



Πανεπιστήμιο Δυτικής Μακεδονίας
Τμήματος Επικοινωνίας και Ψηφιακών Μέσων
Σχολή Ανθρωπιστικών Επιστημών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κοινωνικά Δίκτυα και Προστασία Προσωπικών Δεδομένων

Μπίνια Χριστίνα ΑΜ:5454

Επιβλέπων καθηγητής: Μπάτος Παναγιώτης

Καστοριά, Νοέμβριος 2023

Περίληψη

Η παρούσα πτυχιακή εργασία έχει θέμα την προστασία των προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης και ειδικότερα πόσο καλά γνωρίζει ο μέσος χρήστης για την προστασία των δεδομένων του. Το διαδίκτυο έχει αναπτυχθεί και αναπτύσσεται με ραγδαία ταχύτητα και αποτελεί μία από τις πιο σημαντικές εφευρέσεις της ανθρωπότητας καθώς έχει προσφέρει πολλές δυνατότητες. Καθημερινά τα μέσα κοινωνικής δικτύωσης αποκτούν όλο και περισσότερους χρήστες και γίνονται όλο ένα πιο σημαντικά για ένα μεγάλο ποσοστό του πληθυσμού. Οι χρήστες που χρησιμοποιούν συχνά τα κοινωνικά δίκτυα δίνουν προσωπικές πληροφορίες, όπως όνομα, διευθύνσεις, τοποθεσία και φωτογραφίες. Θα πρέπει να γνωρίσουν τους κινδύνους και άλλες απειλές σχετικά με την ασφάλεια και την ιδιωτικότητά τους στα μέσα κοινωνικής δικτύωσης. Ενώ, οι ιστότοποι κοινωνικής δικτύωσης αποτελούν ένα ισχυρό τρόπο επικοινωνίας, τα δικαιώματα και η ασφάλεια των χρηστών έχουν μειωθεί. Η εργασία χωρίζεται σε 5 κεφάλαια συνολικά. Αρχικά, στο πρώτο κεφάλαιο, γίνεται αναφορά σε θεωρητικό επίπεδο όπου παρουσιάζεται μια ιστορική αναδρομή για την εξέλιξη των κοινωνικών μέσων καθώς και περιγράφονται κάποιες βασικές έννοιες σχετικά με το διαδίκτυο όπως τα μέσα κοινωνικής δικτύωσης και τους κινδύνους που απειλούν την ιδιωτικότητα. Ταυτόχρονα, στο δεύτερο κομμάτι, γίνεται αναφορά για το πως μπορεί να γίνει η συλλογή των προσωπικών δεδομένων ενός χρήστη, στη νομοθεσία και σε διάφορα γνωστά σκάνδαλα. Στη συνέχεια, παρουσιάζεται η έρευνα η οποία πραγματοποιήθηκε μέσω ερωτηματολογίου και έγινε περιγραφική ανάλυση. Η έρευνα εστιάζει περισσότερο στην έλλειψη απορρήτου των ανθρώπων στα κοινωνικά μέσα. Σε εκείνο το σημείο θα ασχοληθούμε με το θέμα τη σχέση που έχουν οι χρήστες με τα μέσα κοινωνικής δικτύωσης και αν παραβιάζεται η ιδιωτικότητα τους. Στο τέλος, παρουσιάζονται τα αποτελέσματα καθώς και κάποιες προτάσεις για τη βελτίωση της προστασίας των προσωπικών δεδομένων από τα μέσα κοινωνικής δικτύωσης. Η προστασία των προσωπικών δεδομένων είναι ένα πολύ σοβαρό ζήτημα στα κοινωνικά δίκτυα και οι χρήστες θα πρέπει να είναι προσεκτικοί σχετικά με το απόρρητο και να προσπαθούν να εξασφαλίζουν την ασφάλειά τους στο διαδίκτυο. Ταυτόχρονα, οι χρήστες πρέπει να καταλάβουν πόσο σημαντική είναι η προστασία των προσωπικών δεδομένων.

Λέξεις Κλειδιά: Διαδίκτυο, Προσωπικά δεδομένα, Μέσα κοινωνικής δικτύωσης,
Ιδιωτικότητα, Απόρρητο

Abstract

The subject of this thesis is about the protection of private data in social media and, specifically, how well does the average user know about the protection of their data. The Internet has evolved and is still evolving at a rapid pace and is considered one of the most important inventions of humankind as it offers a lot of potential for various uses. Each day, social media networks keep gaining new users and are becoming more and more important for a huge portion of the population. Users of social media platforms can provide their personal information such as their name, photos, current location or home address. Internet users have to know about the dangers that threaten their security and privacy in social media platforms. While, social media websites are a powerful means of communication, this has led to the reduction of users' rights and security. This thesis is divided into 5 chapters. The first chapter presents, on a theoretical basis, a historical review of the evolution of social media platforms as well as some terms regarding the Internet like social media networks and the dangers that threaten an individual's privacy. The second chapter focuses on the how an individual's private information can be collected or stolen, as well as some examples about laws regarding privacy in various regions and known privacy violation scandals. The third chapter contains the methodology of the survey and the questionnaire that was provided to the participants. The survey focuses more on the lack of users' privacy in social media. Descriptive analysis was performed, in the fourth chapter and the main focus is more on the lack of users' privacy in social media. At that point, the issue that is addressed is the relationship between users and social media and if their privacy is violated. In the end, the results of the survey are presented but also some suggestions for the reinforcement of privacy in social media. The protection of private information is a very pressing issue in social media. Users should be more wary of their privacy and should be attempting to strengthen their security online. At the same time, they must understand how important the protection of their private information and personal data is.

Keywords: Internet, Private information, Personal data, Social media networks, Privacy

Πίνακας περιεχομένων

Περίληψη	1
Abstract	3
Εισαγωγή	7
Κεφάλαιο 1: Θεωρητικό πλαίσιο (Ορισμοί)	8
1.1 Τεχνολογική εξέλιξη	8
1.2 Η ιστορία του διαδικτύου	8
1.3 Διαδίκτυο	10
1.4 World Wide Web	10
1.5 Web 1.0	11
1.6 Web 2.0	12
1.7 Web 3.0	13
1.7.1 Οι διαφορές μεταξύ του Web 1.0 και Web 2.0	14
1.7.2 Οι διαφορές μεταξύ του Web 2.0 και Web 3.0	15
1.8 Τι είναι τα μέσα κοινωνικής δικτύωσης;	15
1.8.1 Τα μέσα κοινωνικής δικτύωσης, κατά τον Mayfield, έχουν τα εξής χαρακτηριστικά	16
1.8.2 Κατηγοριοποιήσεις των μέσων κοινωνικής δικτύωσης	17
1.9 Ιστορική Εξέλιξη Μέσων Κοινωνικής Δικτύωσης	19
1.9.1 Η Πρώτη Ιστοσελίδα: SixDegrees	19
1.9.2 Ιστοσελίδα: FRIENDSTER	20
1.9.3 Ιστοσελίδα: LinkedIn	21
1.9.4 Ιστοσελίδα: MYSPACE	21
1.9.5 Ιστοσελίδα: Facebook	22
1.9.6 Ιστοσελίδα: Reddit	23
1.9.7 Ιστοσελίδα: YouTube	24
1.9.8 Ιστοσελίδα: X (πρώην Twitter)	24
1.9.9 Ιστοσελίδα: Pinterest	25
1.9.10 Ιστοσελίδα: Instagram	26
1.9.11 Ιστοσελίδα: Snapchat	26
1.9.12 Ιστοσελίδα : TikTok	27
1.9.13 Παράλληλες Εμφανίσεις	27
1.10 Λόγοι επιτυχίας της κοινωνικής δικτύωσης	29
1.11 Οι εφαρμογές των μέσων κοινωνικών δικτύων	29

1.12 Τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης των μέσων κοινωνικών δικτύων.....	31
Κεφάλαιο 2: Νομικά θέματα διαδικτύου	35
2.1. Θέματα απορρήτου και ασφάλειας.....	35
2.2. Οι επιπτώσεις των κοινωνικών δικτύων.....	36
2.3. Ιδιωτικότητα	36
2.3.1. Παραδείγματα παραβίασης της ιδιωτικότητας.....	37
2.4. Η έννοια των προσωπικών δεδομένων.....	38
2.5. Malware – Κακόβουλο λογισμικό.....	40
2.6. Phishing Attacks – Επιθέσεις ηλεκτρονικού «ψαρέματος».....	41
2.7. Cross-Site Scripting – XSS	42
2.8. Τι είναι τα Cookies.....	43
2.9. Επεξεργασία δεδομένων προσωπικού χαρακτήρα	44
2.10. Νομοθεσίες και Πολιτικές Προστασίας (Διεθνές και Ευρωπαϊκό Δίκαιο)	44
2.10.1. Ευρωπαϊκή Νομοθεσία.....	44
2.10.2. Ελληνικό πλαίσιο	45
2.10.3. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (2016/679) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (GDPR).....	47
2.10.4. Νομοθεσία στις Ηνωμένες Πολιτείες της Αμερικής	49
2.11. Τι είναι το απόρρητο στο Διαδίκτυο;	50
2.12. Βασικοί κίνδυνοι που απειλούν το απόρρητο.....	51
2.13. Τεχνολογίες ενίσχυσης της ιδιωτικότητας και προστασίας.....	52
2.14. Σκάνδαλα παραβίασης προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης	53
2.14.1. Σκάνδαλο παραβίασης προσωπικών δεδομένων Facebook - Cambridge Analytica	54
2.14.2. Σκάνδαλο παραβίασης προσωπικών δεδομένων Yahoo!.....	55
2.14.3. Σκάνδαλο παραβίασης προσωπικών δεδομένων «iPhone tracking».....	55
2.14.4. Παραβίαση προσωπικών δεδομένων και πρόσβασης στο X (πρώην Twitter)	56
2.14.5. Σκανδάλο παραβίασης προσωπικών δεδομένων Instagram	58
Κεφάλαιο 3: Μεθοδολογία Έρευνας	59
3.1. Ερωτηματολόγιο.....	59
Κεφάλαιο 4: Ανάλυση αποτελεσμάτων/τρόποι αντιμετώπισης και μελλοντικές επεκτάσεις.....	64
Συμπεράσματα και προτάσεις	100
Βιβλιογραφία	103

Πίνακας Εικόνων

Εικόνα 1: Η εξέλιξη του ARPANET. Πηγή: https://internetpasoapaso.com/arpamet-historia/	10
Εικόνα 2: Οι χρησιμότητες του Web 2.0 (Πηγή: https://commons.wikimedia.org/wiki/File:Web_2.0_Map.svg)	13
Εικόνα 3: Το λογότυπο της ιστοσελίδας SixDegrees (Πηγή: http://www.sixdegrees.com/)	19
Εικόνα 4: Η αρχική ιστοσελίδα του Friendster το 2004. (Πηγή: http://www.friendster.com)	20
Εικόνα 5: Το λογότυπο του LinkedIn (Πηγή: https://www.linkedin.com/)	21
Εικόνα 6: Το λογότυπο του MySpace (Πηγή: https://myspace.com/)	21
Εικόνα 7: Το λογότυπο του Facebook (Πηγή: https://www.facebook.com/)	22
Εικόνα 8: Το λογότυπο του Reddit. (Πηγή: https://www.reddit.com/)	23
Εικόνα 9: Το λογότυπο του YouTube. (Πηγή: https://www.youtube.com/)	24
Εικόνα 10: Το λογότυπο του X . (Πηγή: https://twitter.com/)	24
Εικόνα 11: Το λογότυπο του Pinterest. (Πηγή: https://www.pinterest.com/)	25
Εικόνα 12: Το λογότυπο του Instagram. (Πηγή: https://www.instagram.com/)	26
Εικόνα 13: Το λογότυπο του Snapchat. (Πηγή: https://www.snapchat.com/)	26
Εικόνα 14: Το λογότυπο του TikTok. (Πηγή: https://www.tiktok.com/)	27
Εικόνα 15: Χρονοδιάγραμμα με τις εμφανίσεις των διάφορων κοινωνικών μέσων. (Πηγή: https://www.booksaresocial.com/social-media-timeline/)	28
Εικόνα 16: Η ανάρτηση που είχε γίνει από τους hackers μέσω το λογαριασμού του Joe Biden χρησιμοποιώντας διαχειριστικά εργαλεία του X. (Πηγή: https://www.bloomberg.com/news/articles/2020-07-15/elon-musk-bill-gates-appear-to-have-twitter-accounts-hacked)	57

Εισαγωγή

Η ανάπτυξη της τεχνολογίας έφερε ευκολία στην επικοινωνία των χρηστών. Από την δημιουργία του ARPANET στα μέσα του 20^{ου} αιώνα, αναπτύχθηκε το διαδίκτυο, μία από τις πιο διαδεδομένες τεχνολογίες σήμερα. Με την δημιουργία όλο και περισσότερων ιστοτόπων προέκυψαν τα μέσα κοινωνικής δικτύωσης όπως το Facebook, X (πρώην Twitter), Instagram, κ.λπ., τα οποία χρησιμοποιούνται πλέον από έναν μεγάλο αριθμό ατόμων σε όλο τον κόσμο και αποτελούν σημαντική πηγή επικοινωνίας στη σύγχρονη εποχή. Αυτό έχει ως αποτέλεσμα την άμεση επικοινωνία με άλλους ανθρώπους, την ευκολότερη ενημέρωση και γι' αυτό έχουν γίνει πλέον απαραίτητα στην καθημερινότητα των ατόμων καθώς μπορούν να μοιράζονται ιδέες και πληροφορίες με ένα μεγάλο ποσό χρηστών. Ωστόσο, η χρήση του διαδικτύου και ειδικότερα των μέσων κοινωνικής δικτύωσης μπορούν να επηρεάσουν την ιδιωτικότητα και να παραβιάσουν το απόρρητο δηλαδή τα προσωπικά δεδομένα των χρηστών. Η απελευθέρωση δεδομένων στα κοινωνικά δίκτυα μπορεί να έχει ως αποτέλεσμα την διαρροή ευαίσθητων πληροφοριών, ένα γεγονός που επηρεάζει σε μεγάλο βαθμό την ιδιωτική ζωή των χρηστών. Πολλές φορές οι χρήστες μπορούν να εκτεθούν σε κίνδυνο όταν παραβιαστούν τα προσωπικά τους δεδομένα και γίνονται δημόσια. Στο πρώτο κεφάλαιο, γίνεται μια αναφορά για την εξέλιξη του διαδικτύου, τι είναι τα μέσα κοινωνικής δικτύωσης, με συνοπτική περιγραφή της ιστορίας τους, τους λόγους που έγιναν επιτυχημένα και για τα πλεονεκτήματα και τα μειονεκτήματά τους. Στην συνέχεια, στο δεύτερο κεφάλαιο γίνεται επέκταση στο θέμα σχετικά με τους κινδύνους που επιφέρουν τα μέσα κοινωνικής δικτύωσης στο απόρρητο και στα προσωπικά δεδομένων των χρηστών, στο κακόβουλο λογισμικό, στη νομοθεσία σε διάφορες περιοχές, σε σκάνδαλα και διάφορες τεχνολογίες που ενισχύουν την ιδιωτικότητα. Όπως θα παρουσιαστεί τα μέσα κοινωνικής δικτύωσης έχουν πολλά τέτοια παραδείγματα περιστατικών σχετικά με παραβιάσεις του απόρρητου των χρηστών. Στο τρίτο κεφάλαιο, θα παρουσιαστεί η μεθοδολογία της έρευνας καθώς και το ερωτηματολόγιο που απάντησαν οι ερωτηθέντες. Τα αποτελέσματα της έρευνας παρουσιάζονται στο τέταρτο κεφάλαιο. όπου γίνεται η ανάλυσή τους και τοποθετείται το συμπέρασμα που παρατηρήθηκε από αυτά. Καθώς τα μέσα κοινωνικής δικτύωσης συνεχίζουν να εξελίσσονται είναι σίγουρο ότι η σύγχρονη κοινωνία αλλάζει το οποίο σημαίνει ότι πρέπει να υπάρξουν μέτρα υπέρ της προστασίας των δεδομένων.

Κεφάλαιο 1: Θεωρητικό πλαίσιο (Ορισμοί)

Το πρώτο κεφάλαιο αποτελείται από το θεωρητικό πλαίσιο της πτυχιακής εργασίας, συγκεκριμένα σε αυτό το κομμάτι αναφέρεται η ιστορία του διαδικτύου, τι είναι παγκόσμιος ιστός, η δημιουργία των πρώτων κοινωνικών δικτύων και την εξέλιξή τους όπως το Facebook, Instagram. και η κατηγοριοποίηση των κοινωνικών δικτύων.

1.1 Τεχνολογική εξέλιξη

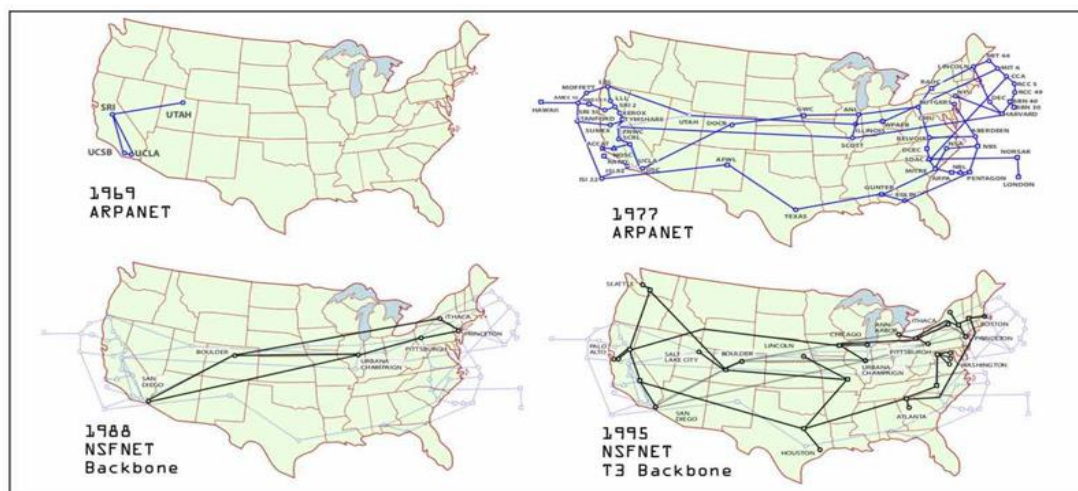
Η τεχνολογική εξέλιξη έδωσε απίστευτη προοπτική για την εξέλιξη του ανθρώπου και προσφέρει πολλά σε διάφορους τομείς όπως την επικοινωνία, την εκπαίδευση, την ενημέρωση, την ψυχαγωγία κ.λπ. Με αυτό τον τρόπο, έχει εισχωρήσει βαθιά στην καθημερινότητα του ανθρώπου και έχει αλλάξει σημαντικά τον τρόπο ζωής. Έτσι, καθώς η τεχνολογία εξελίσσεται με γρήγορους ρυθμούς επηρεάζονται και όλοι οι παραπάνω τομείς. Έχει καταφέρει να βελτιώσει πολλά πράγματα όπως την επικοινωνία και την γρήγορη πρόσβαση στην πληροφορία. Όμως, πέρα από τα θετικά η τεχνολογία έχει πολλά προβλήματα όπως την παραβίαση της **ιδιωτικότητας** και των προσωπικών δεδομένων διότι οι προσωπικές πληροφορίες μπορούν να αποθηκευτούν και να μοιραστούν με άλλους κακόβουλους τρίτους. Παράλληλα, μπορεί να έχει σοβαρές επιπτώσεις στην υγεία του χρήστη, να δημιουργήσει εθισμό και να οδηγήσει στην απομάκρυνση του χρήστη από άλλους ανθρώπους. Τέλος, η τεχνολογία μπορεί να έχει προσφέρει πολλές ευκολίες για τον άνθρωπο αλλά είναι σημαντικό να υπάρχει συνείδηση των κινδύνων που μπορεί να γίνει με την κατάλληλη ενημέρωση και εκπαίδευση.

1.2 Η ιστορία του διαδικτύου

Το διαδίκτυο ποτέ δεν σχεδιάστηκε να έχει την σημερινή μορφή. Τα πρώτα βήματα έγιναν σταδιακά κατά την διάρκεια του Ψυχρού Πόλεμο όταν η αποστολή του δορυφόρου Sputnik από την Σοβιετική Ένωση έκανε το Υπουργείο των Ηνωμένων Πολιτειών της Αμερικής να αναζητήσει μεθόδους με τους οποίους τα δεδομένα θα μπορούσαν να διασκορπιστούν ακόμα και μετά από ατομική επίθεση, τότε οι υπολογιστές ήταν τεράστιοι και δεν έκαναν τίποτα παραπάνω από το να λύνουν

δύσκολα προβλήματα για μια ομάδα φυσικών με αρχηγό τον Richard Feynman. Οι πρώτες προσπάθειες έγιναν από τις Ηνωμένες Πολιτείες της Αμερικής την δεκαετία του '50 και '60 που ανέπτυξαν το **Advanced Research Projects Agency Network** (ARPANET) που δημιουργήθηκε από το γραφείο Τεχνικών Επεξεργασίας Πληροφοριών (IPTO) στον Οργανισμό Προηγμένων Ερευνητικών Έργων (ARPA), μέρος του Υπουργείου Άμυνας των ΗΠΑ ως μέσο επικοινωνίας που θα συνέδεε απομακρυσμένους υπολογιστές το οποίο για εμφανίστηκε για πρώτη φορά το 1966 (Εικόνα 1). Το ARPANET κυκλοφόρησε τον Οκτώβριο του 1969 και χρησιμοποιήθηκε από την κυβέρνηση και ερευνητικά ιδρύματα από το Υπουργείο Άμυνας Ηνωμένων Πολιτειών της Αμερικής. Ο βασικός του στόχος ήταν να μπορεί να συνδέει το Υπουργείο Άμυνας με τους στρατιωτικούς οργανισμούς. Η μετάδοση του πρώτου μηνύματος έγινε όταν πληκτρολογήθηκε η εντολή "login" αλλά ο SDS 940 παρουσίασε σφάλμα αφού πληκτρολογήθηκαν οι δύο πρώτοι χαρακτήρες ("LO"). Η σύνδεση του γινόταν με τέτοιο τρόπο που αν ένας υπολογιστής έχανε την σύνδεση, συνέχιζαν οι υπόλοιποι να λειτουργούν χωρίς να χαθεί η επικοινωνία μεταξύ τους. Ενώ το ARPANET ήταν κλειστό για το ευρύ κοινό, το 1972 συνέχισε να εξαπλώνεται και ήταν συνδεδεμένος με 23 hosts. Το 1974 σταμάτησε να είναι ερευνητικό πρόγραμμα του υπουργείου άμυνας και άρχισε να χρησιμοποιείται σε πανεπιστήμια. Στην δεκαετία του 1980, άρχισε να μεγαλώνει και να επεκτείνεται πέρα από την κυβέρνηση. Το 1981, ο Lawrence Landweber στο Πανεπιστήμιο του Wisconsin κατάφερε να ενώσει την επικοινωνία των πανεπιστημίων χωρίς να είναι συνδεδεμένα με το ARPANET αλλά δημιούργησαν ένα άλλο δίκτυο που ήταν βασισμένο σε πρωτόκολλα TCP/IP που είχε το όνομα NSFNET. Παρ' όλα αυτά εξακολουθούσε να είναι δύσκολο για τους ανθρώπους να συνδεθούν με τον προσωπικό τους υπολογιστή. Το NSFNET που δημιουργήθηκε από το National Science Foundation χρησιμοποιώντας το πρωτόκολλο TCP/IP σύνδεε πέντε κέντρα υπερ-υπολογιστών. Η ραγδαία ανάπτυξη έγινε την δεκαετία του 1990 με την δημιουργία του Παγκόσμιου Ιστού, που βοήθησε σημαντικά στην ανταλλαγή πληροφοριών, καθώς δημιουργήθηκε το ανοικτό δίκτυο και τα πρώτα προγράμματα περιήγησης όπως το Mosaic και το Netscape Navigator και έκανε το διαδίκτυο προσβάσιμο. Η μεγαλύτερη του εξάπλωση έγινε στο μέσο με τέλος της δεκαετίας του 2000 στο οποίο συνέβαλαν η άνοδος των μέσων κοινωνικής δικτύωσης, η αυξανόμενη χρήση των «έξυπνων» κινητών τηλεφώνων (smartphones) και υπολογιστών με αποτέλεσμα να μετατραπεί το διαδίκτυο σε ένα παγκόσμιο δίκτυο. Το

διαδίκτυο είναι ένα εργαλείο για την σημερινή εποχή και αποτελεί μια ανεξάντλητη πηγή πληροφοριών και γνώσεων.



Εικόνα 1: Η εξέλιξη του ARPANET. Πηγή: <https://internetpasoapaso.com/arpamet-historia/>

1.3 Διαδίκτυο

Το διαδίκτυο (internet) είναι ένα παγκόσμιο δίκτυο που συνδέεται με εκατοντάδες πάροχους διαδικτυακών υπηρεσιών. Βασίζεται σε πρωτόκολλα Transmission Control Protocol (TCP) Internet Protocol (IP). Ορίζεται ως «το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών» (Βικιπαίδεια) και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του. Η λέξη διαδίκτυο προκύπτει από την ένωση των λέξεων **δια**σύνδεση (**interconnection**) και δίκτυο (**network**). Το διαδίκτυο χρησιμοποιείται για ψυχαγωγία, ενημέρωση, εκπαίδευση και άλλα. Οι χρήστες μπορούν να μοιράζονται πληροφορίες να επικοινωνούν, να εκφράζουν ελεύθερα την γνώμη τους σχετικά με διάφορα πράγματα και μπορούν επίσης να παίζουν παιχνίδια. Ο καθένας έχει πρόσβαση ανεξαρτήτως από την κοινωνική και γεωγραφική του περιοχή.

1.4 World Wide Web

Ο Παγκόσμιος Ιστός (WWW), ο οποίος δημιουργήθηκε από τον βρετανό επιστήμονα **Tim Berners-Lee** όταν εργαζόταν στο ερευνητικό ίδρυμα **CERN** (Ευρωπαϊκός Οργανισμός Πυρηνικών Ερευνών) στην Ελβετία το 1989, είναι μια τεράστια συλλογή

διακομιστών (server) ιστού που εκτελούν το πρωτόκολλο Hypertext Transfer (http) και μπορούν να παρέχουν έγγραφα με ενσωματωμένα μέσα, προγράμματα και συνδέσμους προς οποιονδήποτε άλλο διακομιστή που επιτρέπουν τον χρήστη να περιηγηθούν σε διαφορές ιστοσελίδες και να συγκεντρώσουν πληροφορίες. Ο Tim Berners-Lee είχε στόχο να μπορούν όλοι οι υπολογιστές του CERN να έχουν πρόσβαση στο σύστημα και να μπορούν να αποθηκεύουν τεράστιο όγκο εγγράφων. Αυτό κατέληξε να είναι μία από τις σπουδαιότερες ανακαλύψεις που έχουν γίνει και σταδιακά εξελίχθηκε στο διαδίκτυο. Την πρώτη δεκαετία του 1989-1999 η δημοτικότητα του παγκόσμιου Ιστού αυξήθηκε σε εκρηκτικό βαθμό. Το URL είναι η διεύθυνση που δηλώνει που βρίσκονται αρχεία του ιστού (χρησιμοποιείται από το πρωτόκολλο HTTP). Πρόκειται για μία τεράστια πηγή πληροφορίας που βρίσκονται αποθηκευμένες σε υπολογιστές και προβάλλονται μέσω ιστοσελίδων. Ο πρώτος πλοηγός ήταν το Mosaic το 1993 και μετά από ένα χρόνο το 1994 εμφανίστηκε ο Netscape Navigator αλλά σύντομα έχασε τους περισσότερους χρήστες του από το Internet Explorer από την Microsoft. Χάρη στην δημιουργία του παγκόσμιου Ιστού, η κοινωνία έχει επηρεαστεί σε μεγάλο βαθμό, η χρήση του είναι εύκολη και ο κάθε χρήστης μπορεί να το χρησιμοποιήσει. Η ανάπτυξη των κοινωνικών μέσων και διάφορων πλατφόρμων οδήγησε στους χρήστες να μπορούν να επικοινωνήσουν με άλλους χρήστες και να εκφράσουν τις απόψεις τους.

1.5 Web 1.0

Web 1.0 αποτελεί την πρώτη εμφάνιση του διαδικτύου από το 1991 έως το 2004 και αποτελεί η πρώτη μορφή που είχε το διαδίκτυο, δηλαδή ο χρήστης αναζητά και διαβάζει την πληροφορία. Ο δημιουργός του ήταν ο Tim Berners-Lee, ένας βρετανός επιστήμονας, ο οποίος ήταν μηχανικός στο λογισμικό CERN και παρουσίασε το Web Server και Web Browser το 1989. Χρησιμοποίησε ένα είδος πρωτόκολλου για την κοινή χρήση εγγράφων και πληροφοριών σε όλο το τοπικό δίκτυο του CERN. Έτσι δημιουργήθηκε η γλώσσα σήμανσης υπερκειμένου (HTML) αλλά και το «*hypertext*». Πρόκειται για την πρώτη γενιά του διαδικτύου καθώς το περιεχόμενο ήταν στατικό και οι χρήστες δεν μπορούσαν να αλληλοεπιδράσουν. Αρχικά το Web 1.0 είχε σκοπό μόνο την παράδοση περιεχομένου, εφόσον εκείνο το διάστημα το διαδίκτυο ήταν περισσότερο πληροφορίες, στοιχεία επικοινωνίας αλλά και περιγραφές προϊόντων και υπηρεσιών. Χάρη στο Web 1.0 ξεκίνησαν να δημιουργούνται οι πρώτες εφαρμογές του

διαδικτύου όπως το ηλεκτρονικό ταχυδρομείο, σε ψηφιακή μορφή βιβλία, μουσική και ειδήσεις. Επιπλέον, εκείνη την εποχή οι ιστοσελίδες ήταν απλές και στατικές καθώς είχαν ελάχιστες επιλογές και οι χρήστες μπορούσαν μόνο να διαβάσουν το κείμενο ή να κάνουν λήψη αρχείων, δηλαδή ήταν παθητικοί χρήστες και δεν είχαν καμία δυνατότητα αλληλεπίδρασης. Ακόμα, οι ιστοσελίδες ήταν πολύ περιορισμένες λόγω της έλλειψης γνώσης της γλώσσας HTML. Επιπλέον, παρουσίαζε έλλειψη διαδραστικότητας και άμεσης επικοινωνίας μεταξύ των χρηστών.

1.6 Web 2.0

Το Web 2.0 (2004-2010) ανακαλύφθηκε από τον Tim ο'Reilly (2004) στην διάρκεια ενός συνεδρίου μεταξύ επικεφαλών επιχειρήσεων και τεχνολογίας. Πρόκειται για την δεύτερη γενιά υπηρεσιών που βασίζεται στο διαδίκτυο. Το Web 2.0 βοηθάει να συνδεθούμε μεταξύ μας, καθώς το περισσότερο περιεχόμενό του δημιουργείται από τους χρήστες. Ο Tim ο'Reilly χαρακτηρίζει το Web 2.0 ως εξής *«Το Web 2.0 είναι η επανάσταση στην επιχειρηματική βιομηχανία του υπολογιστή που προκλήθηκε από τη μετάβαση στο διαδίκτυο ως πλατφόρμα και μια προσπάθεια να κατανοήσουμε κανόνες για επιτυχία σε αυτή τη νέα πλατφόρμα. Κυριότερος ανάμεσα σε αυτούς τους κανόνες είναι ο εξής: Κατασκευάστε εφαρμογές που εκμεταλλεύονται το διαδίκτυο και την ανάπτυξή του ώστε να βελτιώνονται και περισσότεροι άνθρωποι να τις χρησιμοποιούν.»* Το Web 2.0 ορίζεται ως η νέα γενιά του Παγκόσμιου Ιστού που σχετίζεται περισσότερο στο διαδίκτυο. Ο Tim O'Reilly δίνει τον ορισμό ότι το Web 2.0 είναι εξέλιξη του διαδικτύου ως πλατφόρμα η οποία επιτρέπει τη σύνδεση συσκευών και εφαρμογών όλων των τύπων. Γενικά, το Web 2.0 αναφέρεται στις εφαρμογές, οι οποίες εμφανίστηκαν κατά την δημιουργία των κοινωνικών μέσων, και έφεραν σημαντικές αλλαγές αλλάζοντας τον τρόπο χρήσης του διαδικτύου (Εικόνα 2). Στη νέα εποχή, υπάρχει υψηλότερο επίπεδο ανταλλαγής πληροφοριών και διασύνδεσης μεταξύ των συμμετεχόντων. Αυτή η νέα έκδοση επιτρέπει στους χρήστες να συμμετέχουν ενεργά στην εμπειρία αντί να ενεργούν απλώς ως παθητικοί θεατές που λαμβάνουν πληροφορίες. Το Web 2.0 έδωσε την δυνατότητα στους χρήστες να κάνουν διάφορες εργασίες, όπως την επεξεργασία φωτογραφίας, δημιουργία εγγράφων (όπως το Google Docs) κλπ. Το Web 2.0 είναι *«μια κοινωνική και όχι τεχνολογική επανάσταση»* καθώς έφερε την αλλαγή και δημιουργήθηκαν διάφορα blogs και forum τα οποία βοήθησαν

στην ανταλλαγή πληροφοριών και επικοινωνίας. Η δημιουργία κοινωνικών μέσων όπως το X (πρώην Twitter) και το Facebook έχει δώσει στους χρήστες την δυνατότητα να επικοινωνούν με άλλους χρήστες, να δημιουργούν προφίλ, να κοινοποιούν περιεχόμενο, να ανταλλάζουν μεταξύ τους μηνύματα, καθώς επίσης έχουν την δυνατότητα να κοινοποιούν διάφορο περιεχόμενο όπως φωτογραφίες, βίντεο και μουσική σε διάφορα μέσα κοινωνικής δικτύωσης. Το Web 2.0 είναι μια από τις σημαντικότερες ανακαλύψεις της σύγχρονης ζωής που έχει επηρεάσει την επικοινωνία και τον οικονομικό τομέα.

