**Ανοικτό Πανεπιστήμιο Κύπρου**

**Σχολή Οικονομικών Επιστημών και Διοίκησης**

**Πτυχιακό Πρόγραμμα Σπουδών *Αστυνομικές Σπουδές***

**Πτυχιακή Διατριβή**

# ΤΑ ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

**Μαρία Νεοκλέους**

**Επιβλέπων Καθηγητής**
**Δρ. Αναστάσιος Παπαθανασίου**

**Λευκωσία, Ιούνιος, 2023**

**Ανοικτό Πανεπιστήμιο Κύπρου**

**Σχολή Οικονομικών Επιστημών και Διοίκησης**

**Πτυχιακό Πρόγραμμα Σπουδών *Αστυνομικές Σπουδές***

**Πτυχιακή Διατριβή**

# ΤΑ ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

**Μαρία Νεοκλέους**

**Επιβλέπων Καθηγητής**
**Δρ. Αναστάσιος Παπαθανασίου**

**Λευκωσία, Ιούνιος, 2023**

**Ευχαριστίες**

Θέλω να εκφράσω τις θερμές μου ευχαριστίες στον καθηγητή μου, Επίκουρο Καθηγητή Αναστάσιο Παπαθανασίου για την επίβλεψη της πτυχιακής μου εργασίας.

**Περίληψη**

Στην εργασία αυτή εξετάζονται διάφορα εγκλήματα που διαπράττονται στον κυβερνοχώρο. Η εργασία είναι χωρισμένη σε έξι κεφάλαια τα οποία στο σύνολο τους παρουσιάζουν μια γενική εικόνα για τα εγκλήματα του κυβερνοχώρου, ενώ αναλύονται τα κυριότερα από αυτά.

Στο πρώτο κεφάλαιο περιγράφεται η έννοια του κυβερνοεγκλήματος.

Στο δεύτερο κεφάλαιο περιγράφεται η έννοια του οικονομικού εγκλήματος που διαπράττεται στο διαδίκτυο και γίνεται αναφορά στις διάφορες μορφές του καθώς και στους τρόπους αντιμετώπισης του φαινομένου.

Στο τρίτο κεφάλαιο περιγράφεται η έννοια της διαδικτυακής παιδικής πορνογραφίας και αναλύεται των προφίλ των χρηστών της και τρόποι προστασίας από το έγκλημα αυτό.

Στο τέταρτο κεφάλαιο περιγράφεται η έννοια του διαδικτυακού εκφοβισμού, περιγράφονται οι διάφορες μορφές του, γίνεται σύγκριση του με τον παραδοσιακό εκφοβισμό και αναφέρονται τρόποι αντιμετώπισης του φαινομένου αυτού.

Στο πέμπτο κεφάλαιο περιγράφεται η έννοια της διαδικτυακής τρομοκρατίας και αναλύονται οι τύποι των τρομοκρατικών επιθέσεων στον κυβερνοχώρο.

Στο έκτο κεφάλαιο περιγράφεται η έννοια του «hacking», αναλύονται οι κυριότερες κατηγορίες των hacker και οι πιο γνωστοί τρόποι του «hacking».

**ΠΕΡΙΕΧΟΜΕΝΑ**

**Εισαγωγή**

Η εξέλιξη της τεχνολογίας έχει κάνει τεράστια άλματα κυρίως στον τομέα της πληροφορικής και κατ΄ επέκταση στην ανάπτυξη του διαδικτύου. Το Διαδίκτυο έχει γίνει αναπόσπαστο κομμάτι της ζωής του σύγχρονου ανθρώπου, καθότι του παρέχει διευκολύνσεις σε διάφορους τομείς της καθημερινότητας του. Ωστόσο αυτό έχει οδηγήσει στην ανάπτυξη νέων μορφών εγκληματικότητας όπως είναι τα εγκλήματα στον κυβερνοχώρο.

Τα εγκλήματα του κυβερνοχώρου έχουν πάρει τεράστιες διαστάσεις και συνεχώς αυξάνονται και μεταβάλλονται με προσαρμογή στα νέα δεδομένα. Τα χαρακτηριστικά του διαδικτύου ευνοούν τους δράστες να δρουν ανεξέλεγκτα και χωρίς να εντοπίζονται.

Για αυτό οι χρήστες του διαδικτύου θα πρέπει να γνωρίζουν τους κινδύνους που διατρέχουν και να προστατεύονται, αλλά και να τους χειρίζονται ορθά όταν έρχονται αντιμέτωποι με αυτούς.

Στην εργασία αυτή έχουν αναλυθεί τα κυριότερα εγκλήματα του κυβερνοχώρου.

## Κεφάλαιο 1:ΕΙΣΑΓΩΓΗ

### 1.1.Έννοια του κυβερνοεγκλήματος

Κυβερνοέγκλημα είναι το έγκλημα που τελείται με τη χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων(Καργόπουλος Α., 2018) Ο χώρος τέλεσης του εγκλήματος αυτού είναι ο κυβερνοχώρος, που ορίζεται ως «το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση». (Παναγιωτίδης, Π. Κ., 2011)

Το έγκλημα στον κυβερνοχώρο διαπράττεται σε ένα «εικονικό χώρο, κάτω από τον οποίο πληροφορίες που αφορούν ανθρώπους, αντικείμενα, γεγονότα ή γεγονότα που διαμορφώνονται σε μαθηματικά σύμβολα και μεταφέρονται μέσω τοπικών και παγκόσμιων δικτύων» και έχει ως στόχο τα συστήματα υπολογιστών και τα δεδομένα που επεξεργάζονται οι συσκευές. (Μπενέτου, Α., 2021)

Το έγκλημα στον κυβερνοχώρο χωρίζεται σε δύο κατηγορίες. Στην πρώτη κατηγορία ο υπολογιστής και το δίκτυο είναι ο στόχος της αξιόποινης πράξης ενώ στη δεύτερη κατηγορία είναι το μέσο διάπραξης της. Η πρώτη κατηγορία περιλαμβάνει εγκλήματα που αφορούν την εμπιστευτικότητα, την ακεραιότητα, την διαθεσιμότητα των ηλεκτρονικών συστημάτων και των δεδομένων, όπως είναι η παράνομη πρόσβαση και παρακολούθηση, η παρεμβολή στα δεδομένα και στο σύστημα, ενώ η δεύτερη κατηγορία περιλαμβάνει εγκλήματα όπως είναι η πλαστογραφία, η παιδική πορνογραφία και η απάτη. (Sykas, S., 2019)

Η ύπαρξη ηλεκτρονικού υπολογιστή ή μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων όπως είναι το κινητό τηλέφωνο, είναι απαραίτητη για την ύπαρξη του εγκλήματος αυτού. Ο ηλεκτρονικός υπολογιστής μπορεί να είναι ο στόχος της επίθεσης, το μέσο διάπραξης της επίθεσης, όταν χρησιμοποιείται ως εργαλείο για τη διάπραξη της αξιόποινης πράξης και το βοηθητικό μέσο διάπραξης της αξιόποινης πράξης, όταν αυτός χρησιμοποιείται για την φύλαξη στοιχείων και πληροφοριών των δραστών που προβαίνουν στην αξιόποινη πράξη.( Κελεγκουριάδη, Α, & Μαλλιαρού, Α., 2016)

Το κυριότερο χαρακτηριστικό που διακρίνει ένα έγκλημα του κυβερνοχώρου από τα συνηθισμένα εγκλήματα είναι η απουσία της απευθείας επαφής του θύτη και του θύματος, λόγω της φυσικής

απόστασης που υπάρχει ανάμεσα τους. Η απουσία της σωματικής βίας που υπάρχει στα εγκλήματα αυτά δεν το καθιστούν λιγότερο σοβαρό από τα υπόλοιπα εγκλήματα, καθότι σε αυτή την περίπτωση ο θύτης δρα χωρίς να γίνει αντιληπτός και χωρίς να μπορεί να εντοπιστεί με αποτέλεσμα να παραμένει ατιμώρητος. Είναι ένα διεθνικό έγκλημα που δεν περιορίζεται από τα εθνικά σύνορα και μπορεί να συμβεί σε οποιοδήποτε μέρος του κόσμου, καθότι διαπράττεται μέσω του διαδικτύου. Η ευκολία χρήσης του διαδικτύου παρέχει τη δυνατότητα σε οποιοδήποτε χρήστη να ενεργεί με τον τρόπο αυτό, καθότι δεν απαιτούνται εξειδικευμένες γνώσεις και υψηλό πνευματικό επίπεδο, παρά μόνο ένας υπολογιστής και σύνδεση στο διαδίκτυο.(Καρατση, Α. & Νικολάου, Α, 2022)

Άλλα χαρακτηριστικά που διακρίνουν το έγκλημα στον κυβερνοχώρο είναι η ευκολία – δεν απαιτείται μετακίνηση του δράστη, ο οποίος μπορεί να διαπράξει το έγκλημα του με το πάτημα ενός κουμπιού ενώ βρίσκεται οπουδήποτε, η ταχύτητα – το έγκλημα μπορεί να συμβεί σε κλάσματα δευτερολέπτου και μπορεί το θύμα να μην το αντιληφθεί, τα διεθνικά στοιχεία – οι θύτες και τα θύματα μπορεί να βρίσκονται σε διαφορετικά γεωγραφικά μέρη, η ανωνυμία, - το διαδίκτυο παρέχει τεχνολογικές υποδομές που προσφέρουν την ανωνυμία, η δυσκολία εύρεσης αποδεικτικών στοιχείων – οι αποδείξεις αποτελούν ψηφιακά δεδομένα σε ψηφιακά αρχεία και ίχνη, τα οποία δεν εντοπίζονται εύκολα, η διερεύνηση και ανάκριση της Αστυνομίας είναι πολύ δύσκολή, καθότι απαιτούνται εξειδικευμένες γνώσεις και εκπαίδευση και η έλλειψη επαρκούς καταγραφής – τα κυβερνοεγκλήματα είναι περισσότερα από αυτά που φαίνονται στις καταγραφές καθότι είναι δύσκολο να καταγραφούν όλα τα περιστατικά (Παλιάτσου, Θ., 2021).

