χρήση της κρυπτογραφίας στο έγκλημα αποτελεί σημαντική ανησυχία για την επιβολή του νόμου. Οι άνθρωποι βασίζονται όλο και περισσότερο στην τεχνολογία καθιστώντας όλο και πιο επιτακτική την ανάγκη για ανάπτυξη πιο προηγμένων μέτρων ασφαλείας για την καταπολέμηση της εγκληματικής χρήσης τεχνολογιών κρυπτογράφησης. Οι κυβερνήσεις και οι επιχειρήσεις πρέπει να υιοθετήσουν ισχυρά πρωτόκολλα ασφαλείας και καλύτερα ρυθμιστικά μέτρα για την πρόληψη του εγκλήματος και την προστασία των πολιτών τους.

ΚΕΦΑΛΑΙΟ 5ο : ΠΑΡΟΥΣΙΑΣΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

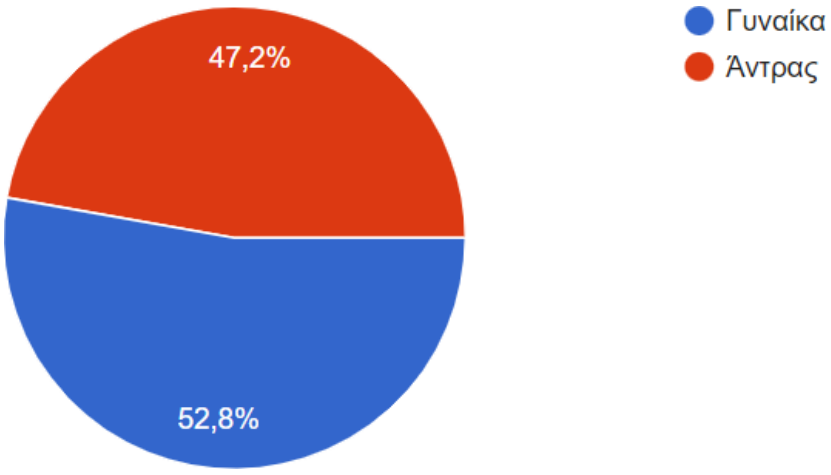
Παρακάτω παρατίθενται τα αποτελέσματα έρευνας που διενεργήθηκε στα πλαίσια της παρούσας πτυχιακής εργασίας στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου, από τη φοιτήτρια Αντωνία Φωτοπούλου υπό την επίβλεψη του καθηγητή Γιώργου Ασημακόπουλου.

Το ερωτηματολόγιο ήταν ανώνυμο και περιλάμβανε 25 σύντομες ερωτήσεις.

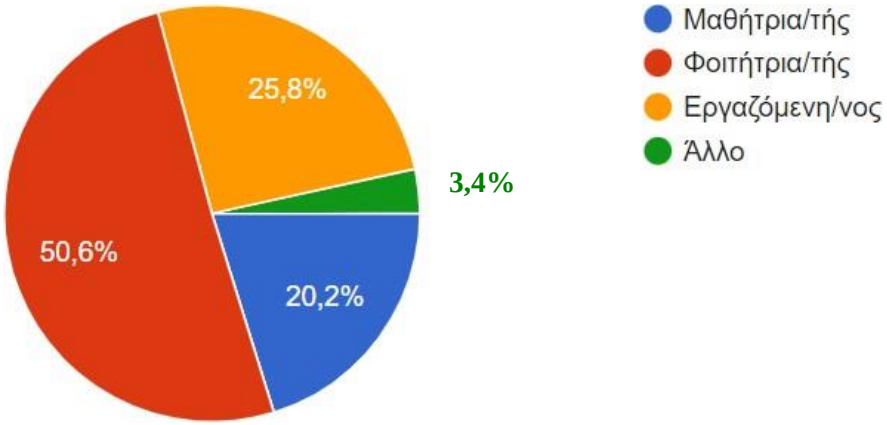
1. Η ηλικία σας;



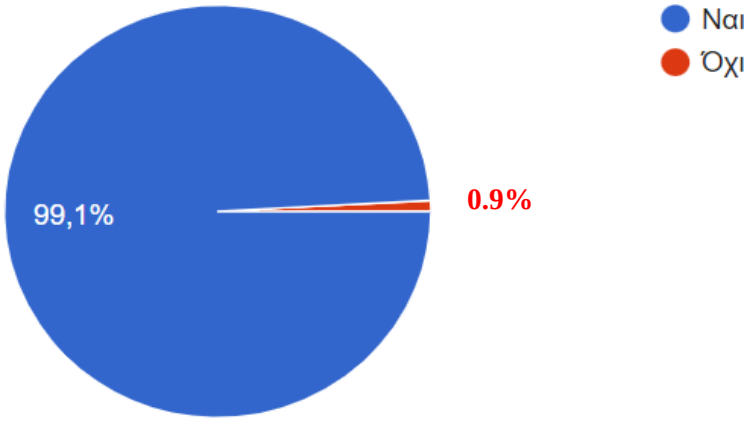
2. Φύλο :



3. Με τι ασχολείστε;

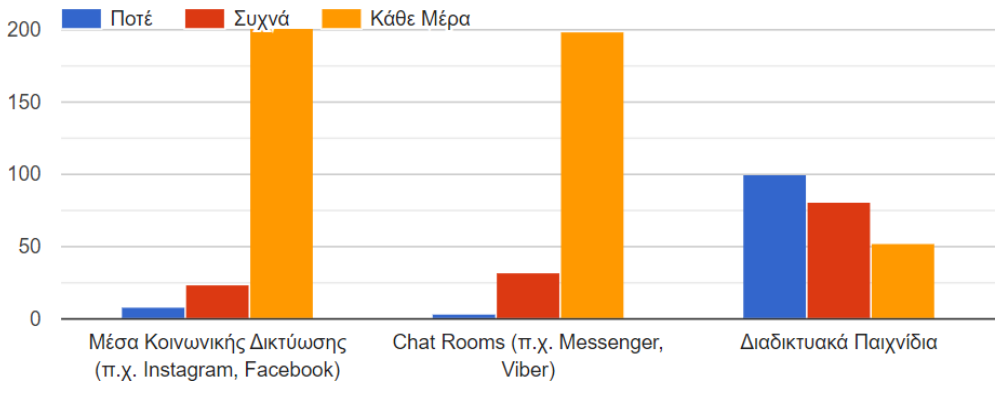


4. Χρησιμοποιείται τα Μέσα Κοινωνικής Δικτύωσης :