1.7 Web 3.0

Το Web 3.0 (2010 – σήμερα) είναι πιο πρόσφατη εξέλιξη του διαδικτύου που μπορεί επίσης να ονομαστεί Web Τρίτης Γενιάς. Επειδή αποτελεί ο τρίτος μετασχηματισμός του διαδικτύου, ο στόχος του ήταν να δημιουργήσει γρήγορες μηχανές αναζήτησης, το οποίο έγινε με τη χρήση της γλώσσας XML σε αντίθεση με το WEB 2.0 που χρησιμοποιούσε XHTML. «Τίποτα δεν είναι σταθερό σε αυτόν τον κόσμο, ούτε ο ιστός.» Ο Tim Berners Lee το χαρακτηρίζει ως «*Semantic Web*». Ο ιστός εξελίσσεται από την αρχή του δηλαδή καθώς το Web 2.0 εξελίχθηκε από το Web 1.0, το Web 3.0 θα



Εικόνα 2: Οι χρησιμότητες του Web 2.0 (Πηγή: https://commons.wikimedia.org/wiki/File:Web_2.0_Map.svg)

αποτελέσει έναν τρόπο που θα φέρει αλλαγές στον τρόπο δημιουργίας ιστοσελίδων καθώς και στην αλληλεπίδραση των ανθρώπων με τους ιστότοπους. «*To Web 3.0* επινοήθηκε για πρώτη φορά από τον John Markoff από την *New York Times* και πρότεινε το *Web 3.0* ως την τρίτη γενιά του *Web* το 2006». Ο βασικός του στόχος είναι να ξεπεράσει

τον παραδοσιακό ιστό χρησιμοποιώντας τεχνολογίες, όπως την τεχνητή νοημοσύνη. Το Web 3.0 χρησιμοποιεί την Blockchain κι άλλες παρόμοιες τεχνολογίες λογισμικού

με τις οποίες δίνεται η δυνατότητα στους χρήστες να αποκτήσουν περισσότερο συμμετοχή στο διαδίκτυο. Το Blockchain είναι ένα τύπος αποκεντρωμένης βάσης δεδομένων στην οποία οι πληροφορίες αποθηκεύονται σε πολλούς υπολογιστές αντί για έναν ή για λίγους κεντρικούς δοκιμαστές. Για αυτό το λόγο οι πληροφορίες σε αυτή τη βάση δεδομένων δεν μπορούν να διαγραφούν ή να κρυφτούν. Η τεχνολογία Blockchain επιτρέπει μεγαλύτερη προστασία της ιδιωτικής ζωής αλλά μπορεί παράλληλα να δώσει όσο το δυνατόν περισσότερη διαφάνεια επειδή πολλά Blockchain, ειδικά εκείνα με ανοιχτό κώδικα, μπορούν να επιθεωρούν διαδικτυακές συναλλαγές και άλλες δραστηριότητες από τον καθένα που έχει σύνδεση στο διαδίκτυο. Όλα αυτά είναι επιθυμητά στο Web 3.0 καθώς ενισχύεται το διαδίκτυο. Στοχεύει περισσότερο στην ενίσχυση των ικανοτήτων των υπολογιστών να μπορούν να κατανοούν και να ερμηνεύουν το περιεχόμενο δημιουργώντας αλληλεπιδράσεις μεταξύ των χρηστών και του ιστού. Χρησιμοποιεί την γλώσσα XML σε αντίθεση με το Web 2.0 που γίνεται χρήση της HTML. Σε αυτή την περίπτωση οι χρήστες έχουν τον έλεγχο το δικό τους δεδομένων. Το Web 3.0 έχει προσφέρει καλύτερες λειτουργίες αναζήτησης στους χρήστες. Έχει ενισχυθεί η χρήση της τεχνητής νοημοσύνης που μπορεί να δώσει την δυνατότητα στον ιστό να παρέχει αυτές τις δυνατότητες.

1.7.1 Οι διαφορές μεταξύ του Web 1.0 και Web 2.0

Στο Web 1.0, η επικοινωνία είναι μονόδρομη. Οι χρήστες συνήθως λαμβάνουν την πληροφορία από σελίδες που είναι στατικές. Το Web 1.0 είναι για ιστοσελίδες ενώ το Web 2.0 για blogs. Επίσης, το Web 1.0 είναι για ανάγνωση, ενώ το Web 2.0 είναι για παραγωγή πληροφορίας. Στο Web 1.0, οι χρήστες διαβάζουν ό,τι άλλοι γράφουν και δεν μπορούν να σχολιάσουν ή να τροποποιήσουν το περιεχόμενο. Επίσης, στο Web 1.0, οι ιστοσελίδες δεν έχουν πολλές δυνατότητες και η επικοινωνία είναι περιορισμένη. Το Web 2.0 δίνει έμφαση στο περιεχόμενο που δημιουργείται από τους χρήστες που είναι γνωστό ως κοινωνική δικτύωση. Επιπλέον, στο Web 1.0 οι χρήστες δεν μπορούσαν να συνεισφέρουν περιεχόμενο. Το Web 1.0 είναι λιγότερο δομημένο σε σχέση με το Web 2.0 το οποίο έχει καταιγισμό ιδεών. Το Web 2.0 άλλαξε το τρόπο μετάδοσης των ειδήσεων καθώς παλαιότερα οι χρήστες έπρεπε να διαβάζουν ειδήσεις από ορισμένους ιστότοπους στα οποία δεν μπορούσαν να παρέμβουν και να εκφράσουν τις απόψεις τους ή την εμπειρία τους. Η εμπειρία του χρήστη είναι περιορισμένη στο

περιεχόμενο που του παρέχεται στο Web 1.0. Το Web 2.0 είναι πιο εύκολο ως προς τον τρόπο κατασκευής ιστοσελίδων που επιτρέπουν στον κάθε χρήστη να ασχοληθεί ως προς το περιεχόμενο της ιστοσελίδας, καθώς κύριο χαρακτηριστικό του είναι τα ιστολόγια (blogs).

1.7.2 Οι διαφορές μεταξύ του Web 2.0 και Web 3.0

Ανάμεσα στο Web 2.0 και το Web 3.0 υπάρχουν σημαντικές διαφορές αφού πρόκειται για δύο διαφορετικές γενιές. Το Web 2.0, χρησιμοποιείται για να δημιουργία περιεχομένου μέσω ιστολογιών και ιστότοπων, καθώς βοηθάει στην ανταλλαγή πληροφοριών. Όλοι οι ιστότοποι κοινής χρήσης βίντεο, κοινωνικής δικτύωσης και τα ιστολόγια είναι παραδείγματα του Web 2.0.

Το Web 3.0 αφορά τον σημασιολογικό ιστό, τις δυναμικές εφαρμογές, την έξυπνη αναζήτηση, την εξατομίκευση, τη συμπεριφορική διαφήμιση, τις διαδραστικές υπηρεσίες και την αλληλεπίδραση μηχανής με μηχανή. Επιπλέον, είναι η τρίτη γενιά του ιστού δηλαδή εστιάζει στην καλύτερη επικοινωνία και κατανόηση μεταξύ των χρηστών και των μηχανών. Το Web 3.0 καθιστά ενεργά τον χρήστη στο διαδίκτυο. Οι χρήστες έχουν επίσης πρόσβαση σε εξελιγμένη τεχνολογία όπως την τεχνητή νοημοσύνη. Αυτές είναι κάποιες από τις διαφορές μεταξύ του Web 2.0 και του Web 3.0.

1.8 Τι είναι τα μέσα κοινωνικής δικτύωσης;

Ο όρος κοινωνικά μέσα δικτύωσης αναφέρεται σε μια τεχνολογία που είναι διαδραστική, βασίζεται σε υπολογιστή και επιτρέπει στους χρήστες να μοιράζονται ιδέες, πληροφορίες, βίντεο, φωτογραφίες και άλλα πράγματα. Όπως αναφέρει ο Αριστοτέλης ο άνθρωπος είναι ένα κοινωνικό ζώο που έχει ανάγκη τους συνανθρώπους του. Σύμφωνα με διδασκαλίες του Αριστοτέλη οι κοινωνικές αυτές οντότητες δημιουργήθηκαν επειδή ο άνθρωπος είναι προορισμένος από τη φύση του να μην μπορεί να υπάρξει μόνος του. Οι πρώτες κοινωνικές δικτυακές υπηρεσίες ξεκίνησαν αρκετά νωρίς, καθώς ο βασικός του στόχος ήταν στο να μπορεί ο χρήστης να συνδέεται ηλεκτρονικά σε μεμονωμένους υπολογιστές έτσι ώστε να επιτευχθεί κοινωνική αλληλεπίδραση και δικτύωση. Στην αρχή της δεκαετίας του 1970 εμφανίστηκε το

ηλεκτρονικό ταχυδρομείο (e-mail). Το USENET ήταν ένα σύστημα που είχε στόχο να υπάρχει επικοινωνία μέσω e-mail για να συνδέονται το πανεπιστήμιο της Βόρειας Καρολίνας και το πανεπιστήμιο του Duke. Τα μέσα κοινωνικής δικτύωσης είναι μια μορφή συνομιλίας που βασίζεται στο διαδίκτυο. Από το 1985 έκαναν τα πρώτα τους δειλά βήματα τα κοινωνικά δίκτυα και εμφανίστηκαν τα πρώτα online chats, όπως το «*The WELL*» (1985). Την δεκαετία του 1990 έκαναν την εμφάνιση τους οι πρώτες σελίδες κοινωνικής δικτύωσης, όπως το «*theglobe.com*» (1994), «*Geocities*» (1994), το «*Tripod*» (1995), το «*classmates*» (1995), το οποίο είχε στόχο την επικοινωνία μεταξύ μαθητών, και το «*SixDegrees.com*» (1997) που θεωρείται ο πρώτος ιστότοπος κοινωνικού δικτύου. Αυτά επιτρέπουν στους χρήστες να δημιουργούν, να επικοινωνούν μεταξύ τους αλλά και να κοινοποιούν περιεχόμενο. Το 2003, εμφανίστηκε το «*Myspace*», το «*LinkedIn*» και το «*Hi5*». Ένα χρόνο αργότερα, το 2004, εμφανίστηκε και το «*Facebook*» που είναι ένα από τα μεγαλύτερα μέσα κοινωνικής δικτύωσης σήμερα. Σήμερα, τα πιο γνωστά κοινωνικά δίκτυα είναι το Facebook, το Instagram, το YouTube, το TikTok, το LinkedIn, το X (πρώην Twitter) και πολλά άλλα. Κάθε μέσο περιλαμβάνει διαφορετικές δυνατότητες και έχουν φέρει αλλαγές στην καθημερινότητα του ανθρώπου ως προς την επικοινωνία, την αναζήτηση της πληροφορίας, την ψυχαγωγία αλλά και την εργασία. Ωστόσο, υπάρχουν και πολλοί κίνδυνοι με την χρήση των κοινωνικών μέσων, όπως την παραβίαση των προσωπικών δεδομένων, για τα οποία έχουν θεσπιστεί νόμοι προστασίας, καθώς και για την ποιότητα ελέγχου του περιεχομένου σε όλα τα μέσα κοινωνικής δικτύωσης. Το κάθε άτομο είναι υπεύθυνο ως προς το περιεχόμενο που αποφασίζει να δημοσιεύσει στα μέσα κοινωνικής δικτύωσης με την προστασία της πολιτικής δεδομένων και των όρων χρήσης της πλατφόρμας κοινωνικής δικτύωσης. Με την γρήγορη εξάπλωση του διαδικτύου, τα μέσα κοινωνικής δικτύωσης μπορούν εύκολα να συλλέγουν προσωπικά δεδομένα και αποτελεί ευθύνη του χρήστη τι θα αποφασίσει να δημοσιεύσει.

1.8.1 Τα μέσα κοινωνικής δικτύωσης, κατά τον Mayfield, έχουν τα εξής χαρακτηριστικά

1. **Συμμετοχή (Participation):** Τα μέσα κοινωνικής δικτύωσης ενθαρρύνουν την συνεισφορά και τα σχόλια από τους ενδιαφερομένους. Η συμμετοχή των χρηστών αποτελεί ένα πολύ σημαντικό παράγοντα μεταξύ των μέσων ενημέρωσης και του

κοινού αναπτύσσοντας έτσι μια ελεύθερη επικοινωνία στην οποία δεν θα υπάρχουν οριοθετημένα πλαίσια.

2. **Διαφάνεια (Openness):** Οι περισσότερες υπηρεσίες μέσω κοινωνικής δικτύωσης είναι ανοιχτές σε σχόλια και συμμετοχή, ενώ σπάνια υπάρχουν εμπόδια στην πρόσβαση και στην χρήση του περιεχομένου.
3. **Συνομιλία (Conversation):** Σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης που αφορούν μόνο την μετάδοση (broadcasting) ενός περιεχομένου σε ένα ακροατήριο, τα Social Media αποτελούν μια συνομιλία διπλής κατεύθυνσης.
4. **Κοινότητα (Community):** Τα μέσα κοινωνικής δικτύωσης μπορούν να βοηθήσουν στην άμεση ανάπτυξη κοινοτήτων με τις οποίες ο χρήστης μπορεί να μοιράζεται τα κοινά του ενδιαφέροντα. Με αυτόν τον τρόπο οι χρήστες μπορούν να μοιράζονται κάποιο κοινό ενδιαφέρον, τις απόψεις τους, να ανταλλάζουν εμπειρίες κλπ.
5. **Συνεκτικότητα (Connectedness):** Τα περισσότερα είδη των μέσων κοινωνικής δικτύωσης αναπτύσσουν την συνεκτικότητα τους κάνοντας χρήση συνδέσεων με άλλες ιστοσελίδες, πόρους και ανθρώπους.

1.8.2 Κατηγοριοποιήσεις των μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης μπορούν να κατηγοριοποιηθούν ανάλογα με διάφορα χαρακτηριστικά που διαθέτουν. Μερικές κύριες κατηγορίες των μέσων κοινωνικής δικτύωσης είναι:

1. **Δίκτυα κοινής χρήσης πολυμέσων (Social Media Sharing Sites):** Παραδείγματα αποτελούν τα: Snapchat, YouTube, Flickr, Vimeo, SoundCloud, MySpace, Instagram. Πρόκειται για μέσα χρήσης πολυμέσων που βοηθούν για την εύρεση και κοινή χρήση φωτογραφιών, βίντεο ή ήχου. Αυτοί οι ιστότοποι κοινωνικής δικτύωσης επιτρέπουν τους χρήστες να μοιράζονται εύκολα πολυμεσικό περιεχόμενο στο διαδίκτυο. Το περιεχόμενο μπορεί να δημοσιευτεί είτε ιδιωτικά είτε δημόσια για όλους τους χρήστες/
2. **Φόρουμ συζήτησης (Forums):** Παραδείγματα αποτελούν τα: Reddit, Digg, Stack Overflow. Βοηθούν τους χρήστες κάνοντας ερωτήσεις, συζητώντας πληροφορίες και ανταλλάσσουν απόψεις για διάφορα θέματα. Ο βασικός στόχος των φόρουμ είναι να διαθέτουν συζητήσεις όπου θα υπάρχουν διάφορες κατηγορίες αλλά και ενδιαφέροντα. Οι χρήστες μπορούν να συμμετέχουν

ενεργά στις συζητήσεις, να παραθέτουν ερωτήσεις, να παρέχουν απαντήσεις και να μοιράζονται γνώμες. Επίσης, σε ορισμένες ιστοσελίδες, οι χρήστες μπορούν να συμμετέχουν σε συζητήσεις ανώνυμα.

3. **Δίκτυα σελιδοδεικτών και επιμέλειας περιεχομένου (social bookmarking):** Παραδείγματα αποτελούν τα: Pinterest, Flipboard. Οι χρήστες μπορούν να αποθηκεύουν συνδέσμους που τους ενδιαφέρουν δημόσια επιτρέποντας στους άλλους να τους βρουν και να τους χρησιμοποιήσουν. Επίσης οι χρήστες μπορούν να οργανώνουν τους συνδέσμους τους με κατηγορίες και ετικέτες για ευκολότερη αναζήτηση.
4. **Ιστολόγια (blogging, micro-blogging):** Παραδείγματα αποτελούν τα: WordPress, Blogger, X (πρώην Twitter). Ένα ιστολόγιο είναι ένα διαδικτυακό περιοδικό στο οποίο η λίστα καταχωρήσεων είναι από την πιο πρόσφατη καταχώρηση στην παλαιότερη. Συνήθως το περιεχόμενό τους μπορεί να είναι οτιδήποτε από σχολιασμούς σε ειδικά θέματα για διάφορα πράγματα, ειδήσεις και άλλα πολλά. Ο κύριος στόχος του είναι η δημοσίευση για κάθε θέμα και υπάρχει κυρίως ελευθερία έκφρασής και εκφράζονται απόψεις σε διάφορα θέματα.
5. **Διαδικτυακές τηλεδιασκέψεις (web-conferencing):** Παραδείγματα αποτελούν τα: Zoom, WebEx, Skype. Δίνει τη δυνατότητα στα άτομα να επικοινωνήσουν σε πραγματικό χρόνο μέσω του διαδικτύου ανεξαρτήτως της γεωγραφικής τους τοποθεσίας μέσω τηλεδιασκέψεων στις οποίες συμμετέχουν πολλοί συνομιλητές από διάφορες τοποθεσίες συνδεδεμένοι από οποιαδήποτε συσκευή, όπως υπολογιστή, τάμπλετ, smartphone κ.λπ.
6. **Wiki:** Παραδείγματα αποτελούν τα: Wikipedia, Fandom. Πρόκειται για διαδικτυακή πλατφόρμα όπου οι χρήστες έχουν τη δυνατότητα να προσθέτουν, να τροποποιούν ή και να διαγράφουν το περιεχόμενο σε συνεργασία με άλλους. Είναι ένα είδος συστήματος διαχείρισης περιεχομένου. Το περιεχόμενο αυτό μπορεί να δημιουργείται χωρίς να υπάρχει κάποιος ιδιοκτήτης ή κάτοχος. Επιπλέον, επιτρέπουν στο χρήστη με την συνεργασία πολλών χρηστών να συνεισφέρουν σε ένα κοινό έργο με αποτέλεσμα να βελτιώνουν το περιεχόμενο και την ακρίβεια των πληροφοριών.
7. **Ιστότοποι κοινωνικής δικτύωσης (social networks):** Παραδείγματα αποτελούν τα: Facebook, X (πρώην Twitter), Discord. Οι ιστότοποι κοινωνικής

δικτύωσης δίνουν την δυνατότητα στους χρήστες δημιουργούν προφίλ, να επικοινωνούν και να μεταδίδουν ιδέες. Οι άνθρωποι μοιράζονται τι συμβαίνει στην ατομική τους ζωή ή γενικότερα πληροφορίες που επιθυμούν να δημοσιεύσουν. Οι χρήστες μπορούν να δημοσιεύσουν κείμενο, φωτογραφίες, βίντεο ενώ παράλληλα άλλοι χρήστες μπορούν να σχολιάζουν και να αξιολογούν περιεχόμενο που δημοσιεύεται. Ταυτόχρονα, υπάρχει και δυνατότητα δημιουργίας ομάδων και σελίδων όπου συγκεντρώνονται χρήστες που έχουν κάποια κοινά ενδιαφέροντα.

1.9 Ιστορική Εξέλιξη Μέσων Κοινωνικής Δικτύωσης

1.9.1 Η Πρώτη Ιστοσελίδα: SixDegrees



Εικόνα 3: Το λογότυπο της ιστοσελίδας SixDegrees (Πηγή: <http://www.sixdegrees.com/>)

Η πρώτη πλατφόρμα μέσου κοινωνικής δικτύωσης που επέτρεπε στους χρήστες να συνδεθούν με το email τους, δημιουργήθηκε το 1997 ήταν το SixDegrees.com. Αυτή η πλατφόρμα διευκόλυνε τους χρήστες όπου μπορούσαν να φτιάξουν προφίλ, λίστες από φίλους και έδινε την δυνατότητα στους φίλους να αλληλεπιδράσουν μεταξύ τους με σύντομα μηνύματα. Η πλατφόρμα συγκέντρωσε περίπου 3,5 εκατομμύρια χρήστες. Αυτό ήταν ένα σημαντικό ορόσημο λαμβάνοντας υπόψη την εποχή στην οποία υπήρχε ο ιστότοπος κοινωνικής δικτύωσης. Ωστόσο, οι χρήστες δεν μπορούσαν να κάνουν πολλά πράγματα με αποτέλεσμα το δίκτυο να κλείσει το 2001. Σύμφωνα με τον ιδρυτή της, A. Weinreich, ο λόγος που απέτυχε ήταν το γεγονός ότι ο ιστότοπος ήταν ότι «η ιστοσελίδα αυτή ήταν πολύ μπροστά από την εποχή της». Το 1997 πουλήθηκε η πλατφόρμα για 125 εκατομμύρια δολάρια. Πριν το SixDegrees, υπήρχε και το

classmates με το οποίο είχαν πολλά κοινά. Ωστόσο μόνο το SixDegrees έδινε την δυνατότητα στους χρήστες να επικοινωνούν μεταξύ τους στέλνοντας μηνύματα.

1.9.2 Ιστοσελίδα: FRIENDSTER



Εικόνα 4: Η αρχική ιστοσελίδα του Friendster το 2004. (Πηγή: <http://www.friendster.com>)

Το Friendster ξεκίνησε από τον Jonathan Abrams και τον Peter Chin τον Μάρτιο του 2002. Η ιδέα ήταν πως θα επέτρεπε τους χρήστες να βρίσκουν και να μιλάνε με φίλους σε όλο τον κόσμο. Στις αρχές του 2003, η πλατφόρμα είχε παραπάνω από 3

εκατομμύρια χρήστες. Ο στόχος του ήταν ώστε όλοι οι χρήστες να μπορούν να αλληλοεπιδρούν με τους παλιούς φίλους τους αλλά και να κάνουν νέους. Οι διακομιστές επιβραδύνονταν πάρα πολύ λόγω προβλημάτων βάσης δεδομένων ή ακόμα και κωδικοποίησης που δεν ήταν βελτιστοποιημένη. Επίσης, ο αριθμός των χρηστών ξεκίνησε να μειώνεται όταν ο ιστότοπος αποφάσισε να διαγράψει ψεύτικα προφίλ αλλά και προφίλ χωρίς φωτογραφία. Επιπλέον ένα άλλο σοβαρό πρόβλημα ήταν πως καθώς το Friendster έγινε δημοφιλές, αυξήθηκε η χρήση της πλατφόρμας. Το 2011 επικεντρώθηκε ως ιστοσελίδα gaming και αφορούσε περισσότερο στην gaming κοινότητα. Οι χρήστες απογοητεύτηκαν, με αποτέλεσμα να χαθεί η εμπιστοσύνη ανάμεσα στους χρήστες και στην ιστοσελίδα και αυτό οδήγησε στην πτώση της εταιρείας. Παράλληλα, είχε πολλά τεχνικά προβλήματα και για αυτό έκλεισε το 2015. Επίσης, το Friendster ήταν αρκετά δημοφιλής στις Φιλιππίνες και στην Ασία αλλά με την εμφάνιση του Myspace και του Facebook έχασε την κυριαρχία του. Πρόκειται για ένα από τα πιο σημαντικά κοινωνικά δίκτυα και είχε μεγάλη επίδραση στην δημιουργία άλλων δικτύων.

1.9.3 Ιστοσελίδα: LinkedIn



Εικόνα 5: Το λογότυπο του LinkedIn (Πηγή: <https://www.linkedin.com/>)

Ιδρύθηκε τον Δεκέμβριο του 2002 από τον Reid Hoffman και τα μέλη της ιδρυτικής ομάδας από το PayPal και το Socialnet.com αλλά ξεκίνησε στις 5 Μαΐου του 2003.

Τώρα ανήκει πλέον στην Microsoft.

Επικεντρώθηκε κυρίως στο επαγγελματικό τομέα. Είναι μια πλατφόρμα που δημιουργήθηκε για επιχειρηματική αλληλεπίδραση δίνοντας την δυνατότητα στους χρήστες να αναζητήσουν εργασία και να δημοσιεύσουν το βιογραφικό τους ενώ οι εργοδότες μπορούν να αναρτήσουν θέσεις εργασίας. Το προφίλ LinkedIn συνήθως περιλαμβάνει πληροφορίες σχετικά με την εργασιακή εμπειρία, τις δεξιότητες, την εκπαίδευση κ.λπ. Το 2016, πουλήθηκε στην Microsoft για 26,4 δισεκατομμύρια δολάρια περίπου. Συγκεκριμένα, ήταν πιο επιτυχημένη ως πλατφόρμα προσλήψεων παρά ως προορισμός περιεχομένου. Τον Ιανουάριο του 2023 το LinkedIn είχε παραπάνω από 900 εκατομμύρια εγγεγραμμένα μέλη. Ανεξάρτητα από αυτό, το LinkedIn είναι μοναδικό ως ένα διαδικτυακό επαγγελματικό δίκτυο και έχει καθιερωθεί ως απαραίτητο εργαλείο για οποιονδήποτε προσλαμβάνει, εμπορεύεται ή πουλά εργασία. Επιπλέον, το LinkedIn είναι αρκετά γνωστό για την επαγγελματική εύρεσή καθώς οι χρήστες μπορούν να αναδείξουν τις δεξιότητές τους, αλλά και να επικοινωνήσουν με επαγγελματίες για να αποκτήσουν συνεργασία.

1.9.4 Ιστοσελίδα: MYSPACE



Εικόνα 6: Το λογότυπο του MySpace (Πηγή: <https://myspace.com/>)

Το Myspace ιδρύθηκε τον Αύγουστο του 2003 στις Ηνωμένες Πολιτείες της Αμερικής. Ήταν το μεγαλύτερο μέσο κοινωνικής

δικτύωσης το διάστημα του 2005-2009. Δημιουργήθηκε από υπαλλήλους της eUniverse που είδαν τους περιορισμούς που είχε το Friendster και αποφάσισαν να υλοποιήσουν ένα μέσο κοινωνικής δικτύωσης που θα είχε περισσότερες δυνατότητες καθώς οι χρήστες μπορούσαν συμμετέχουν και να συνομιλούν σε αντίθεση με το Friendster που περιορίστηκε στα παιχνίδια. Οι πρώτοι χρήστες ήταν υπάλληλοι του

eUniverse και το δίκτυο επεκτάθηκε στέλνοντας προσκλήσεις οι χρήστες μεταξύ φίλων τους για να εγγραφούν στην ιστοσελίδα. Το 2005, το Myspace πουλήθηκε στην Newscorp για 580 εκατομμύρια δολάρια. Μέχρι το τέλος του 2008, η συνολική αξία του δικτύου ήταν 12 δισεκατομμύρια δολάρια. Το 2009, το Myspace ήταν το μεγαλύτερο κοινωνικό μέσο μέχρι που ξεπεράστηκε σε επισκέψεις από ένα νέο αναπτυσσόμενο κοινωνικό μέσο, το Facebook. Ύστερα, ακολούθησε μια καθοδική πορεία με αυξημένο ανταγωνισμό και ξεκίνησε να χάνει τους νεότερους χρήστες οι οποίοι χρησιμοποιούσαν άλλες πλατφόρμες όπως το Facebook. Υπάρχουν πολλοί λόγοι που το MySpace απέτυχε, ο κύριος λόγος είναι ότι επικεντρώθηκε σε χρήστες που ήταν λάτρεις της μουσικής και της ψυχαγωγίας αλλά αυτό οδήγησε στον περιορισμό των χρηστών. Επίσης, η συμφωνία με την Google αξίας 900 εκατομμυρίων δολαρίων είχε καθοριστικό ρόλο καθώς το MySpace προωθούσε διαφημίσεις εντός της ιστοσελίδας. Ωστόσο, αυτό είχε αρνητικά αποτελέσματα όπως την υπερφόρτωση της ιστοσελίδας και δημιουργούσε προβλήματα στην χρήση. Παρ' όλα αυτά το Myspace αποτελεί ένα σημαντικό μέρος για τα κοινωνικά δίκτυα καθώς είναι ένα από τα πρώτα μεγάλα δίκτυα που δημιουργήθηκαν και έδωσαν στους χρήστες πολλές δυνατότητες.

1.9.5 Ιστοσελίδα: Facebook

The image shows the Facebook logo, which consists of the word "facebook" in a bold, blue, lowercase sans-serif font.

Εικόνα 7: Το λογότυπο του Facebook (Πηγή: <https://www.facebook.com/>)

Τον Φεβρουάριο του 2004, δημιουργήθηκε το Facebook από τους Mark Zuckerberg, Eduardo Saverin, Andrew McCollom, Dustin Moskovitz και Chris

Hughes. Ο Mark Zuckerberg που ήταν φοιτητής του Harvard μαζί με τους συμμαθητές του, δημιούργησαν την ιστοσελίδα για φοιτητές του Harvard. Το αρχικό του όνομα ήταν «*the facebook*». Ο κύριος σκοπός του στην αρχή ήταν η σύνδεση φίλων στο πανεπιστήμιο του Harvard και ήταν μόνο μεταξύ φοιτητών. Αργότερα επεκτάθηκε και σε άλλα πανεπιστήμια όπως το Stanford. Ωστόσο, στο Χάρβαρντ κάθε χρόνο εκδίδεται ένα βιβλίο με φωτογραφίες και πληροφορίες από όλους τους μαθητές που ήταν στο πανεπιστήμιο που ονομάζοταν «*Facebook*». Εκείνο το διάστημα το βιβλίο αυτό καθυστέρησε εξαιτίας τυπογραφικού λάθους και προκάλεσε αντιδράσεις στους φοιτητές. Το 2005 έδωσε την δυνατότητα πρόσβασης σε μαθητές συγκεκριμένων

λυκείων και μέλη από ορισμένες μαθητικές κοινότητες. Το 2006 άνοιξε τους ορίζοντές του και σε άτομα 13+ σε όλο τον κόσμο. Τότε δεν υπήρχαν πολλά κοινωνικά μέσα στο Διαδίκτυο που να ανταγωνίζονταν για την προσοχή των χρηστών. Οι περισσότεροι φοιτητές δεν είχαν ακούσει ποτέ για το Friendster, το YouTube δεν υπήρχε κ.λπ. Ο Peter Thiel, συνιδρυτής της PayPal, έκανε την πρώτη επένδυση στο Facebook το 2004, ενώ τον Μάιο του 2005 η Accel έκανε και αυτή επένδυση στη πλατφόρμα. Λίγο αργότερα το Facebook έγινε από τα ταχύτερα αναπτυσσόμενα μέσα κοινωνικής δικτύωσης στο διαδίκτυο. Το Facebook είναι μια πλατφόρμα όπου οι χρήστες μπορούν να δημιουργήσουν προφίλ, να ανεβάσουν φωτογραφίες και βίντεο, να επικοινωνήσουν με φίλους, να κοινοποιήσουν νέα και να κάνουν αναρτήσεις. Το Facebook αποτελεί ένα από τα πιο σημαντικά μέσα καθώς το 2008 ξεπέρασε το MySpace. Μέχρι τον Ιούλιο του 2010 το Facebook είχε φτάσει 500 εκατομμύρια χρήστες και το 2013 είχε φθάσει να έχει πάνω από 1 δισεκατομμύριο χρήστες. Επίσης, το 2014 το Facebook εξαγόρασε για 19 δισεκατομμύρια το WhatsApp αλλά και άλλες εταιρίες όπως το Instagram. Το 2016, η αποτίμηση του Facebook έφτασε τα 350 δισεκατομμύρια δολάρια. Το Facebook έγινε το πιο δημοφιλές δίκτυο στον κόσμο και εξακολουθεί να είναι ένα από τα πιο δημοφιλή κοινωνικά δίκτυα μέχρι και σήμερα.

1.9.6 Ιστοσελίδα: Reddit



Εικόνα 8: Το λογότυπο του Reddit.
(Πηγή: <https://www.reddit.com/>)

Το 2005, ιδρύθηκε το Reddit από τους Steve Huffman και Alexis Ohanian, απόφοιτοι του πανεπιστημίου της Βιρτζίνιας, για το οποίο είχαν πάρει χρηματοδότηση 100.000 δολάρια από το Y Combinator τον Ιούνιο του 2005. Το Reddit είναι ένα κοινωνικό δίκτυο που έχει στόχο να προσφέρει ειδήσεις και όπου οι χρήστες θα μπορούν να δημιουργούν λογαριασμό για να δημοσιεύουν περιεχόμενο αλλά και για να σχολιάζουν άλλες δημοσιεύσεις.

