**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ:**
**«ΔΙΑΧΕΙΡΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΒΙΒΛΙΟΘΗΚΕΣ, ΑΡΧΕΙΑ, ΜΟΥΣΕΙΑ»**

**ΤΜΗΜΑ ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ**
**ΣΧΟΛΗ ΔΙΟΙΚΗΤΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**DEPARTMENT OF ARCHIVAL, LIBRARY AND INFORMATION STUDIES**
**SCHOOL OF MANAGEMENT, ECONOMICS AND SOCIAL SCIENCES**

**Διπλωματική Εργασία**

# Τίτλος Εργασίας

Το «ελεύθερο» διαδίκτυο ως πάροχος πληροφοριών, με έμφαση στην ενημέρωση για τους κινδύνους που ενέχει η χρήση του

**Κωτσάκη Αναστασία (ΑΜ:196682001)**

Επιβλέπων: Κωνσταντίνος Κυπριανός

Αθήνα, Ιανουάριος 2023

# Επιτροπή Εξέτασης

**1.** Κωνσταντίνος Κυπριανός

Konstantinos Kyprianos

Digitally signed by Konstantinos Kyprianos
Date: 2023.01.13 23:04:27 +02'00'

**2.** Δημήτριος Κουής

Dimitrios Kouis

Digitally signed by Dimitrios Kouis
Date: 2023.01.14 11:41:05 +02'00'

**3.** Φωτεινή Ευθυμίου

Foteini Efthymiou

Digitally signed by Foteini Efthymiou
Date: 2023.01.15 19:10:29 +02'00'

# ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη ΚΩΤΣΑΚΗ ΑΝΑΣΤΑΣΙΑ του ΕΥΣΤΑΘΙΟΥ, με αριθμό μητρώου 196682001 φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών «ΔΙΑΧΕΙΡΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ ΒΙΒΛΙΟΘΗΚΕΣ, ΑΡΧΕΙΑ, ΜΟΥΣΕΙΑ» του Τμήματος ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ της Σχολής ΔΙΟΙΚΗΤΙΚΩΝ, ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το Διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Η Δηλούσα

Αναστασία Κωτσάκη

# Ευχαριστίες – Αφιερώσεις

Θέλω αρχικά να ευχαριστήσω τους καθηγητές μου, Κωνσταντίνο Κυπριανό και Φωτεινή Ευθυμίου, για τη βοήθεια και καθοδήγηση που μου προσέφεραν καθ' όλη τη διάρκεια της συνεργασίας μας. Επίσης, ευχαριστώ πολύ την οικογένεια μου και συγκεκριμένα, τη μητέρα μου Παρασκευή Παπαδάτου, η οποία πάντα με στηρίζει και μου δίνει θάρρος να συνεχίσω, όταν όλα φαίνονται δύσκολα.

Τέλος, θα ήθελα να ευχαριστήσω τον σύζυγό μου Ανέστη Ανδρεάδη για τη βοήθεια, στήριξη και κατανόηση που έδειξε σε όλη τη διάρκεια των σπουδών μου. Τον ευχαριστώ κυρίως γιατί αποτέλεσε κίνητρο για συνεχή προβληματισμό και αναζήτηση.

6 Ιανουαρίου 2023

Αναστασία Κωτσάκη

# Περίληψη στα ελληνικά

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ενημέρωση του χρήστη για το «ελεύθερο» Διαδίκτυο με έμφαση στους κινδύνους που ενέχει η χρήση του. Το πλαίσιο μέσα στο οποίο εντάσσεται η εργασία είναι το ευρύτερο επιστημονικό πεδίο «Μέσα και Πληροφοριακή Παιδεία». Οι ειδικότεροι στόχοι της εργασίας αφορούν στα παρακάτω: ενδεικτική καταγραφή των ευρέως χρησιμοποιούμενων δωρεάν μηχανών αναζήτησης και διαδικτυακών πλατφορμών, εντοπισμός των βασικότερων κινδύνων που ενέχει η χρήση τους για τον τελικό χρήστη και συγκεκριμένα του διαδικτυακού εκφοβισμού, της εμπορευματοποίησης των προσωπικών δεδομένων και της απάτης της διαδικτυακής ταυτότητας. Επιπρόσθετα, διερευνώνται οι τρόποι αντιμετώπισης αυτών των κινδύνων όπως είναι η εφαρμογή κωδίκων δεοντολογικής συμπεριφοράς στο Διαδίκτυο και προτείνεται η ενημέρωση των χρηστών μέσω ενδεικτικών σεναρίων εκπαίδευσης.

Η μεθοδολογία που ακολουθήθηκε αφορά στα παρακάτω: εντοπισμός των ελεύθερων μηχανών αναζήτησης ιστού και ιστοσελίδων μέσα από την πλατφόρμα Similarweb, και καταγραφή των βασικών πληροφοριών για αυτές στην διαδικτυακή πλατφόρμα https://kotsakiana.omeka.net/. Στη συνέχεια γίνεται εκτεταμένη συστηματική βιβλιογραφική επισκόπηση για τον εντοπισμό των βιβλιογραφικών πηγών προκειμένου για την απάντηση στο καθένα από τα επιμέρους ερωτήματα που τέθηκαν. Αναλυτικότερα γίνεται διερεύνηση των συχνότερων κινδύνων του ελεύθερου Διαδικτύου, των χαρακτηριστικών τους, των επιπτώσεων και των τρόπων αντιμετώπισής τους. Τέλος, γίνεται σχεδιασμός ενδεικτικών σεναρίων εκπαίδευσης για το καθένα από τα τέσσερα επιμέρους θέματα.

Συνοπτικά, τα αποτελέσματα υπογραμμίζουν ότι οι πιο σημαντικοί κίνδυνοι του Διαδικτύου προκαλούν τεράστιες επιπτώσεις στους χρήστες, αρχικά υλικές – οικονομικές αλλά κυρίως ψυχολογικές, ενώ σημειώθηκε ότι η ενημέρωση και η εκπαίδευση για τα φαινόμενα αυτά είναι το πιο σημαντικό μέτρο προστασίας.

**Λέξεις Κλειδιά:** Ελεύθερες μηχανές αναζήτησης, Ελεύθερες πλατφόρμες Διαδικτύου, Διαδικτυακός εκφοβισμός, Εμπορευματοποίηση προσωπικών δεδομένων, Απάτη διαδικτυακής ταυτότητας, Κανόνες δεοντολογικής συμπεριφοράς στο Διαδίκτυο, Εκπαιδευτικά σενάρια.

# Περίληψη στα αγγλικά

The aim of this thesis is to inform the user about the "free" Internet with an emphasis on the risks involved in its use. The research is related to the field of "Media and Information Literacy". The specific objectives of the research concern the following: an indicative record of the widely used free search engines and online platforms, identification of the main risks that their use entails for the end user, specifically cyberbullying, commercialization of personal data and online fraud identity. In addition, the ways to deal with these risks are explored, such as the application of netiquette rules on the Internet, and it is proposed to inform users through indicative training scenarios.

The methodology followed concerns the following: identification of free web search engines and websites through the Similarweb platform and description of basic information about them on the online platform https://kotsakiana.omeka.net/. After this extensive systematic literature review takes place to identify bibliographic sources that answer each of the specific questions raised. In more detail the literature review concerns the most frequent dangers of the free Internet, their characteristics, their effects and ways of dealing with them. Finally, indicative training scenarios for each of the four specific topics have been designed.

To sum up, the results highlight that the most important risks of the Internet cause huge effects on users, initially material - financial but mainly psychological, while it was found that information and education about these phenomena is the most important protection measure.

**Keywords:** Free Search Engines, Free Internet Platforms, Cyberbullying, Commercialization of Personal Data, Online Identity Fraud, Netiquette rule, Educational Scenarios.

# Πίνακας περιεχομένων

# Πίνακας Σχημάτων

# Πίνακας Πινάκων

# Κεφάλαιο 1. Εισαγωγή

## 1.1 Πλαίσιο, σκοπός και στόχοι της διπλωματικής εργασίας

Το θέμα της παρούσας διπλωματικής εργασίας αφορά στο «ελεύθερο» Διαδίκτυο με έμφαση στους κινδύνους που ενέχει η χρήση του. Το πλαίσιο μέσα στο οποίο εντάσσεται η εργασία είναι το ευρύτερο επιστημονικό πεδίο «Μέσα και Πληροφοριακή Παιδεία».

Σύμφωνα με τον Zou'bi (2021) «Μέσα και Πληροφοριακή Παιδεία» είναι ένας όρος «που αναφέρεται στο «έργο ενδυνάμωσης» των χρηστών, λόγω του ότι στοχεύει στο να βοηθήσει τους χρήστες να κατανοήσουν την κουλτούρα των μέσων που τους περιβάλλουν, να επιλέγουν σωστά τις πληροφορίες αλλά και να τα αντιμετωπίζουν και να συμμετέχουν αποτελεσματικά σε αυτά». Στον όρο περιλαμβάνονται ικανότητες που παρέχουν τη δυνατότητα στους χρήστες :

- να ερευνούν και να έχουν αυξημένη κριτική ικανότητα, ώστε να προωθούν με προσοχή τις πληροφορίες και γενικά το περιεχόμενο όλων των μέσων καθώς και των μέσων ενημέρωσης, αναπτύσσοντας δεξιότητες κατανόησης των ατομικών δικαιωμάτων στο Διαδίκτυο
- να μπορούν να αναγνωρίζουν τις ψεύτικες πληροφορίες και ειδήσεις και να καταπολεμούν το διαδικτυακό εκφοβισμό
- να αντιλαμβάνονται τη σημαντικότητα της ύπαρξης πνευματικών δικαιωμάτων και τα ηθικά ζητήματα που προκύπτουν με τη χρήση και την πρόσβαση σε πληροφορίες
- να έχουν αντίληψη στο πώς να συμμετέχουν σε όλα τα μέσα, όπως τα μέσα ενημέρωσης και πώς να χρησιμοποιούν τις τεχνολογίες της πληροφορίας και της επικοινωνίας ως παραγωγοί πληροφοριών και περιεχομένου, μέσων για την προώθηση της ισότητας, της αυτό-έκφρασης, της πληθώρας μέσων ενημέρωσης, της πληροφόρησης και του διαπολιτισμικού, δια θρησκευτικού και ειρηνικού διαλόγου.

Επίσης είναι χρήσιμο να αναφερθεί η επεξήγηση του όρου από τους Livingstone et al. (2020) οι οποίοι αναφέρουν ότι ο όρος «Μέσα και Πληροφοριακή Παιδεία» περιλαμβάνει τις παρακάτω δεξιότητες :

- Λειτουργικές - δεξιότητες που αφορούν στην πρόσβαση, στην αποθήκευση, στην ανάκτηση και στη διαχείριση δεδομένων, στη χρήση γλώσσας προγραμματισμού, στην επίλυση τεχνικών προβλημάτων και στην αλλαγή των ρυθμίσεων απορρήτου

- Πληροφοριακές - δεξιότητες που αφορούν στην κατανόηση και στην άρθρωση των πληροφοριακών αναγκών, στην ανάλυση, στη σύγκριση, στην αξιολόγηση και στην εφαρμογή δεδομένων και περιεχομένου, στην περιήγηση, στην αναζήτηση και στο φιλτράρισμα δεδομένων και περιεχομένου και στον εντοπισμό κενών προσωπικών ικανοτήτων
- Κοινωνικές - δεξιότητες που σχετίζονται με την επικοινωνία και τη συνεργασία, τους κώδικες δεοντολογικής συμπεριφοράς στο Διαδίκτυο, τη συμμετοχή σε ομάδες, τη διατήρηση, τη διαχείριση και την αφαίρεση επαφών, την ιδιότητα του πολίτη, την οικειοποίηση της παρουσίασης ταυτότητας, τη γνώση του ποιες πληροφορίες αλλά και του πότε πρέπει να κοινοποιούν / να μην κοινοποιούν πληροφορίες
- Δημιουργικές - δεξιότητες που αφορούν στη δημιουργία, την επεξεργασία, τον σχεδιασμό, τη σύνθεση, την παρακολούθηση και την κοινή χρήση περιεχομένου με ηθικό τρόπο, στην κατανόηση των πνευματικών δικαιωμάτων, των αδειών και των κανονισμών των μέσων ενημέρωσης
- Δεξιότητες κινητής τηλεφωνίας - που αφορούν στον εντοπισμό αναγκών, την επίλυση προβλημάτων, την εγκατάσταση εφαρμογών, την παρακολούθηση του κόστους και την πραγματοποίηση αγοράς εντός εφαρμογής
- Ασφάλειας - δεξιότητες που αφορούν στην προστασία των συσκευών, των προσωπικών δεδομένων και της ιδιωτικής ζωής, της υγείας και της ευημερίας καθώς και του περιβάλλοντος

Σκοπός είναι να παρουσιαστούν ενδεικτικά οι ευρέως χρησιμοποιούμενες δωρεάν μηχανές αναζήτησης και πλατφόρμες και να αποτυπωθούν οι βασικές λειτουργίες τους καθώς και η αποστολή τους, ώστε σε πρώτο στάδιο να χαρτογραφηθεί το πεδίο του λεγόμενου «ελεύθερου» Διαδικτύου.

Εν συνεχεία, ειδικότεροι στόχοι είναι να εντοπιστούν οι βασικότεροι κίνδυνοι που ενέχει η χρήση του «ελεύθερου» Διαδικτύου για τον τελικό χρήστη, να καταγραφούν οι τρόποι αντιμετώπισής τους, όπως αυτοί προτείνονται από τη σχετική επιστημονική βιβλιογραφία και τέλος να προταθούν τα αντίστοιχα εκπαιδευτικά σενάρια που θα μπορούσε να υιοθετήσει τόσο ο επιστήμονας της πληροφόρησης όσο και ο εκπαιδευτικός ώστε να συμβάλλει στη σχετική ενημέρωση της όποιας κοινότητας εξυπηρετεί, όπως χρηστών βιβλιοθηκών, μαθητών και φοιτητών.

## 1.2 Ερευνητικά ερωτήματα

Τα ερευνητικά ερωτήματα που απαντώνται με την διπλωματική εργασία είναι :

1ο Ποιες είναι ενδεικτικά οι ευρέως διαδεδομένες ελεύθερες μηχανές αναζήτησης και οι ελεύθερες διαδικτυακές πλατφόρμες; Ποιοι είναι οι στόχοι, η αποστολή και οι λειτουργίες τους για τον τελικό χρήστη;

2ο Τι σημαίνει διαδικτυακός εκφοβισμός (cyberbullying), ποια είναι τα χαρακτηριστικά, οι συνέπειες που προκαλεί και ποιοι είναι οι τρόποι αντιμετώπισής του;

3ο Τι σημαίνει εμπορευματοποίηση των προσωπικών δεδομένων (commercialization of users' digital identity), πώς συμβαίνει και ποιοι είναι οι τρόποι αντιμετώπισης του φαινομένου;

4ο Τι σημαίνει απάτη της διαδικτυακής ταυτότητας (identity fraud), ποια είναι τα είδη απάτης που υπάρχουν, ποιες είναι οι συνέπειες που προκαλεί το φαινόμενο και ποιοι οι τρόποι αντιμετώπισής του;

5ο Ποιοι είναι οι κώδικες δεοντολογικής συμπεριφοράς στο Διαδίκτυο (Netiquette rules);

## 1.3 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε για την εκπόνηση της παρούσας διπλωματικής εργασίας περιλαμβάνει τα ακόλουθα στάδια:

Στάδιο 1ο : Εντοπισμός των ελεύθερων μηχανών αναζήτησης ιστού και ιστοσελίδων μέσα από την πλατφόρμα Website Traffic - Check and Analyze Any Website | Similarweb, και επιλογή των τριών πρώτων σε επισκεψιμότητα από κάθε κατηγορία, έτσι όπως τις έχει κατηγοριοποιήσει η συγκεκριμένη πλατφόρμα.

Στάδιο 2ο : Καταγραφή των πληροφοριών των διαδικτυακών πλατφορμών και ειδικότερα σύντομη περιγραφή, ιστορική αναδρομή, σκοποί και αποστολή στη διαδικτυακή πλατφόρμα https://kotsakiana.omeka.net/, στην οποία δημιουργήθηκαν δύο συλλογές, μία για τις ελεύθερες διαδικτυακές πλατφόρμες και μία για τις ελεύθερες μηχανές αναζήτησης.

Στάδιο 3ο : Εκτεταμένη συστηματική βιβλιογραφική επισκόπηση. Ειδικότερα, για τον εντοπισμό των βιβλιογραφικών πηγών, επιλέχθηκαν η βάση δεδομένων ScienceDirect.com | Science, health and medical journals, full text articles and books και η μηχανή αναζήτησης Μελετητής Google. Οι λέξεις κλειδιά που χρησιμοποιήθηκαν για την αναζήτηση των βιβλιογραφικών πηγών για τα τέσσερα ερωτήματα αναφορικά με τους πιθανούς κινδύνους που ενέχει η χρήση του Διαδικτύου είναι:

- “cyberbullying”
- “commodification of personal data” και “commercialization of data”
- “identity fraud”
- “netiquette rules”

Τα φίλτρα που χρησιμοποιήθηκαν κατά την αναζήτηση είναι η χρονική περίοδος δημοσίευσης, δηλαδή πηγές που δημοσιεύτηκαν από το έτος 2012 και έπειτα, των οποίων το πλήρες περιεχόμενο έπρεπε να είναι στην αγγλική γλώσσα και στην περίπτωση της Google Scholar, ελεύθερα προσβάσιμο.

Στάδιο 4ο : Διαχείριση των πηγών στο πρόγραμμα MS Excel. Για την απάντηση στο καθένα από τα επιμέρους ερωτήματα που τέθηκαν μελετήθηκαν συνολικά οι εβδομήντα **(70)** πιο σχετικές πηγές.

Στάδιο 5ο : Σχεδιασμός και παρουσίαση τεσσάρων εκπαιδευτικών σεναρίων για το καθένα από τα τέσσερα ερευνητικά ερωτήματα της διπλωματικής εργασίας.

## 1.4 Περιορισμοί

Οι περιορισμοί που προέκυψαν κατά την έρευνα είναι οι ακόλουθοι:

Ο αριθμός των ευρέως διαδεδομένων ελεύθερων μηχανών αναζήτησης και ελεύθερων διαδικτυακών πλατφορμών είναι τεράστιος και για το λόγο αυτό καταγράφηκαν ενδεικτικά οι τρεις (3) πιο «επισκέψιμες» από κάθε κατηγορία, οι οποίες φθάνουν τον συνολικό αριθμό εβδομήντα **(70).**

Η αναζήτηση με τον όρο «commodification of personal data» δεν έφερε ικανοποιητικό αριθμό αποτελεσμάτων και χρειάστηκε να γίνει αναζήτηση με δεύτερο όρο για τον συγκεκριμένο κίνδυνο, ο οποίος ήταν «commercialization of data».

Στο τέταρτο ερώτημα, για τους κανόνες δεοντολογικής συμπεριφοράς στο Διαδίκτυο, δεν βρέθηκε το σχετικά πλούσιο βιβλιογραφικό υλικό που υπήρξε για τα τρία προηγούμενα ερωτήματα. Για αυτό το λόγο επιλέχθηκαν και μελετήθηκαν μόνο δέκα πηγές.

# Κεφάλαιο 2. Θεωρητικό μέρος – Βιβλιογραφική έρευνα – Σχετικές προσπάθειες

Το παρόν κεφάλαιο αφορά στην αναλυτική παρουσίαση της υπάρχουσας βιβλιογραφίας γύρω από το θέμα της διπλωματικής εργασίας.

## 2.1 Θεωρητικό μέρος – Βιβλιογραφική έρευνα

## 2.2 Σχετικές προσπάθειες – έρευνες

Με τη συνεχή εξέλιξη της τεχνολογίας και των μέσων τεχνολογιών πληροφοριών και επικοινωνίας έχει αυξηθεί η χρήση του Διαδικτύου και των ηλεκτρονικών πλατφορμών από ανθρώπους ανεξαρτήτως ηλικίας για την κάλυψη καθημερινών αναγκών. Ειδικότεροι λόγοι για τους οποίους έχει αυξηθεί η χρήση τους είναι ψυχαγωγικοί, επαγγελματικοί και εκπαιδευτικοί.

Για το πρώτο ερευνητικό ερώτημα, αναφορικά με τους στόχους, την αποστολή και τις λειτουργίες που προσφέρουν στον τελικό χρήστη κάποιες από τις ευρέως διαδεδομένες ελεύθερες μηχανές αναζήτησης και ελεύθερες διαδικτυακές πλατφόρμες, ο αναγνώστης μπορεί να ανατρέξει στη διαδικτυακή πλατφόρμα https://kotsakiana.omeka.net/, η οποία αποτελεί αναπόσπαστο μέρος της παρούσας διπλωματικής εργασίας.

Παράλληλα όμως με τη συνεχόμενη ανάπτυξη και χρήση του Διαδικτύου έχουν αυξηθεί ανησυχητικά κάποια φαινόμενα όπως ο διαδικτυακός εκφοβισμός (cyberbulling), Giumetti & Kowalski (2022), η παραβίαση της ψηφιακής ιδιωτικότητας (digital identity breach), Sonker et al. (2020), και η εμπορευματοποίηση της ψηφιακής ταυτότητας των χρηστών, με σκοπό τη συγκέντρωση πληροφοριών για διαφήμιση (commercialization of users' digital identities). Επιπρόσθετα, έχουν αναπτυχθεί και διάφοροι κώδικες δεοντολογικής συμπεριφοράς στο Διαδίκτυο, οι οποίοι αν εφαρμόζονταν από την πλειοψηφία των χρηστών θα μπορούσαν να ενδυναμώσουν τις πολυάριθμες διαδικτυακές κοινότητες απέναντι στα παραπάνω φαινόμενα.

Το παρόν κεφάλαιο διερευνά αυτά τα τέσσερα θέματα μέσα από μία συστηματική επισκόπηση της τρέχουσας διεθνούς βιβλιογραφίας, επιχειρώντας να απαντήσει στα τέσσερα αντίστοιχα ερευνητικά ερωτήματα που τέθηκαν προηγουμένως.

### 2.2.1 Μηχανές αναζήτησης και διαδικτυακές πλατφόρμες

#### 2.2.1.1 Ορισμοί

Σύμφωνα με τους Gawer & Srnicek (2021), διαδικτυακή πλατφόρμα ορίζεται ως «μία σειρά από υπηρεσίες που είναι διαθέσιμες στο Διαδίκτυο, συμπεριλαμβανομένων αγορών, μηχανών αναζήτησης, κοινωνικών μέσων, καταστημάτων δημιουργικού περιεχομένου, καταστημάτων εφαρμογών, υπηρεσιών επικοινωνιών, συστημάτων πληρωμών και υπηρεσιών που περιλαμβάνουν τη λεγόμενη «συνεργατική» ή «sharing» ή «gig» οικονομία[1]». Παράλληλα, σύμφωνα με τον ορισμό της Ευρωπαϊκής Επιτροπής, οι «πλατφόρμες» ή «διαδικτυακές πλατφόρμες» ή «ψηφιακές πλατφόρμες», ορίζονται ως «οργανισμοί (ή εταιρείες) που προσφέρουν ψηφιακές υπηρεσίες, διευκολύνουν τις αλληλεπιδράσεις στο Διαδίκτυο μεταξύ δύο ή περισσότερων διακριτών, αλλά αλληλεξαρτώμενων συνόλων χρηστών (είτε οργανισμοί είτε άτομα), που δημιουργούν και εκμεταλλεύονται τα αποτελέσματα του δικτύου» (Gawer & Srnicek, 2021).

Παρότι υπάρχει μεγάλη ποικιλία διαδικτυακών πλατφορμών, οι περισσότερες πλατφόρμες χρησιμοποιούν κοινά χαρακτηριστικά στο σύνολό τους, "όπως οικονομικά, επιχειρηματικά και χαρακτηριστικά διακυβέρνησης για τη δημιουργία και τη διαμόρφωση αξίας" (Gawer & Srnicek, 2021).

Αρχικά, οι λειτουργίες και οι δυνατότητες που παρέχουν μπορεί να οδηγήσουν στη δημιουργία μονοπωλιακών θέσεων, αποκτώντας με αυτόν τον τρόπο οικονομική αξία. Από την άλλη, οι πλατφόρμες διαχειρίζονται την τεράστια παραγωγή, συλλογή και χρήση των δεδομένων μέσω νέων επιχειρηματικών μοντέλων, αποκτώντας επιχειρηματική αξία. Συμπληρωματικά, γίνεται προσπάθεια αύξησης της αποτελεσματικότητας του εμπορίου μέσω χαμηλότερου κόστους αναζήτησης, αναπαραγωγής και επαλήθευσης των δεδομένων και μέσω διευκόλυνσης στις ανταλλαγές / συναλλαγές των δεδομένων. Παράλληλα, γίνεται προσπάθεια δημιουργίας αξίας με την προώθηση της καινοτομίας, καθώς δίνεται η δυνατότητα στις ίδιες, αλλά και σε τρίτες εταιρείες, να δημιουργήσουν τεράστιες ποσότητες συμπληρωματικών προϊόντων και υπηρεσιών. Είναι γνωστό ότι οι πιο γνωστές εταιρείες όπως η Amazon, Google, Microsoft και Apple προσφέρουν τεράστια ποσά για έρευνα και

[1] Είναι "μία νέα μορφή εργασίας μέσω διαδικτυακών πλατφορμών, η οποία γίνεται online. Δεν υπάρχει ακριβής ορισμός στα ελληνικά. Ωστόσο, θα μπορούσε να αποδοθεί ως η «οικονομία της πλατφόρμας», καθώς αφορά τη ζήτηση και προσφορά εργασίας σε διαδικτυακές πλατφόρμες, όπου οι εργαζόμενοι δεν είναι ούτε μόνιμοι, ούτε μερικής απασχόλησης. Είναι επίσης γνωστή ως «platform economy» ή «crowdwork»" fortunegreece.com (2020).

καινοτομία, αποφέροντας σημαντικά οφέλη για τις ίδιες τις επιχειρήσεις, τους καταναλωτές και την κοινωνία Gawer & Srnicek, (2021).

Σύμφωνα με τη σελίδα nibusinessinfo.co.uk (n.d.), μηχανή αναζήτησης είναι «ένα συντονισμένο σύνολο προγραμμάτων που αναζητά και προσδιορίζει στοιχεία σε μία βάση δεδομένων που ταιριάζουν με καθορισμένα κριτήρια». Οι μηχανές αναζήτησης επιτρέπουν στους χρήστες να αναζητούν περιεχόμενο ή/και πληροφορίες στο Διαδίκτυο χρησιμοποιώντας λέξεις κλειδιά.

Ο τρόπος που λειτουργεί είναι : «ένας χρήστης εισάγει ένα ερώτημα σε μία μηχανή αναζήτησης μέσω των λέξεων κλειδιών, και επιστρέφεται μία σελίδα αποτελεσμάτων μηχανής αναζήτησης (SERP), ενώ πολλές φορές οι σελίδες που βρέθηκαν εμφανίζονται με τη σειρά της συνάφειάς τους. Ο τρόπος με τον οποίο γίνεται αυτή η κατάταξη διαφέρει από μηχανή σε μηχανή» (nibusinessinfo.co.uk n.d.) Οι περισσότερες μηχανές αναζήτησης έχουν τρία βασικά βήματα λειτουργίας. Αυτά είναι (nibusinessinfo.co.uk n.d.):

- “Ανίχνευση” - Αυτό αφορά τη συγκέντρωση δεδομένων από το Διαδίκτυο σε μία βάση, η οποία γίνεται μέσω συγκεκριμένων προγραμμάτων, που ονομάζονται spiders, bots ή crawlers, και σαρώνουν το Διαδίκτυο
- “Ευρετηρίαση” - Αυτό γίνεται μέσω της μηχανής αναζήτησης, “η οποία προσπαθεί να κατανοήσει και να κατηγοριοποιήσει το περιεχόμενο μίας ιστοσελίδας μέσω των «λέξεων-κλειδιών»” (nibusinessinfo.co.uk, n.d.)
- “Κατάταξη” - Η ταξινόμηση γίνεται με βάση διάφορους παράγοντες. Κάποιοι από αυτούς μπορεί να είναι η πυκνότητα των λέξεων-κλειδιών, η ταχύτητα και οι σύνδεσμοι. Στόχος της μηχανής αναζήτησης είναι να παρέχει στον χρήστη το πιο σχετικό αποτέλεσμα (nibusinessinfo.co.uk n.d.)

Οι πιο γνωστές μηχανές αναζήτησης όπως αναφέρονται και παρακάτω είναι η Google, η Yahoo, η Yandex, η Naver και το Bing της Microsoft.

#### 2.2.1.2 Σύντομη ιστορική αναδρομή

Αρχικά, η χρήση του Διαδικτύου ήταν αρκετά δύσκολη, καθώς αυτό αποτελούσε μία συλλογή αρχείων χωρίς ταξινόμηση, αχανής σε πληροφορίες και δεδομένα. Η πρώτη δημοφιλής μηχανή αναζήτησης στον Ιστό ήταν το Yahoo! και δημιουργήθηκε το 1994. Οι δημιουργοί της David Filo και Jerry Yang, αντιλήφθηκαν ότι για να χρησιμοποιηθεί πιο αποτελεσματικά το Διαδίκτυο χρειάζονταν να δημιουργήσουν έναν κατάλογο δεδομένων. Πιο συγκεκριμένα στον κατάλογο αυτόν, κατηγοριοποιούσαν χειροκίνητα, διάφορες σελίδες που εντόπιζαν, σε κατηγορίες και υπο- κατηγορίες. Με αυτόν τον τρόπο δημιουργήθηκε το Yahoo και επέτρεπε

στους χρήστες να περιηγηθούν στον κατάλογο για να βρίσκουν νέες πληροφορίες και να ενημερώνονται για νέες ιστοσελίδες (Wikipedia, 2023a).

Στη συνέχεια, εμφανίστηκαν μια σειρά από μηχανές αναζήτησης όπως Magellan, Excite, Infoseek, Inktomi, Northern Light και AltaVista. Το 1998 δημιουργήθηκε η μηχανή αναζήτησης Google από τους Larry Page και Sergey Brin. Η ιδέα πάνω στην οποία βασίστηκε ο κώδικας της ιστοσελίδας ήταν «ο καθορισμός της συνάφειας ενός ιστότοπου από τον αριθμό των σελίδων που αναφέρονται και τη σημασία αυτών των σελίδων που συνδέονταν πίσω στον αρχικό ιστότοπο» (Wikipedia, 2023b). Με λίγα λόγια ενώ οι συμβατικές μηχανές αναζήτησης κατατάσσουν τα αποτελέσματα μετρώντας πόσες φορές εμφανίστηκαν οι όροι αναζήτησης στη σελίδα, εκείνοι διατύπωσαν θεωρίες για ένα καλύτερο σύστημα που ανέλυε τις σχέσεις μεταξύ των ιστότοπων (Wikipedia, 2023b). Αυτός ο αλγόριθμος ονομάστηκε PageRank (Wikipedia, 2023b).

Με την πάροδο του χρόνου δημιουργήθηκαν ακόμα περισσότερες μηχανές αναζήτησης, όπως η Bing της Microsoft, η AOL, η Lycos, η AllTheWeb και άλλες. Ωστόσο, οι σημαντικότερες παραμένουν αυτές της Google, και της Yahoo, διότι από τις δικές τους βάσεις δεδομένων αντλούν τα αποτελέσματα οι περισσότερες μηχανές αναζήτησης.

#### 2.2.1.3 Κατηγοριοποίηση μηχανών αναζήτησης και διαδικτυακών πλατφορμών

Σύμφωνα με την ιστοσελίδα Similarweb.com (2023) από την οποία και αντλήθηκαν τα δεδομένα για τις ιστοσελίδες που περιλαμβάνονται στην παρούσα διπλωματική εργασία, οι κατηγορίες των ιστοσελίδων είναι οι παρακάτω :

1. Arts & Entertainment / Τέχνες και Ψυχαγωγία
2. Business and consumer services / Υπηρεσίες επιχειρήσεων και καταναλωτών
3. Community and society / Κοινότητα και κοινωνία
4. Computers Electronics and technology / Ηλεκτρονική και Τεχνολογία Υπολογιστών
5. eCommerce & shopping / Ηλεκτρονικό εμπόριο και αγορές
6. Finance / Χρηματοοικονομική
7. Food and drink / Φαγητό και ποτό
8. Gambling / Τυχερά παιχνίδια
9. Games / Παιχνίδια
10. Health / Υγεία
11. Heavy industry and engineering / Βαριά βιομηχανία και μηχανική
12. Hobbies and leisure / Χόμπι και ελεύθερος χρόνος
13. Home and garden / Σπίτι και κήπος
14. Jobs and career / Δουλειές και καριέρα
15. Law and government / Νόμος και κυβέρνηση
16. Lifestyle / Τρόπος ζωής
17. News and media / Ειδήσεις και Μέσα Μαζικής Ενημέρωσης
18. Pets and animals / Κατοικίδια και ζώα

19. Reference Materials / Υλικά αναφοράς
20. Science and education / Επιστήμη και εκπαίδευση
21. Sports / Αθλήματα
22. Travel and tourism / Ταξίδι και τουρισμός
23. Vehicles / Οχήματα
24. Adult / Ενήλικες

Στο σημείο αυτό κρίνεται απαραίτητο να γίνει μία σύντομη περιγραφή της ιστοσελίδας. Η σελίδα Similarweb ανήκει σε μία ισραηλινή εταιρεία ανάλυσης ιστοσελίδων που ειδικεύεται στην κίνηση στον ιστό και στην απόδοση των ιστοσελίδων. Διαθέτει εργαλεία που επιτρέπουν την ανάλυση επισκεψιμότητας και συμπεριφοράς των χρηστών σε ιστοτόπους και εφαρμογές. Η σελίδα κατατάσσει τους ιστοτόπους και τις εφαρμογές/ πλατφόρμες με βάση μετρήσεις επισκεψιμότητας και αφοσίωσης. Η κατάταξη υπολογίζεται με βάση τα δεδομένα που συλλέγονται από διαφορετικές πηγές, είτε από δεδομένα της ίδιας της εταιρείας και ενημερώνεται σε μηνιαία βάση. Τέλος, ταξινομεί τις πλατφόρμες σε κατηγορίες και υπο – κατηγορίες (Wikipedia, 2022).

### 2.2.2 Διαδικτυακός εκφοβισμός (Cyberbullying) - ορισμός

Το φαινόμενο του διαδικτυακού εκφοβισμού (cyberbullying) θεωρείται από πολλούς ως η προέκταση του παραδοσιακού εκφοβισμού (πρόσωπο με πρόσωπο), το οποίο εξελίχθηκε μεσώ των προηγμένων κοινωνικών δικτύων. Οι Notar et al. (2013) υποστηρίζουν ότι «σε αντίθεση με τον παραδοσιακό εκφοβισμό, στον οποίο οι επιδείξεις επιθετικότητας μπορεί να είναι εμφανείς στους παρευρισκόμενους, η διάπραξη διαδικτυακού εκφοβισμού συμβαίνει μέσω μη συμβατικών μέσων όπως ανταλλαγή μηνυμάτων, κειμένου, διαδικτυακών αρχείων καταγραφής ιστού ή κοινής χρήσης βίντεο». Μία ακόμα διαφορά, σύμφωνα με τους Watts et al. (2017) είναι ότι ο διαδικτυακός εκφοβισμός μπορεί να συμβεί 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα, από απόσταση, καθώς ο θύτης δε χρειάζεται να είναι στον ίδιο χώρο με το θύμα, όπως συνέβαινε με τον παραδοσιακό εκφοβισμό. Επιπλέον, το κοινό που παρακολουθεί το περιστατικό διαδικτυακού εκφοβισμού είναι πλέον μεγαλύτερο, διότι δεν περιορίζεται στο προαύλιο ενός σχολείου ή στα γραφεία εργασίας (Sabella et al., 2013).

Έπειτα από έρευνα στην πρόσφατη βιβλιογραφία έχουν συλλεχθεί αρκετοί ορισμοί του διαδικτυακού εκφοβισμού. Οι Watts et al. (2017) αναφέρουν ότι ο διαδικτυακός εκφοβισμός ορίζεται «ως η δημοσίευση σχολίων στο Διαδίκτυο με σκοπό τη δυσφήμιση ενός ατόμου, τη δημόσια αποκάλυψη ιδιωτικών γεγονότων του άλλου και την πρόκληση σκόπιμης συναισθηματικής δυσφορίας σε άλλο άτομο». Οι Patchin & Hinduja (2015) χρησιμοποίησαν τον ορισμό που αναφέρει ότι «διαδικτυακός εκφοβισμός είναι η μετάδοση οποιασδήποτε ηλεκτρονικής, οπτικής, γραπτής ή προφορικής επικοινωνίας με κακόβουλη και εσκεμμένη

πρόθεση, εξαναγκασμού, κακοποίησης, βασανισμού ή εκφοβισμού ενός ή περισσότερων ατόμων». Ωστόσο τα περισσότερα αποτελέσματα ορίζουν τον διαδικτυακό εκφοβισμό «ως εσκεμμένη, επιθετική ή εχθρική, επαναλαμβανόμενη πράξη που προκαλείται μέσω της χρήσης υπολογιστών, κινητών τηλεφώνων ή άλλων ηλεκτρονικών συσκευών, από ομάδα ή ένα άτομο, εναντίον θύματος που δεν μπορεί εύκολα να υπερασπιστεί τον εαυτό του» (Chan & Wong, 2020; Dadvar et al., 2013; Dou et al., 2020; Englander et al., 2017; Ifon, 2022; Niu et al., 2020; Patchin & Hinduja, 2015; Sabella et al., 2013; Slonje et al., 2013).

#### 2.2.2.1 Τα χαρακτηριστικά του διαδικτυακού εκφοβισμού

Μελετώντας τον ορισμό του διαδικτυακού εκφοβισμού μπορεί κάποιος εύκολα να εντοπίσει τα χαρακτηριστικά αυτού του φαινομένου, τα οποία είναι η επανάληψη, η πρόθεση για βλάβη και η ανισορροπία δύναμης (Patchin & Hinduja, 2015; Pennell et al., 2022; Sabella et al., 2013; Saleem et al., 2022; Wang & Ngai, 2022; Watts et al., 2017). Ενώ έχουν προστεθεί ακόμα δύο χαρακτηριστικά, αυτά της ανωνυμίας και της προσβασιμότητας (Saleem et al., 2022; Whittaker & Kowalski, 2014). Πιο συγκεκριμένα, η επανάληψη είναι ένα από τα βασικά χαρακτηριστικά για τον λόγο του ότι το διαδικτυακό περιεχόμενο μπορεί να «γίνει viral» πιο εύκολα από το περιεχόμενο εκτός σύνδεσης και μία ανάρτηση μπορεί να γίνει ορατή και κοινοποιήσιμη από μεγαλύτερο μέρος χρηστών. Έτσι αυτή η πράξη επαναλαμβάνεται ελεύθερα από μεγάλο μέρος του συνόλου (Patchin & Hinduja, 2015; Saleem et al., 2022; Watts et al., 2017).