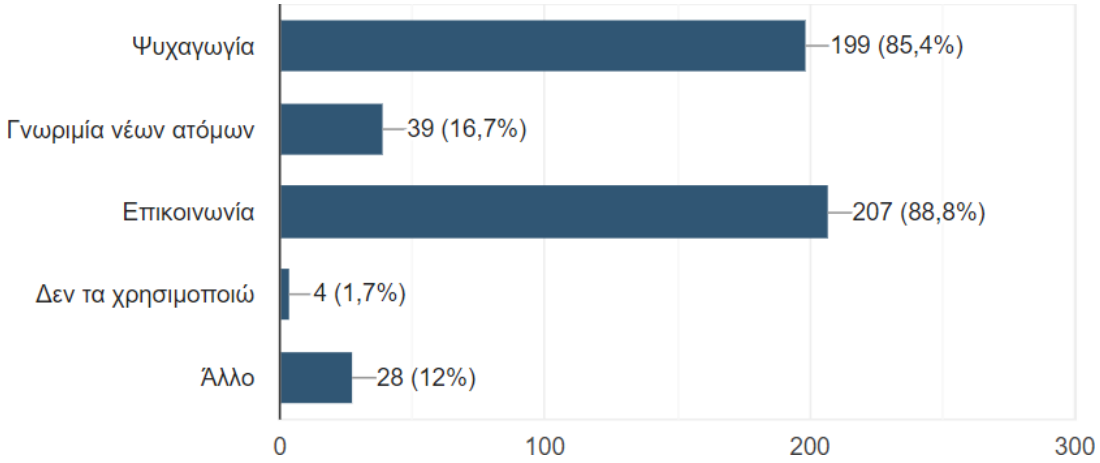
5. Πόσο συχνά χρησιμοποιείται τα εξής :

- Μέσα Κοινωνικής Δικτύωσης
- Chat Rooms
- Διαδικτυακά Παιχνίδια

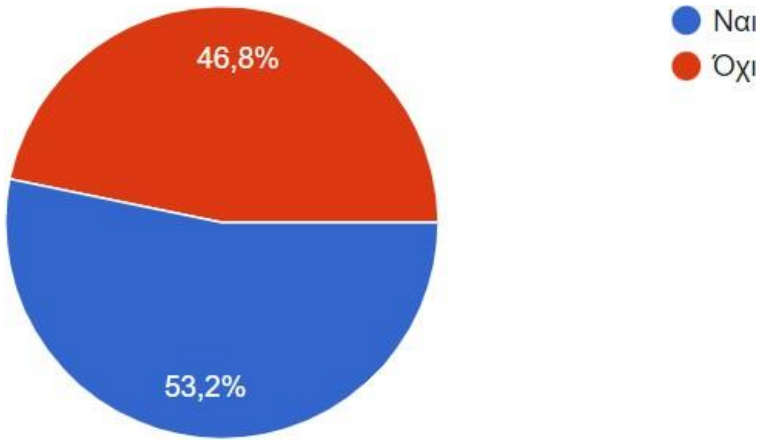


6. Γιατί χρησιμοποιείται τα Μέσα Κοινωνικής Δικτύωσης ;

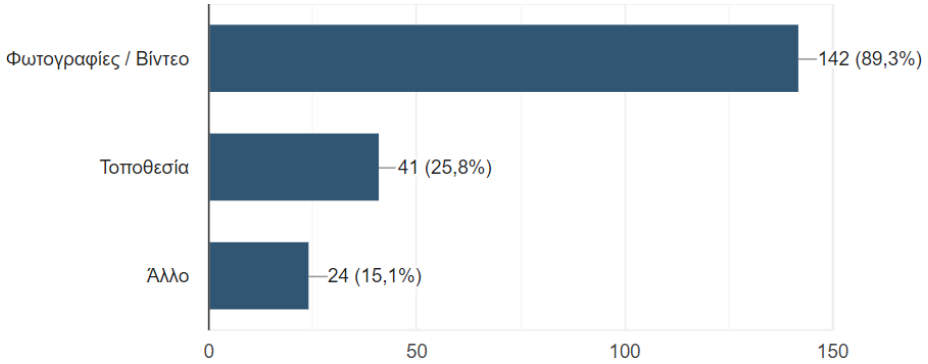
(Περισσότερες από μια απάντηση)



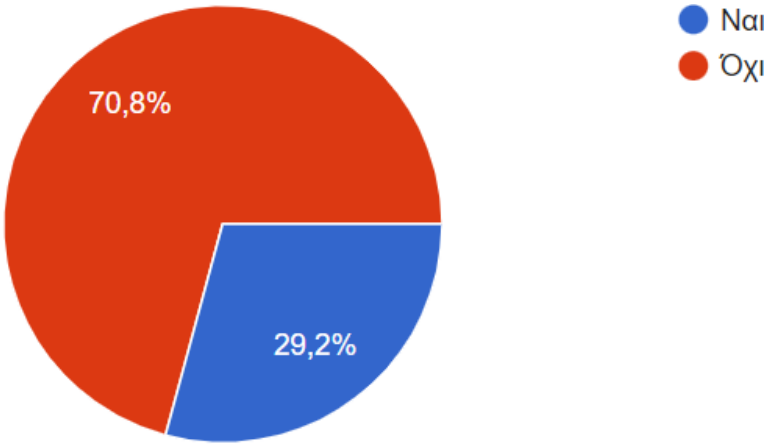
7. Ανεβάζετε προσωπικές καθημερινές σας στιγμές στα Μέσα Κοινωνικής Δικτύωσης :