## Κεφάλαιο 2:ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΝΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

### 2.1.Το οικονομικό έγκλημα στον Κυβερνοχώρο

Το οικονομικό έγκλημα διαπράττεται σε οικονομικό περιβάλλον. Δεν αποτελεί απλώς μια αξιόποινη πράξη με οικονομικό περιεχόμενο, αλλά αποτελεί μια εγκληματική πράξη που εκμεταλλεύεται το οικονομικό σύστημα με σκοπό την αύξηση του κέρδους του δράστη, προκαλώντας ζημιά στο δημόσιο, τις τράπεζες, επιχειρήσεις και το καταναλωτικό κοινό. (Ζησιάδη Ι., Β. (2002):37-38)

Τα κύρια χαρακτηριστικά στοιχεία του οικονομικού εγκλήματος, εκτός από τον οικονομικό του χαρακτήρα είναι το μέγεθος της ζημιάς που προκαλείται στην οικονομία είτε άμεσα είτε με έμμεσο τρόπο, μέσω των μονάδων που απαρτίζουν το οικονομικό σύστημα. (Ζησιάδη Ι., Β. (2002):40)

Η ηλεκτρονική οικονομική εγκληματικότητα αποτελεί μία από τις σύγχρονες μορφές οικονομικής εγκληματικότητας. Με την εξέλιξη της πληροφορικής οι δράστες έχουν τη δυνατότητα να δρουν εγκληματικά μέσω των ηλεκτρονικών υπολογιστών. Οι πράξεις τους επιχειρούνται με την παρεμβολή ενός αυτόματου συστήματος επεξεργασίας ή μετάδοσης δεδομένων. Η δράση τους αυτή καθίσταται σχετικά εύκολη επειδή υπάρχουν πολύ λίγα μέτρα ασφάλειας των υπολογιστών καθότι οι κατασκευαστικές εταιρείες τους πολλές φορές δε θέλουν να επενδύσουν σε αυτή. (Ζησιάδη Ι., Β. (2002):97-99)

### 2.2.Μορφές οικονομικού εγκλήματος στον κυβερνοχώρο

#### 2.2.1 Ξέπλυμα χρήματος

Το ξέπλυμα χρήματος αποτελεί μια διαδικασία τριών σταδίων, με την οποία οι εγκληματίες προσπαθούν να εξαφανίσουν τα χρήματα τους που είναι προϊόν παράνομων δραστηριοτήτων. Αρχικά προσπαθούν να μετατρέψουν τα χρήματα που απόκτησαν παράνομα σε τέτοια μορφή ώστε να μην είναι ύποπτη στις διωκτικές αρχές. Ακολούθως προσπαθούν να διαχωρίσουν τα χρήματα από την παράνομη πηγή τους, μέσω πολλών οικονομικών συναλλαγών και τελικά ολοκληρώνουν την μετατροπή του παράνομου χρήματος ώστε να φαίνεται ότι αποτελεί εισόδημα νόμιμης επαγγελματικής δραστηριότητας. Το διαδίκτυο δίνει την δυνατότητα στους εγκληματίες

να το κάνουν αυτό, καθότι σε αυτό υπάρχει ανωνυμία η οποία καθιστά δύσκολη την πιστοποίηση της ταυτότητας των πελατών μιας εταιρείας. Επίσης μέσω του διαδικτύου μπορούν να καταθέτουν μικρά ποσά σε διάφορους τραπεζικούς λογαριασμούς. (Βλαχοπούλου, Κ.(2007):69)

### 2.2.2 Carbanak

Οι επιθέσεις Carbanak έχουν ξεκινήσει από το 2013 και αποτελούν κλοπές τραπεζών με κακόβουλο λογισμικό, συνολικού ύψους άνω του 1 δισεκατομμύριου δολαρίων. Οι εγκληματίες, οι οποίοι αποτελούν μέλη οργανωτικών εγκληματικών συμμοριών, αποκτούν πρόσβαση σε συστήματα μέσω του ηλεκτρονικού ψαρέματος και ακολούθως τα μεταφέρουν με δόλιο τρόπο στους δικούς τους λογαριασμούς ή σε προγραμματισμένα ATM για τη διανομή μετρητών στους συνεργούς τους που περιμένουν εκεί. Οι δράστες αρχικά στέλνουν ηλεκτρονικό μήνυμα με συνημμένο αρχείο στους υπαλλήλους μιας τράπεζας στόχου. Ακολούθως με το άνοιγμα του αρχείου αυτού οι δράστες κατορθώνουν να έχουν πρόσβαση στον ηλεκτρονικό υπολογιστή του διαχειριστή, παρακολουθούν την οθόνη του διαχειριστή για να μιμηθούν τη συμπεριφορά στο σύστημα μεταφοράς μετρητών, αυξάνουν τα ποσά μεταφοράς, στέλνουν εντολή στις ATM να εκδοθούν μετρητά σε συγκεκριμένο χρόνο ή χρησιμοποιούν το διαδίκτυο ή τις ηλεκτρονικές πληρωμές για μεταφορά του ποσού[1].

### 2.2.3 Επιχειρηματικός συμβιβασμός ηλεκτρονικού ταχυδρομείου

Ο επιχειρηματικός συμβιβασμός ηλεκτρονικού ταχυδρομείου αποτελεί ένα από τα πιο επιζήμια οικονομικά διαδικτυακά εγκλήματα. Στην περίπτωση αυτή οι εγκληματίες στέλνουν μήνυμα στο ηλεκτρονικό ταχυδρομείο μιας επιχείρησης, το οποίο φαίνεται ότι προέρχεται από γνωστό αποστολέα ο οποίος κάνει ένα νόμιμο αίτημα, το οποίο έχει στόχο την παραπλάνηση του παραλήπτη και κατ΄ επέκταση την απόσπαση χρημάτων από την εταιρεία.[2]

[1](https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity,)24/10/21

[2] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

### 2.2.4 Απάτη στο Διαδίκτυο

Η απάτη στο διαδίκτυο αποτελεί μία από τις συχνότερες μορφές ηλεκτρονικού εγκλήματος.

#### 2.2.4.1 Απάτη με e-mail

Οι δράστες χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο στέλνοντας μηνύματα σε ανυποψίαστους χρήστες και χρησιμοποιώντας διάφορες δικαιολογίες προσπαθούν να αποσπάσουν χρήματα από αυτούς. Χαρακτηριστικό παράδειγμα αποτελούν οι Νιγηριανές επιστολές. Εδώ οι δράστες υποδύονταν πρόσωπο Αφρικάνικης καταγωγής που ζητούσε βοήθεια για μεταφορά χρημάτων από τη χώρα του στο εξωτερικό με αντάλλαγμα οικονομικό κέρδος. Έστελναν μήνυμα στο ηλεκτρονικό ταχυδρομείο και ζητούσαν από τα ανυποψίαστα θύματα να ανοίξουν τραπεζικό λογαριασμό στο όνομα τους και στο όνομα του δράστη. Ακολούθως τους ζητούσαν προσωπικά στοιχεία και κατάθεση χρηματικού ποσού στους λογαριασμούς αυτούς. Τελικά οι δράστες μετέφεραν τα χρήματα των θυμάτων σε δικό τους λογαριασμό χρησιμοποιώντας διάφορες προφάσεις και έκλειναν το λογαριασμό των θυμάτων. (Βλαχοπούλου, Κ.(2007):63-65)

#### 2.2.4.2 Απάτη με πιστωτικές κάρτες

Οι ηλεκτρονικές συναλλαγές στο Διαδίκτυο έχουν δώσει τη δυνατότητα στους εγκληματίες να δρουν εγκληματικά. Οι συναλλαγές αυτές εκτελούνται με τη χρήση των πιστωτικών καρτών, χωρίς τη φυσική παρουσία αγοραστή και πωλητή και συνεπώς η απάτη μπορεί να γίνει πιο εύκολα. Επίσης, η πρόοδο της τεχνολογίας επιτρέπει στους εγκληματίες να αποσπούν πιο εύκολα τον αριθμό μιας πιστωτικής κάρτας ή να δημιουργούν αυτόματα αριθμούς πιστωτικών καρτών με τη βοήθεια ειδικών λογισμικών. Το διαδίκτυο επίσης παρέχει την ευκαιρία στους δράστες να αγοράσουν αριθμούς πιστωτικών καρτών που έχουν υποκλαπεί. (Βλαχοπούλου, Κ.(2007):67)

### 2.2.5 Φοροδιαφυγή

Η φοροδιαφυγή συμβαίνει όταν ο φορολογούμενος αποφεύγει να εκπληρώσει τις φορολογικές του οφειλές χρησιμοποιώντας παράνομες πράξεις ή παραλείψεις. (Παπακυριάκου, Θ. (2005):12). Εταιρείες που ασκούν εμπόριο μέσω διάφορων ιστοσελίδων κοινωνικής δικτύωσης και

αποκομίζουν κέρδη εκατομμυρίων ευρώ αποφεύγουν να δηλώσουν τις πωλήσεις τους και δεν εκδίδουν τα αναγκαία παραστατικά, με αποτέλεσμα να μην καταβάλλουν τον οφειλόμενο φόρο.[3]

### 2.3.Τρόποι πρόληψης και προστασίας

Οι κίνδυνοι στον κυβερνοχώρο είναι δύσκολο να ελεγχθούν. Ωστόσο μπορεί να ληφθούν κάποια μέτρα που μπορούν να προστατεύσουν το χρήστη όπως είναι τα ακόλουθα.

### 2.3.1. Διαδικασίες αυθεντικοποίησης

Με τη διαδικασία αυθεντικοποίησης επιβεβαιώνεται ότι η ταυτότητα του χρήστη είναι αυθεντική. Αυτό μπορεί να γίνει με κάτι που έχει ο χρήστης έχει στην κατοχή του, όπως μια έξυπνη κάρτα ή κάτι που έχει ως φυσικό χαρακτηριστικό ή κάτι που να γνωρίζει μόνο αυτός. Η χρήση των προσωπικών χαρακτηριστικών του χρήστη παρέχει περισσότερη ασφάλεια, κυρίως όταν γίνεται σε συνδυασμό με περισσότερες τεχνικές. (Βλαχοπούλου, Κ.(2007):81)

### 2.3.2. Κωδικοί πρόσβασης

Η χρήση κωδικών πρόσβασης αποτελεί επίσης σημαντικό τρόπο προστασίας του διαδικτυακού χρήστη από τους εγκληματίες. Ωστόσο αυτό μπορεί να γίνει με τη σωστή επιλογή τους. Θα πρέπει να γίνεται επιλογή ενός συνδυασμού χαρακτήρων που δεν είναι εύκολο να απομνημονεύονται. Ο κωδικός αυτός δεν πρέπει να γνωστοποιείται σε άλλα πρόσωπα, αλλά να παραμένει μυστικός. (Βλαχοπούλου, Κ.(2007):83)

### 2.3.3. Βιομετρικές τεχνικές

Η χρήση των βιομετρικών τεχνικών στον τομέα των συστημάτων Πληροφορικής βοηθά στην επιβεβαίωση της ταυτότητας του χρήστη μέσω της σύγκρισης ενός χαρακτηριστικού του με χαρακτηριστικό μιας βάσης δεδομένων, καθότι το χαρακτηριστικό αυτό αποτελεί μοναδικό φυσιολογικό η συμπεριφοριστικό χαρακτηριστικό του χρήστη. Ορισμένα παραδείγματα τέτοιων

[3] https://www.kathimerini.gr/economy/local/1052805/forodiafygi-meso-istoselidon-koinonikis-diktyosis-entopise-i-aade/

βιομετρικών τεχνικών είναι η σάρωση του δακτυλικού αποτυπώματος, η αναγνώριση του προσώπου, η σάρωση της φωνής, της ίριδας, του χεριού και της υπογραφής. (Βλαχοπούλου, Κ.(2007):83-88)

### 2.3.4. Διεθνή συνεργασία

Ο διακρατικός χαρακτήρας των εγκλημάτων του διαδικτύου, καθώς και η αστάθεια των ηλεκτρονικών στοιχείων επιβάλλουν τη διεθνή συνεργασία μεταξύ των αρχών επιβολής του Νόμου. Η ουσιαστική και διαδικαστική νομοθεσία μεταξύ των κρατών θα πρέπει να είναι συμβατή και αμοιβαία. Οι αρχές επιβολής του νόμου θα πρέπει να έχουν τη νομική ισχύ να ερευνούν τα συστήματα των υπολογιστών, να διατηρούν τα ηλεκτρονικά αποδεικτικά στοιχεία και να λαμβάνουν άλλα ερευνητικά μέτρα. [1]