Η πρόθεση για βλάβη είναι το δεύτερο χαρακτηριστικό, δηλαδή η πράξη εκφοβισμού γίνεται με σκοπό την πρόκληση βλάβης, ενόχλησης, απειλής, δυσφήμισης και σκόπιμης συναισθηματικής δυσφορίας (Niu et al., 2020; Patchin & Hinduja, 2015; Watts et al., 2017). Ένα ακόμα χαρακτηριστικό είναι η ανισορροπία δύναμης, η οποία στον διαδικτυακό εκφοβισμό δεν έχει να κάνει με τη σωματική δύναμη, αλλά με την τεχνολογική εξειδίκευση και την κοινωνική, οικονομική δύναμη (Wang & Ngai, 2022; Whittaker & Kowalski, 2014). Συγκεκριμένα, τα άτομα που έχουν εξοικείωση με περισσότερα τεχνολογικά μέσα έχουν περισσότερες ευκαιρίες και γνώσεις σχετικές με το Διαδίκτυο, με αποτέλεσμα να γνωρίζουν περισσότερους τρόπους για να διαπράξουν διαδικτυακό εκφοβισμό. Ομοίως, τα άτομα με υψηλότερη κοινωνική θέση και οικονομική ευχέρεια έχουν πρόσβαση σε περισσότερα τεχνολογικά αγαθά για να διαπράξουν εκφοβισμό (Wang & Ngai, 2022; Whittaker & Kowalski, 2014). Το χαρακτηριστικό της ανωνυμίας, το οποίο προστέθηκε με τη πάροδο του χρόνου, είναι και το πιο βασικό (Notar et al., 2013; Niu et al., 2020; Sabella et al., 2013; Saleem et al., 2022; Watts et al., 2017). Αναλυτικότερα, οι Sabella et al. (2013) υποστηρίζουν ότι οι περισσότεροι διαδικτυακοί χρήστες που προβαίνουν σε ενέργειες εκφοβισμού, κρύβονται

πίσω από το «μανδύα ανωνυμίας» και πράττουν χωρίς να ανησυχούν για το αν θα γίνουν αντιληπτοί από τις αρχές. Ταυτόχρονα οι Notar et al. (2013) και Watts et al. (2017) συμπληρώνουν ότι η ανωνυμία προσφέρει μία ασφάλεια και σιγουριά στους θύτες και αυτό κατ' επέκταση τους επιτρέπει να δρουν χωρίς φόβο και ανησυχία για την αποκάλυψή της ταυτότητας τους, με αποτέλεσμα να μειώνεται οποιαδήποτε αναστολή ή ηθικοί φραγμοί που μπορεί να έχουν. Ενώ η χρήση ψευδώνυμων και η δυνατότητα δημιουργίας ψεύτικων προφίλ ηλεκτρονικού ταχυδρομείου, καθιστά πολύ δύσκολο στα θύματα, αλλά και στις αρχές να εντοπίσουν τους δράστες και να τους σταματήσουν. Επιπλέον, η ανωνυμία είναι υπεύθυνη ώστε να ενεργούν οι δράστες ακόμα πιο σκληρά, διότι χωρίς πλέον να τους βασανίζουν ηθικοί φραγμοί και λόγω του ότι δεν έρχονται σε άμεση επαφή με τα θύματα, δεν συνειδητοποιούν την έκταση των πράξεων τους και τη σοβαρότητα της κατάστασης.

Τέλος, ένα ακόμα χαρακτηριστικό είναι η προσβασιμότητα. Πιο συγκεκριμένα, εξαιτίας της εξέλιξης των μέσων επικοινωνίας οι χρήστες του Διαδικτύου χαλαρώνουν και μοιράζονται πιο εύκολα ιδέες, συναισθήματα, σκέψεις και γενικά ιδιωτικές λεπτομέρειες στους κυβερνοχώρους, καθιστώντας με αυτόν τον τρόπο τους εαυτούς τους πιθανά θύματα (Saleem et al., 2022). Παράλληλα, η πρόσβαση στα περισσότερα κοινωνικά δίκτυα είναι ελεύθερη και η χρήση αυτών αρκετά εύκολη, με αποτέλεσμα οι θύτες διαδικτυακού εκφοβισμού να έχουν πρόσβαση στις ιδιωτικές πληροφορίες των άλλων και να μπορούν να τις χρησιμοποιούν όπως επιθυμούν, δηλαδή ή να τις κοινοποιούν ή να τις παραποιούν χωρίς να νοιάζονται για τις συνέπειες.

#### 2.2.2.2 Διαδικτυακός εκφοβισμός και φύλο

Στη βιβλιογραφία γίνονται αρκετές αναφορές στο διαδικτυακό εκφοβισμό σε σχέση με το φύλο, χωρίς ωστόσο να καταλήγει κάποιος ερευνητής, στο ποιο από τα δύο φύλα είναι το επικρατέστερο στο να διαπράξει διαδικτυακό εκφοβισμό. Ωστόσο, σύμφωνα με τους Notar et al. (2013) τα κορίτσια είναι πιο πιθανό να διαδώσουν φήμες για άλλους, ενώ τα αγόρια είναι πιο πιθανό να δημοσιεύσουν προσβλητικές φωτογραφίες και βίντεο. Ακόμα, οι άντρες είναι περισσότερο πιθανό να απειλήσουν για σωματικές βλάβες και να είναι υπεύθυνοι για επιθετικά περιστατικά, ενώ οι γυναίκες είναι πιθανό να εμπλέκονται σε εμπειρίες διαδικτυακού εκφοβισμού που περιλαμβάνουν ψυχολογικό μαρτύριο. Από αυτό γίνεται αντιληπτό ότι και τα δυο φύλα είναι εξίσου πιθανό να διαπράξουν διαδικτυακό εκφοβισμό, χωρίς να υπάρχουν κάποια συνεπή αποτελέσματα που να καταδεικνύουν ότι το ένα φύλο επικρατεί του άλλου.

#### 2.2.2.3 Τα είδη του διαδικτυακού εκφοβισμού

Τα είδη του διαδικτυακού εκφοβισμού είναι (Chan & Wong, 2020; Notar et al., 2013; Watts et al., 2017) :

- η μεταμφίεσή/ πλαστοπροσωπία (Masquerading/Impersonation)
- η επιθετική γλώσσα (Flaming)[2]
- ο αποκλεισμός (Exclusion/Gossip Groups)
- η δυσφήμιση (denigration)
- η παραπλάνηση/έκθεση (trickery and outing)
- η κυβερνο-παρενόχληση (cyberharassment) και
- η καταδίωξη (cyberstalking)

Αναλυτικότερα, η μεταμφίεση συμβαίνει όταν ο διαδικτυακός θύτης παριστάνει ότι είναι κάποιος άλλος και δημοσιεύει ή στέλνει απειλητικές ή επιβλαβείς πληροφορίες για ένα ή πολλά άτομα (Watts et al., 2017). Η επιθετική γλώσσα (flaming) είναι η αποστολή είτε ιδιωτικά είτε σε κάποια διαδικτυακή ομάδα, αγενών ή χυδαίων ή οργισμένων μηνυμάτων ή email, σχετικά με ένα ή πολλά άτομα (Notar et al., 2013; Watts et al., 2017). Ο αποκλεισμός είναι η σκόπιμη απαγόρευση συμμετοχής του θύματος σε μία διαδικτυακή συνομιλία ή ομάδα (Chan & Wong, 2020; Watts et al., 2017). Η δυσφήμιση συμβαίνει όταν ο θύτης αναρτά προσωπικά στοιχεία του θύματος τα οποία είναι αναληθή ή απλώς φήμες ή προσβλητικές φωτογραφίες (Chan & Wong, 2020; Watts et al., 2017). Η παραπλάνηση / έκθεση γίνεται όταν ο θύτης παραπλανά το θύμα ώστε να παρέχει ιδιωτικές ή ευαίσθητες πληροφορίες για τον εαυτό του, τις οποίες στη συνέχεια δημοσιεύει ή στέλνει για τις δουν και άλλοι. Η κυβερνό - παρενόχληση είναι η επανειλημμένη αποστολή προσβλητικών μηνυμάτων. Τέλος, η καταδίωξη στον κυβερνοχώρο (cyber stalking) συμβαίνει όταν αυτά τα προσβλητικά μηνύματα γίνονται απειλητικά και επαναλαμβανόμενα (Watts et al., 2017).

#### 2.2.2.4 Διαδικτυακός εκφοβισμός και ρόλοι

Ο Ifon (2022) υποστηρίζει ότι ο οποιοσδήποτε θα μπορούσε να είναι πιθανός στόχος διαδικτυακού εκφοβισμού ανεξάρτητα από το φύλο, την κοινωνική τάξη, τις πεποιθήσεις, το σεξουαλικό προσανατολισμό, το εκπαιδευτικό επίπεδο και τη θέση (θύμα, θύτης, παρευρισκόμενοι). Ωστόσο υπάρχουν έξι (6) διαφορετικοί ρόλοι που σχετίζονται με το

2 Στη γλώσσα του Διαδικτύου, η επιθετική γλώσσα (flaming (φλόγα)) είναι μία ανάρτηση σε μία ομάδα συζητήσεων, σε μία λίστα αλληλογραφίας ή σε παρόμοιο φόρουμ που επιτίθεται σε άλλο άτομο ή ομάδα ανθρώπων, συνήθως ως απάντηση σε μία προηγούμενη δημοσίευση (What is a flame? (iu.edu), 2022).

διαδικτυακό εκφοβισμό (Notar et al., 2013). Πέρα από τους προφανείς, οι οποίοι είναι ο ρόλος του θύματος (άτομο που εκφοβίζεται) και του θύτη (άτομο που εκφοβίζει), ένας ακόμα ρόλος είναι αυτός του περαστικού, ο οποίος χωρίζεται σε δυο υποκατηγορίες. Η πρώτη υποκατηγορία είναι ο ρόλος του παρατηρητή – υποστηρικτή του εκφοβισμού, δηλαδή αυτού που παρακολουθεί τον εκφοβισμό και ή μένει αμέτοχος ή ενθαρρύνει την πράξη. Και η δεύτερη υποκατηγορία, είναι αυτή του παρατηρητή – προστάτη, ο οποίος είναι αυτός που συμπαραστέκεται στο θύμα, βρίσκει λύση στο πρόβλημα, συνήθως ενημερώνει τις αρχές και γενικότερα προσπαθεί να σταματήσει την πράξη. Ωστόσο υπάρχουν δυο ακόμα ρόλοι. Ο ένας είναι ο ρόλος του εκδικητή, άτομα δηλαδή που έχουν υποστεί στο παρελθόν εκφοβισμό ή διαδικτυακό εκφοβισμό και χρησιμοποιούν το Διαδίκτυο για εκδίκηση, και ο τελευταίος είναι ο ρόλος των θυμάτων εκδικητών, οι οποίοι είναι άτομα που στο παρελθόν έχουν εκφοβίσει άλλους και τώρα δέχονται εκείνα τον εκφοβισμό (Notar et al., 2013).

Συμπληρώνοντας την παραπάνω αναφορά, οι Chan & Wong (2020) εντόπισαν στη μελέτη τους ότι τα θύματα και οι δράστες έχουν πολλά κοινά σημεία, όπως για παράδειγμα εμπειρία σε εγκληματικά γεγονότα, και τελικά δεν είναι δυο ξεχωριστές ομάδες ατόμων. Τα περισσότερα θύματα που έχουν δεχτεί διαδικτυακό ή παραδοσιακό εκφοβισμό μπορεί να είναι τα ίδια παραβάτες και το αντίστροφο, δημιουργώντας έτσι ένα φαύλο κύκλο διαδικτυακού εκφοβισμού.

#### 2.2.2.5 Διαδικτυακός εκφοβισμός και επιπτώσεις

Οι συνέπειες του διαδικτυακού εκφοβισμού σύμφωνα με την βιβλιογραφία, είναι αρκετά σοβαρές και όλες επηρεάζουν τη ψυχική υγεία οποιουδήποτε συμμετέχει στον εκφοβισμό είτε είναι ο θύτης, το θύμα ή ο παρατηρητής. Αναλυτικότερα, οι εμπλεκόμενοι και ιδιαίτερα τα θύματα παρουσιάζουν κοινωνικά, συμπεριφορικά και συναισθηματικά/ψυχολογικά προβλήματα, με κύρια συμπτώματα αυτά της κατάθλιψης, του κοινωνικού άγχους, της χαμηλής αυτοεκτίμησης και της χαμηλής αυτοπεποίθησης (Chan & Wong, 2020; Chillemi et al., 2020; Dou et al., 2020; Englander et al., 2017; Lee et al., 2021; Niu et al., 2020; Pennell et al., 2022; Sabella et al., 2013; Saleem et al., 2022; Watts et al., 2017) . Ενώ οι Sabella et al. (2013) αναφέρουν ότι «από μόνος του ο διαδικτυακός εκφοβισμός δεν μπορεί να οδηγήσει στην αυτοκτονία, ωστόσο επιδεινώνει την αστάθεια και την απελπισία στο μυαλό των θυμάτων που ήδη παλεύουν με αγχωτικές συνθήκες ζωής» και έχει σαν αποτέλεσμα την πρόκληση περιστατικών αυτοτραυματισμού και τη δημιουργία έντονων αυτοκτονικών σκέψεων. Σε αυτό το συμπέρασμα καταλήγουν αρκετοί ακόμη μελετητές (Chan & Wong, 2020; Chillemi et al., 2020; Englander et al., 2017; Saleem et al., 2022; Watts et al., 2017) ενισχύοντας την άποψη ότι άλλη μία συνέπεια του διαδικτυακού εκφοβισμού είναι ότι πολλά

θύματα, πέρα από την κατάθλιψη και τις αυτοκτονικές τάσεις, καταφεύγουν στη χρήση ουσιών και αλκοόλ για να μπορέσουν να διαχειριστούν το κοινωνικό άγχος και τα συναισθήματα κοινωνικής πίεσης που νιώθουν.

Κάποιες ακόμη συνέπειες που έχουν σημειωθεί είναι :

- τα συναισθήματα θυμού που νιώθουν τα θύματα, τα οποία στη συνέχεια τους οδηγούν στο να γίνουν οι ίδιοι διαδικτυακοί εκφοβιστές και να εκδικηθούν τους θύτες (Watts et al., 2017)
- το αίσθημα του φόβου για την ασφάλειά τους, το οποίο οδηγεί πολλούς στο να μετακομίσουν ή να διακόψουν διαπροσωπικές σχέσεις λόγω του ότι δεν μπορούν να διαχειριστούν την πίεση και το στρες, ή τους είναι δύσκολο να εμπιστευτούν ξανά κάποιον (Watts et al., 2017)
- και το αίσθημα της ντροπής, το οποίο τους οδηγεί στον κοινωνικό αποκλεισμό, καθώς ντρέπονται να μοιραστούν αυτό που βιώνουν, να αναζητήσουν βοήθεια και απλά καταλήγουν να αποδέχονται την κατάσταση αδυνατώντας να τη διαχειριστούν (Niu et al., 2020)

Επιπρόσθετα, οι Watts et al. (2017) αναφέρουν, στη μελέτη τους, ότι ο εκφοβισμός στο χώρο εργασίας οδηγεί σε αυξημένα επίπεδα κατάθλιψης, απουσίας και τελικά στην εναλλαγή εργαζομένων.

Όλα αυτά υποδηλώνουν ότι ο διαδικτυακός εκφοβισμός είναι αρκετά επιζήμιος για όσους εμπλέκονται. Αφενός είναι περισσότερο τραυματικός για τους νεότερους, οι οποίοι είναι πιο ευαίσθητοι και δεν έχουν τα κατάλληλα μέσα να διαχειριστούν κάποιες καταστάσεις, αφετέρου είναι αρκετά σκληρός και για τους μεγαλύτερους, ειδικότερα για εκείνους που έχουν περάσει ξανά στο παρελθόν κάποιο παρόμοιο περιστατικό και διατρέχουν μεγάλο κίνδυνο να κλονιστεί ξανά η ευαίσθητη ψυχική τους υγεία (Chillemi et al., 2020).

#### 2.2.2.6 Λόγοι διάπραξης διαδικτυακού εκφοβισμού

Οι λόγοι που κάποιος διαπράττει διαδικτυακό εκφοβισμό σύμφωνα με τους Watts et al. (2017) είναι λόγοι διασκέδασης, λόγοι εκδίκησης και λόγοι κακών διαπροσωπικών σχέσεων. Αρχικά οι Sabella et al. (2013) υποστηρίζουν ότι πολλοί δράστες θεωρούνται ακούσιοι θύτες, διότι πιστεύουν ότι αυτό που κάνουν είναι αστείο ή καλοπροαίρετο πείραγμα και απλώς διασκεδάζουν χωρίς να σημαίνει τίποτα η πράξη τους. Ενισχύοντας αυτή τη θεωρία οι Watts et al. (2017) κάνουν αναφορά στο «τρολλάρισμα» το οποίο θεωρείται από τους διαδικτυακούς θύτες ως ένα είδος ψυχαγωγίας. «Τρολλάρισμα» είναι το πείραγμα ή το

αστείο το οποίο γίνεται από θύτες με σκοπό να περιπαίξουν τα θύματα, και το κάνουν για λόγους ψυχαγωγίας και όχι για λόγους εκφοβισμού ή απειλής.

Οι κακές διαπροσωπικές σχέσεις και τα αρνητικά συναισθήματα που έχουν οι δράστες για τον εαυτό τους είναι ένας ακόμα λόγος διάπραξης εκφοβισμού. Αναλυτικότερα οι Watts et al. (2017) αναφέρουν ότι οι «εκφοβιστές» είναι άτομα που χρειάζονται βοήθεια και έχουν ανάγκη για συναισθηματική υποστήριξη. Επίσης ο Ifon (2022) υποστηρίζει ότι οι διαδικτυακοί «εκφοβιστές» είναι άτομα με αποτυχημένες ταυτότητες, τα οποία απέτυχαν να αναλάβουν τις ευθύνες τους, και να εντοπίσουν το πραγματικό τους πρόβλημα, αλλά προτίμησαν να καταφύγουν σε παράνομες δραστηριότητες για να καλύψουν το κενό της αγάπης, της αυτοεκτίμησης και την ανάγκη που είχαν στο να ανήκουν σε μία ομάδα. Στη μελέτη τους οι Watts et al. (2017) συμπληρώνουν ότι οι κακές διαπροσωπικές σχέσεις και οι αρνητικές αλληλεπιδράσεις με τον περίγυρο οδηγούν σε αύξηση των περιπτώσεων διαδικτυακού εκφοβισμού. Ενώ, οι Chan & Wong (2020) προσθέτουν ότι άτομα με χαμηλή κοινωνική συμπεριφορά, χαμηλούς οικογενειακούς δεσμούς και αρνητικές εμπειρίες διατρέχουν γενικό κίνδυνο τόσο στο να διαπράξουν όσο και στο να γίνουν θύματα διαδικτυακού εκφοβισμού.

Τέλος, ένας ακόμα λόγος για να διαπράξει κάποιος αυτό το φαινόμενο είναι η εκδίκηση, όπως αναφέρθηκε και παραπάνω. Πιο συγκεκριμένα, οι Sabella et al. (2013) αναφέρουν ότι αρκετοί δράστες, διαπράττουν διαδικτυακό εκφοβισμό παρορμητικά και έχουν ως στόχο να εκδικηθούν και να επιστρέψουν την πράξη του εκφοβισμού, νομίζοντας ότι με αυτόν τον τρόπο αποδίδουν δικαιοσύνη.

#### 2.2.2.7 Μέσα και παραδείγματα διάπραξης διαδικτυακού εκφοβισμού

Οι ερευνητές (Notar et al., 2013; Whittaker & Kowalski, 2014) αναφέρουν ότι οι πιο συνηθισμένοι ιστότοποι όπου σημειώνεται ο διαδικτυακός εκφοβισμός είναι το ηλεκτρονικό ταχυδρομείο (email) (21%), τα διαδικτυακά δωμάτια συνομιλίας (chat rooms) (20%), οι ιστότοποι κοινωνικής δικτύωσης (20%) και τα κινητά τηλέφωνα (19%). Ενώ σημειώνονται περιστατικά ακόμη και σε σελίδες γενικού περιεχομένου (20%). Τα κινητά τηλέφωνα είναι το κύριο τεχνολογικό μέσο που χρησιμοποιείται από όλους στις μέρες μας, και είναι το πιο εύκολα προσβάσιμο μέσο για εκφοβιστικές συμπεριφορές, καθώς μέσω αυτού μπορεί κανείς να στείλει γραπτά μηνύματα, να κάνει ανώνυμες κλήσεις, να στείλει φωνητικά μηνύματα και γενικότερα να έχει πρόσβαση στο Διαδίκτυο και σε αρκετές, αν όχι, σε όλες τις πλατφόρμες κοινωνικής δικτύωσης (Notar et al., 2013). Ακόμα το Facebook, το Twitter και το YouTube φαίνεται να κερδίζουν με διαφορά τους άλλους ιστότοπους κοινωνικής δικτύωσης σε

ποσοστά διάπραξης διαδικτυακού εκφοβισμού, καθώς είναι πολύ εύκολο να για πολλούς να παρακολουθούν και να συμμετέχουν μαζικά σε επιθέσεις (Watts et al., 2017).

Κάποια παραδείγματα διαδικτυακού εκφοβισμού είναι όταν (Patchin & Hinduja, 2015):

- Κάποιος δημοσιεύει άσχημα ή προσβλητικά σχόλια για ένα άτομο στο Διαδίκτυο. «Για παράδειγμα στις ΗΠΑ, ένα αγόρι μετά από ένα καυγά που είχε με ένα κορίτσι, προκειμένου να το εκδικηθεί επικόλλησε το πρόσωπο της, σε μία πορνογραφική φωτογραφία και τη διαμοίρασε σε ολόκληρη τη λίστα με τα email του (Li, 2006)»
- Κάποιος δημοσιεύει μία κακή ή προσβλητική φωτογραφία ή βίντεο για ένα άτομο στο Διαδίκτυο. «Για παράδειγμα στην έρευνα του Li (2006) γίνεται αναφορά σε ένα περιστατικό που συνέβη στο Καναδά. Πιο συγκεκριμένα ένα δεκαπεντάχρονο αγόρι βίωσε το διαδικτυακό εκφοβισμό, όταν κάποιοι συμμαθητές του ανέβασαν χωρίς τη θέλησή του ένα βίντεο που τον έδειχνε να αναπαριστά μία σκηνή από την ταινία Star Wars. Εκατομμύρια χρήστες κατέβασαν το βίντεο, το οποίο έγινε αμέσως viral και όλο αυτό του προκάλεσε αρνητικά συναισθήματα, που τον οδήγησαν στο κοινωνικό αποκλεισμό. Παράλληλα, περίπου το ίδιο περιστατικό καταγράφηκε και στην Ιαπωνία, όταν κάποια παιδιά τράβηξαν φωτογραφίες ενός υπέρβαρου αγοριού, ενώ αυτό ήταν στα αποδυτήρια και τις διαμοίρασαν σε τρίτους»
- Κάποιος δημιουργεί μία κακόβουλη ή προσβλητική σελίδα για ένα άτομο στο Διαδίκτυο. «Για παράδειγμα ο Li (2006) αναφέρει ότι στο Κάνσας των ΗΠΑ, μία κοπέλα μέσης εκπαίδευσης, όταν χώρισε με το αγόρι της, για να το εκδικηθεί, δημιούργησε μία σελίδα στην οποία διέδιδε ψευδείς φήμες και απειλητικά σχόλια για αυτό»
- Κάποιος διαδίδει φήμες για ένα άτομο στο Διαδίκτυο. «Για παράδειγμα, στην Καλιφόρνια, στο γυμνάσιο Calabasas δημιουργήθηκε ένας ιστότοπος, ο schoolscandals.com, στον οποίο ανέβαιναν μοχθηρά κουτσομπολιά και ρατσιστικά σχόλια, που αφορούσαν τόσο σε μαθητές όσο και σε εκπαιδευτικούς, όπως ακόμη και τον διευθυντή του γυμνασίου (Li, 2006)»
- Κάποιος παρενοχλεί σεξουαλικά ένα άλλο άτομο με το να στέλνει άσεμνες φωτογραφίες και βίντεο. «Για παράδειγμα, ο Li (2006) αναφέρει ότι στην Αυστραλία μία εννιάχρονη μαθήτρια έλαβε πορνογραφικά μηνύματα στο ηλεκτρονικό της ταχυδρομείο, και ενώ αρχικά όλοι υπέθεσαν ότι ο αποστολέας των μηνυμάτων ήταν κάποιος ενήλικας, η τοπική αστυνομία έπειτα από έρευνα εντόπισε ότι ο δράστης ήταν ένας συμμαθητής της».

Τέλος, κάποια επιπλέον παραδείγματα διαδικτυακού εκφοβισμού, σύμφωνα με τους Patchin & Hinduja (2015), είναι όταν :

- Κάποιος απειλεί ότι θα κοινοποιήσει διαδικτυακά σε τρίτους προσωπικές λεπτομέρειες για ένα άτομο
- Κάποιος υποδύεται ότι είναι ένας άλλος στο Διαδίκτυο και ενεργεί με σκοπό να βλάψει αυτόν τον οποίο υποδύεται
- Κάποιος απαγορεύει την είσοδο σε ομαδική διαδικτυακή ομάδα
- Κάποιος απαγορεύει την είσοδο σε άλλο άτομο σε διαδικτυακά παιχνίδια ή του επιτίθεται επανειλημμένα, στοχοποιώντας τον και αφαιρώντας του το δικαίωμα να διασκεδάσει

### 2.2.3 Εμπορευματοποίηση της ψηφιακής ταυτότητας χρηστών (Commercialization of users' digital identity)

Η εμπορευματοποίηση των ψηφιακών ταυτοτήτων είναι μία νέα πραγματικότητα στην οικονομία που βασίζεται στα προσωπικά δεδομένα και έχει αυξηθεί τρομερά τα τελευταία χρόνια (Malgieri & Custers, 2018). Τα προσωπικά δεδομένα χρησιμοποιούνται ως εμπορεύματα, καθώς θεωρούνται πολύτιμα περιουσιακά στοιχεία, τα οποία είναι απαραίτητα για οικονομικούς και κοινωνικούς σκοπούς (Bottis & Bouchagiar, 2018). Όλο και περισσότερες εταιρείες σήμερα με μικρό ή και καθόλου κόστος μπορούν να δημιουργήσουν υποδομές για τη συλλογή και την αποθήκευση των δεδομένων. Οι εταιρείες αυτές «συλλέγουν, επεξεργάζονται τα δεδομένα μαζικά, τα οργανώνουν, τα τροποποιούν, τα συνδυάζουν, έτσι ώστε να δημιουργηθούν νέα δεδομένα, τα οποία στη συνέχεια θα πουλήσουν ή θα ανταλλάξουν με σκοπό την απολαβή κέρδους» (Bottis & Bouchagiar, 2018). Αυτή η κατάσταση δημιουργεί ηθικά και νομικά ζητήματα σχετικά με την κατάλληλη προστασία των ατόμων και των δεδομένων τους (Tronnier et al., 2022). Η κοινωνία έχει μετατραπεί σε ένα περιβάλλον καθόλου φιλικό ως προς την διαφύλαξη της ιδιωτικής ζωής (Bottis & Bouchagiar, 2018) διότι τα προσωπικά δεδομένα συνδέονται στενά με το απόρρητο ενός υποκειμένου δεδομένων (Malgieri & Custers, 2018). Η εμπορευματοποίηση της ιδιωτικής ζωής θεωρείται ανεπιθύμητη διαδικασία και για αυτό είναι απαραίτητο να χαραχθεί μία κοινή πολιτική σε όλο τον κόσμο ώστε να ρυθμιστεί αυτό το νέο εμπόρευμα και να διαφυλαχθεί η ιδιωτική ζωή των χρηστών (Tronnier et al., 2022).

#### 2.2.3.1 Εμπορευματοποίηση ορισμός

Η εμπορευματοποίηση ως όρος σύμφωνα με τον Sevignani (2013) είναι «η διαδικασία κατά την οποία τα πράγματα μπορούν να γίνουν ανταλλάξιμα στις αγορές είτε ουσιαστικά είτε

λεκτικά». Από την άλλη, η εμπορευματοποίηση των προσωπικών δεδομένων «ενώ θεωρείται από πολλούς ως μία πραγματικότητα, νόμιμη, εμπορικά και κοινωνικά αποδεκτή, μεγάλη μερίδα ανθρώπων την αξιολογούν ως παράνομη, απαράδεκτη και ανήθικη» (Tronnier et al., 2022).

Τα προσωπικά δεδομένα αποκτούν εμπορική αξία επειδή είναι απόρρητα (Bottis & Bouchagiar, 2018). Πιο συγκεκριμένα τα εμπορευματοποιημένα προσωπικά δεδομένα είναι ένα διακριτό πακέτο προσωπικών πληροφοριών, το οποίο έχει συλλεχθεί από ιδιωτικές εταιρείες, έπειτα από συστηματική παρακολούθηση των ανθρώπων, των συνηθειών και των προτιμήσεων τους (Rose, 2021).

Γενικότερα, με την εξέλιξη του Διαδικτύου έχει δημιουργηθεί η εποχή των μεγάλων δεδομένων (Canellopoulou-Bottis & Bouchagiar, 2018) στην οποία «οι προσωπικές πληροφορίες αποτελούν ένα αγαθό μαζικής παραγωγής που καταναλώνεται ως εμπόρευμα αντί να χρησιμοποιείται ως εργαλείο για την προσωπική ανάπτυξη του ατόμου ή την ανάπτυξη δημοκρατικών κοινωνιών» (Canellopoulou-Bottis & Bouchagiar, 2018).

Σύμφωνα με την/τον Rose (2021), οι προσωπικές πληροφορίες έχουν γίνει στόχος εμπορευματοποίησης, ενώ αρκετοί ερευνητές (Tronnier et al., 2022; Versaci, 2018; vom Lehn et al., 2014) θεωρούν ότι η συλλογή, η επεξεργασία και η χρήση των προσωπικών δεδομένων μπορεί να δημιουργήσει αξία. Επιπρόσθετα, οι Tronnier et al. (2022) συμπληρώνουν ότι οι πληροφορίες και τα δεδομένα αποτελούν τους κύριους μοχλούς της ψηφιακής οικονομίας, διότι όλο και πιο συχνά νέα προϊόντα, υπηρεσίες και γενικότερα διαδικασίες συνδέονται με τη συλλογή αλλά και τη δημιουργία νέων πληροφοριών από δεδομένα που έχουν συλλεχθεί (Tronnier et al., 2022).

#### 2.2.3.2 Διαδικασία εμπορευματοποίησης προσωπικών δεδομένων

Στη νέα ψηφιακή πραγματικότητα υπηρεσίες κοινωνικής δικτύωσης, μηχανές αναζήτησης, πλατφόρμες φιλοξενίας, υπηρεσίες επικοινωνίας και πολλά ακόμα επιχειρηματικά μοντέλα βασίζονται στα προσωπικά δεδομένων χρηστών. Τα δεδομένα αυτά θεωρούνται ως αντίθετη απόδοση για τις «δωρεάν» ψηφιακές υπηρεσίες ή για τις εκπτώσεις για ηλεκτρονικές υπηρεσίες και προϊόντα (Malgieri & Custers, 2018). Η άποψη ότι τα προσωπικά δεδομένα είναι «το νέο νόμισμα» είναι μία αποτελεσματική μεταφορά που αντιπροσωπεύει την νέα κατάσταση στην οικονομία (Versaci, 2018).

Οι ιδιωτικές εταιρείες συλλέγουν προσωπικά δεδομένα, τα οποία οι χρήστες του Διαδικτύου είτε έχουν μοιραστεί εκούσια, όπως είναι στοιχεία ταυτότητας, κατοικίας, εργασίας και άλλα, συνήθως κατά την συμπλήρωση ηλεκτρονικών φορμών, είτε ακούσια, όπως αναζητήσεις. Τα

δεδομένα αυτά συλλέγονται, επεξεργάζονται, διατηρούνται και τέλος χρησιμοποιούνται προς πώληση ή ανταλλαγή για οικονομικό πολλές φορές όφελος των ιδιωτικών εταιριών (Bottis & Bouchagiar, 2018).

Οι Bottis & Bouchagiar (2018) και Malgieri & Custers (2018) υποστηρίζουν ότι τα προσωπικά δεδομένα που αφορούν γενικά χαρακτηριστικά όπως φύλο, ηλικία, τοποθεσία έχουν μικρότερη αξία από δεδομένα υγείας ή από ευαίσθητα και πολύ προσωπικά δεδομένα. Ομοίως τα μεμονωμένα χαρακτηριστικά αξίζουν πολύ λιγότερο από ολοκληρωμένα προφίλ χρηστών. Για αυτούς τους λόγους, σύμφωνα με τους Malgieri & Custers (2018) μηχανές αναζήτησης και πλατφόρμες κοινωνικής δικτύωσης όπως η Google, το Facebook και το Twitter έχουν αναπτύξει τεράστια συστήματα παρακολούθησης των χρηστών και αποθήκευσης όλων των δεδομένων τους (Sevignani, 2013).

Τα προφίλ αυτά καθώς και τα μεμονωμένα προσωπικά δεδομένα που έχουν συλλέξει πωλούν ή ανταλλάσσουν με τρίτους εταιρείες παροχών δεδομένων (Cinar & Ateş, 2022). Οι μεσίτες δεδομένων, όπως ονομάζονται και αλλιώς, αγοράζουν και πωλούν τα προσωπικά δεδομένα που έχουν συγκεντρώσει είτε από άλλους παρόχους, από εμπορικές πηγές, από δημόσια αρχεία ή ακόμα και από διαδικτυακές δραστηριότητες (Rose, 2021).

Οι πληροφορίες που έχουν συγκεντρώσει αφορούν στις ακόλουθες κατηγορίες: δημογραφικές, ψυχογραφικές όπως τρόπος ζωής, ενδιαφέροντα, χαρακτηριστικά προσωπικότητας, και συμπεριφορικές όπως αγοραστικές συνήθειες, αναλυτικά στοιχεία χρήσης ιστοσελίδας/εφαρμογής και άλλα (Cinar & Ateş, 2022).

Ο τρόπος που δρουν αυτοί οι μεσίτες για να συλλέξουν τα δεδομένα είναι αρχικά με την «αθώα» αποδοχή των όρων χρήσης μίας σελίδας/εφαρμογής, την οποία η πλειοψηφία αποδέχεται χωρίς να διαβάσει, και στη συνέχεια με τη βοήθεια των «cookies». Τα «cookies» είναι μικρά, μη εκτελέσιμα αρχεία κειμένου, που αποθηκεύονται στο πρόγραμμα περιήγησης και λειτουργούν ως βοηθοί μνήμης για ιστοτόπους (Cinar & Ateş, 2022). Τα «cookies» συγκεντρώνουν όλα τα αιτήματα που κάνει ο χρήστης και έτσι συλλέγονται πληροφορίες σχετικές με τα ενδιαφέροντα, τις προτιμήσεις του χρήστη και σιγά σιγά χτίζονται τα προφίλ των χρηστών (Cinar & Ateş, 2022).

#### 2.2.3.3 Η αξία και τα χαρακτηριστικά των προσωπικών δεδομένων

Η επεξεργασία προσωπικών δεδομένων είναι απαραίτητη για οικονομικούς και κοινωνικά χρήσιμους σκοπούς όπως αναφέρθηκε παραπάνω, όπως η υγειονομική περίθαλψη, η εκπαίδευση ή η πρόληψη της τρομοκρατίας. Πέραν όμως αυτών των σημαντικών λόγων πολλές εταιρείες χρησιμοποιούν τα προσωπικά δεδομένα για ιδιωτικά κέρδη, όπως

στοχευμένες διαφημίσεις, πληροφορίες συμπεριφορών καταναλωτών, αγοραστικών προτιμήσεων και άλλες (Rose, 2021). Αυτό υποδηλώνει ότι τα δεδομένα έχουν οικονομική αξία από μόνα τους χωρίς καν να προλάβουν να τύχουν επεξεργασίας (Versaci, 2018).

Σύμφωνα με τους Tronnier et al. (2022), τα άτομα δεν γνωρίζουν την πραγματική αξία των δεδομένων τους ή τις πιθανές επιπτώσεις της επεξεργασίας στην οποία αυτά υπόκεινται. Ταυτόχρονα οι Botes et al. (2022) υποστηρίζουν ότι οι μεγάλες εταιρείες εδώ και δεκαετίες, πριν ακόμα υπάρξει η συνειδητοποίηση της αξίας των δεδομένων, είχαν αρχίσει να συλλέγουν και να εκμεταλλεύονται όπως αυτές επιθυμούσαν τα δεδομένα που μοιράζονταν ελεύθερα οι χρήστες.

Συμφώνα με τους Malgieri & Custers (2018), τα προσωπικά δεδομένα αποτελούνται από πολλά διαφορετικά χαρακτηριστικά του υποκείμενου των δεδομένων, όπως το όνομα, τη διεύθυνση, και την πόλη κατοικίας του. Κάποια ακόμα χαρακτηριστικά είναι η ημερομηνία γέννησης, το φύλο, η οικογενειακή κατάσταση, το επάγγελμα και άλλα. Πιο προσωπικά χαρακτηριστικά είναι αυτά των ενδιαφερόντων και προτιμήσεων. Οι Malgieri & Custers (2018) προσπάθησαν να ταξινομήσουν τα δεδομένα σε βιογραφικά δεδομένα, δεδομένα υγείας, γενετικά, βιομετρικά, εμπορικά και οικονομικά δεδομένα. Όλα αυτά τα δεδομένα θεωρούνται θεμελιώδη στην κατασκευή προφίλ καταναλωτών, τα οποία θα είναι χρήσιμα σε πολλούς κλάδους. Για παράδειγμα, οι ασφαλιστικές εταιρείες ενδιαφέρονται για τα δεδομένα υγείας, τα βιογραφικά δεδομένα και τα γενετικά δεδομένα, ώστε αφενός να μπορούν να προβλέπουν γενετικές παθήσεις και αφετέρου να μπορούν να προσφέρουν πακέτα πραγματικά χρήσιμα σε καταναλωτές (Botes et al., 2022).

Από την άλλη, οι τράπεζες ενδιαφέρονται για δεδομένα που αφορούν τους χρήστες και τον κύκλο τους, όπως οικογένεια και φίλους, έτσι ώστε να μπορούν να προβλέψουν τη πιστοληπτική τους ικανότητα (Malgieri & Custers, 2018). Ακόμα οι διαφημιστικές εταιρίες ενδιαφέρονται για όλων των ειδών δεδομένων, όπως συνήθειες, τρόπους ζωής, χαρακτηριστικά προσωπικότητας (Malgieri & Custers, 2018) και άλλα, ώστε να μπορούν να προβάλλουν «την τέλεια διαφήμιση», προωθώντας το «κατάλληλο αγαθό» στην «κατάλληλη τιμή» (Bottis & Bouchagiar, 2018). Τέλος, τα δεδομένα υγείας που συλλέγονται από ασθενείς θεωρούνται πάρα πολύ σημαντικά, διότι χρησιμεύουν για προβλέψεις ασθενειών, αλλά και για την πραγματοποίηση μελλοντικών ερευνών που θα ωφελήσουν το γενικό σύνολο (Skovgaard et al., 2019).

#### 2.2.3.4 Κύκλος ζωής των προσωπικών δεδομένων

Σύμφωνα με τους Douilhet & Karanasiou (2016) και Rose (2021), υπάρχουν τέσσερα στάδια στον κύκλο επεξεργασίας των μεγάλων δεδομένων, από την ακατέργαστη μορφή τους έως τη χρήση τους, για να δημιουργηθεί κέρδος. Αυτή είναι η συλλογή, η επεξεργασία, η εξόρυξη και η χρήση. Στο στάδιο της συλλογής τα δεδομένα συλλέγονται με διάφορα μέσα, όπως αναφέρθηκε, είτε με άμεσο και εθελοντικό τρόπο όπως με συμπλήρωση πεδίων πληροφοριών κατά τη διαδικασία κάποιας διαδικτυακής παραγγελίας όπως όνομα, κινητό, φύλο, στοιχεία κατοικίας, είτε έμμεσα κάνοντας αποδοχή των «cookies», τα οποία επιτρέπουν σε ιστοτόπους να αναγνωρίσουν και να συγκεντρώσουν πληροφορίες χρηστών μέσω της διαδικτυακής δραστηριότητας ενός ατόμου (Rose, 2021).

Στο επόμενο στάδιο της επεξεργασίας, τα δεδομένα που είναι συγκεντρωμένα σε βάσεις δεδομένων υπόκεινται σε επεξεργασία είτε από την εταιρεία που τα συνέλεξε είτε από τρίτους «επεξεργαστές δεδομένων». Στη συνέχεια, στο στάδιο της εξόρυξης τα δεδομένα αναλύονται μέσω αλγορίθμων υπολογιστών ή λογισμικά ανάλυσης δεδομένων και αναγνώρισης προτύπων συμπεριφοράς. Αφού αναλυθούν δημιουργούνται νέες πληροφορίες τις οποίες και χρησιμοποιούν στο τελευταίο στάδιο της χρήσης, με σκοπό τη δημιουργία εσόδων. Για παράδειγμα, η αρχική εταιρεία πουλάει ή ενοικιάζει τα τελικά δεδομένα για λόγους στοχευμένης διαφήμισης και άλλων συναλλαγών.