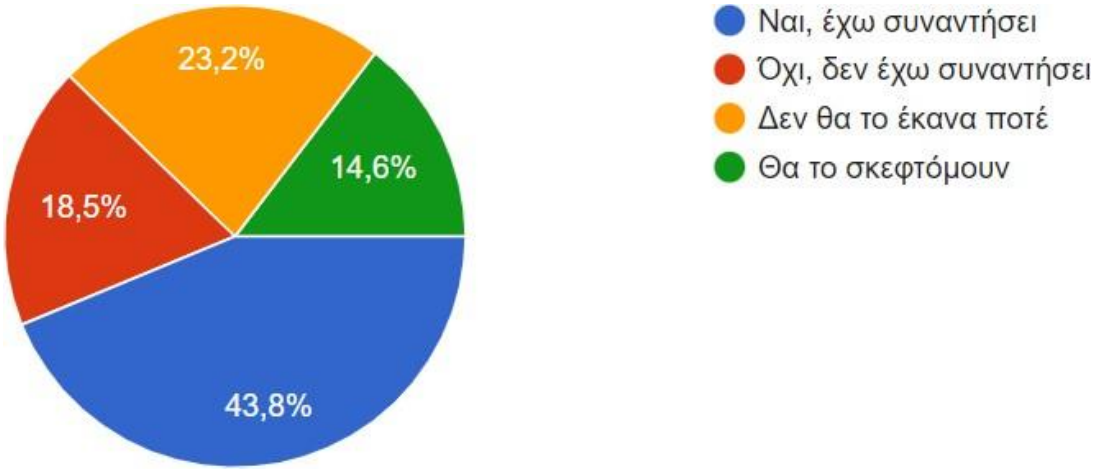
8. Αν Ναι , τι ανεβάζετε ; (Περισσότερες από μια απάντηση)



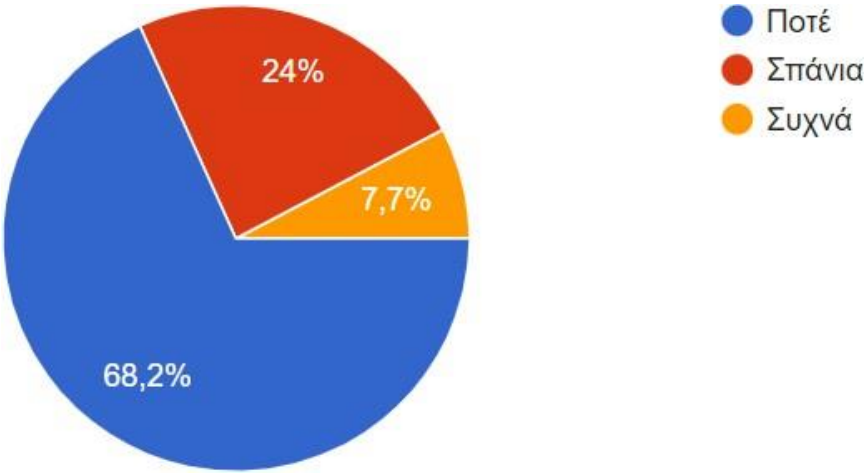
9. Έχετε στείλει σε γνωστό/άγνωστο άτομο ευαίσθητο προσωπικό περιεχόμενο ;



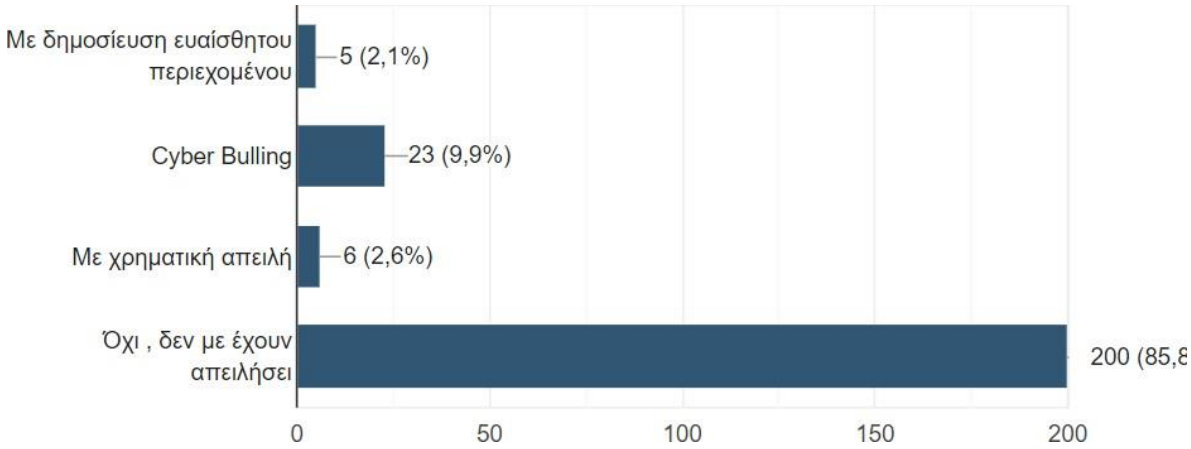
10. Έχετε συναντήσει ή θα σκεφτόσασταν να γνωρίσετε από κοντά κάποιο άτομο που γνωρίσατε σε κάποιο ψηφιακό μέσο ;