### 2.3.5. Ατομική αυτοπροστασία

Ο κάθε χρήστης του διαδικτύου πρέπει να είναι προσεκτικός με τις πληροφορίες που μοιράζεται στο διαδίκτυο και στα κοινωνικά μέσα. Οι προσωπικές πληροφορίες μπορεί να βοηθήσουν τους εγκληματίες να προβλέψουν τους κωδικούς του χρήστη ή να απαντήσουν σε ερωτήσεις ασφαλείας. Επίσης δεν πρέπει να κάνει κλικ σε ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου ή μήνυμα κειμένου που ζητά να ενημερώσει ή να επαληθεύσει τα στοιχεία του λογαριασμού. Θα πρέπει να εξετάζει προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τη διεύθυνση URL και την ορθογραφία που χρησιμοποιούνται σε οποιαδήποτε αλληλογραφία. Οι απατεώνες χρησιμοποιούν μικρές διαφορές για να ξεγελάσουν το μάτι και να κερδίσουν την εμπιστοσύνη του. Ο χρήστης επίσης θα πρέπει να κατεβάζει κάτι με προσοχή και να μην ανοίγει συνημμένο email από κάποιον που δεν γνωρίζει και να προσέχει τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου που του προωθούνται. Επίσης να επαληθεύει προσωπικά τα αιτήματα πληρωμής και αγοράς ή να καλεί το άτομο για να βεβαιώνεται ότι είναι νόμιμο και να επαληθεύει οποιαδήποτε αλλαγή στον αριθμό λογαριασμού ή στις διαδικασίες πληρωμής με το άτομο που υποβάλλει το αίτημα.[4]

[4] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

### 2.3.6. Προστασία Επιχειρήσεων

Οι επιχειρήσεις θα πρέπει αφιερώσουν χρόνο ώστε να προσδιορίσουν που μπορεί να κινδυνεύουν από απάτη. Θα πρέπει να γνωρίζουν, να αξιολογούν και να μειώνουν τους κινδύνους ώστε να υπάρχει έλεγχος της κατάστασης. Υπάρχουν γενικές αρχές που μπορούν να εφαρμόσουν όλες οι επιχειρήσεις. Οι αρχές αυτές βασίζονται σε τέσσερις ουσιαστικούς τομείς, τους οποίους πρέπει να σκεφτούν ώστε να μπορούν να αντιλαμβάνονται μία απάτη. Θα πρέπει να γνωρίζουν τους πελάτες τους, τους υπαλλήλους τους, τους προμηθευτές και τα περιουσιακά τους στοιχεία με σκοπό να προστατεύσουν την επιχείρηση τους. Οι τράπεζες θα πρέπει να επαναπροσδιορίζουν τις διαδικασίες τόσο τις εσωτερικές όσο και αυτές των πελατών που βασίζονται σε μια συνεχή εκτίμηση των πραγματικών περιπτώσεων απάτης, οικονομικού εγκλήματος και διαδικτυακής απειλής. Αυτό θα βοηθήσει στην προστασία τόσο της τράπεζας όσο και των πελατών της,[5]

## Κεφάλαιο 3:ΔΙΑΔΙΚΤΥΑΚΗ ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ

### 3.1.Έννοια της Παιδική πορνογραφία στο διαδίκτυο

Παιδική πορνογραφία είναι η μορφή παρενόχλησης στο διαδίκτυο κατά την οποία υπάρχει «οπτική απεικόνιση ανηλίκου με φανερά σεξουαλική συμπεριφορά»(Γάκη, Α., & Αντωνίου Α.,

[5] tps://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

2014), όπου ανήλικα παιδιά συμμετέχουν σε διάφορα είδη σεξουαλικής αναπαράστασης. (Σταθοπούλου, Ι. Μ., 2022) Είναι και κάθε αναφορά σεξουαλικής δραστηριότητας στην οποία εμπλέκεται άτομο προεφηβικής ηλικίας ή περιλαμβάνει φωτογραφίες, τηλεοπτικές εικόνες και ηχογραφήσεις. . (Κελεγκουριάδη, Α., & Μαλλιαρού, Α., 2016) Η παιδική πορνογραφία μπορεί να οριστεί και ως «η απεικόνιση παδιών, τα οποία είτε μέσω εξαναγκασμού είτε μέσω της πειθούς εμπλέκονται σε σεξουαλική δραστηριότητα, προκειμένου άτομα με σεξουαλικό ενδιαφέρον σε ανήλικους να ικανοποιηθούν» (Sykas, S., 2019).

Η διαδικτυακή παιδική πορνογραφία παρουσιάζει συγκεκριμένα χαρακτηριστικά, τα οποία την κάνουν να ξεχωρίζει από τις συνηθισμένες μορφές παιδικής πορνογραφίας. Με το διαδίκτυο μπορεί οποιοδήποτε πρόσωπο σε οποιοδήποτε μέρος του κόσμου, οποιαδήποτε ώρα, να έχει πρόσβαση σε μεγάλο αριθμό εικόνων πορνογραφίας. Η επίσκεψη των χρηστών του διαδικτύου σε τέτοιες ιστοσελίδες είναι ανώνυμη και ιδιωτική. Οι χρήστες, μέσω του διαδικτύου, μπορούν να επικοινωνήσουν και να ανταλλάξουν εικόνες με άμεσο τρόπο και χωρίς οποιαδήποτε δαπάνη, ενώ οι σχηματικές απεικονίσεις που μπορούν να διανέμουν είναι ποικίλες. Ο κάθε χρήστης έχει τη δυνατότητα τόσο να παρέχει πορνογραφικές εικόνες, ως διακινητής, όσο και να τις δημιουργεί, ως παραγωγός. (Κελεγκουριάδη, Α., & Μαλλιαρού, Α., 2016)

Το διαδίκτυο και οι υπολογιστές παρέχουν την δυνατότητα στους παιδόφιλους να βλέπουν, να ανταλλάσσουν και να αποθηκεύουν παιδικό πορνογραφικό υλικό, ενώ η κοινωνική και τεχνολογική υποστήριξη που προσφέρουν προωθούν την ανάπτυξη και διατήρηση της παιδικής πορνογραφίας σε διεθνές επίπεδο. (Ρουσσοπούλου, Θ., 2023:26) Οι χρήστες επισκέπτονται ένα εικονικό περιβάλλον, το οποίο ταυτόχρονα είναι πραγματικό για τους πρωταγωνιστές, καθότι έχει δημιουργηθεί σε συγκεκριμένο τόπο και χρόνο. Ωστόσο εάν ο χρήστης επιθυμεί το εικονικό περιβάλλον να γίνει πραγματικό μπορεί να επικοινωνήσει άμεσα με τους παραγωγούς, καθώς και να έχει off-line σχέσεις και γνωριμίες. (Κελεγκουριάδη, Α., & Μαλλιαρού, Α., 2016)

Οι υποστηρικτές της ποινικοποίησης της εικονικής παιδική πορνογραφίας υποστηρίζουν ότι η είτε η πραγματική είτε η εικονική απεικόνιση ενός παιδιού σε σεξουαλική δραστηριότητα καθιστά το παιδί θύμα όπως συμβαίνει στην πραγματική παιδική πορνογραφία. Επίσης με την εικονική παιδική πορνογραφία, οι παιδόφιλοι εμπλέκονται σε παιδική κακοποίηση χωρίς φόβο και αναστολές, ενώ πολλές φορές προσπαθούν να πείσουν ανήλικους να συμμετάσχουν σε

πραγματικές καταστάσεις. Αντίθετα, η άλλη πλευρά υποστηρίζει ότι κατά την παραγωγή της εικονικής παιδικής πορνογραφίας δεν επηρεάζεται κάποιο πραγματικό παιδί και ούτε αυτό εμπλέκεται με οποιοδήποτε τρόπο κατά τη διακίνηση και κατοχή της. Δεν έχει οποιαδήποτε επίπτωση σε κάποιο παιδί και επομένως δεν θα πρέπει να απαγορεύεται νομικά. Επίσης υποστηρίζουν ότι με την απαγόρευση της εικονικής παιδικής πορνογραφίας ποινικοποιείται η φαντασία, καθότι η σεξουαλική έλξη προς ένα παιδί δεν έχει οποιαδήποτε επίπτωση σε οποιοδήποτε πραγματικό παιδί. (Sykas, S., 2019)

Η παιδική πορνογραφία ταξινομείται σε δέκα επίπεδα με βάση το περιεχόμενο και τη σοβαρότητα της. Το πρώτο επίπεδο είναι η **εκδηλωτική παιδική πορνογραφία**, το οποίο περιέχει εικόνες μη σεξουαλικού περιεχομένου που προέρχονται από νόμιμες πηγές. Το δεύτερο επίπεδο είναι η **γυμνή απεικόνιση**, το οποίο περιλαμβάνει εικόνες με γυμνά ή ημίγυμνα παιδιά που προέρχονται από νόμιμες πηγές. Το τρίτο επίπεδο είναι η **ερωτική παιδική πορνογραφία**, η οποία περιλαμβάνει εικόνες που λαμβάνονται από παιδιά κρυφά, στις οποίες φαίνονται διάφορα μέρη του σώματος τους. Το τέταρτο επίπεδο είναι το **ποζάρισμα**, το οποίο περιλαμβάνει εικόνες όπου παιδιά ποζάρουν αποκαλύπτοντας διάφορα μέρη του σώματος τους. Το πέμπτο επίπεδο είναι οι **ερωτικές στάσεις**, που περιλαμβάνουν εικόνες όπου γυμνά παιδιά δείχνουν μέρη του σώματος τους. Το έκτο επίπεδο είναι η **εμφανής ερωτική στάση**, που περιλαμβάνει εικόνες όπου τονίζονται τα γεννητικά όργανα. Το έβδομο επίπεδο είναι η **εμφανής σεξουαλική δραστηριότητα**, το οποίο περιλαμβάνει εικόνες όπου ανήλικα παιδιά αναπαριστούν μια σεξουαλική πράξη. Το όγδοο επίπεδο είναι η **επιθετική παιδική πορνογραφία**, που περιλαμβάνει εικόνες όπου υπάρχει σεξουαλική κακοποίηση παιδιών με τη συμμετοχή ενήλικων προσώπων. Το ένατο επίπεδο είναι η **ολοκληρωτική επιθετική παιδική πορνογραφία**, το οποίο περιλαμβάνει τη σεξουαλική κακοποίηση παιδιών από ενήλικες με διεισδυτικό σεξ, αυνανισμό και στοματικό έρωτα. Το δέκατο επίπεδο είναι η **σαδιστική και κτηνώδης παιδική πορνογραφία**, όπου τα παιδιά αισθάνονται πόνο ή αναγκάζονται να έρθουν σε σεξουαλική επαφή με ζώα. (Δημόπουλος, Χ., 2006)

Η διαδικτυακή παιδική πορνογραφία είναι δύσκολο να εκτιμηθεί καθότι το εμπόριο της γίνεται στα κρυμμένα επίπεδα του διαδικτύου. Ωστόσο έχει διαπιστωθεί ότι οι επισκέψεις που γίνονται

σε μια ηλεκτρονική σελίδα παιδικής πορνογραφίας μπορεί να φθάσει το ένα εκατομμύριο μηνιαίως. (Ρουσσοπούλου, Θ., 2023:26)