1.9.7 Ιστοσελίδα: YouTube



Εικόνα 9: Το λογότυπο του YouTube.
(Πηγή: <https://www.youtube.com/>)

Τον Φεβρουάριο του 2005, ιδρύθηκε το YouTube από πρώην υπάλληλους της PayPal, τους Steve Chen, Chad Hurley και Jawed Karim. Αρχικά, ήθελαν να δημιουργήσουν έναν ιστότοπο με σκοπό την ανταλλαγή βίντεο μεταξύ φίλων. Δημιούργησαν το YouTube με στόχο την ανάρτηση βίντεο, κοινοποίησης αλλά και προβολής σε όλο τον κόσμο. Το YouTube, τον Οκτώβριο του 2006, αγοράστηκε από την Google για 1,65 δισεκατομμύρια δολάρια. Η χρήση του στην αρχή απαιτούσε τον Adobe Flash Player, μέχρι που αντικαταστάθηκε από HTML5. Τον Απρίλιο του 2005, δημοσιεύτηκε το πρώτο βίντεο που είχε διάρκεια 18 δευτερόλεπτα από τον ιδρυτή Jawed Karim με τίτλο «*Me at the Zoo*» το οποίο είχε ξεπεράσει τις 45 εκατομμύρια προβολές. Το YouTube δίνει την δυνατότητα στους χρήστες να παρακολουθούν βίντεο και να δηλώσουν αν τους αρέσει ή και να σχολιάσουν. Ενώ εγγεγραμμένοι χρήστες μπορούν να αναρτούν βίντεο, μετά τον Μάρτιο του 2006, υπήρχε όριο στην διάρκεια μικρότερη από δέκα λεπτά καθώς το YouTube παρατήρησε πως πολλά βίντεο που είχαν μεγάλη διάρκεια ήταν συνήθως παράνομη αναπαραγωγή οπτικοακουστικού υλικού. Τον Απρίλιο του 2011, κυκλοφόρησε το YouTube Live και έτσι το YouTube απέκτησε τη δυνατότητα να κάνει ζωντανές μεταδόσεις. Πλέον, το YouTube έχει εξελιχθεί και προσφέρει πολλές δυνατότητες σε πολλούς τομείς.

1.9.8 Ιστοσελίδα: X (πρώην Twitter)



Εικόνα 10: Το λογότυπο του X σήμερα (αριστερά) και το παλιό λογότυπο όταν η πλατφόρμα ονομαζόταν Twitter (δεξιά). (Πηγή: <https://twitter.com/>)

Το X ξεκίνησε τον Μάρτιο του 2006 από τους Jack Dorsey, Noah Glass, Biz Stone και Evan Williams με το όνομα «*Twitter*». Είναι μια πλατφόρμα που λειτουργεί σαν ένα σύστημα μικρο-ιστολογιών (microblogging) και επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν σύντομες αναρτήσεις που ονομαζόταν «*tweets*», τα οποία περιορίζονταν σε 140 χαρακτήρες για κάθε ανάρτηση αλλά το Νοέμβριο του 2017 αυξήθηκαν σε 280 χαρακτήρες. Στις αρχές του Ιουνίου 2023, ο περιορισμός αυξήθηκε στους 4000 χαρακτήρες για χρήστες Premium. Στο X,

μπορείς μόνο να έχεις followers ωστόσο δεν είναι απαραίτητο για τους χρήστες να ακολουθούν ο ένας τον άλλον και συνεπώς κάθε χρήστης μπορεί να ακολουθεί όποιον θέλει. Σημαντικό παράγοντα αποτελούν τα «*hashtags*», ετικέτες που ξεκινούν με το σύμβολο του αριθμού (#) για την ευκολότερη αναζήτηση σχετικών αναρτήσεων. Το 2012, είχε αποκτήσει περισσότερο από 100 εκατομμύρια χρήστες και αναρτιούνταν 340 εκατομμύρια tweets την ημέρα. Επίσης έχει χαρακτηριστεί ως ένα από τα πιο δημοφιλή κοινωνικά δίκτυα για τους νέους στις Ηνωμένες Πολιτείες της Αμερικής. Στις 27 Οκτωβρίου 2022, ο επιχειρηματίας Elon Musk αγόρασε το Twitter για 44 δισεκατομμύρια δολάρια. Στις 22 Ιουλίου 2023, ο Elon Musk ανακοίνωσε την αλλαγή του ονόματος της δημοφιλής ιστοσελίδας από «*Twitter*» σε «*X*», με στόχο να δημιουργήσει μια εφαρμογή για τα πάντα.

1.9.9 Ιστοσελίδα: Pinterest



Εικόνα 11: Το λογότυπο του Pinterest.
(Πηγή: <https://www.pinterest.com/>)

10.000 χρήστες. Είναι ένας ιστότοπος κοινωνικής δικτύωσης όπου δίνεται η δυνατότητα αποθήκευσης εικόνων και η ανακάλυψη πληροφοριών στο διαδίκτυο χρησιμοποιώντας εικόνες και σε μικρότερη κλίμακα, κινούμενα GIF και βίντεο, με τη μορφή πινακίδων. Επιτρέπει στους χρήστες να μοιράζονται εικόνες και να ανακαλύπτουν νέα ενδιαφέροντα προσθέτοντας εικόνες ή βίντεο στους δικούς τους ή άλλους πίνακες, βλέποντας τι έχουν καρφίτσώσει άλλοι χρήστες. Ο ιστότοπος δημιουργήθηκε από τους Ben Silbermann, Paul Sciarra και Evan Sharp και είχε 433 εκατομμύρια παγκόσμιους μηνιαίους ενεργούς χρήστες από τον Ιούλιο του 2022.

Το Pinterest ξεκίνησε τον Δεκέμβριο του 2009 από το δημιουργό iPhone εφαρμογών Ben Silberman και ήταν κλειστό μέχρι τον Μάρτιο του 2010. Μέσα σε 9 μήνες αφού άνοιξε είχε φτάσει στους

1.9.10 Ιστοσελίδα: Instagram



Εικόνα 12: Το λογότυπο του Instagram. (Πηγή: <https://www.instagram.com/>)

Τον Οκτώβριο του 2010 δημιουργήθηκε από τον Kevin Systrom και τον Mike Krieger μία νέα υπηρεσία κοινωνικής δικτύωσης, το Instagram, που βασίζεται στην κοινή χρήση φωτογραφιών και βίντεο. Αρχικά, η πλατφόρμα είχε την ονομασία Burbn και σχετιζόταν με φωτογραφίες, σημειώσεις και τοποθεσίες αλλά αυτό δεν είχε μεγάλη επιτυχία και αποφάσισαν να αναπτύξουν το Burbn και να το μετονομάσουν σε Instagram. Το όνομα του είναι εμπνευσμένο από τις παλιές Polaroid κάμερες που εκτύπωναν άμεσα μια φωτογραφία. Το Δεκέμβριο του 2010 είχε 1 εκατομμύριο εγγεγραμμένους χρήστες. Στην αρχή, περιοριζόταν μόνο σε iOS αλλά έγινε διαθέσιμο και σε Android τον Απρίλιο του 2012. Παράλληλα, το Facebook αγόρασε την υπηρεσία το 2012 για 1 δισεκατομμύριο δολάρια σε ρευστό και μετοχές. Όπως οι περισσότερες εφαρμογές κοινωνικών μέσων, το Instagram επιτρέπει στους χρήστες να ακολουθούν άλλους χρήστες που τους ενδιαφέρουν. Αυτό δημιουργεί μια ροή στην αρχική σελίδα που εμφανίζει πρόσφατες αναρτήσεις. Μπορείτε να κάνετε like σε αναρτήσεις και να τις σχολιάσετε. Τα φίλτρα είναι ένας άλλος λόγος που οδήγησε στην αύξηση της δημοτικότητας του Instagram. Το Instagram σήμερα έχει εξελιχθεί σε ένα σημαντικό εργαλείο τα τελευταία χρόνια και είναι πολύ σημαντικό στον χώρο του μάρκετινγκ, της διαφήμισης και προώθησης.

1.9.11 Ιστοσελίδα: Snapchat



Εικόνα 13: Το λογότυπο του Snapchat. (Πηγή: <https://www.snapchat.com/>)

Το Snapchat εμφανίστηκε το Σεπτέμβριο του 2011. Πρόκειται για εφαρμογή ανταλλαγής μηνυμάτων βίντεο που δημιουργήθηκε από τους Evan Spiegel, Bobby Murphy και Reggie Brown όταν ήταν φοιτητές στο Πανεπιστήμιο του Stanford. Ήθελαν να δημιουργήσουν μια εφαρμογή που θα μπορούσαν οι χρήστες να στέλνουν μεταξύ τους φωτογραφίες και βίντεο και μετά από λίγα δευτερόλεπτα να διαγράφονται αυτόματα. Αρχικά, η εφαρμογή μπορούσε να χρησιμοποιηθεί από μόνο όσοι

είχαν iOS, αλλά αργότερα έγινε διαθέσιμο και για το Android. Χρησιμοποιώντας την εφαρμογή, οι χρήστες μπορούν να τραβήξουν φωτογραφίες, να εγγράψουν βίντεο, να προσθέσουν κείμενο και σχέδια και να τα στείλουν σε μια ελεγχόμενη λίστα παραληπτών. Όταν ο παραλήπτης δει το περιεχόμενο αυτό εξαφανίζεται και δε μπορεί να το ξαναδεί. Παρόμοια, δυνατότητα είναι τα «*stories*» όπου το περιεχόμενο είναι διαθέσιμο μόνο για 24 ώρες. Η πλατφόρμα είναι ιδιαίτερα δημοφιλής σε εφήβους και έχει γύρω στους 186 εκατομμύρια ενεργούς χρήστες.

1.9.12 Ιστοσελίδα : TikTok



Εικόνα 14: Το λογότυπο του TikTok. (Πηγή: <https://www.tiktok.com/>)

Το TikTok δημιουργήθηκε στην Κίνα και κυκλοφόρησε για πρώτη φορά τον Σεπτέμβριο του 2016 από την Bytedance.

Στην αρχή λεγόταν «*Douyin*» και μετονομάστηκε σε TikTok. Έχει πολλές ομοιότητες με το Vine που είχε κλείσει λίγα χρόνια πριν και γρήγορα το Douyin έγινε γνωστό στην Κίνα. Το 2017, η ByteDance αγόρασε την εφαρμογή «*Musical.ly*» και έτσι το Douyin συγχωνεύτηκε και μετονομάστηκε σε TikTok το 2018 με τους παλιούς λογαριασμούς χρηστών του Musical.ly να μεταφέρονται στη νέα εφαρμογή. Το Musical.ly ήταν αρχικά μια πλατφόρμα που επέτρεπε στους χρήστες να δημιουργούν σύντομα βίντεο lip-sync αλλά και κωμικά βίντεο. Κυκλοφόρησε τον Αύγουστο του 2014 και αργότερα συγχωνεύτηκε στο TikTok στις 2 Αυγούστου του 2018. Το TikTok, σήμερα, είναι μια πλατφόρμα κοινωνικών μέσων με κύρια λειτουργία τη δημιουργία, την κοινή χρήση και την ανακάλυψη σύντομων βίντεο. Αυτή η εφαρμογή στοχεύει να παρέχει μια πλατφόρμα για τη νέα γενιά να εκφράσει τις καινοτόμες και δημιουργικές ιδέες. Τον Οκτώβριο του 2020, το TikTok ξεπέρασε τις 2 δισεκατομμύρια λήψεις από κινητά παγκοσμίως.

1.9.13 Παράλληλες Εμφανίσεις

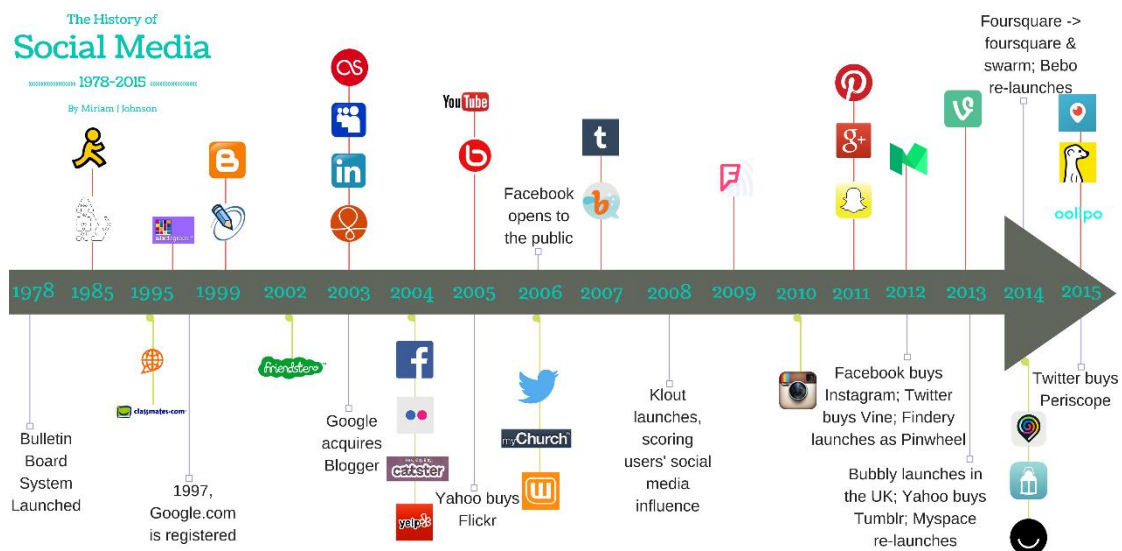
Το 1999, εμφανίστηκε το LiveJournal που δημιουργήθηκε αρχικά από τον Brad Fitzpatrick και λειτουργούσε ως προσωπική πλατφόρμα ημερολογίου. Για να το χρησιμοποιήσει ο χρήστης έπρεπε να εγκατασταθεί ολόκληρο λογισμικό στον

υπολογιστή του. Ωστόσο δεν γνώρισε τόσο μεγάλη ανάπτυξη στις Ηνωμένες Πολιτείες Αμερικής αλλά ήταν δημοφιλές στην Ρωσία. Απέκτησε μεγάλη δημοτικότητα στις αρχές του 2000.

Το 2000, δημιουργήθηκε στην Σουηδία το LunarStorm το οποίο είχε χρηματοδοτηθεί από εμπορικές διαφημίσεις για εφήβους και περιείχε καταλόγους βιβλίων, βιβλία και ημερολόγια.

Το 2001, δημιουργήθηκε η ιστοσελίδα Ryze η οποία είχε στόχο οι χρήστες να αξιοποιήσουν τα επιχειρηματικά τους δίκτυα. Ο ιδρυτής του πρόσθεσε τα πρώτα μέλη από την επιχειρηματική και επιστημονική κοινότητα του Σαν Φρανσίσκο, ενώ οι ιστοσελίδες LinkedIn, Friendster και Tribe συνδέονταν προσωπικά και επαγγελματικά με την ιστοσελίδα Ryze.

Το 2003, δημιουργήθηκε το Hi5 στο οποίο οι χρήστες μπορούσαν να δημιουργήσουν ένα προφίλ όπου θα υπήρχαν οι προσωπικές τους πληροφορίες όπως τα ενδιαφέροντα τους, η ηλικία τους, φωτογραφίες και άλλο επιπλέον περιεχόμενο. Οι χρήστες μπορούσαν να στέλνουν αιτήματα φιλίας μέσω e-mail σε άλλους χρήστες. Το 2010, το Hi5 έγινε μέρος του κοινωνικού σύμπαντος παιχνιδιών. Από τις 3 δισεκατομμύρια επισκέψεις το μήνα ιστοσελίδα έπεσε στα 46 εκατομμύρια και εξαιτίας από αυτό πουλήθηκε στο Tagged.



Εικόνα 15: Χρονοδιάγραμμα με τις εμφανίσεις των διάφορων κοινωνικών μέσων. (Πηγή: <https://www.booksaresocial.com/social-media-timeline/>)

1.10 Λόγοι επιτυχίας της κοινωνικής δικτύωσης

Η τεχνολογική εξέλιξη δημιούργησε πολλά κοινωνικά δίκτυα που είναι απίστευτα δημοφιλής για πολλούς λόγους.

- Η **επικοινωνία και σύνδεση** αποτελεί έναν από τους κύριους λόγους που τα κοινωνικά μέσα προσελκύουν τους ανθρώπους. Οι χρήστες μπορούν να επικοινωνούν με τους φίλους, συγγενείς και γνωστούς, ανεξάρτητα από την απόσταση και τον διαθέσιμο χρόνο τους, και να σχολιάζουν κοινωνικά θέματα. Οι πλατφόρμες των κοινωνικών δικτύων είναι σχεδιασμένες εύκολες και προσβάσιμες για κάθε άνθρωπο είτε γνωρίζει από την τεχνολογία είτε όχι. Οι χρήστες μπορούν εύκολα να δημιουργήσουν προφίλ και να ανεβάσουν φωτογραφίες και βίντεο. Το Facebook αποτελεί ένα δημοφιλές παράδειγμα μέσου κοινωνικής δικτύωσης με αυτά τα χαρακτηριστικά.
- Οι **επιχειρηματικές ευκαιρίες** είναι ένας άλλος λόγος που τα μέσα κοινωνικής δικτύωσης είναι πολύ δημοφιλής. Πολλές επιχειρήσεις τα χρησιμοποιούν για να προωθήσουν, να διαφημίσουν τις υπηρεσίες τους, να ενημερώσουν το κοινό τους και να αποκτήσουν νέους πελάτες. Επίσης, οι χρήστες μπορούν να παρουσιάσουν στο προφίλ τους ένα είδος βιογραφικού ή ακόμα και να αναζητήσουν εργασία πάνω σε οποιοδήποτε τομέα που τους ενδιαφέρει. Μια τέτοια πλατφόρμα είναι το LinkedIn.
- Η **ενημέρωση** γίνεται πιο εύκολη στα μέσα κοινωνικής δικτύωσης αφού νέοι χρήστες τα χρησιμοποιούν για να ενημερώνονται για νέα γεγονότα και εξελίξεις που συμβαίνουν και έχουν τη δυνατότητα παρακολούθησης ειδήσεων.
- Τα κοινωνικά δίκτυα παρέχουν πάρα πολλές **ψυχαγωγικές** δυνατότητες όπου οι χρήστες μπορούν να παρακολουθούν βίντεο, να παίζουν παιχνίδια ή και να επικοινωνούν με άλλους χρήστες.

1.11 Οι εφαρμογές των μέσων κοινωνικών δικτύων

Τα κοινωνικά δίκτυα μπορούν να προσφέρουν πλήθος δυνατοτήτων στην καθημερινή ζωή των χρηστών. Αποτελεί μια σημαντική βάση σε διάφορους τομείς τα τελευταία χρόνια καθώς πρόσφερε πολλές αλλαγές στην σύγχρονη εποχή όπως στην επικοινωνία, στην ενημέρωση, στην ψυχαγωγία και στις επιχειρήσεις.

Μερικά από τα αποτελέσματά της έχουν ως εξής:

Ανάπτυξη επιχειρηματικών δυνατοτήτων

Πολλές είναι οι επιχειρήσεις που χρησιμοποιούν τα κοινωνικά δίκτυα για να μπορέσουν να αυξήσουν τη φήμη τους. Έχουν τη δυνατότητα να επικοινωνούν απευθείας με το κοινό ώστε να υπάρχει αλληλεπίδραση μεταξύ πελάτη και επιχείρησης. Η δημιουργία κοινωνικών δικτύων για τις επιχειρήσεις δίνει πολλές δυνατότητες και ευκαιρίες σε πολλούς τομείς. Μία βασική ικανότητα είναι ότι μπορούν να προβάλλουν τα προϊόντα και τις υπηρεσίες τους και να τα προωθήσουν με χαμηλό κόστος διαφήμισης σε σχέση με άλλα μέσα όπως την τηλεόραση. Παράλληλα, ανοίγουν τους ορίζοντες τους στοχεύοντας ένα περισσότερο κοινό. Επιπλέον, οι πλατφόρμες κοινωνικών δικτύων μπορούν να παρακολουθούν τις αντιδράσεις και τα ενδιαφέροντα του κοινού και με αυτό τον τρόπο να αναλύσουν τα δεδομένα για να προσαρμόζονται οι διαφημίσεις ανάλογα με τις τάσεις που υπάρχουν. Επίσης, οι επιχειρήσεις μπορούν να έχουν απευθείας επικοινωνία με τους χρήστες και να τους βοηθήνε σε ερωτήσεις που έχουν. Τέλος, η εικόνα που θα δημιουργηθεί μέσα από τα κοινωνικά δίκτυα βοηθάει την επιχείρηση έτσι να αναπτυχθεί μια θετική γνώμη για αυτήν.

Εκπαίδευση

Τα κοινωνικά δίκτυα αποτελούν εργαλεία που μπορούν να παρέχουν σε φοιτητές και ιδρύματα πολλές ευκαιρίες για τη βελτίωση μεθόδων μάθησης, καθώς μπορούν να προσφέρουν τη δυνατότητα της κοινής χρήσης και της αλληλεπίδρασης με άλλους διδασκόμενους. Επίσης, τα μέσα κοινωνικής δικτύωσης μπορούν να δώσουν ευκαιρίες στους μαθητές για την διεύρυνση των οριζόντων τους σε διάφορους τομείς. Επιπλέον, πολλά εκπαιδευτικά ιδρύματα δίνουν τη δυνατότητα να συνδέονται οι φοιτητές μέσω κοινωνικών δικτύων όπως στο Facebook ή το YouTube. Τα μέσα κοινωνικής δικτύωσης μπορούν παράλληλα να βοηθήσουν στην ενημέρωση των φοιτητών για χρήσιμες πληροφορίες. Ταυτόχρονα, μπορούν να προσφέρουν στο κοινό εργαλεία που είναι χρήσιμα για την εξαγωγή δεδομένων, το οποίο μπορεί να γίνει με διάφορες δημοσκοπήσεις ή με κάποια έρευνα, και με αυτό τον τρόπο βοηθάει τους μαθητές να παράγουν χρήσιμο περιεχόμενο για μια έρευνα.

Πολιτική

Ένας άλλος λόγος για την χρήση των κοινωνικών δικτύων αποτελεί η συμμετοχή στα πολιτικά πράγματα. Οι πολιτικοί μπορούν να χρησιμοποιούν τα κοινωνικά δίκτυα για να ενημερώσουν το κοινό τους για το πρόγραμμά τους, τις πολιτικές εκστρατείες τους και να κερδίσουν υποστήριξη από ένα μεγάλο αριθμό ατόμων. Επίσης, μπορούν να διεξαχθούν δημοσκοπήσεις σχετικά με την πολιτική σκηνή, δηλαδή οι πολιτικοί μπορούν να χρησιμοποιούν τα κοινωνικά δίκτυα έτσι ώστε να συλλέξουν απόψεις από τους χρήστες. Τέλος, μπορεί να υπάρξει επικοινωνία μεταξύ του κοινού και των πολιτικών μέσω σχολίων και ερωτήσεων που κάνουν οι χρήστες.

1.12 Τα πλεονεκτήματα και τα μειονεκτήματα της χρήσης των μέσων κοινωνικών δικτύων

Τα κοινωνικά δίκτυα αποτελούν ένα σημαντικό κομμάτι στην καθημερινή ζωή των ανθρώπων τα τελευταία χρόνια. Εκτός από τα πλεονεκτήματα έχει και κάποια μειονεκτήματα.

Πλεονεκτήματα:

α) Επικοινωνία

Τα κοινωνικά δίκτυα δίνουν τη δυνατότητα σύνδεσης των χρηστών και να μπορούν να διατηρούν επαφή με την οικογένειά τους και με τους φίλους τους σε περίπτωση που βρίσκονται μακριά και να ενημερώνονται για την ζωή τους. Επίσης, βοηθούν στην διατήρηση των σχέσεων με παλιούς φίλους και συνεργάτες. Τέλος, δίνεται η ευκαιρία να κάνουν νέες γνωριμίες που έχουν κοινά ενδιαφέροντα.

β) Ενημέρωση

Υπάρχει άμεση πρόσβαση στην ενημέρωση καθώς πολλές φορές τα μέσα κοινωνικής δικτύωσης λειτουργούν ως πλατφόρμες μετάδοσης ειδήσεων. Ο χρήστης μπορεί να ενημερώνεται κατευθείαν για τις τελευταίες εξελίξεις σε όλο τον κόσμο ακολουθώντας διαφορά ειδησεογραφικά μέσα, δημοσιογράφους αλλά και άλλες πηγές και έτσι μπορεί να έχει πολλαπλές οπτικές γωνίες. Σημαντικό είναι το γεγονός ότι η ανταλλαγή

πληροφοριών γίνεται σε πραγματικό χρόνο δηλαδή τη στιγμή που εξελίσσονται τα γεγονότα.

γ) Κοινότητες ίδιων ενδιαφερόντων

Τα κοινωνικά δίκτυα επιτρέπουν στους χρήστες να μπορούν να συμμετέχουν σε ομάδες που έχουν τα ίδια ενδιαφέροντα. Χρήστες μπορούν να ανταλλάζουν γνώμες και εμπειρίες με τα μέλη της κοινότητας ανεξάρτητα από τη γεωγραφική τους τοποθεσία.

δ) Διασκέδαση και ψυχαγωγία

Τα κοινωνικά δίκτυα μπορούν να προσφέρουν στους χρήστες ένα παράθυρο στο οποίο μπορούν να ξεφύγουν από την καθημερινή τους ρουτίνα και να χαλαρώσουν. Υπάρχει μεγάλη ποικιλία στο περιεχόμενο ψυχαγωγίας που προσφέρεται και παράλληλα οι χρήστες μπορούν να ανταλλάζουν βίντεο, εικόνες ή και άλλα ψυχαγωγικά πολυμέσα μαζί με τους φίλους τους. Ταυτόχρονα, υπάρχει η ανάγκη των ατόμων για την δημιουργία σχέσεων με άλλα άτομα που έχουν τα ίδια ενδιαφέροντα, όπως κάποια δραστηριότητα, ένα χόμπι κ.λπ.

ε) Εύρεση εργασίας

Οι χρήστες μέσα από διάφορα κοινωνικά δίκτυα μπορούν να παρουσιάσουν τον εαυτό τους με μορφή μοντέρνου βιογραφικού και έχουν την δυνατότητα για αναζήτηση και εύρεση εργασίας ή συνεργασίας, πάνω στον επαγγελματικό τομέα που τους ενδιαφέρει.

Αντίθετα, η πολύωρη ενασχόληση με τα μέσα κοινωνικής δικτύωσης μπορούν να φέρουν και μια σειρά από αρνητικές συνέπειες:

α) Εθισμός στα κοινωνικά δίκτυα

Ο εθισμός αποτελεί έναν από τους πιο γνωστούς κινδύνους υπέρχρησης των κοινωνικών μέσων. Οι εθισμένοι χρήστες περνούν πολλές ώρες στην καθημερινή τους ζωή στα κοινωνικά δίκτυα που μπορεί να τους οδηγήσει στην παραμέληση των καθημερινών υποχρεώσεων όπως την προσωπική τους φροντίδα. Παράλληλα, επειδή ελαττώνεται ο ελεύθερος χρόνος τους λόγω της πολύωρης χρήσης των κοινωνικών μέσων και ως αποτέλεσμα να απομακρύνονται από κοινωνικές αλληλεπιδράσεις.

β) Απώλεια ιδιωτικότητας

Στα μέσα κοινωνικής δικτύωσης οι χρήστες έχουν τη δυνατότητα να μοιράζονται πληροφορίες, φωτογραφίες, βίντεο και άλλα διάφορα στοιχεία για τη ζωή και τα προσωπικά δεδομένα τους που οδηγεί σε διάφορα κακόβουλα άτομα να τα εκμεταλλευτούν και να προβούν σε εγκληματικές ενέργειες όπως την κλοπή ταυτότητας.

γ) Κυβερνο-εκφοβισμός (Cyberbullying)

Περιλαμβάνει αποστολή προσβλητικών, υβριστικών πολιτικών ή χυδαίων μηνυμάτων ή και σχολίων στα κοινωνικά δίκτυα ή σε άλλες πλατφόρμες και την διάδοση ψευδών πληροφοριών μέσω ψευδών προφίλ στοχεύοντας ένα άτομο ή μια ομάδα. Όλα αυτά προκαλούν σοβαρά προβλήματα στην ψυχική υγεία του θύματος ενώ μέσω των ψευδών προφίλ μπορούν να εξαπατήσουν το θύμα και να διαρρεύσουν προσωπικά δεδομένα όπως φωτογραφίες ή προσωπικές πληροφορίες που έχουν στόχο να εκβιάσουν ή να ταπεινώσουν το θύμα.

δ) Κίνδυνος απάτης και κλοπής ταυτότητας

Πρόκειται για ένα σοβαρό θέμα, καθώς επηρεάζονται εκατομμύρια άτομα καθημερινά. Τα θύματα εξαπατώνται και πολλές φορές αφιερώνουν αμέτρητες ώρες ή χρήματα για να μπορέσουν να ξαναεπαναφέρουν αυτά που έχασαν.

ε) Επιδράσεις στην ψυχική υγεία

Η χρήση των μέσων κοινωνικής δικτύωσης μπορεί να επηρεάσει την ψυχική υγεία, ειδικότερα στους νέους, καθώς η συνεχής σύγκριση της ζωής με την ιδανική ζωή των άλλων στα μέσα κοινωνικής δικτύωσης μπορεί να οδηγήσει στο αίσθημα ανεπάρκειας. Επίσης, οδηγείται στην απομόνωση κάποιος που χρησιμοποιεί υπερβολικά τα κοινωνικά με αποτέλεσμα να παραμελήσει τις κοινωνικές αλληλεπιδράσεις και να απομονωθεί ακόμα περισσότερο από τον κόσμο. Έτσι, εμφανίζεται μια έλλειψη ενδιαφέροντος για τα κοινά και οι εικονικές φιλίες αντικαθιστούν τις πραγματικές με αποτέλεσμα ο χρήστης να ζει σε έναν ψεύτικο κόσμο. Παράλληλα, μπορεί να επηρεάσει τη διάρκεια και την ποιότητα του ύπνου.

στ) Μείωση παραγωγικότητας

Η χρήση των κοινωνικών δικτύων μπορεί να επηρεάσει στην παραγωγικότητα καθώς η συνεχής χρήση τους μπορεί να οδηγήσει στην μείωση της προσοχής και της συγκέντρωσης από εργασιακές ή σχολικές δραστηριότητες. Ταυτόχρονα, η διαρκής ενασχόληση με τα μέσα κοινωνικής δικτύωσης μπορεί να οδηγήσει στην εύκολη απόσπαση της προσοχής και σπατάλης του χρόνου από μια εργασία.

ζ) Διασπορά ψευδών ειδήσεων (Fake news)

Η σκόπιμη μετάδοση ανακριβών και παραπλανητικών πληροφοριών προς στους χρήστες μέσω διαφόρων κοινωνικών δικτύων χρησιμοποιώντας τίτλους που προσελκύουν ακόμα περισσότερους χρήστες. Οι χρήστες έτσι αποκτούν μια λανθασμένη εικόνα στην ενημέρωσή τους και παραπληροφορούνται.

Κεφάλαιο 2: Νομικά θέματα διαδικτύου

Στο δεύτερο κεφάλαιο αναλύονται θέματα σχετικά με την προστασία των προσωπικών δεδομένων, παρουσιάζονται οι νομοθεσίες από διεθνή, ευρωπαϊκό και ελληνικό πλαίσιο. Επίσης αναφέρονται κάποια κακόβουλα λογισμικά και τέλος γίνεται αναφορά σε κάποια παγκόσμια σκάνδαλα που έγιναν στα μέσα κοινωνικής δικτύωσης.

2.1. Θέματα απορρήτου και ασφάλειας

Οι βασικοί στόχοι των μέσων κοινωνικής δικτύωσης είναι να αυξήσουν τους χρήστες τους. Πολλοί χρήστες χρησιμοποιούν διάφορες πλατφόρμες όπως το Facebook, το Instagram και άλλα για να δημοσιεύσουν διάφορα πράγματα για την ζωή τους. Πολλές είναι οι φορές που οι χρήστες μοιράζονται πληροφορίες για τον εαυτό τους αλλά και για την ζωή τους δηλαδή για τα διάφορα μέρη στα οποία συχνάζουν, φωτογραφίες και βίντεο. Ωστόσο, πολλά πράγματα που μοιράζονται είναι ιδιωτικά και δεν θα έπρεπε να δημοσιεύονται καθόλου. Επιπλέον, με την σημερινή τεχνολογία, τα περισσότερα τηλέφωνα αποθηκεύουν δεδομένα τοποθεσίας στις φωτογραφίες που δημοσιεύονται στα κοινωνικά δίκτυα. Η συλλογή αυτών των δεδομένων γίνεται με σκοπό να προσφέρονται στους χρήστες εξατομικευμένες υπηρεσίες αλλά και για εμπορικούς σκοπούς. Παράλληλα, αυτά τα δεδομένα μπορούν να παρέχονται και σε τρίτους με αποτέλεσμα την διαρροή του απορρήτου και, συνεπώς, διάφοροι κακόβουλοι να τα εκμεταλλευτούν και να παραβιάσουν την ιδιωτική ζωή των χρηστών. Το απόρρητο δεδομένων προστατεύει αυτές τις πληροφορίες ώστε να μην υπάρχει καμία κακόβουλη πρόσβαση που να παραβιάζει αυτά τα δεδομένα, τα οποία είναι αποθηκευμένα στο διαδίκτυο. Η προστασία των προσωπικών δεδομένων είναι κάτι απαραίτητο καθώς οι πληροφορίες που μοιράζονται στα κοινωνικά δίκτυα μπορούν να χρησιμοποιηθούν για την παρακολούθηση της δραστηριότητας χρηστών, τη στοχευμένη διαφήμιση ή ακόμα να προκαλέσουν κλοπή ταυτότητας. Γι' αυτό πρέπει να υπάρχουν ρυθμίσεις απορρήτου αλλά και ο έλεγχος προς τις πληροφορίες οι οποίες είναι ασφαλείς να υπάρχουν στα μέσα κοινωνικής δικτύωσης.