#### 2.2.3.5 Εμπορευματοποίηση και συνέπειες

Σύμφωνα με τους Malgieri & Custers (2018), "οι ψηφιακές ταυτότητες χρηστών γίνονται όλο και πιο ολοκληρωμένες λόγω της εκθετικής αύξησης των διαθέσιμων δεδομένων και τεχνολογιών για το συνδυασμό και την επεξεργασία των δεδομένων". Επιπλέον, οι συνεχώς αναπτυσσόμενες ψηφιακές τεχνολογίες επιτρέπουν πολύ πιο εύκολα, αυτόματα και οικονομικά, να παρακολουθούνται, να συλλέγονται, να αναλύονται και γενικώς να επεξεργάζονται τα προσωπικά δεδομένα. Το γεγονός αυτό, επιβεβαιώνει την άποψη ότι όλοι οι χρήστες είναι μονίμως εκτεθειμένοι σε συνεχή επιτήρηση (Cinar & Ateş, 2022). Ειδικότερα ο Versaci (2018), θεωρεί ότι η εμπορική εκμετάλλευση των προσωπικών δεδομένων επιφέρει σημαντικές συνέπειες. Η κατάχρηση των προσωπικών δεδομένων, η διαρροή δεδομένων, η κλοπή ταυτοτήτων, η κοινή χρήση δεδομένων με τρίτους, η αύξηση παραβιάσεων διαδικτυακών προφίλ και κατ' επέκταση η συστηματική απώλεια της προσωπικής αυτονομίας είναι μερικές από τις συνέπειες της εμπορευματοποίησης.

Ωστόσο είναι πολύ σημαντικό σε αυτό το σημείο να γίνει αναφορά στη στοχευμένη διαφήμιση και στις ανησυχίες που αυτή προκαλεί. Σήμερα το Διαδίκτυο και οι υπηρεσίες του,

πληρώνονται αν και αρχικά θεωρούνταν «δωρεάν» από τις διαφημίσεις (Canellopoulou-Bottis & Bouchagiar, 2018). Οι ψηφιακές διαφημίσεις έχουν ξεπεράσει κατά πολύ τις παραδοσιακές διαφημίσεις (Cinar & Ateş, 2022).

Αυτό οφείλεται στο ότι η εξελιγμένη τεχνολογία επιτρέπει στους διαφημιστές να έχουν πρόσβαση σε τεράστιο όγκο πληροφοριών των καταναλωτών. Οι πληροφορίες αυτές αφορούν πέρα από κάποια δημογραφικά στοιχεία, τις ανάγκες, τις προτιμήσεις και γενικότερα τα «θέλω» των καταναλωτών. Έτσι η ψηφιακή διαφήμιση χαρακτηρίζεται πολλές φορές ως στοχευμένη, λόγω του ότι στοχεύει σε συγκεκριμένο καταναλωτικό κοινό. Ενώ, από τη μία πλευρά, αυτό διευκολύνει πολύ τη δουλειά των διαφημιστών, από την άλλη, καταπιέζει και προκαλεί αρνητικά συναισθήματα στους χρήστες. Πιο συγκεκριμένα σύμφωνα με τον Sevignani (2013) οι περισσότεροι ενήλικες Αμερικάνοι (66%) δεν θέλουν οι έμποροι να προσαρμόζουν τις διαφημίσεις ανάλογα με τις προτιμήσεις τους, διότι νιώθουν ότι καταπατάται ο προσωπικός τους χώρος.

Τέλος, μία ακόμα συνέπεια της εμπορευματοποίησης είναι η διάκριση των χρηστών. Αναλυτικότερα οι Malgieri & Custers (2018), υποστηρίζουν ότι τα προσωπικά δεδομένα των φτωχών ανθρώπων είναι λιγότερα πολύτιμα, από εκείνα των πλουσίων. Αυτό στηρίζεται στο γεγονός ότι οι πλούσιοι έχουν μεγαλύτερη τάση για κατανάλωση προφανώς εξαιτίας της οικονομικής τους άνεσης, κάτι που δεν ισχύει για την πλειοψηφία των καταναλωτών με χαμηλό εισόδημα. Αυτό έχει σαν αποτέλεσμα να ενισχυθούν οι υπάρχουσες κοινωνικές ανισότητες.

#### 2.2.3.6 Εμπορευματοποίηση και παραδείγματα

Σύμφωνα με τους Malgieri & Custers (2018), διακρίνονται τρεις περιπτώσεις χρήσης προσωπικών δεδομένων :

- Η «δωρεάν» ή με έκπτωση παροχή διαδικτυακών υπηρεσιών
- Η «δωρεάν» ή με έκπτωση παροχή διαδικτυακού περιεχομένου
- Η «δωρεάν» ή με έκπτωση παροχή μίας υπηρεσίας «εκτός σύνδεσης»

Στην πρώτη περίπτωση, της χρήσης διαδικτυακών υπηρεσιών, ως παράδειγμα μπορεί να θεωρηθούν οι «δωρεάν» υπηρεσίες Wi-Fi σε κοινόχρηστους χώρους, όπως στα εμπορικά καταστήματα, στα αεροδρόμια και σε άλλες δημόσιες υπηρεσίες. Οι χρήστες προκειμένου να αποκτήσουν πρόσβαση στο Διαδίκτυο αποδέχονται κάποιους όρους «cookies» και συναινούν στην παροχή δεδομένων Διαδικτύου, όπως ιστορικό αναζήτησης, ιστορικό τοποθεσιών και άλλες πληροφορίες, στις εταιρίες.

Για τη δεύτερη περίπτωση ένα παράδειγμα είναι η πλατφόρμα Spotify. Οι χρήστες μπορούν να έχουν πρόσβαση σε όλο το υλικό της πλατφόρμας δωρεάν και να δημιουργήσουν ένα προφίλ κοινωνικής δικτύωσης, αλλά σαν ανταπόδοση πρέπει να εξουσιοδοτήσουν την πρόσβαση του Spotify στα δεδομένα του προφίλ τους στο Facebook.

Τέλος, στην τρίτη περίπτωση, ως παράδειγμα μπορεί να θεωρηθεί «η έκπτωση στα ασφαλιστήρια συμβόλαια ζωής κατά τη χρήση ιχνηλατών υγείας» (Malgieri & Custers, 2018). Πιο συγκεκριμένα, οι ασφαλιστικές εταιρείες συνεργάζονται με εταιρείες ευεξίας, άθλησης και υγείας και παρέχουν έκπτωση σε ασφαλιστήρια ζωής, αν οι χρήστες επιτρέψουν στις διάφορες συσκευές των εταιριών ευεξίας να παρακολουθήσουν τις δραστηριότητές τους. Με αυτό τον τρόπο οι ασφαλιστικές αποκτούν πρόσβαση σε πληροφορίες σχετικές με τις συνθήκες υγείας, τις καθημερινές συνήθειες και τη ψυχική υγεία, προκειμένου να προβλέψουν τους κινδύνους ή το ακριβές προσδόκιμο ζωής. Για παράδειγμα, όταν «ο John Hancock, ένας από τους μεγαλύτερους ασφαλιστές ζωής στις ΗΠΑ, συνεργάστηκε με τη Vitality, έναν εταιρικό πάροχο ευεξίας, για να προσφέρει στους κατόχους συμβολαίων έκπτωση, όταν άφηναν μια δωρεάν συσκευή, Fitbit, να παρακολουθεί τις δραστηριότητές τους. Οι καταναλωτές λάμβαναν εξατομικευμένους στόχους υγείας και μπορούσαν να καταγράψουν τις δραστηριότητές τους χρησιμοποιώντας διαδικτυακά και αυτοματοποιημένα εργαλεία» (Malgieri & Custers, 2018).

Ωστόσο, μετά από τη βιβλιογραφική επισκόπηση που έγινε, έχουν συλλεχθεί αρκετά ακόμα, παραδείγματα εμπορευματοποίησης δεδομένων.

Αρχικά, οι εταιρείες που παρέχουν δωρεάν την υπηρεσία ηλεκτρονικού ταχυδρομείου, εκμεταλλεύονται τα δεδομένα που μοιράζονται οι χρήστες, τα επεξεργάζονται, τα αναλύουν, τα συσχετίζουν μεταξύ τους και τέλος τα χρησιμοποιούν όπως εκείνες επιθυμούν (Bottis & Bouchagiar, 2018).

Επιπλέον, οι υπηρεσίες κοινωνικής δικτύωσης όπως το Twitter, το Facebook και το Instagram δρουν με συγκεκριμένους τρόπους. Πιο συγκεκριμένα, στο Instagramm ενώ η εγγραφή στην υπηρεσία είναι δωρεάν, οι χρήστες οφείλουν να παραχωρήσουν την άδεια χρήσης του περιεχομένου που δημιουργούν ή/και διαμοιράζουν χωρίς οι ίδιοι να λαμβάνουν κανένα οικονομικό όφελος (Malgieri & Custers, 2018).

Το Facebook, ομοίως, προσφέρει δωρεάν υπηρεσίες στους χρήστες αλλά ταυτόχρονα αναμένει κέρδη από πελάτες που θέλουν να διαφημίσουν τα προϊόντα και τις υπηρεσίες τους (Lehtiniemi, 2017). Αναλυτικότερα, το Facebook επιτρέπει σε επιχειρήσεις να χρησιμοποιούν τους αλγόριθμούς του, για να συλλέξουν μέσω των υπηρεσιών του, προσωπικά δεδομένα που θα χρησιμοποιήσουν οι διαφημιστές για στοχευμένες διαφημίσεις (Cinar & Ateş, 2022).

Η Google επίσης πουλά δεδομένα που έχει συλλέξει μέσω των δωρεάν υπηρεσιών της και ταυτόχρονα επιτρέπει σε διαφημιστές να χρησιμοποιούν τις πλατφόρμες του για να παρουσιάζουν τα προϊόντα και τις υπηρεσίες που ενδιαφέρουν τους χρήστες.

Ακόμα και η πλατφόρμα του LinkedIn έχει συγκεκριμένο τρόπο δράσης. Οι Karanasiou & Douilhet (2016) αναφέρουν ότι το LinkedIn αφενός δεν επιτρέπει στους χρήστες να ανακτήσουν πλήρως τις πληροφορίες που έχουν μοιραστεί, και αφετέρου δεν επιτρέπει σε άλλες εφαρμογές να έχουν πρόσβαση στα δεδομένα αυτά, ακόμα και αν έχει συμφωνήσει ο χρήστης.

Δύο ακόμα παραδείγματα τεράστιας εκμετάλλευσης των προσωπικών δεδομένων είναι αρχικά αυτό της Cambridge Analytica, η οποία συγκέντρωσε απόρρητα δεδομένα από περίπου 87 εκατομμύρια προφίλ στο Facebook, και στη συνέχεια αφού τα παραποίησε τα χρησιμοποίησε σε πολιτικές εκστρατείες (Rose, 2021). Επίσης, η εκτεταμένη παραβίαση των δεδομένων της Fargo Wells, περίπτωση κατά την οποία διέρρευσαν πληροφορίες από 50,000 προσωπικούς αναγνωρίσιμους λογαριασμούς με αποτέλεσμα να απειλούνται με κλοπή ταυτότητας αρκετοί πελάτες.

### 2.2.4 Απάτη ταυτότητας (Identity Fraud)

Με την εμφάνιση και την καθιέρωση της ψηφιακής οικονομίας, έχει εξελιχθεί και εδραιωθεί η απάτη ταυτότητας (Tan et al., 2016). Οι Simon Enoch et al. (2013) θεωρούν ότι ο γρήγορος ρυθμός ανάπτυξης του Ιντερνέτ, καθώς και το γεγονός ότι χρησιμοποιείται σχεδόν για τα πάντα, έχει συνδράμει στο να αυξηθεί ο βαθμός εγκληματικής εκμετάλλευσης στο Διαδίκτυο, όπως η απάτη ταυτότητας, ενώ οι Gyourko & Greeson (2022) αναφέρουν ότι η απάτη ταυτότητας είναι ένα διάχυτο και αυξανόμενο φαινόμενο στις Ηνωμένες Πολιτείες, για το οποίο έχει παρατηρηθεί ότι η συχνότητα να συμβεί στο γενικό πληθυσμό έχει αυξηθεί δραματικά τις τελευταίες δεκαετίες.

Η ευθύνη για τη πρόληψη της κλοπής ταυτότητας εμπίπτει σε τρεις ομάδες σύμφωνα με τον Gilbert & Archer (2011). Στους καταναλωτές που παρέχουν τις πληροφορίες, στους οργανισμούς που συλλέγουν και χρησιμοποιούν τις πληροφορίες και τέλος στους νομοθετικούς φορείς που ρυθμίζουν το χειρισμό προσωπικών πληροφοριών.

Παρ’ όλες τις προσπάθειες των νομοθετών να δημιουργήσουν ένα νομικό πλαίσιο για να μετριαστεί το φαινόμενο, αυτό συνεχίζει να αυξάνεται. Την ίδια στιγμή οι οργανισμοί, που συλλέγουν τις πληροφορίες κάνουν ό,τι μπορούν για να ασφαλίσουν τις πληροφορίες και τα συστήματα τους, αλλά και να προβλέψουν τυχόν κενά που υπάρχουν στα τείχη προστασίας τους. Οι διαδικτυακές δραστηριότητες έχουν γίνει αρκετά περίπλοκες με αποτέλεσμα να

χάνεται η ικανότητα διαχείρισης του τεράστιου όγκου δεδομένων που συλλέγονται (Tan et al., 2016). Ταυτόχρονα, ο καταναλωτής έχει ζωτικό ρόλο στην προστασία των προσωπικών του δεδομένων (Gilbert & Archer, 2011). Η παραμέληση προστασίας των κωδικών ασφαλείας του, η μη συχνή διαγραφή των cookies, η χρήση κοινών φορητών υπολογιστών χωρίς να διαγράφεται το ιστορικό από τις μηχανές αναζήτησης μετά το τέλος της χρήσης, οι ανταποκρίσεις σε επιθέσεις «ψαρέματος», είναι κάποια σημεία απροσεξίας από την πλευρά των χρηστών. Επιπρόσθετα, οι υπηρεσίες κοινωνικής δικτύωσης, που είναι και ο πιο συχνός στόχος αυτών που διαπράττουν την κλοπή ή απάτη ταυτοτήτων, χρησιμοποιούνται χωρίς όρια, με τους χρήστες να μοιράζονται, από γενικές πληροφορίες, όπως λίστες φίλων, δημόσιες ή και ιδιωτικές αναρτήσεις, μέχρι ιδιωτικές συνομιλίες – μηνύματα και ιστορικό χρήσεως εφαρμογών. Όλα αυτά σε συνδυασμό με το ότι οι περισσότερες καθημερινές δραστηριότητες όπως τραπεζικές συναλλαγές, καταναλωτικές αγορές και δραστηριότητες αναψυχής γίνονται διαδικτυακά, αυξάνουν τον κίνδυνο να πέσει κάποιος θύμα αυτού του φαινομένου.

#### 2.2.4.1 Ορισμός

Σε αυτό το σημείο είναι αναγκαίο να οριστεί η απάτη ταυτότητας (identity fraud). Έχει γίνει προσπάθεια από πολλούς να οριστεί σωστά αυτό το φαινόμενο. Πιο συγκεκριμένα οι Cherus et al. (2014), ορίζουν την απάτη ταυτότητας ως «τη χρήση πλαστών, αναγνωριστικών στοιχείων, πλαστών εγγράφων ταυτοποίησης ή κλεμμένης ταυτότητας για τη διάπραξη εγκλημάτων». Οι Soomro et al. (2021) την ορίζουν ως «τη χρήση κλεμμένης κλωνοποιημένης ή παραποιημένης ταυτότητας για τη διάπραξη απάτης».

Από την άλλη οι Gyourko & Greeson (2022) την ορίζουν «ως μη εξουσιοδοτημένη χρήση προσωπικών δεδομένων, από ένα δράστη που επιδιώκει δόλιο, οικονομικό ή υλικό κέρδος σε βάρους του θύματος» και οι Conlin & Ruhi (2021) «ως οποιαδήποτε ενέργεια που περιλαμβάνει την ακατάλληλη χρήση προσωπικών στοιχείων ταυτοποίησης για τη διάπραξη απάτης ή κλοπής».

Από αυτούς τους ορισμούς γίνεται αντιληπτό πρώτον, ότι η απάτη ταυτότητας θεωρείται η χρήση πραγματικών προσωπικών δεδομένων αλλά και παραποιημένων ή πλαστών δεδομένων, και δεύτερον ότι συμβαίνει για να εξαπατήσει τρίτους αλλά και για οικονομικό ή υλικό κέρδος αυτών που τη διαπράττουν. Στο ίδιο συμπέρασμα κατέληξαν και οι Wang et al. (2019), οι οποίοι ορίζουν την απάτη ταυτότητας ως «την πράξη κατά την οποία ένα άτομο χρησιμοποιεί προσωπικές πληροφορίες άλλου ατόμου ή συνδυάζει μερικά πραγματικά δεδομένα με ψευδείς πληροφορίες για να εξαπατήσει ένα τρίτο άτομο».

### 2.2.4.2 Είδη απάτης ταυτότητας

Τα είδη της διαδικτυακής απάτης της ταυτότητας είναι πολλά, αλλά το επικρατέστερο είναι το ηλεκτρονικό ψάρεμα (phishing). Το ηλεκτρονικό ψάρεμα αναφέρεται στα περισσότερα αποτελέσματα της βιβλιογραφικής επισκόπησης (Cherus et al., 2014; Hanka, 2012; Lee, 2020; Liu et al., 2012; Simon Enoch et al., 2013). Γενικότερα, θεωρείται ως το πιο συχνό είδος απάτης που αυξάνεται δραματικά τα τελευταία χρόνια. Το ηλεκτρονικό ψάρεμα είναι η εξαπάτηση των καταναλωτών με σκοπό να παρακινηθούν να αποκαλύψουν προσωπικές οικονομικές πληροφορίες σε έναν ιστότοπο, οι οποίες αποθηκεύονται και χρησιμοποιούνται αργότερα για δόλιες δραστηριότητες (Cross et al., 2014). Σύμφωνα με τους Cherus et al. (2014), είναι μία μορφή ηλεκτρονικής απάτης ταυτότητας στην οποία χρησιμοποιείται ο συνδυασμός κοινωνικών και τεχνικών μέσων για να επιτευχθεί η εξαπάτηση του χρήστη. Ο Lee (2020) αναφέρει το φωνητικό ψάρεμα ως μία σύγχρονη παραλλαγή του κλασικού ηλεκτρονικού ψαρέματος, η οποία βασίζεται στην ενστικτώδη εμπιστοσύνη των χρηστών στην ανθρώπινη φωνή.

Επιπλέον οι Conlin & Ruhi (2021) αναφέρουν και άλλα είδη απάτης ταυτότητας όπως τις απάτες των πιστωτικών καρτών. Τέλος, η πιο ενδελεχής αναφορά στα είδη απάτης ταυτότητας έχει γίνει από τους Cross et al. (2014), οι οποίοι αναφέρουν λεπτομερώς όλα τα είδη που επικρατούν σήμερα. Αυτά είναι :

- Ηλεκτρονικό ψάρεμα (phishing)
- Pharming (σε μία ελεύθερη απόδοση στα Ελληνικά αποτελεί ένα είδος κυβερνο-επίθεσης κατά την οποία είτε τα συστήματα υπολογιστών των θυμάτων παραβιάζονται μέσω πειρατείας ή κακόβουλου λογισμικού, είτε πρόκειται για επίθεση κατά την οποία λογισμικό ανακατευθύνει τα θύματα σε ψεύτικους ιστότοπους και τους ζητείται να εισαγάγουν τα στοιχεία τους)
- Skimming (σε μία ελεύθερη απόδοση στα Ελληνικά οι προσωπικές πληροφορίες «αποφορτίζονται» από τις πλαστικές κάρτες μέσω συσκευών που είναι κρυφά προσαρτημένες σε συσκευές ανάγνωσης καρτών)
- Κακόβουλο λογισμικό – είναι όταν χρησιμοποιείται ή εγκαθίσταται σε υπολογιστές κακόβουλο λογισμικό, όπως ιοί, προκειμένου να τροποποιηθούν οι λειτουργίες εντός προγραμμάτων και αρχείων

Υπάρχει επίσης και μία σειρά από νέες και αναδυόμενες τεχνικές (Cross et al., 2014):

- «SMiShing — προσωπικές πληροφορίες που λαμβάνονται μέσω SMS»
- «Vishing — προσωπικές πληροφορίες που λαμβάνονται μέσω τηλεφώνου»

- «Spear-phishing—υψηλά στοχευμένα ανεπιθύμητα μηνύματα»
- «Koobface στα μέσα κοινωνικής δικτύωσης—όπου αποστέλλονται στα θύματα μηνύματα στα μέσα κοινωνικής δικτύωσης με έναν ιό»
- «Κοινωνικό ηλεκτρονικό ψάρεμα — με το οποίο ο δράστης κερδίζει την εμπιστοσύνη ενός ατόμου και αποκτά πρόσβαση στη λίστα φίλων του ή ως phisher αποκτά μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό ενός χρήστη και αρχίζει να στέλνει ανεπιθύμητα μηνύματα στις άμεσες επαφές του χρήστη»
- «Ιοί καταγραφής κλειδιών—αυτοί οι ιοί καταγράφουν λεπτομέρειες σύνδεσης ή κωδικούς πρόσβασης για τραπεζικούς λογαριασμούς, οι οποίοι για παράδειγμα, μπορούν στη συνέχεια να χρησιμοποιηθούν ή να πωληθούν»
- «Απάτη σε εικονικές πλατφόρμες όπως το 'Second Life'» και
- «Διαδικτυακές απάτες ενοικίασης — με τις οποίες τα πλαστά ενοικιαζόμενα διαμερίσματα διαφημίζονται στο Διαδίκτυο και τα θύματα στέλνουν προσωπικές πληροφορίες ή/και καταθέσεις για να αποδείξουν ότι μπορούν να πληρώσουν το ενοίκιο»

#### 2.2.4.3 Στατιστικά απάτης ταυτότητας

Οι DiSanto (2014) και Soomro et al. (2019), υποστηρίζουν ότι η απάτη ταυτότητας γίνεται όλο και πιο διαδεδομένη λόγω του ότι το Διαδίκτυο και το ψηφιακό περιεχόμενο έχουν εξελιχθεί. Πιο συγκεκριμένα, οι Cherus et al. (2014) υποστηρίζουν ότι σημειώνεται συνεχής αύξηση της κλοπής ταυτότητας και της απάτης, και ο αριθμός των περιπτώσεων κλοπής ταυτότητας βρέθηκε να είναι υψηλότερος σε περιοχές με μεγάλο πληθυσμό όπως στις Ηνωμένες Πολιτείες της Αμερικής.

Επίσης, οι Simon Enoch et al. (2013) αναφέρουν ότι στην Έκθεση της Επιτροπής Οικονομικών και Χρηματοοικονομικών Εγκλημάτων, στην πρώτη θέση κατατάσσονται οι Ηνωμένες Πολιτείες με 65% εγκληματικές δραστηριότητες στον κυβερνοχώρο, στη δεύτερη θέση το Ηνωμένο Βασίλειο με το 9,9%, και στην τρίτη θέση η Νιγηρία με 8%. Οι Gilbert & Archer (2011) αναφέρουν ότι έρευνες που έχουν γίνει στον Καναδά, έδειξαν ότι το 6,5% των ενηλίκων ήταν θύματα απάτης ταυτότητας μέσα σε ένα χρόνο (Gilbert & Archer, 2011). Τέλος, σύμφωνα με μία μελέτη «η απάτη για διαδικτυακές αγορές στο Ηνωμένο Βασίλειο έχει αυξηθεί κατά 50% από τον Μάιο του 2019» (Soomro et al., 2021).

#### 2.2.4.4 Που συμβαίνει και ποιους επηρεάζει

Ο Lee (2020) καταλήγει στο ότι η επικράτηση της διαδικτυακής κλοπής ταυτότητας οφείλεται στις πρόσφατες τεχνολογικές εξελίξεις. Τα σύγχρονα τηλέφωνα, οι υπολογιστές, τα έξυπνα ρολόγια είναι μερικά από τα τεχνολογικά επιτεύγματα της εποχής, που δημιουργούν μεγάλες ευκαιρίες για να διαπραχθούν διαδικτυακά εγκλήματα (Lee, 2020). Στα περισσότερα μέσα αποθηκεύονται σημαντικές προσωπικές πληροφορίες και δεδομένα τα οποία είναι εύκολα να υποκλαπούν από χάκερ.

Σύμφωνα με τους Soomro et al. (2019), το « e-tail business είναι ένας από τους τομείς που επηρεάζονται περισσότερο από διαδικτυακές απάτες». Οι Soomro et al. (2021) εξηγούν ότι τα e - tailers είναι ανάμεσα στους στόχους πρώτης γραμμής για τους απατεώνες ταυτότητας, διότι είναι πιο εύκολο να διαρρηχθούν. Λόγω του ότι η τεχνολογία αλλάζει συνεχώς, οι πολιτικές και οι τρόποι για να αντιμετωπιστούν τα είδη απάτης δεν είναι πάντα αποτελεσματικές.

Ένας ακόμα στόχος των εγκληματιών διαδικτυακής απάτης είναι τα δίκτυα κοινωνικής δικτύωσης, τα οποία περιλαμβάνουν πληροφορίες, οι οποίες αν συλλεχθούν όλες μαζί, μπορεί να κατασκευαστεί ένα ολοκληρωμένο προφίλ, πάνω στο οποίο μπορούν να διαπραχθούν πολλών ειδών απάτες.

#### 2.2.4.5 Συνέπειες απάτης διαδικτυακής ταυτότητας

Η απάτη ταυτότητας είναι ένας από τους πιο συχνά εμφανιζόμενους τύπους εγκλημάτων (Lee, 2020), και ένας από τους πιο μεγάλους κινδύνους που προσπαθούν να αποφύγουν οι χρήστες του Διαδικτύου. Οι Gilbert & Archer (2011) αναφέρουν ότι ακόμα και ο υπουργός οικονομικών των ΗΠΑ, Τζον Σνόου, κάποια στιγμή είχε χαρακτηρίσει την κλοπή ταυτότητας «ως τη μεγαλύτερη απειλή για τους καταναλωτές σήμερα», επειδή επιτίθεται στην εμπιστοσύνη που δείχνουν οι χρήστες στο νέο είδος ψηφιακής οικονομίας. Την ίδια άποψη υποστηρίζουν και οι Tan et al. (2016), προσθέτοντας ότι η απάτη ταυτότητας επηρεάζει πέρα από το ευρύ κοινό, τις τράπεζες και τους εμπόρους ηλεκτρονικού εμπορίου.

Οι έμποροι ηλεκτρονικού εμπορίου υποφέρουν από οικονομικές αλλά και μη ζημίες λόγω του φαινομένου. Η μείωση των πωλήσεων, που ισοδυναμεί με μεγάλη πτώση των εσόδων, η μείωση της τιμής των μετοχών τους και η μείωση του μεριδίου αγοράς είναι μερικές από τις οικονομικές απώλειες στις οποίες υπόκεινται (Soomro et al., 2019). Ενώ ως έμμεση απώλεια αντιμετωπίζουν την αμαύρωση της φήμης τους, κάτι το οποίο κατ' επέκταση βλάπτει σοβαρά το εμπορικό τους σήμα. Αυτό συμβαίνει διότι θεωρούνται υπεύθυνες για την διαρροή των δεδομένων, είτε επειδή το επέτρεψαν είτε επειδή δεν κατάφεραν να το αποτρέψουν (Lord,

2012). Όλα αυτά πέρα από το ότι βλάπτουν την πορεία τους, τους αποτρέπει να αναπτυχθούν σωστά.

Οι χρηματοοικονομικές εταιρείες – τράπεζες βιώνουν εξίσου μεγάλο πλήγμα λόγω του ότι επηρεάζεται η πιστοληπτική ικανότητα των χρηστών τους ή επειδή μπορεί να βρεθούν εκτεθειμένες σε διαδικτυακές συναλλαγές προκαλώντας μεγάλα οικονομικά προβλήματα στις ίδιες αλλά και στους πελάτες τους (Gilbert & Archer, 2011).

Ωστόσο, αυτοί που επηρεάζονται περισσότερο είναι οι χρήστες/ καταναλωτές. Πιο συγκεκριμένα, οι Gyourko & Greeson (2022) υποστηρίζουν ότι μία πολύ σημαντική συνέπεια για τους χρήστες είναι η απώλεια μεγάλων χρηματικών ποσών, μισθών και αποταμιεύσεων, κάτι που επιβεβαιώνεται και από τους Cross et al. (2014), οι οποίοι αναφέρουν ότι το 2012 οι απώλειες σε περισσότερους από 2600 Αυστραλούς υπολογίστηκαν σε πάνω από 113 εκατομμύρια δολάρια. Επίσης, οι Soomro et al., (2021), αναφέρουν ότι η απάτη ταυτότητας προκάλεσε απώλεια 16 δισεκατομμυρίων δολαρίων στις ΗΠΑ μόνο για το 2016.

Εκτός όμως από τις οικονομικές απώλειες τα θύματα της απάτης βιώνουν και συναισθηματικές / ψυχολογικές διαταραχές. Τα ευρήματα που αναφέρουν οι Cross et al. (2014), δείχνουν ότι μία μεγάλη μερίδα ανθρώπων μετά την απάτη, ένιωθε συναισθήματα άγχους, και συναισθήματα προδοσίας, και λόγω αυτών επηρεάστηκε η ψυχολογική τους ευημερία αλλά και οι διαπροσωπικές τους σχέσεις. Επίσης έχει παρατηρηθεί ότι κάποια θύματα, σε ακραίες περιπτώσεις είχαν καταφύγει σε αυτοτραυματισμούς και είχαν ακόμα και αυτοκτονικές σκέψεις.

Επιπλέον, το μεγαλύτερο μέρος των θυμάτων ένιωθε έντονα συναισθήματα θυμού (Cross et al., 2014). Αφενός ένιωθαν ανόητοι και ήταν σε σύγχυση, επειδή έπεσαν θύματα απάτης, και αφετέρου ένιωθαν θυμό, επειδή δεν κατάφεραν να δικαιωθούν (Cross et al., 2014). Όπως αναφέρουν οι Cross et al. (2014), στις περιπτώσεις διαδικτυακών απατών, οι παραβάτες είναι δύσκολο να εντοπιστούν λόγω της ανωνυμίας που τους παρέχει το Ίντερνετ και γενικά λόγω των τεχνολογικών εξελίξεων. Επίσης, συνήθως οι παραβάτες δρουν από το εξωτερικό, και αυτό αυτομάτως καθιστά σχεδόν αδύνατον τον εντοπισμό και τη δίωξή τους. Αυτή η έλλειψη της δυνατότητας υπεράσπισης του εαυτού τους και της δικαίωσής τους έχει σαν αποτέλεσμα τα θύματα να νιώθουν βαθιά απογοήτευση.

#### 2.2.4.6 Παραδείγματα απάτης ταυτότητας

Από τη βιβλιογραφική επισκόπηση έχουν εντοπιστεί πολλά παραδείγματα απάτης ταυτοτήτων, τα οποία έχουν να κάνουν με τράπεζες, μέσα κοινωνικής δικτύωσης και email.

Σύμφωνα με τους DiSanto (2014) και Simon Enoch et al. (2013), οι χάκερ «θεωρούνται η γέφυρα μεταξύ των νομικών κατόχων προσωπικών πληροφοριών και των κλεφτών ταυτότητας, οι οποίοι δεν έχουν τις τεχνικές δεξιότητες για την κλοπή πολύτιμων πληροφοριών ταυτότητας». Συνήθως αυτοί είναι που εκμεταλλεύονται συστήματα για να βλάψουν, να παραμορφώσουν ή να κλέψουν πληροφορίες. Ένα παράδειγμα δράσης είναι αυτό του χάκερ Jeremy Hammond, ο οποίος το 2011 «διείσδυσε σε εσωτερικά συστήματα του Stratfor και έκλεψε αρκετές εκατοντάδες δεδομένων, συμπεριλαμβανομένων εταιρικών email, μη κρυπτογραφημένων αριθμών πιστωτικών καρτών, κρυπτογραφημένων κωδικών πρόσβασης και ¬εμπιστευτικών λιστών πελατών». «Στη συνέχεια, ο Hammond μετέφερε δεδομένα σε έναν διακομιστή στη Νέα Υόρκη και κυκλοφόρησε πληροφορίες μέσω υπερσυνδέσμων προσβάσιμων στο κοινό».

Κάποια ακόμα παραδείγματα είναι οι προσπάθειες των χάκερ να κάνουν υπεξαίρεση σε κεφάλαια τραπεζών με εξαγορά λογαριασμού ή τραπεζικά εμβάσματα, ή υποβολή για τραπεζικό δάνειο βασισμένο σε πλαστά στοιχεία και πλαστούς λογαριασμούς.

Επίσης, η διάπραξη απάτης διαδικτυακής ταυτότητας μπορεί να γίνει και μέσω του ηλεκτρονικού ταχυδρομείου / email. Πιο συγκεκριμένα, οι Conlin & Ruhi (2021), αναφέρουν ότι η πρόσβαση στο email ενός χρήστη μέσω απάτης scamming, θα μπορούσε να οδηγήσει σε έναν αναγνωριστικό αριθμό κοινωνικής δικτύωσης, γεγονός που μπορεί να επιφέρει νέες επιθέσεις σε λογαριασμούς/κάρτες του χρήστη και συνεπώς σε σοβαρές απώλειες για αυτόν.

Ένας ακόμα τρόπος να λάβει κάποιος πληροφορίες για τους τραπεζικούς λογαριασμούς είναι ο ακόλουθος. Αρχικά οι παραβάτες κατασκευάζουν μία πλαστή σελίδα. Έπειτα στέλνουν ηλεκτρονικό μήνυμα, που περιέχει έναν σύνδεσμο για να συνδεθούν τα θύματα στην πλαστή σελίδα. Τα θύματα ξεγελιούνται και νομίζουν ότι βρίσκονται στον ιστότοπο της τράπεζας και έτσι συνδέονται, δίνοντας τον κωδικό και το όνομα χρήστη (Simon Enoch et al., 2013; Wu et al., n.d.).

Τέλος, σημαντικά παραδείγματα απάτης ταυτότητας έχουν συμβεί στα μέσα κοινωνικής δικτύωσης. Το πιο σύνηθες είναι η παραβίαση υπαρχόντων λογαριασμών με σκοπό τη συλλογή πληροφοριών για να συλλεχθούν στοιχεία για την ταυτότητα κάποιου χρήστη (Gilbert & Archer, 2011). Ένα ακόμα παράδειγμα είναι η δημιουργία ψεύτικων λογαριασμών (Tan et al., 2016). Σύμφωνα με τους Cross et al. (2014), έχουν εντοπιστεί πολυάριθμες περιπτώσεις χρηστών που έχουν πέσει θύματα ψεύτικων λογαριασμών. Οι δράστες προσποιούνται κάποιους άλλους, με σκοπό να συνδεθούν ρομαντικά με τα θύματα, έτσι ώστε να υπεξαιρέσουν χρήματα.

Σύμφωνα με τη σελίδα (cyberalert.gr, 2015), αναφέρονται παρακάτω μία σειρά παραδειγμάτων διαδικτυακής απάτης που έχουν καταγραφεί στην Ελλάδα.

- Απάτες με ψευδείς διαγωνισμούς για δώρο-επιταγές από γνωστές αλυσίδες καταστημάτων σούπερ-μάρκετ. Ο τρόπος που γίνεται η απάτη είναι η δημιουργία διαδικτυακών συνδέσμων για την συμμετοχή σε ερωτηματολόγια ή διαγωνισμούς στα οποία θα κερδίσουν οι νικητές δωρεάν επιταγές για σούπερ-μάρκετ. Για να ολοκληρωθεί η διαδικασία η σελίδα ζητάει να καταχωρήσουν προσωπικά στοιχεία, τηλεφωνικούς αριθμούς και διευθύνσεις ηλεκτρονικού ταχυδρομείου. Οι σελίδες είναι αρκετά αληθοφανείς, διότι οι εγκληματίες έχουν χρησιμοποιήσει αρκετές λεπτομέρειες των πραγματικών σελίδων, ακόμα και τα ακριβή λογότυπα των επιχειρήσεων.
- Διαδικτυακή απάτη που υπόσχεται δωρεάν αεροπορικά εισιτήρια. Όπως και το προηγούμενο παράδειγμα έτσι και αυτό λειτουργεί με τη δημιουργία υπερ-συνδέσμων, στις οποίες αν εισέλθει ο χρήστης, θα κερδίσει δωρεάν αεροπορικά εισιτήρια. Για να ολοκληρωθεί η διαδικασία ζητείται η συμπλήρωση κάποιων προσωπικών στοιχείων και του προσωπικού αριθμού τηλεφώνου. Όταν ολοκληρωθεί η καταχώρηση των δεδομένων θα ξεκινήσει αυτόματα η χρέωση του αριθμού τηλεφώνου του, μέσω μηνύματος.
- Απάτη με ταξιδιωτικά πακέτα διακοπών. Στην συγκεκριμένη περίπτωση, δημιουργούνται διαφημίσεις φτηνών πακέτων διοργάνωσης διακοπών, σε διάφορα μέσα κοινωνικής δικτύωσης και μηχανές αναζήτησης. Το θύμα στέλνει χρήματα για να διοργανωθούν οι διακοπές του, αλλά οι δράστες εξαφανίζονται μαζί με τα χρήματα.
- Απάτη με δήθεν αγορές – πωλήσεις αυτοκινήτων. Αυτός ο τρόπος απάτης είναι περίπου ίδιος με τον προηγούμενο. Δημιουργούνται ψεύτικες αγγελίες πώλησης αυτοκινήτων με ψεύτικα στοιχεία και φωτογραφίες, τα οποία τις περισσότερες φορές βρίσκονται σε απομακρυσμένες περιοχές. Αφού το θύμα πειστεί από τον δράστη ότι πρόκειται για ευκαιρία, συμφωνεί για την αγορά και στέλνει ένα χρηματικό ποσό ως προκαταβολή για τη μεταφορά του οχήματος για έλεγχο και μεταβίβαση. Μετά την αποστολή των χρημάτων οι δράστες εξαφανίζονται και οι αγγελίες διαγράφονται χωρίς να υπάρχει τρόπος εντοπισμού.
- Απάτη μέσω διαδικτυακών ραντεβού. Αυτού του είδους απάτης συμβαίνει κυρίως σε σελίδες κοινωνικής δικτύωσης. Εκεί διάφορα άτομα προσελκύουν ανυποψίαστα θύματα για τη δημιουργία γνωριμίας και στην συνέχεια δεσμού. Σταδιακά, αρχίζει η

απαίτηση καταβολής χρημάτων, είτε για δώρα είτε για επίσκεψη από το εξωτερικό όπου δήθεν βρίσκεται ο δράστης. Πέρα από χρήματα μπορεί να ζητήσουν στοιχεία τραπεζικών λογαριασμών. Τέλος, αν τα θύματα δεν δεχτούν να στείλουν χρήματα, ενδέχεται να δεχτούν εκβιασμό για την αποκάλυψη του δεσμού τους.

### 2.2.5 Κώδικες δεοντολογικής συμπεριφοράς στο Διαδίκτυο (Netiquette rules)

Η ανάπτυξη του Διαδικτύου και η εξέλιξη του, καθώς και οι τεράστιες δυνατότητες που προσφέρει, το καθιστά αναπόσπαστο κομμάτι της καθημερινότητας. Οι περισσότεροι το χρησιμοποιούν για αγορές ή ηλεκτρονικό εμπόριο, για ψυχαγωγικούς λόγους όπως παιχνίδια, αλλά και για επικοινωνία (Abifarin & Tsetim, 2018a). Γενικότερα, έχει καθιερωθεί τα τελευταία χρόνια μία νέα μορφή επικοινωνίας, η διαδικτυακή, η οποία επιτυγχάνεται με το email, τα μέσα κοινωνικής δικτύωσης, τα μηνύματα κειμένου και άλλες μορφές διαδικτυακής επικοινωνίας, και επιτρέπει τη συνεχή και χωρίς όρια επικοινωνία και αλληλεπίδραση μεταξύ των χρηστών (Ayhan, 2019). Πλέον το Διαδίκτυο είναι ένας σημαντικός παράγοντας εξέλιξης της κοινωνικής ζωής ενός χρήστη, για αυτό και πρέπει η χρήση του να διέπεται από ορισμένους κανόνες χρήσης δικτύου (netiquette rules).

