# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών**
***Κοινωνικά Πληροφοριακά Συστήματα***


## Μεταπτυχιακή Διατριβή

# Κίνδυνοι που ελλοχεύουν από λανθασμένη ή απρόσεκτη χρήση κοινωνικών δικτύων


**Ελένη Στρατηγοπούλου**

**Επιβλέπων Καθηγητής**

**Κλήμης Νταλιάνης**



**Νοέμβριος 2019**

# Ανοικτό Πανεπιστήμιο Κύπρου

**Σχολή Θετικών και Εφαρμοσμένων Επιστημών**

**Μεταπτυχιακό Πρόγραμμα Σπουδών**

***Κοινωνικά Πληροφοριακά Συστήματα***


# Μεταπτυχιακή Διατριβή

## Κίνδυνοι που ελλοχεύουν από λανθασμένη ή απρόσεκτη χρήση κοινωνικών δικτύων


**Ελένη Στρατηγοπούλου**

**Επιβλέπων Καθηγητής**

**Κλήμης Νταλιάνης**



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα *Κοινωνικά Πληροφοριακά Συστήματα* από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

**Νοέμβριος 2019**

ΛΕΥΚΗ ΣΕΛΙΔΑ

## Περίληψη

Οι Ιστοσελίδες Κοινωνικής Δικτύωσης δεν αποτελούν μόνο τα πιο διαδεδομένα εργαλεία, για την επίτευξη της επικοινωνίας στην σημερινή ψηφιακή εποχή, αλλά επίσης αποτελούν και μια από τις πιο μεγάλες πηγές δεδομένων. Πολλά βέβαια τα οφέλη από τις εφαρμογές δεδομένων τόσο για τους απλούς χρήστες όσο και για τους επαγγελματίες κάθε είδους, αλλά επίσης πολλοί και οι κίνδυνοι, που η παραβίαση τους μπορεί να επιφέρει στους χρήστες των Ιστοσελίδων Κοινωνικής Δικτύωσης. Καθώς το ενδιαφέρον των χρηστών για την χρήση των Ιστοσελίδων Κοινωνικής Δικτύωσης αυξάνεται, αναλογικά αυξάνεται και η ανησυχία για τους κινδύνους που εγκυμονούν.

Οι κίνδυνοι βέβαια δεν αποτελούν νέο φαινόμενο. Υπήρχαν εκεί από την εμφάνιση του ανθρώπινου είδους, είτε ο κίνδυνος αφορούσε συνθήκες διαβίωσης, πολέμους επιδημίες κλπ, είτε οποιονδήποτε άλλο συνδεδεμένο με την κάθε εποχή κίνδυνο. Με την τεχνολογία ωστόσο ή έννοια του κινδύνου συνδέθηκε σύμφωνα με τους ερευνητές, με το "Risk Society" του Ulrich Beck ( 1992) και του Antony Giddens (1991).

Καθώς η τεχνολογία ενσωματώνεται στην Ελληνική Κοινωνία, είτε μέσω των υπολογιστών είτε μέσω φορητών συσκευών- κινητών τηλεφώνων ή και tablet-, αυξάνεται και η ανησυχία για τους κινδύνους που μπορούν να επέλθουν από την αλληλεπίδραση που επιτυγχάνεται μέσω αυτών (στατιστικές δείχνουν ότι πρόσβαση σε κινητά τηλέφωνα έχουν παιδιά από την ηλικία των 10 ετών). Η εξετασθείσα μελέτη της υπάρχουσας βιβλιογραφίας στην Ελλάδα εστιάζει κυρίως σε θέματα εθισμού αλλά και κινδύνους που αφορούν παιδιά και νέους.

Η παρούσα πτυχιακή εργασία σκοπό έχει να διερευνήσει τους κινδύνους που εγκυμονεί η Χρήση των Ιστοσελίδων Κοινωνικής Δικτύωσης στους ενήλικες χρήστες. Η μέθοδος της έρευνας είναι ποσοτική με την χρήση Ερωτηματολογίου στο Διαδίκτυο.

Στην διαδικασία αυτή και μέσα από τα στοιχεία της υλοποιηθείσας έρευνας, θα εντοπίσει την διείσδυση της Χρήσης των Ιστοσελίδων Κοινωνικής Δικτύωσης στους χρήστες του Διαδικτύου, θα εξετάσει τις συμπεριφορές των χρηστών που μπορούν να οδηγήσουν σε έκθεση σε κίνδυνο (θα εξετασθούν συμπεριφορές όπως της Αντίληψης του Κινδύνου, της ιδιωτικότητας/απόρρητο, της εμπιστοσύνης προς τις εταιρείες ΙΚΔ, την ανησυχία για την προστασία της ιδιωτικότητας, τον Αντιληπτό έλεγχο της πληροφορίας, της Αποκάλυψης Προσωπικών Πληροφοριών). Επίσης θα συσχετίσει συμπεριφορές και Κοινωνικό-Δημογραφικά στοιχεία των χρηστών, όπως και της έκθεσης σε Κίνδυνο και Κοινωνικό-Δημογραφικά Στοιχεία των χρηστών. Τα αποτελέσματα της παρούσας έρευνας δείχνουν ότι η έκθεση στον Κίνδυνο σε ΙΚΔ σχετίζεται με το φύλο και επίσης η Συμπεριφορά για την Ιδιωτικότητα και η Αποκάλυψη Προσωπικών Πληροφοριών σχετίζονται με την Ηλικία και σε επιμέρους ερωτήσεις και με το Μορφωτικό Επίπεδο.

## Summary

Social Networking Websites are not only the most widely used tools to facilitate communication in today's digital age, but they are also one of the biggest sources of Big Data. There are of course many benefits of data applications, for both ordinary users and professionals alike, but also there are many risks, that their breach can bring to users of Social Networking Sites. As users' interest in using Social Networking Websites grows, so does their concern about the risks they pose.

Risks are not, of course, a new phenomenon. They have been there since the emergence of the human species, whether the risk was related to living conditions, war epidemics e.t.c., or any other risk associated with each era. However, the concept of risk was associated with technology, according to researchers, with Ulrich Beck's "Risk Society" (1992) and Antony Giddens (1991).

As technology is incorporated into Greek society, either through computers or through mobile devices - mobile phones or tablets - there is also growing concern about the dangers that may arise from the interaction achieved through them (statistics show that access to mobile phones have children from the age of 10 years old). The current study of the existing literature in Greece focuses mainly on addiction issues and risks for children and young people.

The purpose of this thesis is to investigate the risks posed by the use of Social Networking Websites to adult users. The research method is quantitative using an online Questionnaire. In this process, and through the elements of the research conducted, it will identify the penetration of the use of Social Networking Websites to Internet users, examine the behaviors of users that may lead to risk exposure (behaviors such as Risk Taking will be examined, Privacy Behavior, Trust in SNS companies, Privacy Concern, Perceived Control of Information, Information Identity Disclosure). It will also correlate user behaviors and socio-demographic data, as well as exposure to risk and socio-demographic data of users. At the end we present the results of the findings of this research.

The results of the present study show that exposure to Risk in SNS is related to gender and also “Privacy Behavior” and Information Identity Disclosure are related to Age and to Individual Questions and Educational Level.

## Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους επιβλέποντες κκ. Γεώργιο Ερρίκο Χλαπάνη και Κλήμη Νταλιάνη, για την βοήθεια και τις συμβουλές που μου προσέφεραν στην εκπόνηση της μεταπτυχιακής διατριβής.

# Περιεχόμενα

# Κεφάλαιο 1

## 1.1 Εισαγωγή

Τα Διαδίκτυο και τα Κοινωνικά Δίκτυα αποτελούν μέρος της καθημερινότητας ενός μεγάλου μέρους του εθνικού αλλά και του παγκόσμιου πληθυσμού, καθώς οι δυνατότητες επικοινωνίας που προσφέρουν είναι τεράστιες. Οι χρήστες παγκοσμίως μέσα σε μία δεκαετία έχουν αυξηθεί από σχεδόν ένα 1 δισεκατομμύριο το 2010, σε 2.8 δισεκατομμύρια χρήστες το 2019 (Clement, 2019). Αντίστοιχα τις τελευταίες δεκαετίες και η ροή της πληροφορίας έχει αυξηθεί. Όπως αναφέρουν οι Hilbert et al. (2016) η ικανότητα ανταλλαγής της πληροφορίας έχει αυξηθεί από το ισοδύναμο πληροφορίας δύο φύλων εφημερίδας ανά άτομο την ημέρα το 1986, σε έξι ολόκληρες εφημερίδες το 2007, με την Google να μπορεί να διαχειρισθεί περίπου 2000000 ερωτήματα αναζήτησης σε ένα μόνο λεπτό, ενώ οι χρήστες του Facebook να μπορούν να διαμοιρασθούν περίπου 700000 τεμάχια περιεχομένου, αντίστοιχα. Όλη αυτή η πληροφορία ωστόσο εκτός από τα θετικά που μπορεί και προσφέρει (εκπαίδευση, ενημέρωση, ανταλλαγή εμπειριών μεταξύ ιδιωτών, δημιουργίας αμοιβαίων σχέσεων στον επιχειρηματικό τομέα, περιβάλλον και μέσο για νέες προσεγγίσεις και διαύλους ηλεκτρονικής σχέσης και άλλα πολλά), εν τούτοις αποτελεί πηγή για εγκληματίες, και γενικότερα παραβατικές συμπεριφορές. Εγκυμονεί δηλαδή κινδύνους για την Προσωπική και Ψηφιακή Ασφάλεια του ατόμου. Το “Cambridge Analytica Scandal”, όταν το 2014, απέκτησε πρόσβαση, στα δεδομένα των χρηστών του Facebook, αποτελεί μερικώς την απόδειξη για τους εγκυμονούντες κινδύνους και πιο συγκεκριμένα στην συγκεκριμένη περίπτωση, της παραβίασης της ιδιωτικότητας των χρηστών των ΙΚΔ, (μέσω των όρων χρήσης περί του απορρήτου του Facebook ή και άλλων ΙΚΔ - δεν διασφαλίζονται απαραίτητα, τα προσωπικά στοιχεία των χρηστών, καθώς ένα μεγάλο μέρος της αποκαλυφθείσας πληροφορίας, αποκαλύπτεται και από τους ίδιους τους χρήστες στην αλληλεπίδρασή τους) (Todd, 2018) (González-Bailón, 2018). Φαινόμενα όμως όπως το προαναφερθέν υπάρχουν και άλλα, ενδεικτικά αναφέρουμε και το παράδειγμα τη παραβίασης των προσωπικών στοιχείων των χρηστών της Sony το 2011 (“Social Media and Our Privacy”,

2016). Το θέμα της ασφάλειας των χρηστών Ιστοσελίδων Κοινωνικής Δικτύωσης, της παραβίασης των προσωπικών τους δεδομένων και άλλων κινδύνων που προκύπτουν από την παραβίαση των προσωπικών δεδομένων των χρηστών αποτελεί μια ανησυχία που συνοδεύει απαραίτητα την χρήση των Ιστοσελίδων Κοινωνικής Δικτύωσης, τόσο των χρηστών όσο και των ερευνητών ("Today's social network sites," 2017).

## 1.2 Δήλωση του προβλήματος

Τα τελευταία χρόνια η χρήση των Κοινωνικών Δικτύων έχει αυξηθεί και αυξάνεται συνεχώς, εμπλεκόμενα στην καθημερινότητα των χρηστών τους, καθώς αποτελούν εικονικούς κόσμους συνάντησης που διευκολύνουν την επικοινωνία μεταξύ των ατόμων. Τα Κοινωνικά Δίκτυα σήμερα, καθώς επεκτείνονται σε όλους τους τομείς της ανθρώπινης δραστηριότητας, και οι ηλικίες χρήσης των μέσων αυτών διευρύνονται, ενέχουν κινδύνους οι οποίοι συνδέονται και με τις ηλικίες. Μελέτες έχουν αποδείξει ότι η Χρήση Ιστοσελίδων Κοινωνικής Δικτύωσης εγκυμονεί κινδύνους οι οποίοι μπορούν να επιφέρουν αρνητικές συνέπειες στους συμμετέχοντες (Vandoninck, d'Haenens, De Cock, & Donoso, 2012), (Antoniadou & Kokkinos, 2015). Καθώς αυτό το περιβάλλον ενισχύεται από την συνεχή αύξηση των χρηστών του και την αυξανόμενη ροή της παραγόμενης πληροφορίας, είναι σημαντικό να εξετασθεί εάν οι κίνδυνοι και ποιοι κίνδυνοι εμφανίζονται με μεγαλύτερη συχνότητα και σε ποιες ηλικιακές ομάδες. Εάν οι ομάδες αυτές είναι σε θέση να αναγνωρίσουν τις αρνητικές συνέπειες, τους παράγοντες που επηρεάζουν την έκθεσή τους σε κίνδυνους, αλλά και μέσω αυτών των παραγόντων εάν είναι δυνατόν να ευαισθητοποιηθούν οι χρήστες.

## 1.3 Δήλωση σκοπού

Ο σκοπός της παρούσας μελέτης είναι να διερευνηθούν ποιοι είναι οι πιο συχνά εμφανιζόμενοι κίνδυνοι στις ιστοσελίδες Κοινωνικής Δικτύωσης, (και οι έννοιες κλειδιά που είναι συνδεδεμένες με την έκθεση των χρηστών στους κινδύνους, π.χ. Αντίληψη του Κινδύνου, Εμπιστοσύνη σε Εταιρείες ΙΚΔ, Συμπεριφορές σχετικές με Ιδιωτικότητα/Απόρρητο, Ανησυχία για την Ιδιωτικότητα/Απόρρητο, Αντιληπτός έλεγχος πληροφοριών, Αποκάλυψη προσωπικών πληροφοριών). Στην διαδικασία αυτή θα εντοπιστούν οι πιο δημοφιλείς πλατφόρμες Κοινωνικών Δικτύων, ο βαθμός διείσδυσης στους χρήστες του Διαδικτύου καθώς και οι πιθανοί συσχετισμοί μεταξύ

συμπεριφορών έκθεσης σε κινδύνους και Κοινωνικό-Δημογραφικών χαρακτηριστικών των χρηστών, όπως επίσης και ο πιθανός συσχετισμός μεταξύ Κοινωνικό-Δημογραφικών χαρακτηριστικών των συμμετεχόντων και της έκθεσης σε Διαδικτυακούς κινδύνους.

## 1.4 Δομή Διατριβής

Το Κεφάλαιο 2 «Κίνδυνοι και Κοινωνικά Δίκτυα» αναφέρεται στο θεωρητικό πλαίσιο των εννοιών με τις οποίες ασχολείται η διατριβή, μέσα από μια αναλυτική παρουσίαση τόσο των εννοιών του Κινδύνου γενικότερα, όσο και των Κοινωνικών Δικτύων.

Στο Κεφάλαιο 3 «Ανασκόπηση της Βιβλιογραφίας» παρατίθενται τα συγγράμματα τα οποία εξετάσθηκαν για την υλοποίηση της παρούσας διατριβής. Η Αναλυτική παρουσίαση των μελετών παρουσιάζεται θεματικά και ημερολογιακά (ερευνών από την εγχώρια όσο και Διεθνή Βιβλιογραφία).

Στο κεφάλαιο 5 « Πειραματική Μέθοδος με Χρήση Ποσοτικής έρευνας» παρουσιάζονται με λεπτομέρεια τα στοιχεία τα σχετικά με την Μεθοδολογία που ακολουθήθηκε, τον τόπο και το δείγμα της έρευνας, τις άδειες, τα εργαλεία συλλογής δεδομένων, οι μέθοδοι ανάλυσης και οι στατιστικές μέθοδοι που ακολουθήθηκαν για την ανάλυση των δεδομένων.

Στο Κεφάλαιο 5 παρέχονται τα αποτελέσματα της έρευνας. Αρχικά παρουσιάζονται τα αποτελέσματα της Περιγραφικής Στατιστικής και ακολουθούν τα Αποτελέσματα της Επαγωγικής Στατιστικής όπου περιέχονται οι υλοποιηθέντες έλεγχοι και οι συσχετισμοί προκειμένου να απαντηθούν τα επιμέρους διατυπωθέντα ερευνητικά ερωτήματα.

Στο Κεφάλαιο 6 παρέχονται τα Συμπεράσματα που προέκυψαν από την έρευνα, οι σχέσεις με άλλες μελέτες, οι πιθανοί περιορισμοί τα έρευνας και οι περιοχές πιθανών μελλοντικών ερευνών.

Τέλος στο Παράρτημα παρατίθεται το ερωτηματολόγιο που χρησιμοποιήθηκε στην έρευνα.

# Κεφάλαιο 2

# Κίνδυνοι και Κοινωνικά Δίκτυα

## 2.1 Ορισμοί

Στη παρούσα ενότητα θα αναφερθούν οι ορισμοί των εννοιών της παρούσας πτυχιακής εργασίας.

Η επικοινωνία αποτελεί το μέσο για διεύρυνση γνώσεων, ενημέρωση, ψυχαγωγία, εκπαίδευση κλπ. Η μέσω υπολογιστών, διαμεσολαβημένη επικοινωνία (Computer Mediated Communication), επιτρέπει τη σύνδεση και τη δημιουργία δεσμών μεταξύ ατόμων, που μπορεί να βρίσκονται σε διαφορετικά γεωγραφικά σημεία, με τα Κοινωνικά Μέσα (Social Media), Κοινωνικά Δίκτυα (Social-Networks) να γνωρίζουν μεγάλη ανάπτυξη και να αποτελούν έναν από τους πιο δημοφιλείς τρόπους επικοινωνίας.

Ο όρος Social Media σύμφωνα με τους Hwang & Kim, (2015) αναφέρεται σε ένα σύνολο διαδικτυακών εφαρμογών οι οποίες βασίζονται σε ιδεολογικά και τεχνολογικά θεμέλια του Web 2.0 που επιτρέπουν τον διαμοιρασμό περιεχομένου (ιδέες, σκέψεις) που δημιουργούν οι ίδιοι οι χρήστες.

Τα τελευταία χρόνια τα κοινωνικά Δίκτυα (Social Media) έχουν γνωρίσει πολύ μεγάλη άνθηση επιτρέποντας στα άτομα να δημιουργούν περιεχόμενο, να το διαμοιράζονται, να συνδέονται μεταξύ τους με πολύ ταχείς ρυθμούς. Πλατφόρμες (Social Networks Sites) όπως το Facebook, το Twitter, MySpace, LinkedIn, αλλά και blogs, πλατφόρμες για online gaming, όπως Steam κ.λπ., συγκεντρώνουν ένα πολύ μεγάλο αριθμό συμμετεχόντων, οι οποίοι αλληλοεπιδρούν μεταξύ τους (Hwang & Kim, 2015).

Οι Acquisti et Ross (2006) παρουσιάζουν τα κοινωνικά Δίκτυα ως «μια κοινότητα του Διαδικτύου όπου τα άτομα αλληλοεπιδρούν, συχνά μέσω προφίλ που παρουσιάζουν (represent) τη δημόσια προσωπικότητα τους (και τα δίκτυά των συνδέσεων τους) με άλλους».

Ως Κοινωνική Δικτύωση, (ο ορισμός σύμφωνα με το Cambridge Dictionary) αποτυπώνεται, η χρήση ιστοσελίδων και άλλων Διαδικτυακών υπηρεσιών για την επικοινωνία και δημιουργία φίλων, ή και «η δραστηριότητα ανταλλαγής πληροφοριών

και επικοινωνίας με ομάδες ατόμων που χρησιμοποιούν το διαδίκτυο, ιδίως μέσω ιστοσελίδων ειδικά σχεδιασμένων για το σκοπό αυτό» ("SOCIAL NETWORKING | meaning in the Cambridge English Dictionary," n.d.).

Ο Hilgartner (Hilgartner, 1992) αναφέρεται στην έννοια του κινδύνου περιγράφοντας ότι η έννοια αυτή περιέχει 3 διαφορετικές έννοιες, ένα αντικείμενο που θεωρείται ως το αντικείμενο που «θέτει τον κίνδυνο» ("pose" the risk"), μια υποτιθέμενη βλάβη ("a putative harm") και μία σύνδεση μεταξύ του υποκειμένου στον κίνδυνο και στην βλάβη ("and a linkage alleging some form of causation between the object and the harm") (Hilgartner, 1992), (Boholm & Corvellec, 2011). Σύμφωνα δε με τους Bolhom & Corvellec (Boholm & Corvellec, 2011), ο ορισμός αυτός αποτελεί το πλαίσιο για τον ορισμό της έννοιας του κινδύνου (Boholm & Corvellec, 2011)

Οι Rasmussen & Ihlen (2017), ορίζουν τον κίνδυνο (ακολουθώντας τον ορισμό των Klinke & Renn, ως την «πιθανότητα οι ανθρώπινες πράξεις ή γεγονότα να οδηγήσουν σε συνέπειες που βλάπτουν πτυχές πραγμάτων που εκτιμά ο άνθρωπος (who see risk as the "possibility that human actions or events lead to consequences that harm aspects of things that human beings value") (Rasmussen & Ihlen, 2017) & (Renn, 1998)

## 2.2 Κίνδυνοι Εισαγωγή Θεωρητική/ Εννοιολογική εξήγηση (Θεωρητικός Προσδιορισμός)

### *2.1.1 Hazards – Dangers – Risks -Threats*

### Μίνι ιστορική αναδρομή του τι είναι κίνδυνοι

Κίνδυνος είναι μια έννοια που δύσκολα μπορεί κάποιος να δώσει ακριβή ορισμό. Διαφορετικές ερμηνείες για τον κίνδυνο συναντάμε σε διαφορετικές επιστήμες και η αντίληψη των ανθρώπων είναι αντίστοιχη (Weber, 2001), (Renn, 1998).

Στον Μεσαίωνα η έννοια του κινδύνου "danger" ήταν συνδεδεμένη με φυσικές καταστροφές, πολέμους, επιδημίες (Denney, 2005).

Η έννοια του κινδύνου "risk" είναι συνδεδεμένη με την αβεβαιότητα και βέβαια με την σύγχρονη εποχή (Weber, 2001), (Taylor-Gooby & Zinn, 2006). Ως έννοια risk εμφανίστηκε τον 16ο & 17ο αιώνα και συνδέθηκε με τους εξερευνητές. Η λέξη ενσωματώθηκε στην αγγλική γλώσσα από τα Πορτογαλικά και τα Ισπανικά. Αργότερα χρησιμοποιήθηκε και στις επιχειρήσεις και το εμπόριο και τέλος ο όρος επεκτάθηκε και σε άλλες καταστάσεις πιο αβέβαιες (Denney, 2005).

Επιστήμες όπως αυτή των Τεχνολογιών των Μέσων Μαζικής Ενημέρωσης όσο και των Επιστημών των Πληροφοριών και Επικοινωνιών είχαν καθοριστικό ρόλο στην ανάπτυξη των ερευνών για τους κινδύνους, με τις Επιστήμες των Πληροφοριών και Επιστημών (ICT/Information & Communication Technologies), να μετέχουν καθοριστικά στην διαμόρφωση του όρου του κινδύνου "risk," των ευαισθησιών και των αντιλήψεων των σχετικών με τους κινδύνους (Loon, 2002). Φαινόμενα όπως αυτά του Chernobyl και του Challenger (διαστημικό λεωφορείο) το 1986, η πετρελαιοκηλίδα του Exxon Valdez, το 1989, αλλά και άλλα αντίστοιχα γεγονότα, στα οποία δόθηκε μεγάλη δημοσιότητα από τα Μέσα Μαζικής Ενημέρωσης, ανέδειξαν τον κίνδυνο ως το φαινόμενο που συνοδεύει την τεχνική ανάπτυξη. Παράλληλα η αδυναμία διαχείρισης ή και εξάλειψης του κινδύνου από τα διάφορα θεσμικά όργανα ή και τους εμπειρογνώμονες, εδραίωσε την άποψη ότι η αβεβαιότητα και ο κίνδυνος αποτελούν στοιχεία της τεχνικής ανάπτυξης και της τεχνολογίας. Τα φαινόμενα αυτά, (της τεχνικής ανάπτυξης και της τεχνολογίας) εμπεριέχουν επιπλέον και κοινωνικοπολιτικά ζητήματα αποδοχής και ζητήματα ανταγωνισμού, καθώς καινοτομίες όπως η πυρηνική ενέργεια, ή τα γενετικά τροποποιημένα τρόφιμα, ή και άλλα αντίστοιχα, την στιγμή που γίνουν γνωστά εγείρουν μια σειρά διαμαρτυριών και πολιτικών αντιθέσεων, ως φαινόμενο ευαισθητοποίησης του κοινού, για τους πιθανούς κινδύνους που εγκυμονούν (Taylor-Gooby & Zinn, 2006). Ο Weber (2001) αναφέρει ότι οι πολίτες, ως πολίτες και ως καταναλωτές με τις αντιλήψεις τους για τον κίνδυνο επηρεάζουν τις πολιτικές κυβερνήσεων και άλλων οργανισμών και αναφέρει, ως παράδειγμα μεταξύ άλλων, ότι η θέση των καταναλωτών για τα εμφυτεύματα στήθους σιλικόνης, ότι είναι επιβλαβή, οδήγησε τον κατασκευαστή τους σε χρεωκοπία, ανεξάρτητα από τις επιστημονικές παραδοχές που υποστήριζαν, ότι δεν εγκυμονούν κινδύνους. Και οι δύο αυτές παραδοχές ενέταξαν τον κίνδυνο στο κέντρο της κοινωνικής επιστήμης και αποτέλεσε κύριο σημείο μελέτης πολλών ερευνητών (Taylor-Gooby & Zinn, 2006).

Η βιβλιογραφία των κοινωνιολόγων Ulrich Beck το 1992 και του Antony Giddens το 1991 για την "Risk Society" αποτέλεσαν τις πρώτες επιστημονικές έρευνες και δημοσιεύσεις για τον κίνδυνο και οι μελέτες τους παρουσίασαν την άποψη, «ότι ο κίνδυνος αποτελεί δύναμη κοινωνικής αλλαγής», (Loon, 2002) με τον Fox (1999) να υποστηρίζει ότι στο "Risk Society" του Beck, ή έννοια του κινδύνου ως «αποτέλεσμα της τεχνικής καινοτομίας», «έχει ξεφύγει από τον έλεγχο». Στη σημερινή πραγματικότητα και κυρίως μετά την 11η Σεπτεμβρίου 2001 (Τρομοκρατική Επίθεση στους Δίδυμους Πύργους, Νέα Υόρκη), οι τύποι κίνδυνων στην μοντέρνα κοινωνία έχουν αυξηθεί. Την ίδια

στιγμή σύμφωνα με τον Loon (2002) οι σημερινές δυτικές κοινωνίες είναι ασφαλέστερες από ποτέ, με μόνη ίσως εξαίρεση περιοχές που βρίσκονται σε εμπόλεμη κατάσταση, συγκριτικά πάντα με τους κινδύνους τους οποίους οι άνθρωποι αντιμετώπιζαν τον Μεσαίωνα. Ο άνθρωπος, έχει μάθει να ελέγχει πολλές απρόβλεπτες καταστάσεις, σχετικές με ατυχήματα, βία και ασθένειες. Ακόμη και σεισμοί αλλά και εκρήξεις ηφαιστείων μπορούν να προβλεφθούν με σχετική ασφάλεια, και πιθανά όπως έχει υποστηριχθεί και κίνδυνοι σχετικοί με την τρομοκρατία (Loon, 2002). Η πραγματοποίηση ενός κινδύνου, η μετατροπή του κινδύνου σε πράξη υποδηλώνει ότι ο κίνδυνος ο ίδιος δεν είναι πραγματικός, «πρόκειται να γίνει πραγματικότητα», ("risks are not 'real', they are 'becoming-real") (Loon, 2002).

Ο Bernstein (1996) στο βιβλίο του "Against Gods" αναφερόμενος στην ετυμολογική ρίζα του "risk"/κίνδυνος (" η λέξη κίνδυνος προέρχεται από την ιταλική λέξη risicare που σημαίνει τολμώ "to dare") υποστηρίζει, ότι η έννοια του κινδύνου είναι «μάλλον επιλογή από/αντί μοίρα»- "risk is a choice than a fate".

Η πράξη της υλοποίησης της καταστροφής την 11 Σεπτεμβρίου 2001, ανέδειξε το ότι κίνδυνος, σε κάθε περίπτωση, δεν είναι η ίδια η πράξη, αλλά ο κίνδυνος μεταφέρεται σε άλλες αντίστοιχες καταστάσεις εφαρμογής τρομοκρατικών επιθέσεων, ή οποιουδήποτε άλλου κινδύνου, πόλεμο, οικονομική κατάρρευση. Σύμφωνα με τον Peter Bernstein (1996), η διαφοροποίηση μεταξύ του «σύγχρονου ανθρώπου» και του «ανθρώπου του παρελθόντος» (προκάτοχο του σημερινού ανθρώπου), έγκειται στον τρόπο που αντιλαμβάνονται και χειρίζονται τους κινδύνους. Η συστηματική εφαρμογή της επιστήμης, της τεχνολογίας και κυρίως των μαθηματικών αποτελούν μεθόδους ελέγχου των κινδύνων του «σύγχρονου ανθρώπου», είναι ο ίδιος ο άνθρωπος που δημιουργεί τους κινδύνους και όχι ο Θεός όπως πίστευε άνθρωπος του παρελθόντος (Loon, 2002),.

Σύμφωνα με τον Loon (2002) καθοριστική διαφοροποίηση μεταξύ των εννοιών του κινδύνου "risk" και της έννοιας κίνδυνος, επικίνδυνος "hazard» είναι οι αποφάσεις "decisions separate risk from hazards", καθορίζοντας τις αποφάσεις ως «ανθρώπινες ενέργειες και παρεμβάσεις» .

### 2.1.2 Κίνδυνος με την «αρνητική» έννοια

Η έννοια του κινδύνου είναι σχεδόν συνυφασμένη με μια αρνητική χροιά, ως μία έκθεση σε κάτι που μπορεί να προκαλέσει βλάβη στο άτομο, υγεία, προσωπική ποιότητα ζωής, οικονομική απώλεια κ.α., γενικότερα ως κάτι που μπορεί ή και πρέπει να αποφευχθεί, και επιπλέον με κάποιον προσδιορισμό, του ποιος ή τι βρίσκεται σε κίνδυνο ή μπορεί να

χαθεί κλπ. Η έννοια επίσης του κινδύνου μπορεί να αφορά όχι μόνο ένα άτομο αλλά κοινωνίες, πόλεις, ομάδες ατόμων, κάτι πολύ γενικότερο που να αφορά μαζικές καταστροφές. Τρομοκρατία, πτώσεις αεροπλάνων, βόμβες, ομαδικοί σκοτωμοί κ.α.. Το μεγαλύτερο μέρος της βιβλιογραφίας αναφέρεται και σίγουρα όλα τα μέσα Μαζικής Ενημέρωσης αναφέρονται στον κίνδυνο ως κάτι, λόγω του οποίου, ο άνθρωπος, βρίσκεται σε ένα διαρκές άγχος (Lupton & Tulloch, 2002b). Στην έρευνα των Lupton & Tulloch (2002a) η έννοια του κινδύνου αντιμετωπίζεται με την πεσιμιστική της, απαισιόδοξη αντίληψη καθώς διαπίστωσαν ότι οι συμμετέχοντες στην έρευνα που διεξήγαγαν, κατηγοριοποιούν τον κίνδυνο με αρνητική ορολογία και συνδέουν την έννοια του κινδύνου με το «επικίνδυνο» "danger". Αναφέρουν συγκεκριμένα «Τα συναισθήματα του φόβου "fear" και του φόβου "dread" συνδέονταν με τις ερμηνείες του κινδύνου "risk" ως τον κίνδυνο"danger" και το άγνωστο. Η αβεβαιότητα, η ανασφάλεια και η απώλεια ελέγχου για το μέλλον συνδέονταν με τον κίνδυνο "risk", όπως και η ανάγκη να προσπαθήσουμε και να περιορίσουμε αυτήν την απώλεια ελέγχου με την προσεκτική εξέταση των αποτελεσμάτων της ανάληψης κινδύνου» ("The emotions of fear and dread were associated with interpretations of risk as danger and the unknown. Uncertainty, insecurity and loss of control over the future was associated with risk, as was the need to try and contain this loss of control through careful consideration of the results of risk-taking") (Lupton & Tulloch, 2002a).