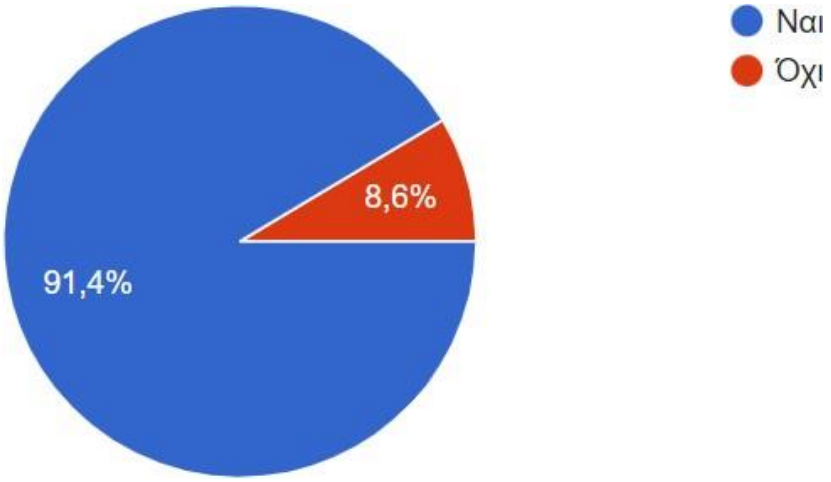
11. Έχετε δεχθεί σεξουαλική παρενόχληση στο Διαδίκτυο ;



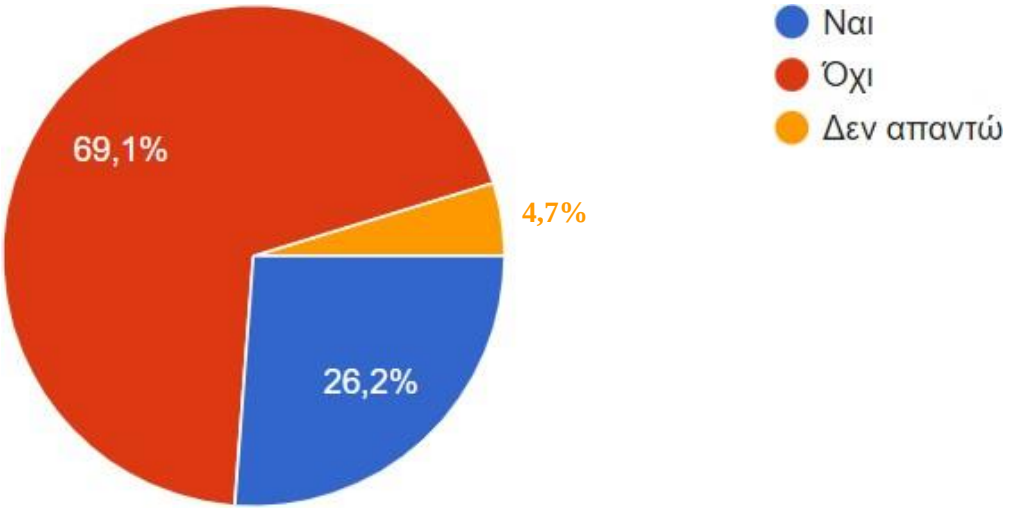
12. Σας έχουν απειλήσει Διαδικτυακά : (Περισσότερες από μια απάντηση)



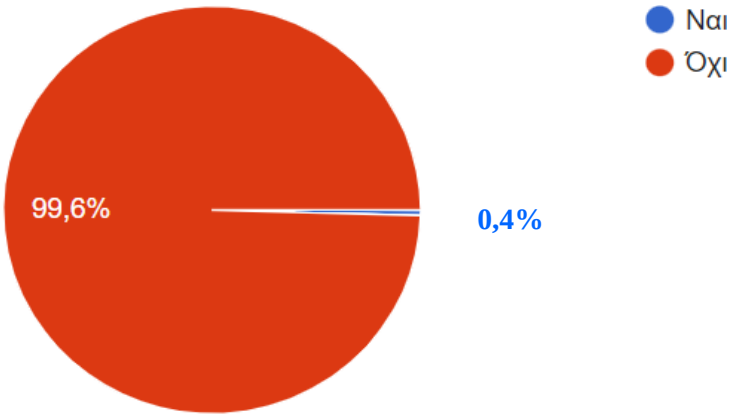
13. Έχεις συναντήσει ακατάλληλο περιεχόμενο στο διαδίκτυο ;



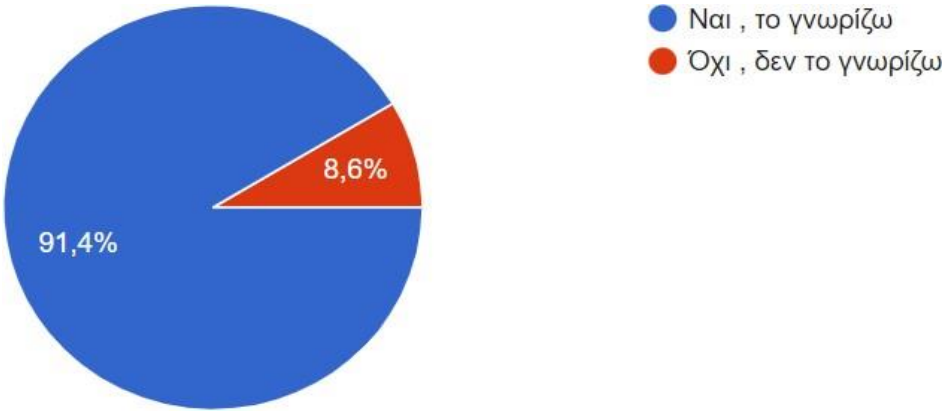
14. Έχετε βρεθεί ποτέ μέλος σε ομαδική συνομιλία όπου διαμοιράζεται ακατάλληλο περιεχόμενο τρίτων ατόμων ;