#### 2.2.5.1 Ορισμός

Ο όρος netiquette σχηματίζεται από το συνδυασμό των λέξεων net και etiquette (Abifarin & Tsetim, 2018b; Arouri & Hamaidi, 2017; Ayhan, 2019; Bartl, n.d.; Iqbal et al., 2021; Yarmohammadian et al., 2012). Net είναι το Διαδίκτυο και etiquette είναι η εθιμοτυπία, δηλαδή οι κανόνες που υποδεικνύουν τον σωστό και ευγενικό τρόπο συμπεριφοράς (Arouri & Hamaidi, 2017).

Έτσι το netiquette αφορά σύμφωνα με τους Khani & Darabi (2014), «κανόνες κατάλληλης επικοινωνιακής συμπεριφοράς στο Διαδίκτυο», ενώ οι Arouri & Hamaidi (2017) το ορίζουν ως «ηθική της ψηφιακής επικοινωνίας και ως κανόνες για τον σωστό και κατάλληλο τρόπο επικοινωνίας, χρησιμοποιώντας ηλεκτρονικές συσκευές ή δραστηριότητες στο Διαδίκτυο».

Επιπρόσθετα οι Abifarin & Tsetim (2018b) συμπληρώνουν ότι το netiquette σημαίνει «σεβασμός στις απόψεις των άλλων χρηστών και υποδεικνύει κάποιους κανόνες ευγένειας κατά τη δημοσίευση σκέψεων ή οποιασδήποτε άλλης μορφής επικοινωνίας στον κυβερνοχώρο».

Αυτοί οι κανόνες απευθύνονται στους χρήστες για να υποδείξουν τον τρόπο με τον οποίο πρέπει να συμπεριφέρονται όταν χρησιμοποιούν το Διαδίκτυο (Bansal et al., 2011). Δίνουν έμφαση στις υποχρεώσεις των χρηστών και στην προσπάθεια διασφάλισης της ευπρέπειας

κατά τη διάρκεια των διαδικτυακών συζητήσεων, προωθώντας τον σεβασμό στους άλλους χρήστες. Αυτή η συμπεριφορά είναι αναγκαία, διότι αυξάνει την ποιότητα των διαδικτυακών επικοινωνιών των χρηστών και δημιουργούνται έτσι τα σωστά θεμέλια πάνω στα οποία χτίζονται αυτές οι νέες μορφές διαδικτυακών σχέσεων (Ayhan, 2019).

#### 2.2.5.2 Λόγοι ύπαρξης

Επί του παρόντος, όπως αναφέρθηκε παραπάνω, οι άνθρωποι ασχολούνται το μεγαλύτερο μέρος της ζωής τους με πλατφόρμες νέων μέσων, κοινωνικής δικτύωσης και με αυτό τον τρόπο αναπτύσσεται η κοινωνική τους ζωή στους διάφορους διαδικτυακούς χώρους. Επίσης, ακόμα και στον επαγγελματικό τομέα η επικοινωνία έχει μετατραπεί σε διαδικτυακή μέσω των ηλεκτρονικών μηνυμάτων που ανταλλάσσονται (Ayhan, 2019).

Αυτό το είδος διαδικτυακής επικοινωνίας διαφέρει πολύ από τον παραδοσιακό τρόπο επικοινωνίας, «πρόσωπο με πρόσωπο», με αποτέλεσμα να υπάρχει ο κίνδυνος δημιουργίας παρεξηγήσεων (Ayhan, 2019). Πιο συγκεκριμένα, η διαδικτυακή επικοινωνία δεν «μαρτυρά» στον χρήστη τον τόνο της φωνής, τη γλώσσα του σώματος και τις εκφράσεις. Είναι πιο απρόσωπη, με αποτέλεσμα να δημιουργούνται παρερμηνείες και εσφαλμένα συμπεράσματα αν ο χρήστης δεν προσέξει τον τρόπο που θα εκφραστεί (Ayhan, 2019).

Για να αποφευχθούν αυτού του είδους οι παρεξηγήσεις πρέπει να συνειδητοποιήσει το σύνολο των ανθρώπων την αξία που έχουν οι κανόνες χρήσης του Διαδικτύου. Αρχικά, οι Arouri & Hamaidi (2017) υποστηρίζουν ότι είναι ζωτικής σημασίας τα ιδρύματα τριτοβάθμιας εκπαίδευσης να ενσωματώσουν τους κανόνες Διαδικτύου στα προγράμματα σπουδών τους. Η δημιουργία σεμιναρίων, εργαστηρίων και μία γενική εκπαίδευση στους κανόνες χρήσης του Διαδικτύου είναι αναγκαία. Παράλληλα, η ανάγκη εκπαίδευσης των χρηστών αρχίζει να καθίσταται αναγκαία ακόμα και από τα ιδρύματα της δευτεροβάθμιας εκπαίδευσης, διότι οι μαθητές του σχολείου αφενός έχουν πρόσβαση σε πολλές πλατφόρμες κοινωνικής δικτύωσης και αφετέρου χρησιμοποιούν πλέον το Διαδίκτυο για εκπαιδευτικούς σκοπούς, λόγω νέων συνθηκών όπως συνέβη με τον covid-19.

Οι Iqbal et al. (2021) αναφέρουν ότι το netiquette μπορεί πλέον, εύκολα να αναγνωριστεί ως ένα νέο πεδίο σπουδών που αφορά την ποιοτική διαδικτυακή εκπαίδευση, διότι το Διαδίκτυο μπαίνει από πολύ νωρίς στη ζωή των χρηστών. Αν οι χρήστες εκπαιδευτούν από την έναρξη χρήσης των μέσων κοινωνικής δικτύωσης και των ηλεκτρονικών μηνυμάτων, θα λυθεί το μεγάλο πρόβλημα έλλειψης γνώσης των κανονισμών που διέπουν τη διαδικτυακή χρήση εφαρμογών και συμμετοχής σε φόρουμ. Το πρόβλημα αυτό έχει δημιουργηθεί λόγω του ότι οι μαθητές αλλά και χρήστες μεγαλύτερης ηλικίας χωρίς γνώσεις, γίνονται μέλη σε

διαδικτυακές ομάδες και χρησιμοποιούν προγράμματα και εφαρμογές, αγνοώντας τα πρότυπα καλής συμπεριφοράς και δρουν μιμούμενοι τους προκατόχους τους, δημιουργώντας έτσι έναν φαύλο κύκλο εσφαλμένης συμπεριφοράς στο Διαδίκτυο.

Οι κανόνες αυτοί είναι απαραίτητο να είναι κατανοητοί από όλους, δηλαδή, φοιτητές, καθηγητές (Arouri & Hamaidi, 2017) αλλά και από εργαζόμενους και νέους (Bartl, n.d.), για αυτό και οι οργανισμοί είναι σωστό να εφαρμόζουν τις κατάλληλες πολιτικές ηλεκτρονικού ταχυδρομείου και να παρέχουν εκπαιδευτικά προγράμματα ενημέρωσης σε όλο το προσωπικό. Με αυτό τον τρόπο θα ενισχύσουν τη διαμόρφωση μίας κουλτούρας που θα προωθεί την ποιότητα των ενδο-εταιρικών σχέσεων.

#### 2.2.5.3 Παραδείγματα μη χρήσης των κανόνων Διαδικτύου

Ένα παράδειγμα μη χρήσης των κανόνων είναι το φαινόμενο επιθετικής γλώσσας (flaming). Σύμφωνα με τους Bansal et al. (2011), το φαινόμενο επιθετική γλώσσα «ορίζεται ως αντικανονική, εχθρική και προσβλητική αλληλεπίδραση των χρηστών». Ενώ επίσης κάνουν λόγο και για έναν ακόμα ορισμό, «αυτόν που περιβάλει την διαδικτυακή κοινότητα για να περιγράψει επιθετικές, εχθρικές και συμπεριφορές με υβριστικό λόγο».

Είναι με λίγα λόγια συμπεριφορά που έχει σκοπό να προσβάλει κάποιον, και μπορεί να συμβεί μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, αναρτήσεων, σχολίων ή με τη δημοσίευση δήλωσης που περιλαμβάνει ύβρεις, έντονη γλώσσα, εχθρικά σχόλια. Αυτού του είδους φαινόμενο μπορεί να παρατηρηθεί πιο συχνά σε συζητήσεις και ιδιωτικές ομάδες αλλά και σε ιστοτόπους ανταλλαγής πληροφοριών (Bansal et al., 2011).

Κάποια ακόμα παραδείγματα μη χρήσης των κανόνων του Διαδικτύου είναι η αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου και η αποστολή ψεύτικων προειδοποιήσεων για ιούς (Ayhan, 2019).

# Κεφάλαιο 3. Μεθοδολογία

## 3.1 Περιγραφή Υλοποίησης – Εφαρμογής

Ο σκοπός της παρούσας διπλωματικής εργασίας είναι να εμβαθύνει στο ρόλο που διαδραματίζει το ελεύθερο Διαδίκτυο ως πάροχος πληροφοριών, εστιάζοντας στο να ενημερώσει τους χρήστες για τους κινδύνους που ενέχει η χρήση του. Παράλληλα, σκοπός είναι να δημιουργηθεί και μία συλλογή με τις κορυφαίες ελεύθερες μηχανές αναζήτησης ιστού και ιστοσελίδες, η οποία να είναι πλούσια σε λεπτομέρειες, ώστε ο ενδιαφερόμενος χρήστης να λαμβάνει εύκολα και γρήγορα μία ενδεικτική αλλά ευρεία εικόνα για αυτές.

Η μεθοδολογία που ακολουθήθηκε για την εκπόνηση της εργασίας περιλαμβάνει τα ακόλουθα στάδια:

**Στάδιο 1ο** : Αρχικά, εντοπίστηκαν οι ελεύθερες μηχανές αναζήτησης ιστού και ιστοσελίδων μέσα από την πλατφόρμα Website Traffic - Check and Analyze Any Website | Similarweb. Ο λόγος που επιλέχθηκε η συγκεκριμένη πλατφόρμα είναι ότι παρέχει υπηρεσίες Web analytics και προσφέρει στους χρήστες στατιστικά στοιχεία σχετικά με την επισκεψιμότητα των ιστοτόπων. Ειδικότερα, για τις μηχανές αναζήτησης, η συγκεκριμένη πλατφόρμα παρέχει μία λίστα, που ανανεώνεται διαρκώς, με τις πιο διαδεδομένες ιστοσελίδες και αφορά τη χρήση τους σε διάφορα μέσα όπως κινητό, υπολογιστή και tablet.

Επιπλέον, αυτή η πλατφόρμα έχει ομαδοποιήσει τις ιστοσελίδες σε είκοσι-τέσσερις (24) κατηγορίες:

1. Arts & Entertainment / Τέχνη και Ψυχαγωγία
2. Business and consumer services / Υπηρεσίες επιχειρήσεων και καταναλωτών
3. Community and society / Κοινότητα και κοινωνία
4. Computers Electronics and technology / Ηλεκτρονικοί υπολογιστές και τεχνολογία
5. eCommerce & shopping / Ηλεκτρονικό εμπόριο και αγορές
6. Finance / Οικονομικά
7. Food and drink / Φαγητό και ποτό
8. Gambling / Τυχερά παιχνίδια
9. Games / Παιχνίδια
10. Health / Υγεία
11. Heavy industry and engineering / Βαριά βιομηχανία και μηχανική
12. Hobbies and leisure / Χόμπι και ελεύθερος χρόνος
13. Home and garden / Σπίτι και κήπος

14. Jobs and career / Δουλειές και καριέρα
15. Law and government / Νόμος και κυβέρνηση
16. Lifestyle / Τρόπος ζωής
17. News and media / Ειδήσεις και Μέσα Μαζικής Ενημέρωσης
18. Pets and animals / Κατοικίδια και ζώα
19. Reference Materials / Υλικά αναφοράς
20. Science and education / Επιστήμη και εκπαίδευση
21. Sports / Αθλήματα
22. Travel and tourism / Ταξίδι και τουρισμός
23. Vehicles / Οχήματα
24. Adult / Ενήλικες

Για τους στόχους της παρούσας διπλωματικής εργασίας έχουν επιλεγεί προς παρουσίαση τρεις (3) πλατφόρμες από την κάθε κατηγορία. Η επιλογή της κάθε ελεύθερης πλατφόρμας έγινε με βάση τα ποσοστά επισκεψιμότητάς της, όπως αυτά καταγράφηκαν από το εργαλείο Similarweb κατά τον Μάιο 2022.

Σημειώνεται ότι στην περίπτωση που οι τρεις (3) πρώτες σε επισκεψιμότητα μηχανές αναζήτησης ιστού και ιστοσελίδων δεν ήταν ελεύθερες, τότε έγινε απλή αναφορά σε αυτές, και επιλέχθηκε η κάθε επόμενη με την υψηλότερη επισκεψιμότητα μηχανή αναζήτησης ιστού και ιστοσελίδα που ήταν ελεύθερη. Συνεπώς, η αναλυτική περιγραφή αφορά μόνο στις ελεύθερες μηχανές αναζήτησης ιστού και ιστοσελίδων, καθώς αυτές αποτελούν αντικείμενο μελέτης της παρούσας διπλωματικής εργασίας.

Για παράδειγμα, στην κατηγορία 4. Computers Electronics and Technology (Ηλεκτρονικοί υπολογιστές και τεχνολογία) επιλέχθηκαν οι ακόλουθες τρεις (3) πλατφόρμες, Google.gr, Facebook.com, Twitter.com, οι οποίες είχαν συνολικά 85.2, 19.1 και 6.8 δισεκατομμύρια χρήστες αντίστοιχα.

**Στάδιο 2ο :** Ουσιαστικά, τα αποτελέσματα της έρευνας στην Similarweb, καταγράφονται σε δύο χωριστές ψηφιακές συλλογές, μία για τις ελεύθερες διαδικτυακές πλατφόρμες και μία για τις ελεύθερες μηχανές αναζήτησης, στη διαδικτυακή πλατφόρμα omeka.net, η οποία δίνει τη δυνατότητα δωρεάν δημιουργίας ψηφιακών συλλογών με βάση το πρότυπο περιγραφής πόρων Dublin Core. Για τους στόχους της παρούσας έρευνας δημιουργήθηκε ένας λογαριασμός (https://kotsakiana.omeka.net/) και η κάθε ελεύθερη διαδικτυακή πλατφόρμα και ελεύθερη μηχανή αναζήτησης αντιμετωπίζεται ως ξεχωριστός πόρος για τον οποίο δίνονται οι ακόλουθες πληροφορίες: μία σύντομη περιγραφή – ορισμός της κάθε ελεύθερης μηχανής αναζήτησης και ιστοσελίδας, σκοποί και αποστολή, ημερομηνία

δημιουργίας, δημιουργός, θέματα – και τέλος κατηγορία στην οποία ανήκει με βάση το εργαλείο Similarweb.

Η συγκεκριμένη μεθοδολογία επιλογής, καταγραφής και παρουσίασης εξυπηρετεί στην εξαγωγή συμπερασμάτων για την ιστορία, τους σκοπούς και την αποστολή των ευρέως χρησιμοποιούμενων ελεύθερων μηχανών αναζήτησης ιστού και ιστοσελίδων. Τα συμπεράσματα αυτά καταγράφονται στο κεφάλαιο 5.2.1 της παρούσας διπλωματικής εργασίας.

**Στάδιο 3ο :** Εκτεταμένη συστηματική βιβλιογραφική επισκόπηση. Ειδικότερα, για τον εντοπισμό των βιβλιογραφικών πηγών, επιλέχθηκαν η βάση δεδομένων ScienceDirect.com | Science, health and medical journals, full text articles and books και η μηχανή αναζήτησης Μελετητής Google. Ο λόγος που επιλέχθηκαν οι συγκεκριμένες βάσεις δεδομένων είναι αφενός ότι η Google Scholar έχει υλικό γενικό, που αφορά πολλές ειδικότητες και είναι μια ευρέως χρησιμοποιούμενη βάση δεδομένων, και αφετέρου η Science Direct είναι μια πιο εξειδικευμένη βάση αποτελεσμάτων με πιο περιορισμένα αποτελέσματα.

Οι λέξεις κλειδιά που χρησιμοποιήθηκαν για την αναζήτηση των βιβλιογραφικών πηγών για τα τέσσερα ερωτήματα αναφορικά με τους πιθανούς κινδύνους που ενέχει η χρήση του Διαδικτύου είναι:

- “cyberbullying”
- “commodification of personal data” και “commercialization of data”
- “identity fraud”
- “netiquette rules”

Τα φίλτρα που χρησιμοποιήθηκαν κατά την αναζήτηση είναι η χρονική περίοδος δημοσίευσης, δηλαδή πηγές που δημοσιεύτηκαν από το έτος 2012 και έπειτα, των οποίων το πλήρες περιεχόμενο έπρεπε να είναι στην αγγλική γλώσσα και στην περίπτωση της Google Scholar, ελεύθερα προσβάσιμο.

**Στάδιο 4ο :** Διαχείριση των πηγών στο πρόγραμμα MS Excel. Για την απάντηση στο καθένα από τα επιμέρους ερωτήματα που τέθηκαν, μελετήθηκαν συνολικά οι **εβδομήντα (70)** πιο σχετικές πηγές.

Πιο συγκεκριμένα, στο Excel καταγράφηκαν αναλυτικά πληροφορίες για τις πηγές που αναζητήθηκαν και επιλέχθηκαν για την ανασκόπηση. Για το κάθε ερώτημα έχουν συμπληρωθεί τέσσερα φύλλα στο Excel. Αυτά είναι:

1. Αποτελέσματα
2. Eligibility Criteria

3. Key concepts
4. Results as APA References

Στο φύλλο **Αποτελέσματα** στην πρώτη στήλη καταγράφηκε η σειρά των αποτελεσμάτων από το 1 ως το 20, δηλαδή ο αριθμός που έπαιρνε το κάθε άρθρο προς μελέτη (π.χ. 1, 2, 3 κλπ.) αφού πρώτα ελεγχόταν η διαθεσιμότητά του. Τα άρθρα που δεν ήταν διαθέσιμα δεν λάμβαναν αυτή την αρίθμηση επειδή απορρίπτονταν. Απλώς κρατήθηκε στη δεύτερη στήλη η αρίθμηση όλων των άρθρων που έφερε η αναζήτηση. Αυτές οι δυο στήλες είναι ίδιες και για τα τέσσερα φύλλα. Στην τρίτη στήλη αναγράφεται η λέξη κλειδί με την οποία έγινε η αναζήτηση και στην τέταρτη στήλη δίνεται ο σύνδεσμος της αναζήτησης. Στην συνέχεια ακολουθούν έντεκα στήλες, στις οποίες αναγράφεται το είδος στο οποίο ανήκει η κάθε πηγή, δηλαδή:

1. Μελέτη / Study
2. Μελέτη περίπτωσης / Case study
3. Ερωτηματολόγιο / Survey
4. Πείραμα / Experiment
5. Βιβλίο / Book
6. Κεφάλαιο βιβλίου / Book Chapter
7. Ανασκόπηση / Review
8. Έκθεση/ αναφορά / Report
9. Έρευνα - Επιστημονικό άρθρο / Research/scientific article
10. Ιστοσελίδα / Website
11. Άλλο / Other

Σε αυτά τα πεδία συμπληρώνονται οι τιμές:

- 0 αν η πηγή δεν ανήκει σε κάποια από τις παραπάνω κατηγορίες
- 1 αν η πηγή ανήκει σε κάποια από τις παραπάνω κατηγορίες
- 2 αν η πηγή δεν είναι διαθέσιμη

Τέλος, στην τελευταία στήλη του πρώτου φύλλου συμπληρώνονται το σύνολο των αποτελεσμάτων.

Στο φύλλο με τίτλο **Eligibility criteria** συμπληρώνονται γενικές πληροφορίες για τα επιλεγμένες πηγές, όπως χρονολογία δημοσίευσης, περίληψη στα ελληνικά και στα αγγλικά και λεπτομέρειες συνάφειας, δηλαδή αν ένα αποτέλεσμα έχει υψηλή, μέτρια, χαμηλή ή καθόλου συνάφεια με το ερώτημα.

Στο τρίτο φύλλο με τίτλο **key concepts** συμπληρώνονται αυτολεξεί αποσπάσματα κειμένου από τις πηγές, τα οποία έχουν επιλεγεί για να χρησιμοποιηθούν στη συγγραφή της διπλωματικής εργασίας. Ανάλογα με τις ανάγκες του κάθε ερωτήματος οι στήλες μπορεί να έχουν ίδιο ή και διαφορετικό όνομα. Για παράδειγμα, σε όλα τα ερωτήματα υπήρχε στήλη με όνομα «Ορισμός των φαινομένων», ή «τρόποι αντιμετώπισης» αλλά στο ερώτημα εμπορευματοποίηση υπάρχει στήλη με τίτλο «κύκλος ζωής των δεδομένων», ενώ στα άλλα δεν υπάρχει.

Τέλος, στο τέταρτο φύλλο με όνομα **Results as APA Reference** συμπληρώνονται οι βιβλιογραφικές αναφορές του κάθε αποτελέσματος με βάση το βιβλιογραφικό πρότυπο APA.

**Στάδιο 5ο :** Σχεδιασμός και παρουσίαση τεσσάρων εκπαιδευτικών σεναρίων για το καθένα από τα τέσσερα ερευνητικά ερωτήματα της διπλωματικής εργασίας. Η δημιουργία τους βασίστηκε στη σελίδα sec.eff.org (n.d.)

Πιο αναλυτικά, το κάθε μάθημα περιλαμβάνει κάποιες γενικές πληροφορίες για το φαινόμενο που παρουσιάζει. Δηλαδή υπάρχουν **οι εισαγωγικές πληροφορίες**, όπου αναλύεται συνοπτικά το φαινόμενο και ο λόγος που είναι απαραίτητη η εκπαιδευτική διαδικασία, **η προτεινόμενη βιβλιογραφία** στην οποία βασίστηκε η θεωρητική ανάλυση του φαινομένου, **προβλήματα που μπορεί να αντιμετωπίσει η διδάσκουσα/ ο διδάσκων** ανάλογα με το κοινό που απευθύνεται, και **συχνές ερωτήσεις και απαντήσεις** που προκύπτουν με την αναφορά του φαινομένου.

Στη δεύτερη ενότητα περιλαμβάνονται πληροφορίες για τη **διάρκεια του μαθήματος**, τους **μαθησιακούς στόχους** και **τα υλικά που απαιτούνται** για να πραγματοποιηθεί το μάθημα. Τέλος, δίνεται το **περιεχόμενο του μαθήματος** και η **εκπαιδευτική μέθοδος** που προτείνεται να ακολουθηθεί για την ολοκλήρωσή του, η οποία συνήθως χωρίζεται σε επιμέρους ενότητες όπως **Προτεινόμενες ερωτήσεις**, **Ομαδική συζήτηση**, **Παιχνίδι ρόλων**, **Παρουσίαση και επεξήγηση του φαινομένου**.

Ο λόγος που αποφασίστηκε να προταθούν αυτά τα ενδεικτικά εκπαιδευτικά σενάρια ήταν το γεγονός ότι η εκπαίδευση των χρηστών και γενικά η ενημέρωση τους για τα φαινόμενα που πραγματεύεται η διπλωματική εργασία, αποτελεί, σύμφωνα με τα αποτελέσματα της βιβλιογραφικής επισκόπησης, έναν από τους αποτελεσματικότερους τρόπος αντιμετώπισης τους.

# Κεφάλαιο 4. Αποτελέσματα – Ευρήματα / Επιτεύγματα

## 4.1 Αναλυτική παρουσίαση αποτελεσμάτων

### 4.1.1 Παρουσίαση δεδομένων

Σύμφωνα με τις κατηγορίες όπως έχουν δοθεί από την σελίδα Similarweb, έγινε καταγραφή των πρώτων τριών ιστοσελίδων από την κάθε κατηγορία. Ο παρακάτω πίνακας αναγράφει την ιστοσελίδα, σε ποια κατηγορία και υποκατηγορία ανήκει, αν είναι διαθέσιμή ελεύθερα ή όχι, καθώς και τους επισκέπτες. Τα αποτελέσματα αφορούν το διάστημα Μάιος 2022.

**Πίνακας 1. Διαδικτυακές εφαρμογές**

| **Θέση** | **ιστοσελίδα** | **Κατηγορία** | **Υποκατηγορία** | **Διαθεσιμότητα** | **Επισκέπτες** |
|---|---|---|---|---|---|
| 1η | Youtube.com | Arts & Entertainment | Streaming &Online TV | ΕΛΕΥΘΕΡΟ | 35.1 B |
| 2η | Netflix.com | Arts & Entertainment | Streaming &Online TV | ΠΛΗΡΩΜΗ | 2.2 B |
| 3η | Bilibili.com | Arts & Entertainment | Animation and comics | ΕΛΕΥΘΕΡΟ | 1.1 B |
| 4η | fandom.com | Arts & Entertainment | Other Arts and Entertainment | ΕΛΕΥΘΕΡΟ | 782.7 M |
| 1η | zillow.com | Business and Consumer Services | Real Estate | ΕΛΕΥΘΕΡΟ | 311.2 M |
| 2η | canadapost-postescanada.ca | Business and Consumer Services | Business Services | ΕΛΕΥΘΕΡΟ | 284.6 M |
| 3η | usps.com | Business and Consumer Services | Shipping and Logistics | ΕΛΕΥΘΕΡΟ | 248.7 M |

| | | | | | |
|---|---|---|---|---|---|
| 1η | jw.org | Community and Society | Faith and Beliefs | ΕΛΕΥΘΕΡΟ | 220.0 M |
| 2η | tinder.com | Community and Society | Dating and Relationships | ΕΛΕΥΘΕΡΟ | 114.1 M |
| 3η | livehdcams.com | Community and Society | Dating and Relationships | ΕΛΕΥΘΕΡΟ | 78.2 M |
| 1η | google.com | Computers Electronics and Technology | Search Engines | ΕΛΕΥΘΕΡΟ | 89.0 B |
| 2η | facebook.com | Computers Electronics and Technology | Social Media Networks | ΕΛΕΥΘΕΡΟ | 19.7 B |
| 3η | twitter.com | Computers Electronics and Technology | Social Media Networks | ΕΛΕΥΘΕΡΟ | 7.1 B |
| 1η | amazon.com | eCommerce & Shopping | Marketplace | ΕΛΕΥΘΕΡΟ | 2.4 B |
| 2η | Ebay.com | eCommerce & Shopping | Marketplace | ΕΛΕΥΘΕΡΟ | 772.7 M |
| 3η | amazon.co.jp | eCommerce & Shopping | Marketplace | ΕΛΕΥΘΕΡΟ / Ίδιο με 1ο | 612.6 M |
| 4η | rakuten.co.jp | eCommerce & Shopping | Marketplace | ΕΛΕΥΘΕΡΟ | 503.8 M |
| 1η | paypal.com | Finance | Banking Credit and Lending | ΕΛΕΥΘΕΡΟ | 507.8 M |
| 2η | tradingview.com | Finance | Investing | ΠΛΗΡΩΜΗ | 205.2 M |
| 3η | coinmarketcap.com | Finance | Investing | ΕΛΕΥΘΕΡΟ | 194.1 M |
| 4η | caixa.gov.br | Finance | Banking Credit and Lending | ΕΛΕΥΘΕΡΟ | 161.3M |

| | | | | | |
|---|---|---|---|---|---|
| 1η | trilltrill.jp | Food and Drink | Other food and drink | ΕΛΕΥΘΕΡΟ | 235.1 M |
| 2η | Cookpad.com | Food and Drink | Cooking and recipes | ΕΛΕΥΘΕΡΟ | 127.5 M |
| 3η | Tabelog.com | Food and Drink | Other food and drink | ΕΛΕΥΘΕΡΟ | 101.5 M |
| 1η | Bet365.com | Gambling | Sports Betting | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 284.3 M |
| 2η | Hdvideosnet.com | Gambling | Sports Betting | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 194.4 M |
| 3η | Pgjazz.com | Gambling | Sports Betting | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 144.9 M |
| 4η | thaudray.com | Gambling | Casinos | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 128.4M |
| 5η | eshkol.io | Gambling | Other Gambling | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 121.9M |
| 6η | caliente.mx | Gambling | Other Gambling | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 108.8M |
| 7η | xosodaiphat.com | Gambling | Lottery | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 108.2M |
| 1η | Twitch.tv | Games | Video Games consoles and accessories | ΕΛΕΥΘΕΡΟ | 1.2 B |
| 2η | Roblox.com | Games | Video Games consoles and accessories | ΕΛΕΥΘΕΡΟ | 995.3 M |

| | | | | | |
|---|---|---|---|---|---|
| 3η | Steampowered.com | Games | Video Games consoles and accessories | ΕΛΕΥΘΕΡΟ | 153.7 M |
| 1η | Healthline.com | Health | Other health | ΕΛΕΥΘΕΡΟ | 239.1 M |
| 2η | Nih.gov | Health | Other health | ΧΩΡΙΣ ΠΡΟΣΒΑΣΗ | 219.6 M |
| 3η | Webmd.com | Health | Health conditions and concers | ΕΛΕΥΘΕΡΟ | 140.7 M |
| 1η | Edf.fr | Heavy Industry and engineering | Energy industry | ΕΛΕΥΘΕΡΟ | 10.8 M |
| 2η | Skyscrapercity.com | Heavy Industry and engineering | Architecture | ΕΛΕΥΘΕΡΟ | 9.6 M |
| 3η | Qcc.com | Heavy Industry and engineering | Construction and maintenance | ΠΛΗΡΩΜΗ | 9.6 M |
| 4η | grainger.com | Heavy Industry and engineering | Construction and maintenance | ΕΛΕΥΘΕΡΟ | 9.7M |
| 1η | Shutterstock.com | Hobbies and Leisure | Photography | ΠΛΗΡΩΜΗ / ΜΕ ΟΡΙΟ | 66.4 M |
| 2η | Flickr.com | Hobbies and Leisure | Photography | ΕΛΕΥΘΕΡΟ / ΠΛΗΡΩΜΗ | 55.7 M |
| 3η | ancestry.com | Hobbies and Leisure | Ancestry and Genealogy | ΠΛΗΡΩΜΗ / ΜΕ ΟΡΙΟ | 47.1 M |
| 1η | Homedepot.com | Home and garden | Other home and garden | ΕΛΕΥΘΕΡΟ | 220.6 M |
| 2η | Ikea.com | Home and garden | Furniture | ΕΛΕΥΘΕΡΟ | 161.7 M |
| 3η | Lowes.com | Home and garden | Home improvement and maintenance | ΕΛΕΥΘΕΡΟ | 148.8 M |
| 1η | Indeed.com | Jobs and Career | Jobs and Employment | ΕΛΕΥΘΕΡΟ | 665.2 M |
| 2η | Myworkdayjobs.com | Jobs and Career | Jobs and Employment | ΧΩΡΙΣ ΠΡΟΣΒΑΣΗ | 59.3 M |

| | | | | | |
|---|---|---|---|---|---|
| 3η | Glassdoor.com | Jobs and Career | Jobs and Employment | ΕΛΕΥΘΕΡΟ | 51.9 M |
| 4η | hh.ru | Jobs and Career | Jobs and Employment | ΕΛΕΥΘΕΡΟ | 76.0M |
| 1η | Gov.uk | Law and Government | Government | ΕΛΕΥΘΕΡΟ | 158.2 M |
| 2η | Service.gov.uk | Law and Government | Government | ΕΛΕΥΘΕΡΟ / ΙΔΙΟ ΜΕ ΤΟ 1ο | 146.9 M |
| 3η | Gosuslugi.ru | Law and Government | Government | ΕΛΕΥΘΕΡΟ | 108.5 M |
| 4η | turkiye.gov.tr | Law and Government | Government | ΕΛΕΥΘΕΡΟ | 105.1 M |
| 1η | Linktr.ee | Lifestyle | Other lifestyle | ΕΛΕΥΘΕΡΟ | 170.4 M |
| 2η | Shein.com | Lifestyle | Fashion and apparel | ΕΛΕΥΘΕΡΟ | 169.2 M |
| 3η | Nike.com | Lifestyle | Fashion and apparel | ΕΛΕΥΘΕΡΟ | 127.3 M |
| 1η | Yahoo.com | News & Media Publishers | | ΕΛΕΥΘΕΡΟ | 3.5 B |
| 2η | Yahoo.co.jp | News & Media Publishers | | ΕΛΕΥΘΕΡΟ / ΙΔΙΟ ΜΕ 1ο | 2.4 B |
| 3η | Naver.com | News & Media Publishers | | ΕΛΕΥΘΕΡΟ | 1.2 B |
| 4η | qq.com | News & Media Publishers | | ΕΛΕΥΘΕΡΟ | 957.8 M |
| 1η | Chewy.com | Pets and Animals | Pet Food and Supplies | ΕΛΕΥΘΕΡΟ | 46.3 M |
| 2η | Vegamovies.cam | Pets and Animals | Pet Food and Supplies | ΕΛΕΥΘΕΡΟ / χωρίς πρόσβαση | 35.2 M |
| 3η | Petfinder.com | Pets and Animals | Pets | ΕΛΕΥΘΕΡΟ | 16.8 M |
| 4η | thedodo.com | Pets and Animals | Pet Food and Supplies | ΕΛΕΥΘΕΡΟ | 10 M |

| | | | | | |
|---|---|---|---|---|---|
| 1η | Wikipedia.org | Reference Materials | Dictionaries and Encyclopedias | ΕΛΕΥΘΕΡΟ | 5.1 b |
| 2η | Quora.com | Reference Materials | Dictionaries and Encyclopedias | ΕΛΕΥΘΕΡΟ | 579.8 M |
| 3η | Deepl.com | Reference Materials | Dictionaries and Encyclopedias | ΕΛΕΥΘΕΡΟ / με όριο | 314.5 M |
| 1η | Accuweather.com | Science and Education | Weather | ΕΛΕΥΘΕΡΟ | 804.8 M |
| 2η | Weather.com | Science and Education | Weather | ΕΛΕΥΘΕΡΟ | 735.2 M |
| 3η | Instructure.com | Science and Education | Education | ΕΛΕΥΘΕΡΟ | 363.8 M |
| 1η | Espn.com | Sports | Other sports | ΕΛΕΥΘΕΡΟ | 488.5 M |
| 2η | Marca.com | Sports | Other sports | ΕΛΕΥΘΕΡΟ | 260.2 M |
| 3η | As.com | Sports | Other sports | ΕΛΕΥΘΕΡΟ | 227.0 M |
| 1η | Booking.com | Travel and Tourism | Accommodation and Hotels | ΕΛΕΥΘΕΡΟ | 564.1 M |
| 2η | Tripadvisor.com | Travel and Tourism | Other travel and tourism | ΕΛΕΥΘΕΡΟ | 167.1 M |
| 3η | Airbnb.com | Travel and Tourism | Accommodation and Hotels | ΕΛΕΥΘΕΡΟ | 99.4 M |
| 1η | Dongchedi.com | Vehicles | Other Vehicles | ΕΛΕΥΘΕΡΟ | 95.2 M |
| 2η | Motorbiscuit.com | Vehicles | Other Vehicles | ΕΛΕΥΘΕΡΟ | 65.8 M |
| 3η | Drom.ru | Vehicles | Other Vehicles | ΧΩΡΙΣ ΠΡΟΣΒΑΣΗ | 62.6 M |
| 4η | autohome.com.cn | Vehicles | Other Vehicles | ΕΛΕΥΘΕΡΟ | 53.6 M |
| 1η | Xvideos | Adult | | | 3.3 B |
| 2η | Xnxx.com | Adult | | | 2.5 B |
| 3η | Pornhub.com | Adult | | | 2.3 B |

Επιπλέον, η πλατφόρμα Similarweb παρέχει λίστα με τις ευρέως χρησιμοποιούμενες μηχανές αναζήτησης για το διάστημα Μάιος 2022.

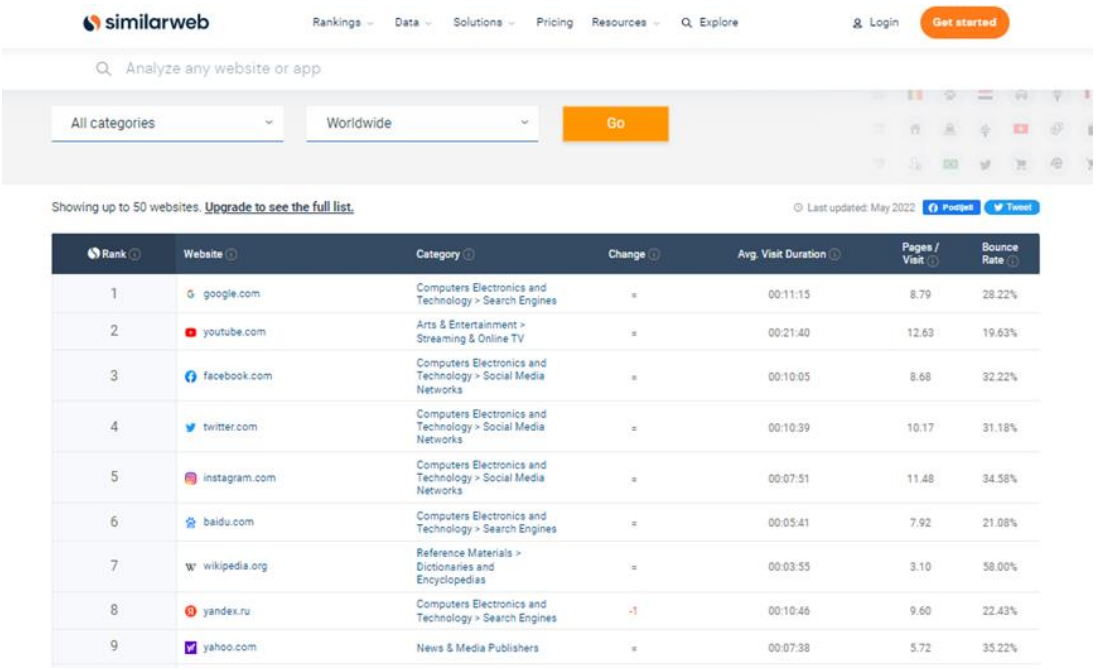
Αυτές συμπεριλαμβάνονται στο παρακάτω πίνακα.

**Πίνακας 2. Μηχανές αναζήτησης**

| **Θέση** | **Μηχανή αναζήτησης** | **Κατηγορία** | **Επισκεψιμότητα** |
|---|---|---|---|
| 1η | **Google.com** | Search Engines | 90.95% |
| 2η | **Yahoo.com** | Search Engines | 3.02% |
| 3η | **Bing.com** | Search Engines | 2.82% |
| 4η | **Naver.com** | Search Engines | 0.48% |
| 5η | **Yandex.com** | Search Engines | 0.47% |

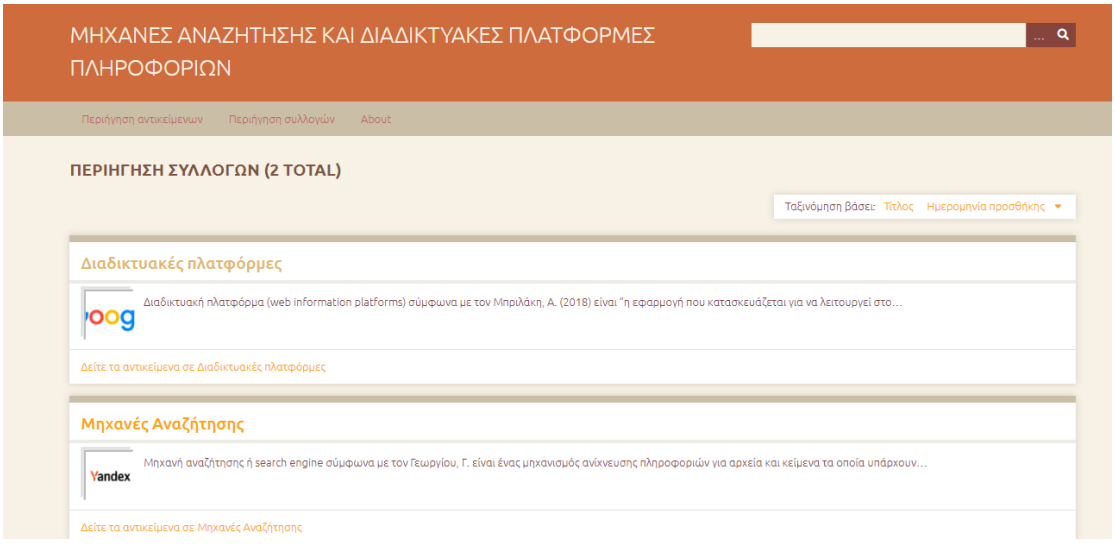
Παρακάτω δίνονται κάποια στιγμιότυπα οθόνης από την ιστοσελίδα Similarweb. Αρχικά, φαίνεται το χρονικό διάστημα που αντλήθηκαν τα δεδομένα (Εικόνα 1.) και στη συνέχεια, δίνεται ένα στιγμιότυπο οθόνης της σελίδας Similarweb που δείχνει κάποιες από τις κατηγορίες και τις υπο-κατηγορίες των πλατφορμών και πώς τις κατατάσσει (Εικόνα 2.)