### 2.1.3 Κίνδυνος με την "θετική" έννοια

Παρά την οποιαδήποτε αρνητική αντιμετώπιση του κινδύνου από τους περισσότερους από εμάς, η έννοια του κινδύνου σίγουρα ενέχει και μια θετική πλευρά. Ο Denney (2005) αναφέρεται στον Anthony Giddens, ο οποίος θεωρούσε την ανάληψη κινδύνου ως τον πυρήνα μιας δυναμικής οικονομίας και προοδευτικής κοινωνίας. Ο κίνδυνος επιπλέον έχει χαρακτηρισθεί ότι αποτελεί την κινητήριο δύναμη πίσω από την καπιταλιστική κοινωνία. Παραδείγματα που αναδεικνύουν τον κίνδυνο πίσω από την άνοδο της καπιταλιστικής κοινωνίας και εποχής αναφέρονται στις εξερευνήσεις του 15ου, 16ου και 17ου αιώνα. Πίσω από τις προσπάθειες των χωρών Ιταλίας, Ισπανίας, Αγγλίας και Πορτογαλίας εκείνης της εποχής υπήρχε η πρόθεση ανάληψης κινδύνου (Denney, 2005). Επιπλέον θα πρέπει να αναφερθούμε στην ανάληψη του κινδύνου πίσω από την επιχειρηματικότητα. Η ανάληψη κινδύνου αναφέρεται ως ένας καθοριστικός παράγοντας στην επιτυχημένη επιχειρηματικότητα. Κίνδυνοι κλειδιά μπορούν να περιγραφούν ως καθοριστικοί λόγοι επιτυχίας (ή και αποτυχίας) σε τομείς όπως η

τεχνολογία, η δημιουργία επαγγελματικών συμπράξεων κ.α. (Denney, 2005). Στην θετική έννοια του κινδύνου θα πρέπει να ενταχθεί και η ανάληψη κινδύνου στα τυχερά παιχνίδια, η οποία στοχεύει στην απόκτηση κερδών (ασχέτως του εκάστοτε αποτελέσματος θετικού ή αρνητικού, περιστασιακού ή και συνολικού). Επιπλέον η ανάληψη κινδύνου ως αποτέλεσμα της αναζήτησης ενθουσιασμού σε δραστηριότητες αναψυχής και προσωπικών δεξιοτήτων, για την επίτευξη των οποίων απαιτείται η εμπλοκή σε επικίνδυνες καταστάσεις, στις οποίες το μέγεθος και ο βαθμός της ανάληψης κινδύνου και της επικινδυνότητας είναι άμεσα συνδεδεμένος με το βαθμό του ενθουσιασμού, του εμπλεκομένου. Από αυτή την άποψη ο κίνδυνος μπορεί να αποτελέσει μια κινητήρια δύναμη για οποιαδήποτε αλλαγή (συμπεριλαμβανομένων παραδειγμάτων της αύξησης του προσωπικού πλούτου μέχρι και της και της επιδίωξης αναλαμβανομένου προσωπικού ρίσκου της αλλαγής του κόσμου) (Renn, 1998), (Denney, 2005).

## 2.3 Τεχνολογίες πληροφοριών και επικοινωνιών & Κίνδυνοι

Οι τεχνολογίες της πληροφορίας και της επικοινωνίας αποτελούν εδώ και αρκετές δεκαετίας μέρος της καθημερινότητας της πλειονότητας των ατόμων, με την βιομηχανία της πληροφορικής να έχει αναπτυχθεί σημαντικά ειδικά κατά το τελευταίο μισό του αιώνα. Ο νέος εξοπλισμός πληροφορικής τόσο αναφορικά με την ικανότητα επεξεργασίας όσο και με την χωρητικότητα της μνήμης έχει εξελιχθεί πολύ και οι νέες συσκευές είναι όχι απλά γρηγορότερες, αλλά επίσης μικρότερες, ελαφρύτερες, φθηνότερες αλλά και πιο εύχρηστες. Αυτό έχει σαν αποτέλεσμα την ευρεία χρήση τους. Ο κλάδος των Επικοινωνιών μαζί με την αρχική βιομηχανία της πληροφορικής είναι πια ένας τομέας που αποκαλείται Τεχνολογία Πληροφοριών και Επικοινωνιών/ΤΠΕ (ICT Information and Communications Technology) και βρίσκεται σε όλο το εύρος της ανθρώπινης δραστηριότητας και σε όλες τις εκδηλώσεις, εκφάνσεις της σύγχρονης κοινωνίας. Η αλληλεξάρτηση των συσκευών και των τεχνολογιών Πληροφοριών και Επικοινωνιών είναι μεγάλη και η οποιαδήποτε ανωμαλία σε οποιοδήποτε εκ των δύο μπορεί να επηρεάσει και πολλά άλλα. Τεχνολογίες Πληροφορίας και Μέσα Μαζικής Ενημέρωσης αποτελούν και παίζουν σημαντικό ρόλο, τόσο στην διαμόρφωση των κινδύνων, στην αντίληψη τους, όσο και στις ευαισθησίες τις οποίες αναπτύσσουμε αναφορικά με την έννοια του κινδύνου. Έτσι από όποια θεωρητική προσέγγιση και εάν αντιλαμβανόμαστε τον κίνδυνο, οι κίνδυνοι αποτελούν πραγματικότητα και μέρος της

κοινωνίας. Μια μικρή αναφορά ήδη έχει γίνει για τους κινδύνους τους προερχόμενους από τα Μέσα Μαζικής Ενημέρωσης και στην αρνητική χροιά, στην οποία δίνουν έμφαση του κινδύνου. Ο Denney (2005) αναφέρει σχετικά «Αν και τα μέσα μαζικής ενημέρωσης περιλαμβάνονται συχνά σε συζητήσεις για την κατανόηση της επιστήμης από τον κόσμο, και θεωρούνται κεντρικά για τη διάδοση των πληροφοριών του κοινού σχετικά με τους κινδύνους πολύ λίγη δουλειά στην πραγματικότητα ασχολείται με μια λιγότερο οργανική και πιο παραγωγική προοπτική των μέσων ενημέρωσης ως δυνάμεις κινδύνου, τους εαυτούς τους… Δηλαδή, τα μέσα ενημέρωσης αποτελούν μέρος του τεχνολογικού αστερισμού μέσω του οποίου οι κίνδυνοι δημιουργούνται». Ο κίνδυνος μέσα από τα Μέσα Μαζικής Ενημέρωσης μπορεί να δημιουργηθεί, μεγεθύνεται και απευθύνεται στο κοινό, στο άτομο. Ουσιαστικά κατασκευάζεται και κυρίως επισημαίνονται είτε μέσω άρθρων, είτε μέσω εικόνων, οι συνέπειες των κινδύνων (Denney, 2005). Η Aro (2016) αναφέρει σχετικά «Το καθεστώς του Ρώσσου Πρόεδρου Vladimir Putin έχει πάρει τον έλεγχο των παραδοσιακών μέσων Ενημέρωσης στην Ρωσία: Τηλεόραση Ραδιόφωνο και Εφημερίδες. Σύμφωνα με όσα δήλωσε ο υπουργός Άμυνας Sergei Shoigu το Κρεμλίνο βλέπει τα Μέσα Μαζικής Ενημέρωσης ως «ένα όπλο»» και σε αυτό το πλαίσιο αναφέρεται και στην πρόθεση του καθεστώτος να ελέγξει πλήρως τα Μέσα Κοινωνικής Δικτύωσης που τα χρησιμοποιούν social media υποστηρικτές του Ρώσσου προέδρου τα λεγόμενα trolls. Απώτερος σκοπός των troll να φοβίσουν άτομα (που η Aro πήρε συνέντευξη), ώστε να σταματήσουν την διάδοση σχολίων για το καθεστώς. Το φαινόμενο αυτό αποκαλεί «απειλή εθνικής ασφάλειας» που πρέπει να αντιμετωπισθεί αναλόγως (Aro, 2016).

Οι τεχνολογίες της Πληροφορίας και Επικοινωνίας έχουν ενισχύσει την ροή των πληροφοριών σε παγκόσμιο επίπεδο, αλλά ταυτόχρονα έχουν συντελέσει και «στην επιτάχυνση του κινδύνου» (Denney, 2005).

Οι Τεχνολογίες Πληροφοριών και Επικοινωνίας και ο κυβερνοχώρος είναι τεχνολογίες, που αλλάζουν την κοινωνία με πολλούς τρόπους, επηρεάζοντας ουσιώδεις εκφάνσεις της κοινωνικής, πολιτιστικής, πολιτικής, θεσμικής και οικονομικής ζωής (Dodge & Kitchin, 2003) Ο μεγάλος όγκος της προσβάσιμης πληροφορίας, όσο και ο απαιτούμενος ελάχιστος χρόνος στην πρόσβασή της, η αμεσότητα της πληροφορίας, αποκαλύπτει ένα νέο κόσμο, που δεν προσφέρει μόνο νέες ευκαιρίες, αλλά ταυτόχρονα και ένα κόσμο κινδύνων.

### 2.3.1 Κυβερνοχώρος – Κίνδυνοι

Η έννοια Κυβερνοχώρος παρουσιάστηκε πρώτη φορά από τον συγγραφέα επιστημονικής φαντασίας William Gibson (Καναδό) το 1981, σε μία ανάγνωση σε κοινό, μιας σύντομης ιστορίας, όπου αποτυπώνονταν, ως ένας φανταστικός κόσμος («συναινετική ψευδαίσθηση») που συμβαίνει κατά την αλληλοεπίδραση ανθρώπου υπολογιστή (Sheldon, 2012). Στον γραπτό λόγο εμφανίζεται το 1984 στην νουβέλα του ίδιου (William Gibson) "Neuromancer", όπου αποτυπώνεται ως «ένας ψηφιακός χώρος δικτυωμένων υπολογιστών που είναι προσβάσιμοι από κονσόλες υπολογιστών», μια αλληλεπίδραση μεταξύ ιδιωτών και εταιρειών για ανταλλαγή πληροφοριών (Dodge & Kitchin, 2003).

Για την έννοια του Κυβερνοχώρου δεν υπάρχει ένας κοινός ορισμός (κυρίως στην επιστημονική έρευνα) και διάφοροι ορισμοί κατά περιόδους έχουν δοθεί στην έννοια αυτή. Ο Benedict (1991) αναφέρει «Ένας απέραντος τεχνητός κόσμος όπου οι άνθρωποι περιηγούνται στον χώρο που βασίζεται στην πληροφορία "και ως" η απόλυτη διεπαφή υπολογιστής-άνθρωπος». Σύμφωνα με τους Rain & Lorents (2010) αντίστοιχα «Κυβερνοχώρος είναι ένα χρονικά εξαρτώμενο σύνολο διασυνδεδεμένων πληροφοριακών συστημάτων και οι ανθρώπινοι χρήστες που αλληλοεπιδρούν με αυτά τα συστήματα».

Σύμφωνα με τον Sheldon (2012), οι ορισμοί που αναφέρονται στον Κυβερνοχώρο εντάσσονται σε δύο διαφορετικά μοντέλα το μοντέλο "inclusive" και το αντίστοιχο "exclusive". Ο διαχωρισμός αυτός αναφέρεται στον τρόπο που αποτυπώνεται ο κυβερνοχώρος. Στο μοντέλο "inclusive" ο κυβερνοχώρος παρουσιάζεται με μια «ορισμένη απτή και ομοιομορφία», αποτυπώνοντας τον, ως χώρο αντίστοιχο «της γης, της θάλασσας, του αέρα και της διαστημικής εξουσίας». Στο μοντέλο "exclusive" ο κυβερνοχώρος παρουσιάζεται ως ένας «πληροφοριακός και εικονικός κόσμος» στον οποίο η υποδομή είναι και αυτή υπονοούμενη. Το κάθε μοντέλο ορισμού δίνει έμφαση σε διαφορετικό σημείο του κυβερνοχώρου ως έννοια. Έτσι στο "inclusive" μοντέλο, δίνεται έμφαση σε στοιχεία όπως οι υπολογιστές, ο κώδικας (προγραμματισμού), τα δίκτυα αλλά και άλλα στοιχεία της υποδομής, στις φυσικές εκδηλώσεις του κυβερνοχώρου, ενώ στο μοντέλο "exclusive" υποδεικνύεται κυρίως ο χώρος, στον οποίο ο άνθρωπος αλληλοεπιδρά, δημιουργεί περιεχόμενο, αποθηκεύει και μεταδίδει τις πληροφορίες», δίνεται έμφαση στο γνωστικό στοιχείο». Το μεγαλύτερο μέρος των ορισμών που αναφέρονται στον κυβερνοχώρου τον αποτυπώνουν όπως το μοντέλο "inclusive". Η αποτύπωση του ορισμού και του περιεχομένου του -τι εμπεριέχει ή τι έχει εξαιρεθεί- με τον ένα ή τον άλλο τρόπο δεν είναι απλά θέμα σημειολογίας αλλά ουσιαστικό, καθώς

κρίνονται θέματα που σχετίζονται με τις «λειτουργίες της εξουσίας», καθορίζεται το εύρος αυτής όπως και οι στρατηγικές που θα ακολουθηθούν στον χώρο αλλά και της λειτουργίας της κυβερνο-δύναμης (Sheldon, 2012).

Το Υπουργείο Άμυνας των Η.Π.Α. ορίζει τον κυβερνοχώρο ως το «παγκόσμιο πεδίο εντός του περιβάλλοντος πληροφοριών που αποτελείται από το αλληλεξαρτώμενο δίκτυο πληροφοριών, τις υποδομές τεχνολογίας και τα δεδομένα κατοίκων, συμπεριλαμβανομένων του Διαδικτύου, τα τηλεπικοινωνιακά δίκτυα, τα συστήματα υπολογιστών, και ενσωματωμένους επεξεργαστές και ελεγκτές» (Theohary, 2018) (Theohary & Harrington, 2015).

Ο κυβερνοχώρος με αυτή την εννοιολογική προσέγγιση, επίσης μπορεί να περιγραφεί και σε επίπεδα σχετικά με την δομή του. Το πρώτο επίπεδο αποτελεί το «φυσικό δίκτυο» (physical network), που αποτελείται από τα γεωγραφικά και φυσικά εξαρτήματα δικτύου, το δεύτερο επίπεδο το «λογικό δίκτυο» (logical network) το οποίο απαρτίζεται από παρεμφερή στοιχεία και τα οποία είναι σε άμεση συνάρτηση με το φυσικό δίκτυο, με παράδειγμα έναν ιστότοπο ο οποίος είναι προσβάσιμος σε μία μόνο διεύθυνση “URL” αλλά μπορεί να βρίσκεται, φιλοξενείται σε πολλούς servers/ διακομιστές και το τελευταίο επίπεδο που αναφέρεται στο φυσικό ή εικονικό πρόσωπο cyber persona που χρησιμοποιεί τους κανόνες του λογικού δικτύου (Theohary & Harrington, 2015).

Τόσο εννοιολογικά όσο και πραγματικά ο κυβερνοχώρος είναι ένα νέο πεδίο, ιδιαίτερα δυναμικό αλλά ταυτόχρονα και νεφελώδες καθώς οι απειλές και οι κίνδυνοι που τον συνοδεύουν αποτελούν τομέα που απαιτεί συνεχή διερεύνηση. Ενώ η σύγχρονη ζωή έχει υποστεί σημαντικές θετικές αλλαγές, τόσο αναφορικά με την προσβασιμότητα αλλά και τις ευκολίες που παρέχει το Διαδίκτυο, και ο εικονικός χώρος του Κυβερνοχώρου, χαρακτηριστικά, τα οποία έχουν αποτυπωθεί αρκετές φορές στην βιβλιογραφία, μόλις σχετικά πρόσφατα η βιβλιογραφία εστιάζει και στους αναδυόμενους κινδύνους που εγκυμονεί και σε επιδράσεις του, που θεωρούνται αρνητικές (Marzano, Lubkina, & Truskovska, 2013).

Η συνδεσιμότητα που προσφέρει ο κυβερνοχώρος, αφορά το μισό ολόκληρης της ανθρωπότητας και συνδέεται αναπόσπαστα με όλες τις εκφάνσεις της εξουσίας, πολιτικής, κοινωνικής, οικονομικής και στρατιωτικής και στρατηγικά εκλαμβάνεται ισότιμος με την γη, τον αέρα και την θάλασσα. Οι κίνδυνοι που προκύπτουν από τις Τεχνολογίες Πληροφορίας και Επικοινωνίας είναι πολλοί αλλά ο ίδιος ο Κυβερνοχώρος είναι μια ειδική κατηγορία κινδύνου μόνος του. Οι κίνδυνοι που αφορούν τον κυβερνοχώρο μπορούν να αφορούν είτε κινδύνους στην σφαίρα των Τεχνολογιών

Πληροφορίας και Επικοινωνιών και στον υπολογιστή, δηλαδή στις υποδομές του κυβερνοχώρου «κίνδυνοι για τον κυβερνοχώρο», είτε κίνδυνοι που προκύπτουν από τον ίδιο τον κυβερνοχώρο και διευκολύνονται από την τεχνολογία του και δεν αφορούν τις υποδομές του, «κίνδυνοι μέσω του κυβερνοχώρου» (Deibert & Rohozinski, 2010). Επιπλέον η κατακερματισμένη και πολυεπίπεδη φύση του Διαδικτύου ενισχύει ακόμη περισσότερο την οποιαδήποτε εγκληματική δραστηριότητα, η οποία ενισχύεται ακόμη περισσότερο, από την μη ύπαρξη ενιαίου κεντρικού κυβερνητικού οργάνου που θα φρόντιζε για τη θέσπιση κανόνων για την κατάλληλη συμπεριφορά και την επιβολή ποινικών νόμων σε συγκεκριμένες χώρες (Stalans & Finn, 2016).

### 2.3.2 Κίνδυνοι που αφορούν Υποδομές του Κυβερνοχώρου.

Οι κίνδυνοι αυτοί αναφέρονται κυρίως αναφορικά με τις υποδομές, όπως έχει ήδη αναφερθεί. Ο σχεδιασμός του Διαδικτύου είναι ένα «ανθεκτικό δίκτυο επικοινωνιών», που όμως δεν υπολείπεται τρωτών σημείων στην ασφάλεια του. Οι ευπάθειες ασφάλειας του Διαδικτύου βρίσκονται στο κέντρο της «κατανεμημένης αρχιτεκτονικής του δικτύου». Η επέκταση του κυβερνοχώρου, από τους περιορισμένους χρήστες της πρώτης φάσης υλοποίησης του - στο πειραματικό ερευνητικό δίκτυο, σε πανεπιστημιακό ερευνητικό δίκτυο - σε ένα αναπόσπαστο μέρος της παγκόσμιας πολιτικής οικονομίας, στην οποία συνυπάρχουν όλες οι σύγχρονες κοινωνίες, έχουν οδηγήσει στην ένταση των ευπαθειών και των τρωτών του στοιχείων. Καθώς αποτελεί μέρος της παγκόσμιας διασύνδεσης, (εμπορικής, εκπαιδευτικής, κυβερνητικής), έχει εφαρμογή και βρίσκεται από «πυρηνικά υποβρύχια» μέχρι και σε συστήματα ελέγχου και οποιαδήποτε ανωμαλία στην κανονικότητα της λειτουργίας του, επηρεάζει την παγκόσμια κοινότητα και φαινόμενα τέτοιου τύπου έρχονται στην επιφάνεια. Το 1988 το Morris Worm, κακόφημο λογισμικό κυκλοφόρησε από λάθος στο διαδίκτυο, με αποτέλεσμα το σταμάτημα της παγκόσμιας κυκλοφορίας του διαδικτύου. Ακόμη περισσότερα σενάρια κακόφημων παραβιάσεων έγιναν γνωστά από την δεκαετία του 1990 στο διαδίκτυο και («ευρύτερα στον χώρο του Κυβερνοχώρου»). Αν και αρκετές φορές μπορούν να δημιουργηθούν εσφαλμένες εντυπώσεις, από τις καταγγελίες και για τις επιπτώσεις που επιφέρουν, ανάλογα κάθε φορά με την πηγή της εκπόρευσης, εντούτοις έχει επιτευχθεί ένα είδος συναίνεσης μεταξύ των «προηγμένων βιομηχανικών κρατών» αναφορικά με τον κυβερνοχώρο αλλά και των κρίσιμων υποδομών του, οι οποίες πρέπει να διασφαλίζονται. Προσπάθειες διασφάλισης του κυβερνοχώρου έχουν υλοποιηθεί, με το τοπίο να μην είναι

ακριβώς ξεκάθαρο, καθώς εμπλέκονται εθνικά και ιδιωτικά συμφέροντα, υπάρχει ελλιπής χρηματοδότηση των οργανισμών των επιφορτισμένων με την διασφάλιση από κινδύνους, του κυβερνοχώρου, αδυναμία συνεννόησης μεταξύ των εμπλεκομένων κάθε φορά εθνικών φορέων κ.α., με αποτέλεσμα πολλές φορές να εμπλέκονται τα θέματα, ως προς διάφορες ενέργειες και επιχειρήσεις που υλοποιούνται, πάντα μέσω του κυβερνοχώρου και πιο συγκεκριμένα μέσω των δικτύων επικοινωνίας, και των οποίων η υλοποίηση αντιμετωπίζει διάφορα θέματα ακόμη και νομικής φύσεως. Παράδειγμα όπως αναφέρουν οι Deibert & Rohozinski, (2010) «κατά τη διάρκεια της εισβολής του 2003 στο Ιράκ το πλήρες φάσμα των επιθετικών δυνατοτήτων επίθεσης δικτύων υπολογιστών περιοριζόταν τόσο από τους νομικούς περιορισμούς όσο και από τους φόβους μιας επεκτατικής επίδρασης στα Ευρωπαϊκά χρηματοπιστωτικά ιδρύματα». Το σίγουρο πάντως είναι ότι παρά τα εκάστοτε προβλήματα, μια διεθνής πρακτική έχει αναπτυχθεί, που αποτελείται από φορείς τόσο κρατικούς όσο και ιδιωτικούς που προσπαθούν να επιλύσουν τους εκάστοτε εμφανιζόμενους κινδύνους (Deibert & Rohozinski, 2010).

### 2.3.3 Κίνδυνοι Μέσω του Κυβερνοχώρου

Ο κυβερνοχώρος και κυρίως το Διαδίκτυο έχει αποτελέσει τον συνδετικό κρίκο μεταξύ ατόμων, ομάδων με ομοειδή χαρακτηριστικά σε παγκόσμιο επίπεδο και συνέτεινε στην δημιουργία πολιτικών δικτύων. Εργαλεία όπως οι μηχανές αναζήτησης, τα blogs αλλά και άλλες μορφές ατομικής έκφρασης, έχουν κυριαρχήσει με σχετική ευκολία, που σε συνδυασμό με τα επικοινωνιακά συστήματα, έχουν οδηγήσει σε εικονικούς κόσμους και κοινότητες, που με την σειρά τους οργανώνονται και δίνουν μορφή σε πολιτικές κοινότητες και πολιτικές δραστηριότητες. Χαρακτηριστικά των νέων καινοτόμων τεχνολογιών, όπως γραπτά μηνύματα «SMS», Facebook, Twitter και blogs, έχουν διευκολύνει την ύπαρξη, αλλά ταυτόχρονα έχουν αποτελέσει και εργαλεία πολιτικών ομάδων ανάπτυξης και επέκτασης. Παράλληλα με τις νέες καινοτόμες τεχνολογίες, η ίδια η σύσταση του Διαδικτύου, η «διανεμημένη, αποκεντρωμένη και σχετικά φθηνή και εύκολη στην απασχόληση «ταιριάζει με την οργανωτική και πολιτική λογική των παγκόσμιων πολιτικών δικτύων», αναφέρουν οι Deibert & Rohozinski (2010). Το τοπικό και οι εκφραζόμενες σε τοπικό επίπεδο, απόψεις και θέσεις, μέσω του Διαδικτύου, έχει οδηγήσει στην επέκταση τους σε παγκόσμιο επίπεδο, όπως και σε παγκόσμιο ακροατήριο. Το περιβάλλον όμως αυτό δεν συνοδεύτηκε απαραίτητα μόνο από θετικά στοιχεία αλλά επίσης και από κινδύνους, κινδύνους οι οποίοι αναδύθηκαν έντονα ως

διαμαρτυρίες αντιπολιτευτικές, ακόμη και με επαναστατικές τάσεις, κατά περίπτωση, εναντίον της εγκαθιδρυμένης πολιτικής εξουσίας. Οι αντιπολιτευόμενες φωνές, ακτιβιστές μέσω του Κυβερνοχώρου μπορούν να βρουν υποστηρικτές και εντός και εκτός συνόρων, ώστε να υποστηρίξουν την θέση τους. Η μέσω του κυβερνοχώρου αυξανόμενη αντίδραση, σε καθεστώτα πιο αυταρχικά, αποτελούν ένα «ρευστό και πολύ αυστηρό κίνδυνο ασφαλείας» και οι κίνδυνοι αυτοί αποκαλούνται σύμφωνα με τους Deibert & Rohozinski (2010), δίκτυα αντίστασης (resistance networks). Η αντίδραση που αναπαράγεται σε καθεστώτα δημοκρατικά, καθώς και εκεί υπάρχουν πάντα αντιπολιτευόμενες φωνές, έστω και διαφορετικού χαρακτήρα, ή ομάδες ιδιωτών κοινωνικής δικαιοσύνης, που και αυτές με την σειρά τους μπορούν να λάβουν μορφή βίαιης αντίδρασης, καθώς και άλλου τύπου εγκληματικές ή τρομοκρατικές οργανώσεις που δρουν στον κυβερνοχώρο με σκοπό την προώθηση των δικών τους σκοπιμοτήτων, ή ακόμη και ομάδες ιδιωτών κοινωνικής δικαιοσύνης, αποκαλούνται σκοτεινά δίκτυα (Dark net), με δύο διαφορετικές μορφές. Η πρώτη μορφή των σκοτεινών δικτύων Dark net αναφέρεται σε «οπλισμένα κοινωνικά κινήματα» διαφορετικών κινήτρων με παραδείγματα την Αλ Καιντα και τα κινήματα των Τζιχαντιστών. Οι πρόγονοι των κινημάτων αυτών σύμφωνα πάντα με τους Deibert & Rohozinski (2010) οι οποίοι αναφέρονται, για τον σκοπό αυτό, στον Kaldor, βρίσκονται στην διάρκεια της δεκαετίας του 1990, σε αυτό που ονομάζονται «νέοι πόλεμοι» σε Σρι Λάνκα, Σομαλία, Τσετσενία, Αφρική και άλλες χώρες, χρησιμοποιώντας τακτικές αντάρτικου αλλά και συμβατικού πολέμου εναντίον των κυβερνήσεων των περιοχών αυτών. Οι ομάδες αυτές έχουν χρησιμοποιήσει ειδικά τον κυβερνοχώρο και πρακτικές όπως μικρού μήκους βίντεο ώστε να δημιουργήσουν εντυπώσεις βοηθητικές προς τον σκοπό τους. Με την εξάπλωση δε μέσων όπως το YouTube και το Twitter, η επιρροή αυτή αυξάνεται καθώς χρησιμοποιούνται και από «δίκτυα πολιτών» (Deibert & Rohozinski, 2010).

Η άλλη μορφή των σκοτεινών δικτύων (Dark net) αναφέρονται σε σχέση με ***τα «διακρατικά εγκληματικά δίκτυα»,*** τα οποία εμφανίζονται κάτω από δύο μορφές. Η μία μορφή αφορά **τα νέα εγκλήματα**, όπως ψάρεμα (phishing), spam, κακόβουλο λογισμικό (malware), κατασκοπεία στον κυβερνοχώρο, οργανωμένες συντονισμένες επιθέσεις σε δίκτυα ή και δικτυακές εφαρμογές (Ddos= Distributed Denial of Service) και τα οποία πολλές φορές κατασκευάζονται και χρησιμοποιούνται «ως μορφές αντίστασης σε αθέμιτες κυβερνητικές ή επιχειρηματικές πρακτικές» (Deibert & Rohozinski, 2010) και ***η δεύτερη μορφή η σχετική με απάτες, παιδική πορνογραφία, κλοπή κ.α.***, εγκλήματα τα οποία είναι πια προσαρμοσμένα στις νέες τεχνολογίες. Ως

Κυβερνοέγκλημα (Cybercrime) αναφέρεται, ορίζεται η εγκληματική δραστηριότητα ή πράξη που υλοποιείται μέσω υπολογιστή με σκοπό οικονομικό, ψυχολογικό ή και προσωπικό όφελος και χρησιμοποιώντας τον Κυβερνοχώρο ως το μέσο επικοινωνίας (Gordon & Ford, 2006) (Petter, Henrik, Martikainen, & Lehner, 2019) (Arora, 2016). Τόσο ο ορισμός του Κυβερνοεγκλήματος, όσο και οι τύποι των κυβερνοεγκλημάτων, δεν αποτελούν ξεκάθαρο τοπίο, καθώς πολλές και διαφορετικές απόψεις έχουν διατυπωθεί. Στην παρούσα ενότητα θα διατηρήσουμε τον διαχωρισμό που αναφέρθηκε προηγουμένως ως «Διακρατικά εγκληματικά Δίκτυα» και τις 2 μορφές του, τα νέα εγκλήματα και τα εγκλήματα που είναι σχετικά με απάτες, παιδική πορνογραφία κλπ.