### 3.2.Προφίλ χρηστών διαδικτυακής παιδικής πορνογραφίας

Ο χρήστης της παιδικής πορνογραφίας στο διαδίκτυο δεν έχει συγκεκριμένο τύπο και συνεπώς δεν είναι εύκολη η αναγνώριση του. Ωστόσο υπάρχουν ορισμένα κοινά χαρακτηριστικά που έχουν οι χρήστες αυτοί. Το πρώτο χαρακτηριστικό είναι ότι οι χρήστες της διαδικτυακής παιδικής πορνογραφίας δεν συμμετέχουν κατ΄ ανάγκη σε πραγματική σεξουαλική κακοποίηση παιδιού. Με το διαδίκτυο μπορούν να ικανοποιήσουν την περιέργεια τους, ανεξάρτητα αν είναι παιδόφιλοι ή όχι. Το δεύτερο χαρακτηριστικό είναι ότι οι χρήστες αυτοί ίσως να έχουν ερωτική σχέση, συγκεκριμένο επάγγελμα, τριτοβάθμια εκπαίδευση, λευκό ποινικό μητρώο, κάτι που καθιστά δύσκολο τον καθορισμό του στερεότυπου τους. Το τρίτο χαρακτηριστικό γνώρισμα τους είναι το λευκό χρώμα, το αρσενικό φύλο, η ηλικία 26-40 ετών κατά την διάπραξη του εγκλήματος και η έντονη απασχόληση με το διαδίκτυο. (Ρουσσοπούλου, Θ., 2023)

Οι χρήστες της διαδικτυακής παιδικής πορνογραφίας μπορούν να ταξινομηθούν σε τρεις κατηγορίες ανάλογα με την ψυχολογική τους προοπτική. Η πρώτη κατηγορία είναι οι **ψυχαγωγικοί χρήστες.** Οι ψυχαγωγικοί χρήστες είναι οι χρήστες που επιδιώκουν την προσωρινή ψυχαγωγία και ίσως να μην παρουσιάσουν μακροπρόθεσμα προβλήματα. Η δεύτερη κατηγορία είναι οι **χρήστες σε κατάσταση κινδύνου**. Οι χρήστες αυτοί ευάλωτα πρόσωπα που εκδηλώνουν την τάση προς την παιδική πορνογραφία λόγω του διαδικτύου. Είναι εγκληματίες μεσαίας επικινδυνότητας και το διαδίκτυο αποτελεί γι αυτούς μέσο ευκαιρίας. Η Τρίτη κατηγορία είναι οι **καταναγκαστικοί χρήστες**. Οι χρήστες αυτοί θεωρούν τα παιδιά σεξουαλικά αντικείμενα και έχουν ανάγκη την παιδική πορνογραφία για να νιώσουν ικανοποίηση. Είναι εγκληματίες ενδογενής επικινδυνότητας, οι οποίοι εκ γενετής νιώθουν σεξουαλική έλξη από τα παιδιά και το διαδίκτυο λειτουργεί γι αυτούς το μέσο ευκαιρίας. (Ρουσσοπούλου, Θ., 2023)

Ωστόσο, η διαφορά μεταξύ των συμπεριφορών τους στο διαδίκτυο μπορεί να τους διακρίνει στις ακόλουθες κατηγορίες, βάση την μορφή εκδήλωσης του αδικήματος. Οι **χρήστες βοσκοί**, οι οποίοι μη εσκεμμένα βρίσκουν εικόνες παιδικής πορνογραφίας, αλλά τις φυλάγουν με επίγνωση

και δεν συσχετίζονται με άλλους χρήστες. Οι **ιδιωτικά φαντασιωμένοι χρήστες**, οι οποίοι σχηματίζουν ψηφιακές εικόνες για να ικανοποιήσουν τις δικές τους σεξουαλικές επιθυμίες και δεν συσχετίζονται με άλλους χρήστες. Οι **χρήστες αλιείς ή ψαράδες**, οι οποίοι ψάχνουν να βρουν παιδική πορνογραφία στο διαδίκτυο και προσπαθούν να συσχετιστούν με άλλους χρήστες. Οι **μη ασφαλή συλλέκτες,** οι οποίοι αναζητούν παιδική πορνογραφία στο διαδίκτυο, κυρίως σε μη ασφαλή δωμάτια. Οι χρήστες αυτοί συσχετίζονται με άλλους χρήστες σε μεγάλο βαθμό, χωρίς να παίρνουν μέτρα ασφάλειας. Οι **ασφαλείς συλλέκτες,** οι οποίοι αποτελούν μέρος μιας κλειστής και μυστικής ομάδας παιδόφιλων, που συσχετίζονται μεταξύ τους σε πολύ μεγάλο βαθμό. Τα μέτρα ασφάλειας που λαμβάνουν είναι υψηλού επιπέδου για να προστατεύουν τις πράξεις τους.

Οι **χρήστες ιπποκόμοι**, οι οποίο δημιουργούν σχέσεις με παιδιά, μέσω του διαδικτύου, με απώτερο σκοπό την άμεση κακοποίηση τους. Οι **ηθικοί αυτουργοί κατάχρησης παιδιών σε ασελγεία**, οι οποίοι διενεργούν σεξουαλική κακοποίηση σε παιδιά και καταφεύγουν στην παιδική πορνογραφία για την ικανοποίηση τους ως παιδόφιλοι. Οι χρήστες αυτοί συνήθως συσχετίζονται με άλλους χρήστες. Οι **χρήστες παραγωγοί,** οι οποίοι παρουσιάζουν την σεξουαλική κακοποίηση των παιδιών με σκοπό να την διανέμουν σε άλλους χρήστες. Οι **χρήστες διανομείς**, οι οποίοι διαδίδουν εικόνες που περιέχουν ασελγείς πράξεις ενήλικων προσώπων σε παιδιά. (Δημόπουλος, Χ., 2006)

### 3.3.Τρόποι προστασίας από την παιδική πορνογραφία

#### 3.3.1.Υποχρεώσεις γονέων

Οι γονείς θα πρέπει να αποκτήσουν την εμπιστοσύνη των παιδιών τους, ούτως ώστε όταν το παιδί έχει ανάγκη για επίλυση οποιασδήποτε απορίας, να καταφεύγει άμεσα και απευθείας σε αυτούς και όχι σε αγνώστους. Επίσης θα πρέπει να τα στηρίζουν και να κατανοούν τις δυσκολίες τους και να αναπτύξουν την επικοινωνία μεταξύ τους, ώστε τα παιδιά να νιώσουν ότι έχουν υποστήριξη από το οικογενειακό και φιλικό τους περιβάλλον, προκειμένου να μην χρειαστεί να καταφύγουν αλλού όταν θα βρεθούν σε κάποια δύσκολη φάση κατά την παιδική τους ηλικίας. (Williams, Elliot & Beech, 2013)

Οι γονείς θα πρέπει να πληροφορούν τα παιδιά τους για τους κινδύνους που υπάρχουν στο διαδίκτυο, ώστε τα παιδιά τους να αντιληφθούν τι συμβαίνει και να μπορούν να προστατεύονται

και αν ακόμη χρησιμοποιούν υπολογιστή χωρίς προστασία. Οι γονείς θα πρέπει επίσης να έχουν πλήρη γνώση των φίλων των παιδιών τους στο διαδίκτυο καθώς και τους ιστοχώρους που επισκέπτονται. Ο υπολογιστής των μικρών παιδιών θα πρέπει να είναι μέσα σε κοινό δωμάτιο της οικογένειας. (Dombrowski, & Gischlar, 2007)

### 3.3.2.Κοινωνικοί λειτουργοί και σχολείο

Η ενημέρωση αποτελεί ένα από τα κυριότερα μέτρα πρόληψης. Τα παιδιά θα πρέπει να ενημερώνονται για τους κινδύνους που διατρέχουν, μέσω του σχολείου, τόσο από τους δασκάλους όσο και από τους κοινωνικούς λειτουργούς. Το σχολείο, ξεκινώντας από το δημοτικό, πρέπει να ενημερώνει τα παιδιά για την ύπαρξη ενήλικων με συγκεκριμένη σεξουαλική συμπεριφορά. Θα πρέπει να μάθουν να χειρίζονται προτάσεις από ενήλικα πρόσωπα σεξουαλικού τύπου, να μπορούν να διαφύγουν από αυτά και να ενημερώνουν άμεσα εχέμυθο πρόσωπο για το συμβάν. Τα παιδιά πρέπει να κατανοήσουν ότι η άρνηση σε τέτοιου είδους προτάσεις είναι αναγκαία για την ασφάλεια τους. (Παπαϊωάννου, Κ., 2000 )

### 3.3.3.Πολιτεία

Η πολιτεία είναι αναγκαίο να συμβάλει και αυτή στην πρόληψη της παιδικής πορνογραφίας. Θα πρέπει να προχωρήσει στην κοινοποίηση του θέματος σε όλους τους πολίτες ενημερώνοντας τους έγκυρα και λεπτομερώς, μέσω της διοργάνωσης προγραμμάτων κοινωνικής ευαισθητοποίησης σε συνεργασία με άλλους φορείς. Επίσης, πρέπει να ενισχύσει την ομάδα δίωξης του ηλεκτρονικού εγκλήματος και μέσω του νομοθετικού πλαισίου πρέπει να παρέχει προστασία και ασφάλεια στο παιδί ενώ ταυτόχρονα να καταδικάζει τον δράστη. (Γάκη, Α., & Αντωνίου, Α., 2014)

## Κεφάλαιο 4:ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

### 4.1.Έννοια του διαδικτυακού εκφοβισμού

Ζούμε στην εποχή της τεχνολογίας όπου η χρήση του διαδικτύου είναι ευρέως διαδεδομένη. Παρά τα θετικά που προσφέρει το διαδίκτυο στην ανθρωπότητα, η κατάχρηση και η λανθασμένη χρήση του έχει συμβάλει στην δημιουργία νέων μορφών εγκληματικών φαινομένων, όπως είναι ο διαδικτυακός εκφοβισμός. (Βάττη, Ι., & Παναγιώτου, Ά., 2019).

Ο διαδικτυακός εκφοβισμός είναι «ένα φαινόμενο επαναλαμβανόμενης επιθετικότητας, παρενόχλησης, προσβολής, ταπείνωσης, ρατσιστικής και αυταρχικής συμπεριφοράς κυρίως σε παιδιά η εφήβους, που δέχονται μέσω της χρήσης του διαδικτύου και των διάφορων ψηφιακών συσκευών». (Λαζαροπούλου, Κ., & Τσαγκρινός, Σ., 2017). Ο θύτης εκδηλώνει την επιθετική του συμπεριφορά μέσω της οθόνης του ηλεκτρονικού υπολογιστή ή του κινητού, χωρίς τη φυσική του παρουσία με σκοπό τον εκφοβισμό του θύματος (Γάκης, Κ. 2021).

Το φαινόμενο αυτό, αποτελεί μια μορφή εκφοβισμού που γίνεται ολοένα και πιο εμφανή μεταξύ των νέων τα τελευταία χρόνια, κυρίως μέσω των ηλεκτρονικών συσκευών, των κινητών τηλεφώνων, των ηλεκτρονικών μηνυμάτων και των ιστοσελίδων. (Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. 2006).