**Εικόνα 1. Σελίδα similarweb**




**Εικόνα 2. Κατάταξη ιστοσελίδων στο similarweb**

Ακόμα, δίνονται κάποια στιγμιότυπα οθόνης της πλατφόρμας omeka.net, και συγκεκριμένα των συλλογών που έχουν δημιουργηθεί (Εικόνα 3. ) και των εγγραφών / αντικειμένων (Εικόνα 4.). Επίσης, δίνονται εικόνες που παρουσιάζουν μία ολοκληρωμένη εγγραφή και των πεδίων που έχουν συμπληρωθεί (Εικόνες 5., 6., 7., 8.)




**Εικόνα 3. Συλλογή δεδομένων στο Omeka.net Συλλογές**


**Εικόνα 4. Συλλογή δεδομένων στο omeka.net Αντικείμενα**


**Εικόνα 5. Παρουσίαση αντικειμένου στο omeka.net 1/4**

## Τίτλος

Youtube.com

## Θέμα

Arts & Entertainment

Τέχνες & Ψυχαγωγία

Streaming &Online TV

Ροή & Διαδικτυακή τηλεόραση

## Περιγραφή

**Περιγραφη** (Wikipedia.com,2022):
Το YouTube είναι μια αμερικανική διαδικτυακή πλατφόρμα κοινής χρήσης βίντεο και κοινωνικών μέσων με έδρα το Σαν Μπρούνο της Καλιφόρνια. Αυτήν τη στιγμή ανήκει στην Google και είναι ο δεύτερος ιστότοπος με τις περισσότερες επισκέψεις, μετά την Αναζήτηση Google.

**Description** (Wikipedia.com,2022): YouTube is an American online video sharing and social media platform based in San Bruno, California. It is currently owned by Google and is the second most visited website after Google search.

**Στόχοι** (Youtube.com,2022):
Οι βασικές αξίες του YouTube περιλαμβάνουν «ελευθερία έκφρασης, ελευθερία πληροφόρησης, ελευθερία ευκαιριών, ελευθερία του ανήκειν». Το YouTube αποκαλεί αυτές τις αξίες τις βασικές του ελευθερίες σύμφωνα με τον σκοπό για τον οποίο ιδρύθηκε η εταιρεία – δίνοντας φωνή.
Με τις τέσσερις αξίες του, το YouTube δημιουργεί ένα περιβάλλον όπου οι άνθρωποι έχουν την ευκαιρία να μοιραστούν ιδέες, να αποκτήσουν πρόσβαση σε οποιαδήποτε πληροφορία αναζητούν, να αρπάξουν ευκαιρίες για νέες ανακαλύψεις και να ανήκουν σε μια κοινότητα. Ένα τέτοιο περιβάλλον αντικατοπτρίζει όλα όσα αντιπροσωπεύει το YouTube.

**Εικόνα 6. Παρουσίαση αντικειμένου στο omeka.net 2/4**

**Goals** (Youtube.com,2022):
YouTube core values comprise "freedom of expression, freedom of information, freedom of opportunity, freedom to belong." YouTube calls these values its essential freedoms in line with the purpose for which the company was founded – giving a voice.
With its four values, YouTube creates an environment where people get an opportunity to share ideas, access any information they are looking for, grab chances for new discoveries, and belong to a community. Such an environment reflects everything that YouTube stands for.

**Αποστολή** (Youtube.com,2022):
Η αποστολή του Youtube είναι να δώσει σε όλους φωνή και να δείξει ότι ο κόσμος είναι καλύτερος όταν ακούει, μοιράζεται και δημιουργεί κοινότητες μέσα από τις ιστορίες που μοιράζεται.

**Mission** (Youtube.com,2022) :
Youtube's mission is to give everyone a voice and to show that the world is better for listening, sharing and building communities through the stories it shares.

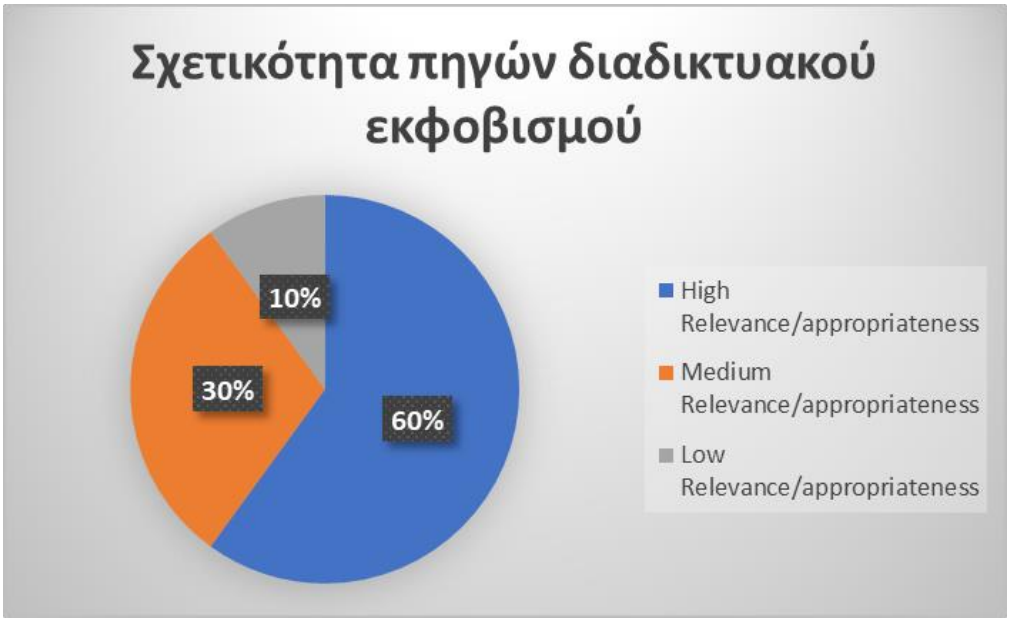
**Σύντομη ιστορία** (Wikipedia.com, 2022):
Το YouTube ιδρύθηκε από τους Steve Chen, Chad Hurley και Jawed Karim. Οι τρεις ήταν πρώτοι υπάλληλοι του PayPal, κάτι που τους άφησε πλούσιους μετά την αγορά της εταιρείας από το eBay.
Το YouTube ξεκίνησε ως startup τεχνολογίας που χρηματοδοτείται από επιχειρηματικά κεφάλαια. Μεταξύ Νοεμβρίου 2005 και Απριλίου 2006, η εταιρεία συγκέντρωσε χρήματα από διάφορους επενδυτές με τη Sequoia Capital, 11,5 εκατομμύρια δολάρια, και την Artis Capital Management, 8 εκατομμύρια δολάρια, να είναι οι δύο μεγαλύτεροι.
Τον Φεβρουάριο του 2005, η εταιρεία ενεργοποίησε το www.youtube.com. Το πρώτο βίντεο ανέβηκε στις 23 Απριλίου 2005. Τον Μάιο, η εταιρεία ξεκίνησε μια δημόσια beta και μέχρι τον Νοέμβριο, μια διαφήμιση της Nike με τον Ronaldinho έγινε το πρώτο βίντεο που έφτασε το ένα εκατομμύριο συνολικές προβολές. Ο ιστότοπος ξεκίνησε επίσημα στις 15 Δεκεμβρίου 2005, οπότε ο ιστότοπος λάμβανε 8 εκατομμύρια προβολές την ημέρα. Τα κλιπ εκείνη την εποχή περιορίζονταν στα 100 megabyte, μόλις 30 δευτερόλεπτα πλάνα.

**Εικόνα 7. Παρουσίαση αντικειμένου στο omeka.net 3/4**


**Εικόνα 8. Παρουσίαση αντικειμένου στο omeka.net 4/4**

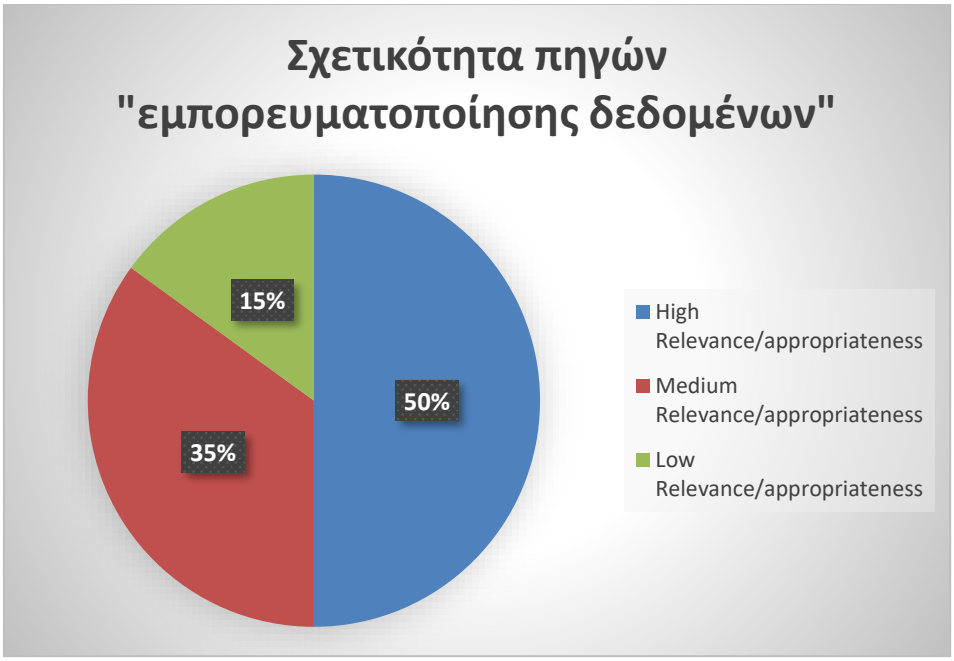
### 4.1.2 Παρουσίαση αποτελεσμάτων βιβλιογραφικής επισκόπησης

Σε αυτό το κεφάλαιο δίνονται γραφήματα που παρέχουν πληροφορίες για τη σχετικότητα των βιβλιογραφικών πηγών των ερωτημάτων. Στη συνέχεια, δίνονται διαγράμματα που αντιστοιχούν στα στατιστικά των ειδών των βιβλιογραφικών πηγών, αν πρόκειται δηλαδή για επιστημονικά άρθρα ή μελέτες ή άλλα είδη. Τέλος, έχουν προστεθεί γραφήματα που απεικονίζουν τα ποσοστά των πηγών ανά έτος δημοσίευσης. Για παράδειγμα, το ποσοστό επί τις εκατό από αυτά που έχουν δημοσιευθεί το 2012 ή το 2022.



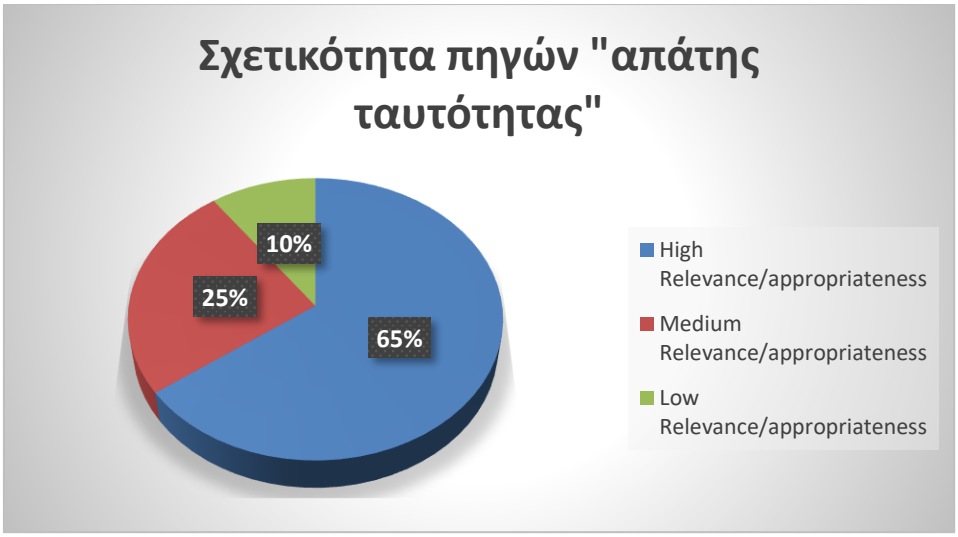

**Εικόνα 9. Σχετικότητα βιβλιογραφικών πηγών cyberbullying**

Το 60% των πηγών του διαδικτυακού εκφοβισμού έχουν υψηλή συνάφεια με το θέμα, το 30% μέτρια συνάφεια και το 10% χαμηλή συνάφεια (Εικόνα 9.).



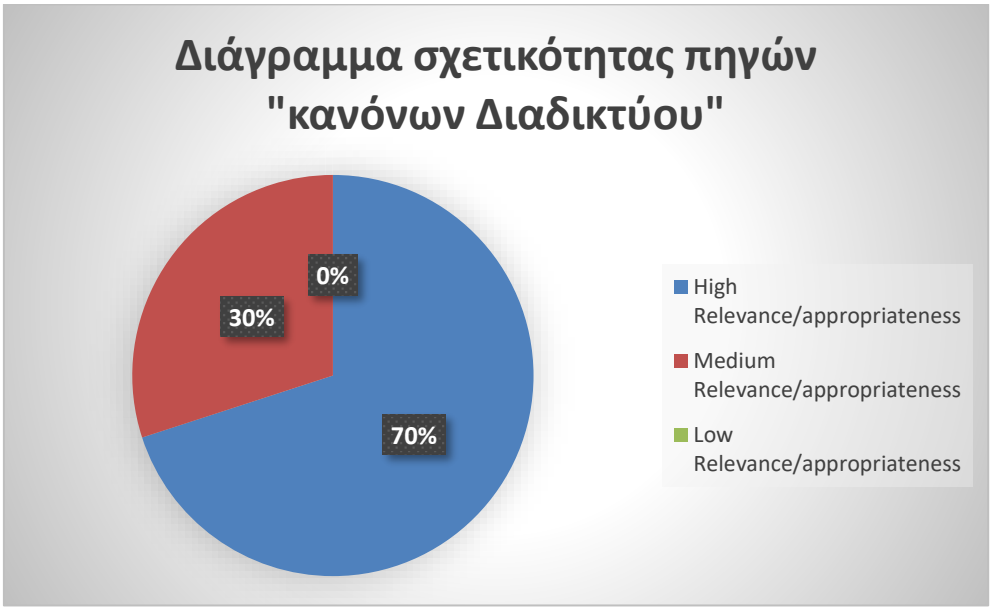

**Εικόνα 10. Σχετικότητα βιβλιογραφικών πηγών commodification of personal data**

Το 50% των πηγών για την εμπορευματοποίηση δεδομένων έχουν υψηλή συνάφεια με το θέμα, το 35% μέτρια συνάφεια και το 15% χαμηλή συνάφεια (Εικόνα 10.).




**Εικόνα 11. Σχετικότητα βιβλιογραφικών πηγών identity fraud**

Το 65% των πηγών για την απάτη ταυτότητας έχουν υψηλή συνάφεια με το θέμα, το 25% μέτρια συνάφεια και το 10% χαμηλή συνάφεια (Εικόνα 11.).

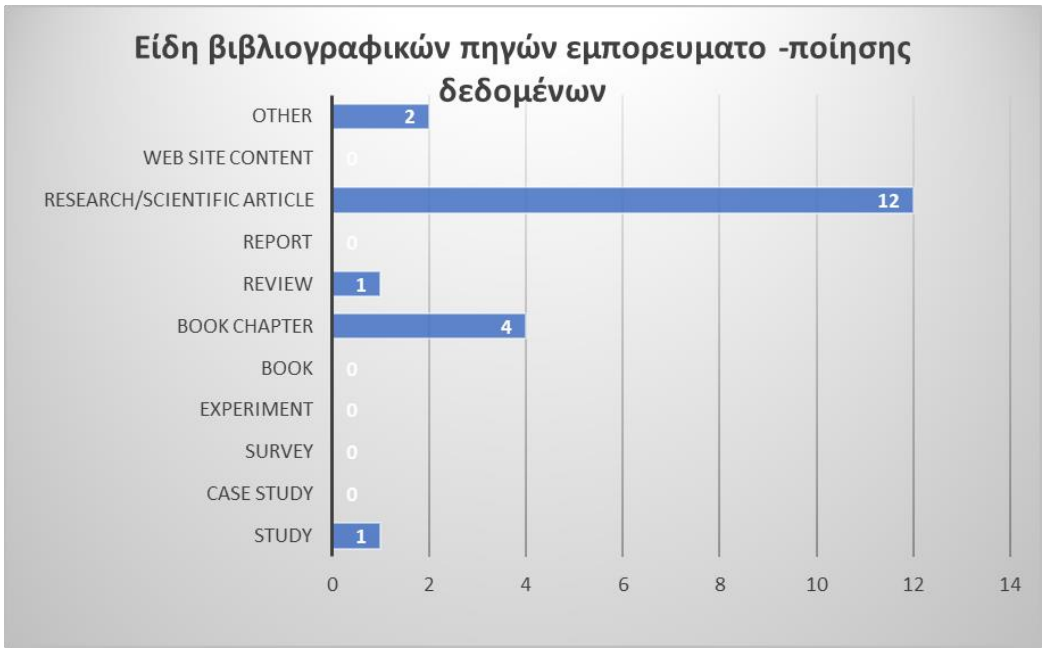



**Εικόνα 12. Σχετικότητα βιβλιογραφικών πηγών netiquette rules**

Το 70% των πηγών για τους κανόνες του Διαδικτύου έχουν υψηλή συνάφεια με το θέμα και το 30% μέτρια συνάφεια. (Εικόνα 12.).


**Εικόνα 13. Στατιστικά για τα είδη των πηγών του cyberbullying**

Από τις είκοσι πηγές που μελετήθηκαν διεξοδικά, εννιά (9) ήταν Έρευνες / Επιστημονικά άρθρα, εννιά (9) ήταν Μελέτες, μία (1) ήταν Κεφάλαιο από βιβλίο και μία (1) πηγή ήταν Μελέτη περίπτωσης (Εικόνα 13.).



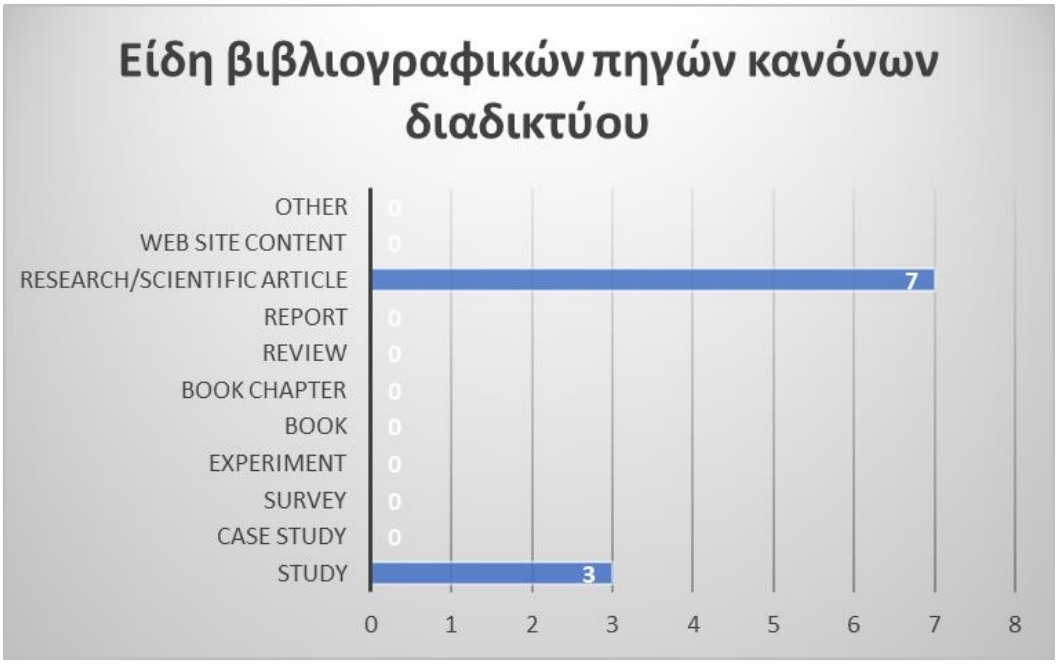

**Εικόνα 14. Στατιστικά για τα είδη των πηγών commodification of data**

Από τις είκοσι πηγές που μελετήθηκαν διεξοδικά, οι δώδεκα (12) ήταν Έρευνες / Επιστημονικά άρθρα, τέσσερις (4) ήταν Κεφάλαιο από βιβλίο, δυο (2) άλλο είδος και

συγκεκριμένα Εργασία συνεδρίου, μία (1) πηγή ήταν Μελέτη και μία (1) πηγή ήταν αναφορά (Εικόνα 14.).


**Εικόνα 15. Στατιστικά για τα είδη των πηγών identity fraud**

Από τις είκοσι πηγές που μελετήθηκαν διεξοδικά, οι δεκατέσσερις (14) ήταν Έρευνες / Επιστημονικά άρθρα, πέντε (5) πηγές ήταν Μελέτη και μία (1) πηγή ήταν αναφορά (Εικόνα 15.).




**Εικόνα 16. Στατιστικά για τα είδη των πηγών netiquette rules**

Από τις δέκα πηγές που μελετήθηκαν διεξοδικά, οι επτά (7) ήταν Έρευνες / Επιστημονικά άρθρα και οι τρεις (3) ήταν Μελέτη (Εικόνα 16.).


**Εικόνα 17. Στατιστικά για τις χρονολογίες των πηγών του cyberbullying**

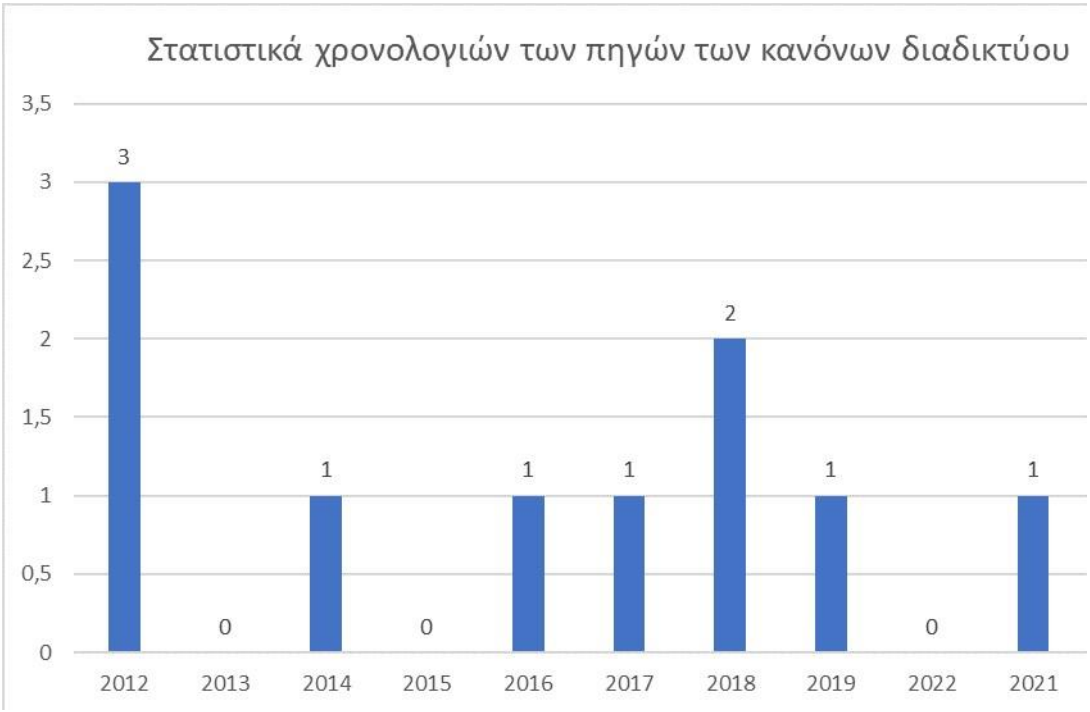
Το μεγαλύτερο ποσοστό πηγών δημοσιεύτηκε το 2020, το 2013 και το 2021. Ενώ το 2014, το 2016 και το 2019 δεν δημοσιεύτηκε καμία πηγή (Εικόνα 17.).


**Εικόνα 18. Στατιστικά για τις χρονολογίες των πηγών του commodification of personal data**

Το μεγαλύτερο ποσοστό πηγών δημοσιεύτηκε το 2018 και το 2019 (Εικόνα 18.).


**Εικόνα 19. Στατιστικά για τις χρονολογίες των πηγών του identity fraud**

Το μεγαλύτερο ποσοστό πηγών δημοσιεύτηκε το 2019, το 2012 και το 2014. (Εικόνα 19.).




**Εικόνα 20. Στατιστικά για τις χρονολογίες των πηγών του netiquette rules**

Το μεγαλύτερο ποσοστό πηγών δημοσιεύτηκε το 2012 και το 2018 (Εικόνα 20.), ενώ τα έτη 2013, 2015 και 2022 δεν δημοσιεύτηκε κάποια σχετική με το θέμα μας πηγή.

## 4.2 Κυριότερα ευρήματα/ αποτελέσματα

Στο συγκεκριμένο κεφάλαιο με τίτλο κυριότερα ευρήματα/αποτελέσματα, κρίθηκε ότι το σημαντικότερο απότοκο της συστηματικής βιβλιογραφικής έρευνας που έγινε στο πλαίσιο της παρούσας διπλωματικής εργασίας, είναι οι τρόποι καταπολέμησης των συχνότερων φαινομένων που αντιμετωπίζει ο χρήστης στο ελεύθερο Διαδίκτυο, αλλά και οι τρόποι ενημέρωσης για τους κώδικες δεοντολογικής συμπεριφοράς που οφείλει να γνωρίζει και να εφαρμόζει. Για το λόγο αυτό, τα τέσσερα υποκεφάλαια που ακολουθούν παρουσιάζουν τους τρόπους αντιμετώπισης και ενημέρωσης για τα θέματα αυτά. Ενώ, στο τελευταίο υποκεφάλαιο (4.3) προτείνονται αντίστοιχα, τέσσερα εκπαιδευτικά σενάρια, τα οποία απευθύνονται σε εκπαιδευτικούς και επιστήμονες της πληροφόρησης οι οποίες/οι επιθυμούν να αναλάβουν σχετική δράση.

### 4.2.1 Τρόποι αντιμετώπισης του διαδικτυακού εκφοβισμού

Όπως αναφέρθηκε διεξοδικά ο διαδικτυακός εκφοβισμός είναι ένα φαινόμενο το οποίο επιφέρει τεράστιες επιπτώσεις στα θύματα και στους θύτες, τόσο σωματικές όσο και συναισθηματικές, ενώ έχει παρατηρηθεί ότι η θυματοποίηση του διαδικτυακού εκφοβισμού προκαλεί αρνητικά συναισθήματα αρκετά στρεσογόνα, τα οποία στη συνέχεια οδηγούν σε αποκλίνουσες συμπεριφορές.

Όλα αυτά καθιστούν σαφές ότι το πρόβλημα πρέπει να αντιμετωπιστεί σωστά και ότι πρέπει να καταβληθούν προσπάθειες για την πρόληψη και την ανταπόκρισή του, ώστε οι νέοι να εξοπλιστούν με τρόπους που τους δίνουν τη δυνατότητα να μειώσουν τον δικό τους κίνδυνο θυματοποίησης (Sabella et al., 2013). Για να μειωθεί το φαινόμενο χρειάζονται ολοκληρωμένες και συλλογικές προσπάθειες μεταξύ διαφόρων υποστηρικτών της νεολαίας, με τους βασικούς να είναι οι σχολικοί σύμβουλοι.

Αρχικά, οι περισσότεροι ερευνητές (Chillemi et al., 2020; Dou et al., 2020; Englander et al., 2017; Ifon, 2022; Kavuk-Kalender & Keser, 2018; Lee et al., 2021; Sabella et al., 2013; Watts et al., 2017) συμφωνούν ότι ο καλύτερος τρόπος αντιμετώπισης είναι η ενημέρωση, καθώς η προσφορά πληροφοριών και η ανάπτυξη σχετικών δεξιοτήτων θα χρησιμεύσουν στην αντιμετώπιση του (Sabella et al., 2013). Η ενημέρωση μπορεί να πραγματοποιηθεί με πολλούς τρόπους και να αφορά τους νέους, τους γονείς αλλά και τους εκπαιδευτικούς.

Οι σχολικοί σύμβουλοι μπορούν να ακολουθήσουν, σύμφωνα με τους Englander et al. (2017) μία σειρά βημάτων για να ενημερώσουν τους γονείς. Αυτά είναι :

- Ενημέρωση για το τι είναι ψηφιακές συσκευές, τι είναι διαδικτυακός εκφοβισμός και ποια είναι τα είδη αυτού
- Ενθάρρυνση να συζητούν σε τακτική βάση με τα παιδιά τους για τη δραστηριότητα τους στο Διαδίκτυο, τις ψηφιακές τους δραστηριότητες και γενικά τυχόν προβλήματα που αντιμετωπίζουν
- Ενθάρρυνση να ακούν και να υποστηρίζουν τους νέους με ψυχραιμία ακόμα και όταν δεν καταλαβαίνουν
- Ενθάρρυνση να μοιράζονται τυχόν προβληματισμούς με ειδικούς, ούτως ώστε, αφενός να αποκτούν μία εμπεριστατωμένη άποψη για το πρόβλημα και αφετέρου για να παρέχουν σωστή καθοδήγηση στα παιδιά

Όσον αφορά τους εκπαιδευτικούς, θα πρέπει να συμβαδίζουν με την νέα τεχνολογία και να έχουν δεχτεί σχετική ενημέρωση για τους κινδύνους του Διαδικτύου, το φαινόμενο του διαδικτυακού εκφοβισμού και τους πιθανούς τρόπους αντιμετώπισης του. Όλα τα παραπάνω είναι απαραίτητα να τα γνωρίζουν, διότι έχει παρατηρηθεί πως η έλλειψη κατανόησης και εκπαίδευσής προκαλεί λανθασμένες αντιδράσεις και περιορίζει την βοήθεια που μπορεί να προσφέρουν (Sabella et al., 2013).

Παράλληλα, σχετικά με την εκπαίδευση των νέων, θα πρέπει να τους παρέχεται ενημέρωση για (Sabella et al., 2013):

- το Διαδίκτυο και τους κινδύνους του
- το φαινόμενο του διαδικτυακού εκφοβισμού
- τις νομικές και συναισθηματικές συνέπειες του
- τους διάφορους τρόπους επίλυσης κοινωνικών προβλημάτων
- τους τρόπους αναγνώρισης και διαχείρισης των συναισθημάτων τους και συμβουλές για το πως να χρησιμοποιούν με ασφάλεια το Διαδίκτυο

Ένας ακόμα τρόπος ενημέρωσης και εκπαίδευσης των νέων σύμφωνα με τους Ifon (2022); Kavuk-Kalender & Keser (2018); Watts et al. (2017) είναι μέσω της αλληλεπίδρασης με άλλους νέους. Αυτό θα επιτευχθεί με το να μιλήσουν μεγαλύτεροι μαθητές σε μικρότερους, για το Διαδίκτυο, τις δυνατότητες του, τους κινδύνους που ελλοχεύει, το φαινόμενο του διαδικτυακού εκφοβισμού και τυχόν συνέπειες που προκαλεί. Αυτή η αλληλεπίδραση θα φέρει καλύτερη επικοινωνία μεταξύ των νέων, και θα αυξήσει τα επίπεδα ευαισθητοποίησης.

Από την άλλη, οι Chillemi et al. (2020); Dou et al. (2020); Ifon (2022); Sabella et al. (2013) θεωρούν ως τρόπο αντιμετώπισης του φαινομένου τη δημιουργία σεμιναρίων και εκπαιδευτικών ενημερωτικών προγραμμάτων. Τα προγράμματα αυτά θα παρέχουν παραδείγματα διαδικτυακού εκφοβισμού, συμβουλές και πιθανούς τρόπους αντιμετώπισης του κάθε παραδείγματος. Επίσης, σαν εκπαιδευτικό πρόγραμμα μπορεί να δημιουργηθεί ένα παιχνίδι ρόλων και δημιουργίας σεναρίων. Στο πλαίσιο αυτό θα μπορούσαν οι ειδικοί να φέρνουν σαν δεδομένο ένα παράδειγμα διαδικτυακού εκφοβισμού και να προτείνουν στις ομάδες ενημέρωσης, τη δημιουργία σεναρίων, στα οποία θα αναπτύσσουν το πρόβλημα και τις συνέπειες που αυτό προκαλεί τόσο στο θύμα, όσο και στο θύτη, αλλά και σε όσους εμπλέκονται σε αυτό. Αυτό θα προσφέρει μία πολυδιάστατη ανάλυση του θέματος, διότι θα αναλύονται όλες οι πιθανές εκδοχές του προβλήματος.

Ένας ακόμη τρόπος αντιμετώπισης σύμφωνα με τους Sabella et al. (2013) και Watts et al. (2017) είναι η δημιουργία πολιτικών και νομικών διαδικασιών. Έρευνες έχουν δείξει ότι η ανάπτυξη κατάλληλων πολιτικών στο σχολικό περιβάλλον, αλλά και η διατήρηση τους, μπορεί να περιορίσει το φαινόμενο και να κρατήσει ασφαλείς τους μαθητές. Παράλληλα, το ίδιο ισχύει και για όλα τα περιβάλλοντα, όπως το εργασιακό. Η ανάπτυξη και η διατήρηση πολιτικών κατά του διαδικτυακού εκφοβισμού μπορεί να προκαλέσει μείωση του φαινομένου. Οι απόψεις ωστόσο διίστανται, διότι οι Pennell et al. (2022) θεωρούν ότι αυτή η στρατηγική «είναι άκαμπτο μέσο» και ανίκανο να δράσει κατασταλτικά για το φαινόμενο.

Τέλος, οι Ifon (2022) και Watts et al. (2017) αναφέρουν σαν τρόπο αντιμετώπισης, τη δημιουργία ενός κεντρικού λογαριασμού email ή ενός επίσημου καναλιού αναφοράς και τεκμηρίωσης περιπτώσεων διαδικτυακού εκφοβισμού, τα οποία θα συνδράμουν στην διαχείριση των θυμάτων και των θυτών, θα παρέχουν άμεση υποστήριξη και συμβουλές, και θα είναι ένας άμεσος τρόπος παροχής βοήθειας στα θύματα, καθώς θα είναι διαθέσιμο 24ώρες το 24ωρο, ηλεκτρονικά και χωρίς να προϋποθέτει φυσική παρουσία, κάτι που φαίνεται να λύνει το πρόβλημα της συστολής εκμυστήρευσης του φαινομένου (Watts et al., 2017).

### 4.2.2 Στρατηγικές βελτίωσης του φαινομένου της εμπορευματοποίησης των προσωπικών δεδομένων

Για όλους τους λόγους που αναφέρθηκαν στα παραπάνω κεφάλαια είναι ιδιαίτερα αναγκαίο να χαραχθεί στρατηγική διαφύλαξης των προσωπικών δεδομένων.

Ο Versaci (2018), αναφέρει ότι η βάση πάνω στην οποία πρέπει να στηριχθεί η προστασία των προσωπικών δεδομένων είναι ο έλεγχος των προσωπικών πληροφοριών και όχι το

απόρρητο αυτών. Πάνω σε αυτό στηρίχθηκαν οι Vom Lehn et al. (2014), οι οποίοι στην μελέτη τους ανέφεραν ένα πρόγραμμα περιήγησης ιστού της εταιρείας Good data. Το πρόγραμμα αυτό, αφού το εγκαταστήσουν οι χρήστες, μπλοκάρει την παρακολούθηση των δεδομένων από τρίτους παρόχους υπηρεσιών και αντ' αυτού τα καταγράφει. Έπειτα, ο χρήστης μπορεί να επιλέξει ποια δεδομένα από αυτά που έχουν καταγραφεί, θα παράσχει στην εταιρεία, για να πουληθούν ανώνυμα στους μεσίτες δεδομένων. Μάλιστα, τα έσοδα από αυτή τη διαδικασία θα δωρίζονται σε μη κερδοσκοπικούς οργανισμούς κοινωνικών αγαθών (Vom Lehn et al., 2014).

Μία ακόμα πρόταση των Vom Lehn et al. (2014), είναι μία νέα υπηρεσία της εταιρείας Reputation.com. Η υπηρεσία αυτή θα επέτρεπε στους χρήστες να μοιραστούν με ελεγχόμενο τρόπο τις πληροφορίες που έχουν συλλεχθεί. Με αυτόν τον τρόπο θα έχουν εκείνοι τον έλεγχο των δεδομένων τους.

Οι Cinar & Ateş (2022) αναφέρουν ότι το Mozilla Firefox και το Apple Safari (μηχανές αναζήτησης) έχουν δημιουργήσει δύο νέες δυνατότητες ενισχυμένης και έξυπνης αντίστοιχα αποτροπής παρακολούθησης, αποκλείοντας από τις μηχανές αναζήτησης τα cookies τρίτων. Αυτό περιορίζει τον διαμοιρασμό των δεδομένων.

Επιπρόσθετα, οι Karanasiou & Douilhet (2016), κάνουν λόγο για μία νέα τεχνική λύση, η οποία επιτρέπει στους χρήστες να αποκτήσουν τον έλεγχο των δεδομένων τους από τους μεσίτες δεδομένων. Ο τρόπος για να επιτευχθεί αυτό είναι ο χρήστης μέσω μίας νέας αρχιτεκτονικής και βελτιωμένης προστασίας να έχει πρόσβαση, να ελέγχει και να ανιχνεύει τα δεδομένα του όταν εκείνα κοινοποιούνται στο Διαδίκτυο.

Ιδιαίτερη μνεία πρέπει να γίνει για τους κανονισμούς προστασίας των δεδομένων. Τα τελευταία χρόνια, όλο και περισσότερες εταιρείες συλλέγουν, όπως ήδη αναφέρθηκε, μεγάλο όγκο δεδομένων από τους πελάτες τους. Συνεχώς αυξάνεται ο όγκος των δεδομένων που συγκεντρώνουν και ταυτόχρονα αυξάνεται και η ανάγκη για την προστασία αυτών των προσωπικών δεδομένων. Για να επιτευχθεί αυτό, οι εταιρείες πρέπει να συμμορφώνονται με τους ενημερωμένους παγκόσμιους κανονισμούς περί απορρήτου δεδομένων που ισχύουν. Στην Ευρώπη ισχύει το GDPR, στον Καναδά το PIPEDA, στην Καλιφόρνια το CCPA και πολλά ακόμα σε άλλες περιοχές. Η διακυβέρνηση των δεδομένων λοιπόν, είναι η λύση για την αποφυγή των ζητημάτων που προκύπτουν με τη συλλογή των δεδομένων (Cinar & Ateş, 2022). Σύμφωνα με τους Cinar & Ateş (2022), «η διακυβέρνηση δεδομένων είναι ένα πλαίσιο που καθορίζει τους ρόλους, τις ευθύνες και τις διαδικασίες σχετικά με τη δημιουργία, τη συλλογή, την επεξεργασία και την προστασία των δεδομένων».

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι η νομοθεσία για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση (El-Khoury, 2021). Είναι ένας ολοκληρωμένος κανονισμός σύμφωνα με τον οποίο η προστασία των προσωπικών δεδομένων θεωρείται θεμελιώδες δικαίωμα (El-Khoury, 2021). Ειδικότερα, σύμφωνα με τον GDPR, η συλλογή και η επεξεργασία προσωπικών δεδομένων είναι νόμιμη εάν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών δεδομένων για έναν ή περισσότερους σκοπούς (Canellopoulou-Bottis & Bouchagiar, 2018).