2.2. Οι επιπτώσεις των κοινωνικών δικτύων

Η εμφάνιση και η εξάπλωση των κοινωνικών δικτύων τα τελευταία χρόνια έχει αυξηθεί ραγδαία. Ένα από τα πιο γνωστά μέσα κοινωνικής δικτύωσης είναι το Facebook που έχει εξαπλωθεί παντού στον κόσμο. Οι πλατφόρμες κοινωνικών δικτύων, μηχανές αναζήτησης, διάφορες εφαρμογές ανταλλαγής μηνυμάτων καταγράφουν τα προσωπικά μας δεδομένα αλλά και τις προτιμήσεις μας αποκτώντας γνώση σχετικά με τα ενδιαφέροντα μας αλλά και με την ζωή μας όπως συνομιλίες, ασχολίες, ταξίδια, αγορές, ψυχική υγεία αλλά και οικονομικά. Ορισμένες από τις επιπτώσεις που μπορεί να προκαλέσει η υπερβολική χρήση των κοινωνικών δικτύων είναι η απομόνωση που οδηγεί στη μείωση της πραγματικής αλληλεπίδρασης με ανθρώπους δημιουργώντας έτσι το αίσθημα της μοναξιάς. Τα μέσα κοινωνικής δικτύωσης μπορούν να αντικαταστήσουν τις φυσικές αλληλεπιδράσεις με ανθρώπους και να δημιουργήσουν επιφανειακές δηλαδή διαδικτυακές σχέσεις. Παράλληλα, η συνεχής υποβάθμιση της προσωπικής εικόνας δηλαδή η σύγκριση με άλλους στα μέσα κοινωνικής δικτύωσης μπορούν να οδηγήσουν στη σε αυξημένο άγχος αλλά και σε χαμηλή αυτοεκτίμηση. Οι χρήστες συχνά μπορούν να δημοσιεύουν μόνο τις θετικές στιγμές τους και εμπειρίες με αποτέλεσμα να δημιουργούν μια παραπλανητική εικόνα σχετικά με την πραγματική τους ζωή.

2.3. Ιδιωτικότητα

Η ανάπτυξη της τεχνολογίας, αλλά παράλληλα και με την διάδοση των μέσων κοινωνικών δικτύων έχει επηρεάσει την ιδιωτικότητα. Ο όρος της ιδιωτικότητας είναι κάτι αρκετά περίπλοκο και δεν αποτελεί μια σταθερή έννοια. Η πρώτη έννοια προήρθε από τον φιλόσοφο Αριστοτέλη στο δοκίμιο του «Πολιτικά». Ο Alan Westin είχε δηλώσει ότι «κανένας ορισμός της ιδιωτικότητας δεν είναι εφικτός, γιατί τα θέματα της ιδιωτικότητας είναι εκ θεμέλιων ζητήματα αξιών, συμφερόντων και εξουσίας». Στην σημερινή εποχή, σε πολλές χώρες του κόσμου η ιδιωτικότητα ως έννοια αναφέρεται σε πολλούς νόμους περί προστασίας δεδομένων. Ο Fernando Volio Jimenez παρατήρησε «με κάποια έννοια, όλα τα ανθρώπινα δικαιώματα είναι πτυχές του δικαιώματος στην ιδιωτικότητα». Ιδιωτικότητα είναι το δικαίωμα που έχει ο χρήστης να διατηρεί τις προσωπικές του πληροφορίες. Οι περισσότεροι χρήστες μοιράζονται προσωπικές πληροφορίες αλλά αυτό δεν σημαίνει ότι θέλουν να κοινοποιηθούν. Αν και στην

σύγχρονη εποχή παρατηρείται ότι όλο και περισσότεροι αδιαφορούν για την ιδιωτικότητα. Παράλληλα, η δημιουργία διάφορων κοινωνικών μέσων οδήγησε στην ανάγκη για την διεύρυνση της προστασίας ενός ατόμου. Η έννοια της ιδιωτικότητας βρίσκεται σε κάθε τομέα τόσο στον ιδιωτικό όσο και στον δημόσιο. Η ανάπτυξη και η εξέλιξη αυτών των τεχνολογιών δημιούργησε όμως σοβαρά ζητήματα με την ασφάλεια, το απόρρητο και την ιδιωτικότητα. Σύμφωνα με μια πρόσφατη έκθεση της Kaspersky, διατυπώθηκε ότι περισσότεροι από τους μισούς χρήστες που χρησιμοποιούν το διαδίκτυο θεωρούν πως η ιδιωτικότητα είναι κάτι το αδύνατο. Πάρα πολλοί χρήστες αγνοούν τη σοβαρότητα αυτού του προβλήματος και υφίστανται να την υποβαθμίζουν. Υπάρχουν πάρα πολλοί κίνδυνοι παραβίασης του απορρήτου και υπάρχουν πάρα πολλά περιστατικά αυτής της παραβίασης. Όλη αυτή η ανάπτυξη της τεχνολογίας έχει φέρει πολλά προβλήματα στο παρασκήνιο όπως την παράνομη πρόσβαση σε προσωπικές πληροφορίες, την υποκλοπή δεδομένων και εγκληματικές πράξεις που είναι κάποιες από τις παραβιάσεις που συμβαίνουν συχνά.

2.3.1. Παραδείγματα παραβίασης της ιδιωτικότητας

Υπάρχουν πολλά παραδείγματα παραβίασης στα μέσα κοινωνικής δικτύωσης, καθώς αποτελεί ένα συχνό φαινόμενο αφού ο χρήστης για να συνδεθεί χρειάζεται κάποιες απαραίτητες πληροφορίες όπως είναι το όνομα χρήστη, κωδικό πρόσβασης αλλά και κάποιες άλλες δευτερεύοντες πληροφορίες. Τα μέσα κοινωνικής δικτύωσης πέρα από αυτές τις πληροφορίες έχουν πρόσβαση στη διεύθυνση IP που θεωρείται μία από τις ιδιωτικές πληροφορίες των χρηστών. Όλα αυτά μπορούν να μοιραστούν σε τρίτους προκειμένου να προσφέρουν σχετικές διαφημίσεις και υπηρεσίες στους χρήστες που χρησιμοποιούν καθημερινά τα μέσα κοινωνικής δικτύωσης. Ένα άλλο σοβαρό ζήτημα είναι η κοινοποίηση φωτογραφιών. Δηλαδή, κάποιος μπορεί να μην έχει κάποιο προφίλ στα μέσα κοινωνικής δικτύωσης αλλά μπορεί να επισημανθεί σε κάποια φωτογραφία ή ανάρτηση χωρίς την συναίνεση του. Παρόμοια και η δημοσίευση ιδιωτικών συνομιλιών, e-mail, ευαίσθητων πληροφοριών, ιατρικών αποτελεσμάτων, ψυχολογικών πληροφοριών ή και οικονομικών στοιχείων μπορούν να γίνει χωρίς την άδεια του ατόμου από άλλους. Αυτά μπορούν να έχουν αρνητικές επιπτώσεις στην προσωπική και επαγγελματική ζωή τους. Μια άλλη σοβαρή παραβίαση της ιδιωτικότητας αποτελεί το γεγονός ότι παρόλο οι χρήστες έχουν το δικαίωμα να

διαγράψουν δεδομένα και προσωπικές πληροφορίες που διαθέτουν στο προφίλ τους και δεν θέλουν να εμφανίζονται πλέον, τα δεδομένα αυτά παραμένουν στις βάσεις δεδομένων του κοινωνικού δικτύου που χρησιμοποιούν. Οι πληροφορίες αυτές αποθηκεύονται για ένα χρονικό διάστημα ως αντίγραφα ασφαλείας. Τέλος, τα ανεπιθύμητα μηνύματα αποτελούν ένα σοβαρό ζήτημα καθώς μπορεί να μοιάζουν σαν μια τυπική ανάρτηση ή μήνυμα αλλά συνήθως περιέχουν διαφημίσεις ή κακόβουλους συνδέσμους που μπορεί να οδηγήσουν σε κάποιους ιστότοπους ηλεκτρονικού ψαρέματος ή κακόβουλου λογισμικού. Τα ανεπιθύμητα μηνύματα συνήθως μπορεί να προέρχονται από παραβιασμένους λογαριασμούς και spam bots.

2.4. Η έννοια των προσωπικών δεδομένων

Τα προσωπικά δεδομένα είναι πληροφορίες που σχετίζονται με ένα άτομο (όνομα, ηλικία, αριθμός ταυτότητας, οικογενειακή κατάσταση, η εκπαίδευση, το επάγγελμα, η διεύθυνσή κατοικίας κ.λπ.). Γενικά πρόκειται για ευαίσθητες πληροφορίες ενός ατόμου. Το απόρρητο μας προστατεύει και εμποδίζει τις πληροφορίες να γίνονται γνωστές σε άλλα άτομα εκτός από αυτά που συνειδητά επιλέγουμε να δώσουμε τις πληροφορίες. Παράλληλα, τα προσωπικά δεδομένα προστατεύονται από την νομοθεσία σε περίπτωση επεξεργασίας. Οι επιχειρήσεις και οι οργανισμοί πρέπει να διατηρούν την ασφάλεια των προσωπικών δεδομένων των χρηστών τηρώντας τους νόμους και τους κανονισμούς και να αποθηκεύουν τα προσωπικά δεδομένα με ασφάλεια χωρίς να παραβιάζονται τα δικαιώματα των χρηστών. Αν υπάρξει παραβίαση του νόμου, ο παραβάτης τιμωρείται με πρόστιμο ή φυλάκιση. Έτσι, οι οργανισμοί και υπηρεσίες που επεξεργάζονται τα προσωπικά δεδομένα πρέπει να ακολουθούν κάποιους κανόνες για να προστατεύουν την ιδιωτικότητα των χρηστών. Ένα σοβαρό πρόβλημα όμως είναι η προφύλαξη των προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης από τους ίδιους τους χρήστες, καθώς οι περισσότεροι άνθρωποι που χρησιμοποιούν τα κοινωνικά δίκτυα σε καθημερινή βάση μπορούν να δημοσιεύουν προσωπικά δεδομένα όπως φωτογραφίες, βίντεο κ.λπ. Παράλληλα, τα προσωπικά δεδομένα επιτρέπεται να επεξεργαστούν αν τα άτομα που του ανήκουν δώσει συναίνεση. Υπάρχουν, όμως, κάποιες φορές που αυτά τα δεδομένα μπορεί να επεξεργαστούν χωρίς την έγκρισή του ατόμου. Σε αυτή την περίπτωση υπάρχουν πάρα πολλοί κακόβουλοι χρήστες που θα προσπαθήσουν να παραβιάσουν τα προσωπικά δεδομένα χωρίς την έγκρισή του

ατόμου. Σύμφωνα με το άρθρο του νόμου 2472/1997 προσωπικά δεδομένα ορίζονται ως «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.» Οι τιμωρίες για τέτοιες παραβιάσεις ανέρχονται από φυλάκιση και χρηματική ποινή. Επιπλέον, ένα άλλο σοβαρό ζήτημα στην προστασία των προσωπικών δεδομένων είναι ότι οι χρήστες έχουν έλλειψη γνώσης και ενημέρωσης σχετικά με τα κοινωνικά δίκτυα και αφήνουν αυτά τα δεδομένα να είναι διαθέσιμα για ανίχνευση και επεξεργασία, ακόμα και χωρίς να το γνωρίζουν. Συνεπώς, τα προσωπικά δεδομένα πρόκειται για τη κάθε πληροφορία που προσδιορίζει ένα άτομο ωστόσο πρέπει να υπάρχει αρκετή προσοχή διότι αυτά όσον αφορά την ιδιωτική ζωή χαρακτηρίζονται ευαίσθητα δεδομένα και πρέπει να έχουν μεγαλύτερη προστασία. Τα ευαίσθητα δεδομένα πρόκειται κυρίως για τις θρησκευτικές και φιλοσοφικές πεποιθήσεις, την φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, υγεία, την κοινωνική πρόνοια καθώς και σχετικά με ποινικές διώξεις ή καταδίκες. Δηλαδή, έχει να κάνει περισσότερο με όσα αφορούν τον ίδιο τον άνθρωπο στο κοινωνικό και πολιτισμικό πλαίσιο. Για αυτό το λόγο τα προσωπικά δεδομένα είναι είτε απλά είτε ευαίσθητα και πρέπει να προστατεύονται από τη νομοθεσία. Η απώλεια των ψηφιακών δεδομένων αποτελεί ένα από τα βασικότερα ζητήματα για τη σύγχρονη κοινωνία, καθώς έφερε νέες μορφές κινδύνων.

Τα προσωπικά δεδομένα είναι δυνατόν να αποκαλύπτονται.

- Όταν κατά τη περιήγηση στο διαδίκτυο, τα προγράμματα περιήγησης διατηρούν αρχείο καταγραφής των σελίδων που επισκέπτονται.
- Όταν σε διάφορους ιστότοπους αποθηκεύονται cookies (πληροφορίες όπως όνομα χρήστη, στοιχεία εγγραφής, προτιμήσεις για ψώνια κ.λπ).
- Όταν γίνεται εγγραφή σε μια ηλεκτρονική υπηρεσία και μας ζητείται να συμπληρώσουμε προσωπικά δεδομένα.
- Όταν γίνονται δημοσιεύσεις σε διάφορα κοινωνικά δίκτυα όπως φωτογραφίες και βίντεο.
- Όταν χρησιμοποιούμε εφαρμογές για μηνύματα και συμμετέχουμε σε ομαδικές συζητήσεις ή τις δημιουργούμε.

Παραδείγματα προσωπικών δεδομένων είναι

- Όνομα και επώνυμο
- Διεύθυνση κατοικίας
- Ηλεκτρονική διεύθυνση (email)
- Αριθμός τηλεφώνου
- Αναγνωριστικός αριθμός χρεωστικής ή πιστωτικής κάρτας
- Διεύθυνση IP
- Αναγνωριστικά cookies
- κ.λπ.

2.5. Malware – Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό γνωστό ως «malware» προσπαθεί να αποκτήσει πρόσβαση στους υπολογιστές και στα προσωπικά δεδομένα. Η επίθεση του μέσω κοινωνικών δικτύων είναι ευκολότερη σε σχέση με άλλες διαδικτυακές υπηρεσίες εξαιτίας της δομής που έχουν τα μέσα κοινωνικής δικτύωσης αλλά και την αλληλεπίδραση μεταξύ των χρηστών. Καθώς σχεδιάστηκε με σκοπό να προκαλέσει κακό σε έναν υπολογιστή, δίκτυο ή χρήστη, το κακόβουλο λογισμικό όταν εισέλθει μπορεί να κλέψει προσωπικά δεδομένα, να ζητήσει λύτρα (ransomware) κ.λπ.

Υπάρχουν διάφοροι τύποι malware:

- Trojan Horse ή αλλιώς backdoor (δούρειος ίππος):** Είναι ένα είδος κακόβουλο λογισμικού το οποίο μιμείται διάφορα προγράμματα ή αρχεία και περιέχουν κρυμμένο κακόβουλο κώδικα. Ο εισβολέας έχει τη δυνατότητα να διαχειριστεί από απόσταση το σύστημα όποτε αυτός θελήσει και μπορεί να συλλέγει προσωπικά δεδομένα όπως κωδικούς πρόσβασης, πληροφορίες πιστωτικών καρτών και άλλα. Επίσης, μπορεί να παρακολουθήσει τη δραστηριότητα των χρηστών χωρίς αυτοί να έχουν κάποια γνώση σχετικά με αυτό.
- Worm (σκουλήκι):** Είναι ένα κακόβουλο λογισμικό που έχει τη δυνατότητα να πολλαπλασιάζεται δημιουργώντας αντίτυπα του εαυτού του από υπολογιστή σε υπολογιστή. Μετά την επίθεση αυτό έχει

απομακρυσμένο έλεγχο στον υπολογιστή και μπορεί να κλέψει δεδομένα από τον υπολογιστή του θύματος ή και να παρακολουθήσει τις ενέργειες του συλλέγοντας προσωπικά δεδομένα με αυτό τον τρόπο. Έχει την ικανότητα να προσβάλει το δίκτυο με συνέπεια να μειωθεί η ταχύτητα της σύνδεσης στο διαδίκτυο και του υπολογιστή.

- γ) **Ransomware (εξαπόλυση χρημάτων):** Πρόκειται για κακόβουλο λογισμικό που στοχεύει να κρυπτογραφήσει τα δεδομένα του θύματος με σκοπό να ζητήσει λύτρα για να τα ξαναεπαναφέρει. Το χρηματικό ποσό που ζητείται πρέπει να έχει πληρωθεί μέσα στο χρονικό διάστημα που δίνεται αλλιώς σβήνεται το κλειδί κρυπτογράφησης. Όμως, δεν υπάρχει κάποια εγγύηση ότι τα δεδομένα θα αποκρυπτογραφηθούν και ότι δεν θα υπάρξει κίνδυνος μελλοντικής μόλυνσης.
- δ) **Virus (ιός):** Είναι κακόβουλο λογισμικό που έχει την δυνατότητα να εγκατασταθεί σε έναν υπολογιστή και να εξαπλωθεί και σε άλλα αρχεία και να τα μολύνει. Οι συνέπειες που μπορεί να επιφέρει ποικίλλουν από μια απλή εμφάνιση στην οθόνη μέχρι και καταστροφή των προσωπικών δεδομένων και του υπολογιστή. Πρώτη φορά αναπτύχθηκε στο ARPANET στις αρχές της δεκαετίας του 1970 και η διάδοσή του γινόταν μέσω του λειτουργικού TENEX.
- ε) **Rootkit:** Πρόκειται για κακόβουλο λογισμικό που μόλις εγκατασταθεί στον υπολογιστή έχει την δυνατότητα να παραμείνει κρυφό ώστε να μην είναι δυνατή ο εντοπισμός του από τους μηχανισμούς ανίχνευσης αντικών (anti-virus) προγραμμάτων. Στόχος του εισβολέα είναι να έχει τον πλήρη έλεγχο του υπολογιστή.

2.6. Phishing Attacks – Επιθέσεις ηλεκτρονικού

«ψαρέματος»

Το ηλεκτρονικό ψάρεμα αποτελεί ένας ακόμα τρόπος επίθεσης στα μέσα κοινωνικής δικτύωσης όπου ο εισβολέας προσπαθεί να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα στέλνοντας ψεύτικα email και μηνύματα στα μέσα κοινωνικής δικτύωσης. Με αυτό τον τρόπο προσποιούνται ότι είναι από τράπεζες, εταιρίες, διάφορους οργανισμούς με στόχο να ζητήσουν από τους χρήστες προσωπικές πληροφορίες. Έτσι,

εξαπατούν τους ανθρώπους με στόχο την υποκλοπή προσωπικών στοιχείων. Ο εισβολέας μπορεί να δημιουργήσει ψεύτικες ιστοσελίδες που έχουν ομοιότητα με γνωστές ιστοσελίδες, όπως για παράδειγμα τα κοινωνικά δίκτυα και τράπεζες, και να στείλουν e-mail ή μηνύματα που συμπεριλαμβάνουν συνδέσμους που οδηγούν προς αυτές τις ιστοσελίδες. Όταν εισέλθει το θύμα σε μία από αυτές, νομίζοντας ότι είναι αυθεντικές, κατοχυρώνει τα προσωπικά του δεδομένα. Ένας άλλος τρόπος είναι ο εισβολέας στέλνει e-mail με επισυναπτόμενα αρχεία που περιέχουν ένα κακόβουλο λογισμικό. Επίσης, το ηλεκτρονικό ψάρεμα πολλές φορές χρησιμοποιείται για την απόκτηση πρόσβασης σε εταιρικά ή κυβερνητικά δεδομένα. Σε αυτό το σημείο ένας εισβολέας μπορεί να στέλνει χιλιάδες μηνύματα γιατί ακόμα και αν ένα μικρό ποσοστό ανταποκριθεί μπορεί να αποκτήσει χρηματικά ποσά ή και προσωπικές πληροφορίες.

2.7. Cross-Site Scripting – XSS

Το Cross-Site scripting είναι μια μορφή επίθεσης σε εφαρμογές στο διαδίκτυο που δίνει στον εισβολέα την ικανότητα να ενσωματώσει κακόβουλο κώδικα σε ασφαλής ιστοσελίδες ή εφαρμογές και στη συνέχεια να τον φορτώσει το πρόγραμμα περιήγησης ενός χρήστη. Ο κώδικας αυτός αποσκοπεί την μεταφορά ευαίσθητων δεδομένων από τον χρήστη στον εισβολέα. Ο εισβολέας μπορεί επίσης να χρησιμοποιήσει XSS για να στείλει ένα κακόβουλο αρχείο σε ένα χρήστη. Ο εισβολέας μπορεί να κλέψει cookies από τον υπολογιστή του χρήστη αλλάζοντας την ιστοσελίδα και έτσι μπορούν και παρακολουθούν το περιεχόμενο του.

Διακρίνονται σε τρεις βασικές κατηγορίες επιθέσεων: μη μόνιμες (reflected), μόνιμες (stored) και DOM επιθέσεις.

1. Reflected XSS: Είναι ένας κακόβουλος κώδικας ο οποίος δεν αποθηκεύεται στη βάση δεδομένων αλλά αυτός ενσωματώνεται όταν ο χρήστης φορτώνει τη σελίδα.
2. Stored (Persistent) XSS: Ο κακόβουλος κώδικας αποθηκεύεται στη βάση δεδομένων της ιστοσελίδας και κάθε φορά που ο χρήστης φορτώνει την ιστοσελίδα περιέχει μέσα ένα κακόβουλο κώδικα που εκτελείται.
3. DOM-based XSS: Πρόκειται για επιθέσεις που σχετίζονται στο μοντέλο DOM καθώς αναπτύχθηκαν από την δημιουργία Web 2.0 εφαρμογών.

2.8. Τι είναι τα Cookies

Τα cookies είναι μικρά αρχεία κειμένου που αποθηκεύονται από ιστότοπους στον υπολογιστή μας όταν τους επισκεπτόμαστε. Τις περισσότερες φορές η πληροφορία είναι κωδικοποιημένες και έχουν τη μορφή ID. Από μόνα τους είναι ακίνδυνα και εξυπηρετούν κρίσιμες λειτουργίες για ιστότοπους, όπως την σύνδεση σε ένα λογαριασμό. Παρ' όλα αυτά, τα cookies μπορούν να αποθηκεύσουν απεριόριστα δεδομένα και αποτελούν μια σημαντική βάση που χρησιμοποιούν οι διαφημιζόμενοι για να μπορούν να παρακολουθούν τις διαδικτυακές δραστηριότητες των χρηστών έτσι ώστε να στοχεύουν τους χρήστες και να τους εξατομικεύουν τις διαφημίσεις. Υπάρχουν διαφορετικά είδη cookies, καθώς χωρίζεται με βάση τη λειτουργικότητα που προσφέρουν. Τα cookies στα κοινωνικά μέσα αποτελούν μικρά κομμάτια πληροφοριών που αποθηκεύονται από έναν ιστότοπο κοινωνική δικτύωσης στα δεδομένα του φυλλομετρητή (internet browser) που χρησιμοποιούμε. Ο βασικός τους στόχος είναι να βοηθήσουν τους ιστότοπους κοινωνικής δικτύωσης να βελτιωθούν και να παρέχουν εξατομικευμένο περιεχόμενο. Τα cookies διακρίνονται σε διαφορετικά είδη ανάλογα με τη λειτουργία τους.

- Τα απλά cookies χρησιμοποιούνται για την αποθήκευση γενικών πληροφοριών. Χρησιμοποιούνται κυρίως στα ηλεκτρονικά καταστήματα και χρησιμεύουν στο να θυμούνται τα προϊόντα που ένας καταναλωτής έχει ήδη επιλέξει για να αγοράσει. Αλλά έχει και κάποιες άλλες χρήσεις όπως πόσες φορές έχουμε επισκεφτεί μια ιστοσελίδα, ποια γλώσσα χρησιμοποιούμε κ.λπ.
- **Session** Cookies: Είναι γνωστά ως προσωρινά cookies και λειτουργούν μόνο όταν ένας χρήστης είναι ενεργός ή συνδεδεμένος με λογαριασμό σε έναν ιστότοπο. Δίνουν τη δυνατότητα στους χρήστες να περιηγούνται σε ιστοσελίδες χωρίς να συμπληρώνουν συνέχεια τις ίδιες πληροφορίες.
- **Tracking** cookies: Ο βασικός του στόχος είναι η βελτίωση υπηρεσιών που μπορεί να προσφέρει μια ιστοσελίδα. Αυτά τα cookies ακολουθούν την διαδικτυακή συμπεριφορά του χρήστη συλλέγουμε τα δεδομένα του. Ταυτόχρονα, άλλα tracking cookies μπορούν να έχουν στόχο την εξατομικευμένη διαφήμιση στους χρήστες και γι' αυτό συγχέονται πολλές φορές.

2.9. Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Τα προσωπικά δεδομένα που έχουν να κάνουν με ένα φυσικό πρόσωπο υπόκεινται σε επεξεργασία σύμφωνα με την Οδηγία 95/46/ΕΚ, σε κάθε επεξεργασία που έχει να κάνει με ένα φυσικό πρόσωπο. Τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα.

2.10. Νομοθεσίες και Πολιτικές Προστασίας (Διεθνές και Ευρωπαϊκό Δίκαιο)

2.10.1. Ευρωπαϊκή Νομοθεσία

Στην Ευρώπη δημιουργήθηκαν οι πρώτοι κανονισμοί για τα προσωπικά δικαιώματα αρκετά νωρίς. Η Ευρωπαϊκή Ένωση παρατήρησε κάποιες αδυναμίες σχετικά με την πνευματική ιδιοκτησία και την προστασία των ανθρωπίνων δικαιωμάτων και γι' αυτό διατύπωσε τη Σύμβαση της Ρώμης της 4ης Νοεμβρίου του 1950. Στο άρθρο 8 αναφέρεται η ανάγκη για την **Προστασία των Δικαιωμάτων του Ανθρώπου** και των θεμελιωδών ελευθεριών, όπως στο δικαίωμα κάθε ανθρώπου να μην παραβιάζεται η προσωπική του ζωή και να γίνεται σεβαστή η οικογενειακή και ιδιωτική του ζωή. Εκτός από αυτό, η συνθήκη αφορά και τις υπηρεσίες και τα εμπορεύματα που περιέχουν πνευματική ιδιοκτησία. Γνωστή και ως **Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ)**. Το πρώτο σημαντικό ορόσημο για την προστασία των προσωπικών δεδομένων κείμενο αποτέλεσε η κοινοτική Οδηγία 95/46/ΕΚ της Ευρωπαϊκής Ένωσης. Αποτελεί σημείο αναφοράς σε όλη την Ευρωπαϊκή Ένωση (ΕΕ) και ο στόχος της είναι προστασία των φυσικών προσώπων όσο αφορά την επεξεργασία προσωπικών δεδομένων αλλά και την ελεύθερη κυκλοφορία αυτών των δεδομένων εντός της Ευρωπαϊκής Ένωσης. Η οδηγία μπήκε σε εφαρμογή στις 24 Οκτωβρίου του 1995 και ο σκοπός της ήταν να εφαρμόζει κείμενο αναφοράς σε θέματα που είχαν να κάνουν με προστασία δεδομένων προσωπικού χαρακτήρα. Η οδηγία εφαρμόζεται στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας με αυτοματοποιημένες διαδικασίες. Δεν εφαρμόζεται στην επεξεργασία δεδομένων τα οποία πραγματοποιούνται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων, η οποία πραγματοποιείται για την άσκηση δραστηριοτήτων που δεν διέπονται από το κοινοτικό δίκαιο, όπως την δημόσια ασφάλεια, την άμυνα ή

την ασφάλεια του κράτους. Στη συνέχεια θεσπίστηκε μια άλλη οδηγία 97/66/EK για την προστασία του άτομο από την επεξεργασία δεδομένων προσωπικού χαρακτήρα της ιδιωτικής ζωής από την ανάπτυξη της ηλεκτρονικής επικοινωνίας. Ωστόσο η οδηγία 2002/58/EK αντικατέστησε την προηγούμενη σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η οδηγία αυτήν έχει περισσότερο σχέση για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Αυτή η οδηγία είναι γνωστή και με την ονομασία «*e-privacy*». Στην συνέχεια τροποποιήθηκε από την Οδηγία 2006/24, η οποία ορίζει ένα χρονικό διάστημα διατήρησης προσωπικών δεδομένων από τους πάροχους. Μετά από την λήξη αυτό του χρονικού διαστήματος (6-24 μήνες), κάθε πάροχος που διαθέτει αυτά τα δεδομένα πρέπει να τα διαγράψει. Στις 25 Μαΐου 2018 τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR) 2016/679, 2 χρόνια αφότου η ΕΕ δεσμεύτηκε για σημαντική μεταρρύθμιση του πλαισίου προστασίας δεδομένων. Ο κανονισμός αντικατέστησε την οδηγία 95/46/EK που είχε ισχύ για 20 χρόνια και παρείχε νέα δικαιώματα σχετικά με την επεξεργασία των προσωπικών δεδομένων και την εύρυθμη λειτουργία της ενιαίας αγοράς. Όσοι είναι μέλη της Ευρωπαϊκής Ένωσης μπορούν να έχουν πληροφορίες σχετικά με το ποιος μπορεί να επεξεργαστεί τα δεδομένα τους, να έχουν πρόσβαση στα δεδομένα τα οποία συλλέγονται και μπορούν να κάνουν αίτηση να διαγραφούν τα δεδομένα τους ολοκληρωτικά. Επιπλέον, μπορούν να ζητήσουν διόρθωση σε δεδομένα που είναι λάθος.

Η ανάπτυξη της τεχνολογίας τα τελευταία χρόνια οδήγησε στην ανάγκη για την προστασία των προσωπικών δεδομένων καθώς τα ανθρώπινα δικαιώματα είναι εκτιμημένα μπροστά σε πολλούς κινδύνους. Ο **Οργανισμός Ηνωμένων Εθνών** (Ο.Η.Ε.) αποτελεί ο θεμελιωτής για τα δικαιώματα των ατόμων στην ιδιωτικότητα. Στόχος του είναι να προσπαθήσει να κάνει την σωστή προώθηση των κοινών αξιών των ανθρώπων και σχετίζονται με τις ελευθερίες και τα δικαιώματα μέσα στον ψηφιακό κόσμο.

2.10.2. Ελληνικό πλαίσιο

Η Ελλάδα αποτέλεσε μια από τις πρώτες χώρες που είχε συνειδητοποιήσει την αξία της προστασίας των προσωπικών δεδομένων. Ο νόμος 2472/1997 κατοχύρωσε την

προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και εγκρίθηκε με σκοπό την εφαρμογή της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ. Αποτελέσε σημαντικό νομικό πλαίσιο για την προστασία της ιδιωτικότητας των προσωπικών δεδομένων. Ο νόμος αυτός σχετίζεται με τους κανόνες που υπάρχουν στην συλλογή και επεξεργασία προσωπικών δεδομένων. Το 2001, μετά την αναθεώρηση του συντάγματος, προστέθηκε στο άρθρο 9, σύμφωνα με τον νόμο 2472/97 (ΦΕΚ Α΄ 50/10.04.1997), του Συντάγματος, το άρθρο 9Α που αναφέρεται στη προστασία των προσωπικών δεδομένων του ατόμου από παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα και στη συνέχεια περιλαμβάνεται η προστασία προσωπικών δεδομένων και απόρρητου στο πεδίο των ηλεκτρονικών επικοινωνιών. Αργότερα, υπήρξαν κάποιες τροποποιήσεις στο νόμο 3471/06 (ΦΕΚ Α΄ 133/28.06.2006) κατοχυρώνοντας το δικαίωμα του ατόμου στην προστασία από την επεξεργασία των δεδομένων του και τη συλλογή τους σε ότι έχει να κάνει με τα ηλεκτρονικά μέσα. Επιπλέον, υπήρξε για πρώτη φορά το δικαίωμα της πληροφόρησης. Πρόκειται για το δικαίωμα που έχει ένα άτομο να μπορεί να ελέγχει αλλά και να αποφασίζει ποια προσωπικά δεδομένα πρέπει να συλλέγονται και να επεξεργάζονται για οποιονδήποτε λόγο. Η νομοθεσία άλλαξε πάλι με τον νέο νόμο 4624/2019 στα πλαίσια του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (2016/679) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016.

Ποινικές κυρώσεις που μπορεί να επιφέρει η μη τήρηση του νόμου στην Ελλάδα σύμφωνα με το **άρθρο 38 του Ν. 4624/2019** θεσπίζονται οι εξής **ποινικές κυρώσεις**:

1. Όποιος, χωρίς δικαίωμα:
 - α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών·
 - β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει,

τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη. Όποιος έχει πάρει, χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει κ,λπ. τιμωρείται με φυλάκιση.

2. Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση α' της παραγράφου 1 ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών, τιμωρείται με φυλάκιση, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.
3. Εάν η πράξη της παραγράφου 2 αφορά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα του άρθρου 9 παράγραφος 1 του ΓΚΠΔ ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή τα σχετικά με αυτά μέτρα ασφαλείας του άρθρου 10 του ΓΚΠΔ, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.
4. Με κάθειρξη μέχρι δέκα (10) ετών τιμωρείται ο υπαίτιος των πράξεων των προηγούμενων παραγράφων, εάν είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον ή να βλάψει άλλον και το συνολικό όφελος ή η συνολική ζημία υπερβαίνει το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ.
5. Εάν από τις πράξεις των παραγράφων 1 έως και 3 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή έως τριακόσιες χιλιάδες (300.000) ευρώ.
6. Τα κακούργηματα που προβλέπονται στο παρόν άρθρο υπάγονται στην αρμοδιότητα του Τριμελούς Εφετείου Κακούρημάτων.

2.10.3. Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (2016/679) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (GDPR)

Τον Ιανουάριο του 2012 η Ευρωπαϊκή Επιτροπή πρότεινε μέτρα σχετικά με την μεταρρύθμιση της προστασίας των προσωπικών δεδομένων κρίνοντας απαραίτητο την ανάγκη να εκσυγχρονισθούν εξαιτίας της ανάπτυξης της τεχνολογίας. Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (679/2016) ή «*General Data Protection Regulation*» (GDPR) της 27 Απριλίου του 2016 με τον οποίο το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο της Ευρωπαϊκής Ένωσης και η Ευρωπαϊκή Επιτροπή ενισχύουν την προστασία δεδομένων για όλους εντός Ευρωπαϊκής Ένωσης. Ο σκοπός του κανονισμού είναι να προστατεύει τα φυσικά πρόσωπα όταν τα δεδομένα τους υπόκεινται σε επεξεργασία από τον ιδιωτικό τομέα και από το μεγαλύτερο μέρος του δημόσιου τομέα. Τα 99 νομικά άρθρα του κανονισμού αποσκοπούν στην ενίσχυση της νομοθεσίας για την προστασία των προσωπικών δεδομένων δίνοντας έτσι στους πολίτες της ΕΕ τον έλεγχο των προσωπικών τους δεδομένων, ενώ τονίζουν τις ιδέες της ελευθερίας, της ασφάλειας και της ισότητας εντός της Ευρωπαϊκής Ένωσης. Ο κανονισμός εφαρμόστηκε στις 25 Μαΐου του 2018. Βασικές αρχές που περιλαμβάνει το GDPR είναι η νομιμότητα, η περιορισμένη συλλογή δεδομένων, ο περιορισμός αποθήκευσης αλλά και της επεξεργασίας. Ο κανονισμός έχει επίδραση σε όλους τους οργανισμούς που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα από πολίτες της Ευρωπαϊκής Ένωσης.

Μερικοί από τους ορισμούς του κανονισμού: (σύμφωνα με το άρθρο 4 ΓΚΠΔ)

1. «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,
2. «επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση

- με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή,
3. «περιορισμός της επεξεργασίας»: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον,
 4. «κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

Σύμφωνα με τους παραπάνω ορισμούς, η επεξεργασία πρόκειται για μια δυνατότητα μπορεί να γίνει είτε από τον άνθρωπο είτε μέσω μηχανών αυτόματα αποκτώντας πρόσβαση στα προσωπικά δεδομένα των χρηστών και με αυτό τον τρόπο να γίνεται η συλλογή δεδομένων.

2.10.4. Νομοθεσία στις Ηνωμένες Πολιτείες της Αμερικής

Το **CLOUD Act** ή «*Clarifying Lawful Overseas Use of Data Act*» θεσπίστηκε το 2018, δύο μήνες πριν εφαρμοστεί το GDPR. Ο συγκεκριμένος νόμος αντικατάστησε τον νόμο του 1986 «*Stored Communications Act*» (SCA). Ο νόμος αυτός τέθηκε για να επιτρέψει στις **Ομοσπονδιακές Αρχές**, με ένταλμα, να συλλέξουν δεδομένα χρηστών εφόσον δεν επηρεάζεται το απόρρητο χρηστών σε άλλες χώρες. Δηλαδή, αν τα δεδομένα ενός χρήστη, ακόμα και πολίτη των Ηνωμένων Πολιτειών της Αμερικής, βρίσκονται σε διακομιστή σε χώρα εκτός των Ηνωμένων Πολιτειών της Αμερικής τότε οι εταιρείες δεδομένων και επικοινωνιών έχουν το δικαίωμα αρνηθούν ένα τέτοιο αίτημα.

Στην πολιτεία της Καλιφόρνια, το 2018, θεσπίστηκε ο νόμος περί απορρήτου των καταναλωτών της Καλιφόρνιας ή «*California Consumer Privacy Act*» (CCPA) και τέθηκε σε ισχύ το 2020. Ο στόχος του είναι η ενίσχυση των δικαιωμάτων απόρρητου και οι προστασία των πολιτών της Καλιφόρνιας. Ο συγκεκριμένος νόμος έχει πολλά κοινά χαρακτηριστικά με τον GDPR της Ευρωπαϊκής Ένωσης αλλά ο CCPA στοχεύει

μόνο στα προσωπικά δεδομένα που οι ίδιοι οι χρήστες ανεβάζουν στα μέσα κοινωνικών δικτύων. Συνοπτικά, οι καταναλωτές έχουν το δικαίωμα να γνωρίζουν ποιες κατηγορίες των προσωπικών δεδομένων συλλέγονται και αν αποκαλύπτονται ή πωλούνται σε τρίτους, το δικαίωμα να ζητήσουν από μια επιχείρηση να διαγράψουν προσωπικές πληροφορίες σχετικά με αυτούς (Όμοια με το άρθρο 17 ή «δικαίωμα στην λήθη» του GDPR»).

2.11. Τι είναι το απόρρητο στο Διαδίκτυο;

Το απόρρητο στο διαδίκτυο είναι ένας όρος που αναφέρεται στην προστασία των πληροφοριών γενικά σε ότι σχετίζεται ιδιωτικές. Είναι η ικανότητα να ελέγχονται ποιες πληροφορίες μπορούμε να αποκαλύψουμε για τον εαυτό μας και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες. Σχεδόν πάντα στο διαδίκτυο υπάρχουν πολλές πληροφορίες σχετικά με τους χρήστες. Τα μη κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να διαβαστούν από τους διαχειριστές του διακομιστή ηλεκτρονικού ταχυδρομείου εάν η σύνδεση δεν είναι κρυπτογραφημένη, ο πάροχος υπηρεσιών διαδικτύου μπορεί να δει κάθε κίνηση της σύνδεσης στο διαδίκτυο (περιήγησή στο διαδίκτυο, ανταλλαγή μηνυμάτων κ.λπ.) και άλλες περιπτώσεις. Οι περισσότεροι χρήστες που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης θέλουν να νιώθουν ασφάλεια για τα προσωπικά τους δεδομένα χωρίς να ανησυχούν μήπως κοινοποιηθούν χωρίς την άδειά τους. Οι χρήστες των μέσων κοινωνικής δικτύωσης πρέπει να προσέχουν την συλλογή των προσωπικών τους δεδομένων. Καθώς ορισμένες πληροφορίες καταγράφονται χωρίς να υπάρχει γνώση ή κάποια συγκατάθεση από τους ίδιους τους χρήστες. Τα δεδομένα μπορεί να συλλέγονται για σκοπούς επιβολής του νόμου και για κυβερνητικούς σκοπούς. Αλλά μπορεί και να συλλέγονται από τρίτους. Όταν οι χρήστες κοινοποιούν πληροφορίες στα κοινωνικά δίκτυα, αυτές παύουν να είναι απόρρητες. Ο αυξανόμενος όγκος προσωπικού περιεχομένου στο διαδίκτυο εκθέτει τους χρήστες σε ένα πρόβλημα απορρήτου που προκαλεί ανησυχίες. Η εμφάνιση ψηφιακών φωτογραφικών μηχανών, η δημιουργία έξυπνων τηλεφώνων που μπορούν να ανεβάσουν περιεχόμενο στο διαδίκτυο έχει κάνει τη διάδοση και συλλογή προσωπικών πληροφοριών όλο και ευκολότερο. Ένα άλλο σημαντικό θέμα είναι τα κοινωνικά δίκτυα καθιστούν δυνατή την χρήση συστήματος εντοπισμού θέσης (GPS) που παρακολουθεί την τοποθεσία του χρήστη. Χωρίς το απόρρητο θα είμασταν

ευάλωτοι στο διαδίκτυο, δεν θα υπήρχε ελευθερία. Γι' αυτό πρέπει να υπάρχει προστασία ώστε να αποφευχθεί η κατάχρηση πληροφοριών από διάφορους οργανισμούς ή ακόμα και χρήστες που προσπαθούν να παραβιάσουν την ιδιωτικότητα άλλων χρηστών. Η νομοθεσία διαφέρει ανάλογα από χώρα σε χώρα. Επομένως, θα πρέπει να είμαστε προσεκτική σχετικά με τις προσωπικές πληροφορίες που ανεβάζουμε σε διάφορες ιστοσελίδες στο διαδίκτυο.

2.12. Βασικοί κίνδυνοι που απειλούν το απόρρητο

Αρχικά, τα μέσα κοινωνικής ζωής αποτελούν έναν τρόπο ανταλλαγής ιδεών και απόψεων καθώς και τη δυνατότητα επικοινωνίας την δημιουργία φίλων αλλά και την εύρεση παλαιότερων που είχαν χαθεί. Ωστόσο, υπάρχουν κάποιοι βασικοί κίνδυνοι οι οποίοι κρύβονται στις ιστοσελίδες των κοινωνικών δικτύων. Επίκεντρο έχουν να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες των χρηστών στα μέσα κοινωνικής δικτύωσης.

α) Ψεύτικα προφίλ

Ένα βασικό πρόβλημα που έχουν όλα τα κοινωνικά δίκτυα είναι τα ψεύτικα προφίλ. Σε αυτή την περίπτωση, ένας εισβολέας μπορεί να δημιουργήσει ένα ψεύτικο λογαριασμό σε κάποιο κοινωνικό δίκτυο με ψεύτικα στοιχεία και να στέλνει μηνύματα σε διάφορους χρήστες, να τους κάνει αιτήματα φιλίας και να στέλνει ανεπιθύμητα μηνύματα. Συνήθως, τα ψεύτικα προφίλ είναι αυτοματοποιημένα ή μη-αυτόματα και πολλές φορές παριστάνουν έναν άνθρωπο. Ο βασικός στόχος που έχουν τα ψεύτικα προφίλ είναι η συλλογή προσωπικών πληροφοριών των χρηστών.

β) Click-jacking

Πρόκειται για μια κακόβουλη τεχνική που έχει στόχο να κάνει τους διαδικτυακούς χρήστες να κάνουν κλικ σε κάτι το οποίο δεν είναι το ίδιο με αυτό που σκόπευαν να κάνουν το κλικ. Σε αυτή την περίπτωση, ο εισβολέας έχει τη δυνατότητα να χειραγωγήσει τους χρήστες των μέσων κοινωνικής δικτύωσης και μπορεί να δημοσιεύσει ανεπιθύμητες αναρτήσεις. Επίσης, μπορεί να αποκτήσει πρόσβαση και στο υλικό των υπολογιστών των χρηστών ώστε, για παράδειγμα, να έχει πρόσβαση στο μικρόφωνο ή στη κάμερα και έτσι να του δίνεται η δυνατότητα να καταγράφει τις

δραστηριότητες το χρηστών. Για να πραγματοποιηθεί μια τέτοια επίθεση μπορεί ο επιτιθέμενος να δημιουργήσει μια διαφανή στρώση πάνω σε μια ιστοσελίδα κρύβοντας με αυτό το τρόπο το πραγματικό περιεχόμενο και στη συνέχεια τοποθετεί πάνω σε αυτή τη στρώση το περιεχόμενο που θέλει ο χρήστης να κάνει το κλικ. Ο χρήστης κάνοντας κλικ στο περιεχόμενο αυτό μπορεί να έχει διάφορες επιπτώσεις όπως επικίνδυνες ενέργειες π.χ. κλοπή προσωπικών πληροφοριών.

γ) Κλοπή ταυτότητας (Identity theft)

Η κλωνοποίηση προφίλ μπορεί να πραγματοποιηθεί από τον εισβολέα ο οποίος έχει κλέψει στοιχεία από έναν ήδη υπάρχον χρήστη δημιουργώντας έτσι ένα ψεύτικο προφίλ με τα στοιχεία που έχει κλέψει. Τα κλεμμένα αυτά στοιχεία μπορούν να χρησιμοποιηθούν σε διάφορα είδη κοινωνικών δικτύων για να κερδίσει την εμπιστοσύνη άλλων χρηστών και να συλλέξει περιεχόμενο από άλλους χρήστες ή να πραγματοποιήσει διάφορες διαδικτυακές απάτες.

δ) Information Leakage

Τα μέσα κοινωνικής δικτύωσης αποτελούν μια καθημερινή χρήση για τους χρήστες και μοιράζονται μερικά από τα προσωπικά τους στοιχεία. Ωστόσο, κάποιοι μοιράζουν τα προσωπικά τους δεδομένα σε υπερβολικό βαθμό. Η κοινή χρήση τέτοιου ευαίσθητου ιδιωτικού περιεχομένου μπορεί να έχει σοβαρές επιπτώσεις στους χρήστες που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης.

2.13. Τεχνολογίες ενίσχυσης της ιδιωτικότητας και προστασίας

Καθώς η τεχνολογία εξελίσσεται το απόρρητο γίνεται ολοένα και πιο σημαντικό ειδικά όταν γίνεται συλλογή ευαίσθητων δεδομένων διότι οι οργανισμοί συλλέγουν και χρησιμοποιούν όλο και περισσότερα δεδομένα και με περισσότερους τρόπους. Για να δημιουργηθεί μια ισορροπία στην ιδιωτικότητα περιλαμβάνεται ένα σύνολο τεχνολογιών που έχουν στόχο την προστασία των προσωπικών δεδομένων. (Privacy-enhancing technologies)

Στόχοι των (PET):

Ο βασικός στόχος των PET είναι η προστασία προσωπικών δεδομένων αλλά και η προστασία του απορρήτου των χρηστών. Έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να αποτρέπουν κάθε είδους διαρροές δεδομένων και να μπορούν να διασφαλίσουν το απόρρητο. Εμποδίζουν τη συλλογή δεδομένων αν υπάρχει κάποια διαρροή. Παράλληλα, υπάρχουν και άλλα PET που αποτρέπουν δαπανηρές παρεμβάσεις δεδομένων μέσω κρυπτογραφικής προστασίας δεδομένων.

Transport Layer Security (TLS) / SSL (Secure Socket Layer)

Είναι κρυπτογραφικά πρωτόκολλα που ο βασικός τους στόχος είναι να διασφαλίσουν την ασφάλεια επικοινωνιών μέσω ενός δικτύου υπολογιστών. Το TLS χρησιμοποιείται κυρίως σε εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο και την ανταλλαγή άμεσων μηνυμάτων. Το πρωτόκολλο SSL σχεδιάστηκε από την Netscape με στόχο την ασφάλεια προσωπικών δεδομένων όταν γίνονται ηλεκτρονικές αγορές και συναλλαγές χρημάτων.

Εικονικό ιδιωτικό δίκτυο (Virtual Private Network)

Πρόκειται για ένα δίκτυο στο οποίο ο χρήστης συνδέεται απομακρυσμένα από τον υπολογιστή του. Η επικοινωνία μέσω αυτού κρυπτογραφείται και έτσι όχι μόνο προστατεύονται προσωπικά δεδομένα αλλά και η πραγματική διεύθυνση IP του χρήστη.

Onion routing

Πρόκειται για ένα σύστημα επικοινωνίας όπου ανάμεσα στον χρήστη και στον τελικό προορισμό υπάρχουν ενδιάμεσοι κόμβοι (relays). Τα δεδομένα κρυπτογραφούνται σε κάθε κόμβο και έτσι δυσκολεύεται η αναγνώριση του περιεχόμενου που μεταδίδεται.

2.14. Σκάνδαλα παραβίασης προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης αποτελούν έναν τρόπο επικοινωνίας και ενημέρωσης εκατομμυρίων ατόμων από όλο τον κόσμο. Καθημερινά όλο και περισσότερα άτομα χρησιμοποιούν το διαδίκτυο προσθέτοντας έτσι τα προσωπικά τους στοιχεία. Κάποια

από τα μεγαλύτερα σκάνδαλα που έχουν δημιουργηθεί στα μέσα κοινωνικής δικτύωσης είναι:

2.14.1. Σκάνδαλο παραβίασης προσωπικών δεδομένων Facebook - Cambridge Analytica

Η Cambridge Analytica είναι μια βρετανική εταιρεία ανάλυσης δεδομένων η οποία δραστηριοποιούνταν στον στρατηγικό σχεδιασμό εκλογικών εκστρατειών. Στις 17 Μαρτίου του 2018 ξέσπασε το σκάνδαλο μεταξύ του Facebook και της Cambridge Analytica και δημιούργησε μεγάλη ανησυχία σε όλο τον κόσμο όταν το Facebook επέτρεψε στην αγγλική εταιρεία ανάλυσης δεδομένων να επεξεργαστεί τα προσωπικά δεδομένα 50 εκατομμυρίων χρηστών χωρίς την έγκρισή τους. Ο Aleksandr Kogan ένας επιστήμονας δεδομένων στο πανεπιστήμιο του Cambridge είχε λάβει την άδεια να αντλήσει τα δεδομένα των χρηστών και ανάπτυξε μια δημοσκόπηση που ονομάζεται «this is your digital life». Χρησιμοποίησε μια εταιρεία που ονομάζεται GSR (Global Science Research) για να δημιουργήσει μια συνεργασία με την SCL Elections Ltd. Το σκάνδαλο έγινε γνωστό όταν ανακαλύφθηκε ότι η Cambridge Analytica είχε πρόσβαση στα προσωπικά δεδομένα εκατομμυρίων χρηστών στο Facebook χωρίς την συναίνεσή τους. Ωστόσο, η Cambridge Analytica έχει ξαναπαραβιάσει δεδομένα 50 εκατομμυρίων χρηστών στις εκλογές των Ηνωμένων Πολιτειών της Αμερικής το 2016 αλλά και για την ψηφοφορία σχετικά με το Brexit στο Ηνωμένο Βασίλειο. Στις 10 Απριλίου, ο Mark Zuckerberg κλήθηκε σε ακρόαση από την δικαστική γερούσια και την επιτροπή εμπορίου όπου η παρουσία του είχε διάρκεια δύο ημέρες. Δήλωσε πως το προσωπικό της εταιρείας εργάζεται στο να αναγνωρίσει πως δημιουργήθηκε το ζήτημα προσωπικών δεδομένων αλλά και πως να προστατεύσει εκατομμύρια χρήστες καθημερινά.

Ενέργειες του Facebook

Όλο αυτό το σκάνδαλο οδήγησε το Facebook να πάρει δραστικές αποφάσεις το 2014. Αποφάσισε να αλλάξει ολόκληρη την πλατφόρμα για να αποφευχθεί η πρόσβαση των εφαρμογών σε δεδομένα. Το Facebook απαγόρευσε σε τέτοιες εφαρμογές να συλλέγουν δεδομένα χωρίς να έχουν κάποια εξουσιοδότηση. Παράλληλα, πρέπει να υπάρχει έγκριση από το ίδιο το Facebook στους προγραμματιστές όταν πρόκειται να ζητηθούν

ευαίσθητα δεδομένα για τους χρήστες. Το Meta Platforms, Inc (πρώην Facebook Inc.), το 2018, ανακάλυψε ότι τα δεδομένα δεν διαγράφηκαν τελικά και για αυτό το λόγο απαγόρευσε και στις δύο εταιρίες τις υπηρεσίες του. Σε αυτό το σημείο το Facebook τόνισε πως θα λάβει ορισμένα μέτρα για να κάνει την πλατφόρμα πιο ασφαλή. Αρχικά, υπήρξε διερεύνηση όλων των εφαρμογών που είχαν πρόσβαση σε μεγάλο αριθμό δεδομένων. Το 2014, ενίσχυσαν τον έλεγχο διαφόρων περιεργων δραστηριοτήτων αλλά και απόκλεισαν προγραμματιστές που δεν συμμορφώνονται στον πλήρη έλεγχο. Επίσης, περιόρισε τα προσωπικά στοιχεία που οι χρήστες δίνουν κατά τη σύνδεση τους.

2.14.2. Σκάνδαλο παραβίασης προσωπικών δεδομένων Yahoo!

Το Σεπτέμβριο του 2016, το Yahoo! αποκάλυψε ότι το 2014 προσβλήθηκε πιθανόν από hacker με συνέπεια την παραβίαση προσωπικών δεδομένων των χρηστών. Στην πρώτη δήλωση, η εταιρεία ανακοίνωσε ότι η επίθεση επηρέασε 500 εκατομμύρια χρήστες και πως εκτέθηκαν ονόματα e-mail, ημερομηνιών γέννησης και αριθμούς τηλεφώνου. Ωστόσο για να καθησυχάσει το κοινό τους, ενημέρωσε πως οι κωδικοί είχαν προστατευτεί μέσω χρήσης του αλγόριθμου bcrypt. Τρεις μήνες μετά, η εταιρεία ανακοίνωσε ότι το 2013 μια άλλη ομάδα hacker κατάφερε να εξασφαλίσει πρόσβαση στα δεδομένα ενός δισεκατομμυρίου χρηστών αλλά αυτή τη φορά δεν περιλάμβανε μόνο ονόματα ή ημερομηνίες γέννησης αλλά και κωδικούς πρόσβασης και ερωτήσεις ασφαλείας των χρηστών με τις αντίστοιχες απαντήσεις. Πάλι, το 2017, η εταιρεία παραδέχτηκε ότι οι hacker στην ουσία είχαν πρόσβαση σε δεδομένα 3 δισεκατομμυρίων χρηστών. Εκείνη την περίοδο το Yahoo! βρισκόταν σε διαπραγματεύσεις με την Verizon, η οποία ήθελε να το αγοράσει και αυτό οδήγησε στην μείωση της αξίας του Yahoo! κατά 350 εκατομμύρια δολάρια.

2.14.3. Σκάνδαλο παραβίασης προσωπικών δεδομένων «iPhone tracking»

Ένα άλλο γνωστό σκάνδαλο είναι το «iPhone tracking» πρόκειται για την συλλογή δεδομένων και την χρήση προσωπικών δεδομένων από την Apple στα iPhone και iOS συσκευές. Υπήρξαν κάποιες ανησυχίες όσον αφορά τον τρόπο με τον οποίο συλλέγονται τα προσωπικά δεδομένα και αποθηκεύονται. Όλα αυτά οδήγησαν τον Steve Jobs να ζητήσει συγγνώμη τον Απρίλιο του 2011. Το συγκεκριμένο σκάνδαλο

έγινε γνωστό όταν δημοσιεύτηκαν έρευνες που έδειχναν πως υπήρχε ένα κρυφό αρχείο παρακολούθησης το οποίο ονομάζεται «iPhone tracker» και κατάγραφε προσωρινά τις τοποθεσίες που ένας χρήστης έχει επισκεφθεί τους τελευταίους 12 μήνες χωρίς αυτοί να γνωρίζουν. Οι ερευνητές δημοσίευσαν ένα πρόγραμμα στο διαδίκτυο ξεκινώντας από τον Ιούνιο όταν κυκλοφόρησε το iOS 4.0 που έδινε την δυνατότητα σε κάθε χρήστη iPhone να βλέπει ένα χάρτη της τοποθεσίας του ανά πάσα στιγμή.

2.14.4. Παραβίαση προσωπικών δεδομένων και πρόσβασης στο X (πρώην Twitter)

Μια άλλη σημαντική επίθεση ήταν στο X (πρώην Twitter) παραβιάζοντας 130 λογαριασμούς. Ωστόσο δεν ήταν κάτι που είχε συμβεί πρώτη φορά στο X. Το 2017, ο λογαριασμός του προέδρου των Ηνωμένων Πολιτειών Αμερικής, Donald Trump, είχε διαγραφεί από έναν υπάλληλο. Τον Ιούλιο του 2020, δημοσιεύτηκε μία ανάρτηση που ζητούσε δωρεές μέσω κρυπτονομίσματος. Αυτό έγινε από επίσημους λογαριασμούς όπως του Elon Musk, της Apple Inc., της Uber Inc., τον Bill Gates καθώς αργότερα προχώρησαν και σε άλλους γνωστούς λογαριασμούς όπως του Jeff Bezos, του Barack Obama, του Joseph R. Biden, του MrBeast, του Mike Bloomberg, της Kim Kardashian αλλά και σε πολλούς άλλους. Οι περισσότεροι από τους λογαριασμούς στους οποίους είχε αποκτηθεί πρόσβαση για την απάτη είχαν τουλάχιστον ένα εκατομμύριο ακόλουθους. Οι αναρτήσεις των hacker έγραφαν ότι πρόκειται για φιλανθρωπικό σκοπό και ότι θα τα επέστρεφαν στον κάθε χρήστη με την διπλάσια αξία Bitcoin που έστελνε σε συγκεκριμένα πορτοφόλια. Στις αναρτήσεις υπήρχαν και κακόβουλοι σύνδεσμοι από διάφορες εταιρίες κρυπτονομισμάτων. Ωστόσο, ο ιστότοπος καταργήθηκε λίγο αργότερα αφού δημοσιεύτηκαν οι αναρτήσεις. Επιπλέον, οι hackers είχαν πρόσβαση σε προσωπικά στοιχεία όπως διευθύνσεις email, αριθμούς τηλεφώνου, ιδιωτικά μηνύματα, εικόνες και βίντεο. Συνολικά, απέκτησαν Bitcoin αξίας άνω των 118000 δολαρίων. Ωστόσο, το πιο σημαντικό είναι ότι το γεγονός ότι «αυτό εξέθεσε την ευπάθεια μιας παγκόσμιας πλατφόρμας μέσω κοινωνικής δικτύωσης με πάνω από 330 εκατομμύρια συνολικά μηνιαίους ενεργούς χρήστες και πάνω από 186 εκατομμύρια καθημερινά ενεργούς χρήστες, συμπεριλαμβανομένων άνω των 36 εκατομμυρίων (20%) στις Ηνωμένες Πολιτείες της Αμερικής.» Τον Ιούλιο

του 2020, οι hacker είχαν προσπαθήσει να ανακτήσουν πρόσβαση στο δίκτυο του X κάνοντας τηλεφωνικές κλήσεις σε υπαλλήλους, λέγοντάς τους ότι είναι από το γραφείο βοήθειας στο τμήμα πληροφοριών της εταιρείας. Με αυτό τον τρόπο προσπάθησαν να κατευθύνουν έναν υπάλληλο σε ιστότοπο ηλεκτρονικού ψαρέματος. Οι hacker έτσι απέκτησαν πρόσβαση σε εργαλεία διαχείρισης γνωστά ως εργαλεία αντιπροσώπου που τους επέτρεπε να μπορούν να αλλάξουν διάφορες ρυθμίσεις σε διάφορους λογαριασμούς από τους παραβιασμένους. Οι hackers είχαν πει στο Vice ότι είχαν πληρώσει άτομα που βρισκόταν μέσα στο X για να αποκτήσουν πρόσβαση σε διαχειριστικά εργαλεία. Επιπροσθέτως, οι hackers αναζήτησαν στο LinkedIn υπαλλήλους που εργάζονταν στο X και είχαν δικαιώματα διαχείρισης στα εργαλεία κατόχου λογαριασμών. Στη συνέχεια, προχώρησαν στο να αποκτήσουν αριθμούς τηλεφώνων από τους υπαλλήλους αλλά και άλλες πληροφορίες επικοινωνίας. Αφού, στοχοποίησαν τα θύματά τους επικοινωνήσαν μαζί τους και λόγω του γεγονότος ότι οι περισσότεροι υπάλληλοι εργαζόταν εξ αποστάσεως εξαιτίας της πανδημίας Covid-19 μπορούσαν να προσποιηθούν ότι ήταν προσωπικό του X. Συνεπώς, απέκτησαν πρόσβαση σε εργαλεία που ήταν μόνο διαθέσιμα στις εσωτερικές ομάδες υποστήριξης και έτσι μπόρεσαν να στοχεύσουν 130 λογαριασμούς του X. Ωστόσο, 45 λογαριασμοί είχαν τη δυνατότητα να επαναφέρουν τους κωδικούς πρόσβασης.

Ενέργειες του X



I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send \$1,000, I will send back \$2,000. Only doing this for 30 minutes.

Εικόνα 16: Η ανάρτηση που είχε γίνει από τους hackers μέσω το λογαριασμού του Joe Biden χρησιμοποιώντας διαχειριστικά εργαλεία του X. (Πηγή: <https://www.bloomberg.com/news/articles/2020-07-15/elon-musk-bill-gates-appear-to-have-twitter-accounts-hacked>)

προσπάθησαν να καταργήσουν τις αναρτήσεις. Αμέσως, υπήρξε άμεση επικοινωνία με τους κατόχους το λογαριασμών που παραβιάστηκαν και έγιναν διάφορες προσπάθειες για να αποκτήσουν πίσω την πρόσβαση σε αυτούς τους λογαριασμούς. Μετά από αυτό, το X ανακοίνωσε πως ήταν «μια συντονισμένη επίθεση κοινωνικής μηχανικής» και

Το X ανακοίνωσε πως οι hackers είχαν καταφέρει να κατεβάσουν προσωπικά στοιχεία από ιδιωτικές συνομιλίες εικόνες και βίντεο. Στη συνέχεια κλείδωσε τους λογαριασμούς στους οποίους είχαν πρόσβαση οι hackers και

ότι εργαζόταν να το διορθώσουν, με συνέπεια να λάβουν κάποια μέτρα σε τομείς όπως στη λήψη δεδομένων της πλατφόρμας αλλά και στην βελτίωση των εργαλείων.

2.14.5. Σκανδάλo παραβίασης προσωπικών δεδομένων Instagram

Ένα άλλο σκάνδαλο που έγινε στα τέλη του Αυγούστου του 2017 όταν ένας hacker κατάφερε να αποκτήσει πρόσβαση σε στοιχεία επικοινωνίας συγκεκριμένων χρηστών της εφαρμογής. Το Instagram ανακοίνωσε πως ο hacker είχε αποκτήσει διευθύνσεις e-mail και αριθμούς τηλεφώνου ορισμένων χρηστών υψηλού προφίλ εκμεταλλευόμενοι ένα σφάλμα στην διεπαφή προγραμματισμού εφαρμογών (API). Ωρες μετά την εισβολή, ο hacker δημιούργησε μια βάση δεδομένων με το όνομα «Doxagram» που επιτρέπει στους χρήστες να αναζητούν στοιχεία επικοινωνίας των θυμάτων για \$10 την αναζήτηση καθώς η λίστα περιείχε 1000 λογαριασμούς που ήταν διαθέσιμοι. Αργότερα, έγινε γνωστό πως ο hacker είχε αποκτήσει πρόσβαση σε 6 εκατομμύρια λογαριασμούς. Αμέσως, το Doxagram έγινε εκτός σύνδεσης αλλά τα στοιχεία επικοινωνίας από δεκάδες διασημότητες συνέχισαν να κυκλοφορούν στο dark web. Το σφάλμα έσπευσε γρήγορα και ενημερώθηκαν οι χρήστες από τους οποίους κλάπηκαν δεδομένα.

ΚΕΦΑΛΑΙΟ 3: ΜΕΘΟΔΟΛΟΓΙΑ ΈΡΕΥΝΑΣ

Η έρευνα με την χρήση ερωτηματολογίου με στόχο την λήψη στατιστικών δεδομένων από έναν πληθυσμό. Το ερωτηματολόγιο έγινε με την χρήση Google Forms και οι απαντήσεις διεξάχθηκαν ανώνυμα. Ύστερα, έγινε ποσοτική ανάλυση η οποία εφαρμόστηκε σε τυχαίο δείγμα. Στη συνέχεια έγινε η συλλογή των δεδομένων της έρευνας και η περιγραφή του δείγματος και παρουσιάζεται ή μέσω στατιστικής ανάλυσης που συλλέχθηκαν με τη βοήθεια κατάλληλου προγράμματος SPSS. Η έρευνα έγινε με την χρήση ερωτηματολογίου. Οι ερωτήσεις ήταν κατά κύριο λόγο κλειστού τύπου καθώς οι ερωτηθέντες είναι υποχρεωμένοι να απαντήσουν αλλά υπάρχουν και ερωτήσεις όπου οι ερωτηθέντες μπορούν να δώσουν πολλαπλές απαντήσεις. Ένα μειονέκτημά αποτελεί βέβαιο το γεγονός ότι πολλά άτομα δεν έχουν συμπληρώσει το ερωτηματολόγιο με αληθινές απαντήσεις με αποτέλεσμα να αλλοιώνουν τις απαντήσεις

3.1. Ερωτηματολόγιο

Το ερωτηματολόγιο αποτελείται από τρεις κατηγορίες. Η πρώτη έχει να κάνει με τα δημογραφικά στοιχεία, η δεύτερη αφορά την συχνότητα χρήσης των μέσων κοινωνικής δικτύωσης και η τρίτη αφορά την γνώση των χρηστών για τους όρους και κανόνες των μέσων κοινωνικής δικτύωσης. Υπάρχουν συνολικά 24 ερωτήσεις.