Ο διαδικτυακός εκφοβισμός παρουσιάζεται συστηματικά από τον θύτη προς το θύμα με αποτέλεσμα να επηρεάζεται η διάθεση του θύματος. Ο θύτης μπορεί να είναι ένα ή περισσότερα πρόσωπα που δρουν εναντίον ενός προσώπου ή μιας ομάδας προσώπων με σκοπό να προκαλέσουν αναστάτωση και επιδιώκουν κάποιες φορές να κάνουν το θύμα να νιώθει ένοχο για την θυματοποίηση του. Ο θύτης προέρχεται κυρίως από προβληματικές οικογένειες και μπορεί να υπήρξε θύμα βίας στο οικογενειακό του περιβάλλον ή ακόμη και θύμα εκφοβισμού, ενώ μπορεί να έχει χαμηλή αυτοεκτίμηση και αυτοπεποίθηση. Το θύμα έχει χαμηλή αυτοπεποίθηση και αυτοεκτίμηση με αδύνατο χαρακτήρα, χωρίς κοινωνικές δεξιότητες, κάτι που το καθιστά ανίκανο να προστατευθεί. Ως εκ τούτου, το θύμα δεν εκφράζει τα συναισθήματα του και εύκολα μπορεί να οδηγηθεί σε κάποια ψυχολογική διαταραχή, όπως είναι η κατάθλιψη και η μελαγχολία ενώ μπορεί να οδηγηθεί και στον τραυματισμό του ίδιου, α`κόμη και στην αυτοκτονία. (Αραμπατζόγλου, Γ. 2022).

Σύμφωνα με έρευνα που έγινε στο Ελληνικό Κέντρο Ασφαλούς Δικτύου ΙΤΕ (2021), περίπου το 15-35% των εφήβων έχει πέσει θύμα διαδικτυακού εκφοβισμού, ενώ το 10-20% των εφήβων έχει

συμμετάσχει σε συμβάντα εκφοβισμού. Αναφορικά με το φύλο, τα κορίτσια έχουν μεγαλύτερη πιθανότητα να συμμετάσχουν σε τέτοια περιστατικά σε σύγκριση με τα αγόρια. Η ηλικία των παιδιών που εμπλέκονται σε διαδικτυακό εκφοβισμό είτε ως θύματα είτε ως θύτες είναι κατά πλειοψηφία 12-16 χρονών. (Μάλλιου, Ε., Λιγνού, Μ., Μαυρουδής, Χ., & Κατσανός, Κ., 2023).

Ο διαδικτυακός εκφοβισμός εξαπλώνεται σε ανησυχητικό βαθμό σε όλο τον κόσμο, καθότι μπορεί να οδηγήσει τα θύματα ακόμη και στο θάνατο. Από μελέτες που έχουν γίνει διαφάνηκε ότι αξιοσημείωτο ποσοστό μαθητών έχει βιώνει τον εκφοβισμό στο διαδίκτυο και έχει γίνει αποδεκτό ότι το φαινόμενο αυτό αποτελεί ένα από τα σοβαρότερα προβλήματα που υπάρχουν. (Τσάγκα, Δ., 2020)

### 4.2.Μορφές διαδικτυακού εκφοβισμού

Ο διαδικτυακός εκφοβισμός μπορεί να εκδηλωθεί με διάφορες μορφές. Μια από τις συχνότερες μορφές είναι η παρενόχληση μέσω της αποστολής επιθετικών, προσβλητικών και απειλητικών μηνυμάτων στο ηλεκτρονικό ταχυδρομείο ή στα μέσα κοινωνικής δικτύωσης. Η δυσφήμηση είναι εξίσου συχνή μορφή διαδικτυακού εκφοβισμού και αποβλέπει στην καταστροφή της δημόσιας εικόνας ενός προσώπου ή των διαπροσωπικών του σχέσεων. Αυτό μπορεί να γίνει μέσω της δημοσιοποίησης υποτιμητικών ή ψευδών στοιχείων αναφορικά με ένα πρόσωπο είτε μέσω ιστοσελίδων είτε μέσω μηνυμάτων. Μια άλλη μορφή διαδικτυακού εκφοβισμού που έχει πάρει τεράστιες διαστάσεις είναι ο κοινωνικός αποκλεισμός. Ο αποκλεισμός αυτός μπορεί να γίνει εσκεμμένα, αποκλείοντας ένα πρόσωπο από μια κοινωνική ομάδα, της οποίας αποτελεί μέλος, χωρίς τη συναίνεση του, αλλά και μέσω ενός μηνύματος το οποίο πληροφορεί ένα πρόσωπο ότι δεν είναι επιθυμητό σε κάποια κοινωνική εκδήλωση ή συνάντηση. (Βάττη, Ι., & Παναγιώτου, Ά., 2019).

Ο Williard (2007) ταξινόμησε τον διαδικτυακό εκφοβισμό σε μηνύματα που αποστέλλονται στο διαδίκτυο, λόγω αντιπαλοτήτων, τα οποία περιέχουν αγενή και χυδαία γλώσσα, σε μηνύματα προσβλητικού περιεχομένου που αποστέλλονται στο διαδίκτυο μεταξύ δύο προσώπων, σε απειλές πρόκλησης βλάβης ή σοβαρού εκφοβισμού που προκαλούν παρενόχληση στο διαδίκτυο ανάμεσα σε τουλάχιστον δύο πρόσωπα, σε απειλές στον κυβερνοχώρο που αποτελούν γενικές δηλώσεις, την αποστολή ή δημοσιοποίηση ψευδών δηλώσεων για ένα πρόσωπο με σκοπό τη δυσφήμιση του, την αποστολή η δημοσιοποίηση δεδομένων με αποστολέα πρόσωπο που προσποιείται κάποιο

άλλο πρόσωπο με στόχο τον επηρεασμό των διαπροσωπικών του σχέσεων, την αποστολή ή δημοσιοποίηση προσωπικών και ευαίσθητων δεδομένων ενός προσώπου, την εξαπάτηση ενός προσώπου με στόχο την συλλογή προσωπικών του στοιχείων και την διάδοση τους σε άλλα πρόσωπα και τον σκόπιμο αποκλεισμό ενός προσώπου από κάποια διαδικτυακή ομάδα. (Μανωλοπούλου, Β., & Μητσιοπούλου, Γ., 2020).

Οι Smith, Madhavi, Calvalho και Tripet (2006) διέκριναν τον διαδικτυακό εκφοβισμό στην αποστολή μηνυμάτων μέσω του κινητού, στην αποστολή εικόνων και βίντεο μέσω του κινητού, μέσω φωνητικών κλήσεων, μέσω της αποστολής μηνυμάτων στο ηλεκτρονικό ταχυδρομείο, μέσω των ομάδων συζήτησης στο διαδίκτυο, μέσω άμεσων μηνύματα και μέσω ιστοσελίδων. (Γάκης, Κ. 2021).

### 4.3.Παραδοσιακός εκφοβισμός vs διαδικτυακός εκφοβισμός

Κάποιοι ερευνητές πιστεύουν ότι ο διαδικτυακός εκφοβισμός αποτελεί επέκταση του παραδοσιακού εκφοβισμού, ενώ κάποιοι θεωρούν ότι είναι διαφορετική μορφή εκφοβισμού με διαφορετικές επιπτώσεις για τους συμμετέχοντες. Οι δύο αυτές μορφές εκφοβισμού συσχετίζονται μεταξύ τους και ο θύτης κατέχει τον ίδιο ρόλο.( Γάκης, Κ., 2021).

Τόσο στον παραδοσιακό όσο και στον διαδικτυακό εκφοβισμό υπάρχουν τα στοιχεία της επιθετικότητας, της επανάληψης της πράξης, της ανισότητας που υπάρχει στη δύναμη του θύτη σε σχέση με αυτή του θύματος και οι αρνητικές εμπειρίες που προκαλούνται στο θύμα. (Γάκης, Κ., 2021).

Ωστόσο υπάρχουν κάποια στοιχεία που διαφοροποιούν τον διαδικτυακό εκφοβισμό από τον παραδοσιακό. Στον διαδικτυακό εκφοβισμό υπάρχει η ανωνυμία του θύτη. Το διαδίκτυο παρέχει τη δυνατότητα στο θύτη να αποκρύβει την πραγματική του ταυτότητα κάνοντας το να δρα πιο εύκολα και χωρίς το φόβο αντιμετώπισης των συνεπειών των πράξεων του, με αποτέλεσμα να ευνοείται από αυτό. Αντίθετα, το θύμα που δεν γνωρίζει την ταυτότητα του θύτη καθίσταται πιο δύσκολο να τον αντιμετωπίσει, με αποτέλεσμα να προκαλείται σε αυτόν περισσότερος φόβος, άγχος και σύγχυση και κατ΄ επέκταση να διαταράσσεται η ψυχολογία του. (Βάττη, Ι., & Παναγιώτου, Ά., 2019) Η ανωνυμία του θύτη δυσκολεύει τις αρχές να τον εντοπίσουν, καθότι δεν

υπάρχει χαρακτηριστικό κοινωνικοδημογραφικό προφίλ, και έτσι προκαλείται περισσότερη ψυχολογική αναστάτωση στο θύμα. (Αραμπατζόγλου, Γ., 2022).

Η γεωγραφική απόσταση είναι επίσης άλλο στοιχείο που διακρίνει τον διαδικτυακό εκφοβισμό από τον παραδοσιακό. Το διαδίκτυο επιτρέπει στο θύτη να δρα οποιαδήποτε ώρα, καθότι δεν απαιτείται η φυσική του επαφή με το θύμα σε σχέση με τον παραδοσιακό εκφοβισμό. Αυτό μειώνει την ενσυναίσθηση του θύτη προς το θύμα. Ο διαδικτυακός εκφοβισμός μπορεί να διαπραχθεί σε παγκόσμιο ακροατήριο λόγω της ανεξέλεγκτης γεωγραφικής απόστασης που υπάρχει σε σύγκριση με τον παραδοσιακό εκφοβισμό που έχει περιορισμένο ακροατήριο, καθότι απαιτείται η φυσική του παρουσία στο χώρο που διαπράττεται ο εκφοβισμός. Όσο μεγαλύτερο είναι το ακροατήριο στο διαδικτυακό εκφοβισμό, τόσο αυξάνεται η δύναμη του θύτη και ταυτόχρονα ο εξευτελισμός του θύματος. Ωστόσο, το ακροατήριο στον παραδοσιακό εκφοβισμό μπορεί να επηρεάσει το θύτη είτε υπέρ του ίδιου, ενισχύοντας τον, είτε αρνητικά υποστηρίζοντας το θύμα.(Βάττη, Ι., & Παναγιώτου, Ά., 2019).

Η χρονική συνέχεια του διαδικτυακού εκφοβισμού τον διαφοροποιεί από τον παραδοσιακό εκφοβισμό. Τα περιστατικά διαδικτυακού εκφοβισμού μπορούν να καταγραφούν στο διαδίκτυο μόνιμα σε σχέση με τα περιστατικά του παραδοσιακού εκφοβισμού που ξεχνιούνται με την πάροδο το χρόνου. Το γεγονός ότι ο διαδικτυακός εκφοβισμός μπορεί να συμβεί οποιαδήποτε ώρα χωρίς περιορισμό οδηγεί τα θύματα να τον νιώθουν ως μια συνεχή κατάσταση που επηρεάζει την προσωπική τους ζωή, ενώ ο θύτης λόγω της δυνατότητας απόκρυψης της ταυτότητας του προκαλεί εκφοβισμό στο θύμα για περισσότερο χρονικό διάστημα. (Βάττη, Ι., & Παναγιώτου, Ά., 2019).