## *Κακόβουλο Λογισμικό «Malware».*

Ως κακόβουλο λογισμικό μπορούν να χαρακτηριστούν διαδικτυακά ρομπότ (bots), ιοί (viruses), σκουλήκια (worms). Τα bots αποτελούν το μέσον το οποίο συνδέει προσωπικούς υπολογιστές με τα botnets «δίκτυο από διαδικτυακά ρομπότ», ώστε να δημιουργήσουν κανάλια επικοινωνίας και στοχεύουν στον άμεσο και εξ αποστάσεως έλεγχο ενός ή περισσοτέρων προσωπικών υπολογιστών. Μέσω των botnet συνήθως μεταδίδεται κακόβουλο λογισμικό. Μέσω του ιού (virus) μολύνονται οι υπολογιστές και συνήθως οι ιοί συνδέονται με προγράμματα ή και έγγραφα. Τα σκουλήκια (worms) αποτελούν αυτόνομα προγράμματα. Ο πρώτος ιός (virus) για υπολογιστές ο “Brain” αποτελεί δημιούργημα 2 Πακιστανών αδελφών, το 1986, οι οποίοι τοποθέτησαν στον κώδικα του προγράμματος, τα προσωπικά τους στοιχεία (ονόματα, τηλέφωνα κλπ.) και το λογισμικό τους, μέσα σε ένα χρόνο ταξίδεψε σε όλο τον κόσμο. Ο σκοπός του Brain, στην πραγματικότητα δεν ήταν κακόβουλος, απλά θέμα περιέργειας των δημιουργών του. Άλλοι τρόποι και άλλες μορφές κακόβουλου λογισμικού, ή κυρίως στρατηγική αποτελούν τα “watering-holes” («τρύπες ποτίσματος»), που στόχο έχουν μεγάλες εταιρείες ή οργανισμούς. Κοινή μέθοδο, επίσης, αποτελεί η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου με κακόβουλο σύνδεσμο, σε άτομο ή ομάδες ατόμων, το οποίο αποκαλείται “spear phishing” «δόλωμα ψάρεμα». Ο αποστολέας συνήθως ενός τέτοιου μηνύματος είναι κάποιο πρόσωπο ή πηγή αξιόπιστη και ο σύνδεσμος οδηγεί σε μια εικονική πόρτα και σε εξωτερικούς χρήστες. Επίσης θα πρέπει να αναφερθούν και τα “air-gapped” δίκτυα («αεροπορικό χάσμα ή κενά αέρος»), τα οποία είναι συστήματα υπολογιστών που δεν συνδέονται στο διαδίκτυο και δεν είναι ευάλωτα σε επιθέσεις ιών (viruses) και σκουλήκια (worms), στην πραγματικότητα όμως μπορούν να προσβληθούν,

από σύνδεση πάνω τους, εξωτερικών συσκευών «μολυσμένων», όπως παραδείγματος χάριν, συσκευών ανάγνωσης δακτυλικού αποτυπώματος (Theohary & Harrington, 2015)

### *Δίκτυο από διαδικτυακά ρομπότ "Botnet"*

Botnet είναι ένα Δίκτυο από Διαδικτυακά ρομπότ, που απαρτίζεται από ένα σύνολο οικιακών ή και εταιρικών υπολογιστών τα οποία είναι μεταξύ τους συνδεδεμένα με ένα πρόγραμμα (bot/ρομπότ). Όλα τα bot/ρομπότ δεν είναι κακόβουλα και τα botnet μπορούν να εξυπηρετούν είτε νόμιμες είτε παράνομες δραστηριότητες. Μια νόμιμη δραστηριότητα είναι η δυνατότητα υποστήριξης επιχειρήσεων των καναλιών «Διαδικτυακής Αναμετάδοσης Συνομιλίας» ("Internet Relay Chat" (IRC)), για την χρήση δικαιωμάτων διαχειριστή σε ομάδα ή ομάδες συγκεκριμένων ατόμων. Πάντως το μεγαλύτερο μέρος των botnet, δεν εξυπηρετούν νόμιμους σκοπούς. Στο bot/ρομπότ πρόγραμμα που συνδέει τους υπολογιστές έχει πρόσβαση ένας μόνο χρήστης. Ο χρήστης που ελέγχει τα botnet αποκαλείται βουκόλος (herder) ή δράστης (perpetrator) ή και «κύριος των bot» "bot master". Ο κώδικας που συνδέει τα Δίκτυα των διαδικτυακών ρομπότ επιτρέπουν την επικοινωνία στο Διαδίκτυο. Τα botnet συνήθως χρησιμοποιούν ευπάθειες των πλατφορμών Microsoft Windows, ώστε να επιτύχουν την καταστροφή του προσωπικού υπολογιστή, χωρίς συνήθως ο χρήστης του υπολογιστή να το αντιληφθεί. Τα botnet είναι συνήθως προγράμματα αυτοματοποιημένα και ενσωματωμένα κρυφά στο Διαδίκτυο και αποτελούν απειλές που έχουν μολύνει δισεκατομμύρια οικοδεσπότες (hosts) σε παγκόσμιο επίπεδο. Εξαπλώνονται με πολύ υψηλές ταχύτητες και συνεργάζονται μεταξύ τους σε μία κοινή κακόβουλη ενέργεια. Η μόλυνση των υπολογιστών υλοποιείται με τρόπο, που οι μολυσμένοι υπολογιστές να λειτουργούν ως φαντάσματα, που κάποιος τα λειτουργεί από απόσταση (ο herder ή perpetrator, ή bot master). Η αλληλογραφία και τα ανεπιθύμητα μηνύματα αποστέλλονται από τα botnet, χωρίς ούτε ο κεντρικός υπολογιστής αλλά ούτε και ο ίδιος ο χρήστης του υπολογιστή να το γνωρίζουν. Ένα χαρακτηριστικό της μόλυνσης του υπολογιστή από botnet, είναι η αργή ανταπόκριση του υπολογιστή. Οι πρώτοι δημιουργοί botnet ήταν συνήθως πολύ εξειδικευμένοι προγραμματιστές. Με την εξέλιξη της τεχνολογίας από το 2004 και μετά, η δημιουργία botnet αποτελεί μια εύκολη διαδικασία. Τα botnet αποτελούν σήμερα με πολύ μεγάλη απειλή για την ασφάλεια του δικτύου και είναι ευρέως γνωστό ότι το 80% κατά προσέγγιση, της συνολικής κυκλοφορίας ηλεκτρονικής αλληλογραφίας είναι ανεπιθύμητη (spam) και ένα μεγάλο μέρος αυτής αποστέλλονται μέσω botnet. Τα botnet επίσης μπορούν να χρησιμοποιηθούν

και σε επιθέσεις Ddos “Distributed Denial of Service” (Theohary & Harrington, 2015) (Liu, Xiao, Ghaboosi, Deng, & Zhang, 2009) (Hoque, Bhattacharyya, & Kalita, 2015).

***Ddos “Distributed Denial of Service”*** «***Κατανεμημένη άρνηση παροχής υπηρεσίας»***

Τα botnets συνήθως χρησιμοποιούνται σε επιθέσεις Ddos που στόχο έχουν την υπερφόρτωση ή και απενεργοποίηση του δικτύου, του υπό επίθεση συστήματος, καταναλώνοντας το εύρος ζώνης δικτύου (bandwidth) και που έχει ως αποτέλεσμα την προσωρινή ή επ’ αόριστον διακοπή των παρεχόμενων υπηρεσιών του δικτύου. Μια επίθεση Ddos είναι μια συντονισμένη επίθεση που υλοποιείται μέσα από πολλούς εκτεθειμένους οικοδεσπότες (hosts). Οι επιθέσεις αυτού του τύπου κατακλύζουν τον στόχο τους με αιτήσεις ώστε να καταναλώσουν το μεγαλύτερο εύρος, του εύρους του δικτύου του στόχου τους. Είναι πολύ αποτελεσματικές επιθέσεις καθώς εκμεταλλεύονται τις ευπάθειες του συστήματος (λογισμικό ή λειτουργικό) του στόχου τους, και των οποίων δύσκολα αποκαθίσταται η βλάβη. Κάθε «μεμονωμένο πακέτο είναι ένα νόμιμο αίτημα» πρόσβασης και μόνο το σύνολο όλων των πακέτων τελικά προσβάλλει το σύστημα. Πολύ σημαντικά στοιχεία για την προσβολή, είναι η ένταση της επίθεσης, και ο αριθμός των κεντρικών υπολογιστών που χρησιμοποιούνται για την επίθεση και η ζημιά είναι ανάλογη. Ο μεγάλος αριθμός συμμετεχόντων κεντρικών υπολογιστών μπορεί να διακόψει το δίκτυο σε πολύ μικρό χρόνο. Σκοπός μιας Ddos επίθεσης είναι η απενεργοποίηση ενός συγκεκριμένου δικτύου, ή η μη ανταπόκριση του δικτύου, ώστε οι νόμιμοι χρήστες να μην μπορούν να το χρησιμοποιήσουν και να μην έχουν πρόσβαση σε παρεχόμενες από το σύστημα πληροφορίες, σε όλη την διάρκεια της επίθεσης. Μια επίθεση Ddos μπορεί να έχει πολλούς φορείς (όπου φορέας “Vector” αποκαλείται, είναι η πορεία της επίθεσης). Για να υλοποιηθεί η Ddos επίθεση ο επιτιθέμενος ακολουθεί τέσσερα συγκεκριμένα βήματα. Πρώτο βήμα **α.** Να συλλέξει πληροφορίες με σάρωση του δικτύου ώστε να εντοπίσει ευάλωτους οικοδεσπότες (hosts) που θα τους χρησιμοποιήσει αργότερα για να υλοποιήσει την επίθεση, **β.** Να επιτύχει το κατέβασμα από τους οικοδεσπότες του κακόβουλου λογισμικού στους «προσβεβλημένους οικοδεσπότες» οι επονομαζόμενοι και ζόμπι ή φαντάσματα, ώστε να επιτευχθεί ο έλεγχος από τον επιτιθέμενο, **γ.** με την έναρξη της επίθεσης να δώσει την εντολή τα «ζόμπι» να στείλουν πακέτα επίθεσης συγκεκριμένης έντασης στο θύμα **και τέλος** να καθαρίσει όλο το ιστορικό και τα αρχεία από την μνήμη. Η επίθεση μπορεί να απευθύνεται σε διάφορους στόχους όπως: δρομολογητές (routers), συνδέσμους (links) τοίχους προστασίας (firewalls) αλλά και άλλα αμυντικά συστήματα, και αναφορικά με το θύμα τον

υπολογιστή και την υποδομή του δικτύου του, το λειτουργικό του σύστημα, εφαρμογές του αλλά και τρέχουσες επικοινωνίες του. Στόχος τέτοιου τύπου επιθέσεων συνήθως αποτελούν υπηρεσίες όπως τράπεζες, υπηρεσίες πληρωμών με πιστωτικές κάρτες και σκοπός τους είναι ο εκβιασμός, εκδίκηση αλλά και ακτιβιστικές ενέργειες. Η εγκληματικότητα στον Κυβερνοχώρο σε παγκόσμιο επίπεδο αυξάνεται και καθώς δεν υπάρχουν αξιόπιστα στατιστικά στοιχεία είναι δύσκολο να μετρηθεί. Σύμφωνα με τους Deibert & Rohozinski (2010), στις Ηνωμένες Πολιτείες της Αμερικής το 2006, αναφέρθηκε ότι στον κυβερνοχώρο οι απώλειες από οικονομικά εγκλήματα υπερέβησαν τα 105 δισεκατομμύρια δολάρια (Theohary & Harrington, 2015) (Liu et al., 2009) (Hoque et al., 2015) (Deibert & Rohozinski, 2010).

Στην Εικόνα 1 ενδεικτικά παραθέτουμε πίνακα με πληροφορίες για τους κορυφαίους κινδύνους του 2018 (με συγκριτικά στοιχεία για το 2017) που ελήφθη από την https://cdn.comparitech.com/wp-content/uploads/2019/04/9-top-cybersecurity-threats-2018-statistics.jpg (“300+ Terrifying Cybercrime & Cybersecurity Statistics [2019 EDITION],” 2019).

| Top Threats 2017 | Assessed Trends 2017 | Top Threats 2018 | Assessed Trends 2018 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ➲ | 1. Malware | ➲ | → |
| 2. Web Based Attacks | ↑ | 2. Web Based Attacks | ↑ | → |
| 3. Web Application Attacks | ↑ | 3. Web Application Attacks | ➲ | → |
| 4. Phishing | ↑ | 4. Phishing | ↑ | → |
| 5. Spam | ↑ | 5. Denial of Service | ↑ | ↑ |
| 6. Denial of Service | ↑ | 6. Spam | ➲ | ↓ |
| 7. Ransomware | ↑ | 7. Botnets | ↑ | ↑ |
| 8. Botnets | ↑ | 8. Data Breaches | ↑ | ↑ |
| 9. Insider threat | ➲ | 9. Insider Threat | ↓ | → |
| 10. Physical manipulation/ damage/ theft/loss | ➲ | 10. Physical manipulation/ damage/ theft/loss | ➲ | → |
| 11. Data Breaches | ↑ | 11. Information Leakage | ↑ | ↑ |
| 12. Identity Theft | ↑ | 12. Identity Theft | ↑ | → |
| 13. Information Leakage | ↑ | 13. Cryptojacking | ↑ | NEW |
| 14. Exploit Kits | ↓ | 14. Ransomware | ↓ | ↓ |
| 15. Cyber Espionage | ↑ | 15. Cyber Espionage | ↓ | → |

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Εικόνα 1: Κορυφαίες απειλές/Κίνδυνοι Ασφαλείας του 2018, Ανακτήθηκε από https://cdn.comparitech.com/wp-content/uploads/2019/04/9-top-cybersecurity-threats-2018-statistics.jpg

## Άλλες μορφές εγκλημάτων που χρησιμοποιούν νέες τεχνολογίες.

Άλλοι κίνδυνοι σχετικοί με τον Κυβερνοχώρο αποτελούν η καταστολή της διαφωτιστικής ομιλίας ή λόγοι φυλετικών ή άλλων διακρίσεων. Επίσης θα πρέπει να αναφερθεί και η παραβίαση και κλοπή της πνευματικής ιδιοκτησίας. Διαδικασίες που στόχευαν στην προστασία του κυβερνοχώρου είτε κατά των ανθεκτικών δικτύων είτε του σκοτεινού δικτύου, αύξησαν μεθόδους όπως η ηλεκτρονική παρακολούθηση (μειονοτικών ή και άλλων ομάδων), το οποίο και αυτό με την σειρά του, αποτελεί και ένα κίνδυνο για τα ανθρώπινα δικαιώματα και την ανθρώπινη έκφραση (Lucchi, 2015).

Η διατήρηση της ανωνυμίας στον κυβερνοχώρο, όπως και η εμφάνιση του ατόμου με πλαστή ταυτότητα ενισχύει την εγκληματικότητα, η οποία στον εικονικό κόσμο είναι πιο δύσκολο να εντοπισθεί και να διωχθεί, σε σχέση πάντα με τον φυσικό χώρο. Εφαρμογές, η χρήση άβαταρ (avatar), οι συσκευές μιας χρήσης και ο βαθύς ιστός (deep web), στον οποίο δύσκολα ανιχνεύεται ο παραβατικός χρήστης (εξαιτίας των πρόσθετων μέτρων ασφαλείας του ιστού), συντελούν στην απόκρυψη των παραβατικών ή και εγκληματικών συμπεριφορών και συναλλαγών. Νέοι εικονικοί κόσμοι, αίθουσες συνομιλιών στον κυβερνοχώρο έχουν δημιουργήσει μια υπόγεια αγορά που διακινεί ναρκωτικές ουσίες, την παιδική πορνογραφία, την πορνεία, ακόμη και δημιουργία κυνηγών με σκοπό τις «σεξουαλικές αλληλεπιδράσεις με άτομα που έχουν μολυνθεί με τον ιό του HIV (aids) με σκοπό την επιμόλυνση για διάφορους λόγους (Stalans & Finn, 2016).

Ποιο κοινοί κίνδυνοι στον κυβερνοχώρο και το διαδίκτυο γενικότερα αποτελούν οι διαδικτυακές απάτες (Online scams), η διαδικτυακή πορνεία (On Line Sexual Solicitation/ Prostitution), Διαδικτυακή παρενόχληση (Cyber harassment), Διαδικτυακός εκφοβισμός (Cyberbullying), Αποπλάνηση (On Line Grooming), Διαδικτυακά Τυχερά παιχνίδια (On Line Electronic Gambling). Πολλοί από τους εγκυμονούντες κινδύνους του Κυβερνοχώρου και του Διαδικτύου γενικότερα, πλήττουν παιδιά και νεαρούς ενήλικες, ηλικιακές ομάδες που απαιτούν και ιδιαίτερη προσοχή. Καθώς πολλοί από τους κινδύνους αυτούς αφορούν και κινδύνους στα κοινωνικά Δίκτυα, που ακολουθούν ως κεφάλαιο, και για την αποφυγή επανάληψης θα αναφέρουμε μερικούς κινδύνους και τους ορισμούς τους στο παρόν σημείο και οι υπόλοιποι θα αναλυθούν στο επόμενο κεφάλαιο.

***Διαδικτυακές απάτες (Online scams)***

Καθώς το Διαδίκτυο αποτελεί χώρο ο οποίος διευκολύνει την επιχειρηματική δραστηριότητα επίσης προκαλεί και τους κάθε είδους απατεώνες. Μερικά παραδείγματα Διαδικτυακών απατών αποτελούν: **α.** Η δημιουργία από απατεώνες Ιστοτόπων Ψεύτικων (spoof web sites & email security alerts), με σκοπό την πρόκληση επίσκεψης από άτομα, με σκοπό να αποκαλύψουν προσωπικές πληροφορίες (κωδικούς password, τραπεζικούς λογαριασμούς κλπ., ενσωματώνοντας ένα σύνδεσμο, του οποίου στόχο αποτελεί η επίσκεψη. **β.** ηλεκτρονικά μηνύματα με ενσωματωμένους συνδέσμους που περιέχουν ιούς, (Virus hoax emails) **γ.** απάτες λοταρίας (Lottery Frauds), συνήθως αποτελούν μηνύματα ηλεκτρονικού ταχυδρομείου, στα οποία ενημερώνεται ο παραλήπτης ότι έχει κερδίσει χρήματα ή κάποιο άλλο βραβείο και απαιτούνται τα προσωπικά του στοιχεία προκειμένου να το διεκδικήσει, **δ.** απάτες με πιστωτικές κάρτες

(Credit Card Fraud) που σκοπό έχει την κλοπή των στοιχείων των πιστωτικών καρτών από χάκερς για κατάχρηση. Όλες οι Διαδικτυακές απάτες έχουν το ίδιο σκοπό την αποκάλυψη προσωπικών στοιχείων του ατόμου και των χρηματοπιστωτικών του συναλλαγών προς ίδιο όφελος των απατεώνων. (Vadza, 2011) (Diomidous et al., 2016).

***Διαδικτυακή πορνεία (OnLine sexual Solicitation)***

Η διαδικτυακή σεξουαλική προσβολή (πορνεία), αφορά πράξεις που ενθαρρύνουν την συζήτηση ή σεξουαλική πράξη ή και διαμοιρασμό σεξουαλικών πληροφοριών». Ο κίνδυνος αυτός όταν αφορά παιδιά και νεαρούς ενήλικες προκαλεί φαινόμενα άγχους, κατάθλιψης και αναπτυξιακές διαταραχές (Schulz, Bergen, Schuhmann, Hoyer, & Santtila, 2015).

***Διαδικτυακός εκφοβισμός (Cyberbullying)***

Ως Διαδικτυακός εκφοβισμός, ορίζεται «η χρήση τεχνολογιών της πληροφορίας και επικοινωνιών για τη υλοποίηση και στήριξη της σκόπιμης, επανειλημμένης και εχθρικής συμπεριφοράς ενός ατόμου ή μιας ομάδας με σκοπό την πρόκληση βλάβης σε άλλους». Το καθοριστικό για τον Διαδικτυακό εκφοβισμό, είναι ότι υλοποιείται μέσω του Διαδικτύου. Τα μέσα μπορούν να είναι προσωπικοί υπολογιστές ή και τηλέφωνα (Floros, Siomos, Fisoun, Dafouli, & Geroukalis, 2013).

***Διαδικτυακή Παρενόχληση (Cyber harassment)***

Ως παρενόχληση θεωρείται η προσωπική επίθεση μεταξύ ενός θύτη και ενός θύματος συνήθως ομότιμων. Η διαδικτυακή παρενόχληση, είναι η ηλεκτρονική παρενόχληση, δηλαδή η (παρενόχληση) μέσω χρήσης τεχνολογίας πληροφοριών και επικοινωνιών και πολλές φορές μπορεί να αναφέρεται και συνώνυμα με τον εκφοβισμό. Η Διαδικτυακή παρενόχληση πολλές φορές ενέχει και πορνογραφία εκδίκησης (Beran & Li, 2005)(Citron & Franks, 2014).

***Διαδικτυακή Αποπλάνηση (On Line Grooming)***

Ο όρος αποπλάνηση περιγράφει τις πράξεις αρχικού σταδίου, στις οποίες ένας ενήλικας προβαίνει, προκειμένου να κερδίσει την εμπιστοσύνη ενός παιδιού ή νεαρού ενήλικα ή οποιονδήποτε άλλο, ώστε να εξασφαλίσει μαζί του μία προσωπική συνάντηση και που τελικό στόχο έχει, να τον κακοποιήσει σεξουαλικά. Μια τέτοια Διαδικτυακή πράξη υλοποιείται μέσω διάφορων αιθουσών συνομιλίας. Η αρχική προσέγγιση του νεαρού ατόμου από τον παραβάτη, συνήθως δεν είναι σεξουαλική, αλλά συνήθως ο στόχος είναι, η σεξουαλική κακοποίηση (McAlinden, 2012) (Diomidous et al., 2016).

***Διαδικτυακά Τυχερά παιχνίδια (On Line Electronic Gambling)***

Αποτελεί την πράξη μέσω της οποίας, 2 ή περισσότερα άτομα συναντώνται στο Διαδίκτυο με σκοπό το στοίχημα. Οι ηλεκτρονικές μηχανές τυχερών παιχνιδιών (electronic Gambling Machines), έχουν πολλά κοινά σημεία με τα παιχνίδια υπολογιστών. Σύμφωνα με τους Collins et al. (2012), οι μηχανές αυτές αρχικά τοποθετούνταν μόνο σε καζίνο όπου η πρόσβαση επιτρεπόταν σε ηλικίες μεγαλύτερες των 21 ετών. Τελευταία όμως η τοποθέτηση τέτοιων μηχανών, επιτρέπεται σε πολλούς χώρους, όπως καφέ, εστιατόρια κλπ. Η ηλεκτρονική τους έκδοση δε, είναι προσβάσιμη σε όλους, μέσα από το Διαδικτυακό περιβάλλον, μέσω και εικονικών μηχανών. Σε μερικές Ευρωπαϊκές χώρες η Διαδικτυακή συμμετοχή σε τέτοια παιχνίδια θεωρείται νόμιμη. Η συμμετοχή σε αυτού του τύπου τα παιχνίδια, μπορεί να οδηγήσει σε οικονομικές απώλειες αλλά επίσης και σε ψυχολογικά προβλήματα όπως εθισμό (K. Collins et al., 2012) (Diomidous et al., 2016).

Ο Κυβερνοχώρος και το Διαδίκτυο γενικότερα, έχει κατηγορηθεί και για μια σειρά άλλων κινδύνων, που σχετίζονται με την κακή χρήση του ή και την υπερβολική χρήση του (internet abuse), η οποία έχει επιπτώσεις στο άτομο και στην συμπεριφορά του (Συμπεριφορικοί κίνδυνοι). Οι επιπτώσεις αυτές στο άτομο ορίζονται, και η έννοια του αυτού του κινδύνου, γενικεύεται, ως κίνδυνος για το ίδιο το άτομο. Άτομα δε όπως παιδιά και έφηβοι επηρεάζονται αρνητικά από την υπερβολική χρήση ή και την κατάχρηση των τεχνολογιών των υπολογιστών και του Διαδικτύου γενικότερα και λόγω της ανωριμότητας, λόγω της ηλικίας, αλλά και άλλων ψυχολογικών παραγόντων, αποτελούν δε μια πιθανή ομάδα κινδύνου. (Andreassen, 2015)

Τέτοιοι κίνδυνοι είναι, ο Διαδικτυακός Εθισμός, Εθισμός στα Online παιχνίδια, Διάφορα Φυσικά Προβλήματα.

## *Διαδικτυακός Εθισμός*

Ο διαδικτυακός Εθισμός αποτελεί άλλη μια μορφή εθισμού και ως διαταραχή είναι επικίνδυνη, όπως και οι άλλες μορφές. Ως διαδικτυακός εθισμός περιγράφεται η αδυναμία διακοπής της υπερβολικής χρήσης του διαδικτύου, η τάση να θεωρείται χωρίς νόημα ο χρόνος εκτός Διαδικτύου και συνοδεύεται από φαινόμενα επιθετικότητας και υπερβολικού ερεθισμού κατά την περίοδο της στέρησης, μια ψυχιατρική κατάσταση που περιλαμβάνει δυσπροσάρμοστες και παθολογικές συμπεριφορές. Η υπερβολική χρήση του Διαδικτύου προκαλεί δυσκολίες στο άτομο, στο σπίτι, στο σχολείο ή στο χώρο εργασίας και στην ψυχολογική ζωή του χρήστη. Οι νέοι είναι πιο επιρρεπείς σε αυτή την μορφή εθισμού καθώς η σχέση τους με την τεχνολογία είναι στενή. Επίσης αυτή η μορφή

εθισμού μπορεί να οδηγήσει και σε άλλες ψυχιατρικές διαταραχές (Öztürk, Bektas, Ayar, Özgüven Öztornacı, & Yağcı, 2015).

Σε όλη την προηγούμενη ενότητα ασχοληθήκαμε με τον κυβερνοχώρο, τους κινδύνους ασφαλείας και τα εργαλεία που χρησιμοποιούν άτομα ή ομάδες για να δημιουργήσουν κινδύνους επιθέσεις κλπ. αλλά και κινδύνους που αφορούν άτομα γενικότερα και που προκύπτουν **από πιθανή λανθασμένη ή και αλόγιστη χρήση του Διαδικτύου**. Ο κυβερνοχώρος όμως δεν απαρτίζεται μόνο από επιτιθέμενους και απατεώνες κάθε είδους. Υπάρχουν και οι συνηθισμένοι χρήστες, οι οποίοι είναι και η πλειοψηφία. Η καταγραφή των δραστηριοτήτων των ανθρώπων που αλληλοεπιδρούν στον Κυβερνοχώρο έχουν κατηγοριοποιηθεί και διαχωρισθεί με διάφορους τρόπους. Όλες οι προσπάθειες κατηγοριοποίησης δεν ήταν ολοκληρωμένες καθώς περιείχαν 2 ή 3 διαφορετικές κατηγορίες χρήσης. Διάφοροι ερευνητές, όπως ο Tavari, ο Spinello, και άλλοι, αναφέρει ο Jaeger (2012) «έχουν διαχωρίσει τις δραστηριότητες του κυβερνοχώρου σε παραλλαγές των υποσυνόλων από μια προοπτική φιλοσοφικών, δεοντολογικών ή ηθικών προβλημάτων» ή αντίστοιχα ο Conway ο οποίος περιέγραψε ένα μοντέλο 3 επιπέδων, σχεδιασμένο που περιέχει εκτός από την κανονική χρήση, την κακή χρήση και την επιθετική χρήση. Ωστόσο ο Jaeger (2012) προτείνει ένα πιο πλήρες μοντέλο καταγραφής της ανθρώπινης συμπεριφοράς στον κυβερνοχώρο 5 επιπέδων. Οι 5 κατηγορίες του Jaeger, είναι «**1.** Χρήση (use) κανονική και νόμιμη χρήση του κυβερνοχώρου, με παραδείγματα το σερφινγκ, τα μηνύματα, ηλεκτρονικό εμπόριο, το ηλεκτρονικό ταχυδρομείο. **2.** Λανθασμένη χρήση (misuse), όπου περιλαμβάνει τις κακές πράξεις που προκαλούν ανωμαλία ή προσβάλουν άλλες διαδικτυακές τοποθεσίες, συμπεριλαμβανομένων των διαμαρτυριών και τους βανδαλισμούς με παραδείγματα την πορνογραφική ηλεκτρονική πειρατεία (hacking) σε εχθρική ιστοσελίδα, πρόσθεση πολιτικού σλόγκαν. **3.** Επιθετική χρήση (offensive use), που περιλαμβάνει πραγματική ζημιά, κλοπή, απάτη, εκβίαση ή εμπορική κατασκοπεία, που δεν είναι εγκλήματα ή που δεν μπορούν πρακτικά να διωχθούν, με παραδείγματα την ηλεκτρονική πειρατεία σε ιατρικά αρχεία διάσημων ατόμων λόγω της περιέργειας και δημόσια διάδοση. **4.** Κυβερνοέγκλημα (Cybercrime), τις εγκληματικές πράξεις με δυνατότητα δίωξης, με παραδείγματα ηλεκτρονική πειρατεία σε βάσεις δεδομένων Τραπεζικών οργανισμών για κλοπή ταυτότητα με σκοπό το κέρδος. **5.** Κυβερνο-τρομοκρατία (Cyberterrorism), εγκλήματα με πολιτικά κίνητρα και παραδείγματα ηλεκτρονική πειρατεία σε συστήματα SCADA (εποπτεία ελέγχου και η απόκτηση δεδομένων/ Supervisory Control and Data

Acquisition) για να ανοίξουν διαρροές των φραγμάτων ή να απενεργοποιηθεί ηλεκτρικό δίκτυο" (Jaeger, 2012).

**Παράγοντες κινδύνων στον Κυβερνοχώρο (Trust)**

Το Διαδίκτυο και ο κυβερνοχώρος επεκτείνει την ανθρώπινη επικοινωνία σχεδόν σε όλες τις ανθρώπινες δραστηριότητες και στη βάση είκοσι τεσσάρων ωρών ημερησίως καθ' όλη την διάρκεια της εβδομάδος.

Οι νέες επιστημονικές και τεχνολογικές καινοτομίες είναι άμεσα συνδεδεμένες με την έννοια της αβεβαιότητας και του κινδύνου. Τα μέλη μιας κοινωνίας βιώνουν και αντιλαμβάνονται την αβεβαιότητα και τον κίνδυνο με διαφορετικό τρόπο από τον αντίστοιχο τρόπο των επιστημόνων. Η αντίληψη της έννοιας του κινδύνου εξαρτάται από την οπτική της πλευράς που εξετάζει τον κίνδυνο. Για παράδειγμα οι εμπειρογνώμονες βλέπουν τον κίνδυνο «ως αλυσίδες αιτιών και γεγονότων» οι απλοί, κοινοί άνθρωποι «έχουν την τάση να τον βλέπουν σε ένα κοινωνικό πλαίσιο σχέσεων». (B. S. Collins & Mansell, 2004)

Το γεγονός της διαφορετικής οπτικής του κινδύνου έχει αναφερθεί και πιθανώς θα αναφερθεί και σε άλλα σημεία της παρούσας εργασίας καθώς αποτελεί και μια ουσιαστική παράμετρο της έννοιας του κινδύνου. Τα μέλη μιας κοινωνίας αντιμετωπίζουν ένα σύστημα κοινωνικό, τεχνικό – τεχνολογικό, με απρόβλεπτους πολλές φορές τρόπους, μπορούν να εμπιστευτούν ή όχι το σύστημα ακόμη και όταν παρουσιάζονται αυξημένοι κίνδυνοι. Οι Frewer et al (1998), αναφέρουν ότι δεν υπάρχει ένα μοναδικός τρόπος να αντιμετωπισθεί οποιαδήποτε νέα τεχνολογία, με την έννοια ενός μοναδικού μοτίβου που θα αποτελεί «ένα είδος προγνωστικής βεβαιότητας» για την αντιμετώπιση της κάθε νέας τεχνολογικής καινοτομίας, καθώς υπάρχουν ιδιαιτερότητες στην κάθε διαφορετική τεχνολογία. Οι άνθρωποι επιλέγουν να χρησιμοποιήσουν μια τεχνολογία στη βάση των αποκομιζόμενων ωφελειών από αυτή και όχι στη βάση των κινδύνων «ή ανησυχούν περισσότερο για τα οφέλη που θα προκύψουν».

Η εμπιστοσύνη αποτελεί τον συνδετικό κρίκο της κοινωνίας, αναφέρει ο Yeo (2013) παραθέτοντας την φράση του John Locke, του 1663 (trust is the bond of society), και επισημαίνει ότι τείνει να συμφωνήσει με αυτό καθώς η εμπιστοσύνη είναι συνυφασμένη με την καθημερινότητα του κάθε ανθρώπου σε οποιαδήποτε πράξη και εάν επιλέξει να υλοποιήσει και ταυτόχρονα συνδεδεμένη και με την έννοια του ρίσκου, του κινδύνου (Yeo, 2013). Ο Slovic (1993) συνδέει την διαχείριση του κινδύνου με την εμπιστοσύνη, ο ίδιος αναφέρει «Πιο πρόσφατα, αναγνωρίστηκε μια άλλη σημαντική πτυχή του προβλήματος της αντίληψης κινδύνου. Αυτός είναι ο ρόλος της εμπιστοσύνης. Τα

τελευταία χρόνια έχουν υπάρξει πολυάριθμα άρθρα και έρευνες που δείχνουν τη σημασία της εμπιστοσύνης στη διαχείριση των κινδύνων και την τεκμηρίωση της εξαιρετικής δυσπιστίας που έχουμε σήμερα σε πολλά από τα άτομα, τις βιομηχανίες και τα ιδρύματα που είναι υπεύθυνα για τη διαχείριση του κινδύνου».