Ενότητα Α: Δημογραφικά στοιχεία

1. Φύλλο
 - Άνδρας
 - Γυναίκα
2. Ηλικιακή ομάδα
 - Έφηβος
 - Ενήλικας από 18 έως 35 ετών
 - Ενήλικας άνω των 35 ετών
3. Μορφωτικό επίπεδο
 - Βασική εκπαίδευση (απόφοιτος Δημοτικού ή Γυμνασίου)
 - Απόφοιτος Λυκείου

- Πτυχιούχος Πανεπιστημίου
 - Κάτοχος μεταπτυχιακού ή διδακτρικού διπλώματος
4. Περιοχή Κατοικίας
- Αστική
 - Αγροτική

Ενότητα Β: Χρήση μέσων κοινωνικής δικτύωσης

5. Σε ποια μέσα κοινωνικής δικτύωσης είστε ενεργός;
- Facebook
 - Twitter
 - Instagram
 - TikTok
 - Pinterest
 - Discord
 - YouTube
 - Άλλο
6. Πόσο χρόνο αφιερώνετε συνήθως στα μέσα κοινωνικής δικτύωσης κάθε μέρα;
- 1-2 ώρες
 - 3-6 ώρες
 - Πάνω από 6 ώρες
7. Γιατί χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης;
- Ενημέρωση
 - Κοινωνική Δικτύωση
 - Ψυχαγωγία / Διασκέδαση
 - Υπηρεσίες
 - Άλλο
8. Πόσο καιρό πιστεύετε ότι θα μπορούσατε να μείνετε μακριά από τα μέσα κοινωνικής δικτύωσης;
- Καθόλου
 - Μία μέρα
 - Μία εβδομάδα
 - Ένα μήνα
 - Περισσότερο

9. Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;
- Φωτογραφία
 - Ηλικία
 - Όνομα
 - Διεύθυνση
 - Στοιχεία επικοινωνίας
10. Πόσο συχνά δημοσιεύετε στα μέσα κοινωνικής δικτύωσης;
- Πολύ συχνά
 - Συχνά
 - Σπανίως
 - Ποτέ

Ενότητα Γ: Γνώση όρων και κανόνων των μέσων κοινωνικής δικτύωσης

11. Έχετε διαβάσει ποτέ την πολιτική ασφάλειας των μέσων κοινωνικής δικτύωσης που χρησιμοποιείτε;
- Ναι
 - Όχι
12. Γνωρίζετε αν επιλέξετε να διαγράψετε κάτι που έχετε ήδη δημοσιεύσει, διαγράφεται οριστικά;
- Ναι
 - Όχι
 - Δεν γνωρίζω
13. Γνωρίζετε αν ένας ιστότοπος ή μια εφαρμογή έχει πολιτική απορρήτου, αυτό σημαίνει ότι δεν θα κοινοποιήσει τα προσωπικά σας στοιχεία σε κανέναν.
- Ναι
 - Όχι
 - Δεν γνωρίζω
14. Γνωρίζετε για το πόσο συχνά πρέπει να αλλάζετε τον κωδικό πρόσβασής σας;
- Μια φορά το μήνα
 - Μια φορά το χρόνο
 - Κάθε μέρα
 - Ποτέ
 - Δεν γνωρίζω

15. Όταν ένας ιστότοπος έχει πολιτική απορρήτου, σημαίνει ότι ο ιστότοπος...
- Έχει δημιουργήσει μια σύμβαση μεταξύ της ίδιας και των χρηστών της σχετικά με τον τρόπο χρήσης των δεδομένων τους
 - Συλλέγει, χωρίς περιορισμό, προσωπικά δεδομένα του χρήστη.
16. Εάν ένας ιστότοπος χρησιμοποιεί cookies, σημαίνει ότι ο ιστότοπος μπορεί να...
- Συλλέγει προσωπικές πληροφορίες για έναν χρήστη
 - Περιέχει ένα μοναδικό αναγνωριστικό για έναν υπολογιστή
 - Κρατάει τον χρήστη συνδεδεμένο σε μια ιστοσελίδα κοινωνικής δικτύωσης χωρίς να ξανάεισάγει κωδικούς πρόσβασης
17. Γνωρίζετε αν η νομοθεσία καλύπτει την προστασία των προσωπικών σας δεδομένων επαρκώς;
- Ναι
 - Όχι
 - Δεν γνωρίζω
18. Πιστεύετε ότι οι ιστότοποι κοινωνικής δικτύωσης είναι ασφαλείς;
- Ναι
 - Όχι
19. Σε κλίμακα από το 1 έως το 5, θεωρείτε ότι τωρινή ενημέρωση για τους κινδύνους του διαδικτύου είναι αρκετή;
20. Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης ;
21. Πιστεύετε ότι τα ίδια μέσα κοινωνικής δικτύωσης είναι υπεύθυνα για την ενημέρωση των χρηστών της σχετικά με τις ρυθμίσεις απορρήτου
- Ναι
 - Όχι
22. Θεωρείτε τον εθισμό στα μέσα κοινωνικής δικτύωσης εξίσου σημαντικό με την προστασία προσωπικών δεδομένων εφόσον μπορεί να την επηρεάσει.
- Ναι
 - Όχι
23. Προειδοποιείτε τους φίλους/συγγενείς σας για το πως να προστατέψουν τα προσωπικά τους δεδομένα;
- Ναι
 - Όχι

24. Εάν γνωρίζετε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζετε να τα χρησιμοποιείτε;

➤ Ναι

➤ Όχι

Κεφάλαιο 4: Ανάλυση αποτελεσμάτων/τρόποι αντιμετώπισης και μελλοντικές επεκτάσεις

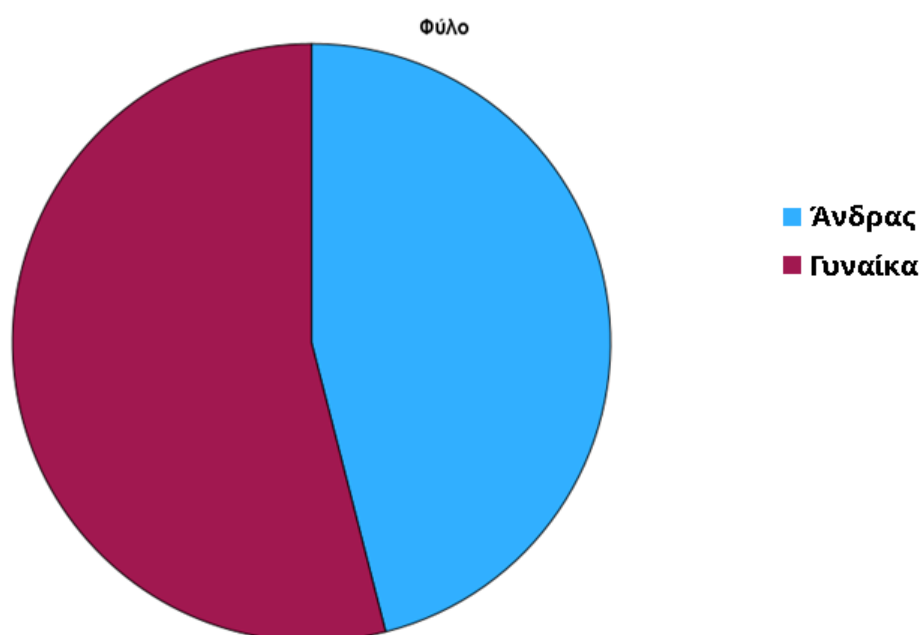
Ανάλυση δημογραφικών στοιχείων (Ενότητα Α)

1. Φύλο

Στην έρευνα συμμετείχαν 213 άτομα συνολικά, από τα οποία τα 115 είναι γυναίκες και 98 ήταν άνδρες. Οι γυναίκες αποτελούν την πλειοψηφία του δείγματος με ποσοστό 54%, έναντι του ποσοστού των ανδρών 46%..

Πίνακας 1: Φύλο

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Άνδρας	98	46,0	46,0	46,0
	Γυναίκα	115	54,0	54,0	100,0
	Total	213	100,0	100,0	



Διάγραμμα 1: Κατανομή δείγματος ως προς το φύλο των ερωτηθέντων.

1. Ηλικιακή ομάδα

Υπάρχουν τρεις ηλικιακές κλίμακες. Το μεγαλύτερο ποσοστό ανήκει στους ενήλικες από 18 μέχρι 35 με 191 απαντήσεις (89,7%). Στην συνέχεια, το δεύτερο μεγαλύτερο ποσοστό το είχαν οι έφηβοι από τους οποίους απάντησαν 14 άτομα (6,6%) και τέλος πολύ μικρή ήταν η συμμετοχή ατόμων μεταξύ των ενήλικων άνω των 35 ετών με 8 απαντήσεις (3,8%).

Πίνακας 2: Ηλικιακή ομάδα

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ενήλικας άνω των 35 ετών	8	3,8	3,8	3,8
	Ενήλικας από 18 έως 35 ετών	191	89,7	89,7	93,4
	Έφηβος	14	6,6	6,6	100,0
Total		213	100,0	100,0	



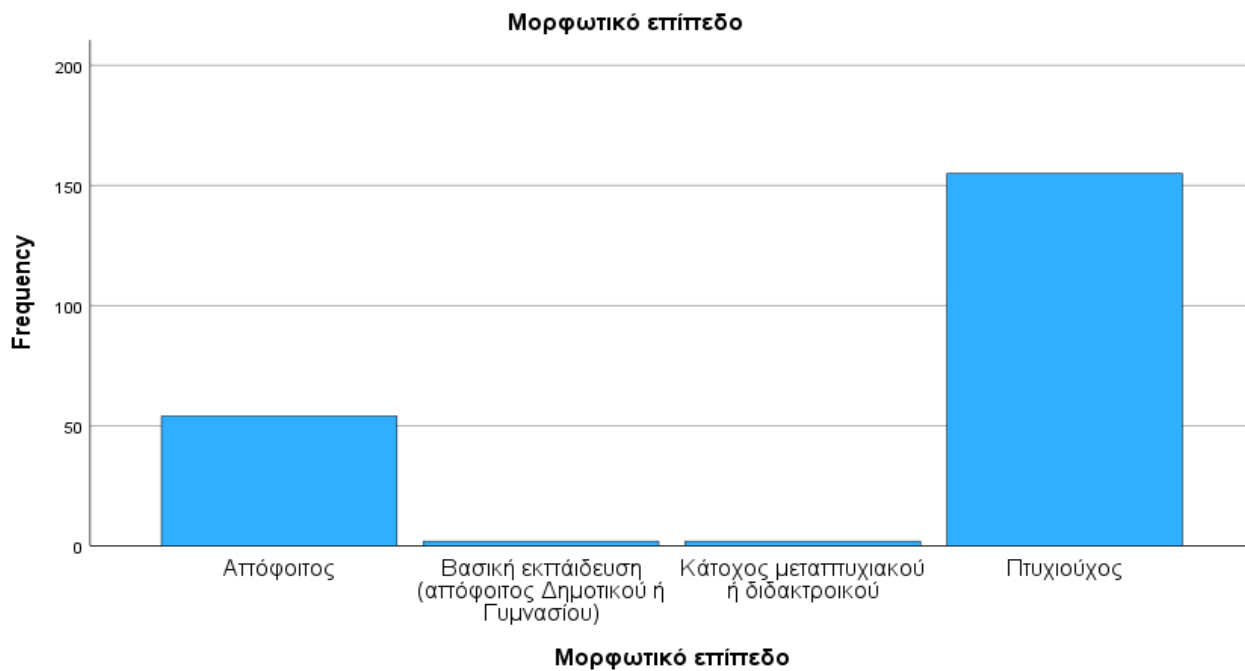
Διάγραμμα 2: Κατανομή δείγματος ως προς την ηλικιακή ομάδα των ερωτηθέντων.

3. Μορφωτικό επίπεδο

Στο μορφωτικό επίπεδο, το οποίο κατά κύριο λόγο είναι γενικά υψηλό, παρατηρούμε ότι η πλειοψηφία του δείγματος ανήκει στην κατηγορία πτυχιούχος πανεπιστημίου με 155 απαντήσεις (72,8%). Στη δεύτερη θέση, οι απόφοιτοι λυκείου με 54 απαντήσεις (25,4%). Επίσης, δύο άτομα απάντησαν κάτοχος μεταπτυχιακού ή διδακτορικού διπλώματός (0,9%) και άλλα δύο άτομα απάντησαν βασική εκπαίδευσή (απόφοιτος δημοτικού ή γυμνασίου) (0,9%).

Πίνακας 3: Μορφωτικό επίπεδο

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Απόφοιτος Λυκείου	54	25,4	25,4	25,4
Βασική εκπαίδευση (απόφοιτος Δημοτικού ή Γυμνασίου)	2	,9	,9	26,3
Κάτοχος μεταπτυχιακού ή διδακτορικού διπλώματος	2	,9	,9	27,2
Πτυχιούχος Πανεπιστημίου	155	72,8	72,8	100,0
Total	213	100,0	100,0	



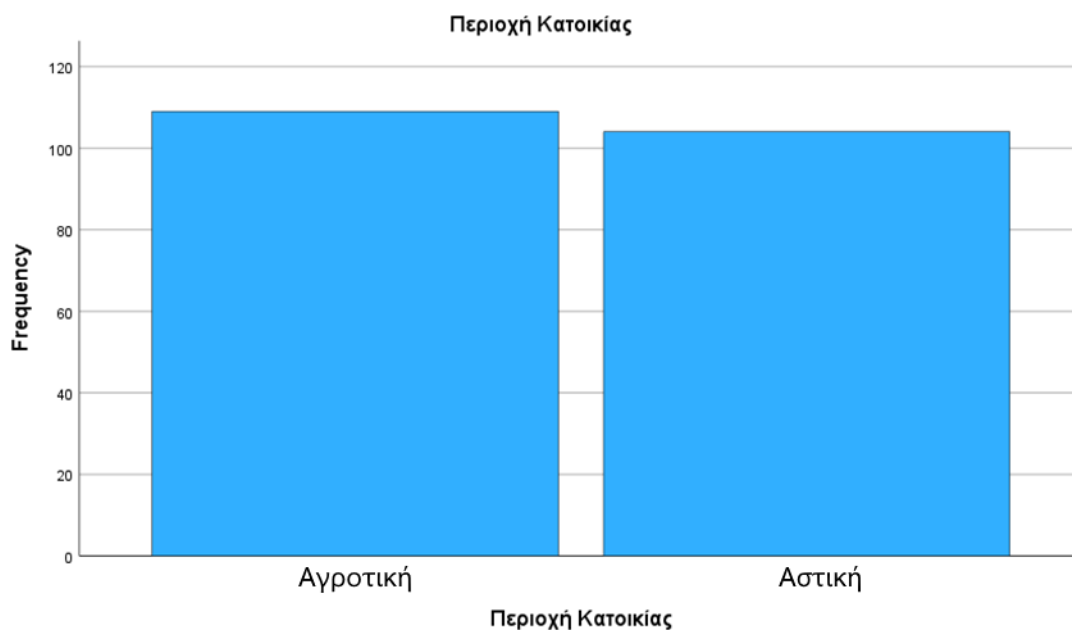
Διάγραμμα 3: Κατανομή δείγματος ως προς το μορφωτικό επίπεδο των ερωτηθέντων.

4. Περιοχή Κατοικίας

Η πλειοψηφία του δείγματος απάντησε ότι κατοικεί σε αγροτική περιοχή με 109 απαντήσεις (51,2%) ενώ με σε αστική περιοχή με 104 απαντήσεις (48,8%).

Πίνακας 4: Περιοχή κατοικίας.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Αγροτική	109	51,2	51,2	51,2
	Αστική	104	48,8	48,8	100,0
	Total	213	100,0	100,0	



Διάγραμμα 4: Κατανομή δείγματος ως προς την περιοχή κατοικίας των ερωτηθέντων.

Ανάλυση χρήση μέσων κοινωνικής δικτύωσης (Ενότητα Β)

5. Σε ποια μέσα κοινωνικής δικτύωσης είστε ενεργός;

Η πλειοψηφία του δείγματος το δήλωσε ότι χρησιμοποιεί το Instagram με 199 απαντήσεις (93,4%). Για άλλα μέσα δηλώθηκε πως χρησιμοποιεί το YouTube με 192 απαντήσεις (90,1%), το Facebook με 159 απαντήσεις (74,6%), το TikTok με 138 απαντήσεις (64,8), το Pinterest με 129 απαντήσεις (60,6%) και Discord με 93 απαντήσεις (43,7%), το X (στο ερωτηματολόγιο είχε το όνομα «Twitter») με 60 απαντήσεις (28,2%) και ένα μικρό ποσοστό (49,8%) δήλωσαν ότι χρησιμοποιούν κάποιο άλλο μέσο κοινωνικής δικτύωσης με 106 απαντήσεις.

Πίνακας 5: Σε ποια μέσα κοινωνικής δικτύωσης είστε ενεργός;

		Freque ncy	Percent	Valid Percent	Cumulative Percent
Valid	Facebook, Instagram	2	,9	,9	,9
	Facebook, Instagram, Discord	2	,9	,9	1,9

Facebook, Instagram, Discord, Άλλο	1	,5	,5	2,3
Facebook, Instagram, Discord, YouTube, Άλλο	1	,5	,5	2,8
Facebook, Instagram, Pinterest, Discord, YouTube	1	,5	,5	3,3
Facebook, Instagram, Pinterest, Discord, YouTube, Άλλο	4	1,9	1,9	5,2
Facebook, Instagram, Pinterest, YouTube	10	4,7	4,7	9,9
Facebook, Instagram, Pinterest, YouTube, Άλλο	2	,9	,9	10,8
Facebook, Instagram, TikTok, Discord	1	,5	,5	11,3
Facebook, Instagram, TikTok, Discord, Άλλο	1	,5	,5	11,7
Facebook, Instagram, TikTok, Discord, YouTube	1	,5	,5	12,2
Facebook, Instagram, TikTok, Discord, YouTube, Άλλο	5	2,3	2,3	14,6
Facebook, Instagram, TikTok, Pinterest	1	,5	,5	15,0
Facebook, Instagram, TikTok, Pinterest, Άλλο	1	,5	,5	15,5
Facebook, Instagram, TikTok, Pinterest, Discord	1	,5	,5	16,0

Facebook, Instagram, TikTok, Pinterest, Discord, YouTube	8	3,8	3,8	19,7
Facebook, Instagram, TikTok, Pinterest, Discord, YouTube, Άλλο	17	8,0	8,0	27,7
Facebook, Instagram, TikTok, Pinterest, YouTube	9	4,2	4,2	31,9
Facebook, Instagram, TikTok, Pinterest, YouTube, Άλλο	9	4,2	4,2	36,2
Facebook, Instagram, TikTok, YouTube	9	4,2	4,2	40,4
Facebook, Instagram, TikTok, YouTube, Άλλο	7	3,3	3,3	43,7
Facebook, Instagram, YouTube	10	4,7	4,7	48,4
Facebook, Instagram, YouTube, Άλλο	5	2,3	2,3	50,7
Facebook, Pinterest, YouTube, Άλλο	1	,5	,5	51,2
Facebook, TikTok, Discord, YouTube	1	,5	,5	51,6
Facebook, TikTok, Pinterest, Discord, YouTube	1	,5	,5	52,1
Facebook, TikTok, Pinterest, Discord, YouTube, Άλλο	1	,5	,5	52,6
Facebook, TikTok, Pinterest, YouTube	1	,5	,5	53,1

Facebook, TikTok, Pinterest, YouTube, Άλλο	1	,5	,5	53,5
Facebook, Twitter, Instagram, Discord, YouTube, Άλλο	1	,5	,5	54,0
Facebook, Twitter, Instagram, Pinterest, Discord, YouTube	1	,5	,5	54,5
Facebook, Twitter, Instagram, Pinterest, Discord, YouTube, Άλλο	3	1,4	1,4	55,9
Facebook, Twitter, Instagram, Pinterest, YouTube	2	,9	,9	56,8
Facebook, Twitter, Instagram, Pinterest, YouTube, Άλλο	3	1,4	1,4	58,2
Facebook, Twitter, Instagram, TikTok, Discord, YouTube, Άλλο	2	,9	,9	59,2
Facebook, Twitter, Instagram, TikTok, Pinterest, Discord, YouTube	3	1,4	1,4	60,6
Facebook, Twitter, Instagram, TikTok, Pinterest, Discord, YouTube, Άλλο	15	7,0	7,0	67,6
Facebook, Twitter, Instagram, TikTok, Pinterest, YouTube	4	1,9	1,9	69,5

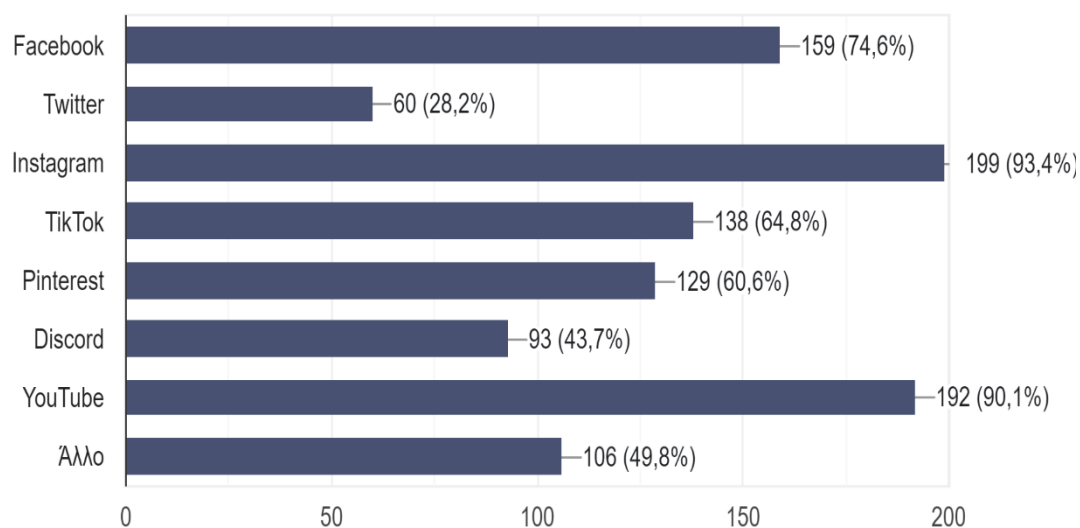
Facebook, Twitter, Instagram, TikTok, Pinterest, YouTube, Άλλο	4	1,9	1,9	71,4
Facebook, Twitter, Instagram, TikTok, YouTube	2	,9	,9	72,3
Facebook, Twitter, Instagram, YouTube, Άλλο	1	,5	,5	72,8
Facebook, Twitter, TikTok, Discord, YouTube	2	,9	,9	73,7
Facebook, Twitter, TikTok, YouTube	1	,5	,5	74,2
Facebook, YouTube	1	,5	,5	74,6
Instagram	6	2,8	2,8	77,5
Instagram, Άλλο	1	,5	,5	77,9
Instagram, Discord	1	,5	,5	78,4
Instagram, Pinterest, Discord, YouTube	1	,5	,5	78,9
Instagram, Pinterest, Discord, YouTube, Άλλο	3	1,4	1,4	80,3
Instagram, Pinterest, YouTube	1	,5	,5	80,8
Instagram, Pinterest, YouTube, Άλλο	2	,9	,9	81,7
Instagram, TikTok, Discord	1	,5	,5	82,2
Instagram, TikTok, Discord, YouTube	1	,5	,5	82,6

Instagram, TikTok, Pinterest, Discord, YouTube	1	,5	,5	83,1
Instagram, TikTok, Pinterest, Discord, YouTube, Άλλο	3	1,4	1,4	84,5
Instagram, TikTok, Pinterest, YouTube	2	,9	,9	85,4
Instagram, TikTok, Pinterest, YouTube, Άλλο	2	,9	,9	86,4
Instagram, TikTok, YouTube	8	3,8	3,8	90,1
Instagram, TikTok, YouTube, Άλλο	2	,9	,9	91,1
Instagram, YouTube	2	,9	,9	92,0
TikTok, Pinterest, Discord, YouTube	1	,5	,5	92,5
Twitter, Discord, Άλλο	1	,5	,5	93,0
Twitter, Instagram, Pinterest, Discord, Άλλο	1	,5	,5	93,4
Twitter, Instagram, Pinterest, YouTube	1	,5	,5	93,9
Twitter, Instagram, Pinterest, YouTube, Άλλο	1	,5	,5	94,4
Twitter, Instagram, TikTok, Discord, YouTube	2	,9	,9	95,3
Twitter, Instagram, TikTok, Discord, YouTube, Άλλο	1	,5	,5	95,8

Twitter, Instagram, TikTok, Pinterest, Discord, YouTube	1	,5	,5	96,2
Twitter, Instagram, TikTok, Pinterest, Discord, YouTube, Άλλο	1	,5	,5	96,7
Twitter, Instagram, TikTok, Pinterest, YouTube	3	1,4	1,4	98,1
Twitter, Instagram, YouTube	1	,5	,5	98,6
Twitter, Instagram, YouTube, Άλλο	1	,5	,5	99,1
Twitter, Pinterest, Discord, YouTube, Άλλο	1	,5	,5	99,5
Twitter, TikTok, Pinterest, YouTube, Άλλο	1	,5	,5	100,0
Total	213	100,0	100,0	

5. Σε ποια μέσα κοινωνικής δικτύωσης είστε ενεργός;

213 απαντήσεις



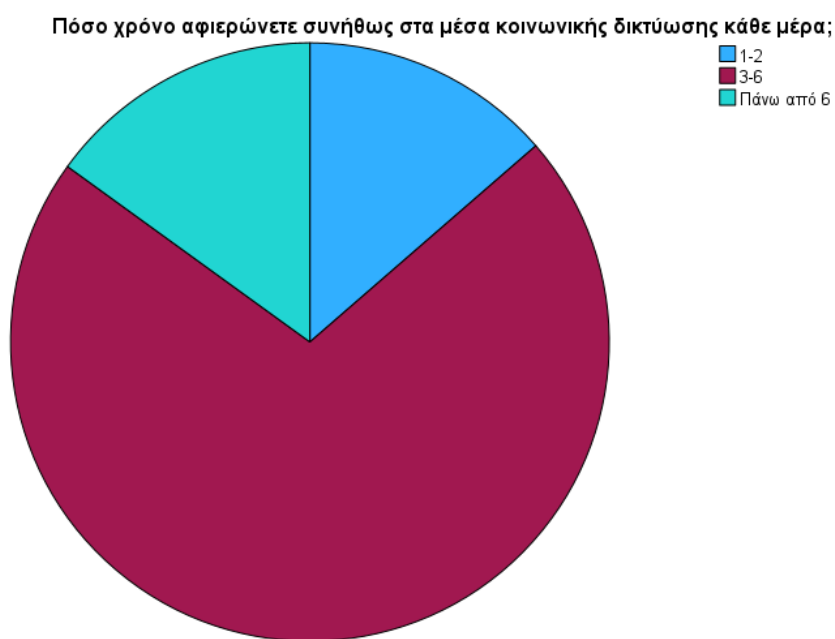
Διάγραμμα 5: Κατανομή δείγματος ως προς το σε ποια μέσα κοινωνικής δικτύωσης είναι ενεργοί οι ερωτηθέντες.

6. Πόσο χρόνο αφιερώνετε συνήθως στα μέσα κοινωνικής δικτύωσης κάθε μέρα;

Προχωρώντας στην ερευνά, διευρύνεται πόσο χρόνο αφιερώνουν στα μέσα κοινωνικής δικτύωσης κάθε μέρα. Η πλειοψηφία απάντησε 3-6 ώρες με 152 απαντήσεις (71,4%), οι υπόλοιποι 32 απάντησαν πάνω από 6 ώρες (15%) και 1-2 ώρες απάντησαν 29 χρήστες (13,6%). Παρατηρείται πως οι περισσότεροι χρήστες αφιερώνουν συνήθως πάνω από 3 ώρες την ημέρα στα μέσα κοινωνικής δικτύωσης.

Πίνακας 6: Πόσο χρόνο αφιερώνετε συνήθως στα μέσα κοινωνικής δικτύωσης κάθε μέρα;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 ώρες	29	13,6	13,6	13,6
	3-6 ώρες	152	71,4	71,4	85,0
	Πάνω από 6 ώρες	32	15,0	15,0	100,0
	Total	213	100,0	100,0	



Διάγραμμα 6: Κατανομή δείγματος ως προς το πόσο χρόνο αφιερώνουν στα μέσα κοινωνικής δικτύωσης οι ερωτηθέντες.

7. Γιατί χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης;

Η πλειοψηφία των ερωτηθέντων δήλωσε ότι χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης για ψυχαγωγία και διασκέδαση με 210 απαντήσεις (98,6%), για ενημέρωση

με 207 απαντήσεις (97,2%), για κοινωνική δικτύωση με 197 απαντήσεις (92,5%), για υπηρεσίες με 172 απαντήσεις (80,8%) και 133 άτομα απάντησαν άλλο (62,4%).

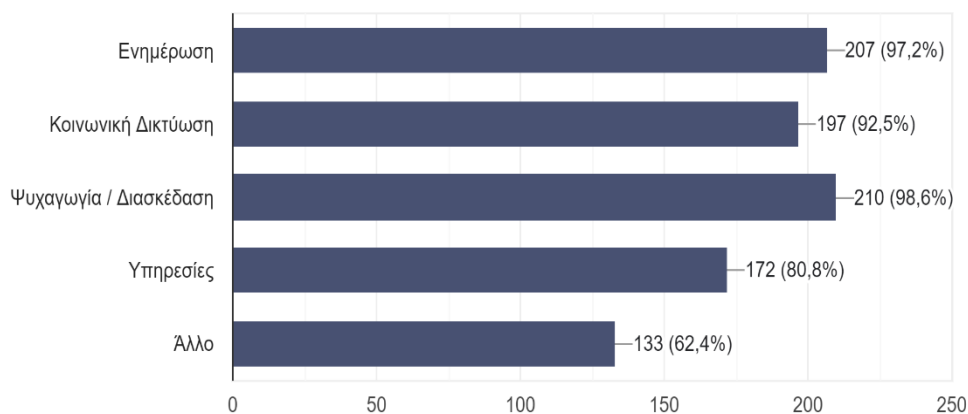
Πίνακας 7: Γιατί χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ενημέρωση	1	,5	,5	,5
	Ενημέρωση, Κοινωνική Δικτύωση, Υπηρεσίες, Άλλο	1	,5	,5	,9
	Ενημέρωση, Κοινωνική Δικτύωση, Ψυχαγωγία / Διασκέδαση	20	9,4	9,4	10,3
	Ενημέρωση, Κοινωνική Δικτύωση, Ψυχαγωγία / Διασκέδαση, Άλλο	8	3,8	3,8	14,1
	Ενημέρωση, Κοινωνική Δικτύωση, Ψυχαγωγία / Διασκέδαση, Υπηρεσίες	43	20,2	20,2	34,3
	Ενημέρωση, Κοινωνική Δικτύωση, Ψυχαγωγία / Διασκέδαση, Υπηρεσίες, Άλλο	121	56,8	56,8	91,1
	Ενημέρωση, Ψυχαγωγία / Διασκέδαση	4	1,9	1,9	93,0
	Ενημέρωση, Ψυχαγωγία / Διασκέδαση, Άλλο	2	,9	,9	93,9

Ενημέρωση, Ψυχαγωγία / Διασκέδαση, Υπηρεσίες	6	2,8	2,8	96,7
Ενημέρωση, Ψυχαγωγία / Διασκέδαση, Υπηρεσίες, Άλλο	1	,5	,5	97,2
Κοινωνική Δικτύωση	1	,5	,5	97,7
Κοινωνική Δικτύωση, Ψυχαγωγία / Διασκέδαση	3	1,4	1,4	99,1
Ψυχαγωγία / Διασκέδαση	2	,9	,9	100,0
Total	213	100,0	100,0	

7. Γιατί χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης;

213 απαντήσεις



Διάγραμμα 7: Κατανομή δείγματος ως προς το λόγο που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης οι ερωτηθέντες.

8. Πόσο καιρό πιστεύετε ότι θα μπορούσατε να μείνετε μακριά από τα μέσα κοινωνικής δικτύωσης

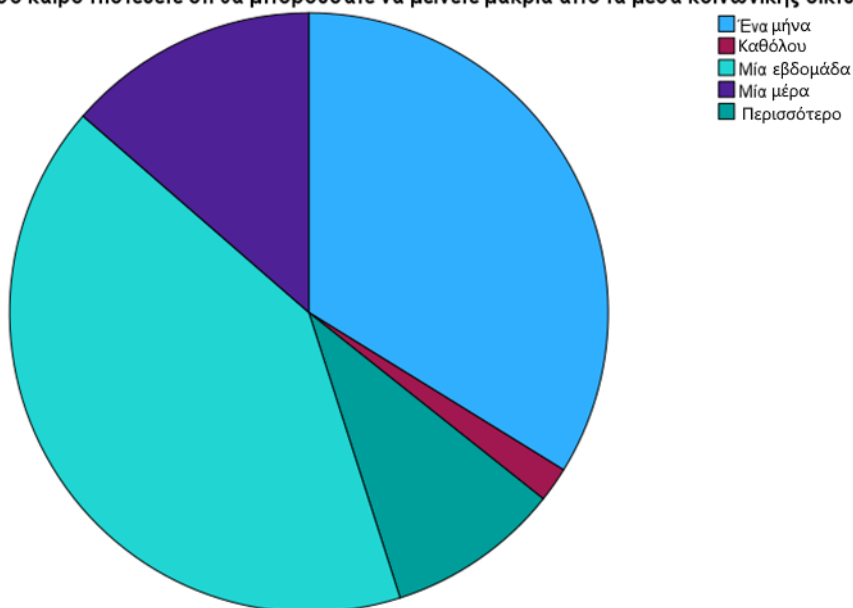
Συνεχίζοντας την έρευνα οι χρήστες ρωτήθηκαν πόσο καιρό πιστεύουν ότι θα μπορούσαν να μείνουν μακριά από τα μέσα κοινωνικής δικτύωσης. Τα ποσοστά δείχνουν ότι το 41,3% θα μπορούσε μια εβδομάδα (88 απαντήσεις), το 33,8% θα

μπορούσε ένα μήνα (72 απαντήσεις), το 13,6% θα μπορούσε για μια μέρα (29 απαντήσεις), ενώ το 1,9% απάντησαν καθόλου (4 απαντήσεις).