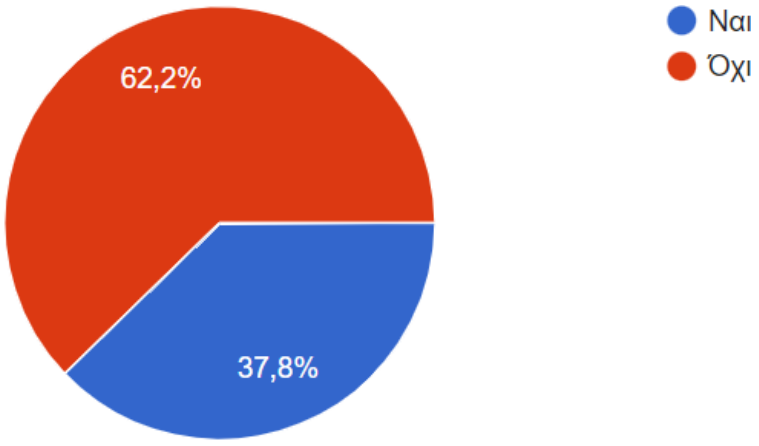
15. Έχετε ποτέ δεχθεί πρόκληση μέσα από κάποια πλατφόρμα για συμμετοχή σε κάποιο διαδικτυακό " παιχνίδι " αυτοκτονίας (π,χ. Jonathan Galindo , Blue Whale);



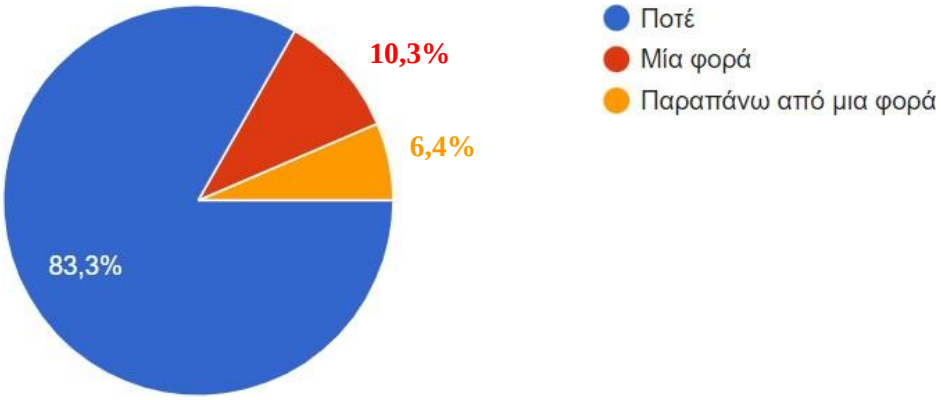
16. Γνωρίζετε ότι εντός του διαδικτύου υπάρχουν και Ιστοσελίδες υψηλής επικινδυνότητάς και ένα κομμάτι γνωστό και ως Dark Web ;



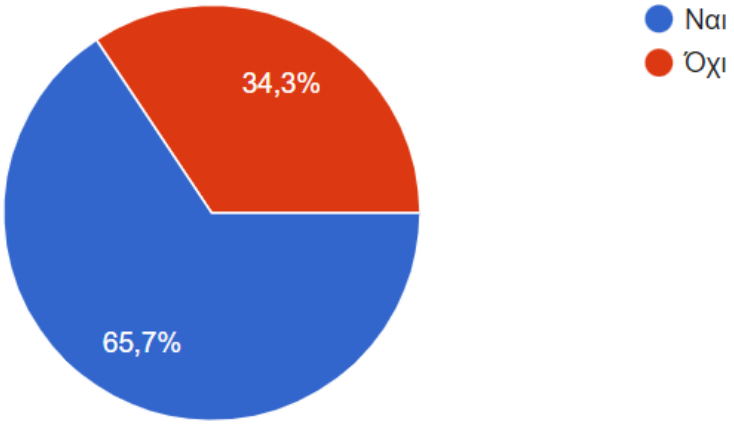
17. Έχετε αναζητήσει πληροφορίες σχετικά με την διαφορά του περιεχομένου στο Dark Web και στο ευρύ διαδεδομένο διαδίκτυο ;



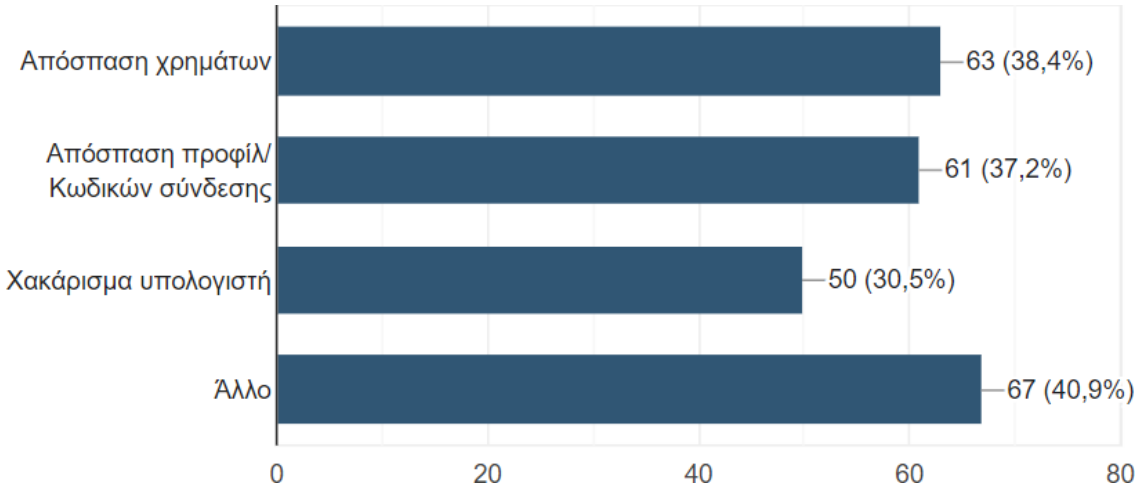
18. Έχετε συνδεθεί έστω και από περιέργεια στο Dark Web ή σε κάποια επικίνδυνη ιστοσελίδα ;