Οι έννοιες της εμπιστοσύνης και του κινδύνου έχουν γίνει όλο και πιο σημαντικές για την κατανόηση της ζωής μέσα σε ένα σύνθετο κοινωνικό-τεχνικό σύστημα (B. S. Collins & Mansell, 2004).

Η εμπιστοσύνη μεταξύ των ανθρώπων, είτε και μεταξύ ανθρώπου και συστήματος, είναι πολύ σημαντική. Είναι δε απαραίτητη σε συστήματα κοινωνικό-τεχνικά όπως ο κυβερνοχώρος. Η διαμεσολαβημένη επικοινωνία (CMC) είναι αποπροσωποποιημένη και οι πραγματικές ταυτότητες των ατόμων που συμμετέχουν και επικοινωνούν στον κυβερνοχώρο και γενικότερα στο Διαδίκτυο δεν φαίνονται, αντίθετα κρύβονται πίσω από διάφορες ιστοσελίδες και ψηφιακούς αντιπροσώπους. Η αίσθηση των ατόμων αναφορικά με την εμπιστοσύνη και το Διαδίκτυο, συχνά είναι συνδεδεμένη με το ηλεκτρονικό εμπόριο- (δεν γνωρίζουν τον προμηθευτή και τις ιδιότητες των προϊόντων, το θέμα της πληρωμής και εάν πληρώσουν κλπ. εάν θα εξασφαλίσουν είτε την παραλαβή του προϊόντος ή της δυνατότητας επιστροφής και πιθανά και άλλες σκέψεις αναφορικά με την εμπιστοσύνη απέναντι στην ίδια την πράξη της εξ αποστάσεως αγοράς- μπορώ να τον εμπιστευτώ?) και της συναλλαγής που πρόκειται να υλοποιήσουν, καθώς και για τα παρεχόμενα στοιχεία που ο κάθε συναλλασσόμενος στην ψηφιακή εποχή παρέχει στο ψηφιακό χώρο. Η παροχή προσωπικών στοιχείων εγείρει μια ανησυχία στο άτομο (πολλές φορές ακόμη και στην άμεση συναλλαγή στα χαρτιά, όταν απέναντι μας έχουμε κάποιον που δεν τον γνωρίζουμε) ειδικά όταν δεν γνωρίζεις με ποιον τρόπο θα χρησιμοποιηθούν τα προσωπικά σου στοιχεία από κάποιον άγνωστο με τον οποίο πρέπει να συνδιαλλαγείς. Ανησυχία επίσης μπορεί να εγείρεται και αναφορικά με τις εφαρμογές λογισμικού ή ακόμη και για τα συστήματα που διαμεσολαβούνται στην οποιαδήποτε ψηφιακή επικοινωνία (Yeo, 2013). Καθοριστικό σημείο για την εμπιστοσύνη στον κυβερνοχώρο, υποστηρίζει η Yeo (2013), αποτελεί η προέλευση και η ακεραιότητα των δεδομένων και της πληροφορίας. Είναι απαραίτητο να μπορούμε να βασιστούμε στη γνώση και στις πληροφορίες που παρέχουν οι ειδικοί και οι εμπειρογνώμονες. Είναι αυτοί που μπορούν και πρέπει να παίζουν καθοριστικό ρόλο στην διασφάλιση της εμπιστοσύνης. Οι τεράστιες δυνατότητες που παρέχει η ψηφιακή επικοινωνία και ο διαμοιρασμός της γνώσης και της πληροφορίας, ο τεράστιος όγκος πληροφοριών με τον οποίο στην καθημερινότητα βρισκόμαστε απέναντι, είναι πολύ σημαντικό να γνωρίζουμε

τί ή ποια πληροφορία ή ποια γνώση ή ποιον πρέπει να εμπιστευτούμε. Σε κάθε παρεχόμενη πληροφορία από όπου και εάν προέρχεται αυτή, από οποιοδήποτε οργανισμό ή επιχείρηση, όσο αξιόπιστη και εάν είναι αυτή, τελικά αυτός που θα αξιολογήσει την τελική πληροφορία είναι ο κάθε ένας από εμάς. Η αξιοπιστία και η φήμη του προμηθευτή είναι σημαντική- σε πράξεις αγοραπωλησιών μέσω του διαδικτύου, όπως παραδείγματος είναι πολύ πιθανότερο να εμπιστευτούμε ένα γνωστό προμηθευτή βιβλίων από έναν άγνωστο - αλλά ακόμη και αυτό βασίζεται στην δική μας αντίληψη. Αντίστοιχη είναι και η αντίληψη και η γνώση για τον οργανισμό ή τον ειδικό ή τους εμπειρογνώμονες από όπου έρχεται η πληροφορία. Η φήμη και η αξιοπιστία του Οργανισμού είναι σημαντική και πολλές φορές είναι πολύ πιθανό να εμπιστευτούμε κάποιον άγνωστο με βάση την σύνδεσή της με κάποια πηγή στην οποία έχουμε εμπιστοσύνη. Η κρίση του καθένα από εμάς είναι πολύ σημαντική καθώς αποτελεί το καθοριστικό στοιχείο στο οποίο θα βασιστούμε για να αξιολογήσουμε την παρεχόμενη πληροφορία (Yeo, 2013).

Για τους Collins & Mansell (2004), η εμπιστοσύνη μπορεί να αποτελέσει σε δυναμικά κοινωνικό τεχνικά συστήματα, όπως ο κυβερνοχώρος, καθοριστικό παράγοντα για την πρόβλεψη νέων μέτρων για την πρόληψη κατά των εγκλημάτων που μπορούν να διεξαχθούν σε αυτόν. Έννοιες όπως εμπιστοσύνη και κίνδυνος είναι χαρακτηριστικά τα οποία εμπεριέχονται σε κάθε κοινωνικό τεχνικό σύστημα και οι άνθρωποι αξιολογούν τόσο τους κινδύνους όσο και την αξιοπιστία του συστήματος. Ο κυβερνοχώρος ως σύστημα είναι το κέντρο πολλών τεχνολογικών-τεχνικών αλλά και κοινωνικών ιδιοτήτων, που δεν είναι ως τέτοιες καινούριες, αλλά τομείς τους όπως η διαχείριση ψηφιακών ταυτοτήτων, οι διαδικασίες και τα εργαλεία που χρησιμοποιούνται προκειμένου να καταστεί η ανταποδοτικότητα και η αξιοπιστία του συστήματος είναι πολύ σημαντικοί για την λειτουργία του και κατ' επέκταση και για τους χρήστες του. Η εμπιστοσύνη σε ένα σύστημα και ειδικότερα στις Τεχνολογίες Πληροφοριών και Επικοινωνιών, αποτελεί παράγοντα υλοποίησης μιας οποιασδήποτε πράξης. Η αντίληψη του κινδύνου επίσης μπορεί να ενισχυθεί ή να μειωθεί ανάλογα με διάφορους παράγοντες κοινωνικούς και τεχνικούς. Η ανθρώπινη συμπεριφορά απέναντι στους κινδύνους είναι κάθε φορά σχετική. Οι άνθρωποι είναι διατεθειμένοι να επιδείξουν εμπιστοσύνη σε κάποιο κοινωνικοτεχνικό σύστημα ανεξαρτήτως του εάν αντιλαμβάνονται υψηλό ή χαμηλό δείκτη κινδύνου. Θέματα που απαιτούν εμπιστοσύνη προς τον κυβερνοχώρο ως σύστημα είναι η ασφάλεια και η αξιοπιστία του ως σύστημα, που θα πρέπει να εξασφαλίζεται, που μπορεί να αφορά αρχικά τα συστήματα

υπολογιστών, η ταυτοποίηση και ο έλεγχος της ταυτότητας στον κυβερνοχώρο, με τρόπο που θα εξασφαλίζεται η αναγνώριση πρόσωπο με πρόσωπο (αντίστοιχη της δια ζώσης αντίστοιχης επικοινωνίας) που θα πρέπει να εξευρεθούν ισοδύναμα αναγνώρισης προσώπων με πρόσωπα ή και χειρόγραφων υπογραφών (B. S. Collins & Mansell, 2004).
Η αξιοπιστία ενός συστήματος όπως ο κυβερνοχώρος (διαδικτυακού πληροφοριακού συστήματος που ενσωματώνει υπολογιστικά συστήματα, συστήματα επικοινωνιών και ανθρώπους ως χρήστες αλλά και ως χειριστές), είναι πολυδιάστατη. Περιέχει στοιχεία όπως η ορθότητα, η αξιοπιστία, η ασφάλεια (με τις συμβατικές έννοιες του απορρήτου, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας), της ιδιωτικής ζωής, της ασφάλειας της φυσικής ζωής – ανθρώπινης ύπαρξης- και της επιβίωσης, και όλα αυτά πρέπει να εξασφαλίζονται ώστε να εξασφαλίζεται η κατά το δυνατόν, με λιγότερους κινδύνους, λειτουργία του. Είναι μάλλον γνωστό, ότι δύσκολα, κάτι τέτοιο επιτυγχάνεται, καθώς η κάθε διάσταση δεν είναι αυτόνομη, η ίδια η αξιοπιστία εξαρτάται από όλες τις σχετικές διαστάσεις και πιθανά κάποιες εξ αυτών, όπως η ασφάλεια, να αποτελεί μεγαλύτερη πρόκληση, αλλά τελικά είναι μια πρόκληση προς υλοποίηση και όπως αναφέρουν οι Collins and Mansell “cyberspace is being developed in an environment that Beck and Giddens have called the ‘risk society” (B. S. Collins & Mansell, 2004).

## 2.4 Κοινωνικά Δίκτυα & Κοινωνικά Μέσα

### *2.4.1* Γενικά για τα Κοινωνικά Δίκτυα ( Social Networks) & Κοινωνικά Μέσα (Social Media)

Πρωτοπόροι της Κοινωνιολογίας (και στα Κοινωνικά Δίκτυα) θεωρούνται οι Emile Durkheim (Γάλλος Κοινωνιολόγος) και ο Γερμανός Ferdinand Tonnies ( Γερμανός Κοινωνιολόγος) προς το τέλος του 18ο αιώνα (Edosomwan, Prakasan, Kouame, Watson, & Seymour, 2011).
Σύμφωνα με τους Wasserman & Faust (1994) ένα κοινωνικό Δίκτυο συν αποτελείται, απαρτίζεται από ανθρώπινες οντότητες και τις μεταξύ των σχέσεις. Την έννοια του κοινωνικού Δικτύου εντοπίζουμε στην βιβλιογραφία κάτω από διαφορετικούς ορισμούς. Οι Walker et al. (1977), περιγράφουν το κοινωνικό δίκτυο, και καθορίζουν επίσης τα χαρακτηριστικά τα οποία το χαρακτηρίζουν. Αναφέρουν ότι το κοινωνικό δίκτυο του ατόμου ορίζεται σαν το σύνολο επαφών μέσω των οποίων διατηρεί την κοινωνική του ταυτότητα, από τους οποίους υποστηρίζεται συναισθηματικά, υλικά με την λήψη

υπηρεσιών πληροφοριών αλλά και αποτελεί επέκταση των επαφών του. Έτσι το κοινωνικό δίκτυο του ατόμου απαρτίζεται από φίλους συγγενείς, συναδέλφους και συνεργάτες και ενώνονται με δεσμούς φιλίας και κοινά συμφέροντα. Τα χαρακτηριστικά του Κοινωνικού Δικτύου είναι **α.** το μέγεθος, ένα σύνολο ατόμων με τα οποία διατηρεί ένα κοινωνικό δεσμό, **β.** Αντοχή των δεσμών, ένα σύνολο συνδυαστικών χαρακτηριστικών, όπως είναι τα κοινά συμφέροντα, η οικειότητα κ.α. **γ**. Πυκνότητα, που είναι ο βαθμός που τα μέλη ενός κοινωνικού δικτύου επικοινωνούν μεταξύ τους χωρίς απαραίτητα την παρουσία του αρχικού μέλους, **δ**. Ομοιογένεια του Δικτύου, του οποίου τα μέλη μοιράζονται κοινά χαρακτηριστικά, ηλικία, φύλο, εθνικότητα κοινωνική θέση, επιδεικνύουν παρόμοιες συμπεριφορές σε κοινωνικές αξίες και τον τρόπο ζωής και **ε.** Την διασπορά των μελών, που αποτελεί τον τρόπο με τον οποίο τα μέλη επικοινωνούν διαπροσωπικά σε γεωγραφική απόσταση, όπως και το μέσο μεταφοράς (Walker et al., 1977).

Αυτό αποτελούσε το κοινωνικό Δίκτυο του ατόμου (εκτός της σφαίρας του Διαδικτύου και των υπολογιστών), στο παρελθόν, όπου η αναφορά σε ένα κοινωνικό Δίκτυο αφορούσε μια κοινωνική εκδήλωση με συμμετοχή ατόμων, φίλων σε ένα φιλικό περιβάλλον για ποτό ή τσάι. Σήμερα ο όρος Κοινωνικό Δίκτυο έχει μετατεθεί και αναφέρεται πρωτίστως σε ένα ηλεκτρονικό περιβάλλον και η προσωπική επαφή (face to face) έχει αντικατασταθεί από την διαμεσολαβημένη μέσω υπολογιστή επικοινωνία (Kapoor, n.d.). Παρόλα αυτά κάποια από τα στοιχεία που αναφέρουν οι Walker et al, είναι κοινά με τα νέα Κοινωνικά Δίκτυα, όπου η Διαμεσολαβημένη επικοινωνία μέσω υπολογιστών είναι το κυρίαρχο στοιχείο.

Τα κοινωνικά δίκτυα μπορούν να εκτείνονται σε ένα εύρος που να ξεκινούν από παραδοσιακά κοινωνικά δίκτυα, όπως η μεταξύ ατόμων ανταλλαγή αλληλογραφίας μέχρι τα τεχνολογικά δίκτυα που συνδέουν υπολογιστές μεταξύ τους στο Διαδίκτυο και τα αντίστοιχα κοινωνικά δίκτυα, που έχουν ενώσει ανθρώπους μεταξύ τους. (Kleinberg, 2008).

Ο όρος Social Media σύμφωνα με τους Hwang & Kim, (2015) αναφέρεται σε ένα σύνολο διαδικτυακών εφαρμογών οι οποίες βασίζονται σε ιδεολογικά και τεχνολογικά θεμέλια του Web 2.0 που επιτρέπουν τον διαμοιρασμό περιεχομένου (ιδέες, σκέψεις), που δημιουργούν οι ίδιοι οι χρήστες.

Οι Kaplan & Haenlein (2009) αντίστοιχα υιοθετούν την ίδια ορολογία, αλλά επιπλέον αναφέρουν ότι μέσα σε αυτόν τον γενικότερο όρο της έννοιας του Κοινωνικού Μέσου (Social Media) υπάρχει μια κατηγοριοποίηση των εφαρμογών σε επιμέρους κατηγορίες,

ανάλογα με τις δύο έννοιες που ενυπάρχουν σε αυτόν- ο όρος Κοινωνικός (Social) και ο όρος του Μέσου (Media). Ό όρος του μέσου Media, σύμφωνα με το λεξικό αναφέρεται σε «Τα μέσα είναι ο πληθυντικός τύπος μέσου, ο οποίος (σε γενικές γραμμές) περιγράφει κάθε κανάλι επικοινωνίας. Αυτό μπορεί να περιλαμβάνει οτιδήποτε από τυπωμένο χαρτί έως ψηφιακά δεδομένα και περιλαμβάνει τέχνη, ειδήσεις, εκπαιδευτικό περιεχόμενο και πολλές άλλες μορφές πληροφόρησης. Τα ψηφιακά μέσα, τα οποία αποτελούν ένα ολοένα και πιο τεράστιο τμήμα των σύγχρονων επικοινωνιών, αποτελούνται από περίπλοκα κωδικοποιημένα σήματα που μεταδίδονται μέσω διαφόρων μορφών φυσικών και εικονικών μέσων, όπως καλώδιο οπτικών ινών και δίκτυα υπολογιστών» ("What is Media?," n.d.)

Μέσα από μια σύνθεση των ανωτέρω, **Κοινωνικά Μέσα,** πιο συγκεκριμένα, είναι «οι εφαρμογές και οι ιστότοποι που βασίζονται στο Διαδίκτυο, που προωθούν την κοινή χρήση περιεχομένου που δημιουργείται από χρήστες, την επικοινωνία και τη συμμετοχή σε μεγάλη κλίμακα». Οι εφαρμογές αυτές περιλαμβάνουν διαφορετικά είδη όπως blogs, Κοινωνικά Δίκτυα και podcasts ήχου (Cooper, 2019). Ένα blog σύμφωνα με το Merriam Webster λεξικό είναι 2 πράγματα, 1: «υπολογιστές: ένας ιστότοπος που περιέχει ηλεκτρονικές προσωπικές αναλύσεις, σχόλια και συχνά υπερσυνδέσεις, βίντεο και φωτογραφίες που παρέχονται από τον συγγραφέα και επιπλέον, το περιεχόμενο ενός τέτοιου ιστότοπου» και 2: «ένα κανονικό χαρακτηριστικό που εμφανίζεται ως τμήμα μιας ηλεκτρονικής δημοσίευσης που συνήθως σχετίζεται με ένα συγκεκριμένο θέμα και αποτελείται από άρθρα και προσωπικά σχόλια από έναν ή περισσότερους συγγραφείς» ("Definition of BLOG," n.d.) Πολλές ιστοσελίδες φιλοξενούν blogs χρηστών με πολύ γνωστό παράδειγμα το WordPress. Άλλη μορφή συνεργατικής δημιουργίας περιεχομένου είναι τα "Wikis" ιστότοποι στους οποίους οι χρήστες δημιουργούν «ενημερωτικό περιεχόμενο» και παράδειγμα αυτής της μορφής είναι η Wikipedia. Ακόμη μια μορφή Κοινωνικών Μέσων είναι και τα Διαδικτυακά παιχνίδια πολλών παικτών (Multiplayer Online Games) στα οποία οι χρήστες επικοινωνούν μεταξύ τους κατά την διάρκεια του Διαδικτυακού παιχνιδιού συμμετέχοντας σε ένα εικονικό κόσμο (virtual world). Δημοφιλή παιχνίδια τέτοιου τύπου είναι το World of Warcraft, αλλά και το Second Life που δίνει την δυνατότητα στους χρήστες να δημιουργούν Avatar, στην αλληλεπίδραση με τους άλλους χρήστες. Μηνύματα ηλεκτρονικού ταχυδρομείου, ανταλλαγή άμεσων μηνυμάτων αλλά και κοινή χρήση βίντεο αποτελούν πιο γενικές κατηγορίες Κοινωνικών Μέσων, ιδιότητες που έχουν ενσωματωθεί σε Κοινωνικά Δίκτυα (Cooper, 2019).

Ο όρος Κοινωνικά Δίκτυα Social Networks Sites (SNSs), σύμφωνα με τους Boyd & Ellison (2007), αναφέρεται σε Διαδικτυακές υπηρεσίες: α. που επιτρέπουν στους χρήστες να δημιουργούν ένα δημόσιο ή ημιδημόσιο προφίλ σε ένα οριοθετημένο σύστημα, β. να δημιουργούν λίστα με άλλους χρήστες με τους οποίους είναι διασυνδεδεμένοι και γ. να βλέπουν τους διασυνδεδεμένους χρήστες των επαφών τους. Η διασύνδεση μεταξύ των χρηστών εξαρτάται κάθε φορά από το site. Παράδειγμα πολύ δημοφιλούς Κοινωνικού Δικτύου είναι το Facebook.

Podcast είναι «ένας τύπος ψηφιακού μέσου, συνήθως ήχου, που διατίθεται σε μια σειρά επεισοδίων ή τμημάτων και μεταδίδεται με ροή ή μεταφορτώνεται από τον τελικό χρήστη μέσω του Διαδικτύου. Τα podcasts μπορούν να διατεθούν προγραμματισμένα ή να φορτωθούν τυχαία στον ιστό» ("What is a Podcast?," n.d.)

Όπως έχει ήδη αναφερθεί, η επικοινωνία στα Κοινωνικά Δίκτυα είναι διαμεσολαβημένη μέσω υπολογιστή. Η Διαμεσολαβημένη Επικοινωνία μέσω υπολογιστή, περιλαμβάνει διάφορα συστήματα ηλεκτρονικών μηνυμάτων, ηλεκτρονικά συστήματα τηλεδιασκέψεων, που εμπλουτίζονται με ήχο και βίντεο συνδέσεων και μπορεί να είναι σύγχρονη (συνομιλία/chat) ή ασύγχρονη (ηλεκτρονικό ταχυδρομείο/email). (Derks, Fischer, & Bos, 2008)

### 2.4.2 Διαφορές μεταξύ Κοινωνικών Δικτύων - Κοινωνικών Μέσων

Ενώ οι όροι Social Media και Social Network χρησιμοποιούνται πολλές φορές με την ίδια έννοια, αλλά και εναλλάξ, είναι δύο διαφορετικά πράγματα.

Κοινωνική Δικτύωση είναι, όπως έχει ήδη αναφερθεί, «η δραστηριότητα ανταλλαγής πληροφοριών και επικοινωνίας με ομάδες ατόμων που χρησιμοποιούν το διαδίκτυο, ιδίως μέσω ιστοσελίδων ειδικά σχεδιασμένων για το σκοπό αυτό» ("SOCIAL NETWORKING | meaning in the Cambridge English Dictionary," n.d.)

Τα Κοινωνικά Μέσα (Social Media) σύμφωνα με τους Edosomwan et al. (2011), είναι τα μέσα που χρησιμοποιεί το άτομο για τη μετάδοση και ανταλλαγή πληροφοριών κατά την αλληλεπίδρασή του με άλλα άτομα. Κοινωνική Δικτύωση (Social Networking) είναι η πράξη κατά την οποία τα άτομα που έχουν κοινά ενδιαφέροντα εμπλέκονται, συνδέονται, προκειμένου να δημιουργήσουν σχέσεις και συνεργασίες «μέσω της κοινότητας». Στην πραγματικότητα υπάρχουν αρκετές διαφορές μεταξύ των δύο διαφορετικών εννοιών/ορολογιών. Η πρώτη αφορά τον ορισμό, (ορισμοί οι οποίοι ήδη αναφέρθηκαν). Η δεύτερη διαφορά αναφέρεται στον τρόπο επικοινωνίας. Το Κοινωνικό Μέσο είναι το σύστημα, ένα κανάλι επικοινωνίας, όχι μια διεύθυνση επικοινωνίας ή μια τοποθεσία

επίσκεψης. Το κοινωνικό Δίκτυο έχει την επικοινωνία στο κέντρο της, μια επικοινωνία 2 κατευθύνσεων, αμφίδρομη που οδηγεί στην δημιουργία και ανάπτυξη σχέσεων. Ως Τρίτη διαφορά αναφέρουν την "διαφορά απόδοσης επένδυσης" (Return of Investment ROI) μεταξύ των δύο μέσων. Ως τέταρτη διαφοροποίηση, τη μη αυτοματοποιημένη δραστηριότητα στα Κοινωνικά Μέσα, στα οποία η απάντηση σε ερωτήσεις ή της ενημέρωσης, είναι μια διαδικασία που απαιτεί χρόνο και κόπο, ενώ η επικοινωνία στα Κοινωνικά Δίκτυα είναι άμεση μεταξύ των επαφών που ο χρήστης θα επιλέξει να συνομιλήσει ή να αλληλοεπιδράσει. Τέλος τα κοινωνικά Μέσα δεν επιτρέπουν την διαχείριση σχολίων, ή την διόρθωση λαθών ή οποιαδήποτε άλλα δεδομένα από τους χρήστες για λόγους έκφρασης όπως επαγγελματικής ή προσωπικής άποψης (Edosomwan et al., 2011).

### 2.4.3 Υπηρεσίες στα Μέσα Κοινωνικής Δικτύωσης & Χρήση

Το εύρος των παρεχόμενων υπηρεσιών που προσφέρουν τα Μέσα κοινωνικής Δικτύωσης στους χρήστες τους, ποικίλουν – ανάλογα με το site, όπως και το εύρος των ενδιαφερόντων αλλά και των πρακτικών που προωθεί το κάθε μέσο (Social Network Site). Διασύνδεση μεταξύ ατόμων γνωστών μεταξύ τους ή ακόμη και άγνωστων, στη βάση κοινών ενδιαφερόντων κοινωνικών ή πολιτικών ή πολιτιστικών ή εθνικών ή φυλετικών ή φύλλου ή και κάθε άλλου τύπου. Ενσωμάτωση τηλεπικοινωνιακών υπηρεσιών, υπηρεσίες διαμοιρασμού video, φωτογραφιών κλπ. (Boyd & Ellison, 2007).
Εφαρμογές όπως το Facebook και το Myspace, αφορούν κυρίως φιλικού τύπου διασυνδέσεις και χρησιμοποιούνται κυρίως για διασκέδαση και επικοινωνία και εφαρμογές και πλατφόρμες όπως το LinkedIn, κυρίως για επαγγελματικές επαφές. (Kapoor, n.d.). Η δομή ενός κοινωνικού Δικτύου είναι συνήθως απλή. Ο χρήστης συνδέεται στο κοινωνικό Δίκτυο δημιουργώντας ένα προφίλ που περιέχει αρχικά προσωπικές πληροφορίες, τα ενδιαφέροντά του (βιβλία, μουσική κ.α.) και φυσικά τις επαφές του, φίλους. Η πρόσθεση επαφών/φίλων τις περισσότερες φορές και ανάλογα με την πλατφόρμα ή το Μέσο Κοινωνικής Δικτύωσης απαιτεί την αποδοχή του προστιθέμενου. (Kapoor, n.d.). Σύμφωνα με τους Boyd & Ellison (2007) «η δημόσια εικόνα των επαφών του χρήστη είναι ένα ζωτικό συστατικό των ιστοσελίδων κοινωνικής δικτύωσης» (Boyd & Ellison, 2007).
Σύμφωνα με τους Boyd & Ellison (2007) η μοναδικότητα των Δικτύων κοινωνικής Δικτύωσης οφείλεται όχι τόσο στην δυνατότητα συνάντησης αγνώστων μεταξύ τους ατόμων, αλλά μάλλον εξαιτίας της δυνατότητας δημοσιοποίησης των προσωπικών

κοινωνικών δικτύων του καθενός εξ αυτών, που μπορεί να οδηγήσει σε πιθανή διασύνδεση με άλλα άτομα, διασύνδεση που διαφορετικά δεν θα ήταν δυνατή (Boyd & Ellison, 2007).

Τα κοινωνικά Δίκτυα επιτρέπουν στους χρήστες να επικοινωνούν, να κοινοποιούν σκέψεις ιδέες, φωτογραφίες, είτε μεταξύ φίλων είτε και μεταξύ αγνώστων (publicly) μεταξύ τους είτε μέσω του Διαδικτύου και του υπολογιστή τους είτε μέσω των κινητών τους τηλεφώνων. (Kapoor, n.d.).

### 2.4.4 Ιστορική Αναδρομή - Σύντομη Ανασκόπηση των Μέσων Κοινωνικής Δικτύωσης (Ιστότοπων Κοινωνικής Δικτύωσης)

Απαραίτητη προϋπόθεση για την ύπαρξη των Κοινωνικών Δικτύων όπως τα γνωρίζουμε σήμερα υπήρξε βέβαια η ανάπτυξη του Διαδικτύου και του παγκόσμιου ιστού WWW (World Wide Web).

Οι Edosomwan et al. (2011) αναφέρουν ότι η δημιουργία του ηλεκτρονικού ταχυδρομείου **(email)** αποτελεί μια πρώτης μορφής κοινωνικού Δικτύου, την δεκαετία του 1960, αν και το Διαδίκτυο έγινε διαθέσιμο στο κοινό μόλις το 1971. Το ηλεκτρονικό ταχυδρομείο αποτελούσε μια πρώτης μορφής επικοινωνία μεταξύ δύο διαδικτυακά συνδεμένων υπολογιστών για την αποστολή και λήψη ηλεκτρονικού ταχυδρομείου. Ακολουθεί η δημιουργία του **APRANET (1969),** μιας πρώιμης μορφής δικτύου υπολογιστών διαμοιρασμού χρόνου (time-sharing) που αποτέλεσε και την βάση του Διαδικτύου. Τρίτη μορφή δικτύου αποτελεί η **CompuServe** το 1969, που αποσκοπούσε σε υπηρεσίες διαμοιρασμού χρόνου, υπό καθεστώς ενοικίασης, χρόνου υπολογιστών της εταιρείας. Ακολουθεί την δεκαετία του 1970 «η δημιουργία παιχνιδιών εικονικού κόσμου σε πραγματικό χρόνο με παιχνίδια ρόλων, διαδραστική φαντασία και διαδικτυακή ομιλία» τα αποκαλούμενα **MUD** (Multi User Domain or Multi User Dimension or Multi User Dungeon), των οποίων η δομή ήταν γραπτό κείμενο από χρήστες, που πληκτρολογούσαν εντολές «χρησιμοποιώντας μια φυσική γλώσσα». Το 1978 δημιουργείται το «Σύστημα Πίνακα Ανακοινώσεων» **BBS** (Board Bulletin Boards- που θεωρείται και ο προκάτοχος του Παγκόσμιου ιστού (www)), στο οποίο οι χρήστες συνδέονταν με σκοπό τη φόρτωση ή κατέβασμα λογισμικού, την ενημέρωση ή και την ανταλλαγή μηνυμάτων. Η σύνδεση υλοποιούνταν μέσω modem (διαμορφωτή) και μιας τηλεφωνικής συσκευής και έναν χρήστη την φορά. Και το επόμενο βήμα αποτελεί η δημιουργία του **Usenet** το 1980, ένα είδος δικτύου για ανάρτηση άρθρων ή ειδήσεων, το οποίο δεν χρησιμοποιούσε μόνο έναν διακομιστή (server) ή διαχειριστή, αλλά οι ειδήσεις

προωθούνταν μέσα από διαφορετικούς διακομιστές (servers) για την ροή ειδήσεων. (Edosomwan et al., 2011).

Τα τεχνολογικά θεμέλια στα οποία βασίζονται τα Κοινωνικά Δίκτυα (Social Media) είναι το Web 2.0, μια τεχνολογία που εμφανίζεται το 2004 και περιγράφει μια δεύτερη γενιά του World Wide Web, που προσδιορίζεται στην ικανότητα των χρηστών να συνεργάζονται και να ανταλλάσσουν πληροφορίες διαδικτυακά - δημιουργία περιεχομένου από όλους τους χρήστες με συνεργατικό και συμμετοχικό τρόπο (UGC User Generated Content). Το κλίμα που δημιουργήθηκε από την εμφάνιση του Web 2, άλλαξε τις επιχειρήσεις, το εμπόριο και το τοπικό, από εκείνο το σημείο και μετά, έγινε παγκόσμιο, είτε αυτό ήταν Μέσα Μαζικής Ενημέρωσης, είτε επιχειρήσεις (Eder, 2012) Οι Kaplan & Haenlein (2009), ωστόσο, περιγράφουν ένα περιστατικό (περίπου 20 χρόνια νωρίτερα από το 2004), αναφορικά με το πρώτο blog που δημιούργησαν οι ο Bruce και η Susan Abelson, το «Open Diary», που αφορούσε την διασύνδεση συγγραφέων ημερολογίου σε έναν «πρώιμο ιστότοπο κοινωνικής δικτύωσης», που ενώ το ονόμασαν "Weblog" τελικά «γελοιωδώς», όπως αναφέρουν, το μετονόμασε ένας blogger σε «we blog»» ένα χρόνο αργότερα.