### 4.4.Αντιμετώπιση του διαδικτυακού εκφοβισμού

Το πρόσωπο που γίνεται θύμα διαδικτυακού εκφοβισμού πρέπει να σταματήσει άμεσα την επικοινωνία με το θύτη και να το αναφέρει στου γονείς του ή σε άλλο ενήλικο πρόσωπο που μπορεί να το βοηθήσει. Ο κάθε χρήστης του διαδικτύου πρέπει να φιλτράρει τα ηλεκτρονικά μηνύματα που παραλαμβάνει από πρόσωπα που τον παρενοχλούν και να μπλοκάρει την είσοδο τους στους προσωπικούς του χώρους. (Λαζαροπούλου, Κ., & Τσαγκρινός, Σ., 2017).

Το θύμα μπορεί επίσης να αναπτύξει διάφορες στρατηγικές διαχείρισης του διαδικτυακού εκφοβισμού, που μπορεί να είναι συναισθήματα, σκέψεις και δραστηριότητες, προκειμένου να μειώσει τις αρνητικές επιπτώσεις που επιφέρει σε αυτούς το φαινόμενο αυτό. Οι πιο συνηθισμένες στρατηγικές αυτές η απόκτηση καινούργιων φίλων, αναζήτηση στήριξης από την κοινωνία, τα αντίποινα καθώς και στρατηγικές όπως είναι η αγνόηση του θύτη. Το κάθε θύμα, θα πρέπει να επιλέξει τη στρατηγική που θεωρεί καταλληλότερη, ούτως ώστε να μπορέσει να αντιμετωπίσει με επιτυχία την στρεσογόνα κατάσταση που βρίσκεται. Η επιλογή της σωστής στρατηγικής διαχείρισης θα επιφέρει μεταβολή των αρνητικών συναισθημάτων του θύματος, αλλά και πιθανής επανάληψης του περιστατικού. (Τσάγκα, Δ., 2020)

Η σωστή εκπαίδευση και διαπαιδαγώγηση στα σχολεία μπορεί να καταστείλει το φαινόμενο του διαδικτυακού εκφοβισμού. Εμπειρική έρευνα διεξήχθηκε το 2016 στη Στ΄ τάξη του Δημοτικού σχολείου Καλαμαριάς μέσα από το μάθημα των Θρησκευτικών, η οποία περιλάμβανε μεταξύ άλλων τη σύνταξη ηλεκτρονικού βιβλίου από τους συμμετέχοντες μαθητές με θέμα τον διαδικτυακό εκφοβισμό και ακολούθως την διανομή του βιβλίου αυτού σε άλλα σχολεία και βιβλιοθήκες. Πριν από την έρευνα οι μαθητές που ήταν θύματα διαδικτυακού εκφοβισμού κυριεύονταν από αρνητικά συναισθήματα όπως είναι ο πόνος, η θλίψη, η αγωνία, το αίσθημα κατωτερότητας, η ανασφάλεια, η δυστυχία και η μοναξιά. Αντίθετα, οι μαθητές που ήταν θύτες κυριαρχούνταν από επιθετικότητα, αντιπαλότητα, παρορμητικότητα, εγωισμό, υπεροπτική στάση, λεκτική και σωματική βία και χλευασμό. Μετά την έρευνα, μέσα από ανώνυμα ερωτηματολόγια και προφορικές απόψεις διαπιστώθηκε ότι κάποια από τα χαρακτηριστικά των μαθητών, είτε των θυμάτων ή θυτών είτε των υπόλοιπων μαθητών είχαν μετατραπεί σε θετικά συναισθήματα υπέρ της προσπάθειας αντιμετώπισης του φαινομένου του εκφοβισμού όπως είναι ο αλτρουισμός, η αλληλεγγύη, η αλληλοβοήθεια, ο αλληλοσεβασμός, η αλληλοκατανόηση, η ενσυναίσθηση. (Παπαθωμά, Α., 2017)

## Κεφάλαιο 5:ΔΙΑΔΙΚΤΥΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

### 5.1.Εννοια της Διαδικτυακής τρομοκρατίας

Η νέα εποχή της τεχνολογίας και συγκεκριμένα το διαδίκτυο έχει μετατρέψει την κλασσική τρομοκρατία σε κυβερνοτρομοκρατία. Το διαδίκτυο έχει μετατραπεί σε ένα ισχυρό εργαλείο για τους τρομοκράτες, ενώ η πρόσβαση τους σε πληροφορίες και δεδομένα γίνεται ολοένα και ευκολότερη. Οι εξτρεμιστές και οι τρομοκρατικές οργανώσεις, μέσω του κυβερνοχώρου, πραγματοποιούν επιθέσεις σε υπολογιστές ή προκαλούν καταστροφή σε εθνικές υποδομές, υποδηλώνοντας τη σοβαρή διάσταση της νέας τρομοκρατίας. Αυτό προκαλεί αναστάτωση στις κυβερνήσεις της υφηλίου και η απειλή της δημόσιας ασφάλειας αποτελεί κύριο ζήτημα της παγκόσμιας ατζέντας. (Κοκτσίδου, Κ., 2021)

Η κυβερνο-τρομοκρατία αποτελεί μια μορφή τρομοκρατίας, η οποία λαμβάνει χώρα στο διαδίκτυο και επιφέρει σημαντικές αρνητικές συνέπειες. Τα χαρακτηριστικά της ανωνυμίας και της δυσκολίας εντοπισμού οποιουδήποτε χρήστη στο διαδίκτυο δίνουν την ευκαιρία στους τρομοκράτες να οργανώνονται με τον τρόπο αυτό. Το F.B.I. υποστηρίζει ότι η διαδικτυακή τρομοκρατία είναι «η πολιτικά υποκινούμενη προσχεδιασμένη επίθεση σε υπολογιστές, προγράμματα υπολογιστών, ευαίσθητες πληροφορίες και δεδομένα που έχουν ως αποτέλεσμα την άσκηση βίας από μυστικούς πράκτορες ή υπερεθνικές ομάδες σε άμαχο πληθυσμό». (Καράτση, Α., & Νικολάου, Α., 2022)

Η συνεχιζόμενη εξάρτηση του κόσμου από την συνδεσιμότητα σε ένα εικονικό δίκτυο τον κάνει πιο ευάλωτο στην διαδικτυακή τρομοκρατία. Η εξάπλωση της συνδεσιμότητας, εξαπλώνει ταυτόχρονα και τους κινδύνους καθώς αυτό υποβοηθά τους τρομοκράτες και τους εξτρεμιστές. Με την εξέλιξη των στρατηγικών στρατολόγησης τους και της εκπαίδευσης των τρομοκρατών στον κυβερνοχώρο αυξάνονται και οι τεχνικές ικανότητες τους, ενώ οι επιθέσεις τους θα είναι πιο γνωστές λόγω της διαδεδομένης χρήσης των Μέσων Κοινωνικής Δικτύωσης.(Παλιάτσου, Θ., 2021).

Χαρακτηριστικό παράδειγμα διαδικτυακής τρομοκρατίας είναι η περίπτωση του δεκαεφτάχρονου Αμερικανού που δρούσε με το όνομα «Chameleon». Το πρόσωπο αυτό εντοπίστηκε να κλέβει δορυφορικές εικόνες των στρατιωτικών ιστοσελίδων των Η.Π.Α. και ακολούθως του δόθηκε χρηματική προκαταβολή των 1000 δολαρίων με σκοπό την ανταλλαγή του software, ενώ θα

εξασφάλιζε ακόμη 10000 δολάρια με την ολοκλήρωση της αποστολής του. Ωστόσο δεν ήταν επιτυχές το σχέδιο του καθότι συνελήφθηκε από το FBI πριν μεταδώσει τα στοιχεία. Το πρόσωπο αυτό υπολογίζεται ότι ήταν μέλος της οργάνωσης του Osama Bin Laden και κρίθηκε ύποπτος για τον βομβαρδισμό των Αμερικανικών βάσεων της Ανατολικής Αφρικής το 1998. (Λασηθιωτάκη, Φ., 2015)

Το διαδίκτυο παρέχει πλεονεκτήματα στους τρομοκράτες που καταφεύγουν σε αυτό καθότι είναι φθηνότερο από άλλες μεθόδους τρομοκρατίας, δεν εντοπίζονται εύκολα οι κινήσεις τους, έχουν τη δυνατότητα να επιτεθούν σε πολλούς στόχους την ίδια ώρα ενώ αυτοί βρίσκονται σε οποιοδήποτε μέρος και μπορούν να παραμείνουν ανώνυμοι λόγω της ελευθερίας έκφρασης που υπάρχει στο χώρο του διαδικτύου. Με τη χρήση του διαδικτύου μπορούν να έχουν πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων, παρακάμπτοντας τις ασφαλιστικές δικλείδες των Μ.Μ.Ε.( Αγγελάκης, Χ, & Ιωσηφέλλη, Α., 2018))

Για παράδειγμα, σύμφωνα με την έρευνα που διενεργήθηκε αναφορικά με το περιστατικό της 11ης Σεπτεμβρίου 2011 που δέχθηκαν κτύπημα οι δίδυμοι πύργοι, διαπιστώθηκε ότι οι τρομοκράτες επικοινωνούσαν μεταξύ τους μέσω ενός μεγάλου δικτύου στο διαδίκτυο προκειμένου να συντονίζουν τις κινήσεις τους. (Σαριδάκη, Ι., 2017).

Μελέτες έχουν δείξει ότι σημαντικός αριθμός ιστοσελίδων περιέχουν τον τρόπο δράσης των τρομοκρατών της ισλαμικής τρομοκρατίας. Το ισλαμικό κράτος προσπαθεί μέσω του διαδικτύου, με ενεργό και επιτυχή τρόπο, να τραβήξει το ενδιαφέρων ξένων μαχητών που προέρχονται από την Ευρώπη και την Αμερική, με τη χρήση κοινωνικών δικτύων όπως είναι το youtube και το twitter. Οι τρομοκράτες μπορούν να έχουν άμεση σύνδεση με τους ενδιαφερομένους ακροατές και οι συνδέσεις αυτές μπορούν να αναπαράγονται στο διαδίκτυο και συγκεκριμένα στις ιστοσελίδες κοινωνικής δικτύωσης.(Καραλή, Ε., 2019)

### 5.2.Τύποι τρομοκρατικών επιθέσεων στον κυβερνοχώρο

Το Κέντρο για τη Μελέτη της Τρομοκρατίας και του Παράνομου Πολέμου, στην Μεταπτυχιακή Σχολή του Ναυτικού στο Μοντερέι της Καλιφόρνιας ταξινόμησε τις ικανότητες της διαδικτυακής τρομοκρατίας σε 3 κατηγορίες. Η πρώτη κατηγορία είναι η «απλή- μη δομημένη». Η κατηγορία αυτή περιλαμβάνει την ικανότητα εκτέλεσης απλών παραβιάσεων εναντίον συγκεκριμένων

συστημάτων, με τη χρήση εργαλείων φτιαγμένων από άλλα πρόσωπα. Ο τύπος αυτός παρέχει μικρή ανάλυση του στόχου και περιορισμένες ικανότητες ελέγχου. Η δεύτερη κατηγορία είναι η «προηγμένη δομή». Η κατηγορία αυτή περιλαμβάνει την ικανότητα εκτέλεσης προχωρημένων επιθέσεων σε διάφορα συστήματα ή δίκτυα, καθώς και την παραγωγή πρωταρχικών εργαλείων εισβολής. Ο τύπος αυτός παρέχει σημαντική ανάλυση στόχων και διοικητικές ικανότητες. Η Τρίτη κατηγορία είναι η «σύνθετη συντονισμένη». Η κατηγορία αυτή περιλαμβάνει την ικανότητα εκτέλεσης συντονισμένων επιθέσεων, που μπορούν να επιφέρουν διαταραχές μαζικά σε ολοκληρωμένες άμυνες. Ο τύπος αυτός περιλαμβάνει την ικανότητα παραγωγής εργαλείων πειρατείας, ενώ παρέχουν πολύ σημαντική ανάλυση στόχων. (Σαρτέρη, Β., 2020)