Πίνακας 8: Πόσο καιρό πιστεύετε ότι θα μπορούσατε να μείνετε μακριά από τα μέσα κοινωνικής δικτύωσης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ένα μήνα	72	33,8	33,8	33,8
	Καθόλου	4	1,9	1,9	35,7
	Μία εβδομάδα	88	41,3	41,3	77,0
	Μία μέρα	29	13,6	13,6	90,6
	Περισσότερο	20	9,4	9,4	100,0
	Total	213	100,0	100,0	

Πόσο καιρό πιστεύετε ότι θα μπορούσατε να μείνετε μακριά από τα μέσα κοινωνικής δικτύωσης;



Διάγραμμα 8: Κατανομή δείγματος ως προς την διάρκεια που μπορούν να απέχουν οι ερωτηθέντες από τα μέσα κοινωνικής δικτύωσης.

9. Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;

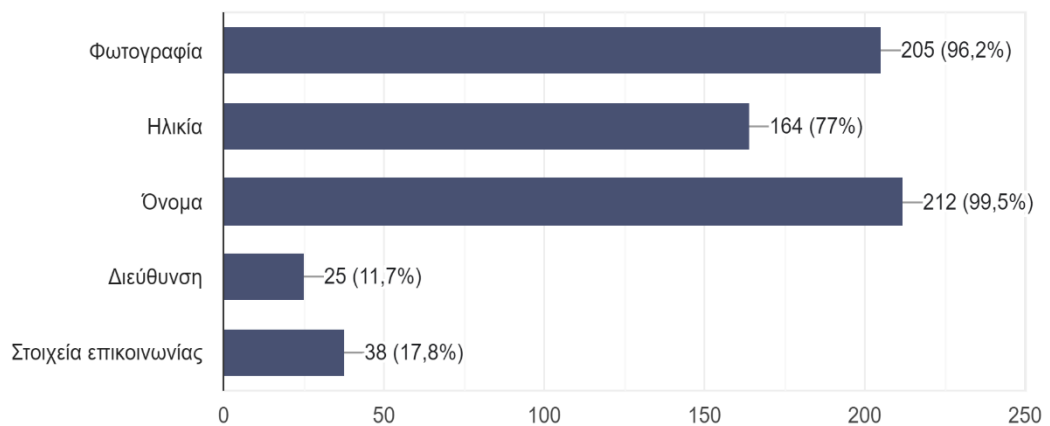
Προχωρώντας στην έρευνα ζητήθηκε από τους χρήστες να επιλέξουν ποια προσωπικά στοιχεία έχουν δώσει στα μέσα κοινωνικής δικτύωσης. Οι ερωτηθέντες σε ένα μεγάλο αριθμό απάντησαν 212 άτομα όνομα (99,5%), 205 άτομα απάντησαν φωτογραφία (96,2%) και 164 άτομα ηλικία (77%). Σημαντικό αποτελεί το γεγονός ότι μόνο το 11,7% έχει μοιραστεί τη διεύθυνση (25 απαντήσεις) και 17,8% έχουν δώσει στα μέσα κοινωνικής δικτύωσης στοιχεία επικοινωνίας (38 απαντήσεις).

Πίνακας 9: Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ηλικία, Όνομα	4	1,9	1,9	1,9
	Ηλικία, Όνομα, Διεύθυνση	1	,5	,5	2,3
	Όνομα	3	1,4	1,4	3,8

Φωτογραφία, Ηλικία	1	,5	,5	4,2
Φωτογραφία, Ηλικία, Όνομα	113	53,1	53,1	57,3
Φωτογραφία, Ηλικία, Όνομα, Διεύθυνση	7	3,3	3,3	60,6
Φωτογραφία, Ηλικία, Όνομα, Διεύθυνση, Στοιχεία επικοινωνίας	17	8,0	8,0	68,5
Φωτογραφία, Ηλικία, Όνομα, Στοιχεία επικοινωνίας	21	9,9	9,9	78,4
Φωτογραφία, Όνομα	46	21,6	21,6	100,0
Total	213	100,0	100,0	

9. Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;
213 απαντήσεις



Διάγραμμα 9: Κατανομή δείγματος ως προς το ποια στοιχεία έχουν δώσει οι ερωτηθέντες στα μέσα κοινωνικής δικτύωσης.

10. Πόσο συχνά δημοσιεύετε στα μέσα κοινωνικής δικτύωσης;

Μετάπειτα, ζητήθηκε από τους χρήστες να απαντήσουν πόσο συχνά δημοσιεύουν στα μέσα κοινωνικής δικτύωσης. 32,9% απάντησαν ότι δημοσιεύουν σπάνια στα μέσα κοινωνικής δικτύωσης (70 απαντήσεις), 39,4% απάντησαν ότι δημοσιεύουν συχνά (84 απαντήσεις), 26,3% απάντησαν πολύ συχνά (56 απαντήσεις), ενώ 1,4% απάντησε ποτέ (3 απαντήσεις).

Πίνακας 10: Πόσο συχνά δημοσιεύετε στα μέσα κοινωνικής δικτύωσης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Πολύ συχνά	56	26,3	26,3	26,3
	Ποτέ	3	1,4	1,4	27,7
	Σπανίως	70	32,9	32,9	60,6
	Συχνά	84	39,4	39,4	100,0
	Total	213	100,0	100,0	



Διάγραμμα 10: Κατανομή δείγματος ως προς το πόσο συχνά δημοσιεύουν οι ερωτηθέντες στα μέσα κοινωνικής δικτύωσης.

Ανάλυση χρήση μέσων κοινωνικής δικτύωσης (Ενότητα Β)

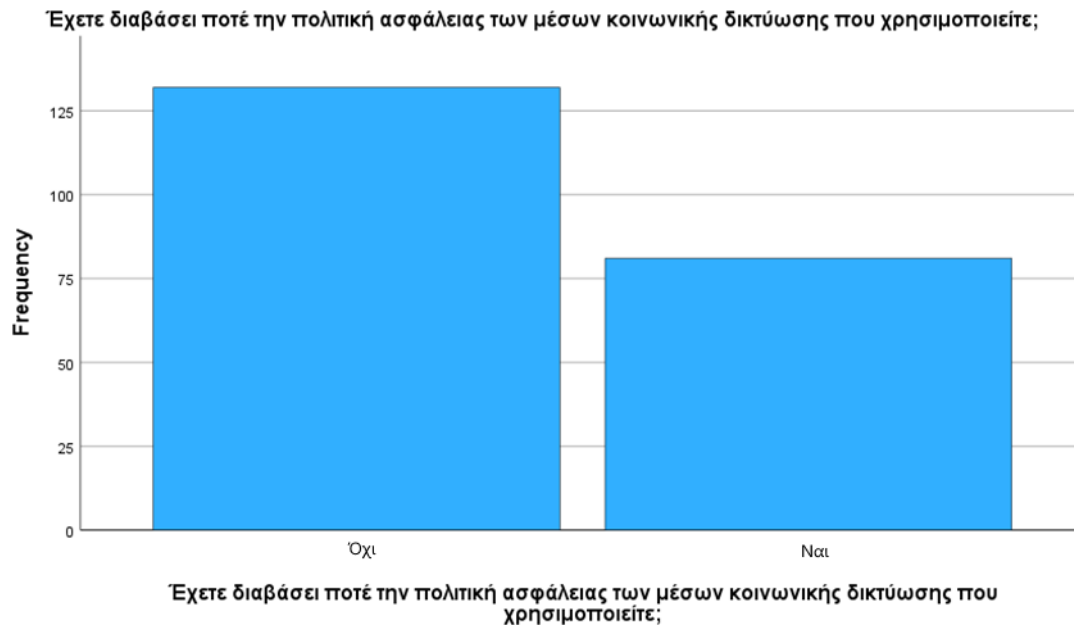
11. Έχετε διαβάσει ποτέ την πολιτική ασφάλειας των μέσων κοινωνικής δικτύωσης που χρησιμοποιείτε;

Μια πολύ σημαντική ερώτηση αποτελεί αν οι ερωτηθέντες έχουν διαβάσει ποτέ την πολιτική ασφάλειας των μέσων κοινωνικής δικτύωσης που χρησιμοποιούν. Το μεγαλύτερο ποσοστό (62%) απάντησαν όχι (132 απαντήσεις) και το 38% απάντησαν ναι (81 απαντήσεις).

Πίνακας 11: Έχετε διαβάσει ποτέ την πολιτική ασφάλειας των μέσων κοινωνικής δικτύωσης που χρησιμοποιείτε;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Όχι	132	62,0	62,0	62,0
	Ναι	81	38,0	38,0	100,0

Total	213	100,0	100,0
-------	-----	-------	-------



Διάγραμμα 11: Κατανομή δείγματος ως προς το αν έχουν διαβάσει ποτέ οι ερωτηθέντες την πολιτική ασφάλειας των μέσων κοινωνικής δικτύωσης που χρησιμοποιούν.

12. Γνωρίζετε αν επιλέξετε να διαγράψετε κάτι που έχετε ήδη δημοσιεύσει, διαγράφεται οριστικά;

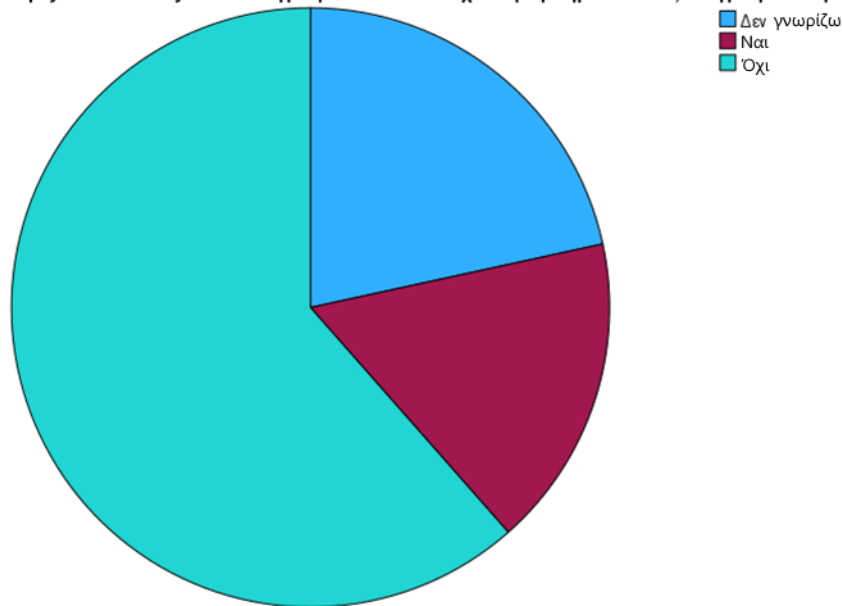
Στην ερώτηση «Γνωρίζετε αν επιλέξετε να διαγράψετε κάτι που έχετε ήδη δημοσιεύσει, διαγράφεται οριστικά;», οι περισσότεροι απάντησαν όχι (61,5%) με 131 απαντήσεις, στη συνέχεια 46 άτομα απάντησαν ότι δεν γνωρίζουν (21,6%) και 36 άτομα απάντησαν ναι (16,9%).

Πίνακας 12: Γνωρίζετε αν επιλέξετε να διαγράψετε κάτι που έχετε ήδη δημοσιεύσει, διαγράφεται οριστικά;

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Δεν γνωρίζω	46	21,6	21,6	21,6

Ναι	36	16,9	16,9	38,5
Όχι	131	61,5	61,5	100,0
Total	213	100,0	100,0	

Γνωρίζετε αν επιλέξετε να διαγράψετε κάτι που έχετε ήδη δημοσιεύσει, διαγράφεται οριστικά;



Διάγραμμα 12: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες ότι αν διαγράψουν κάτι στα μέσα κοινωνικής δικτύωσης διαγράφεται οριστικά.

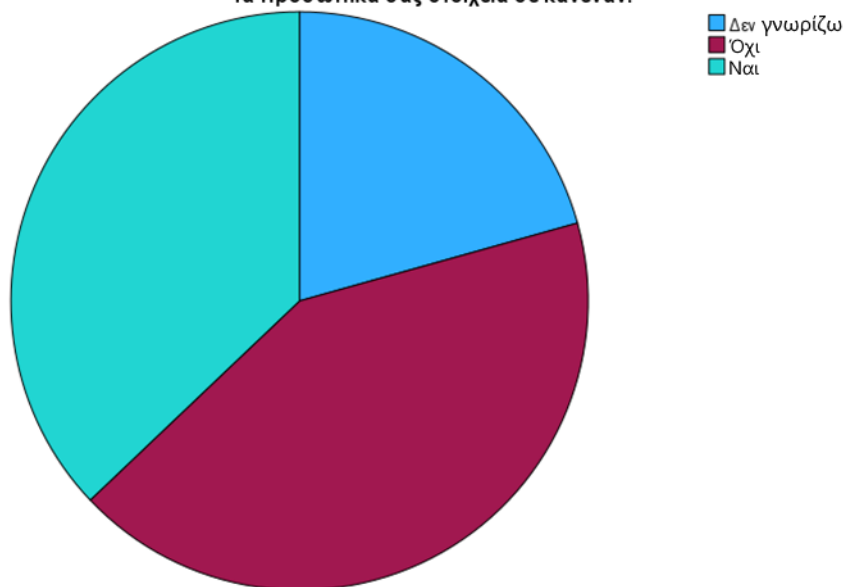
13. Γνωρίζετε αν ένας ιστότοπος ή μια εφαρμογή έχει πολιτική απορρήτου, αυτό σημαίνει ότι δεν θα κοινοποιήσει τα προσωπικά σας στοιχεία σε κανέναν.

Προχωρώντας στην έρευνα διευρύνεται γίνεται η ερώτηση αν γνωρίζουν οι ερωτηθέντες ότι ένας ιστότοπος ή μια εφαρμογή που έχει πολιτική απορρήτου αυτό σημαίνει ότι δεν θα κοινοποιήσει τα προσωπικά τους στοιχεία σε κανένα. Αρχικά, οι χρήστες απάντησαν όχι (42,3%) με 90 απαντήσεις, καθώς ένα 37,1% απάντησε ναι με 79 απαντήσεις και το 20,7% συμφώνησε ότι δε γνωρίζει με 44 απαντήσεις.

Πίνακας 13: Γνωρίζετε αν ένας ιστότοπος ή μια εφαρμογή έχει πολιτική απορρήτου, αυτό σημαίνει ότι δεν θα κοινοποιήσει τα προσωπικά σας στοιχεία σε κανέναν.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Δεν γνωρίζω	44	20,7	20,7	20,7
	Όχι	90	42,3	42,3	62,9
	Ναι	79	37,1	37,1	100,0
	Total	213	100,0	100,0	

Γνωρίζετε αν ένας ιστότοπος ή μια εφαρμογή έχει πολιτική απορρήτου, αυτό σημαίνει ότι δεν θα κοινοποιήσει τα προσωπικά σας στοιχεία σε κανέναν.



Διάγραμμα 13: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες ότι αν δεν θα κοινοποιηθούν τα προσωπικά στοιχεία σε έναν ιστότοπο μέσω κοινωνικής δικτύωσης που έχει πολιτική απορρήτου.

14. Γνωρίζετε για το πόσο συχνά πρέπει να αλλάζετε τον κωδικό πρόσβασής σας;

Τα αποτελέσματα της έρευνας δείχνουν υψηλό ποσοστό 64,8% στο μια φορά το χρόνο με 138 απαντήσεις. Έπειτα το 17,8% απάντησε μια φορά το μήνα με 38 απαντήσεις, το 13,1% απάντησε ότι δεν γνωρίζει με 28 απαντήσεις και 4,1% απάντησε κάθε μέρα με 9 απαντήσεις.

Πίνακας 14: Γνωρίζετε για το πόσο συχνά πρέπει να αλλάζετε τον κωδικό πρόσβασής σας;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Δεν γνωρίζω	28	13,1	13,1	13,1
	Κάθε μέρα	9	4,2	4,2	17,4
	Μια φορά το μήνα	38	17,8	17,8	35,2
	Μια φορά το χρόνο	138	64,8	64,8	100,0
	Total	213	100,0	100,0	



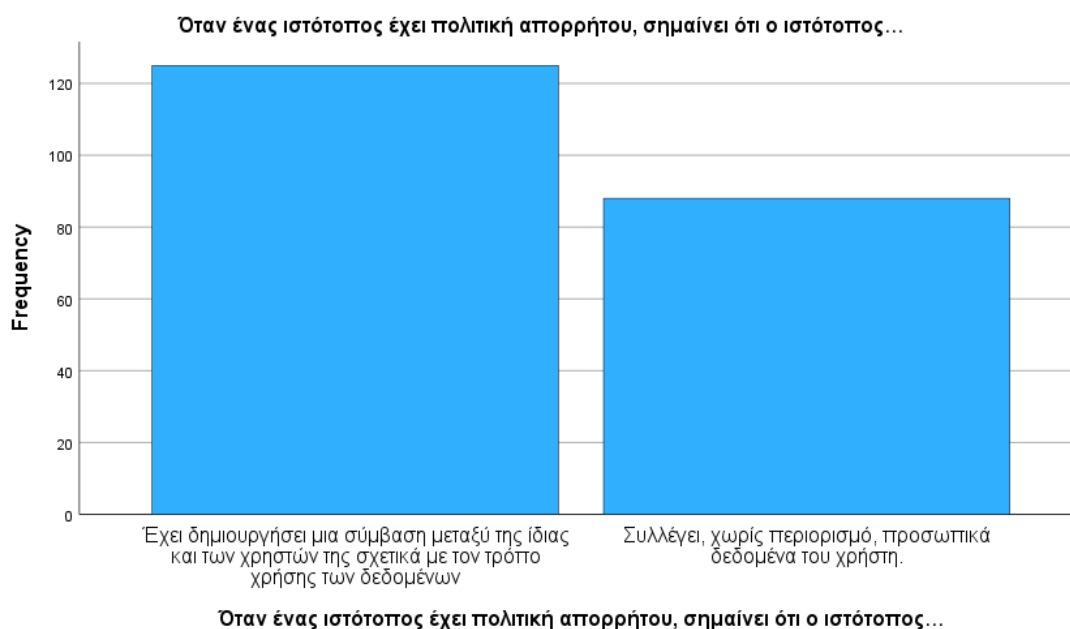
Διάγραμμα 14: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες πόσο συχνά πρέπει να αλλάζουν τον κωδικό πρόσβασης τους.

15. Όταν ένας ιστότοπος έχει πολιτική απορρήτου, σημαίνει ότι ο ιστότοπος...

Στην συνέχεια στην ερώτηση «Όταν ένας ιστότοπος έχει πολιτική απορρήτου σημαίνει ότι ο ιστότοπος...», μεγάλο ποσοστό των χρηστών (58,7%) απάντησε ότι έχει δημιουργήσει μια σύμβαση μεταξύ της ίδιας και των χρηστών της σχετικά με τον τρόπο χρήσης των δεδομένων τους με 125 απαντήσεις και 41,3% απάντησε συλλέγει χωρίς περιορισμό προσωπικά δεδομένα του χρήστη με 88 απαντήσεις.

Πίνακας 15: Όταν ένας ιστότοπος έχει πολιτική απορρήτου, σημαίνει ότι ο ιστότοπος...

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Έχει δημιουργήσει μια σύμβαση μεταξύ της ίδιας και των χρηστών της σχετικά με τον τρόπο χρήσης των δεδομένων τους	125	58,7	58,7	58,7
	Συλλέγει, χωρίς περιορισμό, προσωπικά δεδομένα του χρήστη.	88	41,3	41,3	100,0
Total		213	100,0	100,0	



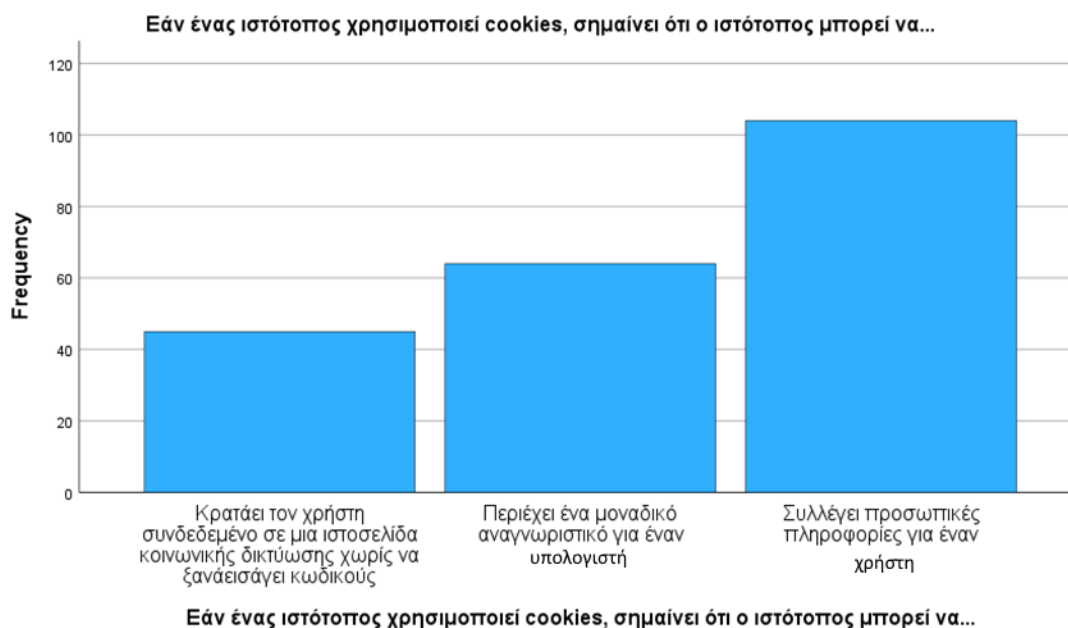
Διάγραμμα 15: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες τι είναι η πολιτική απορρήτου σε έναν ιστότοπο.

16. Εάν ένας ιστότοπος χρησιμοποιεί cookies, σημαίνει ότι ο ιστότοπος μπορεί να...

Στα αποτελέσματα στην ερώτηση «Εάν ένας ιστότοπος χρησιμοποιεί cookies, σημαίνει ότι ο ιστότοπος μπορεί να...», βλέπουμε ότι το μεγαλύτερο ποσοστό (48,8%) έχει απαντήσει πως συλλέγει προσωπικές πληροφορίες για έναν χρήστη, το 30% απάντησε πως περιέχει ένα μοναδικό αναγνωριστικό για έναν υπολογιστή και τέλος το 21,1% απάντησε ότι κρατάει τον χρήστη συνδεδεμένο σε μια ιστοσελίδα κοινωνικής δικτύωσης χωρίς να ξαναεισάγει κωδικούς πρόσβασης.

Πίνακας 16: Εάν ένας ιστότοπος χρησιμοποιεί cookies, σημαίνει ότι ο ιστότοπος μπορεί να...

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Κρατάει τον χρήστη συνδεδεμένο σε μια ιστοσελίδα κοινωνικής δικτύωσης χωρίς να ξαναεισάγει κωδικούς πρόσβασης	45	21,1	21,1	21,1
	Περιέχει ένα μοναδικό αναγνωριστικό για έναν υπολογιστή	64	30,0	30,0	51,2
	Συλλέγει προσωπικές πληροφορίες για έναν χρήστη	104	48,8	48,8	100,0
	Total	213	100,0	100,0	



Διάγραμμα 16: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες τι κάνουν τα cookies σε έναν ιστότοπο.

17. Γνωρίζετε αν η νομοθεσία καλύπτει την προστασία των προσωπικών σας δεδομένων επαρκώς;

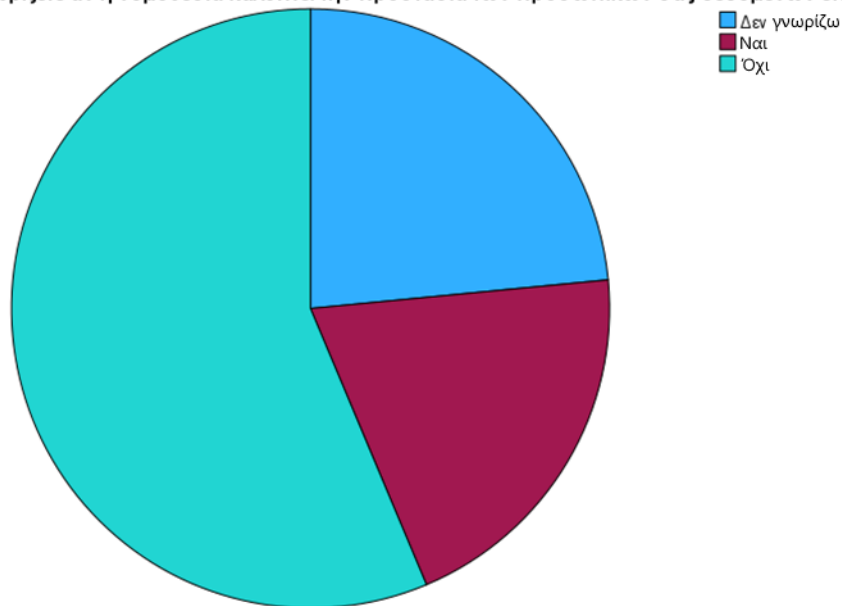
Τα αποτελέσματα της έρευνας δείχνουν πως το 56,3% απάντησε όχι με 120 απαντήσεις, το 23,5 % πως δεν γνωρίζει αν η νομοθεσία καλύπτει την προστασία των προσωπικών δεδομένων επαρκώς (50 απαντήσεις) και το 20,2% απάντησε ναι με 43 απαντήσεις.

Πίνακας 17: Γνωρίζετε αν η νομοθεσία καλύπτει την προστασία των προσωπικών σας δεδομένων επαρκώς;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Δεν γνωρίζω	50	23,5	23,5	23,5
	Ναι	43	20,2	20,2	43,7

Όχι	120	56,3	56,3	100,0
Total	213	100,0	100,0	

Γνωρίζετε αν η νομοθεσία καλύπτει την προστασία των προσωπικών σας δεδομένων επαρκώς;



Διάγραμμα 17: Κατανομή δείγματος ως προς το αν γνωρίζουν οι ερωτηθέντες αν η νομοθεσία τους προστατεύει τα προσωπικά δεδομένα με επάρκεια.

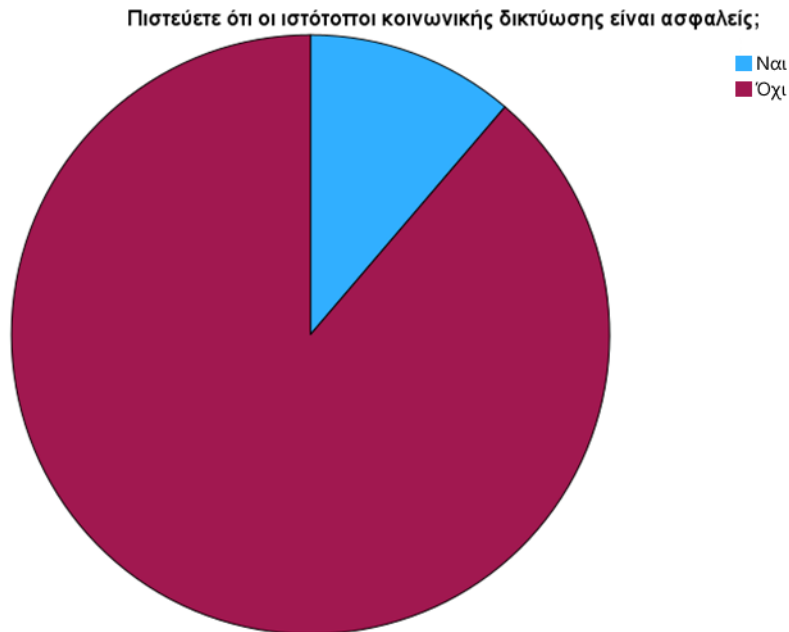
18. Πιστεύετε ότι οι ιστότοποι κοινωνικής δικτύωσης είναι ασφαλείς;

Στην ερώτηση αυτήν, το μεγαλύτερο ποσοστό (88,7%) με 189 απαντήσεις δήλωσε όχι και το 11,3% με 24 απαντήσεις δήλωσαν ναι.

Πίνακας 18: Πιστεύετε ότι οι ιστότοποι κοινωνικής δικτύωσης είναι ασφαλείς;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	24	11,3	11,3	11,3

Όχι	189	88,7	88,7	100,0
Total	213	100,0	100,0	



Διάγραμμα 18: Κατανομή δείγματος ως προς το αν πιστεύουν οι ερωτηθέντες ότι οι ιστότοποι μέσω κοινωνικής δικτύωσης είναι ασφαλείς.

Ενοτητα Δ (Θέματα γενικού ενδιαφέροντος για τα μέσα κοινωνικής δικτύωσης)

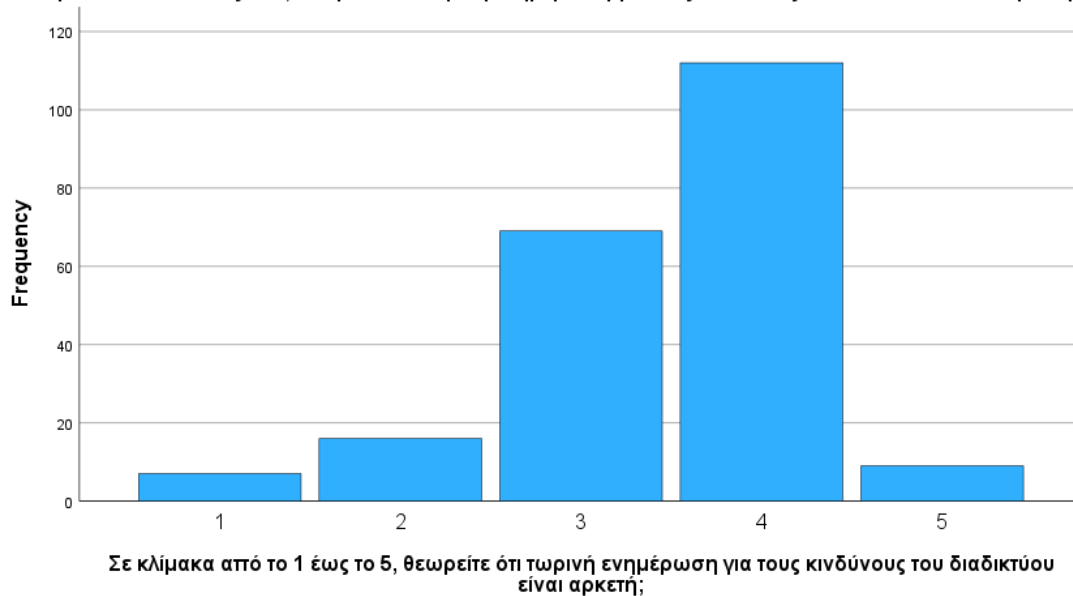
19. Σε κλίμακα από το 1 έως το 5, θεωρείτε ότι τωρινή ενημέρωση για τους κινδύνους του διαδικτύου είναι αρκετή;

Στην ερώτηση αυτή, τα μεγαλύτερα ποσοστά τείνουν προς την υψηλή ενημέρωση για τους κινδύνους. Σε κλίμακα από το 1 (χαμηλή ενημέρωση) έως το 5 (υψηλή ενημέρωση) οι περισσότεροι χρήστες (52,6%) απάντησαν το 4 με 112 απαντήσεις έπειτα με 32,4% το 3 με 69 απαντήσεις, το 7,5% το 2 και ένα μικρότερο ποσοστό 4,2% το 5 και 3,3% το 1.

Πίνακας 19: Σε κλίμακα από το 1 έως το 5, θεωρείτε ότι τωρινή ενημέρωση για τους κινδύνους του διαδικτύου είναι αρκετή;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	7	3,3	3,3	3,3
	2	16	7,5	7,5	10,8
	3	69	32,4	32,4	43,2
	4	112	52,6	52,6	95,8
	5	9	4,2	4,2	100,0
	Total	213	100,0	100,0	

Σε κλίμακα από το 1 έως το 5, θεωρείτε ότι τωρινή ενημέρωση για τους κινδύνους του διαδικτύου είναι αρκετή;



Διάγραμμα 19: Κατανομή δείγματος ως προς την ικανοποίηση των ερωτηθέντων για την τωρινή ενημέρωση για τους κινδύνους του Διαδικτύου.