Οι Douilhet & Karanasiou (2016), αναφέρουν επίσης, ότι το GDPR αυξάνει τα δικαιώματα που έχουν τα άτομα επί των δεδομένων τους, καθώς και τον περιορισμό αυτών. Επιπρόσθετα, οι Tronnier et al. (2022) αναφέρουν ότι «ο GDPR περιλαμβάνει επίσης ορισμένες ηθικές πτυχές, όπως η διαφάνεια και η λογοδοσία στις σχέσεις μεταξύ των υποκειμένων των δεδομένων και των υπεύθυνων επεξεργασίας δεδομένων». Τέλος, σύμφωνα με το GDPR, η συγκατάθεση πρέπει να «δίδεται ελεύθερα, συγκεκριμένα, ενημερωμένα και ξεκάθαρα» (Cinar & Ateş, 2022).

Στις Ηνωμένες Πολιτείες και πιο συγκεκριμένα στην Καλιφόρνια, το 2018 ψηφίστηκε ο νόμος, περί απορρήτου των καταναλωτών της (CCPA). Πιο συγκεκριμένα, ο νόμος αυτός παρέχει στους κατοίκους της Καλιφόρνια, νέα δικαιώματα για την προστασία και την διατήρηση της εξουσίας επί των προσωπικών τους στοιχείων, «όπως το δικαίωμα ενός χρήστη να ζητήσει από μία επιχείρηση να διαγράψει οποιεσδήποτε προσωπικές πληροφορίες που έχει συλλέξει» και το δικαίωμα «να κατευθύνει επιχειρήσεις που πουλούν προσωπικές πληροφορίες για τους καταναλωτές σε τρίτους, ώστε να μην πουλήσουν τις προσωπικές του πληροφορίες». Γενικότερα, ο CCPA θεσπίζει τόσο τα όρια απορρήτου όσο και τις υποχρεώσεις των επιχειρήσεων που διαχειρίζονται δεδομένα καταναλωτών στην Καλιφόρνια (Rose, 2021).

Τέλος, στη Νότια Αφρική υπάρχει ο νόμος για την προστασία Προσωπικών Πληροφοριών (POPIA). Συγκεκριμένα στοχεύει στην προώθηση της προστασίας των προσωπικών πληροφοριών που επεξεργάζονται δημόσιοι και ιδιωτικοί φορείς (Botes et al., 2022).

Από αυτά τα τρία παραδείγματα, είναι αρκετά σαφές ότι όλο και περισσότερες χώρες προσπαθούν να εντάξουν ειδικούς νόμους και καταστατικά στη νομοθεσία τους, που θα προστατεύουν τους καταναλωτές και τις προσωπικές τους πληροφορίες.

Στην Ελλάδα, το Υπουργείο Προστασίας του Πολίτη σε συνεργασία με την Ελληνική Αστυνομία δημιούργησε τον ιστότοπο, www.cyberalert.gr, στον οποίο αναφέρεται τι είναι το κυβερνο-έγκλημα και ποιοι είναι οι διαδικτυακοί κίνδυνοι παρέχοντας συμβουλές αποφυγής και προφύλαξης.

Κάποιοι από τους τρόπους αποφυγής που αναφέρει η σελίδα είναι οι παρακάτω :

- Εγκατάσταση ενός προγράμματος προστασίας από ιούς, σε όλες τις συσκευές που έχουν πρόσβαση στο Διαδίκτυο, ηλεκτρονικό υπολογιστή, κινητό τηλέφωνο και tablet, και συνεχή μέριμνα για αναβαθμίσεις και ενημερώσεις
- Αποφυγή χρήσης κοινόχρηστων υπολογιστών και δικτύων για την πραγματοποίηση ηλεκτρονικών παραγγελιών. Ο λόγος είναι για να μην καταχωρούνται τα προσωπικά στοιχεία σε υπολογιστή τρίτου
- Διαγραφή ιστορικού και υποθηκευμένων κωδικών ή cookies από υπολογιστές τρίτων, και υπενθύμιση να γίνεται πάντα αποσύνδεση από πλατφόρμες και ηλεκτρονικό ταχυδρομείο, ειδικά όταν έχει γίνει χρήση υπολογιστή ή συσκευή τρίτου
- Διατήρηση προγραμμάτων διαχείρισης αποθήκευσης κωδικών
- Αποφυγή καταχώρησης του αριθμού του κινητού τηλεφώνου σε αναδυόμενα παράθυρα, τα οποία εμφανίζονται σε διαδικτυακές σελίδες, εάν πρώτα δεν γίνει ανάγνωση και κατανόηση των ορών και των χρεώσεων, που προσφέρουν οι εκάστοτε υπηρεσίες

### 4.2.3 Τρόποι αντιμετώπισης της απάτης της διαδικτυακής ταυτότητας

Υπάρχουν όπως αναφέρθηκε πολλοί τρόποι για έναν απατεώνα/ χάκερ να διαπράξει απάτη ταυτότητας. Αντίστοιχα υπάρχουν αρκετοί τρόποι αντιμετώπισης του φαινομένου (Conlin & Ruhi, 2021).

Οι Soomro et al. (2019) προτείνουν για την αντιμετώπιση αυτού του φαινομένου, τα 8 στάδια διαχείρισης της απάτης ταυτότητας. Αυτά είναι :

- Η αποτροπή
- Η πρόληψη
- Ο εντοπισμός
- Ο μετριασμός
- Η ανάλυση
- Η πολιτική
- Η διερεύνηση
- Η δίωξη

Η αποτροπή είναι το στάδιο, στο οποίο γίνεται η προσπάθεια να σταματήσει η πράξη ή να μην συμβεί καθόλου. Για να επιτευχθεί αυτό πρέπει να γίνει αναλυτική επεξήγηση και γενικά οι καταναλωτές πρέπει να είναι ενήμεροι για τις συνέπειες που θα αντιμετωπίσουν αυτοί που διαπράττουν το έγκλημα (Soomro et al., 2019). Ουσιαστικά, μέσω του φόβου γίνεται

προσπάθεια να αποτραπεί η ενέργεια της απάτης. Αυτό υποστηρίζει και ο Lee (2020), αναφέροντας ότι ο φόβος για τον κρατικό έλεγχο και τη φυλάκιση είναι αυτό που βοηθούσε τις αστυνομικές δυνάμεις στη Κίνα, για να πραγματοποιήσουν έρευνες για το φαινόμενο.

Το επόμενο στάδιο της πρόληψης αφορά τον διαδικτυακό οργανισμό σε συνδυασμό με τους πελάτες/χρήστες. Στόχος είναι οι διαδικτυακοί οργανισμοί να πάρουν κάποια μέτρα προστασίας, όπως να τοποθετήσουν κάποιο ισχυρό σύστημα ελέγχου ταυτότητας, για την ασφάλεια των πληροφοριών και των επικοινωνιών των χρηστών ή να εκπαιδεύσουν τους εργαζόμενους τους ώστε να αποδίδουν αποτελεσματικά στα περιστατικά πρόληψης της απάτης (Soomro et al., 2019).

Η ανίχνευση της απειλής μπορεί να συμβεί πριν, κατά τη διάρκεια ή και μετά την πράξη (Soomro et al., 2019). Αυτό το στάδιο λειτουργεί όταν αποτυγχάνει το στάδιο πρόληψης. Σύμφωνα με τους Conlin & Ruhi (2021) για την ανίχνευση των απειλών μπορούν να χρησιμοποιηθούν πολλαπλοί αλγόριθμοι ML, οι οποίοι μπορούν να ανιχνεύσουν την απειλή και να βοηθήσουν τον μετριασμό του προβλήματος. Οι αλγόριθμοι είναι μία αποτελεσματική μέθοδος, διότι πλέον έχουν εξελιχθεί κατά πολύ οι κακόβουλες μέθοδοι που χρησιμοποιούν οι δράστες. Επιπρόσθετα, οι Tan et al. (2016) αναφέρουν ότι μπορεί να χρησιμοποιηθεί ως μέθοδος ανίχνευσης, ο παγκόσμιος πάροχος τεχνολογίας ψηφιακής επαλήθευσης Trustev, που ειδικεύεται στην επικύρωση της ταυτότητας σε πραγματικό χρόνο. Το Trustev είναι μία παγκόσμια πλατφόρμα λογισμικού που αναπτύσσει διαδικτυακές λύσεις επαλήθευσης ταυτότητας και συνδυάζει την ανθρώπινη νοημοσύνη με τη μηχανική μάθηση. Η προσέγγιση που ακολουθεί είναι να συνδυάζει τα μεγάλα δεδομένα με τη διαχείριση της ψηφιακής ταυτότητας και να αναπτύσσει το κοινωνικό δακτυλικό αποτύπωμα που ανιχνεύει ποιοι χρήστες είναι πιθανό να διαπράξουν δόλια δραστηριότητα και ποιοι όχι (Tan et al., 2016). Επιπλέον, παρέχει υπηρεσίες ελέγχου και σε διαδικτυακούς λιανοπωλητές και σε μεμονωμένους χρήστες.

Ο μετριασμός, είναι το στάδιο που ακολουθεί, όταν ανιχνευθεί κάποια ύποπτη δραστηριότητα και είναι πολύ σημαντικό να συμβαίνει σε πραγματικό χρόνο, την στιγμή δηλαδή που θα εντοπιστεί η απειλή (Soomro et al., 2019). Το πρόγραμμα Trustev, αποτελεί μία λύση στον μετριασμό, διότι μπορεί να δράσει και να προειδοποιήσει τους χρήστες ή να διαφυλάξει τα δεδομένα (Tan et al., 2016). Ακόμα, οι αλγόριθμοι είναι μία άμεση μέθοδος για τον μετριασμό, διότι και αυτοί είναι κατασκευασμένοι να δρουν σε πραγματικό χρόνο, τη στιγμή που χρειάζεται να αποτρέπουν τη διαρροή των δεδομένων (Conlin & Ruhi, 2021). Επιπρόσθετα, τα μέσα κοινωνικής δικτύωσης έχουν πολλές λειτουργίες που βοηθούν στον μετριασμό της απειλής (Wu et al., n.d.). Πιο συγκεκριμένα, το Facebook χρησιμοποιεί μία

σειρά μέτρων για την προστασία του απορρήτου χρηστών. Καταγράφει τις διευθύνσεις IP, τα προγράμματα περιήγησης ιστού και τις συσκευές που χρησιμοποιούνται για κάθε λογαριασμό. Έτσι όταν γίνεται προσπάθεια σύνδεσης από διαφορετική συσκευή ή άλλη/ απόρρητη IP, το Facebook προσκαλεί το νέο χρήστη να ταυτοποιήσει την ταυτότητα του, κάνοντας του κάποιες μυστικές ερωτήσεις (Wu et al., n.d.). Ομοίως με το Facebook και άλλα προγράμματα και εφαρμογές χρησιμοποιούν συστήματα που παρακολουθούν τους λογαριασμούς, τις εκτελέσεις προγραμμάτων και τη δραστηριότητα του δικτύου και μόλις ανιχνεύσουν κάποια ύποπτη δραστηριότητα προσπαθούν να ελέγξουν την ταυτότητα του χρήστη με ερωτήσεις αυθεντικότητας.

Η ανάλυση είναι το στάδιο που πραγματοποιείται εφόσον συμβεί η πράξη. Αφενός αναλύονται οι μέθοδοι και η φύση της απάτης, και αφετέρου αναλύονται τα αίτια που επέτρεψαν να πραγματοποιηθεί αυτή. Επίσης αναλύονται και τα προηγούμενα στάδια, όπως της πρόληψης, του εντοπισμού και του μετριασμού, έτσι ώστε να γίνουν προτάσεις βελτίωσης (Soomro et al., 2019).

Η πολιτική μπορεί να θεωρηθεί η ουσία για τη διαχείριση την εγκληματικών πράξεων. Στο στάδιο πολιτικής δίνεται μία κατευθυντήρια γραμμή πάνω στην οποία στηρίζονται όλες οι ενέργειες αντιμετώπισης. Η δημιουργία και η διατήρηση μίας πολιτικής είναι απαραίτητη για να καθοδηγούνται οι εργαζόμενοι αλλά και η ίδια η επιχείρηση (Soomro et al., 2021). Για αυτό και πρέπει να ενθαρρύνονται να συμμετέχουν στις διαδικασίες σχεδιασμού της, οι εργαζόμενοί της, οι οποίοι πέρα από τον διαμοιρασμό προσωπικών εμπειριών, με το να συμβάλουν στο σχεδιασμό της πολιτικής, αποκτούν κίνητρο για να συμμορφώνονται σε αυτήν (Soomro et al., 2021). Αυτό είναι σημαντικό, διότι με αυτόν τον τρόπο αποφεύγονται οι ενδο-εταιρικές διαρροές δεδομένων. Επίσης, είναι σωστό οι τράπεζες και οι διαδικτυακοί οργανισμοί να ενημερώνουν τους συνεργάτες και όλα τα μέλη που απασχολούν, για την πολιτική που επικρατεί για να συμμορφώνονται σε αυτήν. Η συμμόρφωση στις πολιτικές είναι εξίσου σημαντική με την δημιουργία τους (Soomro et al., 2021).

Η διερεύνηση είναι το επόμενο στάδιο. Στο πλαίσιο της απάτης διαδικτυακής ταυτότητας πρέπει να διεξάγεται συστηματική έρευνα μετά την πράξη, για τη συλλογή αποδεικτικών στοιχείων, τα οποία συνδράμουν στο να εξεταστούν οι περιπτώσεις απάτης. Σε περίπτωση που οι κρατικές υπηρεσίες δεν μπορούν να διεξάγουν την έρευνα, την αναλαμβάνουν επιχειρηματικές εταιρείες και στο τέλος των ερευνών είναι υπόχρεοι να αναφέρουν τα αποδεικτικά στοιχεία που συνέλλεξαν στις κρατικές υπηρεσίες για να προχωρήσει η διαδικασία στο στάδιο της δίωξης (Soomro et al., 2019).

Στο τελευταίο στάδιο ξεκινάει η διαδικασία της δίωξης. Οι επιχειρήσεις και οι κρατικές υπηρεσίες, εφόσον έχουν τα αποδεικτικά στοιχεία, ξεκινούν τις διαδικασίες δίωξης. Στον τομέα της απάτης ταυτότητας, η δίωξη είναι απαραίτητη για:

- να τιμωρηθεί ο απατεώνας και να μην επαναλάβει την πράξη
- να ανακτηθούν οι απώλειες (αν είναι οικονομικές) ή να επέλθει ηθική δικαίωση στα θύματα
- να ενισχυθεί η φήμη της επιχείρησης έτσι ώστε να μη χάσει άλλους καταναλωτές

Ένα στάδιο ή αλλιώς, ένας ακόμα πολύ βασικός τρόπος αντιμετώπισης που δεν αναφέρθηκε είναι η ενημέρωση και η εκπαίδευση των χρηστών. Είναι γνωστό ότι οι περισσότερες πληροφορίες ταυτότητας αποσπώνται από τον ίδιο τον καταναλωτή. Οι DiSanto (2014) και Gilbert & Archer (2011) υποστηρίζουν ότι ένα συντονισμένο πρόγραμμα εκπαίδευσης πελατών, σχετικά με τη νομοθεσία, το απόρρητο και κάποιες τεχνικές λύσεις είναι πολύ χρήσιμο να πραγματοποιείται. Θα πρέπει οι χρήστες να ενημερώνονται για :

- την αποφυγή επικίνδυνων συμπεριφορών
- το πώς να δημιουργούν ασφαλείς κωδικούς πρόσβασης
- το πώς να περιορίζουν τις προσωπικές πληροφορίες που μοιράζονται σε ιστοτόπους

Ομοίως, οι Soomro et al. (2019) και οι Cross et al. (2014) θεωρούν ότι οι διαδικτυακοί οργανισμοί πρέπει, πέρα από εκπαίδευση, να παρέχουν καλύτερη και σαφέστερη πληροφόρηση για τους κινδύνους και την αποφυγή αυτών.

Χαρακτηριστικό παράδειγμα είναι η προσπάθεια του Facebook να ενημερώσει και να εκπαιδεύσει τους χρήστες του, δίνοντας τους τη δυνατότητα να έχουν πρόσβαση σε μία επίσημη σελίδα που έχουν δημιουργήσει, η οποία αναφέρει πληροφορίες σχετικές με τις ρυθμίσεις απορρήτου και ασφάλειας (Wu et al., n.d.).

Συμπληρωματικά με τα όσα αναφέρθηκαν παραπάνω, η ιστοσελίδα cyberalert.com (2022) σημειώνει μια σειρά ενεργειών που μπορεί να ακολουθήσει κανείς για να προφυλαχθεί από τις διαδικτυακές απάτες. Αυτές οι ενέργειες είναι :

- Αποφυγή απάντησης σε email που ζητούν στοιχεία τραπεζικού λογαριασμού
- Αποφυγή «ανοίγματος» μηνυμάτων από άγνωστους αποστολείς
- Αποφυγή «ανοίγματος» αρχείων που βρίσκονται συνημμένα σε email από άγνωστους αποστολείς
- Αποφυγή συμπλήρωσης φορμών με προσωπικά στοιχεία, για συμμετοχή σε διαγωνισμούς από άγνωστες πηγές

- Αποφυγή αποστολής σε διαδικτυακές έρευνες προσωπικά στοιχεία και οικονομικά δεδομένα
- Ανάγνωση πάντα των ορών χρήσης μίας ιστοσελίδας πριν την αποδοχή τους
- Αποφυγή διαμοιρασμού προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης και σε ιστοσελίδες διοργάνωσης διαδικτυακών ραντεβού
- Διεξαγωγή έρευνας των ατόμων με τα οποία συνομιλούν οι χρήστες, καθώς και έλεγχος του προφίλ που έχουν στα μέσα κοινωνικής δικτύωσης για επιβεβαίωση ότι πρόκειται για πραγματικό πρόσωπο
- Αποφυγή διαμοιρασμού υλικού, όπως φωτογραφίες και βίντεο, τα οποία μπορούν να χρησιμοποιηθούν αργότερα για εκβιασμό
- Αποφυγή αποστολής χρημάτων για προκαταβολές σε άτομα που δεν είναι οικεία
- Προσπάθεια για έρευνα των ψηφιακών καταστημάτων, μέσω των αξιολογήσεων και των κριτικών που έχουν γίνει από άλλους χρήστες, πριν την ολοκλήρωση κάποιας διαδικτυακής αγοράς
- Αγορά προϊόντων από ιστοσελίδες, με πιστωτικές κάρτες ή προπληρωμένες κάρτες για αποφυγή κλοπής τραπεζικών στοιχείων
- Διαγραφή ιστορικού και cookies

### 4.2.4 Βασικές κατευθύνσεις δεοντολογικής συμπεριφοράς στο Διαδίκτυο

Οι κατευθυντήριες γραμμές των κανόνων Διαδικτύου αφορούν κάποιους γενικούς κανονισμούς χρήσης του Διαδικτύου αλλά και συγκεκριμένες συμβουλές που αφορούν στον τρόπο χρήσης των μέσων κοινωνικής δικτύωσης, των φόρουμ και στη σύνταξη ηλεκτρονικών μηνυμάτων – επιστολών.

Η λίστα με τις γενικές συμβουλές αναφέρει τι πρέπει να αποφεύγει ο κάθε χρήστης σύμφωνα με τους Abifarin & Tsetim (2018b), πρόκειται για :

- «Αποφυγή χρήσης υβριστικής ή απειλητικής γλώσσας»
- «Αποφυγή δημοσίευσης ρατσιστικών, προσβλητικών και ομοφοβικών σχολίων»
- «Αποφυγή αποστολής ανεπιθύμητων μηνυμάτων σε ιδιωτικές ομάδες ή ιδιωτικές συνομιλίες»
- «Αποφυγή χρήσης ψευδώνυμων, ή χρήση ταυτότητας τρίτου ατόμου»
- «Αποφυγή διανομής παράνομου υλικού»
- «Αποφυγή απόκτησης προσωπικών πληροφοριών τρίτου προσώπου»
- «Αποφυγή παρενόχλησης ατόμων»
- «Αποφυγή χρήσης κακής γραμματικής ή ορθογραφίας»

- «Αποφυγή κοινοποίησης προσωπικών στοιχείων τρίτου χωρίς την άδεια τους»
- «Αποφυγή υβριστικών ή υποτιμητικών σχολίων»
- «Αποφυγή δημοσιεύσεων με κεφαλαία γράμματα»

Συμπληρωματικά με την παραπάνω λίστα, ο Ayhan (2019) αναφέρει ότι πρέπει να υπάρχει επιείκεια στα λάθη των άλλων και πρέπει να υπάρχει προσοχή στον τρόπο έκφρασης. Επιπλέον, οι Yarmohammadian et al. (2012) συμπληρώνουν ότι για να αποφευχθούν παρεξηγήσεις πρέπει να προσέχουν όλοι οι χρήστες τον τόνο τους και να αποφεύγουν να εκφράζουν γραπτά συναισθήματα όπως σαρκασμό.

Κάποιοι κανόνες για την σωστή χρήση του email είναι οι παρακάτω (Abifarin & Tsetim, 2018b; Ayhan, 2019; Khani & Darabi, 2014):

- «Η αποφυγή χρήσης ακρωνύμιων»
- «Η αποφυγή δημοσίευσης άσχετων σχολίων»
- «Η αποφυγή αποστολής ανεπιθύμητων μηνυμάτων ή μηνυμάτων που περιλαμβάνουν άσχετες πληροφορίες»
- «Η αποφυγή ορθογραφικών λαθών, και κακής γραμματικής»
- «Η προσεκτική σύνταξη μηνυμάτων ηλεκτρονικού ταχυδρομείου καθώς τα μηνύματα αυτά μπορούν να αποθηκευτούν για πάντα και να χρησιμοποιηθούν πολλές φορές»
- «Η αποφυγή αστείων ή ειρωνικών σχολίων καθώς όπως αναφέρθηκε μπορεί να παρεξηγηθούν»
- «Η προσπάθεια ύπαρξης ενός επιπέδου τυπικότητας»
- «Η προσπάθεια χρήσης απλής γλώσσας για να γίνεται πιο εύκολα κατανοητή»
- «Η άμεση απάντηση επιβεβαίωσης παραλαβής κάποιου μηνύματος»
- «Ο χαιρετισμός στην έναρξη και στο τέλος ενός μηνύματος»

Οι κανόνες που αφορούν τα μέσα κοινωνικής δικτύωσης και τα φόρουμ είναι σύμφωνα με τους Abifarin & Tsetim, 2018b:

- «Η αποφυγή ανάρτησης μη εξουσιοδοτημένων εμπορικών επικοινωνιών ή περιεχόμενων/ πληροφοριών χρηστών χωρίς την συγκατάθεση τους»
- «Η αποφυγή παρενόχλησης και εκφοβισμού άλλου χρήστη»
- «Η αποφυγή ανάρτησης απειλητικού ή γεμάτου μίσους σχολίου ή πορνογραφικού υλικού»
- «Η αποφυγή ανάρτησης ή αποστολής ιού ή κακόβουλου υλικού»
- «Η αποφυγή παροχής ψευδών προσωπικών πληροφοριών»

Γενικότερα τα περισσότερα μέσα κοινωνικής δικτύωσης έχουν ένα σύνολο κανόνων χρήσης, και τα περισσότερα φόρουμ αναφέρουν συγκεκριμένους κανόνες συμπεριφοράς ούτως ώστε να επιτρέψουν την είσοδο και την παραμονή κάποιου σε αυτά. Για αυτό είναι απαραίτητο πριν την συμμετοχή ή την έναρξη χρήσης και ανάρτησης σε αυτά, όλοι οι χρήστες να ενημερώνονται και να συμμορφώνονται με αυτούς. Αυτοί οι κανόνες ονομάζονται και αλλιώς κανόνες πολιτικής και χρησιμοποιούνται για την προστασία των χρηστών και των προσωπικών τους πληροφοριών (Abifarin & Tsetim, 2018b).

## 4.3 Εκπαιδευτικά σενάρια

### 4.3.1 Διαδικτυακός εκφοβισμός

#### Εισαγωγικές Πληροφορίες

Ο διαδικτυακός εκφοβισμός (cyberbullying) είναι φαινόμενο που έχει αυξηθεί στις μέρες μας, λόγω της καθημερινής και πολλές φορές χωρίς όρια χρήσης του Διαδικτύου. Θύματά του είναι νέοι αλλά και μεγαλύτεροι σε ηλικία. Το φαινόμενο έχει πολλές μορφές και μπορεί να συμβεί είτε στο εκπαιδευτικό είτε και στο εργασιακό περιβάλλον. Το συγκεκριμένο εκπαιδευτικό σενάριο απευθύνεται σε εκπαιδευτικούς αλλά και σε επιστήμονες της πληροφόρησης που επιθυμούν να σχεδιάσουν ένα σεμινάριο/μάθημα για να ενημερώσουν τις κοινότητες που εξυπηρετούν (μαθητές, φοιτητές αλλά και το ευρύτερο κοινό) για το διαδικτυακό εκφοβισμό, τα είδη του, τις συνέπειες που προκαλεί και τους πιθανούς τρόπους αντιμετώπισής του.

#### Προτεινόμενη βιβλιογραφία


- Chan, H. C., & Wong, D. S. (2020). The overlap between cyberbullying perpetration and victimisation: exploring the psychosocial characteristics of Hong Kong adolescents. *Asia Pacific Journal of Social Work and Development*, *30*(3), 164-180. https://doi.org/10.1080/02185385.2020.1761436
- Notar, C. E., Padgett, S., & Roden, J. (2013). Cyberbullying: A review of the literature. *Universal journal of educational research*, *1*(1), 1-9. ERIC - EJ1053975 - Cyberbullying: A Review of the Literature, Universal Journal of Educational Research, 2013

- Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. *Aggression and Violent Behavior*, *23*, 69-74. https://doi.org/10.1016/j.avb.2015.05.013
- Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. Computers in Human behavior, 29(6), 2703-2711.
- Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, *69*, 268-274. https://doi.org/10.1016/j.chb.2016.12.038
- Κωτσάκη, Α. (2023). *Το «ελεύθερο» διαδίκτυο ως πάροχος πληροφοριών, με έμφαση στην ενημέρωση για τους κινδύνους που ενέχει η χρήση του* (Διπλωματική Εργασία, Πανεπιστήμιο Δυτικής Αττικής, Σχολή Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης). Κεφάλαια 2.2.2, 4.2.1, 5.2.2.


## Προβλήματα που μπορεί να αντιμετωπίσει η διδάσκουσα/ο διδάσκων

- Κάποιοι εκπαιδευόμενοι πιθανώς δυσκολεύονται να ανοιχτούν και να μοιραστούν προσωπικές εμπειρίες
- Κάποιοι εκπαιδευόμενοι που μπορεί να έχουν υπάρξει θύματα διαδικτυακού εκφοβισμού με την αναφορά και μόνο του φαινομένου, μπορεί να ταραχθούν
- Μπορεί να υπάρξουν δυσκολίες στο να αντιληφθεί το εκπαιδευόμενο κοινό τις πραγματικές συνέπειες του προβλήματος

## Συχνές Ερωτήσεις και Απαντήσεις

**Ο εκφοβισμός (bullying) είναι το ίδιο με το διαδικτυακό εκφοβισμό (cyberbullying);**

Ο διαδικτυακός εκφοβισμός είναι η εξέλιξη του εκφοβισμού. Η ανάπτυξη του Διαδικτύου, οι διαρκείς εξελίξεις και η εμφάνιση των νέων μέσων κοινωνικής δικτύωσης, και διαδικτυακών πλατφορμών, καθώς και το γεγονός ότι το Διαδίκτυο είναι αναπόσπαστο κομμάτι της καθημερινότητας, έχει προκαλέσει αύξηση του φαινομένου του διαδικτυακού εκφοβισμού. Όλα αυτά σε συνδυασμό με το χρόνο που ξοδεύουν οι νέοι στο Διαδίκτυο, το καθιστά ένα φαινόμενο με ανησυχητικά ποσοστά θυματοποίησης.

Οι διαφορές μεταξύ τους είναι

- Ο διαδικτυακός εκφοβισμός έχει σκοπό την συναισθηματική βλάβη και όχι τόσο τη σωματική όπως έχει ο εκφοβισμός

- Ο διαδικτυακός εκφοβισμός μπορεί να συμβεί 24 ώρες το 24ώρο, από οπουδήποτε (μέσω του Διαδικτύου και των κοινωνικών δικτύων) και όχι μόνο στα πλαίσια του σχολείου, όπως κυρίως συμβαίνει με τον εκφοβισμό
- Ο διαδικτυακός εκφοβισμός προσφέρει ανωνυμία στον θύτη και έτσι είναι πιο δύσκολο να εντοπιστεί ο δράστης
- Ο διαδικτυακός εκφοβισμός έχει μεγαλύτερη διάρκεια διότι μπορεί να επαναλαμβάνεται σε πολλά μέσα κοινωνικής δικτύωσης
- Φαινόμενα διαδικτυακού εκφοβισμού μπορεί να γίνουν γνωστά με αστραπιαία ταχύτητα και να παραμείνουν για ένα διάστημα στη δημοσιότητα (viral)

Οι ομοιότητες μεταξύ των δύο εννοιών αφορούν στην πρόκληση βλάβης είτε σωματικής είτε συναισθηματικής. Και στις δύο μορφές του φαινομένου ένα βασικό χαρακτηριστικό είναι η ανισορροπία δύναμης. Δηλαδή ο εκφοβισμός ασκείται συνήθως από τους σωματικά δυνατούς στους αδύναμους και ο διαδικτυακός εκφοβισμός αντίστοιχα, ασκείται από αυτούς που έχουν πιο πολλές τεχνολογικές γνώσεις ή πιο εύκολη πρόσβαση σε τεχνολογικά μέσα.

**Είναι τόσο σοβαρό το φαινόμενο του διαδικτυακού εκφοβισμού;**

Ο διαδικτυακός εκφοβισμός είναι ένα σοβαρό φαινόμενο του οποίου οι συνέπειες μπορούν να επηρεάσουν τα θύματα κυρίως σωματικά αλλά περισσότερο συναισθηματικά. Έχει παρατηρηθεί ότι τα θύματα αποκτούν πολλά αρνητικά συναισθήματα, όπως άγχος, αγωνία και συναισθήματα θλίψης. Όλα αυτά μπορεί να προκαλέσουν κοινωνικό αποκλεισμό, αλλά το πιο σοβαρό από όλα είναι η κατάθλιψη και οι αυτοκτονικές τάσεις.

**Μπορούν να δικαιολογηθούν οι θύτες;**

Οι θύτες του διαδικτυακού εκφοβισμού έχει παρατηρηθεί ότι μπορεί να είναι άτομα χαμηλού κοινωνικού επιπέδου, με ελλείψεις βασικών διαπροσωπικών σχέσεων. Είναι συνήθως άτομα τα οποία μπορεί να έχουν βιώσει τα ίδια τον κοινωνικό αποκλεισμό, νιώθουν παραγκωνισμένα και αυτός είναι ο κύριος λόγος που μπορεί να διαπράττουν την πράξη. Επιπλέον, μία μεγάλη μερίδα δραστών διαδικτυακού εκφοβισμού, έχει σημειωθεί, ότι μπορεί να είναι άτομα τα οποία έχουν βιώσει διαδικτυακό ή ακόμα και παραδοσιακό εκφοβισμό, και με αυτόν τον τρόπο εκδικούνται τους θύτες.

Αυτά δεν δικαιολογούν τους δράστες, ωστόσο εξηγούν σε ένα βαθμό, τον λόγο που διαπράττουν την πράξη.

**Μπορεί να συμβεί και εκτός εκπαιδευτικού πλαισίου;**

Ο διαδικτυακός εκφοβισμός συμβαίνει κυρίως εκτός του σχολικού περιβάλλοντος, καθώς τα μέσα κοινωνικής δικτύωσης και γενικότερα το Διαδίκτυο μπορεί να χρησιμοποιηθεί από

οπουδήποτε. Επίσης, έχουν σημειωθεί πολλά περιστατικά διαδικτυακού εκφοβισμού ακόμα και σε εργασιακό περιβάλλον μεταξύ των συναδέλφων.

**Θα βοηθούσε αν περιορίζαμε τη χρήση του Διαδικτύου;**

Ο διαδικτυακός εκφοβισμός δεν θα περιοριζόταν αν σταματούσαμε να χρησιμοποιούμε το Διαδίκτυο και τα μέσα που υπάρχουν. Αντιθέτως, θα μπορούσαμε μέσω του Διαδικτύου να αναπτύξουμε κανάλια και σελίδες στα οποία θα μπορούν να απευθύνονται τα θύματα, έτσι ώστε αφενός να μοιράζονται το πρόβλημα και να μην νιώθουν μόνοι τους, αφετέρου, μέσω της συζήτησης μπορεί να βρεθεί και τυχόν λύση στο πρόβλημα που μπορεί να αντιμετωπίζουν.

## Σχεδιασμός μαθήματος

Διάρκεια 1 : 30 ώρα

## Μαθησιακοί στόχοι

Οι εκπαιδευόμενοι θα μάθουν :

- τί είναι ο διαδικτυακός εκφοβισμός
- ποια είναι τα χαρακτηριστικά του
- ποια είναι τα είδη του διαδικτυακού εκφοβισμού
- τους λόγους που μπορεί να συμβεί
- τις συνέπειες που προκαλεί σε όσους εμπλέκονται στο φαινόμενο
- που μπορούν να απευθυνθούν σε περίπτωση που «πέσουν» θύματα

## Απαιτούμενα

Για να διεκπεραιωθεί το σεμινάριο/μάθημα θα χρειαστεί, υπολογιστής με πρόσβαση σε βιντεοπροβολέα, λευκός πίνακας με μαρκαδόρους.

## Περιεχόμενο μαθήματος

Καλωσόρισμα και παρουσίαση του εκπαιδευτή και του θέματος του σεμιναρίου/μαθήματος.

**Εκπαιδευτική μέθοδος**: Το σεμινάριο/μάθημα προτείνεται να έχει κυρίως τη μορφή ερωτήσεων από τον εκπαιδευτή, απαντήσεων από τους εκπαιδευόμενους, μετά την ανάταση του χεριού τους και στη συνέχεια να δίνεται η σωστή απάντηση μέσω της προβολής ολιγόλεπτων βίντεο ή σχετικών παρουσιάσεων. Επίσης, προτείνεται η μέθοδος της ομαδικής συζήτησης και το παιχνίδι ρόλων.

### Ενότητα 1η - Προτεινόμενες ερωτήσεις:

- Γνωρίζετε τι είναι διαδικτυακός εκφοβισμός; Μετά την απάντηση προτείνεται η προβολή βίντεο ή/και παρουσίασης που θα περιλαμβάνει τον ορισμό
- Γνωρίζετε πόσα είδη διαδικτυακού εκφοβισμού μπορεί να υπάρχουν; Μετά την απάντηση προτείνεται η προβολή βίντεο ή/και παρουσίασης για τα είδη του διαδικτυακού εκφοβισμού
- Θεωρείτε ότι οι συνέπειες του φαινομένου μπορούν να προκαλέσουν σημαντικές επιπτώσεις στην ψυχολογία όλων όσων εμπλέκονται σε αυτόν; Μετά την απάντηση προτείνεται η προβολή βίντεο ή/και παρουσίασης για τις συνέπειες στα θύματα, τους παρατηρητές του φαινομένου αλλά ακόμα και των δραστών

### Ενότητα 2η – Συζήτηση

Σε αυτό το σημείο προτείνεται η προβολή βίντεο ή/και παρουσίασης για παραδείγματα διαδικτυακού εκφοβισμού που έχουν καταγραφεί παγκοσμίως. Αν κάποιοι από τους εκπαιδευόμενους υπήρξαν οι ίδιοι θύματα ή μάρτυρες διαδικτυακού εκφοβισμού, προτείνεται να δοθεί η ευκαιρία να μοιραστούν την εμπειρία τους

### Ενότητα 3η – Παιχνίδι ρόλων

Στη συνέχεια, οι εκπαιδευόμενοι θα μπορούσαν να χωριστούν ανά ομάδες 4 ή 5 ατόμων. Σε αυτό το σημείο προτείνεται να τους δοθεί ένα σενάριο/ παράδειγμα διαδικτυακού εκφοβισμού, στο οποίο θα πρέπει ομαδικά να σκεφτούν τί συνέπειες θα έχει για το θύμα, τον δράστη, τον παρατηρητή. Επίσης θα πρέπει να σκεφτούν πως θα μπορούσε το θύμα να αντιμετωπίσει την κατάσταση και που θα μπορούσε να απευθυνθεί.

Μετά την παρουσίαση του σεναρίου από την κάθε ομάδα, ο εκπαιδευτής μπορεί να ενημερώνει τους εκπαιδευόμενους για την σελίδα saferinternet4kids.gr στην οποία μπορούν να ενημερωθούν περαιτέρω για το θέμα αλλά και να απευθυνθούν για να καταγγείλουν κάποιο περιστατικό.

## 4.3.2 Εμπορευματοποίηση των προσωπικών δεδομένων

### Εισαγωγικές Πληροφορίες

Η εμπορευματοποίηση προσωπικών δεδομένων (Commercialization of users' digital identity) είναι η διαδικασία κατά την οποία τα προσωπικά δεδομένα αντιμετωπίζονται σαν εμπορεύματα, αποκτούν αξία και τελικά πωλούνται για την απολαβή κέρδους. Η εμπορική εκμετάλλευση των δεδομένων προκαλεί τρομερές συνέπειες στους χρήστες και πρέπει να

περιοριστεί. Το συγκεκριμένο εκπαιδευτικό σενάριο απευθύνεται σε εκπαιδευτικούς αλλά και σε επιστήμονες της πληροφόρησης που επιθυμούν να σχεδιάσουν ένα σεμινάριο/μάθημα για να ενημερώσουν τις κοινότητες που εξυπηρετούν (μαθητές, φοιτητές αλλά και το ευρύτερο κοινό) σχετικά με το φαινόμενο της εμπορευματοποίησης των δεδομένων, τι συνέπειες που προκαλεί και τρόπους προφύλαξης.

## Προτεινόμενη βιβλιογραφία


- Bottis, Maria, and George Bouchagiar. "Personal data v. big data: Challenges of commodification of personal data." *Open Journal of Philosophy* 8, no. 03 (2018): 206. Personal Data v. Big Data: Challenges of Commodification of Personal Data (scirp.org)
- Malgieri, G., & Custers, B. (2018). Pricing privacy–the right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289-303. https://doi.org/10.1016/j.clsr.2017.08.006
- Rose, B. (2020). The Commodification of Personal Data and the Road to Consumer Autonomy through the CCPA. *Brook. J. Corp. Fin. & Com. L.*, *15*, 521. The Commodification of Personal Data and the Road to Consumer Autonomy through the CCPA Notes 15 Brooklyn Journal of Corporate, Financial & Commercial Law 2020-2021 (heinonline.org)
- Cinar, N., & Ateş, S. (2022). Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *Çınar, N., & Ateş, S.(2022)." Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era", in Filimowicz, M.(Ed.) Privacy: Algorithms and Society, Routledge*. Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era by Naim Cinar, Sezgin Ateş :: SSRN
- Tronnier, F., Pape, S., Löbner, S., & Rannenberg, K. (2022). A Discussion on Ethical Cybersecurity Issues in Digital Service Chains. In *Cybersecurity of Digital Service Chains* (pp. 222-256). Springer, Cham. [PDF] A Discussion on Ethical Cybersecurity Issues in Digital Service Chains
- Κωτσάκη, Α. (2023). *Το «ελεύθερο» διαδίκτυο ως πάροχος πληροφοριών, με έμφαση στην ενημέρωση για τους κινδύνους που ενέχει η χρήση του* (Διπλωματική Εργασία, Πανεπιστήμιο Δυτικής Αττικής, Σχολή Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης). Κεφάλαια 2.2.3, 4.2.2, 5.2.3.

## Προβλήματα που μπορεί να αντιμετωπίσει η διδάσκουσα/ο διδάσκων

- Κάποιοι εκπαιδευόμενοι μπορεί να δυσκολευτούν να αντιληφθούν τον ορισμό του φαινομένου και τις τρομερές συνέπειες που προκαλεί στις ζωές τους, λόγω της ηλικίας
- Μπορεί να υπάρχει πρόβλημα κατανόησης των πολιτικών διαφύλαξης των προσωπικών δεδομένων

## Συχνές Ερωτήσεις και Απαντήσεις

**Τί είναι η εμπορευματοποίηση προσωπικών δεδομένων (Commercialization of users' digital identity)**

Είναι η διαδικασία κατά την οποία τα προσωπικά δεδομένα αντιμετωπίζονται σαν εμπορεύματα, αποκτούν αξία και τελικά πωλούνται για την απολαβή κέρδους.