Στην δεκαετία του 1990, δημιουργούνται αρκετές πλατφόρμες κοινωνικής δικτύωσης.

**Το SixDegrees.com** θεωρήθηκε ευρέως, ότι είναι η πρώτη ιστοσελίδα Κοινωνικής, που δημιουργήθηκε **το 1997**, με κύρια χαρακτηριστικά την δημιουργία προφίλ του χρήστη την δημιουργία λίστας φίλων και στις αρχές του 1998 επέτρεψε την περιήγηση στις λίστες φίλων. Και τα δύο χαρακτηριστικά του SixDegrees.com (δημιουργία προφίλ και λίστα φίλων υπήρχαν ανεξάρτητα ως ιδιότητες σε άλλα site) (Boyd & Ellison, 2007). Το όνομά του βασίζεται στο «six degrees of separation» έξι βαθμοί διαχωρισμού στην βάση του ότι τα άτομα διαχωρίζονται μεταξύ τους από 6 ή λιγότερες κοινωνικές επαφές (Hayes, 2000), που το έκανε γνωστό το 1990 ο John Guare σε ένα ομώνυμο έργο. Σύμφωνα με τον Kleinberg (2008) αυτό βασιζόταν στα πειράματα που διεξήγαγε ο Ψυχολόγος Stanley Milgram "the small world experiment" το 1967 (Barabasi, 2012). Το Sixdegrees.com το έτος 2000, σταμάτησε να παρέχει τις υπηρεσίες του, για λόγους επιχειρηματικής βιωσιμότητας (Boyd & Ellison, 2007).

**LiveJournal** ιστοσελίδα το **1999** και τα άτομα χαρακτηρίζουν άτομα ως φίλους με σκοπό την παρακολούθηση των περιοδικών τους και για να διαχειριστούν τις ρυθμίσεις απορρήτου.

**Cyworld**, (εικονικός κόσμος) **το 1999,** ιστοσελίδα στην Κορέα η οποία προσθέτει λειτουργίες διαχείρισης φίλων το 2001 (Boyd & Ellison, 2007).

**LunaStorm το 2000** (επίσημα). Σουηδική εμπορική «διαδικτυακή κοινότητα» που περιείχε φίλους, βιβλίο επισκεπτών αλλά και σελίδες ημερολογίου. Η LunaStorm ξεκίνησε το 1996, σχεδιάστηκε από τον Richard Ericsson, αφορούσε εφήβους και θεωρείται η πρώτη Ευρωπαϊκή ψηφιακή κοινότητα (Boyd & Ellison, 2007) (Edosomwan et al., 2011).

**Ryze.com** το 2001, με σκοπό την ενδυνάμωση των επιχειρηματικών δικτύων ατόμων. Πρώτη παρουσίαση του ιδρυτή τους σε ομάδα φίλων του, κυρίως επιχειρηματίες επενδυτές – οι οποίοι αποτέλεσαν και τους μελλοντικούς επενδυτές των επόμενων δημιουργηθέντων πλατφορμών κοινωνικής δικτύωσης. Οι ιστοσελίδες www.Tribe.net, www.LinkedIn.com και www.friendster.com συνδέθηκαν επαγγελματικά με την Ryze.com (Boyd & Ellison, 2007).

**Wikipedia 2001** Ξεκίνησε με 270 εισαγωγικά άρθρα και σε ένα χρόνο αυξήθηκαν σε 19700 άρθρα, που αναδεικνύουν την σπουδαιότητα του δικτύου (Eder, 2012).

**Friendster 2002** Ξεκίνησε με στόχο να ενώσει φίλους για να συναντηθούν. Τα μέλη του αυξήθηκαν πολύ γρήγορα, καθώς 3 διαφορετικές ομάδες «υιοθέτησαν» την χρήση του (bloggers, gay men και καλλιτέχνες). Επέτρεπε στους χρήστες να δημιουργούν προφίλ και να μπορούν να δουν φίλους φίλων μέχρι και 4 βαθμούς, περιορισμός, που οδήγησε τους χρήστες, να δημιουργούν ψεύτικα προφίλ. Προβλήματα τεχνικά και κοινωνικά οδήγησαν σε απογοητευμένους χρήστες (Boyd & Ellison, 2007).

**LinkedIn 2002** Ξεκίνησε με έδρα την Καλιφόρνια. Ιδρυτές της οι Reid Hoffman ,Allen Blue, Konstantin Guericke Eric Ly και Jean-Luc Vaillant και ξεκίνησε δραστηριότητα το 2003. Σκοπός του LinkedIn οι επαγγελματικές επαφές του χρήστη (διαφορετικός προσανατολισμός από τις μέχρι τότε αντίστοιχες πλατφόρμες που είχαν ψυχαγωγικό στόχο). Το προφίλ του χρήστη εδώ, περιέχει στοιχεία επαγγελματικά, πληροφορίες σχετικές με εργασιακό υπόβαθρο, ιστορικό εκπαίδευσης, απασχόλησης και η διαφήμιση των προσωπικών τους δεξιοτήτων. Η προώθηση της σταδιοδρομίας προς αναζήτηση εργασίας και οι συστάσεις από άλλους χρήστες αποτελούν χαρακτηριστικά της. Επίσης από το 2005 οι εταιρείες μπορούσαν να δημοσιεύουν λίστες εργασίας και να αναζητούν εργαζόμενους. Το 2011, το LinkedIn, είχε πάνω από 100 εκατομμύρια μέλη και το 2016 «αποκτήθηκε από την Microsoft» με παρουσία σε πάνω από 200 χώρες και 500 εκατομμύρια μέλη (Gregersen, n.d.).

**MySpace 2003** ως ανταγωνιστική πλατφόρμα προς τις Friendster, Xanga και της AsianView (Boyd & Ellison, 2007). Συνιδρυτές Chris DeWolfe, Brad Greenspan, Tom Anderson και Josh Berman. Ο Bran Greenspan ήταν συνιδρυτής και Διευθύνων

Σύμβουλος της eUniverse και χρησιμοποίησε τις υποδομές της, για την δημιουργία του MySpace. Πολύ νωρίς απέκτησε πολλούς χρήστες, αρχικά από τους εγγεγραμμένους χρήστες της eUniverse, αλλά επίσης προσέλκυσε και πολλούς καλλιτέχνες και μουσικά συγκροτήματα, οι οποίοι μπορούσαν να διαφημίζουν την δουλειά τους, μέσω της πλατφόρμας. Οι χρήστες της ήταν κυρίως νεαρά άτομα και έφηβοι. Μεταξύ 2005 και 2008 ήταν η πιο δημοφιλής πλατφόρμα κοινωνικής δικτύωσης στον κόσμο (Jowitt, 2017).

**Facebook 2004** Ιδρύθηκε από ομάδα φοιτητών του Harvard university με επικεφαλής τον Mark Zuckerberg (και τους Eduardo Saverin, Dustin Moskovitz, and Chris Hughes). Ξεκίνησε κυρίως δραστηριότητα, αρχικά μόνο σε φοιτητές του Harvard και γρήγορα επεκτάθηκε και σε άλλα πανεπιστήμια, όπως το MIT και το Stanford. Μετά το 2006 δόθηκε προσβασιμότητα σε αυτό, ανεξαρτήτου φοιτητικής ιδιότητας, από την ηλικία των 13 ετών. Σήμερα το Facebook ξεπερνά τα 2.3 δισεκατομμύρια χρήστες, που ο αριθμός αυτός αντιστοιχεί στο 1/3 του παγκόσμιου πληθυσμού (Terrell, 2015).

Πολλές ιστοσελίδες Κοινωνικών Δικτύων δημιουργήθηκαν από το 2003 και μετά και σε συντομία θα αναφέρουμε κάποιες.

**Flickr 2004** Ξεκίνησε δραστηριότητα, Ιδρύθηκε από την Ludicorp και τους Stewart Butterfield και Caterina Fake. Το Flickr είναι μια υπηρεσία φιλοξενίας εικόνων και βίντεο. Στην αρχή της λειτουργίας του εστίασε κυρίως σε αναρτήσεις φωτογραφιών (με μια αίθουσα συζήτησης για φωτογραφίες σε πραγματικό χρόνο) που γρήγορα εγκαταλείφθηκε. Τα εργαλεία που παρέχει ενώνουν άτομα με κοινό ενδιαφέρον την φωτογραφία σε όλο τον κόσμο (“Flickr Company History,” n.d.).

**YouTube 2005** Ιδρυτές Chad Hurley, Steve Chen Jawed Karim, πρώην υπάλληλοι του PayPal. Η αρχική ιδέα για την δημιουργία του, υπήρξε περίπου ένα χρόνο νωρίτερα, από την ίδρυσή του. Το πρώτο βίντεο αναρτήθηκε τον Απρίλιο του 2005 και τον Σεπτέμβριο του 2005, το βίντεο τους (μια διαφήμιση για την Nike), έλαβε ένα εκατομμύριο «χτυπήματα» (hit). Το 2006 αγοράστηκε από την Google και σήμερα το YouTube έχει πάνω από ένα δισεκατομμύριο χρήστες (σχεδόν το μισό αριθμό χρηστών του Διαδικτύου παγκοσμίως)(“The history of YouTube,” 2016). Σύμφωνα με τους Montes-Vozmediano et al. (2018), το περιεχόμενο του YouTube είναι «ειδικά για εφήβους και η πρόσβαση σε αυτό το κοινωνικό δίκτυο είναι ένα από τα πρώτα πράγματα που κάνουν τα άτομα όταν ξεκινούν στον ψηφιακό τομέα, ανεξάρτητα από τη συσκευή που χρησιμοποιούν για να συνδεθούν με αυτό».

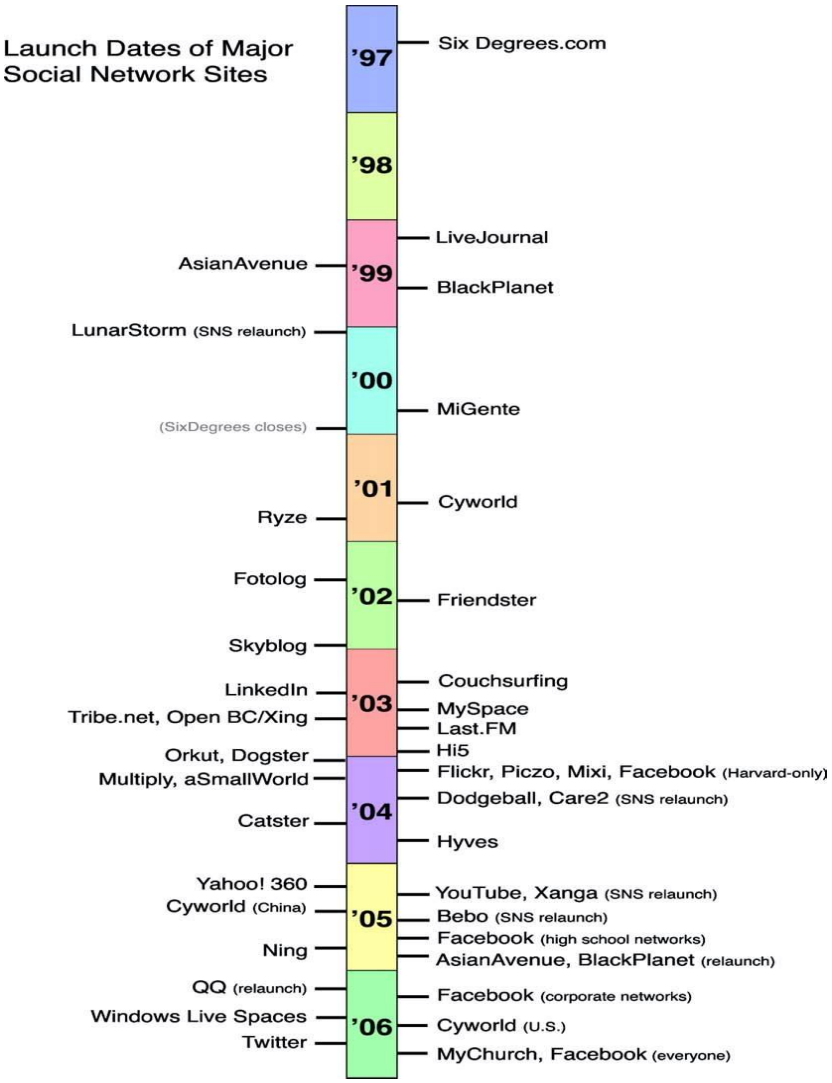
**Twitter 2006** Ιδρυτές Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams. Η επικοινωνία γίνεται με σύντομα μηνύματα που ονομάζονται tweets. Το πρώτο μήνυμα στάλθηκε από τον Dorsey στις 21 Μαρτίου 2006, που ο ίδιος το αποκάλεσε twttr. Καθώς ο αρχικός του σχεδιασμός ήταν για πλατφόρμα μηνυμάτων, τα αρχικά μηνύματα είχαν περιορισμό 140 χαρακτήρων, που ως ιδιότητα διατηρήθηκε μέχρι και το 2017. Το 2017 το όριο αυξήθηκε στους 280 χαρακτήρες (MacArthur, 2019).

Από το 2007 και μετά ο αριθμός των Πλατφορμών Κοινωνικής Δικτύωσης πολλαπλασιάστηκε και υπάρχουν χιλιάδες πλατφόρμες, όχι απαραίτητα, όλες πολύ δημοφιλείς (Rangwala, 2017).

**Instagram 2010** Ιδρυτές Kevin Systrom and Mike Krieger. Η αρχική του έκδοση τον Οκτώβριο του 2010, ήταν αποκλειστικά σε λειτουργικό IOS. Αγοράστηκε από το Facebook το 2012 και οι χρήστες του ανέρχονται σε πάνω από 600000 (Eudaimonia, 2017)

**Snapchat 2011** Ιδρυτές Evan Spiegel και Bobby Murphy (και Reggie Brown) πρώην φοιτητές του Stanford university το 2011 δημιούργησαν μια εφαρμογή που την αποκαλούσαν Picaboo, η οποία δεν πέτυχε, δεν «απογειώθηκε» (never got off the ground). Χωρίς τον Reggie Brown μετά (εξαιτίας κάποιων διαφωνιών), ξεκίνησαν το Snapchat. Το Φεβρουάριο του 2017, οι ενεργοί χρήστες ( ημερησίως) του Snapchat ανέρχονταν σε 160 εκατομμύρια ("A Brief History of Snapchat | Adsoup," n.d.) Το Snapchat έγινε γνωστό, ως η πρώτη προσδιορισμένη εφαρμογή κοινωνικών μέσων, μέσω κινητού τηλεφώνου (mobile) και ενισχύει την αλληλεπίδραση των χρηστών με έμφαση στα εικονικά αυτοκόλλητα και στοιχεία ενισχυμένης πραγματικότητας ("Snap shares skyrocket on first earnings beat with revived user growth," n.d.).

Στην Εικόνα 2, ενδεικτικά περιέχεται Χρονοδιάγραμμα των ημερομηνιών έναρξης πολλών σημαντικών Ιστοσελίδων Κοινωνικής δικτύωσης (Boyd & Ellison, 2007).




*Εικόνα 2: Χρονοδιάγραμμα έναρξης πολλών & σημαντικών Ιστοσελίδων Κοινωνικής Δικτύωσης και ημερομηνιών, όταν οι Διαδικτυακοί ιστότοποι επανεκκινήθηκαν με χαρακτηριστικά Ιστοσελίδων Κοινωνικής Δικτύωσης ( SNS)*

### 2.4.5 Τύποι Κοινωνικών Δικτύων

Τα κοινωνικά Δίκτυα ανάλογα με τον σκοπό που εξυπηρετούν μπορούν να διακριθούν στις κάτωθι κατηγορίες.

**Κοινωνική Δικτύωση (Social Networking)** Κύριος στόχος των Ιστοσελίδων Κοινωνικής Δικτύωσης αποτελεί η αλληλεπίδραση των χρηστών του με τελικό σκοπό την ανάπτυξη και εδραίωση κοινωνικών σχέσεων. Παραδείγματα τέτοιων ιστοσελίδων αποτελούν το Facebook, Twitter κ.α. (Tarinidis I. et al., n.d.)

**Κοινή Χρήση Πολυμέσων (Multimedia sharing)** Είναι οι ιστότοποι που επιτρέπουν τον διαμοιρασμό, αρχείων πολυμέσων μεταξύ των χρηστών τους. Παραδείγματα τέτοιων ιστοσελίδων είναι το YouTube, Flickr και το Instagram (Tarinidis I. et al., n.d.)

**Επαγγελματικά Κοινωνικά Δίκτυα (Professional Social Network)** Είναι οι Ιστότοποι που σκοπό έχουν την παροχή υπηρεσιών που ανοίγουν ευκαιρίες απασχόλησης των συμμετεχόντων χρηστών του. Επιπλέον μπορούν να δίνουν την δυνατότητα στις επιχειρήσεις, ανάρτησης θέσεων απασχόλησης. Μπορούν να είναι προσδιορισμένα είτε στους επαγγελματίες ή θεματικά σε συγκεκριμένα επαγγέλματα και συμφέροντα. Παράδειγμα LinkedIn (Tarinidis I. et al., n.d.).

**Πληροφορίες / Ενημέρωση (Information)**

Οι ιστοσελίδες ενημερωτικού περιεχομένου αναφέρονται και κατά κόρον χρησιμοποιούνται, από άτομα που αποσκοπούν στην εξεύρεση λύσεων σε προβλήματα καθημερινότητας. Ενδεικτικό παράδειγμα η αναζήτηση και εξεύρεση λύσεων, στην σε φιλικές προς το περιβάλλον και την κατοικία, βελτιώσεις. Παράδειγμα «Κάντο μόνος σου» (Do it yourself/DYI) (Tarinidis I. et al., n.d.).

**Εκπαιδευτικές (Educational)**

Τα εκπαιδευτικά κοινωνικά δίκτυα είναι δίκτυα, όπου υλοποιείται η συνεργασία μεταξύ μαθητών, σπουδαστών και δασκάλων ή καθηγητών, για υλοποίηση ακαδημαϊκών προγραμμάτων. Η αλληλεπίδραση μπορεί να συμβαίνει και μέσω ιστολογίων (blogs) ή και φόρα (forum). Τέτοιου είδους συστήματα είναι δημοφιλή τα τελευταία χρόνια. (Tarinidis I. et al., n.d.) Είναι δε πολύ συνηθισμένες και στην εκπαίδευση ενηλίκων αλλά και στην εξ' αποστάσεως εκπαίδευση.

**Hobbies**

Αφορούν Κοινωνικά δίκτυα θεματικά, σχετικά με ευχάριστη ατομική ενασχόληση (χόμπι) στα οποία αλληλοεπιδρούν τα άτομα για αναζήτηση θεμάτων σχετικών με τα ενδιαφέροντα τους. Θεματικοί ιστότοποι στους οποίους τα άτομα βρίσκουν εκτός από πληροφορίες αλλά και ολόκληρες κοινότητες με τα ίδια ενδιαφέροντα για να ανταλλάξουν απόψεις κλπ. (Tarinidis I. et al., n.d.).

**Academic**

Αφορούν ιστότοπους που σχετίζονται με θέματα έρευνας και στα οποία τα άτομα δημοσιεύουν, έρευνες ή αναζητούν θέματα ερευνητικού ενδιαφέροντος. Παράδειγμα Academia EDU (Tarinidis I. et al., n.d.).

### 2.4.6 Πλεονεκτήματα

Οι Kaplan M. Andreas & Haenlein Michael (2009), αναφέρουν ότι σύμφωνα με το Forester Research, το δεύτερο τρίμηνο του 2008 υπήρξε μια σημαντική αυξητική διαφοροποίηση μεταξύ των Χρηστών του Διαδικτύου που συμμετείχαν σε Δίκτυο Κοινωνικής Δικτύωσης (Social Network) σε σχέση με το αντίστοιχο ποσοστό του 2007 (75% των χρηστών του Διαδικτύου το 2008, έναντι 56% το 2007). Τον Ιανουάριο του 2009 στην πλατφόρμα του Facebook οι ενεργοί εγγεγραμμένοι χρήστες του, ανέρχονταν στα 175 εκατομμύρια (χρήστες) (Kaplan M. Andreas & Haenlein Michael, 2009) και, σύμφωνα με το site του Facebook, τον Ιούνιο του 2019, οι ενεργοί μηνιαίοι χρήστες του ανέρχονταν στα 2.41 δισεκατομμύρια ("Company Info | Facebook Newsroom," n.d.) που επιβεβαιώνεται και από αντίστοιχα site που παρέχουν στατιστικά στοιχεία ("Statistics," n.d.). Τα μεγέθη αυτά συγκρινόμενα με πληθυσμούς κρατών, αναλογικά είναι επιβλητικά καθώς είναι πολύ μεγαλύτερα (παράδειγμα: Γερμανία 80 εκατομμύρια πληθυσμός) (Kaplan M. Andreas & Haenlein Michael, 2009). Αντίστοιχα το Flickr (ιστοσελίδα για ανάρτηση φωτογραφιών και βίντεο (video), φιλοξενούσε πάνω από 3 δισεκατομμύρια φωτογραφίες, αντίστοιχα μέγεθος πολύ μεγαλύτερο από εκθέματα πολλών μουσείων (παράδειγμα το Μουσείο του Λούβρου στο Παρίσι με συλλογή εκθεμάτων περίπου 300000 τεμάχια) (Kaplan M. Andreas & Haenlein Michael, 2009).

Η μεγάλη αυτή αύξηση των χρηστών των Μέσων Κοινωνικής Δικτύωσης από μόνη της υποδηλώνει ότι υπάρχουν πολλά πλεονεκτήματα τα οποία οι χρήστες που τα χρησιμοποιούν, βρίσκουν σε αυτά.

Στην Εικόνα: 3 Ενεργοί Χρήστες Facebook Ιούνιος 2019 (Q2 2019) παρουσιάζονται οι Μηνιαίοι Ενεργοί Χρήστες του Facebook ("Facebook users worldwide 2019," n.d.).

Οι Marzano et all (2013) αναφέρουν ότι στα αναμφισβήτητα πλεονεκτήματα που προσφέρουν οι Τεχνολογίες Πληροφορίας (Information & Communication Technology ) και τα Κοινωνικά Δίκτυα (Social Media, Social Networks), - είναι το ότι η συμμετοχή σε διαδικτυακά παιχνίδια, διευκολύνει την αυτογνωσία, ή αντίστοιχα ότι μπορεί να βελτιώσει την αυτοεκτίμηση δίνοντας την ευκαιρία στον συμμετέχοντα να πειραματισθεί με την ταυτότητά του και να επιλέξει συνειδητά το τι επιθυμεί, π.χ. στο Second life.

Οι χρήσεις των Κοινωνικών Δικτύων που έχουν εντοπισθεί και καταγραφεί σε διάφορες έρευνες είναι πολλές. Οι Alhabash & Ma (2017), αναφέρουν ότι έχουν εντοπισθεί πολλά και διαφορετικά κίνητρα χρήσης των Ιστοσελίδων Κοινωνικής Δικτύωσης. Η Κοινωνική Σύνδεση, Κοινή ταυτότητα, φωτογραφίες, αναζήτηση πληροφοριών, ευχάριστο

περιεχόμενο, κοινωνική έρευνα, σερφινγκ και ενημερώσεις κατάστασης, κοινωνική αλληλεπίδραση, χαλάρωση, διασκέδαση, έκφραση γνώμης, η συνάντηση με ομοειδή άτομα, συντροφικότητα, κοινωνική υποστήριξη. Οι Yisa et al. (2016) αναφέρουν « Τα Κοινωνικά Δίκτυα προσφέρουν πολλά πλεονεκτήματα και χρησιμότητα. Μπορούν να χρησιμοποιούνται για αυξήσεις σε πωλήσεις, για εκπαίδευση για να συναντήσει νέους φίλους ή παλιούς, και ακόμη και ως εργαλείο επικοινωνίας με το ευρύ κοινό».

Αντίστοιχα χαρακτηριστικά πλεονεκτήματα αναφέρουν και οι Kuss & Griffiths (2017) που προκύπτουν από την συμμετοχή και χρήση των κοινωνικών Δικτύων και αναφέρουν διαφορετικά κίνητρα είτε αυτά αφορούν την ικανοποίηση του χρήστη και έχουν σχέση με την αναζήτηση πληροφοριών, είτε με το να δημιουργήσουν ταυτότητα – παρουσίαση του εαυτού με τρόπο που ενισχύει την εμφάνιση του εαυτού του ατόμου, είτε την ψυχαγωγία. Η ικανοποίηση επίσης βασικών ανθρώπινων αναγκών καλύπτονται από την χρήση των Κοινωνικών Δικτύων, δηλαδή η ασφάλεια, που αφορά την δυνατότητα του χρήστη να επιλέγει με ποιους μοιράζεται, ποιες πληροφορίες, η σύνδεση που αφορά την επιλεκτική σύνδεση ατόμων που είναι προσωπική επιλογή του χρήστη, η εκτίμηση που προκύπτει από την αύξηση των φίλων του χρήστη και η αυτοπεποίθηση που έχει να κάνει με την προσωπική εμφάνιση του εαυτού, την οποία κερδίζει μέσα από τον οποιονδήποτε τρόπο παρουσίασης του εαυτού επιλέξει ο ίδιος αλλά και από την βοήθεια που μπορεί ο ίδιος να παρέχει σε φίλους που την χρειάζονται (Kuss & Griffiths, 2017).

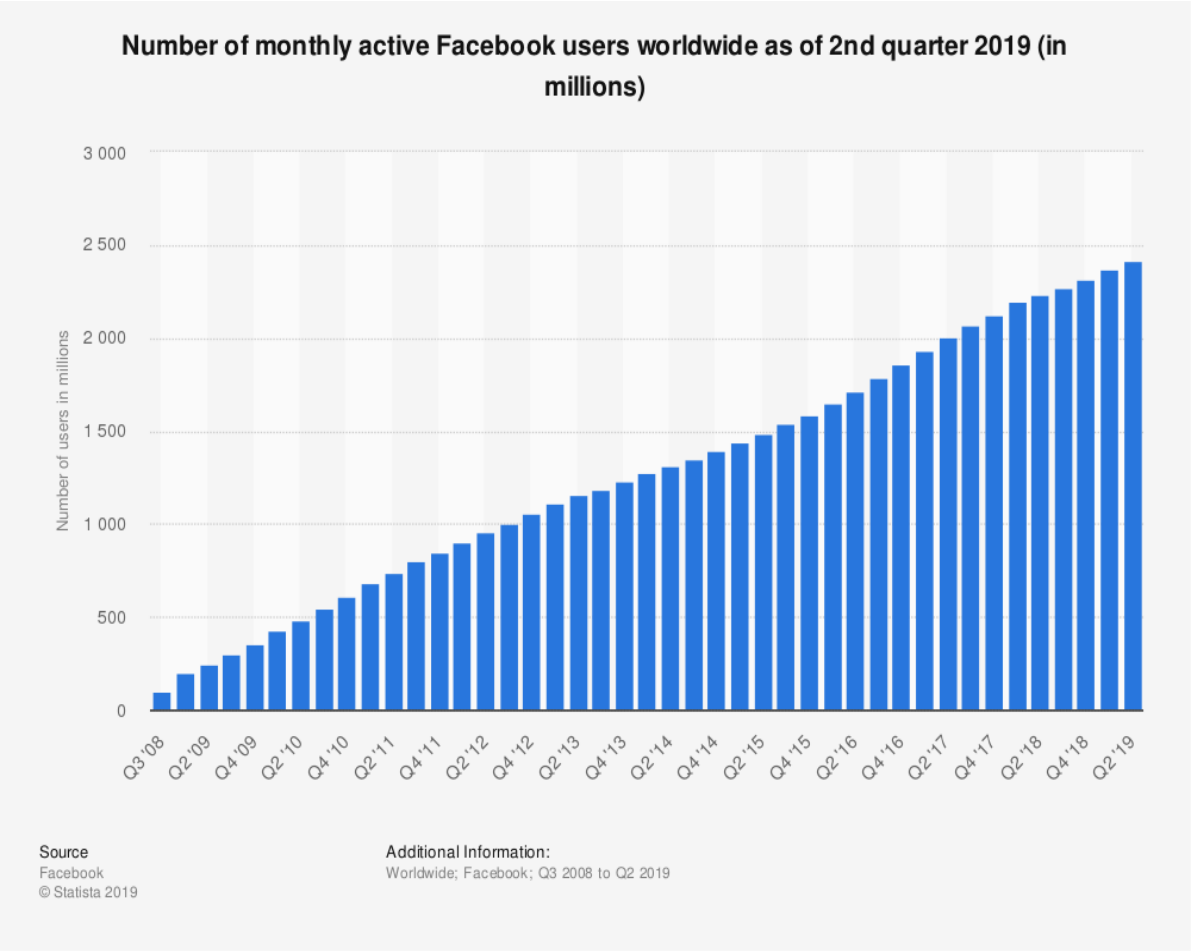
Η δυνατότητα ενδυνάμωσης των κοινωνικών δεσμών, τα πλεονεκτήματα που μπορεί να προσφέρουν στην διάχυση της πληροφορίας, της γνώσης ή την πιο εύκολη και γρήγορη διαμόρφωση και εκκίνηση κοινωνικών κινημάτων αλλά και άλλα πολλά πλεονεκτήματα. Σύμφωνα με τους Ellison et al. (2007) το κοινωνικό κεφάλαιο, -οι πόροι που αποκτώνται από τις μεταξύ των ανθρώπων σχέσεις - ή και ως τα πλεονεκτήματα που απορρέουν από τις σχέσεις με άλλα άτομα (Wilson, Gosling, & Graham, 2012), αποτελεί μια έννοια που αποτελεί τον συνδετικό κρίκο μιας κοινωνίας. Η αύξηση του Κοινωνικού κεφαλαίου αυξάνει την δέσμευση των ατόμων στη κοινότητα, και την αποτελεσματικότητα στην κινητοποίηση συλλογικών δράσεων. Η μείωση του κοινωνικού κεφαλαίου οδηγεί σε κοινωνικές αναταραχές (με τάσεις αυξητικές) και μεγαλύτερη δυσπιστία μεταξύ των μελών μιας κοινότητας. Αναφορικά με το άτομο, το κοινωνικό κεφάλαιο του επιτρέπει να αποκομίζει πόρους από τα μέλη των κοινοτήτων ή δικτύων στα οποία αλληλοεπιδρά. Το αποτέλεσμα αυτού είναι οι πληροφορίες που αποκτά, οι προσωπικές σχέσεις που συνάπτει, η συνάντηση με άτομα ξένα προς το περιβάλλον του ατόμου μπορεί να του δώσει πρόσβαση σε απασχόληση, αλλά και οι δεσμοί που συνάπτει με φίλους σχετίζονται

με δείκτες προσωπικής αυτοεκτίμησης και ικανοποίηση από την ύπαρξη και την ζωή. Στην έρευνα δε που διεξήγαν μεταξύ χρηστών του Facebook βρήκαν άμεσο συσχετισμό την χρήσης του Κοινωνικού Δικτύου και της διατήρησης και δημιουργίας του Κοινωνικού Κεφαλαίου (Ellison et al., 2007). Επίσης οι Kraut & Burke (2015) διαπίστωσαν ότι η ανταλλαγή μηνυμάτων στο Facebook συνδέεται με την αύξηση του κοινωνικού κεφαλαίου του χρήστη, ενώ αντίστοιχα, η ενημέρωση για τα άτομα, δεν συνδέεται. Η χρήση και συμμετοχή σε Κοινωνικά Δίκτυα σύμφωνα με τους Kuss & Griffiths (2017), αναφέρουν ότι έχει γίνει μια καθημερινή ευχάριστη δραστηριότητα αναψυχής για τους συνδεόμενους σε αυτά χωρίς περιορισμούς στον χώρο και στον χρόνο. Η Κοινωνική Δικτύωση είναι τρόπος ζωής και σχέσης και αυτό υποστηρίζεται και αφορά ιδιαίτερα τους νέους ανθρώπους οι οποίοι έχουν γαλουχηθεί μέσα στην τεχνολογία, η οποία αποτελεί αναπόσπαστο μέρος της ύπαρξής τους και των οποίων η συνδεσιμότητα έχει ενσωματωθεί στην καθημερινή τους ζωή.