Οι τρομοκρατικές επιθέσεις στον κυβερνοχώρο μπορούν να ταξινομηθούν σε πέντε τύπους, με βάση την μέθοδο της επίθεσης. Ο πρώτος τύπος είναι η «εισβολή», δηλαδή η επίθεση που αποσκοπεί στην πρόσβαση σε συστήματα υπολογιστών και δικτύων με σκοπό να λάβει ή να αλλάξει πληροφορίες. Ο δεύτερος τύπος είναι η «καταστροφή», δηλαδή η επίθεση που αποσκοπεί στην πρόσβαση σε συστήματα υπολογιστών και δικτύων για να προκαλέσει σημαντικές ζημιές και καταστροφή. Ο τρίτος τύπος είναι η «παραπληροφόρηση», δηλαδή η μέθοδος που αποβλέπει στην μετάδοση φημών ή πληροφοριών με σκοπό να προκληθούν αρνητικές συνέπειες σε καθορισμένο στόχο. Ο τέταρτος τύπος είναι η «άρνηση υπηρεσίας». Οι επιθέσεις αυτές στοχεύουν κυρίως σε ιστοσελίδες επιχειρήσεων που προβάλλονται προϊόντα ή υπηρεσίες, με σκοπό να διακόψουν τις διαδικαστικές λειτουργίες. Ο πέμπτος τύπος είναι η «αλλαγή ιστοτόπων», δηλαδή η επίθεση που αποσκοπεί στην αφαίρεση των ιστοτόπων συγκεκριμένων προσώπων, είτε με την εξ΄ ολοκλήρου αλλαγή τους με δικά τους προπαγανδιστικά μηνύματα ή είτε με τον επαναπροσανατολισμό των χρηστών σε άλλους ιστότοπους. (Σαρτέρη, Β., 2020)

## Κεφάλαιο 6:ΚΑΚΟΒΟΥΛΕΣ ΕΙΣΒΟΛΕΣ ΣΕ ΔΙΚΤΥΑ(HACKING)

### 6.1.Έννοια του Hacking

Οι κακόβουλή εισβολή σε ένα δίκτυο ή όπως είναι γνωστή με τον όρο hacking, αποτελεί «η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικών υπολογιστών η οποία καταρχήν δεν γίνεται με σκοπό την δολιοφθορά ή την καταστροφή αλλά για την ικανοποίηση για την παράκαμψη των συστημάτων ασφαλείας των ηλεκτρονικών υπολογιστών». Η έννοια αυτή αφορά κακόβουλες επιθέσεις στα συστήματα και τους υπολογιστές μέσω του διαδικτύου.(Ζαννιάς, Α., & Τσιμπούκας, Δ., 2017)

Ο όρος hacking μπορεί να αφορά «μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν αυξημένες ικανότητες, ορισμένες από τις οποίες μπορούν να χαρακτηριστούν ως παράνομες ή και εγκληματικές. Η εισβολή σε ένα τρίτο σύστημα ακόμα και αν δεν είναι κακόβουλη, ενέχει παράνομο χαρακτήρα. Ο επιτιθέμενος διεισδύοντας σε ένα τρίτο σύστημα αποκτά γνώσεις για το επίπεδο ασφάλειας του, εντοπίζει αδύνατα σημεία του και στη συνέχεια μπορεί να διαπράξει κακόβουλη επίθεση ή ακόμα και να δημοσιοποιήσει τις πληροφορίες που έχει συγκεντρώσει σε καποιον τρίτο που θα προχωρήσει αργότερα σε μια ή περισσότερες επιθέσεις». (Αγγελάκης, Χ., & Ιωσηφέλλη, Α, 2018).

Οι hackers είναι προγραμματιστές υπολογιστών, με εξειδικευμένες γνώσεις στα συστήματα υπολογιστών και κάποιες φορές εκμεταλλεύονται τις γνώσεις αυτές προκειμένου να εξασφαλίσουν φήμη, δύναμη, χρήμα. Τις περισσότερες φορές είναι οπαδοί της τεχνολογίας και κατέχουν πολύ υψηλές ικανότητες, σε επίπεδο εμπειρογνωμόνων αναφορικά με ειδικό πρόγραμμα ή γλώσσα προγραμματισμού. (Σαρτέρη, Β., 2020) Ένας hacker μπορεί να χαρακτηριστεί ως «το άτομο που έχει πολλές τεχνικές γνώσεις για τους υπολογιστές, αλλά και προχωρημένες γνώσεις προγραμματισμού, μπορεί να εντοπίσει αδυναμίες σε συστήματα υπολογιστών, να λύνει τεχνικά προβλήματα, να βελτιώνει εφαρμογές αλλά και να συνεργάζεται με άλλους όμοιους του για την επίλυση των προβλημάτων των υπολογιστών, χωρίς όμως να προξενεί κάποια ζημιά» (Λυκούρεσης, Ι., & Φραντζέσκου, Π., 2021)

Ο hacker εισβάλλει κακόβουλα σε ένα ξένο ηλεκτρονικό υπολογιστή με σκοπό να επιτύχει την εξ αποστάσεως διαχείριση του. Με την εισβολή του στον ξένο ηλεκτρονικό υπολογιστή μπορεί χωρίς τη φυσική του παρουσία, να τον διαχειριστεί, να εκτελέσει εργασίες, να ανεβάσει ιστοσελίδες, να

ανοιγοκλείνει τη οθόνη, να τυπώνει στον εκτυπωτή με τέτοιο τρόπο που θα μπορούσε να τα κάνει με τη φυσική του παρουσία εκεί. Ό hacker μπορεί να κάνει πλήρη εισβολή στον υπολογιστή με το δικαίωμα του διαχειριστή του συστήματος του ή απλή εισβολή με το δικαίωμα χρήστη του συστήματος. (Παπαγγελή, Α., 2015)

Μια επίθεση hacker αποτελείται από τέσσερα στάδια. Στο πρώτο στάδιο ο hacker συγκεντρώνει όλες τις αναγκαίες πληροφορίες σχετικά με τον ηλεκτρονικό υπολογιστή που θα θέσει σαν στόχο. Στο δεύτερο στάδιο καταφέρνει και εισβάλει στο σύστημα αποκτώντας πρόσβαση. Στο τρίτο στάδιο εκμεταλλεύεται το σύστημα, αφαιρώντας ή καταστρέφοντας δεδομένα από τον υπολογιστή ή μπορεί να το χρησιμοποιήσει για να δράσει και στο διαδίκτυο. Στο τέταρτο στάδιο εξαφανίζει τα ίχνη του, καλύπτοντας την πρόσβαση του στο σύστημα καθότι δεν έχει σκοπό να καταστρέψει εξ ολοκλήρου το σύστημα. (Παπαγγελή, Α., 2015)

Το hacking ενώ μπορεί να θεωρηθεί εγκληματικό, κάποιες χώρες χρειάζονται την εμπειρογνωμοσύνη για την ασφάλεια των πληροφοριών, με τη γνώση του hacking, προκειμένου να γίνει κατορθωτός ο χειρισμός των απειλών που υπάρχουν στον κυβερνοχώρο, κυρίως στους τομείς των επιχειρήσεων, της πολιτικής, της εθνικής ασφάλειας και των κοινωνικών μέσων. (Μπενέτου, Α., 2021)

### 6.2.Κατηγορίες hacker

Η λέξη hacker «προέρχεται από την αγγλική ρίζα hack που σημαίνει κόψιμο και την επεξεργασία ξύλου και κατά συσχέτιση, ο hacker μπορεί να «πελεκεί» εφαρμογές, προγράμματα, δίκτυα με περίτεχνο και έξυπνο τρόπο. Οι hackers είναι πολύ έξυπνα πρόσωπα και πολύ καλοί γνώστες των προγραμμάτων και λειτουργιών των δικτύων.(Ζαννιάς, Α., & Τσιμπούκας, Δ., 2017)

Οι hackers μπορούν να ταξινομηθούν σε 3 κατηγορίες. Η πρώτη κατηγορία είναι οι **Black Hat – Hackers**. Οι Black Hat –Hackers, λειτουργούν σε οργανωμένες ομάδες δημιουργώντας παράνομα και κατασκοπευτικά προγράμματα με σκοπό να καταστρέψει ή να κάνει κλοπές σε δίκτυα άλλων προσώπων. Εισβάλλουν σε δίκτυα κατασκοπεύοντας τα και καταστρέφουν ιστοσελίδες σπάζοντας τους κωδικούς. Τα κυριότερα εγκλήματα που διαπράττουν στον κυβερνοχώρο είναι οι επιθέσεις DOS/DDOS που επιβαρύνουν τους διακομιστές στο διαδίκτυο, η παραμόρφωση των ιστοσελίδων αντικαθιστώντας τις κύριες φωτογραφίες με αγενή συνθήματα, η κλοπή ταυτότητας και

προσωπικών πληροφοριών και ο τηλεχειρισμός μεγάλου αριθμού προσωπικών υπολογιστών και προγραμματισμός των «ζόμπι» για την εκτέλεση spam. Αυτή η κατηγορία hackers δρα με κίνητρο το χρήμα και όχι για κάποια ιδεολογία. Η δεύτερη κατηγορία είναι οι **White Hat –Hackers**. Οι hackers αυτοί είναι ταλαντούχοι χρήστες στην ασφάλεια του υπολογιστή για παροχή προστασίας σε δίκτυα υπολογιστών και λειτουργού με έντιμα κίνητρα. Συνήθως, εργάζονται ως φρουροί ασφαλείας μιας εταιρείας. Επίσης στην κατηγορία αυτοί ανήκουν και οι hackers που είναι τεχνικοί υπολογιστών και ασχολούνται με την παραγωγή έξυπνων προγραμμάτων. Η Τρίτη κατηγορία είναι οι **Grey Hat –Hackers**. Οι hackers αυτοί κατέχουν βασικές και ενδιάμεσες δεξιότητες της τεχνολογίας, και τους αρέσει να αποσυναρμολογούν και να αλλάζουν τα δικά τους συστήματα. Τα κυριότερα εγκλήματα που διαπράττουν είναι η κοινή χρήση αρχείων ταινιών ή η χρήση παράνομου λογισμικού. Ο σκοπός της δράσης τους είναι η μάθηση και ο πειραματισμός με τα ηλεκτρονικά συστήματα. Με την εισβολή τους στα συστήματα δεν καταστρέφουν ή προξενούν ζημιά σε αυτά, αλλά συνήθως το κάνουν για να αποδείξουν την αδυναμία της ασφάλειας τους. Δρουν μόνοι τους χωρίς να επιδιώκουν οποιοδήποτε κέρδος, ενώ καταδικάζουν τους Black Hat – Hackers .(Ζαννιάς, Α., & Τσιμπούκας, Δ., 2017)

### 6.3. Τρόποι κακόβουλης εισβολής σε δίκτυα

Οι συνηθέστεροι τρόποι κακόβουλης εισβολής σε δίκτυα που πραγματοποιούν οι hackers ταξινομούνται στις εξής κατηγορίες:

1. **SQL Injections:** Η SQL Injection είναι η τεχνική με την οποία οι hackers μπορούν να εκμεταλλευτούν τις αδυναμίες της ασφάλειας ενός λογισμικού που εκτελεί ένα ιστότοπο. Χρησιμοποιείται για να επιτεθεί σε οποιαδήποτε βάση δεδομένων SQL, η οποία δεν έχει ασφάλεια ή έχει αδύνατη ασφάλεια. Αρχικά εισάγεται μέρος του κώδικα SQL σε ένα πεδίο, κυρίως στο πεδίο όνομα χρήστη ή στο πεδίο του κωδικού πρόσβασης προκειμένου ο hacker να επιτύχει την πρόσβαση του σε ένα λογαριασμό ή ιστότοπο ενός χρήστη. Η τεχνική αυτή είναι μια εντολή που προσπαθεί να αλλάξει το περιεχόμενο της βάσης δεδομένων ώστε να επιτευχθεί η σύνδεση. Επίσης μπορεί να ανακτήσει πληροφορίες όπως για παράδειγμα ο αριθμός ή ο κωδικός πρόσβασης μιας πιστωτικής κάρτας από ιστότοπους που δεν είναι ασφαλής.