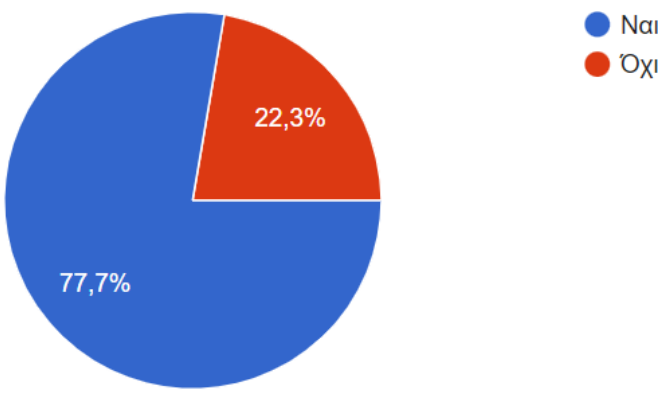
19. Σας έχει συμβεί ενώ πλοηγήστε σε κάποιο ιστότοπο ή μέσω μηνύματος να σας "ανοίξει" κάποιο ύποπτο αναδυόμενο παράθυρο ή link :



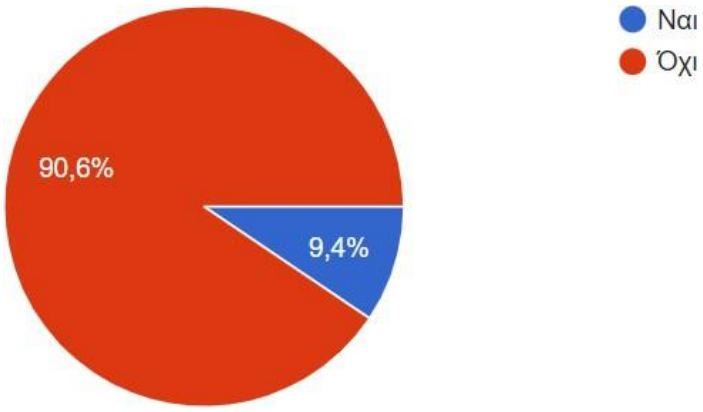
20. Αν Ναι , ποιος ήταν ο σκοπός του ; (Περισσότερες από μια απάντηση)



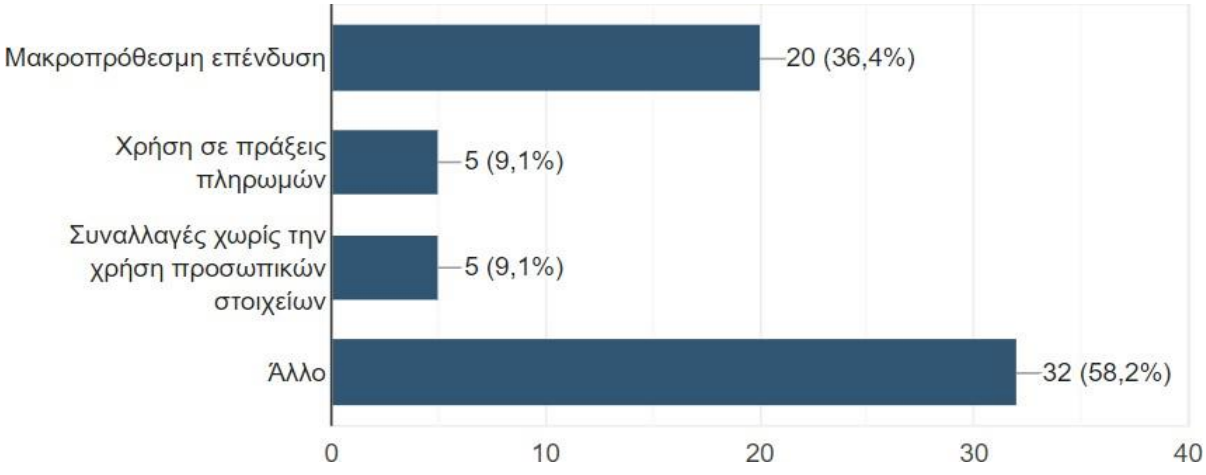
21. Γνωρίζετε την ύπαρξη των κρυπτονομισμάτων (π.χ. Bitcoins);



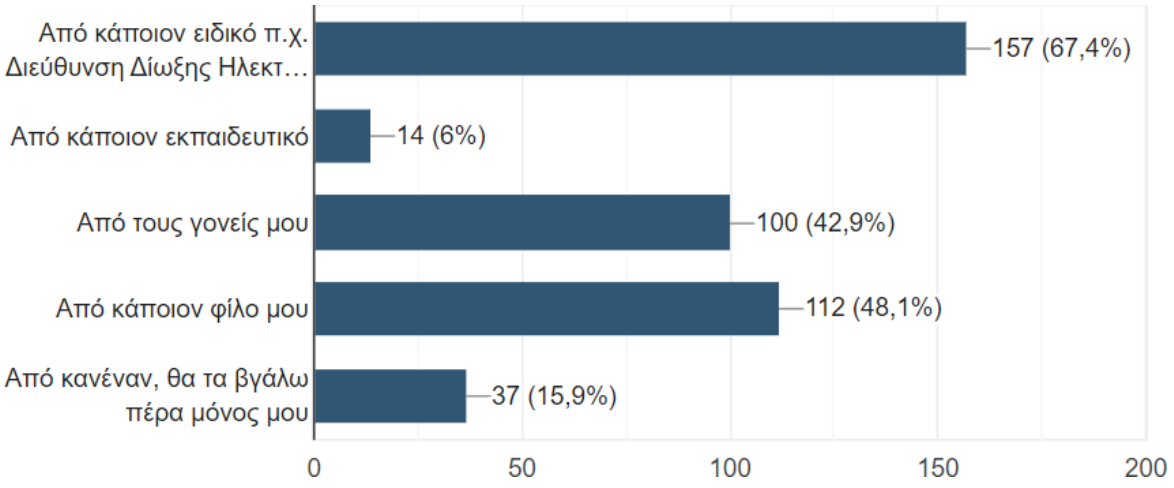
22. Έχετε χρησιμοποιήσει κρυπτονομίσματα;



23. Αν Ναι , ποιος ήταν ο σκοπός για τον οποίο αγοράσατε ή πληρώσατε με κρυπτονομισμάτων (π.χ. Bitcoins); (Περισσότερες από μια απάντηση)



24. Αν κάτι σου συμβεί διαδικτυακά από ποιον θα ζητήσεις βοήθεια; (Περισσότερες από μία απάντηση)



Η έρευνα πραγματοποιήθηκε Μάρτιο του 2022-Απρίλιο του 2023 στα πλαίσια εκπόνησης της παρούσας πτυχιακής εργασίας. Πιο συγκεκριμένα, συμμετείχαν 233 άτομα όλων των ηλικιών .Διενεργήθηκε με τη μορφή ανώνυμου online ερωτηματολογίου το οποίο συμπληρώθηκε από τις μονάδες ανάλυσης κυρίως μέσω Social Media (Facebook).