**Πως συμβαίνει η συγκέντρωση των δεδομένων;**

Οι μηχανές αναζήτησης, οι πλατφόρμες κοινωνικής δικτύωσης και άλλα μέσα, συγκεντρώνουν μέσω εξελιγμένων συστημάτων, πληθώρα προσωπικών και ευαίσθητων δεδομένων. Αυτά τα έχουν μοιραστεί οι χρήστες είτε εν γνώση τους, με τη δημιουργία προφίλ σε κάποιο μέσω κοινωνικής δικτύωσης, είτε εν αγνοία τους, με την αναζήτηση διάφορων πληροφοριών σε μηχανές αναζήτησης. Όλα αυτά συγκεντρώνονται και αναλόγως αν αποτελούν ολοκληρωμένα προφίλ ή μεμονωμένα δεδομένα αποκτούν μεγαλύτερη ή μικρότερη αξία αντίστοιχα.

**Τί είναι τα cookies;**

Τα cookies, σύμφωνα με τον Cinar (2022) είναι μικρά, μη εκτελέσιμα αρχεία κειμένου, που αποθηκεύονται στο πρόγραμμα περιήγησης και λειτουργούν ως βοηθοί μνήμης για ιστοτόπους. Τα cookies συγκεντρώνουν όλα τα αιτήματα αναζητήσεων που κάνει ο χρήστης στις μηχανές αναζήτησης συσσωρεύοντας πληροφορίες σχετικές με τα ενδιαφέροντα και τις προτιμήσεις των χρηστών και χτίζοντας σταδιακά τα διαδικτυακά προφίλ τους (Cinar & Ateş, 2022).

**Ποια δεδομένα μπορούν να συλλεχθούν για να χρησιμοποιηθούν για τη δημιουργία διαδικτυακών προφίλ;**

Τα προσωπικά δεδομένα που συγκεντρώνονται μπορεί να είναι το φύλο, η ηλικία, ο τόπος κατοικίας, η οικογενειακή κατάσταση, το επάγγελμα, αλλά και πιο υποκειμενικά όπως τα ενδιαφέροντα και οι αγοραστικές προτιμήσεις των καταναλωτών.

**Είναι τόσο σοβαρό το φαινόμενο;**

Το φαινόμενο μπορεί να προκαλεί σημαντικές συνέπειες στους χρήστες, όπως κατάχρηση των προσωπικών τους δεδομένων, διαρροή αυτών, κλοπή διαδικτυακών ταυτοτήτων, κοινή χρήση δεδομένων με τρίτους, αύξηση των παραβιάσεων διαδικτυακών προφίλ και κατ' επέκταση συστηματική απώλεια της προσωπικής αυτονομίας. Ωστόσο, αυτό που κατά κύριο λόγο συνεπάγεται το συγκεκριμένο φαινόμενο είναι η στοχευμένη διαφήμιση.

**Τι είναι η στοχευμένη διαφήμιση;**

Στοχευμένη διαφήμιση είναι η διαφήμιση που έχει συγκεκριμένο στόχο και αποδέκτη. Ο τρόπος που δημιουργείται αυτού του είδους η διαφήμιση είναι με τη συγκέντρωση πληροφοριών, αρχικά δημογραφικών αλλά και πιο προσωπικών όπως αγοραστικές συνήθειες, ιστορικό αναζητήσεων και προβολής στον συγκεκριμένο χρήστη.

**Υπάρχουν τρόποι προφύλαξης και αποφυγής του προβλήματος;**

Κάποιοι τρόποι αποφυγής και προφύλαξης είναι :

- Η εγκατάσταση ενός προγράμματος προστασίας από ιούς, σε όλες τις συσκευές που έχουν πρόσβαση στο Διαδίκτυο
- Η αποφυγή χρήσης κοινόχρηστων υπολογιστών και δικτύων για την πραγματοποίηση ηλεκτρονικών παραγγελιών
- Η διαγραφή ιστορικού και αποθηκεμένων κωδικών από υπολογιστές τρίτων, και η υπενθύμιση να γίνεται πάντα αποσύνδεση από πλατφόρμες και ηλεκτρονικό ταχυδρομείο
- Η αποφυγή καταχώρησης του αριθμού του κινητού τηλεφώνου σε αναδυόμενα παράθυρα, τα οποία εμφανίζονται σε διαδικτυακές σελίδες, εάν πρώτα δε γίνει ανάγνωση και κατανόηση των ορών και των χρεώσεων που προσφέρουν οι εκάστοτε υπηρεσίες

**Θα βοηθούσε αν περιορίζαμε την χρήση του Διαδικτύου;**

Το φαινόμενο της εμπορευματοποίησης των προσωπικών δεδομένων δεν θα περιοριστεί αν σταματήσουμε να χρησιμοποιούμε το Διαδίκτυο και τα μέσα που υπάρχουν. Θα περιοριστεί

μόνο αν οι χρήστες ενημερωθούν για τους τρόπους προφύλαξης και προστασίας των δεδομένων που μοιράζονται. Παράλληλα, είναι γενικά αναγνωρισμένο ότι η συλλογή των προσωπικών δεδομένων, η επεξεργασία και η χρήση αυτών είναι χρήσιμη για κοινωνικούς σκοπούς όπως η υγειονομική περίθαλψη, η εκπαίδευση ή η πρόληψη της τρομοκρατίας.

## Σχεδιασμός μαθήματος

Διάρκεια 1 : 30 ώρα

## Μαθησιακοί στόχοι

Οι εκπαιδευόμενοι θα μάθουν :

- τί είναι η εμπορευματοποίηση των προσωπικών δεδομένων
- ποια είναι η αξία και τα χαρακτηριστικά των προσωπικών δεδομένων
- πώς συμβαίνει το φαινόμενο
- τί συνέπειες προκαλεί
- πώς μπορούν να προφυλαχθούν οι χρήστες
- πως μπορούν να προφυλαχθούν οι χρήστες

## Απαιτούμενα

Για να διεκπεραιωθεί το μάθημα θα χρειαστεί, υπολογιστής με πρόσβαση σε βιντεοπροβολέα, λευκός πίνακας με μαρκαδόρους και λευκές κόλλες με στυλό.

## Περιεχόμενο μαθήματος

Καλωσόρισμα και παρουσίαση του εκπαιδευτή και του θέματος του σεμιναρίου/μαθήματος.

**Εκπαιδευτική μέθοδος**: Το σεμινάριο/μάθημα προτείνεται να έχει κυρίως τη μορφή ερωτήσεων από τον εκπαιδευτή, απαντήσεων από τους μαθητές μετά την ανάταση του χεριού τους και στη συνέχεια να δίνεται η σωστή και ολοκληρωμένη απάντηση μέσω της προβολής ολιγόλεπτων βίντεο ή σχετικών παρουσιάσεων. Παράλληλα προτείνεται να χρησιμοποιηθεί η μέθοδος της ομαδικής συζήτησης. Τέλος, προτείνεται μια θεωρητική παρουσίαση των μεθόδων προφύλαξης.

**Ενότητα 1η - Προτεινόμενες ερωτήσεις:**

- Γνωρίζετε το φαινόμενο της εμπορευματοποίησης των προσωπικών δεδομένων;
- Γνωρίζετε ποια δεδομένα μπορούν να συλλέξουν, να πωλήσουν ή να ανταλλάξουν οι μεσίτες των δεδομένων;
- Γνωρίζετε από πού μπορεί να αντλούνται τα προσωπικά δεδομένα;
- Γνωρίζετε κάποιες από τις συνέπειες του φαινομένου;
- Γνωρίζετε ή έχετε ακούσει ποτέ τον όρο στοχευμένη διαφήμιση;

Μετά από την κάθε απάντηση προτείνεται προβολή παρουσίασης ή και βίντεο που θα αναφέρεται στο φαινόμενο.

**Ενότητα 2η – Συζήτηση**

- Σε αυτό το σημείο ο εκπαιδευτής προτείνεται να μοιράσει μία λευκή κόλλα στους εκπαιδευόμενους και να τους ζητήσει να σκεφτούν ή να εντοπίσουν σε ποιες μηχανές αναζήτησης και πλατφόρμες κοινωνικής δικτύωσης μπορεί να συλλέγουν προσωπικά δεδομένα
- Αφού δοθούν 5 με 10 λεπτά, προτείνεται να ζητηθεί από τους εκπαιδευόμενους να παρουσιάσουν κάποια από τα παραδείγματα που σκέφτηκαν, ώστε να γίνει συζήτηση και ανάλυση αυτών
- Μετά την παρουσίαση προτείνεται να γίνει προβολή βίντεο στο οποίο θα αναφέρονται τα παραδείγματα επώνυμων πλατφορμών όπως του Facebook, του Instagram, της google και του LinkedIn (Για σχετικά παραδείγματα δείτε στο κεφάλαιο 2.2.3.6 στη Διπλωματική Εργασία της Κωτσάκη, Α. (2023)).

**Ενότητα 3η – Παρουσίαση και επεξήγηση**

Στο τέλος της συζήτησης ο εκπαιδευτής προτείνεται να αναφέρει κάποιες στρατηγικές βελτίωσης που έχουν καθιερωθεί παγκοσμίως, και να παρουσιάσει κάποιους τρόπους προφύλαξης και αποφυγής του φαινομένου.

### 4.3.3 Απάτη διαδικτυακής ταυτότητας

## Εισαγωγικές Πληροφορίες

Η απάτη διαδικτυακής ταυτότητας είναι ένα διάχυτο και συχνό φαινόμενο που σχετίζεται με την εξέλιξη της τεχνολογίας και την αύξηση χρήσης του Διαδικτύου. Η ευθύνη για αυτό υπάγεται στους καταναλωτές, κυρίως λόγω μη φιλτραρίσματος των δεδομένων που μοιράζονται, και μη ορθής χρήσης των μηχανών αναζήτησης και των πλατφόρμων κοινωνικής δικτύωσης, στους οργανισμούς και στις εταιρείες παροχής εφαρμογών και τέλος στους

νομοθετικούς φορείς. Το συγκεκριμένο εκπαιδευτικό σενάριο απευθύνεται σε εκπαιδευτικούς αλλά και σε επιστήμονες της πληροφόρησης που επιθυμούν να σχεδιάσουν ένα σεμινάριο/μάθημα για να ενημερώσουν τις κοινότητες που εξυπηρετούν (μαθητές, φοιτητές αλλά και το ευρύτερο κοινό) για την απάτη της διαδικτυακής ταυτότητας, τις συνέπειες που προκαλεί και κάποιους τρόπους προφύλαξης.

## Προτεινόμενη βιβλιογραφία


- Soomro, Z. A., Shah, M. H., & Thatcher, J. (2021). A framework for ID fraud prevention policies in E-tailing sector. *Computers & Security*, *109*, 102403. https://doi.org/10.1016/j.cose.2021.102403
- Tan, F. T. C., Guo, Z., Cahalane, M., & Cheng, D. (2016). Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. *Information & Management*, *53*(7), 878-891. https://doi.org/10.1016/j.im.2016.07.002
- Archer, N. (2012). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*. Vol. 19 No. 1, pp. 20-36. https://doi.org/10.1108/13590791211190704
- Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and issues in crime and criminal justice*, (474), 1-6. https://search.informit.org/doi/abs/10.3316/informit.312913302944818
- Κωτσάκη, Α. (2023). *Το «ελεύθερο» διαδίκτυο ως πάροχος πληροφοριών, με έμφαση στην ενημέρωση για τους κινδύνους που ενέχει η χρήση του* (Διπλωματική Εργασία, Πανεπιστήμιο Δυτικής Αττικής, Σχολή Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης). Κεφάλαια 2.2.4, 4.2.3, 5.2.4.


## Προβλήματα που μπορεί να αντιμετωπίσει η διδάσκουσα/ο διδάσκων

- Κάποιοι εκπαιδευόμενοι, λόγω ηλικίας, μπορεί να μην αντιλαμβάνονται το μέγεθος τους προβλήματος.

## Συχνές Ερωτήσεις και Απαντήσεις

**Τι είναι η απάτη διαδικτυακής ταυτότητας;**

Είναι η χρήση πραγματικών ή και ψευδών δεδομένων ή και ο συνδυασμός αυτών, με σκοπό την εξαπάτηση τρίτων ή την απολαβή οικονομικού ή υλικού κέρδους.

**Υπάρχουν πολλά είδη;**

Σύμφωνα με τους Cross, Smith & Richards (2014) τα πιο συνήθη είδη διαδικτυακής απάτης είναι:

- Ηλεκτρονικό ψάρεμα (phishing)
- Pharming - δεν υπάρχει ελληνικός όρος αλλά περιφραστικά θα μπορούσαμε να πούμε ότι είναι ένα είδος κυβερνο- επίθεσης κατά την οποία είτε τα συστήματα υπολογιστών των θυμάτων παραβιάζονται μέσω πειρατείας ή κακόβουλου λογισμικού είτε ένα λογισμικό ανακατευθύνει τα θύματα σε ψεύτικους ιστότοπους όπου τούς ζητείται να εισαγάγουν τα στοιχεία τους
- Skimming - δεν υπάρχει ελληνικό όρος αλλά περιφραστικά θα μπορούσαμε να πούμε ότι προσωπικές πληροφορίες «αποφορτίζονται» από τις πλαστικές κάρτες μέσω συσκευών που είναι κρυφά προσαρτημένες σε συσκευές ανάγνωσης καρτών
- Κακόβουλο λογισμικό (π.χ. ιοί) – χρησιμοποιείται ή εγκαθίσταται σε υπολογιστές προκειμένου να τροποποιηθούν οι λειτουργίες εντός προγραμμάτων και αρχείων

**Που μπορεί να συμβεί ;**

Το φαινόμενο μπορεί να συμβεί στα μέσα κοινωνικής δικτύωσης, αλλά ειδικότερα στους λογαριασμούς των χρηστών, και μπορεί να πλήξει το ηλεκτρονικό εμπόριο. Επίσης, μπορεί να συμβεί μέσω των έξυπνων συσκευών, κινητών, ρολογιών και άλλων τέτοιων μέσων, λόγω του ότι σε αυτά αποθηκεύονται πολλά προσωπικά δεδομένα και ένας χάκερ μπορεί πολύ εύκολα να τα διαρρήξει.

**Τι είναι ο χάκερ;**

Χάκερ θεωρείται το άτομο που έχει τεχνολογικές γνώσεις και μπορεί να εισβάλει σε υπολογιστικά συστήματα και να υποκλέψει πληροφορίες και δεδομένα.

**Είναι μόνο οικονομικές οι συνέπειες του φαινομένου ή και ψυχολογικές;**

Οι συνέπειες του φαινομένου δεν είναι μόνο οικονομικές και υλικές, αλλά και συναισθηματικές. Πιο συγκεκριμένα, πολλοί χρήστες που έχουν πέσει θύμα απάτης, αποκτούν συναισθήματα άγχους, φοβίες, προβλήματα στις διαπροσωπικές τους σχέσεις, ανασφάλεια και έλλειψη εμπιστοσύνης προς τους άλλους.

**Οι συνέπειες βλάπτουν μόνο τους καταναλωτές;**

Οι συνέπειες αυτού του φαινομένου πλήττουν πέρα από τους καταναλωτές, τις τράπεζες και τις εταιρείες ηλεκτρονικού εμπορίου. Η μείωση των πωλήσεων, η μείωση της τιμής των μετοχών, και η αμαύρωση της φήμης των εταιρειών είναι κάποιες από τις συνέπειες που υφίστανται. Όλα αυτά βλάπτουν τη πορεία τους γεγονός που τούς αποτρέπει να αναπτυχθούν σωστά.

**Θα βοηθούσε αν περιορίζαμε την χρήση του Διαδικτύου;**

Το φαινόμενο δε θα περιοριστεί αν περιορίσουμε τη χρήση του Διαδικτύου. Αυτό που θα μπορούσαν να κάνουν οι χρήστες είναι να ενημερωθούν για τους κινδύνους και το φαινόμενο και να εκπαιδευτούν στο πώς να αποφεύγουν τις επικίνδυνες συμπεριφορές, πώς να προφυλάσσουν τα δεδομένα και τους λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης και γενικά πώς να περιορίζουν τα προσωπικά δεδομένα που μοιράζονται στο Διαδίκτυο.

## Σχεδιασμός μαθήματος

Διάρκεια 1 : 30 ώρα

## Μαθησιακοί στόχοι

Οι μαθητές θα μάθουν :

- τι είναι η απάτη διαδικτυακής ταυτότητας
- πόσα είδη υπάρχουν
- που μπορεί να συμβεί
- τι συνέπειες προκαλεί και ποιους βλάπτει
- τρόπους προφύλαξης

## Απαιτούμενα

Για να διεκπεραιωθεί το μάθημα θα χρειαστεί, υπολογιστής με πρόσβαση σε βιντεοπροβολέα, λευκός πίνακας με μαρκαδόρους και λευκές κόλλες.

## Περιεχόμενο μαθήματος

Καλωσόρισμα και παρουσίαση του εκπαιδευτή και του θέματος του μαθήματος.

**Εκπαιδευτική μέθοδος**: Το σεμινάριο/μάθημα προτείνεται να έχει κυρίως τη μορφή αναλυτικής παρουσίασης του φαινομένου από τον εκπαιδευτή, μέσω της προβολής

ολιγόλεπτων βίντεο ή σχετικών παρουσιάσεων. Στη συνέχεια, προτείνεται να χρησιμοποιηθεί η μέθοδος της ομαδικής συζήτησης και το παιχνίδι ρόλων.

### Ενότητα 1η – Παρουσίαση θέματος :

Οι ενότητες που προτείνονται για αναλυτική παρουσίαση με βίντεο, διαφάνειες ή συνδυασμό αυτών είναι :

- Τί είναι η απάτη της διαδικτυακής ταυτότητας
- Πόσα είδη απάτης υπάρχουν
- Ποιες είναι οι συνέπειες που προκαλεί στους καταναλωτές
- Ποιους μπορεί να βλάψει πέρα από τους χρήστες
- Υπάρχει τρόπος αντιμετώπισης και προφύλαξης

### Ενότητα 2η – Παιχνίδι ρόλων

Στη συνέχεια, προτείνεται να ζητηθεί από τους εκπαιδευόμενους να χωριστούν σε ομάδες 4 με 5 ατόμων. Η κάθε ομάδα θα πρέπει να καταγράψει από 1 έως 3 παραδείγματα απάτης της διαδικτυακής ταυτότητας και παράλληλα να περιγράψει ή να εντοπίσει το λόγο που συνέβη, καθώς και τι θα μπορούσε να κάνει διαφορετικά το θύμα για να αποφύγει τον κίνδυνο. Τέλος, προτείνεται να ζητηθεί στις ομάδες να παρουσιάσουν την εργασία τους στην αίθουσα.

### Ενότητα 3η – Ομαδική συζήτηση

Στην επόμενη ενότητα προτείνεται να μοιραστεί στους εκπαιδευόμενους ένα φυλλάδιο που να περιλαμβάνει μία σειρά ενεργειών τις οποίες πρέπει να ακολουθούν οι χρήστες για να αποφύγουν να πέσουν θύματα διαδικτυακής απάτης. Αφού δοθεί στους εκπαιδευόμενους λίγος χρόνος για να μελετήσουν το φυλλάδιο, προτείνεται να ερωτηθούν:

- αν θέλουν κάποια επεξήγηση
- αν πιστεύουν ότι κάποιος από τους κανόνες δεν είναι χρήσιμος
- αν θέλουν να προσθέσουν κάποιον κανόνα ή κάποια συμβουλή

### 4.3.4 Κανόνες χρήσης του Διαδικτύου

## Εισαγωγικές Πληροφορίες

Οι κανόνες χρήσης του Διαδικτύου ή αλλιώς netiquette rules είναι κανόνες κατάλληλης επικοινωνιακής συμπεριφοράς στο Διαδίκτυο και είναι απολύτως απαραίτητοι για τη σωστή ανάπτυξη της νέας μορφής διαδικτυακής επικοινωνίας που έχει δημιουργηθεί, αλλά και για τη σωστή χρήση και λειτουργία της νέας ψηφιακής πραγματικότητας. Το συγκεκριμένο εκπαιδευτικό σενάριο απευθύνεται σε εκπαιδευτικούς αλλά και σε επιστήμονες της πληροφόρησης που επιθυμούν να σχεδιάσουν ένα σεμινάριο/μάθημα για να ενημερώσουν τις κοινότητες που εξυπηρετούν (μαθητές, φοιτητές αλλά και το ευρύτερο κοινό) σχετικά με την ύπαρξη των κανόνων χρήσης του Διαδικτύου.

## Προτεινόμενη βιβλιογραφία


- Abifarin, F. P., & Tsetim, P. Z. (2018). Impact of training on compliance with netiquette rules by students. Impact of training on compliance with netiquette rules by students (futminna.edu.ng)
- Arouri, Y. M., & Hamaidi, D. A. (2017). Undergraduate students' perspectives of the extent of practicing netiquettes in a jordanian southern university. *International Journal of Emerging Technologies in Learning, 12*(3), 84-97.
- https://doi.org/10.3991/ijet.v12i03.6424
- Atalay, G. E. (2019). Netiquette in online communications: youth attitudes towards netiquette rules on new media. *New Approach Media Commun*, *225*.
  [PDF] Netiquette in online communications: youth attitudes towards netiquette rules on new media
- Khani, R., & Darabi, R. (2014). Flouting the netiquette rules in the academic correspondence in Iran. *Procedia-Social and Behavioral Sciences*, *98*, 898-907. https://doi.org/10.1016/j.sbspro.2014.03.498
- Κωτσάκη, Α. (2023). *Το «ελεύθερο» διαδίκτυο ως πάροχος πληροφοριών, με έμφαση στην ενημέρωση για τους κινδύνους που ενέχει η χρήση του* (Διπλωματική Εργασία, Πανεπιστήμιο Δυτικής Αττικής, Σχολή Διοικητικών, Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης). Κεφάλαια 2.2.5, 4.2.4, 5.2.5.

## Προβλήματα που μπορεί να αντιμετωπίσει η διδάσκουσα/ο διδάσκων

- Οι νέοι εκπαιδευόμενοι μπορεί να αντιδράσουν στους κανόνες, λόγω του ότι χρησιμοποιούν ήδη από πολύ μικρή ηλικία το Διαδίκτυο και μπορεί να μην τους είναι εύκολο να συμμορφωθούν σε αυτούς.
- Ένας ακόμα λόγος αντίδρασης στους κανόνες χρήσης Διαδικτύου είναι το γεγονός ότι είναι κανόνες, και έχει παρατηρηθεί ότι οι νέοι αντιδρούν όταν πρόκειται να ακολουθήσουν κανόνες.

## Συχνές Ερωτήσεις και Απαντήσεις

**Τι είναι οι κανόνες χρήσης Διαδικτύου (netiquette rules) ;**

Οι κανόνες χρήσης του Διαδικτύου σύμφωνα με τους Khani & Darabi (2014), ορίζονται ως «οι κανόνες κατάλληλης επικοινωνιακής συμπεριφοράς στο Διαδίκτυο». Απευθύνονται σε όλους τους χρήστες και είναι ένα είδος υποχρέωσης που έχουν όλοι οι χρήστες όταν χρησιμοποιούν το Διαδίκτυο.

**Για ποιο λόγο είναι σημαντική η ύπαρξη των κανόνων χρήσης του Διαδικτύου;**

Η νέα μορφή διαδικτυακής επικοινωνίας που έχει δημιουργηθεί, σε συνδυασμό με το ότι το Διαδίκτυο έχει κατακλίσει τόσο το εκπαιδευτικό όσο και το εργασιακό περιβάλλον έχουν μετατρέψει την επικοινωνία σε απρόσωπη, με αποτέλεσμα να γίνονται πιο εύκολα παρεξηγήσεις και παρερμηνείες μηνυμάτων. Για να αποφευχθούν αυτές οι παρεξηγήσεις, αλλά και για να αναπτυχθεί πιο σωστά η κοινωνική ζωή των νέων χρηστών, η οποία εξαρτάται σε μεγάλο βαθμό από την διαδικτυακή επικοινωνία, πρέπει όλοι οι χρήστες να γνωρίζουν τους κανόνες χρήσης του Διαδικτύου και να τους ακολουθούν όταν χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο και γενικά τις πλατφόρμες κοινωνικής δικτύωσης. Κατ' επέκταση όταν ένας χρήστης συμπεριφέρεται με ευγένεια στο Διαδίκτυο θα μπορεί πιο εύκολα να αποφύγει φαινόμενα διαδικτυακού εκφοβισμού, απάτης διαδικτυακής ταυτότητας και άλλους κινδύνους.

**Υπάρχουν κανόνες για όλων των ειδών επικοινωνίας ;**

Οι κανόνες χρήσης του Διαδικτύου αφορούν τη χρήση του ηλεκτρονικού ταχυδρομείου, τη λειτουργία των μέσων κοινωνικής δικτύωσης όπως Facebook, Twitter και γενικά τη συμμετοχή των χρηστών σε ομάδες κοινωνικής δικτύωσης. Εν κατακλείδι αφορούν όλα τα είδη διαδικτυακής επικοινωνίας.

## Σχεδιασμός μαθήματος

### Διάρκεια

1 : 30 ώρα

### Μαθησιακοί στόχοι

Οι εκπαιδευόμενοι θα μάθουν :

- Τί είναι γενικά οι κανόνες χρήσης του Διαδικτύου
- Για ποιους λόγους είναι σημαντικοί αυτοί οι κανόνες και γιατί πρέπει να τους ακολουθούμε
- Ποιοι είναι και που μπορούμε να τους χρησιμοποιούμε; Για παράδειγμα στο email, στα μέσα κοινωνικής δικτύωσης και στα διαδικτυακά φόρουμ

### Απαιτούμενα

Για να διεκπεραιωθεί το σεμινάριο/μάθημα θα χρειαστεί, υπολογιστής με πρόσβαση σε βιντεοπροβολέα, λευκός πίνακας με μαρκαδόρους.

### Περιεχόμενο μαθήματος

Καλωσόρισμα και παρουσίαση του εκπαιδευτή και του θέματος του μαθήματος.

**Εκπαιδευτική μέθοδος**: Το σεμινάριο/μάθημα προτείνεται να έχει κυρίως τη μορφή ερωτήσεων από τον εκπαιδευτή, απαντήσεων από τους εκπαιδευόμενους μετά την ανάταση του χεριού τους. Στη συνέχεια, προτείνεται να γίνει ένα παιχνίδι ρόλων. Τέλος, προτείνεται να χρησιμοποιηθεί η μέθοδος της ομαδικής συζήτησης και να δοθεί ένα φυλλάδιο με όλες τις συμβουλές και τους κανόνες χρήσης του Διαδικτύου.

### Ενότητα 1η - Προτεινόμενες ερωτήσεις:

- Γνωρίζετε αν υπάρχουν ειδικοί κανόνες συμπεριφοράς για τους χρήστες, όταν χρησιμοποιούν το Διαδίκτυο; Ναι ή όχι
- Γνωρίζετε κάποιους από αυτούς τους κανόνες; Για παράδειγμα μήπως πρέπει να αποφεύγετε κάποιες συμπεριφορές;
- Σάς έχει τύχει να πρέπει να συμμορφωθείτε σε συγκεκριμένους κανόνες με τη συμμετοχή σας σε κάποια διαδικτυακή ομάδα ή κάποιο φόρουμ. Για παράδειγμα υπάρχουν ομάδες στο Facebook που για να δεχτούν ένα μέλος, πρέπει εκείνο να

συναινέσει και να ακολουθήσει κάποιους κανόνες. Αν δεν τους ακολουθεί μετά την τρίτη επίπληξη διαγράφεται από την ομάδα.

## Ενότητα 2η – Παιχνίδι ρόλων

- Οι εκπαιδευόμενοι χωρίζονται σε ομάδες και τους δίνεται ένα σενάριο. Έστω ότι η κάθε ομάδα εκπαιδευόμενων θέλει να δημιουργήσει μία ομάδα σε ένα από τα γνωστά μέσα κοινωνικής δικτύωσης. Προτείνεται να τούς κατευθύνετε ώστε να σκεφτούν το θέμα της ομάδας και τούς βασικούς κανόνες συμπεριφοράς, να τους καταγράψουν και να τούς παρουσιάσουν στην υπόλοιπη τάξη

## Ενότητα 3η – Συζήτηση

Μετά το τέλος όλων των παρουσιάσεων μπορεί να γίνει συζήτηση για τα κοινά και διαφορετικά τους σημεία. Τέλος, προτείνεται να μοιραστεί το σχετικό φυλλάδιο, το οποίο μπορεί να συμπεριλαμβάνει συμβουλές και πράξεις που θα πρέπει να αποφεύγουν οι χρήστες, όταν χρησιμοποιούν το Διαδίκτυο και συγκεκριμένα το ηλεκτρονικό ταχυδρομείο και τα μέσα κοινωνικής δικτύωσης. Αφού δοθεί στους εκπαιδευόμενους λίγος χρόνος για να δουν το φυλλάδιο, προτείνεται να ερωτηθούν :

- αν θέλουν κάποια επεξήγηση
- αν πιστεύουν ότι κάποιος από τους κανόνες δεν είναι χρήσιμος
- αν θέλουν να προσθέσουν κάποιον κανόνα ή κάποια συμβουλή

# Κεφάλαιο 5. Συζήτηση – Συμπεράσματα – Μελλοντικές επεκτάσεις

Το τελευταίο κεφάλαιο αφιερώνεται αφενός σε μία συνοπτική ανακεφαλαίωση της παρούσας διπλωματικής εργασίας αφετέρου στα συνοπτικά συμπεράσματα ανά ερευνητικό ερώτημα. Επίσης, γίνεται αναφορά σε τυχόν τρόπους για την αξιοποίηση της έρευνας.

## 5.1 Ανακεφαλαίωση

Το Διαδίκτυο όπως αναφέρθηκε διεξοδικά στην παρούσα εργασία, παίζει σημαντικό ρόλο στην καθημερινότητα όλων, καθώς παρέχει δυνατότητες που την διευκολύνουν και την βελτιώνουν. Χρησιμοποιείται για λόγους ψυχαγωγίας, για ηλεκτρονικές αγορές, στην εργασία, στην εκπαίδευση, και γενικά για την καθημερινή επικοινωνία όλων. Ταυτόχρονα χρησιμοποιείται από τη μεγαλύτερη μερίδα ανθρώπων, όλων των ηλικιών και ανεξαρτήτου εκπαιδευτικού επιπέδου. Η καθημερινή χρήση λοιπόν, σε συνδυασμό με την τεράστια εξέλιξή του, έχει φέρει στο προσκήνιο πολλούς κινδύνους.

Ο σκοπός της παρούσας εργασίας ήταν αφενός η ενημέρωση των χρηστών για τους συχνούς κινδύνους του ελεύθερου Διαδικτύου, τα χαρακτηριστικά τους, το που μπορεί να λάβουν χώρα τα φαινόμενα, τις επιπτώσεις τους, και αφετέρου να δοθούν διάφοροι τρόποι αντιμετώπισης και προφύλαξης από αυτούς. Η ενημέρωση των χρηστών προέκυψε ότι είναι ο πιο αποτελεσματικός τρόπος προστασίας. Οι τρόποι ενημέρωσης όπως αναφέρθηκαν, μπορεί να γίνουν με σεμινάρια, εκπαιδευτικά προγράμματα και τη δημιουργία πολιτικών ορθής χρήσης. Παράλληλα οι κανόνες δεοντολογικής συμπεριφοράς Διαδικτύου είναι ίσως ο πιο σημαντικός τρόπος ενημέρωσης και εκπαίδευσης των χρηστών για τη σωστή χρήση και συμπεριφορά του Διαδικτύου.

Ένας ακόμα σκοπός της εργασίας ήταν η συλλογή και η περιγραφή των πιο συχνά χρησιμοποιούμενων μηχανών αναζήτησης και διαδικτυακών πλατφορμών. Η συγκέντρωση αυτών των πληροφοριών συνεισφέρει στη κατάληξη κάποιων συμπερασμάτων όσων αφορά τους σκοπούς και τις αποστολές των διαδικτυακών πλατφορμών, όπως για παράδειγμα οι πλατφόρμες «εκδότες ειδήσεων και μέσων ενημέρωσης» έχουν στόχο:

- την άμεση ενημέρωση των χρηστών
- την προσπάθεια εξυπηρέτησης όλων των αναγκών
- την παροχή ποικίλων υπηρεσιών όπως email και άλλα

Η μεθοδολογία που ακολουθήθηκε για την αποπεράτωση της εργασίας ήταν συγκεκριμένη. Αρχικά για τη βιβλιογραφική επισκόπηση συλλέχθηκε το υλικό από τις πιο γνωστές βάσεις δεδομένων, έτσι ώστε το υλικό να είναι επιστημονικά τεκμηριωμένο και αρκετά σχετικό. Επίσης οι διαδικτυακές συλλογές που δημιουργήθηκαν ήταν ένα σημαντικό μέσο περιγραφής των πιο γνωστών ελεύθερων μηχανών αναζήτησης και των ελεύθερων διαδικτυακών πλατφορμών, και συνείσφερε ώστε να συγκεντρωθούν σε μια βάση δεδομένων οι περισσότερες πληροφορίες για αυτά.

Ακόμη, η δημιουργία των πρότυπων μαθημάτων είναι ένα σημαντικό κομμάτι της εργασίας, επειδή στηρίχθηκε στο θεωρητικό πλαίσιο και στα αποτελέσματα της βιβλιογραφικής επισκόπησής. Τα μαθήματα αυτά αφορούν τους κινδύνους που έχουν αναφερθεί στην εργασία και επίσης τους κανόνες δεοντολογικής συμπεριφοράς. Οι πληροφορίες και οι εκπαιδευτικές μέθοδοι που χρησιμοποιήθηκαν στα μαθήματα έχουν στηριχθεί στα υπό-κεφάλαια της εργασίας και θεωρείται ως το πιο αποτελεσματικό μέσο ενημέρωσης και εκπαίδευσής των χρηστών.

Τα αποτελέσματα της παρούσας διπλωματικής εργασίας όπως αναφέρθηκε και παραπάνω είναι ένα σημαντικό κομμάτι της έρευνας. Οι επιπτώσεις των κινδύνων είναι τεράστιες και πέρα από οικονομικά προβλήματα, τα ψυχολογικά προβλήματα είναι τα πιο σοβαρά. Τα αρνητικά συναισθήματα που νιώθουν τα θύματα, η απομόνωση και τα συναισθήματα άγχους και κατάθλιψης, μπορούν να στιγματίσουν για αρκετό καιρό τα θύματα. Είναι πολύ σημαντικό να ακολουθούνται οι τρόποι αντιμετώπισης και προφύλαξης των χρηστών που έχουν προταθεί στην εργασία, καθώς να προωθείται η ενημέρωση των χρηστών.

## 5.2 Συζήτηση / Συμπεράσματα

### 5.2.1. Συμπεράσματα ελεύθερων διαδικτυακών πλατφορμών

Στο πλαίσιο της παρούσας διπλωματικής εργασίας εξετάστηκε μία σειρά από διαδικτυακές πλατφόρμες που παρέχουν ελεύθερο περιεχόμενο και δωρεάν υπηρεσίες.

Οι βασικές κατηγορίες αυτών αναφέρονται στο κεφάλαιο 2.2.1. Συμπερασματικά, θα μπορούσαμε να πούμε ότι οι βασικές ομοιότητες που φέρουν είναι οι ακόλουθες:

- Δημιουργία ηλεκτρονικών κοινοτήτων / ομάδων, στις οποίες οι χρήστες συμμετέχουν για :
    - να συνδεθούν με άτομα με κοινά ή διαφορετικά ενδιαφέροντα,
    - να εκφράσουν απόψεις, ιδέες και εμπειρίες

- να επικοινωνήσουν με άλλους και να κοινωνικοποιηθούν (Τέχνες και Ψυχαγωγία, Κοινότητα και κοινωνία, Παιχνίδια, Βαριά βιομηχανία και μηχανολογία, Αθλητισμός , Ηλεκτρονικοί υπολογιστές και τεχνολογία)

- Παροχή πληροφοριών και ενημερώσεων στους χρήστες για όλα τα θέματα (Τέχνες και Ψυχαγωγία, Κοινότητα και κοινωνία, Φαγητό και ποτό, Υγείας, Νόμος και κυβέρνηση, Εκδότες ειδήσεων και μέσων ενημέρωσης, Υλικά αναφορά, Επιστήμη και εκπαίδευση, Ταξίδια και τουρισμός, Οχήματα, Ηλεκτρονικοί υπολογιστές και τεχνολογία)
- Δημιουργία καινοτόμων υπηρεσιών και προϊόντων προκειμένου να εξυπηρετηθούν σωστά και αποτελεσματικά οι καταναλωτές (Τέχνες και Ψυχαγωγία, Επιχειρηματικές και καταναλωτικές υπηρεσίες, Ηλεκτρονικό Εμπόριο & αγορές, Οικονομικών, Παιχνίδια, Υγείας, Βαριά βιομηχανία και μηχανολογία, Χόμπι και τον Ελεύθερο χρόνο, Εργασία και Καριέρα, Νόμος και κυβέρνηση, Lifestyle, Εκδότες ειδήσεων και μέσων ενημέρωσης, Επιστήμη και εκπαίδευση)
- Άμεση και αποτελεσματική εξυπηρέτηση των χρηστών (Τέχνες και Ψυχαγωγία, Επιχειρηματικές και καταναλωτικές υπηρεσίες, Κοινότητα και κοινωνία, Ηλεκτρονικό Εμπόριο & αγορές, Οικονομικών, Βαριά βιομηχανία και μηχανολογία, Χόμπι και τον Ελεύθερο χρόνο, Σπίτι και κήπος, Νόμος και κυβέρνηση, Lifestyle, Εκδότες ειδήσεων και μέσων ενημέρωσης, Κατοικίδια και ζώα)
- Δημιουργία ασφαλούς εργασιακού περιβάλλοντος που σέβεται τους εργαζομένους και προωθεί την ανάπτυξη του ομαδικού πνεύματος (Επιχειρηματικές και καταναλωτικές υπηρεσίες, Ηλεκτρονικό Εμπόριο & αγορές, Οικονομικών, Βαριά βιομηχανία και μηχανολογία, Σπίτι και κήπος, Εργασία και Καριέρα, Υλικά αναφορά, Ταξίδια και τουρισμός)
- Παροχή έμπιστων υπηρεσιών και διαδικασιών που θα προστατεύουν και θα κρατάνε ασφαλή το απόρρητο και τα δεδομένα των χρηστών (Επιχειρηματικές και καταναλωτικές υπηρεσίες, Κοινότητα και κοινωνία, Ηλεκτρονικό Εμπόριο & αγορές, Νόμος και κυβέρνηση, Ταξίδια και τουρισμός, Ηλεκτρονικοί υπολογιστές και τεχνολογία)
- Δημιουργία αισθήματος σεβασμού στη μοναδικότητα και διαφορετικότητα των χρηστών και των αναγκών τους (Οικονομικών, Σπίτι και κήπος, Εκδότες ειδήσεων και μέσων ενημέρωσης, Υλικά αναφορά, Επιστήμη και εκπαίδευση)
- Δημιουργία αισθήματος ελευθερίας έκφρασης (Τέχνες και Ψυχαγωγία, Κοινότητα και κοινωνία, Ηλεκτρονικοί υπολογιστές και τεχνολογία)

- Ψυχαγωγία (Παιχνίδια, Οχήματα).