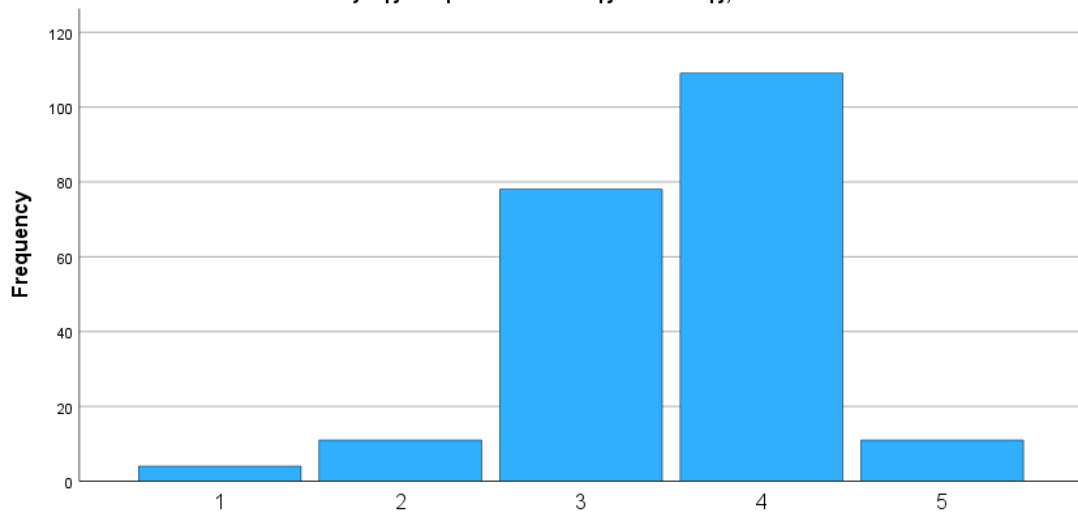
20. Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης ;

Ο βαθμός ανησυχίας των χρηστών σχετικά με την προστασία της ιδιωτικής τους ζωής στα μέσα κοινωνικής δικτύωσης εμφανίζεται σε μεγάλο βαθμό καθώς τα μεγαλύτερα ποσοστά δείχνουν υψηλή ανησυχία σε κλίμακα από το ένα (χαμηλή ανησυχία) ως το 5 (υψηλή ανησυχία). Οι περισσότεροι χρήστες απάντησαν το 4 με 51,2%, έπειτα το 36,6% απάντησε το 3, 10,1 % απάντησαν το 2 και το 5 (5,2% και για τις δύο ομάδες) και ένα μικρό ποσοστό (1,9%) το 1. Το γεγονός αυτό δείχνει πως οι περισσότεροι χρήστες γνωρίζουν τους κινδύνους και μόνο ένα μικρό ποσοστό δεν έχει μεγάλη ανησυχία.

Πίνακας 20: Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	1,9	1,9	1,9
	2	11	5,2	5,2	7,0
	3	78	36,6	36,6	43,7
	4	109	51,2	51,2	94,8
	5	11	5,2	5,2	100,0
	Total	213	100,0	100,0	

Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης;



Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης;

Διάγραμμα 20: Κατανομή δείγματος ως προς την ανησυχία των ερωτηθέντων για την προστασία της ιδιωτικής τους ζωής στα μέσα κοινωνικής δικτύωσης.

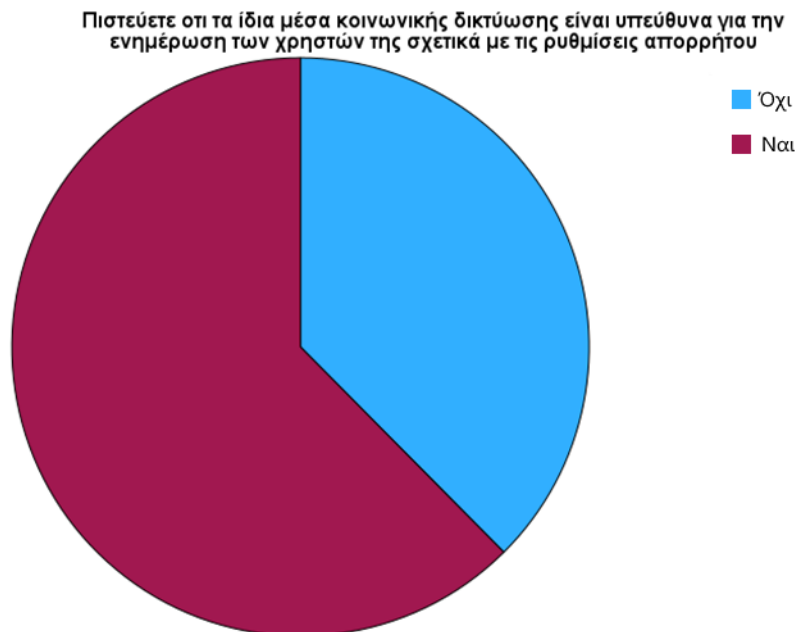
21. Πιστεύετε ότι τα ίδια μέσα κοινωνικής δικτύωσης είναι υπεύθυνα για την ενημέρωση των χρηστών της σχετικά με τις ρυθμίσεις απορρήτου;

Στο παρακάτω διάγραμμα παρατηρούμε πώς οι ερωτηθέντες δεν πιστεύουν ότι τα ίδια τα μέσα κοινωνικής δικτύωσης είναι υπεύθυνα για την ενημέρωση των χρηστών σχετικά με τις ρυθμίσεις του απορρήτου ποσοστό καθώς το 62,4% απάντησε όχι και το 37,6% απάντησε ναι.

Πίνακας 21: Πιστεύετε ότι τα ίδια μέσα κοινωνικής δικτύωσης είναι υπεύθυνα για την ενημέρωση των χρηστών της σχετικά με τις ρυθμίσεις απορρήτου;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	80	37,6	37,6	37,6
	Όχι	133	62,4	62,4	100,0

Total	213	100,0	100,0
-------	-----	-------	-------



Διάγραμμα 21: Κατανομή δείγματος ως προς αν πιστεύουν οι ερωτηθέντες για ότι τα ίδια τα μέσα κοινωνικής δικτύωσης πρέπει να είναι υπεύθυνα για την ενημέρωση των χρηστών σχετικά με τις ρυθμίσεις απορρήτου.

22. Θεωρείτε τον εθισμό στα μέσα κοινωνικής δικτύωσης εξίσου σημαντικό με την προστασία προσωπικών δεδομένων εφόσον μπορεί να την επηρεάσει;

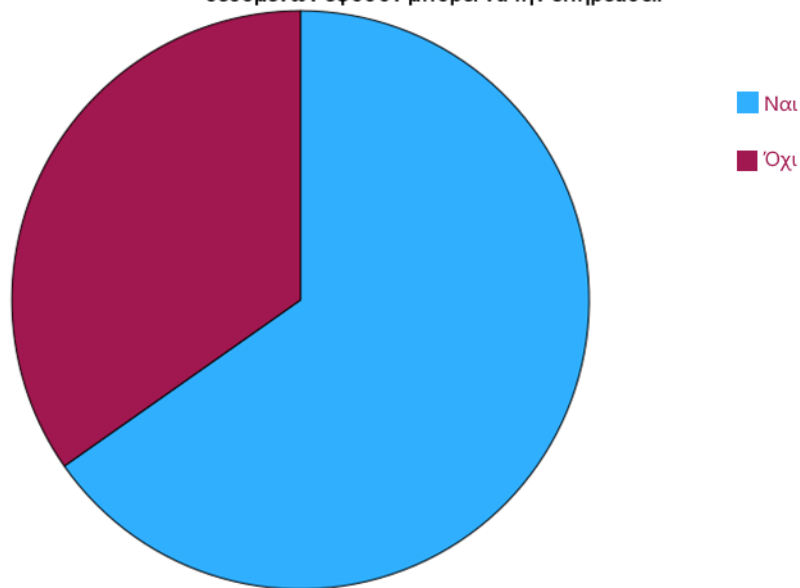
Στην επόμενη ερώτηση ένα μεγάλο ποσοστό (65,3%) απάντησε πως μπορεί να την επηρεάσει (ναι) και το 34,7% απάντησε όχι.

Πίνακας 22: Θεωρείτε τον εθισμό στα μέσα κοινωνικής δικτύωσης εξίσου σημαντικό με την προστασία προσωπικών δεδομένων εφόσον μπορεί να την επηρεάσει;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	139	65,3	65,3	65,3

Όχι	74	34,7	34,7	100,0
Total	213	100,0	100,0	

Θεωρείτε τον εθισμό στα μέσα κοινωνικής δικτύωσης εξίσου σημαντικό με την προστασία προσωπικών δεδομένων εφόσον μπορεί να την επηρεάσει.



Διάγραμμα 22: Κατανομή δείγματος ως προς αν θεωρούν οι ερωτηθέντες ότι ο εθισμός στα μέσα κοινωνικής δικτύωσης έχει ρόλο στο να επηρεάσει την προστασία των προσωπικών δεδομένων.

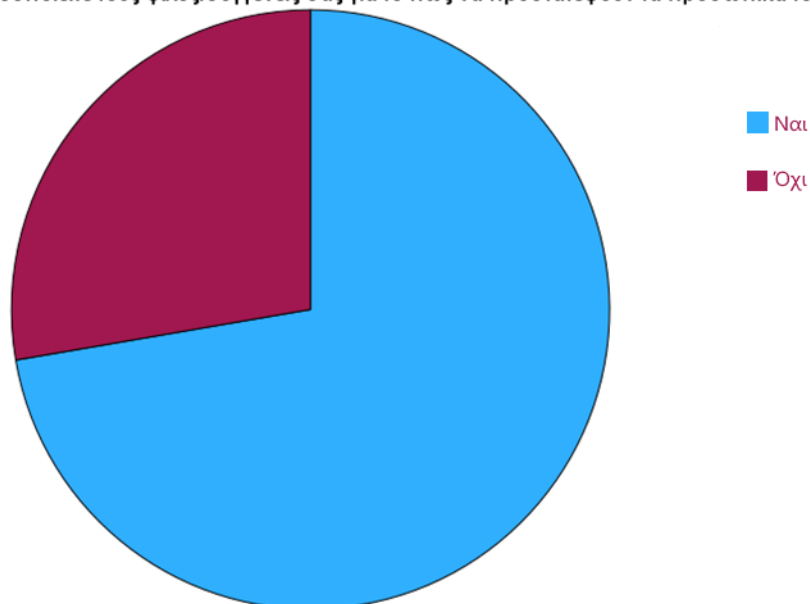
23. Προειδοποιείτε τους φίλους/συγγενείς σας για το πως να προστατέψουν τα προσωπικά τους δεδομένα;

Η πλειοψηφία των ερωτηθέντων δήλωσε πως προτρέπουν τους φίλους/συγγενείς να προστατέψουν τα προσωπικά τους δεδομένα απαντώντας ναι (72,3%) ενώ το 27,7% απάντησε όχι.

Πίνακας 23: Προειδοποιείτε τους φίλος/συγγενείς σας για το πως να προστατέψουν τα προσωπικά τους δεδομένα;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	154	72,3	72,3	72,3
	Όχι	59	27,7	27,7	100,0
	Total	213	100,0	100,0	

Προειδοποιείτε τους φίλους/συγγενείς σας για το πως να προστατέψουν τα προσωπικά τους δεδομένα;



Διάγραμμα 23: Κατανομή δείγματος ως προς οι ερωτηθέντες ενημερώνουν φίλους ή και συγγενείς για την ασφάλεια των προσωπικών τους δεδομένων.

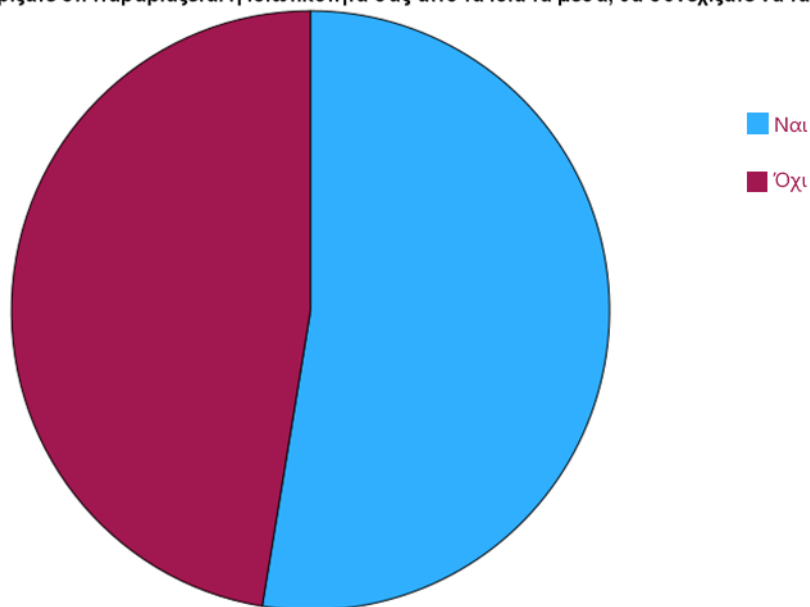
24. Εάν γνωρίζατε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζατε να τα χρησιμοποιείτε;

Τέλος, σε αυτή τη σημαντική ερώτηση, η πλειοψηφία (52,6%) απάντησαν ναι ενώ το 47,4% απάντησε όχι.

Πίνακας 24: Εάν γνωρίζατε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζατε να τα χρησιμοποιείτε;

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ναι	112	52,6	52,6	52,6
	Όχι	101	47,4	47,4	100,0
	Total	213	100,0	100,0	

Εάν γνωρίζατε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζατε να τα χρησιμοποιείτε;



Διάγραμμα 24: Κατανομή δείγματος ως προς αν οι ερωτηθέντες θα συνέχιζαν να χρησιμοποιούν ένα συγκεκριμένο μέσο κοινωνικής δικτύωσης παρά το γεγονός ότι παραβιάζεται η ιδιωτικότητά τους.

Συμπεράσματα και προτάσεις

Συμπερασματικά, η εξέλιξη της τεχνολογίας έχει επηρεάσει σημαντικά την κοινωνία καθώς τα κοινωνικά δίκτυα αποτελούν ένα βασικό κομμάτι στην καθημερινή ζωή των ανθρώπων. Η κυριαρχία των μέσων κοινωνικής δικτύωσης έφερε στην επιφάνεια ένα άλλο σημαντικό πρόβλημα που έχει να κάνει με τον περιορισμό και την απώλεια της ιδιωτικότητας. Ως συνέπεια, η ασφάλεια των πληροφοριών των χρηστών έχει μειωθεί εξαιτίας των παραβιάσεων που κάνουν διάφοροι ιστότοποι κοινωνικής δικτύωσης. Οι πλατφόρμες των μέσων κοινωνικής δικτύωσης πρέπει να εφαρμόσουν μέτρα

προστασίας τα οποία είναι απαραίτητα να υπάρχουν διαρκώς για την βελτίωση της ασφάλειας των χρηστών και της διασφάλισης της ιδιωτικότητάς τους. Τα αποτελέσματα της έρευνας έδειξαν πως ένα μεγάλο ποσοστό χρηστών των μέσων κοινωνικής δικτύωσης δεν προσέχουν αρκετά. Επίσης, η παραβίαση προσωπικών δεδομένων αποτελεί ένα σοβαρό ζήτημα και χρειάζεται μεγάλη προσοχή. Ωστόσο, τα μέσα κοινωνικών δικτύων πρέπει να προστατεύουν αυτά τα δεδομένα και να ακολουθούν βασικές αρχές προστασίας των προσωπικών δεδομένων. Οι ανησυχίες των χρηστών έχουν επίσης αυξηθεί λόγω της εμφάνισης όλο και περισσότερων κινδύνων που υπάρχουν στα μέσα κοινωνικών δικτύων.

Οι ιστοσελίδες κοινωνικής δικτύωσης μέσα από την πολιτική απορρήτου, η οποία πρέπει πάντα να είναι διαθέσιμη στο διαδίκτυο, ξεκαθαρίζουν τη θέση και τη στάση τους απέναντι σε θέματα που έχουν να κάνουν με την ιδιωτικότητα των χρηστών.

Βέβαια, υπάρχουν κάποιες προτάσεις σχετικά με τη σωστή χρήση των προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης.

- ❖ Θα πρέπει να μην δημοσιεύονται ευαίσθητες πληροφορίες που έχουν να κάνουν με τον αριθμό τηλεφώνου, διεύθυνση κατοικίας κ.λπ.
- ❖ Καμία προσωπική πληροφορία δεν θα πρέπει να δίνεται χωρίς άδεια και χωρίς καλό λόγο από τον ίδιο τον χρήστη.
- ❖ Θα πρέπει να γίνεται η επιλογή ισχυρού κωδικού πρόσβασης και να γίνεται επίσης η συχνή αλλαγή του. Με τη χρήση πολύπλοκων κωδικών θα είναι δύσκολο για κάποιους να μαντέψουν (μέσω ονομάτων ή ημερομηνιών) ή να βρουν μέσω εξαντλητικής δοκιμής κωδικούς χρηστών. Αν δίνεται η δυνατότητα, προτείνεται και η ενεργοποίηση επαλήθευσης δύο παραγόντων ή «Two-Factor Authentication» (2FA) που κάνει την ανεπιθύμητη πρόσβαση σε λογαριασμό ενός χρήστη πιο δύσκολη.
- ❖ Να υπάρχει συχνή ενημέρωση για τις πολιτικές απορρήτου και τους όρους χρήσης των πλατφόρμων κοινωνικής δικτύωσης για τις αλλαγές που κάνουν οι ιστότοποι αυτοί σχετικά με τα προσωπικά δεδομένα, όπως είναι τα cookies κ.λπ.
- ❖ Να μην δημοσιεύονται προσωπικές πληροφορίες που έχουν να κάνουν με την ασφάλεια.

- ❖ Αποφυγή αποδοχής αιτημάτων φιλιών από άγνωστα άτομα καθώς η επικοινωνία με αυτά μπορεί να είναι επικίνδυνη και να οδηγήσει σε συλλογή προσωπικών πληροφοριών.
- ❖ Προτείνεται να χρησιμοποιείται λογισμικό ασφάλειας (anti-malware, anti-virus κ.λπ.) αλλά και να γίνεται η συχνή αναβάθμιση του λογισμικού του υπολογιστή σας που με τις οποίες λύνονται διάφορα προβλήματα που προκαλούν ευπάθειες.
- ❖ Θα πρέπει να υπάρχει ενημέρωση σχετικά με τη χρήση των μέσων κοινωνικής δικτύωσης ώστε να γίνεται η χρήση τους με μεγαλύτερη ασφάλεια.
- ❖ Όταν γίνεται σύνδεση στο προσωπικό σας λογαριασμό σε ηλεκτρονικές συσκευές τρίτων ατόμων θα πρέπει μετά να γίνεται αποσύνδεση από αυτές τις συσκευές.
- ❖ Θα πρέπει να είμαστε προσεκτικοί με διάφορους άγνωστους συνδέσμους που μπορεί να στείλει κάποιος γιατί μπορεί να αποτελούν τρόπο με τον οποίο διάφοροι hackers προσπαθούν να κλέψουν προσωπικά δεδομένα.
- ❖ Ιδανικά θα έπρεπε να αποφεύγεται η δημοσίευση κάθε προσωπικού στοιχείου όπως η διεύθυνση αλλά και την καθημερινότητα μας, καθώς τέτοια στοιχεία μπορούν να χρησιμοποιηθούν ως ενδείξεις για να αποσπάσουν κακόβουλοι και άλλες πληροφορίες.

Αν ο κάθε χρήστης ακολουθούσε αυτές τις συμβουλές, θα μπορούσε να εξασφαλίσει μεγαλύτερη ασφάλεια στα προσωπικά του δεδομένα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ανάκτηση από Τεχνολογική εξέλιξη, θετικές & αρνητικές επιπτώσεις στην κοινωνία μας (πρόσβαση 19 Μάιου 2023): <https://spartan.gr/news/tecnologiki-ekseliksi-thetikes-arnitikes-epiptoseis-stin-koinonia-mas>
- Alexander, R. (2021, Απρίλιος). *Διαφορά μεταξύ Web 1.0 και Web 2.0 και Web 3.0.* (πρόσβαση 1 Μάιου 2023 <https://el.strephonsays.com/web-1-0-and-vs-web-2-0-and-vs-web-3-0-12872>)
- Casey Newton. (2017). *An Instagram hack hit millions of accounts, and victims' phone numbers are now for sale.* (πρόσβαση 30 Ιουλίου 2023) <https://www.theverge.com/2017/9/1/16244304/instagram-hack-api-bug-doxagram-selena-gomez>
- Categorization of Social Media.* (πρόσβαση 2 Μάιου 2023) <https://atallen.wordpress.com/2011/01/24/categorization-of-social-media/>
- Choudhury, N. *World Wide Web and Its Journey from Web 1.0 to Web 4.0 .* (πρόσβαση 30 Μάιου 2023) <https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf>
- CNN. *Οι 10 υποθέσεις παραβίασης προσωπικών δεδομένων που συγκλόνισαν τον κόσμο.* (πρόσβαση 30 Ιουνίου 2023) <https://www.cnn.gr/kosmos/story/131498/oi-10-ypotheseis-paraviasis-prosopikon-dedomenon-poy-sygklonisan-ton-kosmo>
- Fogg, S. (2021, Οκτώβριος 15). *What Are Cookies? A Helpful Guide to Internet & Computer Cookies.* (πρόσβαση 1 Αυγούστου 2023) <https://termly.io/resources/articles/what-are-cookies/>
- HUSSAIN, A. (2022). *What Is Identity Theft? Definition, Types, and Examples.* (πρόσβαση 15 Αυγούστου 2023) <https://www.investopedia.com/terms/i/identitytheft.asp>
- Isaacson, W. (2015, Οκτώβριος). *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution Paperback.*

- KOZLOWSKA, I. (2018). *Facebook and Data Privacy in the Age of Cambridge Analytica*. (πρόσβαση 2 Αυγούστου 2023) <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/>
- Mayfield, A. *what is social media*. (πρόσβαση 20 Μαΐου 2023) http://crmexchange.com/uploadedFiles/White_Papers/PDF/What_is_Social_Media_iCrossing_ebook.pdf
- Meredith, S. *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*. (πρόσβαση 3 Αυγούστου 2023) <https://www.cnbc.com/2018/04/10/facebookcambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>.
- Myspace*. (πρόσβαση 24 Μαΐου 2023) <https://www.britannica.com/topic/Myspace>
- Οδηγία 2006/24/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων*. (πρόσβαση 2 Ιουνίου 2023) <https://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX%3A32006L0024>
- Stumbles, T. (2018, February). *History of YouTube: a timeline*. (πρόσβαση 25 Μαΐου 2023) <https://www.officetimeline.com/blog/youtube-history-timeline>
- The History of Reddit*. (πρόσβαση 24 Μαΐου 2023) <https://www.honorsociety.org/articles/history-reddit>
- The Role Of Social Media In Education*. (πρόσβαση 19 Αυγούστου 2023) <https://www.jbcnschool.edu.in/blog/social-media-in-education/>
- Twitter Investigation Report*. (πρόσβαση 27 Μαΐου 2023) https://www.dfs.ny.gov/Twitter_Report?fbclid=IwAR3iKe5H2v6BQ-eIPfIxnNVo2iljoKQzahEqHdRmp50YWX6lQHvJey33JQk
- Web 3.0 έναντι Web 2.0: κύριες διαφορές*. (πρόσβαση 4 Μαΐου 2023) <https://www.informatique-mania.com/el/linternet/web-3-0-vs-web-2-0-principales-differencesslug/>

- What Are The Types of Social Media?* (πρόσβαση 30 Μαΐου 2023)
<https://blog.digimind.com/en/insight-driven-marketing/what-are-the-types-of-social-media>
- What is Data Leakage?* (πρόσβαση 5 Αυγούστου 2023)
<https://www.forcepoint.com/cyber-edu/data-leakage>
- Wikipedia. *California Consumer Privacy Act*. (πρόσβαση 1 Σεπτεμβρίου 2023)
https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act
- Wikipedia. *Clickjacking*. (πρόσβαση 13 Αυγούστου 2023)
<https://en.wikipedia.org/wiki/Clickjacking>
- Wikipedia. *Cross-site scripting*. (πρόσβαση 11 Αυγούστου 2023)
https://en.wikipedia.org/wiki/Cross-site_scripting
- Wikipedia. *Facebook*. (πρόσβαση 1 Μαΐου 2023)
<https://en.wikipedia.org/wiki/Facebook>
- Wikipedia. *Friendster*. (πρόσβαση 1 Μαΐου 2023)
<https://en.wikipedia.org/wiki/Friendster>
- Wikipedia. *Hi5* . (πρόσβαση 1 Ιουλίου 2023) <https://en.wikipedia.org/wiki/Hi5>
- Wikipedia. *Instagram*. (πρόσβαση 1 Μαΐου 2023)
<https://en.wikipedia.org/wiki/Instagram>
- Wikipedia. *Internet privacy*. (πρόσβαση 5 Ιουλίου 2023)
https://en.wikipedia.org/wiki/Internet_privacy
- Wikipedia. *LinkedIn*. (πρόσβαση 2 Μαΐου 2023)
<https://en.wikipedia.org/wiki/LinkedIn>
- Wikipedia. *LiveJournal*. (πρόσβαση 5 Μαΐου 2023)
<https://en.wikipedia.org/wiki/LiveJournal>
- Wikipedia. *Phishing*. (πρόσβαση 27 Αυγούστου 2023)
<https://el.wikipedia.org/wiki/Phishing>

- Wikipedia. *Pinterest*. (πρόσβαση 3 Μαΐου 2023)
<https://en.wikipedia.org/wiki/Pinterest>
- Wikipedia. *Privacy-enhancing technologies*. (πρόσβαση 19 Ιουλίου 2023)
https://en.wikipedia.org/wiki/Privacy-enhancing_technologies
- Wikipedia *SixDegrees.com*. (πρόσβαση 1 Μάιου 2023)
<https://en.wikipedia.org/wiki/SixDegrees.com>
- Wikipedia. *Snapchat*. (πρόσβαση 16 Μαΐου 2023)
<https://en.wikipedia.org/wiki/Snapchat>
- Wikipedia. *Social media*. (πρόσβαση 28 Μαρτίου 2023)
https://en.wikipedia.org/wiki/Social_media#cite_note-1
- Wikipedia. *Tik Tok*. (πρόσβαση 4 Μαΐου 2023) <https://en.wikipedia.org/wiki/TikTok>
- Wikipedia. *Twitter*. (πρόσβαση 8 Μάιου 2023) <https://en.wikipedia.org/wiki/Twitter>
- Wikipedia. (πρόσβαση 27 Μαρτίου 2023) *World Wide Web*. Ανάκτηση από
https://en.wikipedia.org/wiki/World_Wide_Web
- Wikipedia. (πρόσβαση 2023) *Ιστορία του Διαδικτύου*. Ανάκτηση από
https://el.wikipedia.org/wiki/%CE%99%CF%83%CF%84%CE%BF%CF%81%CE%AF%CE%B1_%CF%84%CE%BF%CF%85_%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85
- Wikipedia. *Κακόβουλο λογισμικό*.
https://el.wikipedia.org/wiki/%CE%9A%CE%B1%CE%BA%CF%8C%CE%B2%CE%BF%CF%85%CE%BB%CE%BF_%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CF%8C
- Zuckerberg, M. (2018, March 21). *I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue. We have a responsibility to protect your data, and if we can't then we* [Facebook status update].
<https://www.facebook.com/zuck/posts/10104712037900071?pnref=story>

Άρθρο 2 - Νόμος 2472/1997 - Ορισμοί. <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-2472-1997/arthro-2-nomos-2472-1997-orismoι>

Άρθρο 4 – Γενικός Κανονισμός για την Προστασία Δεδομένων – Ορισμοί. <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679>

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). <https://www.uoi.gr/dioikisi/gdpr/>

Επεξεργασία δεδομένων προσωπικού χαρακτήρα. <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:114012>

Ζ.Παπαμήτσου, Α. Β. (2012, Μάιος). ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΑΓΚΟΣΜΙΟΥ ΙΣΤΟΥ. Αθήνα.

Ζαφειρόπουλος, Κ. (2015). Πως γίνεται μια επιστημονική εργασία. ΚΡΙΤΙΚΗ .

Η αξία των μέσων κοινωνικής δικτύωσης για μια επιχείρηση. <https://www.cactusweb.gr/%CE%B7-%CE%B1%CE%BE%CE%AF%CE%B1-%CF%84%CF%89%CE%BD-%CE%BC%CE%AD%CF%83%CF%89%CE%BD-%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE%CF%82-%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CF%83%CE%B7%CF%82/>

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/. (χ.χ.). *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, (πρόσβαση 25 Αυγούστου 2023) <https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679>.

Καρακώστας, Ι. Κ. (2012, Νοέμβριος). *Το Δίκαιο των ΜΜΕ*. Αθήνα.

Κατηγορίες μέσων κοινωνικής δικτύωσης. (πρόσβαση 1 Αυγούστου 2023) Ανάκτηση από <https://worktime.gr/katigories-meson-koinonikis-diktyos/>

Κουτσαμπλασης, Π. (2011). ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΑΝΘΡΩΠΟΥ –ΥΠΟΛΟΓΙΣΤΗ: Αρχές, Μεθοδοί και Παραδείγματα. Στο Κ. Π., *ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΑΝΘΡΩΠΟΥ –ΥΠΟΛΟΓΙΣΤΗ: Αρχές, Μεθοδοί και Παραδείγματα* (σσ. 40-42). Αθήνα: Κλειδάριθμος.

Νομοθεσία προσωπικών δεδομένων. (πρόσβαση 20 Αυγούστου 2023) Ανάκτηση από https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpika/nomothesia_prwso pikwn

ΝΟΜΟΣ 3471/2006. (πρόσβαση 21 Αυγούστου 2023) <https://www.kodiko.gr/nomothesia/document/155678/nomos-3471-2006#:~:text=%CE%A3%CE%BA%CE%BF%CF%80%CF%8C%CF%82%20%CF%84%CF%89%CE%BD%20%CE%B4%CE%B9%CE%B1%CF%84%CE%AC%CE%BE%CE%B5%CF%89%CE%BD%20%CF%84%CF%89%CE%BD%20%CE%AC%CF%81%CE%B8%CF%81%CF%89%CE%BD,%CF%83%>

ΝΟΜΟΣ 4624/2019. (πρόσβαση 22 Αυγούστου 2023) <https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019>

Αστανάστας, Ε. (2015). Τα 4 είδη Malware (κακόβουλα λογισμικά) που κυκλοφορούν σήμερα. (πρόσβαση 29 Αυγούστου 2023) <https://www.safer-internet.gr/ta-4-eidi-malware-pou-kukloforoun/>

Οδηγία 97/66/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. (πρόσβαση 24 Αυγούστου 2023) <https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A31997L0066>

Πλεονεκτήματα και μειονεκτήματα των κοινωνικών δικτύων. (πρόσβαση 21 Ιουλίου 2023) <https://el.economy-pedia.com/11030785-advantages-and-disadvantages-of-social-networks>

Τί είναι η ιδιωτικότητα;. (πρόσβαση 11 Ιουλίου 2023) <https://antiauthor.wordpress.com/2011/08/06/%CF%84%CE%AF-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7->

%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1/

Τι είναι τα cookies;. (2018, Νοεμβρίου 25). (πρόσβαση 2 Ιουλίου 2023)
<https://www.homodigitalis.gr/posts/3079>

Τι είναι το Phishing και ποιές οι τεχνικές του ηλεκτρονικού “ψαρέματος”;. (πρόσβαση 2 Ιουλίου 2023) <https://www.tsouk.gr/ti-einai-to-phishing-kai-poiies-oi-technikes-toy-ilektronikoy-psarematos/>

Φιλάνδρας, Κ. (χ.χ.). Προσωπικά δεδομένα και ποινικό δίκαιο. (πρόσβαση 27 Αυγούστου 2023)

<https://www.mcaounilaw.gr/%CE%BD%CE%B5%CE%B1/494-%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1-%CE%BA%CE%B1%CE%B9-%CF%80%CE%BF%CE%B9%CE%BD%CE%B9%CE%BA%CF%8C-%CE%B4%CE%AF%CE%BA%CE%B1%CE%B9%CE%BF>

Κωνσταντινίδου, Μ. (2017). Η ασφάλεια των προσωπικών δεδομένων στα κοινωνικά δίκτυα στην Ελλάδα (Διπλωματική εργασία). Πανεπιστήμιο Πελοποννήσου, Τρίπολη.

<https://amitos.library.uop.gr/xmlui/bitstream/handle/123456789/3591/%CE%97%20%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%20%CF%84%CF%89%CE%BD%20%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD%20%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD%20%CF%83%CF%84%CE%B1%20%CE%BC%CE%AD%CF%83%CE%B1%20%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE%CF%82%20%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CF%83%CE%B7%CF%82%20%CF%83%CF%84%CE%B7%CE%BD%20%CE%95%CE%BB%CE%BB%CE%AC%CE%B4%CE%B1.pdf?sequence=1&isAllowed=y>

Μοσχοπούλου, Ε. (2022). ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΚΑΙ Η ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (Διπλωματική Εργασία). Πανεπιστήμιο Μακεδονίας, Θεσσαλονίκη.

<https://dspace.lib.uom.gr/bitstream/2159/26556/1/MoschopoulouEleniMsc2022.pdf>

Κόλλια Φ, Κονδυλίδου Ι, Γραμμένου Α, . (2021) “ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ” (Πτυχιακή Εργασία). Πανεπιστήμιο Πατρών, Πάτρα.

<http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/9583/1/%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1-%CF%83%CF%84%CE%B1-%CE%9C%CE%AD%CF%83%CE%B1-%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE%CF%82-%CE%94%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CF%83%CE%B7%CF%82-2-1-1%20%284%29.pdf?sequence=1&isAllowed=y>