Σκοπός, λοιπόν της παρούσας μελέτης ήταν η διερεύνηση της σχέσης ανάμεσα στο χρόνο χρήσης του διαδικτύου από ανθρώπους όλων των ηλικιών, με την εμφάνιση εγκληματικής συμπεριφοράς στον χώρο του διαδικτύου και πιο συγκεκριμένα με την μορφή του διαδικτυακού εκφοβισμού, τον διαμοιρασμό ευαίσθητου προσωπικού περιεχομένου καθώς επίσης και τις γνώσεις και εμπειρίες τους σχετικά με το Dark Web και τα κρυπτονομίσματα. Ειδικότερα, η έρευνα αποσκοπούσε στο να διαπιστωθούν οι πιθανότητες που υπάρχουν οι χρήστες να έχουν δεχτεί διαδικτυακό εκφοβισμό, σεξουαλική παρενόχληση, χακάρισμα του προφίλ τους μέσω των Μέσων Κοινωνικής Δικτύωσης καθώς επίσης και σε τι ποσοστό από αυτούς έχουν συμφωνήσει να συναντήσουν κάποιον άγνωστο που γνωρίσαν στα Social Media, έχουν μοιραστεί προσωπικό ευαίσθητο περιεχόμενο ή έχουν συμμετέχει σε ομαδικές συνομιλίες στις οποίες διακινείται ακατάλληλο περιχεόμενο.

Το (52,8%) των ερωτηθέντων ήταν γυναίκες και το (47,2%) άντρες. Από αυτά το μεγαλύτερο ποσοστό των ερωτηθέντων με (55,4%) ήταν 18-24 χρονών ενώ μικρότερο ποσοστό συμμετοχής κατείχαν οι ηλικίες 30-40 με (5,6%). Η πλειοψηφία ήταν φοιτητές

και μαθητές. Όσον αφορά τα ευρήματα διαπιστώθηκε ότι σχεδόν όλοι κάνουν χρήση των Μέσων Κοινωνικής Δικτύωσης καθημερινά με την ψυχαγωγία και επικοινωνία να κατέχουν τις υψηλότερες θέσεις προτίμησης με (85,4%) και (88,8%) αντίστοιχα.

Το (46,8%) παραδέχτηκε ότι κάνει ανάρτηση προσωπικών καθημερινών στιγμών εκ των οποίων το (89,3%) αφορά βίντεο και φωτογραφίες , ωστόσο το (70,8%) από τους ερωτηθέντες δεν μοιράζεται μέσω Διαδικτύου ευαίσθητο προσωπικό περιχεόμενο.

Μεγάλο είναι το ποσοστό του (43,8%) των ατόμων που απάντησαν ότι έχουν συναντήσει κάποιον άγνωστο που γνωρίσαν στα Social Media μαζί με το (14,6%) το οποίο θα το σκεφτόταν. Η έρευνα έδειξε ότι το (68,2%) δεν έχει πέσει θύμα online σεξουαλικής παρενόχλησης ενώ ότι το (31,7%) παρενοχλείτε σπάνια έως συχνά.

Όσον αφορά τα ευρήματα διαπιστώθηκε ότι ένα σημαντικό ποσοστό του δείγματος δεν έχει δεχτεί διαδικτυακό εκφοβισμό, ενώ μικρότερα ποσοστά παρατηρήθηκαν στο Cyber Bulling ενός ατόμου (9,9%) ακολουθούν η απειλή για απόσπαση χρηματικών ποσών (2,6%) και η δημοσιοποίηση ευαίσθητου προσωπικού περιεχομένου (2,1%).

Η συντριπτική πλειοψηφία (91,4%) έχει συναντήσει ακατάλληλο περιεχόμενο στο Διαδίκτυο με ένα ποσοστό της τάξης του (26,2%) να έχει συμμετάσχει σε ομαδικές συνομιλίες στις οποίες διαμοιράστηκε ακατάλληλο περιεχόμενο τρίτων ενώ σχεδόν κανένας (99,6%) δεν έχει συμμετάσχει σε διαδικτυακά παιχνίδια αυτοκτονίας.

Εννέα στους δέκα ερωτηθέντες (91,4%) γνώριζαν την ύπαρξη ιστοσελίδων υψηλής επικινδυνότητας αλλά το (62,2%) δεν ήξερε τη διαφορά του World Wide Web και του Dark Web.

Από επιμέρους στοιχεία προέκυψε ότι το (83,3%) δεν έχει προσπαθήσει να συνδεθεί στον Σκοτεινό Ιστό, το (10,3%) συνδέθηκε μόνο μια φορά ενώ με ποσοστό (6,4%) περισσότερες από μια φορές.

Στην ερώτηση αν όσο πλοηγούνταν στο Διαδίκτυο ή μέσω κάποιου μηνύματος ήρθαν αντιμέτωποι με ύποπτα αναδυόμενα παράθυρα ή link το (65,7%) απάντησε θετικά με (38,4%) να υποστηρίζουν ότι ο σκοπός τους ήταν για απόσπαση χρημάτων, το (37.2%) για απόσπαση κωδικών σε προφίλ των Social Media , το (30,5%) για χακάρισμα του

υπολογιστή και (40,9%) για κάτι άλλο.