Ωστόσο, σε κάποιες πλατφόρμες εντοπίστηκαν οι ακόλουθες διαφορές, «οι οποίες κατά βάση είναι σχετικές με την ποικιλία περιεχομένου που παρουσιάζεται»:

- Η δυνατότητα αποθήκευσης περιεχομένου χρηστών, όπως φωτογραφιών, και βίντεο (Χόμπι και Ελεύθερο χρόνο)
- Η προσπάθεια ανάπτυξης συνείδησης κόστους και η δημιουργία οικονομικών και ανταγωνιστικών επιλογών (Σπίτι και κήπος)
- Η προώθηση του ηλεκτρονικού εμπορίου (Lifestyle)
- Η ανάπτυξη της ευαισθητοποίησης για τα κατοικίδια ζώα (Κατοικίδια και ζώα)
- Η προώθηση της εκπαιδευτικής διαδικασίας (Επιστήμη και εκπαίδευση)
- Η προώθηση του αθλητισμού (Αθλητισμός)
- Η διευκόλυνση της αγοραπωλησίας οχημάτων (Οχήματα)
- Η προσπάθεια ανάπτυξης και διατήρησης φήμης που θα εκπέμπει σεβασμό στους πελάτες, την κοινωνία και τους συνεργάτες (Εκδότες ειδήσεων και μέσων ενημέρωσης).

### 5.2.2. Συμπεράσματα διαδικτυακού εκφοβισμού

Ο διαδικτυακός εκφοβισμός είναι η εξελιγμένη μορφή του παραδοσιακού εκφοβισμού, που συμβαίνει μέσω του Διαδικτύου και των νέων τεχνολογικών μέσων.

Τα χαρακτηριστικά του είναι η επανάληψη, η πρόθεση για βλάβη, η ανισορροπία δύναμης, η ανωνυμία και η προσβασιμότητα.

Το φύλο δεν παίζει κάποιο ρόλο στη διάπραξη διαδικτυακού εκφοβισμού, καθώς έρευνες δείχνουν ότι τόσο οι άντρες όσο και οι γυναίκες μπορούν να τον διαπράξουν.

Υπάρχουν επτά είδη διαδικτυακού εκφοβισμού. Η μεταμφίεση, το flaming, ο αποκλεισμός, η δυσφήμιση, η παραπλάνηση / έκθεση, η παρενόχληση και η καταδίωξη. Όλα αυτά έχουν σαν στόχο να προκαλέσουν συναισθηματική δυσφορία στα θύματα.

Σύμφωνα με τις έρευνες, μπορούν να υπάρξουν έξι ρόλοι ατόμων που σχετίζονται με τον διαδικτυακό εκφοβισμό. Το θύμα, ο θύτης, ο παρατηρητής – υποστηρικτής του εκφοβιστή, ο παρατηρητής – προστάτης του θύματος, ο εκδικητής και ο θύτης σε ρόλο θύματος.

Οι επιπτώσεις πλήττουν τη ψυχική υγεία όλων όσων συμμετέχουν σε αυτόν, δηλαδή είτε είναι το θύμα, ο θύτης ή ο παρατηρητής. Και αυτά που προκαλούν είναι ψυχολογικά, κοινωνικά και συναισθηματικά προβλήματα, όπως στρες, κοινωνικό άγχος, κατάθλιψη και σε κάποιες περιπτώσεις αυτά τα συναισθήματα οδηγούν σε αυτοκτονικές τάσεις.

Οι λόγοι διάπραξης διαδικτυακού εκφοβισμού είναι η ψυχαγωγία και η διασκέδαση, η εκδίκηση και η απόδοση δικαιοσύνης ή αντίποινων και οι κακές διαπροσωπικές σχέσεις, δηλαδή χαμηλή αυτοεκτίμηση ή προσπάθεια προσέλκυσης της προσοχής.

Τα μέσα στα οποία συμβαίνει είναι το email, τα διαδικτυακά δωμάτια συνομιλίας, οι ιστότοποι κοινωνικής δικτύωσης, αλλά μπορεί να συμβεί και μέσω γραπτών και φωνητικών μηνυμάτων σε κινητά τηλέφωνα και από ανώνυμους αποστολείς.

Ο καλύτερος τρόπος αντιμετώπισης αυτού του φαινομένου είναι η ενημέρωση. Η ενημέρωση για τα χαρακτηριστικά του ίδιου του φαινόμενου, τις επιπτώσεις και τους τρόπους προφύλαξης. Τα άτομα που θα πρέπει να ενημερωθούν είναι μαθητές, εκπαιδευτικοί, νέοι γονείς και γενικά οι νέοι. Ο τρόπος ενημέρωσης θα μπορούσε να λάβει χώρα με την πραγματοποίηση σεμιναρίων, εκπαιδευτικών προγραμμάτων και συναντήσεων με ειδικούς συμβούλους.

### 5.2.3. Συμπεράσματα εμπορευματοποίησης προσωπικών δεδομένων

Η εμπορευματοποίηση προσωπικών δεδομένων είναι η διαδικασία κατά την οποία τα προσωπικά δεδομένα αντιμετωπίζονται σαν εμπορεύματα, αποκτούν αξία και τελικά πωλούνται για την απολαβή κέρδους.

Οι μηχανές αναζήτησης, οι πλατφόρμες κοινωνικής δικτύωσης και άλλα μέσα, συγκεντρώνουν μέσω εξελιγμένων συστημάτων, πληθώρα προσωπικών και ευαίσθητων δεδομένων. Αυτά τα έχουν μοιραστεί οι χρήστες είτε εν γνώση τους (με την δημιουργία προφίλ σε κάποιο μέσω κοινωνικής δικτύωσης) είτε εν αγνοία τους (με την αναζήτηση διάφορων πληροφοριών σε μηχανές αναζήτησης). Όλα αυτά συγκεντρώνονται και ανάλογα αν είναι ολοκληρωμένα προφίλ ή μεμονωμένα δεδομένα αποκτούν μεγαλύτερη ή μικρότερη αξία αντίστοιχα.

Η αξία που αποκτούν, αφορά τη δημόσια εξέλιξη, την περίθαλψη, την εκπαίδευση, ακόμα και την πρόληψη της τρομοκρατίας. Ωστόσο, η αξία τους, αφορά πολλές εταιρείες και διαφημιστές, οι οποίοι αποκτούν κέρδος δημιουργώντας και προωθώντας στοχευμένες διαφημίσεις και προβλέψεις καταναλωτικών συμπεριφορών.

Τα προσωπικά δεδομένα που συγκεντρώνονται μπορεί να είναι το φύλο, η ηλικία, ο τόπος κατοικίας, η οικογενειακή κατάσταση, το επάγγελμα, αλλά και τα ενδιαφέροντα και οι αγοραστικές προτιμήσεις των καταναλωτών.

Όλα αυτά είναι χρήσιμα για ασφαλιστικές εταιρείες, για τράπεζες, διαφημιστικές εταιρείες αλλά ακόμα και για τον δημόσιο οργανισμό υγείας.

Ο κύκλος ζωής των δεδομένων αποτελείται από τέσσερα στάδια. Την συλλογή, την επεξεργασία, την εξόρυξη και τη χρήση των δεδομένων.

Οι συνέπειες της εμπορευματοποίησης των δεδομένων είναι πολλές. Είναι η διαρροή των δεδομένων, η κοινή χρήση δεδομένων σε τρίτους και η παραβίαση λογαριασμών από τρίτους. Ωστόσο, η πιο σημαντική και η πιο άμεσα συνδεδεμένη με το φαινόμενο συνέπεια, είναι η στοχευμένη διαφήμιση. Η διαφήμιση, δηλαδή που στοχεύει σε συγκεκριμένο κοινό και έχει κατασκευαστεί από πληροφορίες που είναι σχετικές με :

- το διαδικτυακό προφίλ του κάθε χρήστη, (ένα προφίλ που έχει κατασκευαστεί από εταιρείες ή πλατφόρμες)
- τις αγοραστικές συνήθειες
- το ιστορικό αναζητήσεων

Δεδομένα δηλαδή που έχουν αποκτηθεί παράνομα από εταιρείες ώστε να δημιουργήσουν το «τέλειο προϊόν». Αυτό καταπιέζει τους καταναλωτές και προσβάλει το ιδιωτικό απόρρητο.

Η καλύτερη στρατηγική διαφύλαξης των δεδομένων είναι ο έλεγχος τους, και ο έλεγχος του βαθμού που θα έχουν πρόσβαση οι εταιρείες και οι πλατφόρμες σε αυτά.

Για να επιτευχθεί αυτό πρέπει να ενισχυθεί η ανάπτυξη κανονισμών απορρήτου των δεδομένων αλλά και η συμμόρφωση σε αυτούς. Τέτοιοι κανονισμοί είναι το GDPR, το PIPEDA το CCPA και άλλα.

Παράλληλα, οι πιο διαδεδομένοι τρόποι προφύλαξης των προσωπικών δεδομένων είναι :

- Η εγκατάσταση ενός προγράμματος προστασίας από ιούς, σε όλες τις συσκευές που έχουν πρόσβαση στο Διαδίκτυο
- Η διαγραφή του ιστορικού αναζητήσεων και των αποθηκευμένων κωδικών από υπολογιστές τρίτων
- Η διαρκής και συστηματική ενημέρωση και εκπαίδευση του χρήστη του Διαδικτύου

### 5.2.4. Συμπεράσματα απάτης διαδικτυακής ταυτότητας

Η απάτη διαδικτυακής ταυτότητας είναι ένα διάχυτο και συχνό φαινόμενο που σχετίζεται με την εξέλιξη της τεχνολογίας και την αύξησης χρήσης του Διαδικτύου. Η ευθύνη για αυτό, βαρύνει τόσο τους καταναλωτές, κυρίως λόγω μη φιλτραρίσματος των δεδομένων που μοιράζονται και κακής χρήσης των μηχανών αναζήτησης και των πλατφορμών κοινωνικής δικτύωσης, όσο και τους οργανισμούς και τις εταιρείες παροχής εφαρμογών αλλά και τους νομοθετικούς φορείς.

Η απάτη διαδικτυακής ταυτότητας ορίζεται ως η χρήση πραγματικών ή και ψευδών δεδομένων ή και ο συνδυασμός αυτών, με σκοπό την εξαπάτηση τρίτων ή με στόχο την απολαβή οικονομικού ή υλικού κέρδους.

Τα πιο γνωστά είδη απάτης είναι το phishing, το φωνητικό phishing, το pharming, το skimming, και το κακόβουλο λογισμικό όπως ιοί.

Η απάτη ταυτότητας αυξάνεται συνεχώς, λόγω της αύξησης του Διαδικτύου και της αύξησης χρήσης των ψηφιακών μέσων. Τα στατιστικά δείχνουν ότι όλο και περισσότεροι ενήλικες έχουν πέσει θύματα ή γνωρίζουν περιπτώσεις απάτης ταυτότητας.

Μπορεί να συμβεί στα μέσα κοινωνικής δικτύωσης και μέσω των έξυπνων συσκευών, κινητών, ρολογιών και άλλων τέτοιων μέσων, καθώς οι χάκερ μπορούν να έχουν εύκολα πρόσβαση στα δεδομένα που έχουν αποθηκευτεί σε αυτά.

Οι συνέπειες αυτού του φαινομένου πλήττουν πέρα από τους καταναλωτές, τις τράπεζες και τους εμπόρους ηλεκτρονικού εμπορίου. Παράλληλα, οι καταναλωτές δεν βιώνουν μόνο υλικές και οικονομικές απώλειες, αλλά και συναισθηματικές, καθώς πολλοί αποκτούν συναισθήματα άγχους, φοβίες και ρήξεις σε διαπροσωπικές σχέσεις, λόγω ανασφάλειας και έλλειψης εμπιστοσύνης.

Ως τρόποι αντιμετώπισης του φαινομένου προτείνονται οκτώ στάδια διαχείρισης της απάτης. Αυτά είναι η αποτροπή, η πρόληψη, ο εντοπισμός, ο μετριασμός, η ανάλυση, η πολιτική, η διερεύνηση και η δίωξη. Πέρα από αυτά όμως το πιο σημαντικό μέτρο είναι η ενημέρωση των χρηστών για το φαινόμενο και η εκπαίδευση για σωστή χρήση και προφύλαξη.

Επιπλέον, έχουν προτείνονται καλές πρακτικές που μπορούν να προστατεύσουν τους χρήστες από το να πέσουν θύματα αυτού του φαινομένου:

- Αποφυγή «ανοίγματος» μηνυμάτων από άγνωστους αποστολείς και «κατέβασμα» των επισυναπτόμενων αρχείων
- Αποφυγή συμπλήρωσης φορμών με προσωπικά ή τραπεζικά στοιχεία, για συμμετοχή σε διαγωνισμούς από άγνωστες πηγές
- Ανάγνωση πάντα των ορών χρήσης μίας ιστοσελίδας πριν την αποδοχή τους
- Προσπάθεια για έρευνα των ψηφιακών καταστημάτων, μέσω των αξιολογήσεων και των κριτικών που έχουν γίνει από άλλους χρήστες, πριν την ολοκλήρωση κάποιας διαδικτυακής αγοράς
- Αγορά προϊόντων από ιστοσελίδες, με πιστωτικές κάρτες ή προπληρωμένες κάρτες για αποφυγή κλοπής τραπεζικών στοιχείων

### 5.2.5. Συμπεράσματα των κανόνων χρήσης Διαδικτύου

Οι κανόνες χρήσης του Διαδικτύου (netiquette rules) είναι οι κανόνες κατάλληλης επικοινωνιακής συμπεριφοράς στο Διαδίκτυο και είναι απαραίτητοι για τη σωστή χρήση και λειτουργία της νέας ψηφιακής πραγματικότητας.

Οι λόγοι ύπαρξης και προώθησης των κανόνων είναι πολλοί. Αρχικά πρέπει όλοι να γνωρίζουν να χρησιμοποιούν σωστά το Διαδίκτυο διότι παίζει καθοριστικό ρόλο στην εξέλιξη της κοινωνικής ζωής, στην εκπαίδευση, στην εργασία και σε πολλούς ακόμη τομείς.

Ο πιο αποτελεσματικός τρόπος ενημέρωσης και επιμόρφωσης είναι η δημιουργία σεμιναρίων και εκπαιδευτικών προγραμμάτων για όλες τις ηλικίες. Ενώ πολλοί καταλήγουν ότι πρέπει να δημιουργηθεί εισαγωγικό μάθημα και να διδάσκεται στα πανεπιστήμια.

Οι κανόνες χρήσης του Διαδικτύου αφορούν τη χρήση του ηλεκτρονικού ταχυδρομείου, τη λειτουργία των μέσων κοινωνικής δικτύωσης όπως Facebook, Twitter, και γενικά τη συμμετοχή των χρηστών σε ομάδες κοινωνικής δικτύωσης. Εν κατακλείδι, αφορούν όλα τα είδη διαδικτυακής επικοινωνίας.

## 5.3 Αξιοποίηση / Πρακτικές προεκτάσεις της έρευνας

Η παρούσα διπλωματική εργασία απευθύνεται σε εκπαιδευτικούς και επιστήμονες της πληροφόρησης και προσφέρει σημαντικές λεπτομέρειες και αναλυτικές πληροφορίες για το «ελεύθερο» Διαδίκτυο. Όσοι τη διατρέξουν μπορούν να ενημερωθούν για τους σημαντικότερους κινδύνους που ενέχει η χρήση του, καθώς και τους τρόπους αντιμετώπισης αυτών. Παράλληλα, τα εκπαιδευτικά σενάρια που έχουν δημιουργηθεί στο πλαίσιο της εργασίας μπορούν να αξιοποιηθούν από τους αναγνώστες της εργασίας, αφενός για να ενημερωθούν οι ίδιοι για τα φαινόμενα αφετέρου για να τα χρησιμοποιήσουν ώστε να ενημερώσουν τρίτους, όπως για παράδειγμα φοιτητές και μαθητές ή και το κοινό κάποιας βιβλιοθήκης. Σημειώνεται ότι αυτή η ενημέρωση εντάσσεται στο πλαίσιο του επιστημονικού πεδίου Μέσα και Πληροφοριακή Παιδεία.

Οι διαδικτυακές συλλογές που έχουν δημιουργηθεί στην πλατφόρμα omeka.net είναι ένα πολύ σημαντικό εργαλείο για όλους, διότι εκεί έχουν συγκεντρωθεί και αναλυθεί οι κορυφαίες σε επισκεψιμότητα ελεύθερες διαδικτυακές πλατφόρμες και μηχανές αναζήτησης. Με αυτόν τον τρόπο ο αναγνώστης μπορεί να αντλήσει σημαντικές πληροφορίες για αυτές, όπως τη σύντομη περιγραφή τους, την ιστορική αναδρομή, τους στόχους και την αποστολή τους. Τέλος, το κάθε εκπαιδευτικό σενάριο που προτείνεται στο πλαίσιο της παρούσας εργασίας έχει αναρτηθεί σε μία ξεχωριστή συλλογή στην πλατφόρμα

omeka.net και έχει διασυνδεθεί με τις εγγραφές των πλατφορμών και των μηχανών αναζήτησης ιστού, μέσω θεματικών ετικετών.

## 5.4 Μελλοντικές επεκτάσεις / Πρακτικές Προεκτάσεις της Έρευνας

Κάποιες μελλοντικές προεκτάσεις που θα μπορούσαν να γίνουν στην έρευνα αφορούν στην εμβάθυνση του καθενός από τα θέματα της βιβλιογραφίας. Για παράδειγμα, ένας ερευνητής θα μπορούσε να ασχοληθεί σε βάθος ειδικά για το θέμα του διαδικτυακού εκφοβισμού, κ.ο.κ. Ταυτόχρονα, μία πρακτική προέκταση της έρευνας θα μπορούσε να πραγματοποιηθεί με το να εφαρμόσει κάποιος ερευνητής τα εκπαιδευτικά σενάρια και στη συνέχεια να τα αξιολογήσει μέσω ερωτηματολογίων. Τα αποτελέσματα αυτής της διαδικασίας θα μπορούσαν να συμβάλλουν σε προτάσεις για βελτιστοποίηση των προτεινόμενων σεναρίων ή ακόμα για δημιουργία νέων, τα οποία να απευθύνονται σε ξεχωριστές ηλικιακές ομάδες, όπως παιδιά, εφήβους, νέους, άτομα τρίτης ηλικίας κ.ά.

Ακόμη, μία πρακτική προέκταση θα μπορούσε να είναι ο εμπλουτισμός των σελίδων στην πλατφόρμα omeka.net με περισσότερες ελεύθερες διαδικτυακές πλατφόρμες και μηχανές αναζήτησης. Με αυτό τον τρόπο θα μπορούσε να υπάρχει μία σελίδα που να ανανεώνεται διαρκώς και να περιλαμβάνει σημαντικές λεπτομέρειες για τις κορυφαίες μηχανές αναζήτησης και πλατφόρμες του Διαδικτύου.

# Βιβλιογραφικές Αναφορές


Abifarin, F. P., & Tsetim, P. Z. (2018a). *Impact of training on compliance with netiquette rules by students*. http://repository.futminna.edu.ng:8080/jspui/handle/123456789/6247

Abifarin, F. P., & Tsetim, P. Z. (2018b). *Impact of training on compliance with netiquette rules by students*. http://repository.futminna.edu.ng:8080/jspui/handle/123456789/6247

Arouri, Y. M., & Hamaidi, D. A. (2017). Undergraduate Students' Perspectives of the Extent of Practicing Netiquettes in a Jordanian Southern University. *International Journal of Emerging Technologies in Learning (IJET)*, *12*(03), 84–97. https://doi.org/10.3991/IJET.V12I03.6424

Ayhan, A. (2019). New Approaches in Media and Communication. *New Approaches in Media and Communication*, 1–432. https://doi.org/10.3726/B15661

Bansal, A., Mahadev Sharma, S., Kumar, K., Aggarwal, A., Goyal, S., Choudhary, K., Chawla, K., Jain, K., & Bhasin, M. (2011). Classification of Flames in Computer Mediated Communications. *International Journal of Computer Applications*, *14*(6), 975–8887.

Bartl, R. (n.d.). Impact of Netiquette on Email Communication. *Journal of Applied Leadership and Management*, *5*, 35–61.

Botes, M., Olckers, A., Labuschaigne, M., Botes, M., Olckers, A., & Labuschaigne, M. (2022). Data commercialisation in the South African health care context. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *24*(1). https://doi.org/10.17159/1727

Bottis, M., & Bouchagiar, G. (2018). Personal Data v. Big Data in the EU: Control Lost, Discrimination Found. *Open Journal of Philosophy*, *8*, 192–205. https://doi.org/10.4236/ojpp.2018.83014

Canellopoulou-Bottis, M., & Bouchagiar, G. (2018). Personal Data v. Big Data: Challenges of Commodification of Personal Data. *Intellectual Property: Other EJournal*, *08*(03), 206–215. https://doi.org/10.4236/OJPP.2018.83015

Chan, H. C., & Wong, D. S. W. (2020). The overlap between cyberbullying perpetration and victimisation: exploring the psychosocial characteristics of Hong Kong adolescents. *Https://Doi.Org/10.1080/02185385.2020.1761436*, *30*(3), 164–180. https://doi.org/10.1080/02185385.2020.1761436

Cherus, J., Githeko, J., Siror, J., & Njagi, K. (2014). Identity Fraud: A Literature Review and Future Research Directions. *ADRRI Journal (Multidisciplinary)*, *5*(5), 36–53. https://doi.org/10.55058/ADRRIJ.V5I5.47

Chillemi, K., Abbott, J. A. M., Austin, D. W., & Knowles, A. (2020). A Pilot Study of an Online Psychoeducational Program on Cyberbullying That Aims to Increase Confidence and Help-Seeking Behaviors Among Adolescents. *Cyberpsychology, Behavior and Social Networking*, *23*(4), 253–256. https://doi.org/10.1089/CYBER.2019.0081

Cinar, N., & Ateş, S. (2022). Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4041963

Conlin, B., & Ruhi, U. (2021). Current Research Landscape of Machine Learning Algorithms in Online Identity Fraud Prediction and Detection. *2021 IEEE International Conference on Technology Management, Operations and Decisions, ICTMOD 2021*. https://doi.org/10.1109/ICTMOD52902.2021.9739308

Cross, C., Smith, R., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and Issues in Crime and Criminal Justice*. http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi474.pdf

cyberalert.gr. (2015). *Απάτες μέσω Διαδικτύου*. Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. https://cyberalert.gr/apates-meso-diadiktiou/

Dadvar, M., Trieschnigg, D., Ordelman, R., & de Jong, F. (2013). Improving cyberbullying detection with user context. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7814 LNCS*, 693–696. https://doi.org/10.1007/978-3-642-36973-5_62

DiSanto, P. (2014). *Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud*. https://papers.ssrn.com/abstract=2515578

Dou, G., Xiang, Y., Sun, X., & Chen, L. (2020). Link Between Cyberbullying Victimization and Perpetration Among Undergraduates: Mediating Effects of Trait Anger and Moral Disengagement . *Psychology Research and Behavior Management*, *13*, 1269–1276. https://doi.org/10.2147/PRBM.S286543

Douilhet, E., & Karanasiou, A. P. (2016). Legal responses to the commodification of personal data in the era of big data: The paradigm shift from data protection towards data ownership. *Effective Big Data Management and Opportunities for Implementation*, 130–139. https://doi.org/10.4018/978-1-5225-0182-4.CH009

Notar, C., Padgett, S., & Roden, J. (2013). Cyberbullying: A Review of the Literature. *Universal Journal of Educational Research*, *1*(1), 1–9. https://doi.org/10.13189/UJER.2013.010101

El-Khoury, M. (2021). The impact of data protection laws: Global and MENA perspectives. *2021 22nd International Arab Conference on Information Technology, ACIT 2021*. https://doi.org/10.1109/ACIT53391.2021.9677394

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining Cyberbullying. *Pediatrics*, *140* (Suppl 2), S148–S151. https://doi.org/10.1542/PEDS.2016-1758U

fortunegreece.com. (2020, February 18). *Τι είναι η gig economy και πώς άλλαξε τον κλάδο της απασχόλησης παγκοσμίως | Fortunegreece.com*. Fortunegreece.Com. https://www.fortunegreece.com/article/ti-ine-i-gig-economy-ke-pos-allaxe-ton-klado-tis-apascholisis-pagkosmios/

Gawer, A., & Srnicek, N. (2021). *Online platforms: Economic and societal effects* (European Parliament, Ed.). https://kclpure.kcl.ac.uk/portal/files/149143202/EPRS_STU_2021_656336_EN.pdf

Gilbert, J., & Archer, N. (2011). Consumer identity theft prevention and identity fraud detection behaviours. *Journal of Financial Crime*, *19*(1), 20–36. https://doi.org/10.1108/13590791211190704/FULL/PDF

Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via Social Media and Well-Being. *Current Opinion in Psychology*, 101314. https://doi.org/10.1016/J.COPSYC.2022.101314

Gyourko, J. R., & Greeson, J. K. P. (2022). Annual Credit Checks for Adolescent Youth in Foster Care: Factors Associated with Identity Fraud Victimization. *Https://Doi.Org/10.1177/10775595221101504*, *2022*(0), 1–12. https://doi.org/10.1177/10775595221101504

Hanka, O. (2012). How to prevent identity fraud in locator/identifier - Split architectures. *2012 International Conference on Computing, Networking and Communications, ICNC'12*, 683–689. https://doi.org/10.1109/ICCNC.2012.6167510

Ifon, J. C. (2022). Management of Cyberbullying: A Qualitative Exploratory Case Study of a Nigerian University. *International Journal of Bullying Prevention 2022*, 1–17. https://doi.org/10.1007/S42380-022-00124-Y

Iqbal, S., Hanif, R., Ali, F., Tahir, M., Minhas, R., Yasmeen, R., Khokhar, A., & Laique, T. (2021). Teachers' Perceptions of Netiquette Practices by undergraduate Dental Students During

Online Classes in Covid-19 Pandemic. *Pakistan Journal of Medical and Health Sciences*, *15*(12), 3498–3500. https://doi.org/10.53350/PJMHS2115123498

Karanasiou, A. P., & Douilhet, E. (2016). Never mind the data: The legal quest over control of information & the networked self. *Proceedings - 2016 IEEE International Conference on Cloud Engineering Workshops, IC2EW 2016*, 100–105. https://doi.org/10.1109/IC2EW.2016.39

Kavuk-Kalender, M., & Keser, H. (2018). Cyberbullying Awareness in Secondary and High Schools. *World Journal on Educational Technology: Current Issues*, *10*(4), 25–36. www.wj-et.eu

Khani, R., & Darabi, R. (2014). ScienceDirect Flouting the Netiquette Rules in the Academic Correspondence in Iran. *Procedia-Social and Behavioral Sciences*, *98*, 898–907. https://doi.org/10.1016/j.sbspro.2014.03.498

Lee, C. S. (2020). A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea. *Crime, Law and Social Change*, *74*(2), 201–218. https://doi.org/10.1007/S10611-020-09885-3/FIGURES/1

Lee, S. S., Song, H., & Park, J. H. (2021). Exploring Risk and Protective Factors for Cyberbullying and Their Interplay: Evidence from a Sample of South Korean College Students. *International Journal of Environmental Research and Public Health*, *18*(24). https://doi.org/10.3390/IJERPH182413415

Lehtiniemi, T. (2017). Personal Data Spaces: An Intervention in Surveillance Capitalism? *Surveillance & Society*, *15*(5), 626–639. https://doi.org/10.24908/ss.v15i5.6424

Li, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International*, *27*(2), 157–170. https://doi.org/10.1177/0143034306064547

Liu, W., Ren, P., Sun, D., & Wang, Z. (2012). Research in techniques of personal identity management. *Proceedings - 2012 International Conference on Control Engineering and Communication Technology, ICCECT 2012*, 912–915. https://doi.org/10.1109/ICCECT.2012.53

Livingstone, S., Burton, P., Cabello, P., Helsper, E., Kanchev, P., Kardefelt-Winther, D., Perovic, J., Stoilova, M., & Yu, S.-H. (2020). Media and Information Literacy among Children on Three Continents: Insights into the Measurement and Mediation of Well-being. *Media and Information Literacy in Critical Times: Re-Imagining Learning and Information Environments*.

Lord, J. (2012). The case for strong identities. *Computer Fraud & Security*, *2012*(5), 16–17. https://doi.org/10.1016/S1361-3723(12)70043-X

Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289–303. https://doi.org/10.1016/J.CLSR.2017.08.006

nibusinessinfo.co.uk. (n.d.). *What is a search engine and how do they work? | nibusinessinfo.co.uk*. Invest Northern Ireland in Partenship with Nidirect. Retrieved January 6, 2023, from https://www.nibusinessinfo.co.uk/content/what-search-engine-and-how-do-they-work

Niu, G., He, J., Lin, S., Sun, X., & Longobardi, C. (2020). Cyberbullying Victimization and Adolescent Depression: The Mediating Role of Psychological Security and the Moderating Role of Growth Mindset. *International Journal of Environmental Research and Public Health*, *17*(12), 1–13. https://doi.org/10.3390/IJERPH17124368

Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. *Aggression and Violent Behavior*, *23*, 69–74. https://doi.org/10.1016/J.AVB.2015.05.013

Pennell, D., Campbell, M., Tangen, D., & Knott, A. (2022). Should Australia have a law against cyberbullying? Problematising the murky legal environment of cyberbullying from perspectives within schools. *Australian Educational Researcher*, *49*(4), 827–844. https://doi.org/10.1007/S13384-021-00452-W/TABLES/1

Rose, B. (2021). THE COMMODIFICATION OF PERSONAL DATA AND THE ROAD TO CONSUMER AUTONOMY THROUGH THE CCPA. *Brooklyn Journal of Corporate, Financial & Commercial Law*, *15*(2). https://brooklynworks.brooklaw.edu/bjcfcl/vol15/iss2/8

Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior*, *29*(6), 2703–2711. https://doi.org/10.1016/J.CHB.2013.06.040

Saleem, S., Khan, N. F., Zafar, S., & Raza, N. (2022). Systematic literature reviews in cyberbullying/cyber harassment: A tertiary study. *Technology in Society*, *70*, 102055. https://doi.org/10.1016/J.TECHSOC.2022.102055

sec.eff.org. (n.d.). *Lessons | Security Education Companion*. Security Education Companion. Retrieved January 6, 2023, from https://sec.eff.org/topics/

Sevignani, S. (2013). The commodification of privacy on the internet. *Science and Public Policy*, *40*(6), 733–739. https://doi.org/10.1093/SCIPOL/SCT082

Similarweb.com. (2023). *Website Traffic - Check and Analyze Any Website | Similarweb*. Similarweb. https://www.similarweb.com/

Simon Enoch, Y., Kolawole John, A., & Emmanuel Olumuyiwa, A. (2013). Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique. *IJACSA) International Journal of Advanced Computer Science and Applications*, *4*(3). www.ijacsa.thesai.org

Skovgaard, L. L., Wadmann, S., & Hoeyer, K. (2019). A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. *Health Policy*, *123*(6), 564–571. https://doi.org/10.1016/J.HEALTHPOL.2019.03.012

Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, *29*(1), 26–32. https://doi.org/10.1016/J.CHB.2012.05.024

Sonker, A., Kumar, S., & Sharma, S. (2020). A Review of Dangers on Internet. *Interdisciplinary Cycle Research*, *XII*(VII), 548–553.

Soomro, Z. A., Ahmed, J., Shah, M. H., & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: a systematic review. *Journal of Enterprise Information Management*, *32*(2), 301–324. https://doi.org/10.1108/JEIM-06-2018-0110/FULL/PDF

Soomro, Z. A., Shah, M. H., & Thatcher, J. (2021). A framework for ID fraud prevention policies in E-tailing sector. *Computers & Security*, *109*, 102403. https://doi.org/10.1016/J.COSE.2021.102403

Tan, F. T. C., Guo, Z., Cahalane, M., & Cheng, D. (2016). Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution. *Information & Management*, *53*(7), 878–891. https://doi.org/10.1016/J.IM.2016.07.002

Tronnier, F., Pape, S., Löbner, S., & Rannenberg, K. (2022). A Discussion on Ethical Cybersecurity Issues in Digital Service Chains. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13300 LNCS*, 222–256. https://doi.org/10.1007/978-3-031-04036-8_10/TABLES/2

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ERCL-2018-1022

vom Lehn, H., Koepsell, D., & Cunningham, S. (2014). *On data markets as a means to privacy protection: An ethical evaluation of the treatment of personal data as a commodity*. https://repository.tudelft.nl/islandora/object/uuid%3A5b5c8888-9670-464c-945f-8f586bd77235

Wang, L., & Ngai, S. S. yum. (2022). Cyberbullying Perpetration Among Chinese Adolescents: The Role of Power Imbalance, Fun-seeking Tendency, and Attitude Toward Cyberbullying. *Journal of Interpersonal Violence*, *37*(23–24), NP21646–NP21671. https://doi.org/10.1177/08862605211062988/ASSET/IMAGES/LARGE/10.1177_08862605211062988-FIG1.JPEG

Wang, W., Zhang, J., Li, Q., Zong, C., & Li, Z. (2019). Are You for Real? Detecting Identity Fraud via Dialogue Interactions. *EMNLP-IJCNLP 2019 - 2019 Conference on Empirical Methods in Natural Language Processing and 9th International Joint Conference on Natural Language Processing, Proceedings of the Conference*, 1762–1771. https://doi.org/10.48550/arxiv.1908.06820

Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, *69*, 268–274. https://doi.org/10.1016/J.CHB.2016.12.038

Whittaker, E., & Kowalski, R. M. (2014). Cyberbullying Via Social Media. *Https://Doi.Org/10.1080/15388220.2014.949377*, *14*(1), 11–29. https://doi.org/10.1080/15388220.2014.949377

Wikipedia.org. (2022a, July 25). *Omeka - Wikipedia*. Wikipedia. https://en.wikipedia.org/wiki/Omeka

Wikipedia.org. (2022b, November 16). *Similarweb - Wikipedia*. Wikipedia.Org. https://en.wikipedia.org/wiki/Similarweb

Wikipedia.org. (2023a, January 3). *Yahoo! - Wikipedia*. Wikipedia.Org. https://en.wikipedia.org/wiki/Yahoo!

Wikipedia.org. (2023b, January 6). *Google - Wikipedia*. Wikipedia.Org. https://en.wikipedia.org/wiki/Google

Wu, S.-H., Chou, M.-J., Tseng, C.-H., Lee, Y.-J., & Chen, K.-T. (n.d.). *Detecting In-Situ Identity Fraud on Social Network Services: A Case Study on Facebook*. https://doi.org/10.1145/2567948.2577308

Yarmohammadian, M., Abzari, M., & Iravani, H. (2012). Information and communications technology, culture, and medical universities; organizational culture and netiquette

among academic staff. *Journal of Education and Health Promotion*, *1*(1), 6. https://doi.org/10.4103/2277-9531.94414

Zou'bi, R. al. (2021). The impact of media and information literacy on acquiring the critical thinking skill by the educational faculty's students. *Thinking Skills and Creativity*, *39*, 100782. https://doi.org/10.1016/J.TSC.2020.100782

# Πρόσθετη Βιβλιογραφία


Ahn, D., Jeon, S., & Yoo, B. (2012). Your age is showing: An analysis of identity fraud in online game classification systems. Paper presented at the *ACM International Conference Proceeding Series,* 239-246.

Back, B. -., & Ha, I. -. (2017). A platform for supporting automatic data storing and visualization of public and private big data. Paper presented at the *ACM International Conference Proceeding Series, , Part F132530* 12-17.

Cirac-Claveras, G. (2019). Weather satellites: Public, private and data sharing. the case of radio occultation data. *Space Policy, 47*, 94-106.

Kalender, K. M. (2018). Cyberbullying awareness in secondary and high-schools. *World Journal on Educational Technology: Current Issues, 10*(4), 191-202. doi:10.18844/wjet.v10i4.4082

Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism?. *Surveillance & Society*, *15*(5), 626-639.

Linek, S. B., & Ostermaier-Grabow, A. (2018). Netiquette between students and their lecturers on Facebook: Injunctive and descriptive social norms. *Social Media+ Society*, *4*(3), 2056305118789629.

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, 93010-93022.

Marcoccia, M. (2012). The internet, intercultural communication and cultural variation. *Language and Intercultural Communication*, *12*(4), 353-368.

Ng, I. C. (2018). Can you own your personal data? the hat (hub-of-all-things) data ownership model.

Nuakoh, E. B., & Anwar, M. (2018). Detecting impersonation in social network sites (SNS) using artificial immune systems (AIS). Paper presented at the *Conference Proceedings - IEEE SOUTHEASTCON, , 2018-April*

Olweus, D. (2012). Cyberbullying: An overrated phenomenon?. *European journal of developmental psychology*, *9*(5), 520-538.

Olweus, D., & Limber, S. P. (2018). Some problems with cyberbullying research. Current opinion in psychology, 19, 139-143.

Richardson, B., & Waldron, D. (2019). Fighting back against synthetic identity fraud. *McKinsey on Risk*, *7*, 1-6.

Volkov, D. V., Zubov, M. V., & Masehnovich, A. G. (2019). Microsegmentation problems associated with multiple distribution of qualitative characteristics in the analysis of the user profile. *International Journal of Advanced Trends in Computer Science and Engineering, 8*(4), 1348-1352.

# Παράρτημα Ι – Διαδικτυακή πλατφόρμα omeka.net

Η διαδικτυακή πλατφόρμα Omeka.net αποτελεί αναπόσπαστο μέρος της παρούσας διπλωματικής εργασίας. "Το Omeka (γνωστό και ως Omeka Classic) είναι ένα δωρεάν σύστημα, ανοιχτού κώδικα, το οποίο διαχειρίζεται περιεχόμενο για διαδικτυακές ψηφιακές συλλογές" (Wikipedia, 2022). Ως διαδικτυακή εφαρμογή, επιτρέπει στους χρήστες να δημοσιεύουν και να εκθέτουν αντικείμενα πολιτιστικής κληρονομιάς. Είναι μία εξελιγμένη λύση λογισμικού αποθετηρίου όπως το DSpace και το Fedora, "το Omeka εστιάζει στην οθόνη και χρησιμοποιεί ένα μη εγκεκριμένο πρότυπο μεταδεδομένων Dublin Core" Wikipedia, (2022).

Για τις ανάγκες τις διπλωματικής εργασίας έχουν δημιουργηθεί τρεις διαδικτυακές συλλογές στο πρόγραμμα omeka.net. Η πρώτη περιλαμβάνει τις τρεις (3) πρώτες σε επισκεψιμότητα και ελεύθερες διαδικτυακές πλατφόρμες, η δεύτερη συλλογή περιλαμβάνει τις πέντε (5) κορυφαίες ελεύθερες μηχανές αναζήτησης και η τρίτη συλλογή περιλαμβάνει τα τέσσερα (4) εκπαιδευτικά σενάρια που σχεδιάστηκαν στο πλαίσιο της παρούσας διπλωματικής εργασίας.

Η κάθε εγγραφή για τις δύο πρώτες συλλογές αποτελείται από τον τίτλο, τις κατηγορίες και υπο- κατηγορίες που ταξινομείται η κάθε εφαρμογή/ μηχανή αναζήτησης από την ιστοσελίδα SimilarWeb, τον δημιουργό της, την χρονολογία δημοσίευσης και τις αναφορές από όπου συλλέχθηκαν οι πληροφορίες που αναφέρονται. Επίσης γίνεται μία συνοπτική, αλλά αναλυτική περιγραφή των αντικειμένων, η οποία περιλαμβάνει σύντομη περιγραφή της πλατφόρμας, την αποστολή και τους στόχους που έχει η καθεμία και μια σύντομη ιστορική αναδρομή. Όλα τα παραπάνω παρέχονται στην ελληνική και την αγγλική γλώσσα.

Παράλληλα, δίνεται η επίσημη σελίδα του κάθε αντικειμένου, και μία εικόνα με το λογότυπο. Τέλος, στην τελευταία καρτέλα συμπληρώνονται ετικέτες (tags) οι κατηγορίες και οι υπο – κατηγορίες, έτσι ώστε ο χρήστης να μπορεί να κάνει αναζήτηση ανά κατηγορία και όχι ανά συλλογή.

Αντίστοιχα η τρίτη συλλογή περιγράφει συνοπτικά το εκπαιδευτικό σενάριο, το οποίο ο ενδιαφερόμενος μπορεί να ανακτήσει σε μορφή PDF.

Ο αναγνώστης μπορεί να έχει πρόσβαση σε αυτή μέσω του συνδέσμου https://kotsakiana.omeka.net/

# Παράρτημα ΙΙ – Αρχείο MS Excel βιβλιογραφικής επισκόπησης

Το αρχείο MS Excel της βιβλιογραφικής επισκόπησης με τίτλο mthesis_kotsaki_alis.xls αποτελεί αναπόσπαστο μέρος της παρούσας διπλωματικής εργασίας.