### *2.4.7 Μειονεκτήματα*

Θα πρέπει ωστόσο να αναφερθούν και τα μειονεκτήματά τους. Η υπερβολική χρήση μπορεί να οδηγήσει σε φαινόμενα εθισμού, σε φαινόμενα απομόνωσης, η χρήση σε έκθεση σε περιεχόμενο πορνογραφικό και σε άσεμνο, σε Cyberbullying, σε κατάθλιψη και άλλα αντίστοιχα φαινόμενα.

Η χρήση των κοινωνικών Δικτύων δεν είναι απαραίτητο ότι μπορεί να προκαλέσει «σοβαρές αρνητικές συνέπειες στην ζωή του χρήστη» όπως αναφέρουν οι Turel (2012), σε σχέση με άλλες τεχνολογίες, όπως το Διαδικτυακό παιχνίδι (Online gaming), στην πραγματικότητα όμως, «παράγει ισχυρή ανεπαρκή αυτοπαρατήρηση και ανεπαρκή αυτοαντίδραση μεταξύ άλλων συνήθων τεχνολογιών». Οι Kuss & Griffiths (2017) επίσης αναφέρουν εκτός των μειονεκτημάτων της υπερβολικής χρήσης ή του εθισμού, επιπλέον και την «Κυβερνοπαρακολούθηση» (Cyberstalking) και το «Μπανιστήρι» (voyeurism), ως κίνητρα χρήσης, που και τα δύο χαρακτηριστικά, μπορούν να έχουν αρνητικές επιπτώσεις στην ευημερία και υγεία των ατόμων. Ωστόσο οι εγκυμονούντες κίνδυνοι στα Κοινωνικά Δίκτυα θα εξετασθούν στο αμέσως επόμενο κείμενο.




*Εικόνα: 3 Ενεργοί Χρήστες Facebook Ιούνιος 2019 (Q2 2019) Ανακτήθηκε από https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/*

## 2.5 Κίνδυνοι & Απειλές στα Κοινωνικά Δίκτυα

### 2.5.1 Κίνδυνοι σε Κοινωνικά Δίκτυα Γενικά

Τα οφέλη από την χρήση των Κοινωνικών Δικτύων αφθονούν και έχουν ήδη αναφερθεί όπως και η μεγάλη διείσδυση, που αυτά έχουν, μέσα στις σύγχρονες κοινωνίες και σε πολύ μεγάλα τμήματα του παγκόσμιου πληθυσμού. Επίσης όμως ενέχουν και πολλούς και σοβαρούς κινδύνους. Οι κίνδυνοι, που κατά καιρούς αναφέρονται, ότι προέρχονται από την χρήση της τεχνολογίας και των κοινωνικών Δικτύων, είναι πολλοί και συνεχώς ανανεώνονται. Οι επιπτώσεις δε, που μπορούν να έχουν στο άτομο ποικίλουν, δεν προέρχονται απαραίτητα μόνο από την συνάντηση αγνώστων μεταξύ τους ατόμων, που αποτελούσε και αποτελεί ένα μεγάλο φόβο από την αλληλεπίδραση ατόμων που μεταξύ τους δεν γνωρίζονται, αλλά και κίνδυνοι όπου σχετίζονται με την αποκάλυψη

προσωπικών στοιχείων στο Διαδίκτυο, την ελλιπή φροντίδα ασφάλειας από την μεριά του χρήστη και ή και την υπερβολική χρήση, τον Εθισμό και τις διαφορετικές μορφές του, που απαντώνται. Επίσης θα πρέπει να αναφερθεί ότι ένα μεγάλο μέρος των κινδύνων που σχετίζονται με την τεχνολογία την σχετική με τα Κοινωνικά Δίκτυα αφορούν κινδύνους σχετικούς με την Ιδιωτική Ζωή και το Απόρρητο.

Οι Christofides et all (2012b) αναφέρουν ότι έρευνες δείχνουν ότι ο διαμοιρασμός προσωπικών πληροφοριών αποτελεί πληροφορία προσβάσιμη από εργοδότες του σήμερα ή και μελλοντικούς, αλλά και από επίδοξους εκβιαστές οι οποίοι μπορούν να χρησιμοποιήσουν τις διαθέσιμες διαδικτυακά πληροφορίες (Christofides et al., 2012b).

Από τον διαμοιρασμό των προσωπικών πληροφοριών, μπορούν να αναδυθούν κίνδυνοι που αφορούν διαφορετικές ηλικιακές ομάδες, ανάλογα με την χρήση του Κοινωνικού Δικτύου αλλά και την αποκαλυφθείσα πληροφορία. Οι Christofides et all. (2012b) αναφέρουν ότι οι κίνδυνοι, που προκύπτουν από την αποκάλυψη πληροφοριών, ερευνήθηκαν και κατηγοριοποιήθηκαν στη βάση του περιεχομένου της αποκαλυπτόμενης πληροφορίας. Η έρευνα αφορούσε κυρίως κινδύνους που εκτίθενται τα παιδιά. Κίνδυνοι που προκύπτουν από α. ακατάλληλο περιεχόμενο, β. από ανεπιθύμητες επαφές και γ. κίνδυνοι από ακατάλληλη συμπεριφορά (όταν τα παιδιά λαμβάνουν α. ακατάλληλο περιεχόμενο, β. ανεπιθύμητες επαφές και γ. ακατάλληλη συμπεριφορά). Αντίστοιχα αναφέρουν, υλοποιηθείσες έρευνες μεταξύ εφήβων χρηστών του Facebook, που η δημοσιοποίηση εμπειριών τους, όπως η κατάχρηση αλκοόλ ή άλλης παραβατικής συμπεριφοράς, οδήγησε σε συνέπειες επιβολής αναστολής φοίτησης ή ακόμη και σε ποινικές διώξεις. Για τους ενήλικες, αντίστοιχες συνέπειες σε επαγγελματικά περιβάλλοντα, δεν γίνονται απαραίτητα πάντα γνωστές καθώς ένας υποψήφιος μπορεί να αποκλεισθεί από την προσφερόμενη θέση εργασίας χωρίς να αναφερθεί η αιτία. Σύμφωνα με τους Christofides et all. (2012), και το CareerBuilder το 2009, στις Ηνωμένες Πολιτείες της Αμερικής οι εργοδότες σε ένα ποσοστό 45% ελέγχουν τους υποψήφιους εργαζομένους τους στα κοινωνικά δίκτυα και ότι ακόμη ένα 11% αναφέρουν ότι θα το κάνουν στο μέλλον (Christofides et al., 2012b).

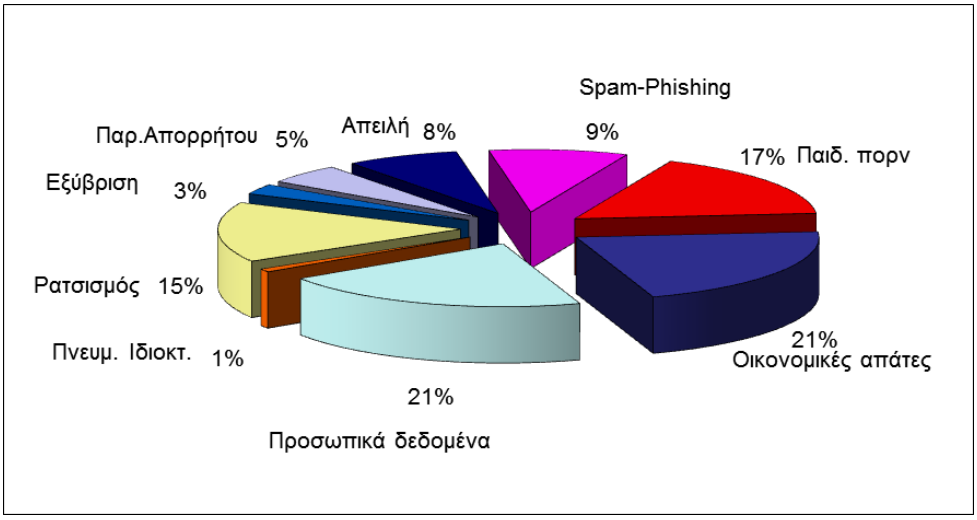
Επιπλέον κίνδυνοι που έχουν αναφερθεί από την ανάρτηση και δημοσιοποίηση προσωπικών στοιχείων και σχολίων, σε μέσα Κοινωνικής Δικτύωσης και έχουν προκύψει από έρευνες, αφορούν δυσφορία και καταστάσεις ψυχοφθόρες. Σύμφωνα με τους Christofides et all (2012b), σε διαδικτυακή έρευνα των Juvonen & Gross του 2008, αναφορικά με τον Διαδικτυακό Εκφοβισμό (Cyberbullying), οι συμμετέχοντες έφηβοι σε

ποσοστό 72% ανέφεραν ότι είχαν γίνει αποδέκτες εκφοβισμού, (τουλάχιστον σε μία περίπτωση), στη προηγούμενη χρονική περίοδο (Christofides et al., 2012b).

Οι Banyai et all (2017), αναφέρουν ότι δεν έχει υπάρξει συμφωνία μεταξύ των ερευνητών αναφορικά με το θέμα της προβληματικής χρήσης των Κοινωνικών Δικτύων και της εκτεταμένης χρήσης εφαρμογών όπως το Facebook, Snapchat κ.α. και αναφέρουν έρευνες, οι οποίες πιστοποιούν ότι στις Ηνωμένες Πολιτείες της Αμερικής, το Facebook είναι μεταξύ των πιο δημοφιλών ιστοσελίδων, στις ηλικίες ατόμων μεταξύ 13-17 ετών, ότι το 71% των εφήβων συμμετέχουν σε πάνω από μια ιστοσελίδα κοινωνικής Δικτύωσης, ενώ το 24% των ενηλίκων βρίσκονται σχεδόν συνεχώς στο Διαδίκτυο χρησιμοποιώντας το κινητό τους τηλέφωνο (Bányai et al., 2017).

Η εκτεταμένη και συνεχής χρήση των Μέσων Κοινωνικής Δικτύωσης αναφέρουν οι Banyai et all (2017), κάτι που έχει ήδη αναφερθεί και από τους Marzano et all (2013), προκαλούν αρνητικά αποτελέσματα και μπορεί να προκαλέσουν προβλήματα στην προσωπική, κοινωνική ή και την επαγγελματική ζωή των ατόμων που τα χρησιμοποιούν (Bányai et al., 2017) & (Marzano et al., 2013). Ειδικά για την κατηγορία των νέων ατόμων όπως αναφέρει η Kimberly Young (2010) τα στοιχεία μέχρι σήμερα δείχνουν ότι οι κίνδυνοι που αφορούν και παρουσιάζονται στους νέους στα Κοινωνικά Μέσα, είναι παρεμφερείς με άλλους αντίστοιχους κινδύνους του Διαδικτύου.

Στην Ελλάδα το 2015 οι αναφορές για κινδύνους στο Ελληνικό Κέντρο Ασφαλούς Διαδικτύου παρουσιάζονται ενδεικτικά Εικόνα 4. Από τις 4000 περίπου καταγγελίες όπως αναφέρεται στην Ιστοσελίδα, ένα ποσοστό ίσο με 17%, αφορούσαν Παιδική πορνογραφία (Safeline, n.d.).




*Εικόνα 4: SafeLine Στατιστικά στοιχεία Ελληνικού Κέντρου Ασφαλούς Διαδικτύου Ανακτήθηκε από https://internet-safety.sch.gr/index.php/articles/parents/item/378-%CF%83%CF%84%CE%B1%CF%84%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AC-%CF%83%CF%84%CE%BF%CE%B9%CF%87%CE%B5%CE%AF%CE%B1-safeline-%CE%B3%CE%B9%CE%B1-%CF%84%CE%BF-2015*

## 2.6 Κατηγοριοποίηση των Κινδύνων

Οι Fire et al. (2014) κατηγοριοποιούν τους κινδύνους που αφορούν τους χρήστες των Κοινωνικών Δικτύων στη βάση 4 διαφορετικών κατηγοριών.
Η πρώτη κατηγορία αφορά κινδύνους Ιδιωτικότητας και Ασφάλειας (κλασσικές απειλές). Η δεύτερη κατηγορία αφορά, νέους κινδύνους που αφορούν την υποδομή των Κοινωνικών Δικτύων, εστιάζονται κυρίως εκεί και η υποδομή των Κοινωνικών Δικτύων χρησιμοποιείται, για να τρωθεί η Ιδιωτικότητα και η ασφάλεια των Χρηστών των Κοινωνικών Μέσων. Η Τρίτη κατηγορία αποτελεί ένα συνδυασμό απειλών προκειμένου να επιφέρουν μεγαλύτερους κινδύνους. Η τέταρτη κατηγορία αφορά κυρίως κινδύνους που σχετίζονται με παιδιά και με μέσο το Κοινωνικό Δίκτυο (Fire et al., 2014).

### 2.6.1 Κλασικές απειλές/Κίνδυνοι

Οι κλασικές απειλές αφορούν την χρήση των παρεχόμενων προσωπικών πληροφοριών του χρήστη στο ή στα Κοινωνικά Δίκτυα που αλληλοεπιδρά, με τελικό σκοπό, την επίθεση στον χρήστη και στους φίλους του, χρησιμοποιώντας τις προσωπικές πληροφορίες του χρήστη, ανάλογα προσαρμοσμένες. Τέτοιου τύπου απειλές αποτελούν το κακόβουλο λογισμικό, ανεπιθύμητη αλληλογραφία (spam), επιθέσεις phishing, Spammers, Cross-Site Scripting (XSS), Διαδικτυακές απάτες. Αυτοί οι κίνδυνοι αν και δεν είναι νέοι, εντούτοις εξακολουθούν να αποτελούν μεγάλο πρόβλημα, καθώς εξαιτίας της δομής και της φύσης των Κοινωνικών Δικτύων εξαπλώνονται πολύ γρήγορα. Στόχος του κινδύνου τα προσωπικά στοιχεία του χρήστη, πληροφορίες όπως τραπεζικοί λογαριασμοί , αριθμοί πιστωτικών καρτών, κωδικοί ασφαλείας, και όπως αναφέρουν οι Fire et al. (2014) «ακόμη και το εύρος ζώνης του δικτύου του χρήστη» με σκοπό να στέλνουν ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου (Fire et al., 2014).

#### Κακόβουλο Λογισμικό (Malware)

Σκοπός αυτού του λογισμικού, η εγκατάστασή του, στον υπολογιστή του χρήστη με σκοπό την κλοπή των προσωπικών στοιχείων, του χρήστη. Εγκαθίσταται στον υπολογιστή του χρήστη και μέσω της δομής του Κοινωνικού Δικτύου επεκτείνεται, σε συνδεδεμένα άτομα με τον προσβεβλημένο χρήστη. Υπάρχει περίπτωση να χρησιμοποιήσει τα «διαπιστευτήρια του χρήστη», στα οποία έχει αποκτήσει πρόσβαση και να στείλει προσωποποιημένα μηνύματα σε φίλους, του προσβεβλημένου χρήστη. Πρώτο δείγμα τέτοιου κακόβουλου λογισμικού το Coobface το οποίο επεκτάθηκε μέσω Κοινωνικών Δικτύων, όπως το Facebook, Skype, Twitter κ.α. (Fire et al., 2014).

## Ηλεκτρονικό Ψάρεμα (Phishing)

Αποτελεί δημιούργημα Κοινωνικής Μηχανικής (Social Engineering), που σκοπό έχει στην πρόσβαση και απόκτηση ευαίσθητων πληροφοριών του χρήστη μέσω «παραποίησης ενός αξιόπιστου τρίτου μέρους» (Fire et al., 2014). Το «Social Engineering, στο κομμάτι της ασφάλειας των πληροφοριών, αναφέρεται στην ψυχολογική χειραγώγηση των ανθρώπων, που στοχεύει στην εκτέλεση πράξεων ή τη διάδοση εμπιστευτικών πληροφοριών» (Oweis, Alrababa, Oweis, Owais, & Alansari, 2014). Οι χρήστες των Κοινωνικών Δικτύων που αλληλοεπιδρούν, αποτελούν σύμφωνα με τους Fire et al. (2014), πολύ πιθανούς στόχους «ηλεκτρονικού ψαρέματος» «λόγω του κοινωνικού και εμπιστευτικού χαρακτήρα». Η προσβολή του Facebook, με δημιουργία πλαστών σελίδων χρηστών, αποτελεί ένα χαρακτηριστικό παράδειγμα.

## Spammers

Αποτελεί ένα κίνδυνο, κατά τον οποίο χρήστες δημιουργούν και χρησιμοποιούν ανεπιθύμητα μηνύματα, διαφημίσεις, εναντίον άλλων χρηστών, μέσω της ιστοσελίδας Κοινωνικής Δικτύωσης, στην οποία δημιουργούν ψεύτικα προφίλ. Επίσης πάλι μέσω της Ιστοσελίδας Κοινωνικής Δικτύωσης, έχουν την δυνατότητα να δημιουργήσουν σχόλια, σε σελίδες, με μεγάλη επισκεψιμότητα στο Δίκτυο. Το Twitter έχει πληγεί από spam μηνύματα. Το 2009 το ποσοστό spam μηνυμάτων του Twitter, ανέρχονταν σε 9% και το 2010 με αποτελεσματικές πρακτικές του Twitter μειώθηκε στο 1% (Fire et al., 2014).

## Cross-Site Scripting (XSS)

Αφορά επιθέσεις σε Διαδικτυακές εφαρμογές, επίθεση κατά την οποία ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη του χρήστη προς κάποια εφαρμογή, και εκτελεί το κακόβουλο λογισμικό (worms), με σκοπό την συλλογή προσωπικών πληροφοριών. Οι ιστοσελίδες Κοινωνικής Δικτύωσης είναι επιρρεπείς σε XSS επιθέσεις (Fire et al., 2014).

## Διαδικτυακές απάτες

Και σε αυτή την κατηγορία κινδύνου, σκοπός του επιτιθέμενου είναι η εκμετάλλευση του χρήστη, με σκοπό κάποια απάτη, χρησιμοποιώντας το Διαδίκτυο. Είναι μια παλαιότερη μορφή απάτης, προσαρμοσμένη στις νέες τεχνολογίες, το Διαδίκτυο και τα Κοινωνικά Δίκτυα. Σκοπός του «απατεώνα», η εμπιστοσύνη του χρήστη και η αποκάλυψη προσωπικών του στοιχείων, με σκοπό προσωπικό τους όφελος, οικονομικό συνήθως. Η δημοσίευση των προσωπικών στοιχείων, από τον χρήστη στο προφίλ τους, στις Ιστοσελίδες Κοινωνικής Δικτύωσης, υποκλέπτονται και με πειρατεία χρησιμοποιούν τους λογαριασμούς των χρηστών και ζητούν από φίλους τη μεταφορά χρημάτων σε προσωπικό τους λογαριασμό με κάποια δικαιολογία (Fire et al., 2014).

### 2.6.2 Σύγχρονες απειλές/Κίνδυνοι

Είναι απειλές που σχετίζονται με το περιβάλλον των Κοινωνικών Δικτύων και στοχεύουν στα προσωπικά στοιχεία του χρήστη και των επαφών του. Ο εισβολέας σε κάθε περίπτωση προσπαθεί να συνδεθεί με τον χρήστη και τις επαφές του, δημιουργώντας ψεύτικο προφίλ και να ξεκινήσει ένα αίτημα φιλίας σε στοχευμένο χρήστη. Με την αποδοχή φιλίας από τον χρήστη, τα στοιχεία του, τα δεδομένα του είναι εκτεθειμένα και στην διάθεση του εισβολέα. Απόρρητο και Ιδιωτικότητα και τελικά η ασφάλεια του χρήστη και σε αυτή την κατηγορία κινδύνων ο στόχος. **Clickjacking** (κακόβουλη πρακτική του χειρισμού της δραστηριότητας ενός χρήστη ενός ιστότοπου, αποκρύπτοντας υπερσυνδέσμους κάτω από νόμιμο περιεχόμενο με δυνατότητα κλικ, προκαλώντας έτσι στον χρήστη να εκτελεί ενέργειες που δεν γνωρίζει). **De-Anonymization Attacks (**Επιθέσεις από ανωνυμοποίησης) είναι η δυνατότητα από-ανωνυμοποίησης των χρηστών ΙΚΔ. Πολλές ΙΚΔ δίνουν την δυνατότητα στους χρήστες να δημιουργήσουν λογαριασμούς χρησιμοποιώντας ψευδώνυμα (Ιστοσελίδες όπως το Myspace, to Twitter, με σκοπό να προστατέψουν την ανωνυμία τους). Οι επιθέσεις αυτές έχουν στόχο, εξεύρεσης τρόπων, προκειμένου να αποσπάσουν τις πραγματικές πληροφορίες των στοιχείων των χρηστών μέσω τεχνικών όπως τα cookies , τα μέλη της ομάδας του χρήστη, κ.α., ώστε να καταφέρουν να εντοπίσουν τα πραγματικά στοιχεία του χρήστη. **Ψεύτικα Προφίλ (Fake Profiles**) είναι τα social bots ή και sybils, τα οποία είναι ψεύτικά προφίλ χρηστών που μιμούνται ανθρώπινες συμπεριφορές σε ιστοσελίδες Κοινωνικής Δικτύωσης. **Identity Clone Attacks** Αποτελεί την αντιγραφή του προφίλ ενός χρήστη είτε στο ίδιο δίκτυο είτε σε διαφορετικά, με σκοπό την εξαπάτηση φίλων και επαφών του χρήστη και διαμόρφωση σχέσης εμπιστοσύνης τρίτων με το ψεύτικο προφίλ. **Inference Attacks** επιθέσεις συμπερασμάτων στοχεύουν σε μη δημοσιευμένα προσωπικά στοιχεία του χρήστη, όπως ευαίσθητα προσωπικά δεδομένα, θρησκευτικές πεποιθήσεις, σεξουαλικός προσανατολισμός κ.α., των οποίων η γνώση αποκτάται με διάφορες τεχνικές, είτε εξόρυξης δεδομένων, είτε μέσω της τυπολογίας του δικτύου αλλά είτε και από συλλογή πληροφοριών από φίλους και λοιπές επαφές του χρήστη. **Face Recognition** Οι αναρτημένες φωτογραφίες του χρήστη που υπάρχουν είτε στο προφίλ του χρήστη, ή σε άλλα σημεία με φίλους κλπ. μπορούν να χρησιμοποιηθούν, ώστε να εντοπισθούν οι χρήστες, χωρίς να το γνωρίζουν ή να συμφωνούν απαραίτητα. **Information Leakage** Οι δημοσιευμένες πληροφορίες των χρηστών των Ιστοσελίδων Κοινωνικής Δικτύωσης, πολλές φορές αφορούν ευαίσθητα προσωπικά δεδομένα, των οποίων η διαρροή μπορεί να έχει, αρνητικές επιπτώσεις για τους χρήστες, είτε αυτές

μπορούν να χρησιμοποιηθούν από ασφαλιστικές εταιρείες, για εντοπισμό πληροφοριών υγείας χρηστών ώστε να μην αποδώσουν ασφάλιστρα κλπ. **Location Leakage** Η αποκάλυψη πληροφοριών σχετικών, με τον τόπο παρουσίας του χρήστη, η οποία πολύ εύκολα επιτυγχάνεται, μέσω των έξυπνων συσκευών και των κινητών τηλεφώνων, αρκετές φορές μπορούν να αποτελέσουν στόχο εξεύρεσής τους, σε πραγματικό χρόνο. Πληροφορίες που μπορούν να χρησιμοποιηθούν από εγκληματίες με σκοπό την βλάβη του χρήστη. Αρκετές φορές οι χρήστες αναρτούν φωτογραφίες ή και βίντεο που αποκαλύπτουν την τρέχουσα τοποθεσία τους. Η αναρτημένη με αυτό τον τρόπο φωτογραφία, μπορεί να οδηγήσει σε εντοπισμό τους – καθώς πολλές φορές η μεταφορτωμένη φωτογραφία μπορεί να έχει ετικέτα τοποθεσίας (geotag) και τελικά σε κακόβουλες πράξεις από εγκληματίες ή άλλους παραβάτες. **Socware** χρησιμοποιείται και διανέμεται μέσω μηνυμάτων που περιέχουν σύντομο μήνυμα και μία διεύθυνση url και εμφανίζονται στον τοίχο του χρήστη και στην ροή ειδήσεων, στις ιστοσελίδες κοινωνικής δικτύωσης. (Fire et al., 2014). Μέσω αυτής της διαδικασίας ο χρήστης οδηγείται στην εγκατάσταση κακόβουλου λογισμικού, το οποίο στέλνει τις αναρτήσεις σε φίλους, επαφές του χρήστη, για λογαριασμό του ("What is Socware | IGI Global," n.d.).

### 2.6.3 Συνδυαστικές Απειλές

Συνδυασμός απειλών εναντίον του χρήστη, μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να δημιουργήσει μια πιο εξελιγμένη επίθεση. Αυτό σημαίνει παλιές και νέες μορφές απειλών. Για παράδειγμα η χρήση Ηλεκτρονικού ψαρέματος (fishing) προκειμένου να αποσπάσει κωδικό ή κωδικούς ασφαλείας και στη συνέχεια με την δημοσίευση ενός μηνύματος στο χρονολόγιο του χρήστη (clickjacking), παροτρύνοντας τις επαφές του χρήστη να κάνουν κλικ στην ανάρτηση, να επιτύχει την εγκατάσταση ενός ιού κρυφού στον υπολογιστή τους. Στις παλιές μορφές απειλών και κινδύνων, όπως ένας ιός σε υπολογιστή ενός χρήστη, η αποκατάσταση του υπολογιστή μπορούσε να υλοποιηθεί με επανεγκατάσταση του λειτουργικού, ή και την αλλαγή των κωδικών πρόσβασης και την ακύρωση των οποιωνδήποτε πιστωτικών, τα στοιχεία των οποίων είχαν υποκλαπεί (Fire et al., 2014). «Ωστόσο, για να ανακάμψει από μια σύγχρονη επίθεση στο διαδικτυακό κοινωνικό δίκτυο που "κλέβει την πραγματικότητά σας", πρέπει να καταβληθεί μεγαλύτερη προσπάθεια, επειδή η επαναφορά των προσωπικών πληροφοριών είναι υπερβολικά χρονοβόρα και όχι πάντα εφικτή. Για παράδειγμα, μπορείτε να αλλάξετε τη

διεύθυνση ηλεκτρονικού ταχυδρομείου σας, αλλά θα ήταν πολύ πιο δύσκολο να αλλάξετε τη διεύθυνση κατοικίας σας όπως αναφέρουν οι Fire et al. (2014).

### 2.6.4 Κίνδυνοι και Απειλές σε παιδιά

Πολλά από τα Μέσα Κοινωνικής Δικτύωσης προορίζονται για χρήση από εφήβους και ενήλικες, κάποια εξ αυτών δεν έχουν καθόλου όριο ηλικίας και κάποια εξ αυτών απευθύνονται και σε παιδιά. Είναι αναμφισβήτητο ότι τα Μέσα Κοινωνικής Δικτύωσης προσφέρουν πολλές ευκαιρίες στους νέους ανθρώπους ταυτόχρονα όμως συνδέονται και με κινδύνους.

Οι χρήστες των Κοινωνικών Δικτύων ανεξαρτήτως ηλικίας είναι εκτεθειμένοι σε όλες τις προαναφερόμενες απειλές και κινδύνους. Τα παιδιά, όμως και οι έφηβοι αποτελούν και ένα τελείως διαφορετικό στόχο και εκτίθενται και σε άλλους κινδύνους. **Online Predators, Risky Behaviors, Cyberbullying (& Cyber abuse)** (Fire et al., 2014).

## Online predators

Αφορά την προστασία της ασφάλειας, των προσωπικών δεδομένων των παιδιών. Η συγκεκριμένη απειλή αναφέρεται στους παιδόφιλους και τον κίνδυνο που αυτοί εγκυμονούν για τα παιδιά. Διαδικτυακοί παιδόφιλοι (αποκαλούνται και ως Διαδικτυακά αρπακτικά/online predators), αποτελούν ένα μεγάλο κίνδυνο καθώς μπορούν να επιφέρουν σοβαρές βλάβες στα θύματα τους. Η οργάνωση "Kids Online" της Ευρωπαϊκής Ένωσης, έχει καθιερώσει μια τυπολογία για την κατανόηση της συγκεκριμένης βλάβης και των συνεπειών που επιφέρουν. Αναφέρονται ως οι: **Βλάβες από περιεχόμενο** που αφορά την έκθεση των παιδιών σε πορνογραφικό υλικό ή γενικότερα σεξουαλικό περιεχόμενο, **βλάβη από επαφή** που αφορά την επαφή ενός ενήλικα με ένα παιδί με σκοπό την σεξουαλική εκμετάλλευση ή και κακοποίηση, **βλάβη από συμπεριφορά** που αφορά τις επικίνδυνες συμπεριφορές που μπορεί να επιδείξει το παιδί ως αρχάριος, επιθετικές ή επικίνδυνες συμπεριφορές. Η σεξουαλική εκμετάλλευση των παιδιών από ενήλικες περιλαμβάνει περιπτώσεις, κατά τις οποίες ένας ενήλικας προσπαθεί με διάφορους τρόπους να προσελκύσει ένα παιδί ή νεαρό άτομο και τις μεθόδους που μπορεί να ακολουθήσει διαδικτυακά. Η εικόνα αυτή περιλαμβάνει ένα ενήλικα ο οποίος προσποιείται τον φίλο σε ένα παιδί, με στόχο την απαγωγή ή βιασμό. Στόχος του επιτιθέμενου η συλλογή προσωπικών στοιχείων του παιδιού όπως και την προσωπική συνάντηση μαζί του. Οι μέθοδοι όμως που χρησιμοποιούνται τελικά απαιτούν πολύ περισσότερες ενέργειες και είναι πιο περίπλοκη. Τις περισσότερες φορές όπως αναφέρουν οι Fire et al. (2014), όταν οι διαδικτυακές συνομιλίες ενέχουν σεξουαλικές

συζητήσεις, τα παιδιά γνωρίζουν ότι συνομιλούν με ενήλικα και τις περισσότερες φορές εάν τελικά επιτευχθεί μια προσωπική επαφή μεταξύ ενός αρπακτικού (predator) και ενός παιδιού, μέχρι ενός σημείου, υπάρχει η γνώση για σεξουαλική δραστηριότητα. Συνήθως αυτού του τύπου οι συνομιλίες περιέχουν την χρήση άμεσων και ηλεκτρονικού ταχυδρομείου μηνυμάτων, "chatting" κ.α. ώστε να επιτευχθεί η δημιουργία σχέσης. Τις περισσότερες φορές όμως η προσωπική συνάντηση ενός ενήλικα με ένα παιδί δεν αφορά σεξουαλική δραστηριότητα, καθώς όμως απαιτεί γονική συναίνεση, εάν υλοποιηθεί χωρίς αυτή, τότε θεωρείται έγκλημα (Fire et al., 2014).