Το (77,7%) του δείγματος γνώριζε την ύπαρξη των κρυπτονομισμάτων, όπως είναι το Bitcoin, με την πλειονότητα (90,6%) να μην τα έχουν χρησιμοποιήσει. Από το (9,4%) που είχε χρησιμοποιήσει κρυπτονομίσματα το (36,4%) το διέθεσε για μακροπρόθεσμες επενδύσεις, το (9,1%) για ανώνυμες πληρωμές ενώ το (58,2%) για κάτι άλλο.

Τέλος στην ερώτηση σε ποιον θα απευθυνόντουσαν για βοήθεια στην περίπτωση που αντιμετώπιζαν κάποιο διαδικτυακό πρόβλημα η δημοφιλέστερη απάντηση με (67,4%) ήταν από την Δίωξη Ηλεκτρονικού Εγκλήματος, έπειτα ακολουθούσε με (48,1%) από κάποιον φίλο, (42,9%) από γονείς ενώ το (15,9%) υποστήριξε ότι θα έβρισκαν λύση μόνοι τους.

ΒΙΒΛΙΟΓΡΑΦΊΑ

Δημόπουλος Νικ, Χαράλαμπος (2006). Εγκλήματα της Γενετήσιας Εκμετάλλευσης Ανηλίκων. Εκδόσεις Νομική Βιβλιοθήκη.

Ευαγγελία Κούρτη (2003). Η επικοινωνία στο Διαδίκτυο. Εκδόσεις Ελληνικά Γράμματα.

Καλογρίδου-Καλυβά Μαργαρίτα (2011). Οι πολλές όψεις του διαδικτύου. Χρήση, Κατάχρηση, Εθισμός, Αντίλογος, Διάλογος.Εκδόσεις Δρόμων.

Νίκος Λέανδρος (2005). Το διαδίκτυο. Ανάπτυξη και Αλλαγή. Εκδόσεις Καστανιώτης.

Σφακιανάκης, Εμμανουήλ, Σιώμος Κωνσταντίνος, Φλώρος Γεώργιος (2012). Εθισμός στο διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου. Εκδόσεις Λιβάνης.

Antony Mayfield (2008). What is Social Media. eBook by iCrossing.

Fedean Ammous (2022). Ο κανόνας του Bitcoin. Εκδόσεις Κέδρος.

Richard Amores-Peirluigi Paganini & Gianni Motta., (2012). The Deep Dark Web: the hidden world.

Sameer Hinduja-Justin W. Patchin. (2012). *School Climate 2.0: Preventing Cyberbullying and Sexting One Classroom at a Time*. Publication Corwin Press.

Stephan Pincock (2008). Κρυπτογραφία. Κώδικες και Κρυπτογράμματα Από τους Αρχαίους Φαραώ μέχρι την Κβαντική Κρυπτογραφία. Εκδόσεις Τραυλός.

William Stallings (2012). Κρυπτογραφία και Ασφάλεια Δικτύων. Αρχές και Εφαρμογές. Εκδόσεις Εκδοτικός Όμιλος Ίων.

ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

Άρθρο 23 της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των παιδιών κατά της γενετήσιας εκμετάλλευσης και κακοποίησης με το Ν.3727/08(ΦΕΚ Α' 257/18.12.2008). Ανάκτηση από https://www.hellenicparliament.gr/UserFiles/67715b2c-ec81-4f0c-ad6a-476a34d732bd/7486748.pdf

Κώδικας Δεοντολογικής Συμπεριφοράς (Netiquette). Ανάκτηση από https://el.wikipedia.org/wiki/Netiquette

Κακοποίηση και Εκμετάλλευση Μέσω Διαδικτύου (2016) – Χαμόγελο του παιδιού. Ανάκτηση από https://www.hamogelo.gr/gr/el/ta-nea-mas/kakopoiisi-kai-ekmetalleisi-meso-diadiktiou/

Μέθοδοι Επίθεσης Διαδικτύου. Ανάκτηση από https://sites.google.com/site/eisagogestadiktyaypologiston1/diadiktyo-internet/methodoi-epitheses-kai-tropoi-apophyges-epitheseon

Παιδική Πορνογραφία,Sextortion, Online Games, Phishing – Παιδαγωγικό Ινστιτούτο Κύπρου. Ανάκτηση από https://internetsafety.pi.ac.cy/parents/parents-child-pornography/

Τι είναι η παιδική πορνογραφία (2019). Ανάκτηση από https://www.provataslaw.gr/νέα/τι-είναι-η-παιδική-πορνογραφία

Blue Whale (2017). Ανάκτηση από https://www.news247.gr/kosmos/paichnidia-aytoktonias-i-omologia-sok-toy-dimioyrgoy-toy-blue-whale.6507371.html

Bitcoin. Ανάκτηση από https://bitcoin.org/el/faq#what-is-bitcoin

Child Sexual Abuse. Ανάκτηση από https://www.thorn.org/blog/redefining-child-pornography/

Craven Samantha, Brown Sarah- Gilchrist Elizabeth (2006). Sexual grooming of children: review of literature and theoretical considerations, Journal of Sexual Aggression. Ανάκτηση από https://www.nationalcac.org/wp-content/uploads/2019/05/Sexual-grooming-of-children-Review-of-literature-and-theoretical-considerations-Craven-2006.pdf

Emily A. Vogels., (2022). Teens and Cyberbullying 2022. Pew Research Center. Ανάκτηση από https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022

Fire Fairy (2017). Ανάκτηση από https://www.dailymail.co.uk/news/article-4290590/Fire-fairy-game-tells-children-turn-gas-stoves.html

Facebook Report third quarter 2022. Ανάκτηση από https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Third-Quarter-2022-Results/default.aspx

Surface Web, Deep Web, Dark Web -- What's the Difference? (2016). Ανάκτηση από https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web---whats-the-difference