2. **Κλοπή κωδικών πρόσβασης (FTP):** Ο εισβολές ψάχνει στο σύστημα του θύματος στοιχεία σύνδεσης FTP, τα οποία στη συνέχει τα μεταφέρει στο δικό του σύστημα που βρίσκεται στον υπολογιστή του και ακολούθως επιτυγχάνει την σύνδεση στον ιστότοπο και αλλάζει τις ιστοσελίδες όπως επιθυμει. Η παραβίαση του κωδικού πρόσβασης FTP

είναι ευκολότερη όταν οι webmasters αποθηκεύουν τις πληροφορίες σύνδεσης τους στον ιστότοπο σε υπολογιστές με χαμηλή ασφάλεια.

3. **Cross-site scripting**: Είναι ένας τρόπος παράκαμψης του συστήματος ασφαλείας, γνωστός και ως XSS. Σε μια επίθεση XSS μολύνεται μια ιστοσελίδα με κακόβουλο κώδικα ή πρόγραμμα από την πλευρά του πελάτη. Ακολούθως, όταν ο πελάτης επισκεφθεί την ιστοσελίδα αυτή ο κώδικας μεταφορτώνεται σε ένα πρόγραμμα περιήγησης και εκτελείται. Ο εισβολέας εισάγει κυρίως HTML, JavaScript, VBScript, ActiveX ή Flash σε μια αδύνατη εφαρμογή με σκοπό να εξαπατήσει και να εξασφαλίσει εμπιστευτικά στοιχεία.

(Σαρτέρη, Β., 2020)

## 8. Βιβλιογραφία/ Ιστοσελίδες


Dombrowski, S.C.,Gischlar, K.L., & Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: *A major dilemma of the internet. Child Abuse Review*, 16,153-170 στο Γάκη, Α., & Αντωνίου, Α. Σ. (2014). Μορφές διαδικτυακής παρενόχλησης (διαδικτυακή αποπλάνηση και παιδική πορνογραφία): *προτάσεις αντιμετώπισης*. Πανελλήνιο Συνέδριο Επιστημών Εκπαίδευσης, 2014(2), 683-692.

Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. Dfes puplications. στο Θανοπούλου, Μ. (2015). Διαδικτυακός εκφοβισμός σε εφήβους και ο ρόλος της οικογένειας.

Sykas, S. (2019). Digital crime and crime within a digital environment: *The child pornography case*. Homo Virtualis, 2(1), 57-62.

Williams, R., Elliot, I. & Beech, A. R. (2013) Identifying sexual grooming themes used by internet sex offenders. Deviant Behavior, 34, 135-152 στο Γάκη, Α., & Αντωνίου, Α. Σ. (2014). Μορφές διαδικτυακής παρενόχλησης (διαδικτυακή αποπλάνηση και παιδική πορνογραφία): *προτάσεις αντιμετώπισης*. Πανελλήνιο Συνέδριο Επιστημών Εκπαίδευσης, 2014(2), 683-692.

Αγγελάκης, Χ. Ν. Α., & Ιωσηφέλλη, Α. Α. (2018). Ηλεκτρονικό έγκλημα: *Μόρφες και αντιμετώπιση*.

Αραμπατζόγλου, Γ. (2022). Διαδικτυακός εκφοβισμός εν μέσω κορονοϊού (Doctoral dissertation, Πανεπιστήμιο Δυτικής Μακεδονίας. Σχολή Κοινωνικών και Ανθρωπιστικών Επιστημών. Τμήμα Επικοινωνίας και Ψηφιακών Μέσων.).

Βάττη, Ι., & Παναγιώτου, Ά. (2019). Τεχνικές ανάλυσης δεδομένων για τη μελέτη της ψυχολογίας, του διαδικτυακού εκφοβισμού και του επιθετικού λόγου στις πλατφόρμες κοινωνικής δικτύωσης (Doctoral dissertation, Βάττη Ιωάννα, Παναγιώτου Άγγελος).

Βλαχοπούλου, Κ.(2007). Ηλεκτρονικό Έγκλημα: Μορφές – Πρόληψη – Αντιμετώπιση, Νομική Βιβλιοθήκη: Αθήνα

Γάκη, Α., & Αντωνίου, Α. Σ. (2014). Μορφές διαδικτυακής παρενόχλησης (διαδικτυακή αποπλάνηση και παιδική πορνογραφία): *προτάσεις αντιμετώπισης*. Πανελλήνιο Συνέδριο Επιστημών Εκπαίδευσης, 2014(2), 683-692.

Γάκης, Κ. (2021). Διερεύνηση φαινομένων σχολικού και διαδικτυακού εκφοβισμού, ψυχοκοινωνικής επάρκειας και στρατηγικών αντιμετώπισης αγχογόνων καταστάσεων μαθητών προεφηβικής και εφηβικής ηλικίας με και χωρίς ΔΕΠ/Υ (Doctoral dissertation, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ). Σχολή Επιστημών Αγωγής. Τμήμα Παιδαγωγικό Δημοτικής Εκπαίδευσης. Τομέας Ειδικής Παιδαγωγικής και Ψυχολογίας).

Δημόπουλος, Χ. (2006). Εγκλήματα της Γενετίσιας Εκμετάλλευσης Ανηλίκων. Αθήνα: Νομική Βιβλιοθήκη

Ζαννιάς, Α., & Τσιμπούκας, Δ. (2017). Κατανόηση του ηλεκτρονικού εγκλήματος και στρατηγικές πρόληψης και αντιμετώπισής του, σε εθνικό και προσωπικό επίπεδο.

Ζησιάδη Ι., Β. (2002). Η Οικονομική Εγκληματικότητα: *Το ουσιαστικό και δικονομικό οικονομικό ποινικό δίκαιο*, Εκδόσεις Σάκκουλα Α. Ε.: Αθήνα-Θεσσαλονίκη

Καραλή, Ε. (2019). Η διάσταση της Ισλαμικής τρομοκρατίας στο διαδίκτυο κανονιστικές και νέες μορφές προπαγάνδα.

Καρατση, Α., & Νικολάου, Α. (2022). Ηλεκτρονικό Έγκλημα *Μορφές, Τεχνολογίες, Αντίμετρα και Συνέπειες*

Καργόπουλος Α., (2018). Κυβερνοέγκλημα:Βασικές έννοιες και ζητήματα ουσιαστικού ποινικού δικαίου(διαθέσιμο στο http:www.esdi.gr>epimorfosi>kargopoulos)

Κελεγκουριάδη, Α. Α., & Μαλλιαρού, Α. Α. (2016). Διαδικτυακή παιδική πορνογραφία. *Η συμβολή των κοινωνικών λειτουργών στην πρόληψη και την ενημέρωση.*

Κοκτσίδου, Κ. Β. (2021). Η τρομοκρατία στον κυβερνοχώρο. Μελέτη περίπτωσης Isis (Doctoral dissertation, University of Piraeus (Greece)).

Λαζαροπούλου, Κ. Α., & Τσαγκρινός, Σ. Α. (2017). Ψηφιακές απειλές κατά των ανηλίκων και τρόποι αντιμετώπισης.

Λασηθιωτάκη, Φ. (2015). Ηλεκτρονικό έγκλημα.

Λυκούρεσης, Ι., & Φραντζέσκου, Π. (2021). Ηλεκτρονικό έγκλημα.

Μάλλιου, Ε., Λιγνού, Μ., Μαυρουδής, Χ., & Κατσανός, Κ. (2023). Γνώσεις και Αντιλήψεις Νέων σχετικά με τον Διαδικτυακό Εκφοβισμό. Open Schools Journal for Open Science, 6(2).

Μανωλοπούλου, Β., & Μητσιοπούλου, Γ. (2020). Σχολικός και Διαδικτυακός εκφοβισμός στην ύστερη εφηβική ηλικία.

Μπενέτου, Α. (2021). Το Ηλεκτρονικό Έγκλημα

Παλιάτσου, Θ. (2021). Υβριδικός πόλεμος και τρομοκρατία στο διαδίκτυο (Doctoral dissertation, University of Piraeus (Greece)).

Παναγιωτίδης, Π. Κ. (2011). Το έγκλημα στον κυβερνοχώρο: *μορφές, αντιμετώπιση και νομική προστασία* (Master's thesis).

Παπαγγελή, Α. (2015). Η δογματική φυσιογνωμία του διαδικτυακού ηλεκτρονικού εγκλήματος και η διεθνής διάσταση της κατασταλτικής εναρμόνισης.

Παπαθωμά, Α. Δ. (2017). Η αντιμετώπιση του φαινομένου του Διαδικτυακού Εκφοβισμού μέσα από το Μάθημα των Θρησκευτικών. Ζητήματα Διδακτικής των Θρησκευτικών, 1, 338-346.

Παπαϊωάννου, Κ. (2000). Παιδιά – Γονείς – Κοινωνικοί Λειτουργοί. Αθήνα: Ελλην στο Κελεγκουριάδη, Α. Α., & Μαλλιαρού, Α. Α. (2016). Διαδικτυακή παιδική πορνογραφία. Η συμβολή των κοινωνικών λειτουργών στην πρόληψη και την ενημέρωση.

Παπακυριάκου, Θ. (2005). Φορολογικό ποινικό δίκαιο: *Η ποινική προστασία των φορολογικών αξιώσεων του Ελληνικού Δημόσιου και της Ε.Ε. στην ελληνική έννομη τάξη*, Εκδόσεις Σάκκουλα Α. Ε.: Αθήνα-Θεσσαλονίκη

Ρουσσοπούλου, Θ. (2023). Παιδική Πορνογραφία.

Σαριδάκη, Ι. Δ. (2017). Ηλεκτρονικό έγκλημα και προσωπικά δεδομένα στην Ευρωπαϊκή Ένωση.

Σαρτέρη, Β. (2020). Ηλεκτρονικό έγκλημα.

Σταθοπούλου, Ι. Μ. (2022). Κυβερνοέγκλημα: απειλές και προκλήσεις για το μέλλον.

Τσάγκα, Δ. (2020). Ο ηλεκτρονικός εκφοβισμός μεταξύ των εφήβων Δυτικής Αττικής: *Η συχνότητα εμφάνισης του φαινομένου και τρόποι αντιμετώπισης.*

https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity, (13/06/213)

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise, (13/06/2023)

https://www.kathimerini.gr/economy/local/1052805/forodiafygi-meso-istoselidon-koinonikis-diktyosis-entopise-i-aade/(13/06/2023)