**Επικίνδυνες συμπεριφορές**

Αυτή η μορφή περιλαμβάνει συνδυαστικές μεθόδους επικοινωνίας παιδιών με ενήλικες ξένους, διαδικτυακές, είτε σε εικονικούς κόσμους, είτε συνομιλίας σε δωμάτια με αλληλεπιδράσεις, σεξουαλικές συζητήσεις, προσφέροντας ή με δόλο αποκτηθείσες προσωπικές πληροφορίες φωτογραφίες ή και άλλα προσωπικά δεδομένα. Η κάθε μια εκ των προαναφερόμενων αλληλεπιδράσεων και συμπεριφορών, ενέχουν ούτως ή άλλως κίνδυνο, συνδυαστικές περισσότερων παρόμοιων συμπεριφορών μπορούν να δημιουργήσουν πολύ μεγάλο άγχος, σχετικό με την προσωπική ασφάλεια του παιδιού (Fire et al., 2014). Σύμφωνα με τους Fire et al. (2014) ομάδες που είναι ευάλωτες σε τέτοιου τύπου κινδύνους, κατάχρησης του Διαδικτύου, είναι προσδιορίσιμες, και επιπλέον οι κατηγορίες των παιδιών που εκτίθενται περισσότερο σε τέτοιου είδους κινδύνους είναι παιδιά ευάλωτα, με ιστορικό σωματικής κακοποίησης ή σεξουαλικής κακοποίησης, με προβλήματα κατάθλιψης ή αντιμετωπίζουν προβλήματα κοινωνικής αλληλεπίδρασης.

**Κυβερνοεκφοβισμός "CyberBullying"**

Ο όρος Κυβερνοεκφοβισμός (Cyberbullying) έχει την βάση του στον όρο εκφοβισμό με την παραδοσιακή έννοια του όρου, εξαιτίας των ομοιοτήτων που παρουσιάζουν (πρόθεση, μέθοδο και συνέπειες). Ο Κυβερνοεκφοβισμός ορίζεται ως «η χρήση της τεχνολογίας για την παρενόχληση, την απειλή, την αμηχανία ή την στόχευση άλλου ατόμου. Εξ ορισμού, εμφανίζεται στους νέους. Όταν εμπλέκεται ένας ενήλικας, μπορεί να ανταποκριθεί στον ορισμό της παρενόχλησης στον κυβερνοχώρο ή του cyberstalking, ένα έγκλημα που μπορεί να έχει νομικές συνέπειες και να περιλαμβάνει χρόνο φυλάκισης» ("Cyberbullying (for Parents)—KidsHealth," n.d.). Στον ορισμό αυτό επίσης θα πρέπει να αναφέρουμε και την αδυναμία του θύματος να αντιδράσει (Antoniadou, Kokkinos, & Markos, 2016).

Αυτή η μορφή του Διαδικτυακού Εκφοβισμού υλοποιείται στις πλατφόρμες Κοινωνικής Δικτύωσης με μέσα, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα SMS, συζητήσεις διαδικτυακές, κινητά τηλέφωνα. Ο επιτιθέμενος χρησιμοποιεί την πλατφόρμα Κοινωνικής Δικτύωσης παρενοχλώντας το θύμα είτε μέσω μηνυμάτων, παρατηρήσεων, απειλών – επαναλαμβανομένων- είτε δημοσιεύοντας φωτογραφίες ή βίντεο του θύματος, είτε και με άλλες ενοχλητικές συμπεριφορές. Ο Κυβερνοεκφοβισμός αποτελεί ένα συχνό φαινόμενο στις Ιστοσελίδες Κοινωνικής Δικτύωσης, των οποίων η υποδομή χρησιμοποιείται για την διάδοση ενοχλητικών φημών, φωτογραφιών και βίντεο. Συνήθως αυτή η μορφή απευθύνεται και αφορά παιδιά, σε μεγαλύτερο βαθμό από ότι σε ενήλικες. Πρόσφατη έρευνα σε 18687 γονείς από 24 διαφορετικές χώρες, έκανε γνωστό ότι ένα ποσοστό γονέων της τάξης του 12%, ανέφεραν ότι το παιδί τους έχει υποστεί κυβερνοεκφοβισμό, επίσης ότι συμπεριφορές τέτοιες παρατηρούνται κατά κόρον σε ιστοσελίδες Κοινωνικών Δικτύων όπως το Facebook, με καταστροφικά αποτελέσματα για το θύμα που μπορεί να είναι, ακόμη και αυτοκτονίες (Fire et al., 2014). Σύμφωνα με τους Livingstone & Brake (2010), στα χαρακτηριστικά των εφήβων εντάσσεται μια διαδικασία πειράγματος “teasing”, ως κάτι κοινότυπο, με αναρτήσεις στις ιστοσελίδες Κοινωνικής Δικτύωσης «αμήχανων ή προσβλητικών» φωτογραφιών, η οποία όμως έχει αυξηθεί, γεγονός που εντείνει και τις ανησυχίες για τον κυβερνοεκφοβισμό. Σε έρευνα του 2006, στο Ηνωμένο Βασίλειο, ένα ποσοστό 69% ανέφερε ότι είχε υποστεί εκφοβισμό κατά τον προηγούμενο χρόνο, στην πραγματικότητα όμως, μόνο ένα 7%, ανέφερε ότι έλαβε κάποιο μήνυμα, ηλεκτρονικό ταχυδρομείο, με το οποίο έγινε ο εκφοβισμός. Τα ποσοστά στις ΗΠΑ, που έχουν αναφέρει ότι έχουν υποστεί εκφοβισμό, είναι στο 72% σε παιδιά ηλικίας 12-17%, - ενώ το ποσοστό αυτό σε σχολείο, βρέθηκε να είναι της τάξης του 85% (Livingstone & Brake, 2010). Οι συνέπειες του Κυβερνοεκφοβισμού, όπως και του παραδοσιακού εκφοβισμού, έχουν συνδεθεί με φαινόμενα συναισθηματικής δυσφορίας, παραβατικής συμπεριφοράς, κοινωνικό άγχος και χαμηλότερης αυτοεκτίμησης (Floros et al., 2013), ενόχλησης, κατάθλιψη. Πολλές φορές στην διαδικασία του κυβερνοεκφοβισμού, δεν είναι απαραίτητα συμμετέχοντες, μόνο το θύμα και ο θύτης αλλά μπορούν να υπάρχουν και άλλοι συμμετέχοντες, οι οποίοι να υποστηρίζουν τον θύτη, ή να παρατηρούν το φαινόμενο και τους εμπλεκόμενους ή ακόμη και να έχουν διττό ρόλο (Antoniadou et al., 2016). Οι παραβάτες στον κυβερνοεκφοβισμό είναι συνήθως άτομα της ίδιας ηλικίας όπως και τα θύματα, στο κοντινό περιβάλλον του θύματος. Η ανωνυμία πίσω από την οποία κρύβεται ο παραβάτης καθιστά το κόστος της πράξης μικρό, ο χώρος δε του

διαδικτύου, και των Μέσων κοινωνικής Δικτύωσης, (τα οποία είναι στην διάθεση των νέων και των παιδιών, και λόγω της εκπαιδευτικής δραστηριότητας), ευνοούν την γρήγορη διάδοση μιας οποιασδήποτε φήμης ή αρνητικού σχολίου ή άλλης επίθεσης. Στη πραγματικότητα ο χώρος του Διαδικτύου ενισχύει την παραβατική συμπεριφορά, καθώς ο παραβάτης εξασφαλίζεται, πίσω όχι μόνο από την ανωνυμία αλλά και από την μη επίβλεψη κατά την διάρκεια της πλοήγησής του στο Διαδίκτυο. Η πρόσβαση στο Διαδίκτυο είναι εύκολη, αλλά εξίσου εύκολη είναι η παράλογη χρήση του, που το καθιστά πολύ επικίνδυνο ειδικά για τους νέους χρήστες, χωρίς την απαιτούμενη αλλά και διακριτική επίβλεψη (Floros et al., 2013).

Έχει ήδη αναφερθεί ότι το μεγαλύτερο μέρος αυτών των κινδύνων και απειλών αφορούν στην ασφάλεια του χρήστη και στα Προσωπικά του Δεδομένα.

Το μεγαλύτερο μέρος των προαναφερθέντων κινδύνων αφορούν τις περισσότερες φορές **λανθασμένη ή απρόσεκτη** χρήση με αποκάλυψη προσωπικών πληροφοριών εκ μέρους του χρήστη, ενέργεια που εγείρει εγκληματικές πράξεις από τρίτους και εμπλέκει τον χρήστη σε κίνδυνο.

## 2.7 Ιδιωτικότητα και Ασφάλεια

Η πολύ μεγάλη άνθηση του Διαδικτύου και των Κοινωνικών Μέσων, (όπως έχει ήδη αναφερθεί), έχει επιδεινώσει πολύ, θέματα όπως η Ιδιωτικότητα και η ασφάλεια. Ήδη από το προηγούμενο τμήμα του κειμένου αναφέραμε ότι κυρίως, οι κίνδυνοι που αφορούν τους τελικούς χρήστες, σχετίζονται και στοχεύουν στα προσωπικά στοιχεία του χρήστη, που ο ίδιος, (πιο συχνά) ηθελημένα από ότι αθέλητα «δημοσιεύει». Οι Yisa et al. (2016), υποστηρίζουν το αντίστοιχο, ότι οι περισσότεροι κίνδυνοι οι σχετικοί με τις τεχνολογίες της Πληροφορίας και τα Κοινωνικά Δίκτυα είναι σχετικοί με την Ιδιωτικότητα (Privacy) και επίσης το ίδιο αναφέρουν και οι Dienlin & Metzger (2016) «Οι περισσότεροι κίνδυνοι σχετίζονται με πλευρές της Ιδιωτικότητας …».

Η Ιδιωτικότητα (Privacy), ορίζεται ως «το δικαίωμα κάποιου να κρατήσει τα προσωπικά του θέματα και τις σχέσεις του μυστικές (“PRIVACY | meaning in the Cambridge English Dictionary,” n.d.)». Διάφορες μελέτες υπάρχουν αναφορικά με την Ιδιωτικότητα, πολλοί ερευνητές έχουν μελετήσει το θέμα, αλλά δεν έχουν καταλήξει σε μια κοινή ορολογία, αναφορικά με την έννοια της Ιδιωτικότητας, όπως υποστηρίζουν τόσο οι Houghton & Joinson (2010), αλλά και οι Zhang et al. (2011). Η έννοια της Ιδιωτικότητας στην εκτός Διαδικτύου ζωής φαίνεται να αντιμετωπίζεται πιο απλά, καθώς το άτομο είναι πιο εύκολο να την διαφυλάξει (μπορεί πιο εύκολα να επιλέξει του τι πληροφορίες σχετικά με

τον εαυτό του και τις σχέσεις μπορεί ή και θέλει να αποκαλύψει), το θέμα της Ιδιωτικότητας όμως στα διαδίκτυο και ακόμη περισσότερο στα κοινωνικά Δίκτυα γίνεται ακόμη πιο περίπλοκο. Εγείρεται το θέμα, όπως υποστηρίζουν οι Zhang et al. (2011), του τι είναι Ιδιωτικότητα. Για τον λόγο αυτό ερευνητές έχουν προτείνει και εξετάσει διαφορετικές διαστάσεις της Ιδιωτικότητας. Όπως αναφέρουν οι Houghton & Joinson (2010), διάφορες διαστάσεις της Ιδιωτικότητας έχουν μελετηθεί, και αναφέρεται στους Burgoon, Parrott, le Poire, & Kelley, οι οποίοι μελετούν 4 διαφορετικές διαστάσεις τις Ιδιωτικότητας και τελικά την προσδιορίζουν ως «την ικανότητα να ελέγχει και να περιορίζει την φυσική, αλληλεπιδραστική, ψυχολογική και ενημερωτική πρόσβαση στον εαυτό ή την ομάδα του».

Η συμμετοχή σε Ιστοσελίδες Κοινωνικής Δικτύωσης απαιτεί την δημιουργία προσωπικού προφίλ, και εάν αυτό αφορά εταιρεία και αρκετά εταιρικά δεδομένα. Οι δημοσιευμένες πληροφορίες μπορούν να οδηγήσουν σε κινδύνους για την ασφάλεια των οργανισμών την έκθεση των εταιρικών δεδομένων στο κοινό, αλλά επίσης αυτές οι πληροφορίες μπορούν να εκτίθενται και στους χώρους εργασίας. Η ανάρτηση προσωπικών πληροφοριών από μέρους του χρήστη σε Ιστοσελίδες Κοινωνικής Δικτύωσης, αφήνει τον χρήστη σε δημόσιο έλεγχο, με τρόπο που αυτό μπορεί να χρησιμοποιηθεί εναντίον του. Οι δημοσιευμένες πληροφορίες μπορούν να οδηγήσουν σε κινδύνους ασφαλείας, κλοπή ταυτότητας, διαδικτυακή παρακολούθηση, παρενόχληση και άλλους κινδύνους (Williams et al., 2009).

Στην πραγματικότητα η αποκάλυψη πληροφοριών στα Κοινωνικά Δίκτυα είναι εγγενής των συστημάτων αυτών. Είναι ένας από τους βασικούς λόγους συμμετοχής των χρηστών σε αυτά. Τα περιβάλλοντα αυτά είναι με τέτοιο τρόπο οργανωμένα ώστε η πληροφορία να διαδίδεται και αυτό σχετίζεται με τα θετικά που προσφέρουν στο άτομο, καθώς ενισχύουν την δημιουργία και διατήρηση φίλων, σχέσεις υποστήριξης, πληροφορίες, (Taddei & Contena, 2013), ενημέρωση, εκπαίδευση κ.α..

Οι Yisa et al. (2016) αναφέρουν ότι το θέμα της Ιδιωτικότητας αποτελεί αναφαίρετο δικαίωμα του χρήση των Μέσων Κοινωνικής Δικτύωσης ωστόσο, διάφοροι ερευνητές που έχουν μελετήσει το θέμα, υποστηρίζουν σχεδόν την άποψη, ότι αυτό είναι εξαιρετικά δύσκολο έως και ανέφικτο, αναφερόμενη στην άποψη των Lucas & Borisov «ότι οι παραβιάσεις της ιδιωτικής ζωής είναι αναπόφευκτες, ανεξάρτητα από τις προσπάθειες των "ιδιοκτητών" των Κοινωνικών Δικτύων (OSNS ) "και των χρηστών"».

Η Ιδιωτικότητα των πληροφοριών αποτελεί μια ανησυχία των χρηστών των Κοινωνικών Δικτύων. Οι πληροφορίες που αποκαλύπτονται στο Διαδίκτυο μπορούν να παραμείνουν

για πάντα εκεί διαθέσιμες, σε όποιον μπορεί να αποκτήσει πρόσβαση χωρίς ο χρήστης που έχει προβεί στην δημοσίευση να το γνωρίζει (Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014).

Ενώ κάποιοι από τους κινδύνους αυτούς μπορεί να είναι εγγενείς στα ίδια τα κοινωνικά δίκτυα, στην πραγματικότητα ενισχύονται από τον ανθρώπινο παράγοντα. Η ασφάλεια είναι ένας σοβαρός κίνδυνος και υπάρχει κίνδυνος να ενισχυθεί είτε από ελλιπή γνώσεων του χρήστη για την διαχείριση του κινδύνου την ώρα που βρίσκεται στο Διαδίκτυο ή απλά αλληλοεπιδρά, ή ακόμη και από το γεγονός ότι οι χρήστες αδιαφορούν για την ίδια την ασφάλειά τους. Αυτό μπορεί να έχει ως αποτέλεσμα την εκμετάλλευση τους από διάφορους εισβολείς, οι οποίοι προσβλέπουν σε προσωπικό όφελος, οικονομικό, κοινωνικό ή και ψυχολογικό.

Υπάρχουν 3 διαφορετικές πηγές διαρροής των προσωπικών πληροφοριών στα Μέσα Κοινωνικής Δικτύωσης, μέσω των οποίων πλήττεται η Ιδιωτικότητα και οδηγεί στην έκθεση σε κινδύνους (Yisa et al., 2016).

Αρχικά από τους ίδιους τους χρήστες (ηθελημένα ή αθέλητα), οι οποίοι πολλές φορές αγνοούν και δεν ασχολούνται με τις ρυθμίσεις ασφαλείας. Μελέτες όπως υποστηρίζουν οι Yisa et al. (2016), έχουν καταγράψει την αδιαφορία των χρηστών για την Προστασία της Ιδιωτικότητας τους και της προσωπικής τους ζωής (αγνοώντας τις ρυθμίσεις ασφαλείας) και αυτό είναι πιο κοινό στους νέους ηλικιακά χρήστες των Ιστοσελίδων Κοινωνικής Δικτύωσης, αν και είναι ενήμεροι, των κινδύνων που εγκυμονούν. Οι ενήλικες χρήστες ανησυχούν περισσότερο για τους κινδύνους ασφαλείας με αποτέλεσμα να φροντίζουν τις ρυθμίσεις Ασφαλείας και Απορρήτου. «Η αυτοπαραβίαση της Προστασίας της Ιδιωτικότητας εκθέτει το άτομο σε κινδύνους όπως της υπερβολικής αποκάλυψης πληροφοριών και της ανεπιθύμητης παρακολούθησης cyber stalking» (Yisa et al., 2016).

Δεύτερη πηγή αποτελούν τα ίδια τα Μέσα Κοινωνικής Δικτύωσης, οι εταιρείες. Τα ίδια τα Κοινωνικά Μέσα, ευνοούν (είναι στον γενετικό τους κώδικα), και προτρέπουν την ανταλλαγή πληροφοριών καθώς αποτελεί λειτουργικό μέρος των υπηρεσιών που παρέχουν. Τα συστήματα όμως υποστήριξης των εταιρειών (των Κοινωνικών Μέσων) δεν είναι ικανοποιητικά (δεν επαρκούν), εξαιτίας «των αδύναμων μηχανισμών ασφαλείας» που διατηρούν, όπως αναφέρουν οι Yisa et al. (2016), «είναι σχεδόν αδύνατο να εξασφαλιστεί ταυτόχρονα η χρηστικότητα, η λειτουργικότητα και η ασφάλεια». Αυτό σημαίνει ότι τα συστήματά τους είναι επιρρεπή σε εισβολείς και παραβιάσεις. Επίσης θα πρέπει να αναφερθεί και η σκόπιμη, από πλευράς των εταιρειών, διάθεση ή και πώληση

των προσωπικών δεδομένων των χρηστών για λόγους κερδοσκοπικούς (υπηρεσίες διαφημίσεων) (Yisa et al., 2016).

Τρίτη και τελευταία μορφή παραβίασης της Ιδιωτικότητας οφείλεται σε κάποιους κακόβουλους, νόμιμους χρήστες των Κοινωνικών Δικτύων. Οι Yisa et al. (2016) αναφέρονται σε μελέτη που αφορούσε τους χρήστες του Facebook και εντόπισε ότι έως και το 10% των χρηστών, είναι είτε ψεύτικοι είτε διπλοί λογαριασμοί. Αυτό αφήνει τους χρήστες του Κοινωνικού Δικτύου, εκτεθειμένους σε κινδύνους όπως, «ανεπιθύμητα μηνύματα (spamming), κοινωνική μηχανική (social engineering), κλοπή ταυτότητας, επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing) και κακόβουλα προγράμματα (Yisa et al., 2016).

Είναι πολύ σημαντικό για τους χρήστες των Κοινωνικών Δικτύων να είναι ενήμεροι για τους κινδύνους που εγκυμονούν από την αποκάλυψη τόσο πληροφοριών όσο και των ρυθμίσεων απορρήτου των Ιστοσελίδων Κοινωνικής Δικτύωσης που συμμετέχουν.

### 2.7.1 **Κίνδυνοι που αφορούν Εταιρείες (Big Data** & Πιθανές εναλλακτικές χρήσης)

Οι πληροφορίες για τα προσωπικά δεδομένα των χρηστών των ΙΚΔ εγείρει ανησυχία τα τελευταία χρόνια. Η φύση των ΙΚΔ είναι συνυφασμένη με την αποκάλυψη και διαμοιρασμό των προσωπικών πληροφοριών των χρηστών τους. Αποτελεί δε ένα θέμα αρκετά ενδιαφέρον τόσο για τους απλούς χρήστες ή τους ερευνητές είτε και για τις εταιρείες των ΙΚΔ ή και για όσους ασχολούνται με την προώθηση προϊόντων (διαφημιστές). Big Data αποτελούν οι βάσεις δεδομένων των χρηστών, ή όπως πιο συγκεκριμένα αναφέρουν οι Alashoor et al (2017) είναι τα "σύνολα δεδομένων των οποίων το μέγεθος είναι πέρα από την ικανότητα τυπικών εργαλείων λογισμικού βάσης δεδομένων να συλλαμβάνουν, να αποθηκεύουν, να διαχειρίζονται και να αναλύουν"(Alashoor et al., 2017). Η διαχείριση δε αυτών των δεδομένων, καθώς μπορεί να εξυπηρετήσει πολλούς και διαφορετικούς σκοπούς, έχει υιοθετηθεί από εταιρείες ΙΚΔ όπως το Facebook, Twitter και άλλες εταιρείες ΙΚΔ, οι οποίες έχουν αποκτήσει την δυνατότητα μέσω της τεχνολογίας να διαχειριστούν «ψηφιακούς φακέλους σε επίπεδο λεπτομέρειας» (Alashoor et al., 2017). Όπως αναφέρθηκε ήδη πολλοί οι σκοποί που μπορούν να εξυπηρετηθούν από την επεξεργασία τους. Και φυσικά και μεγάλη η ανησυχία για τα δεδομένα των χρηστών, όπως ασφάλεια Ιδιωτικότητα ή η αξιοπιστία των δεδομένων που μπορούν να αποτελούν λόγους παρεμπόδισης χρήσης ΙΚΔ. Ο

κίνδυνος δηλαδή, να χρησιμοποιηθούν τα προσωπικά δεδομένα των χρηστών, με τρόπο που να μην τον εγκρίνουν, ή να μην το θέλουν. Η πρόσβαση στα δεδομένα των χρηστών των ΙΚΔ, αποτελεί μια σχετικά εύκολη διαδικασία, αρκετά προγράμματα λογισμικού (δωρεάν και μη), που μπορούν να παρέχουν προσωπικά δεδομένα χρηστών ΙΚΔ, τα οποία χρησιμοποιούν είτε εταιρείες προκειμένου να διαμορφώσουν την πολιτική προσέγγισης των υποψήφιων πελατών τους, ανάλογα με τα ενδιαφέροντά τους, ή αντίστοιχα, κακόβουλοι τρίτοι, με σκοπό εγκληματικές ενέργειες, οι οποίες έχουν ήδη αναλυθεί προγενέστερα στο κείμενο. Οι Alashoor et al. (2017), διαπίστωσαν σε έρευνα που υλοποίησαν, ότι η ενημέρωση για τα big data είχε αρνητικό αντίκτυπο, ενώ η ευαισθητοποίηση από τα big data και τις επιπτώσεις που μπορούν να επιφέρουν, είχε θετικό αντίκτυπο για την προστασία της ιδιωτικής ζωής. Και αντίστοιχα οι ανησυχία για την προστασία της Ιδιωτικότητας και της προσωπικής ζωής, επηρέασε την ακρίβεια των παρεχόμενων πληροφοριών από μεριά των χρηστών, σχετικά με τις παρεχόμενες πληροφορίες από μέρους τους. Αναφορικά με την διαχείριση αυτών των στοιχείων θα πρέπει επιπλέον να αναφερθούν και άλλες αιτίες χρήσης τους. Όπως αναφέρει ο Hilbert (2016), η παραγωγή των Big Data, στην πραγματικότητα υπάρχει και αναφέρει τα θετικά που μπορούν να προκύψουν από την παραγωγή τους. Υπάρχουν και παράγονται – επομένως μπορούν να χρησιμοποιηθούν εναλλακτικά. Αποτελούν μια μορφή «εναλλακτικών δεδομένων χαμηλού κόστους» και μπορούν να αποτελέσουν πηγή δεδομένων σε έρευνες. Παράδειγμα παραθέτει την περίπτωση της αναζήτησης στην Google, της αναζήτησης κοινών όρων αναζήτησης για την πρόβλεψη της εποχικής γρίπης μεταξύ 2003-2008, που μπορεί να χρησιμοποιηθεί για την δημιουργία στατιστικών για την πρόληψη ή διάδοση ασθενειών, χρησιμοποιώντας χαμηλού κόστους δεδομένα σε πραγματικό χρόνο. Μπορούν να αποτελέσουν τυχαία δειγματοληψία καθώς αποτελεί «ψηφιακό αποτύπωμα αυτού που συμβαίνει στον πραγματικό κόσμο». Η στατιστική αξία των Big data μπορεί να εξαρτηθεί κάθε φορά από την συσχέτιση των υπό έρευνα μεταβλητών. Σημαντικό στοιχείο η στατιστική αξία του δείγματος καθώς είναι σε πραγματικό χρόνο αλλά και το πεδίο έρευνας (Hilbert, 2016).

# Κεφάλαιο 3

# Ανασκόπηση της Βιβλιογραφίας

## 3.1 Προσδιορισμός λέξεων κλειδιών (Identity Key Terms):

Social Media, Social Network, Online Dangers, Risks, Threats, Addiction, Privacy, Cyberbullying, Careless Use, Internet, Cyberspace, Κοινωνικά Δίκτυα, Κοινωνικά Μέσα, Κίνδυνοι, Διαδίκτυο, Κυβερνοχώρος.

Η επιλογή των λέξεων κλειδιών έγινε με βάση το ερευνητικό θέμα της Δ.Ε. και σε συνδυασμό με τα ερευνητικά ερωτήματα που τέθηκαν προς διερεύνηση.

Για την διερεύνηση του θέματος χρησιμοποιήθηκαν οι λέξεις κλειδιά (identity key terms), που υπάρχουν μέσα στον τίτλο της μελέτης και σε συνδυασμό με τα ερευνητικά ερωτήματα. Οι όροι κλειδιά είναι: Social Media, Social Networks (Κοινωνικά Δίκτυα), On line (Διαδικτυακοί), Dangers, Risks (Κίνδυνοι), Threats, Privacy (Ιδιωτικότητα), Addiction (Εθισμός), Cyberbullying (Ηλεκτρονική Παρενόχληση), Careless Use (Απρόσεκτη Χρήση) αυτόνομες ή και συνδυαστικά μεταξύ τους.

## 3.2 Εντοπισμός Βιβλιογραφικών Πηγών

Η αναζήτηση της επιπλέον, της προτεινόμενης βιβλιογραφίας από τον επιβλέποντα, πραγματοποιήθηκε μέσω του εργαλείου MyAthens και πιο συγκεκριμένα του εργαλείου «Ebsco Discovery Service» της Ακαδημαϊκής Βιβλιοθήκης και των βάσεων δεδομένων στα οποία προσφέρει πρόσβαση το OUC (Open University of Cyprus). Για τον εντοπισμό της σχετικής, με το θέμα μας, βιβλιογραφίας, εκτός των λέξεων κλειδιών που αναφέρθηκαν, επιλέχθηκαν συγγράμματα στη βάση της σχετικότητας του θέματος και εφαρμόσθηκαν επιπλέον κριτήρια – περιορισμοί “Peer Reviewed” (Αξιολογημένα) «Ακαδημαϊκά Περιοδικά» (“Academic Journals”), «Κριτικές» (“Reviews”) και «Συνέδρια» (“Conferences”), ώστε μέσα από ένα μεγάλο μέρος διαθέσιμης βιβλιογραφίας να εντοπισθούν και τελικά επιλεχθούν τα καταλληλότερα & σημαντικότερα συγγράμματα για την υλοποίηση της έρευνας. Δευτερευόντως ως εργαλείο αναζήτησης

χρησιμοποιήθηκε και το Google Scholar.

## 3.3 Επιλογή Βιβλιογραφίας για Ανασκόπηση

Η κριτική αξιολόγηση των άρθρων επεκτάθηκε με διερεύνηση των επιστημομετρικών δεικτών, στο Google Scholar (https://scholar.google.gr) ώστε να εξασφαλισθεί η εγκυρότητα και αξιοπιστία τους, προκειμένου να ενταχθούν στην παρούσα ανασκόπηση βιβλιογραφίας τόσο στην βάση θεματικής σχετικότητας όσο και των citations (citations reported by Google Scholar).

- A review of research on cyber-bullying in Greece (Antoniadou & Kokkinos, 2015), cited by 19.
- Adolescent Online Cyberbullying in Greece: The Impact of Parental Online Security Practices, Bonding, and Online Impulsiveness (Floros et al., 2013), cited by 231.
- African youths and the dangers of social networking: a culture-centered approach to using social media (Ephraim, 2013), cited by 23.
- Age differences in privacy attitudes, literacy and privacy management on Facebook (Kezer, Sevi, Cemalcilar, & Baruh, 2016), cited by 26.
- Cyberbullying Among Greek High School Adolescents (Gkiomisi, Gkrizioti, Gkiomisi, Anastasilakis, & Kardaras, 2017), cited by 1.
- Digital Dangers and Cyber-Victimisation: A Study of European Adolescent Online Risky Behaviour for Sexual Exploitation (DeMarco et al., 2017), cited by 3.
- Do questions matter on children's answers about internet risk and safety? (Ponte, Simões, & Jorge, 2013) cited by 11.
- Dysfunctional internet behaviour symptoms in association with personality traits (Tsiolka, Bergiannaki, Margariti, Malliori, & Papageorgiou, 2017), cited by 2.
- Examining Characteristics and Associated Distress Related to Internet Harassment: Findings From the Second Youth Internet Safety Survey (Ybarra, Mitchell, Wolak, & Finkelhor, 2006), Cited by 649.
- Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information (Hajli & Lin, 2016), cited by 97.
- Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences, (Debatin, Lovejoy, Horn, & Hughes, 2009), cited by 1253.

- Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults (Christofides, Muise, & Desmarais, 2012a), cited by 207.
- INTERNET ADDICTION: THE EMERGENCE OF A NEW CLINICAL DISORDER (Young, Kimberly S., 1996), cited by 5399.
- Internet social network communities: Risk taking, trust, and privacy concerns, (Fogel & Nehmad, 2009), cited by 1050.
- Internet use and misuse: a multivariate regression analysis of the predictive factors of internet use among Greek adolescents (Tsitsika et al., 2009), cited by 185.
- On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications (Livingstone & Brake, 2010), cited by 415.
- Possible common correlates between bullying and cyber-bullying among adolescents (Antoniadou et al., 2016), cited by 29.
- Predicting Facebook users online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior (Saeri et al., 2014), cited by 45.
- Problematic Internet Use Among Greek University Students: An Ordinal Logistic Regression with Risk Factors of Negative Psychological Beliefs, Pornographic Sites, and Online Games (Frangos, Frangos, & Sotiropoulos, 2011), cited by 128.
- Problematic Social Media Use: Results from a Large-Scale Nationally Representative Adolescent Sample (Bányai et al., 2017), cited by 88.
- Re-visiting internet addiction among Taiwanese students: a cross-sectional comparison of students' expectations, online gaming, and online social interaction (Lee, Ko, & Chou, 2015), cited by 41.
- Risk factors and psychosocial characteristics of potential problematic and problematic internet use among adolescents: A cross-sectional study (Kormas, Critselis, Janikian, Kafetzis, & Tsitsika, 2011), cited by 208.
- Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior, (Christofides et al., 2012b), cited by 138.
- Security issues in Online Social Networks (Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, & Yan Chen, 2011), cited by 180.
- Should I stay or should I go? The moderating effect of self-image congruity and trust on social networking continued use (Kourouthanassis, Lekakos, & Gerakis, 2015), cited by 19.

- Social networking sites and contact risks among Flemish youth (Vandoninck et al., 2012), cited by 39.
- Social networking sites: finding a balance between their risks and benefits (Mitchell & Ybarra, 2009), cited by 38.
- Teen Videos on YouTube: Features and Digital Vulnerabilities (Montes-Vozmediano et al., 2018), cited by 8.
- The role of personality and depression in problematic use of social networking sites in Greece (Giota & Kleftaras, 2013), cited by 38.
- The threats of social networking: Old wine in new bottles? (Weir, Toolan, & Smeed, 2011), cited by 44.
- Use of Social Networking Sites and Risk of Cyberbullying Victimization: A Population-Level Study of Adolescents (Sampasa-Kanyinga & Hamilton, 2015), cited by 23.
- When Sharing Is a Bad Idea: The Effects of Online Social Network Engagement and Sharing Passwords with Friends on Cyberbullying Involvement (Meter & Bauman, 2015), cited by 25.

## 3.4 Ανασκόπηση προηγούμενων ερευνών / Περίληψη Βασικών Θεμάτων

Η Δομή της Βιβλιογραφικής ανασκόπησης θα γίνει στην βάση του Διαχωρισμού Διαδίκτυο και Κοινωνικά Δίκτυα, στην διεθνή Βιβλιογραφία, όσο και στην Ελληνική πραγματικότητα. Μέσα στην κάθε Θεματική ενότητα, θα εξετασθεί η βιβλιογραφία θεματικά και χρονικά και αναφορικά με τον Εθισμό αλλά και με κινδύνους που αφορούν την Προσωπική ζωή, Εκφοβισμό και λοιπούς κινδύνους. Αντίστοιχα θα εξετασθεί η βιβλιογραφία και για την Ελληνική Πραγματικότητα.

### 3.4.1 Διεθνείς Έρευνες

#### 3.4.1.1 Διαδίκτυο

##### 3.4.1.1.1 Διαδίκτυο και Εθισμός Διεθνής Βιβλιογραφία.

Από τους πρώτους που ασχολήθηκαν με το θέμα του εθισμού στο Διαδίκτυο είναι η **Kimberly Young** (1996)**,** η οποία διερεύνησε την ύπαρξη Εθισμού στο Διαδίκτυο και την

έκταση των προβλημάτων που δημιουργήθηκαν από πιθανή κατάχρηση. Η έρευνα που διεξήγαγε αφορούσε σε 2 ομάδες εθελοντών, οι οποίοι συγκεντρώθηκαν με διάφορους τρόπους από απάντηση σε αγγελίες εφημερίδων έως και αναζητούντες λέξεις όπως εθισμός στο Διαδίκτυο. Η μία με εξαρτημένους χρήστες Διαδικτύου (dependents) και μια ομάδα ελέγχου από μη εθισμένους χρήστες Διαδικτύου. Η έρευνα έγινε μέσω ενός Διαγνωστικού Ερωτηματολογίου το οποίο περιείχε 8 ερωτήσεις. Τα αποτελέσματα της έρευνας Αναφορικά με τα αποτελέσματα: Α: Χρόνος/ εβδομάδα χρήσης Διαδικτύου - Εξαρτημένοι = Μ 38,5 SD=8,04, -Μη Εξαρτημένοι= Μ 4,9 SD 4,7/εβδομάδα. Εντόπισε Προβλήματα: Εξαρτημένοι: αναφορικά με την υπερβολική χρήση, προβλήματα στην προσωπική, οικογενειακή και σε επαγγελματική ζωή που έχουν αναγνωρισθεί σε εθισμούς όπως αλκοολισμός, παθολογικό παιχνίδι (Pathological gambling), διατροφικές διαταραχές κλπ. Μη Εξαρτημένοι: Δεν αναφέρθηκαν προβλήματα εξαιτίας της χρήσης, παρά μόνο αδυναμία διαχείρισης χρόνου-Διαδικτυακού Χρόνου (Young, Kimberly S., 1996).

**Οι Lee et al** (2015), στην Ταιβάν, διερεύνησαν τους παράγοντες/ συντελεστές της συμπεριφοράς που εξηγούν την σχέση μεταξύ της προσδοκίας και του εθισμού στο Διαδίκτυο, σύμφωνα με την θεωρία της προσδοκίας. Η έρευνα είχε δείγμα 25573 συμμετέχοντες από τις συνολικές 25 χώρες τις Ταιβάν (Εθνική έρευνα) και διενεργήθηκε από το Υπουργείο Παιδείας της Ταιβάν. Οι συμμετέχοντες ήταν (13978) μαθητές ανωτέρων τάξεων Γυμνασίου & (11775) μαθητές κατωτέρω τάξεων Γυμνασίου. Στα αποτελέσματα τα αγόρια και των δύο ηλικιών παρουσίασαν μεγαλύτερη δραστηριότητα στα Διαδικτυακά παιχνίδια συγκριτικά με τα κορίτσια. Στις υπόλοιπες δραστηριότητες και πιο συγκεκριμένα στο blogging τα κορίτσια και των δύο επιπέδων παρουσίασαν στατιστικά μεγαλύτερα ποσοστά έναντι των αγοριών. Αναφορικά με την Σχέση μεταξύ των Διαδικτυακών παιχνιδιών και Διαδικτυακών κοινωνικών συμπεριφορών τα παιχνίδια και διαδικτυακές συνομιλίες αποτελούσαν τις πιο συχνές δραστηριότητες στο Διαδίκτυο, με μια ισχυρότερη τάση να οδηγήσουν τους εφήβους σε εθισμό, καθώς ικανοποιούν ανάγκες όπως αυτές της φιλίας/συντροφικότητας αλλά και των επιτεύξεων- που αποτελούν και τις δύο μεγαλύτερες ανάγκες των εφήβων. Καθώς το δείγμα αφορούσε μαθητές από την Ταιβάν τα αποτελέσματα δεν μπορούν να γενικευθούν και για άλλους χρήστες άλλων χωρών (Lee et al., 2015).

#### 3.4.1.1.2 Διαδίκτυο και Κίνδυνοι που αφορούν Προσωπική Ζωή

**Οι Ponte et al** (2013), στην Πορτογαλία, ερευνούν απαντήσεις παιδιών αναφορικά με την αντίληψή τους για τους Διαδικτυακούς κινδύνους. Οι κίνδυνοι που εξετάζονται αφορούν Σεξουαλικό περιεχόμενο, Βίαιο ή επιθετικό περιεχόμενο, συνομιλία με ξένους τόσο αναφορικά με επαφές όσο και επικοινωνία, Αποκάλυψη προσωπικών στοιχείων, ακατάλληλο περιεχόμενο, επικοινωνία από ξένους, εκφοβισμός. Η έρευνα αφορούσε 2 διαφορετικά δείγματα σε 2 διαφορετικές περιόδους. Αποτελέσματα: οι 4 ποιο κοινοί κίνδυνοι είναι Α. σεξουαλικού περιεχομένου Β. Βίαιο ή επιθετικό περιεχόμενο Γ. Συνομιλία με ξένους τόσο της επαφής όσο και της επικοινωνίας Δ. Αποκάλυψη στοιχείων προσωπικού περιεχομένου. Και ακολουθούν Ε. Ακατάλληλο περιεχόμενο ΣΤ. Επικοινωνία από ξένους Ζ. Εκφοβισμός κ.α. (Ponte et al., 2013).

#### 3.4.1.1.3 Διαδίκτυο και λοιποί Κίνδυνοι

Οι Ybarra, Mitchell et al. το 2006 στις ΗΠΑ διερεύνησαν τα χαρακτηριστικά των νέων ατόμων που αποτελούν στόχους Διαδικτυακής παρενόχλησης αλλά και τα χαρακτηριστικά της αναφερόμενης δυσφορίας, δυστυχίας, ως αποτελέσματος του συμβάντος. Έγινε έρευνα τηλεφωνική στις ΗΠΑ σε ένα δείγμα 1500 ατόμων ηλικίας μεταξύ 10-17 ετών και στην περίοδο μεταξύ Μαρτίου και Ιουνίου 2005. Το 51% των συμμετεχόντων στην έρευνα του YISS-2 ήταν γυναίκες έφηβοι. Ένα 77% των συμμετεχόντων ήταν έφηβοι ηλικίας μεταξύ 13-17 ετών και ένα 23% ήταν προ έφηβοι 10-12 ετών. Εκπαίδευση: 1 στους 5 ενήλικες (22%) δήλωσαν ανώτατη εκπαίδευση και αντίστοιχα 1 στους 5 (22%) μεταπτυχιακή εκπαίδευση. Η μεθοδολογία και οι ερωτήσεις βασίστηκαν στην Πρώτη Διαδικτυακή έρευνα στους νέους (YISS-1—First Youth Internet Safety Survey) του 2000 και οι συμμετέχοντες είχαν χρησιμοποιήσει το Διαδίκτυο τουλάχιστον μία φορά στην περίοδο των προηγούμενων. Τα αποτελέσματα της έρευνας 1500 συμμετέχοντες και συνολικά 130 νέοι θεωρήθηκαν ως υποβληθέντες σε παρενόχληση και οι ίδιοι εμφάνισαν στοιχεία θλίψης, δυστυχίας (distress). Αποτελέσματα: Χαρακτηριστικά των νέων ως στόχο Παρενόχλησης: 9% των συμμετεχόντων δήλωσαν Διαδικτυακή παρενόχληση τουλάχιστον μία φορά το προηγούμενο έτος. Ηλικιακά ήταν ελάχιστα μεγαλύτεροι των αντίστοιχων που δεν είχαν υποστεί, 58% των στόχων ήταν γυναίκες και το αντίστοιχο των μη 50%. 83% των στόχων λευκοί και το 7% Λατίνοι έναντι των μη στόχων όπου 75% λευκοί και το 9%

Λατίνοι. Χαμηλού εισοδήματος και μη τα ποσοστά ήταν αντίστοιχα 32% μη στόχοι και 35% οι στόχοι. Παράγοντες κινδύνου σχετικοί με επεισόδια Παρενόχλησης: 38% των υποβληθέντων σε Διαδικτυακή παρενόχληση ανέφεραν συναισθήματα δυσφορίας και δήλωσαν ότι φοβούνται εξαιτίας του περιστατικού. Επαναλαμβανόμενη παρενόχληση (3 φορές) παρατηρήθηκε σε ποσοστό 44% έναντι των μη σε ποσοστό 25% (Ybarra et al., 2006).

**Οι DeMarco et al., το 2017**, στην Ευρώπη, ερευνούν το είδος του Διαδικτυακού κινδύνου και πιο συγκεκριμένα της Διαδικτυακής σεξουαλικής Θυματοποίησης στο οποίο εκτίθενται οι έφηβοι, μελετώντας την συμπεριφορά μιας ομάδας εφήβων από διάφορες ευρωπαϊκές χώρες. Έγινε έρευνα και εκ των υστέρων ανάλυση νεαρών ατόμων ηλικίας μεταξύ 18-25 ετών από τρεις ευρωπαϊκές χώρες για τις εμπειρίες τους αναφορικά με συμπεριφορές ανάληψης κινδύνου στην περίοδο της εφηβείας τους (12-16 ετών). Οι 1166 συμμετέχοντες ανήκαν, ήταν ανώτερης εκπαίδευσης,- 340 από το Ηνωμένο Βασίλειο, 529 από την Ιρλανδία και 297 από την Ιταλία. Αποτελέσματα: Δημογραφικά Η μέση ηλικία του δείγματος ήταν τα 21, 23 έτη (με εύρος 18-25, SD=2.16), και το 72% των συμμετεχόντων να είναι θηλυκού γένους. Το μεγαλύτερο μέρος δήλωσε κύρια δραστηριότητα Φοιτητής με ένα 23% να έχουν πλήρη απασχόληση και ένα 5% να δηλώνει άνεργο. Το μεγαλύτερο μέρος των συμμετεχόντων δήλωσε ότι είναι εθνικότητας της χώρας στην οποία συμμετείχε. Επίσης το 83% δήλωσε ετερόφυλοι (σεξουαλικά) και ένα 10%, άλλο (LGBQT), αναφορικά με την σεξουαλική του προτίμηση. Αναφορικά με τις σχέσεις με τους γονείς, καλές σχέσεις το 59% της Ιρλανδίας, το 53% του Ηνωμένου Βασιλείου & 32% των Ιταλών. Πολύ Κακές σχέσεις αντίστοιχα δήλωσε 10% των Ιρλανδών, 8% των συμμετεχόντων του Ηνωμένου Βασιλείου & 17% των Ιταλών. Πάνω από το 23% των συμμετεχόντων δήλωσε ευτυχισμένα χρόνια εφηβείας και ένα 64% του δείγματος ότι είχαν καλούς φίλους στην περίοδο της διαμόρφωσης τους. Επικίνδυνη συμπεριφορά on line & offline ( όχι σεξουαλική) Βασικός παράγοντας άξονα (Principal Axis Factoring (PAF)) εφαρμόστηκε για να εξετάσει την δομή των παραγόντων που σχετίζονται με τους κινδύνους online & offline. Η ανάλυση των στοιχείων (Cronbach's alpha) έδειξε Μέτρια online επικίνδυνη συμπεριφορά (.66) Η μέτρηση για συνάντηση αγνώστων ξένων ομότιμων η άλλους ενήλικες ήταν χαμηλή (.53) και για την παρενόχληση είτε online είτε offline ήταν επίσης μέτρια (0.68). Για την επιθετική συμπεριφορά τόσο online & offline (του συμμετέχοντα ως παρενοχλούντα) η ανάλυση έδειξε ισχυρή συσχέτιση μεταξύ των δύο (0.59). Η σεξουαλική πρόσκληση (sexual

solicitation), τα αιτήματα και η προσοχή: Ο συσχετισμός μεταξύ των 4 στοιχείων ήταν πολύ σημαντική και κυμαινόταν από 0.60- 0.80 (DeMarco et al., 2017)

### 3.4.1.1 Κοινωνικά Δίκτυα

#### 3.4.1.1.1 Κοινωνικά Δίκτυα και Εθισμός

**Οι Banyai et al το 2017** στην Ουγγαρία, διερευνούν τις «ψυχομετρικές ιδιότητες της κλίμακας Bergen (Bergen Social Media Addiction Scale (BSMAS)) για τον εθισμό στα κοινωνικά Δίκτυα σε ένα δείγμα Ούγγρων εφήβων» και προσπαθεί να εκτιμήσει την προβληματική χρήση των κοινωνικών δικτύων αντίστοιχα σε ένα δείγμα Ούγγρων εφήβων σε εθνικό επίπεδο. Αποτελέσματα: Δημογραφικά στοιχεία 50,94% συμμετεχόντων άρρενες με μέση ηλικία 16.62 έτη (mean age 16.62 χρόνια, SD=0.96). Χρήση σε ώρες των Κοινωνικών Δικτύων ήταν 23.16 ώρες / εβδομάδα (SD = 15.57). Σημαντική διαφορά παρατηρήθηκε στη εβδομαδιαία χρήση μεταξύ των φύλων αρρένων & θηλέων. Προβληματική Χρήση Κοινωνικών Δικτύων. 3 κατηγορίες «καθόλου κινδύνου (no risk)» 78,3% των συμμετεχόντων σε Κοινωνικά Δίκτυα ( 70,7% του συνολικού Δείγματος) «Χαμηλού κινδύνου (low risk)» 17,2% των συμμετεχόντων (15,5% αντίστοιχα) «Σε κίνδυνο (at risk)». Η ομάδα που ανήκε στην κατηγορία σε κίνδυνο, η κατηγορία των συμπτωμάτων της στέρησης και της ανοχής ήταν αυξημένα συγκριτικά με άλλες διαστάσεις. Μέλη της προβληματικής χρήσης ήταν πιθανότερο να είναι θηλυκά, να χρησιμοποιούν το Διαδίκτυο και τα Κοινωνικά Δίκτυα περισσότερο από 30 ώρες/ εβδομάδα, να έχουν χαμηλότερη αυτοεκτίμηση και υψηλότερα επίπεδα κατάθλιψης από ότι οι άλλες 2 ομάδες (Bányai et al., 2017).

#### 3.4.1.1.2 Κοινωνικά Δίκτυα Κίνδυνοι Προσωπική ζωή

**Οι Debatin Lovejoy Horn & Hughes το 2009** στις ΗΠΑ εξετάζουν την αντίληψη των χρηστών αναφορικά με τα θέματα της Ιδιώτικότητας (ιδιωτικού απορρήτου), των κινδύνων αλλά και τα οφέλη από την χρήση του Facebook. Αποτελέσματα: 68% των συμμετεχόντων ήταν γυναίκες, το 95%, και ηλικιακά η μεγαλύτερη ομάδα ενήλικες 22-24 ετών (27%). Μισοί από τους συμμετέχοντες είχαν λογαριασμό Facebook για 2 χρόνια και το 37% εξ' αυτών, έλεγχε τον λογαριασμό του καθημερινά με το 25% αυτού, 3φορές/

ημέρα και το 23%, 5 φορές/ ημέρα. Ο μέσος χρόνος ήταν για τους μισούς συμμετέχοντες να δαπανούν 15 λεπτά / κάθε φορά ενώ ένα 20% δαπανούσε μέχρι 30 λεπτά/φορά και ένα 20% δαπανούσε μέχρι 5 λεπτά/ φορά. Ένα ποσοστό 29% ανέφερε ότι ο λογαριασμός τους του Facebook ήταν ενεργός ή ανοιχτός για όσο χρονικό διάστημα ήταν στο Διαδίκτυο. Οφέλη: πιο συγκεκριμένα την αλληλεπίδραση με φίλους ανέφερε ένα 83% των συμμετεχόντων. Κίνδυνοι και αρνητικές επιπτώσεις όπως: παρακολούθηση (stalking), κουτσομπολιά ή φήμες (gossip), παρενόχληση (harassment), ή κλοπή προσωπικών δεδομένων ανέφεραν ότι υπέστη και είχαν προσωπική άποψη, ένα ποσοστό 18% των συμμετεχόντων. Αναφορικά με την πρόσβαση στα προσωπικά στοιχεία των συμμετεχόντων 47% ότι περιόρισαν την πρόσβαση στα προσωπικά τους στοιχεία λόγω προσωπικής εγρήγορσης και ένα 38% εξαιτίας πληροφοριών των οποίων έγιναν δέκτες. Στα υποθετικά ερωτήματα αναφορικά με την Ιδιωτικότητα και την γνώση από μέρους των χρηστών, η μεγάλη πλειοψηφία δήλωσε ότι γνωρίζει τις ρυθμίσεις για την Ιδιωτικότητα και προστατεύει τα προσωπικά τους δεδομένα και αντίστοιχα το αντίθετο στους συμμετέχοντες που δεν γνώριζαν τις ρυθμίσεις του απορρήτου και της ιδιώτικότητας. Αναφορικά με το υποθετικό ερώτημα της υπερίσχυσης των πλεονεκτημάτων πάνω από τους κινδύνους από την αποκάλυψη των προσωπικών τους στοιχείων, αυτό υποστηρίχθηκε (Debatin et al., 2009).

**Οι Fogel & Nehmad, το 2009** στις ΗΠΑ, εξετάζουν θέματα έκθεσης σε κίνδυνους καθώς και θέματα Ιδιώτικότητας σε ιστοσελίδες Κοινωνικής Δικτύωσης. Αποτελέσματα: Δημογραφικά Στοιχεία: Μέσος όρος ηλικίας 22 ετών, ίση συμμετοχή μεταξύ ανδρών και γυναικών. Δημιουργία Προφίλ σε ιστοσελίδες Κοινωνικής Δικτύωσης. Τα ¾ των συμμετεχόντων διατηρούν λογαριασμό σε Σελίδες Κοινωνικής δικτύωσης με αυτή του Facebook να είναι ελαφρώς μεγαλύτερη από αυτή του MySpace. Ανάληψη κινδύνου, εμπιστοσύνη και Ιδιωτικότητα σύγκριση μεταξύ των εχόντων και μη, λογαριασμό σε ιστοσελίδες Κοινωνικής Δικτύωσης: Μεγαλύτερη ανάληψη κινδύνου από τους έχοντες λογαριασμό σε σχέση με τους μη έχοντες και με το Facebook να θεωρείται πιο αξιόπιστο. Στοιχεία ταυτότητας: Μεγαλύτερη αποκάλυψη προσωπικών στοιχείων από τους έχοντες λογαριασμό σε Ιστοσελίδες Κοινωνικής Δικτύωσης που δηλώνει μικρότερη ανησυχία για την αποκάλυψη προσωπικών στοιχείων στις ιστοσελίδες. Αποκάλυψη στοιχείων ταυτότητας στο διαδίκτυο. Τα άτομα με λογαριασμό σε Κοινωνικά Δίκτυα έδειξαν μικρότερη ανησυχία για την αποκάλυψη προσωπικών στοιχείων στο Διαδίκτυο. Συγκρίσεις μεταξύ Ανδρών και Γυναικών αναφορικά με την ανάληψη κινδύνου, εμπιστοσύνης και ιδιώτικότητας οι άνδρες είχαν μεγαλύτερη βαθμολογία ενώ

αντίστοιχα οι γυναίκες μεγαλύτερη ανησυχία για την αποκάλυψη προσωπικών στοιχείων και αποκαλύπτουν λιγότερα προσωπικά στοιχεία σε σχέση με τους άνδρες (Fogel & Nehmad, 2009).

**Οι Christofides et al** (2012a) στον Καναδά, ερευνούν την ύπαρξη πραγματικών διαφορών μεταξύ εφήβων και ενηλίκων ως προς την αποκάλυψη προσωπικών πληροφοριών και την συμπεριφορά προστασίας της προσωπικής τους ζωής. Η Διαδικτυακή Έρευνα έγινε σε Ερευνητικό Κέντρο Επιστημών μεταξύ 2 ομάδων απαρτιζόμενων από 288 Εφήβους και 285 Ενήλικες. Τα αποτελέσματα έδειξαν: Χρόνος Χρήσης του Facebook: Ενήλικες :M 27,84 SD 14,48 μήνες, Έφηβοι: M 14,84 SD 14,84 μήνες, με μεγαλύτερους χρόνους/ ημέρα να δαπανούν οι Έφηβοι. Ενήλικες: M 38,2/ λεπτά SD 57,25 λεπτά, Έφηβοι: M 55,9/λεπτά SD 62,25 λεπτά. Αποκάλυψη Πληροφοριών: Έφηβοι : Αναφέρθηκε ότι ήταν πιο πιθανό να αποκαλύψουν προσωπικές πληροφορίες από ότι οι ενήλικες με ένα ποσοστό 35,4% των εφήβων και ένα 29% των ενηλίκων να αναφέρουν ότι υπάρχει πιθανότητα να αποκαλύψουν πληροφορίες στο Facebook. Τόσο οι Ενήλικες όσο και οι Έφηβοι με μεγαλύτερη ανάγκη για Δημοτικότητα και μικρότερη ανησυχία για τις συνέπειες, ήταν πολύ πιθανότερο να αποκαλύψουν προσωπικές πληροφορίες, η ηλικία, όπως και ο δαπανηθείς χρόνος στο Facebook, προέβλεψε μεγαλύτερη αποκάλυψη πληροφοριών από τους Εφήβους και όχι από τους Ενήλικες. Έλεγχος Πληροφοριών (Facebook ρυθμίσεις απορρήτου).Ενήλικες και Έφηβοι: και για τις δύο ομάδες, η συνειδητοποίηση των συνεπειών από την αποκάλυψη πληροφορίας ήταν ο σημαντικότερος παράγοντας για τον έλεγχο της πληροφορίας. Οι ενήλικες φάνηκε να έχουν μικρότερη επίγνωση για τις συνέπειες από ότι οι Έφηβοι. Αναφορικά με το χρόνο που δαπανά κανείς στο Facebook ως παράγοντα για τον έλεγχο των πληροφοριών δεν φαίνεται να έχει διαφοροποίηση μεταξύ των 2 ομάδων, ήταν αντίστοιχος τόσο για τους ενήλικες όσο και για τους Εφήβους. Οι γυναίκες ήταν πιθανότερο να ελέγξουν τις πληροφορίες συγκριτικά με τους άνδρες. Παράγοντες όπως η ηλικία, μεγαλύτερη αυτοεκτίμηση, όπως και χαμηλότερα επίπεδα εμπιστοσύνης αποτελούν καθοριστικά στοιχεία για τον έλεγχο των πληροφοριών περισσότερο στους Εφήβους παρά στους Ενήλικες. Περισσότερες ομοιότητες παρά διαφορές έχουν οι δύο ομάδες Έφηβοι με ενήλικες μεταξύ τους αναφορικά με την προστασία της προσωπικής ζωής (Christofides et al., 2012a).

**Οι Christofides, Muise, & Desmarais, το 2012**, στον Καναδά, διερευνούν τα αποτελέσματα από την επίδραση μιας αρνητικής εμπειρίας στις ρυθμίσεις απορρήτου του Facebook και εξετάζουν ποιοτικά την φύση και τους τύπους των αρνητικών εμπειριών που βιώνουν οι έφηβοι στο Facebook. Η Έρευνα γίνεται μεταξύ 256 χρηστών του Facebook ηλικίας 12-18 ετών, 156 κορίτσια και 96 αγόρια. Αποτελέσματα:26,7% ανέφερε ότι είχε μια κακή εμπειρία στο Facebook. Μετά από θεματική ανάλυση των αναφερομένων κακών εμπειριών, 4 διαφορετικές μορφές παρενόχλησης μελετήθηκαν: Εκφοβισμός/ Ευτέλεια, Ανεπιθύμητη επαφή, έκθεση και χωρίς πρόθεση αποκάλυψη και παρεξήγηση. Εκφοβισμός/Ευτέλεια 52% των συμμετεχόντων που είχε κακή εμπειρία στο Facebook, ήταν σχετική με εκφοβισμό παρενόχληση και ευτέλεια από συνομήλικους που αποτελεί και την πιο κοινή κακή εμπειρία. Ανεπιθύμητη επαφή: 23% των εχόντων κακή εμπειρία ανέφερε ανεπιθύμητα αιτήματα από φίλους ή μηνύματα από ξένους που αποτελεί την αμέσως επόμενη συχνότερα αναφερόμενη κακή εμπειρία. Έκθεση και χωρίς πρόθεση αποκάλυψη: 17% ανέφερε αυτή την εμπειρία που συνήθως είναι η ανάρτηση από φίλους πληροφορίας ή φωτογραφίας που το ίδιο το άτομο δεν θα αναρτούσε. Παρεξηγήσεις: 7% αφορούσε πληροφορίες αναρτημένες στο Διαδίκτυο που δημιούργησαν παρανόηση. Συνήθως αφορούσε φίλους ή εργοδότη. Η υπόθεση της παρούσας έρευνας ότι έχοντας κακή εμπειρία στο Facebook οδηγεί σε αυξημένη χρήση των ρυθμίσεων απορρήτου, και επίσης ότι αυτή η συμπεριφορά θα διαμεσολαβείται από την γνώση των ρυθμίσεων μέσω της παρούσας έρευνας πιστοποιήθηκε. Οι χρήστες που αντιμετώπισαν μια κακή εμπειρία στο Facebook ήταν πιθανότερο να γνωρίζουν περισσότερα για τις ρυθμίσεις απορρήτου (Christofides et al., 2012b).

**Οι Saeri, Ogilvie, La Macchia, Smith, & Louis το 2014,** στην Αυστραλία, μελετούν την Διαδικτυακή Προστασία της προσωπικής ζωής στο Facebook σε σχέση με την θεωρία της Προγραμματισμένης Συμπεριφοράς (Planned Behavior), και ταυτόχρονα εξετάζει, λαμβάνει υπόψη το ρόλο των περιγραφικών κανόνων, των αντιλαμβανομένων κινδύνων και της εμπιστοσύνης. Έγινε έρευνα. Βολικό δείγμα πρωτοετών φοιτητών Ψυχολογίας 119 ατόμων, που ταυτόχρονα ήταν χρήστες Facebook. Αποτελέσματα: Πραγματοποιήθηκε μια ιεραρχική ανάλυση πολλαπλής παλινδρόμησης για να προβλεφθεί η πρόθεση. Διαδικτυακή Προστασία Ιδιωτικής ζωής Προθέσεις και Συμπεριφορά: τα δημογραφικά στοιχεία εξηγούν το 6% της διακύμανσης στις προθέσεις προστασίας της ιδιωτικής ζωής, ($F(2.108) = 3.50$, $p = .034$). Οι μεγαλύτερες ηλικίες είχαν μεγαλύτερες προθέσεις να προφυλάξουν την Ιδιωτική τους ζωή ($\beta = .20$,$p = .032$, $sr2 =$

.04), χωρίς να υπάρχουν διαφορές ως προς το φύλο (β = .14, p = .126, sr2 = .02). Όταν οι συμμετέχοντες αντελήφθησαν ότι «σημαντικοί άλλοι» ενέκριναν την προστασία της Προσωπικής Ζωής στο Διαδίκτυο έδειξαν μεγαλύτερες προθέσεις προστασίας της (β = .29, p = .003, sr2 = .06). Το αντίστοιχο συνέβη και όταν οι συμμετέχοντες παρατήρησαν ότι «σημαντικοί άλλοι» προστατεύουν την δικής τους Προσωπική Ζωή στο Διαδίκτυο, & αντίστοιχα επέδειξαν μεγαλύτερες προθέσεις προστασίας της Προσωπικής τους Ζωής (β = .27, p = .005, sr2 = .05). Ο αντιληπτός κίνδυνος ήταν θετικά συνδεδεμένος με την πρόθεση της προστασίας της Προσωπικής Ζωής (β = .17, p = .044, sr2 = .03). Η εμπιστοσύνη, αντίθετα, δεν ήταν σημαντικά συσχετισμένη (β < .01, p = .970, sr2 < .01) Συμπεριφορά: Οι γυναίκες επέδειξαν μεγαλύτερη προστασία Προσωπικής Ζωής από ότι οι άνδρες. Ενώ αντίστοιχα όχι η ηλικία (Saeri et al., 2014).

**Οι Kezer, Sevi, Cemalcilar, & Baruh, το 2016** στις ΗΠΑ, εξετάζουν την χρήση του Facebook, συμπεριφορές σχετικά με το απόρρητο, την παιδεία/ εκπαίδευση για το διαδικτυακό απόρρητο, την αποκάλυψη αλλά και την συμπεριφορά για την αποκάλυψη προσωπικών δεδομένων στο Facebook, για τρεις ηλικιακές ομάδες ατόμων α.18-40, β. 41-65 και γ. 65+ (συγκριτικά μεταξύ τους). Η έννοια του απορρήτου προσεγγίζεται πολυδιάστατα. Σε 1540 άτομα ζητήθηκε η συμμετοχή στην έρευνα. Από αυτούς οι 600 απάντησαν και από τους 600 οι 518 ήταν χρήστες του Facebook και στους οποίους χρήστες, εστίασε και η έρευνα. Οι συμμετέχοντες ήταν μεταξύ των ηλικιών 18 – 85 ετών ( 53,3% γυναίκες ). Οι συμμετέχοντες έλαβαν μετρητά ή δώρο κάρτα από την «Qualtrics». Οι συμμετέχοντες χωρίστηκαν σε ομάδες ανάλογα με τη ηλικία και οι τρείς ομάδες ήταν συγκριτικά όμοιες μεταξύ τους αναφορικά με την εκπαίδευση τους. Χρήση Διαδικτύου\ κοινωνικών δικτύων και χαρακτηριστικά αναφορικά με το δίκτυο των φίλων του Facebook και των χρήσεων του Facebook συγκριτικά μεταξύ των ηλικιακών ομάδων σε όρους χρήσης του Διαδικτύου σε χρόνια (e, F(2, 510) = 0.348, p > .05 ) αλλά και σε ώρες ημερήσιας χρήσης του Διαδικτύου (Welch's F(2, 135.80) = 2.576, p > .05), δεν φαίνεται να εμφανίζει μεγάλες διαφορές. Μικρότερη χρήση του Διαδικτύου ωστόσο έχουν οι συμμετέχοντες 65+ κατά την διάρκεια του Σαββατοκύριακου (Welch's F(2, 130.14) = 9.659, p < .001) Ηλικιακές διαφορές στη Χρήση Facebook, αποκάλυψη και προστασία προσωπικών δεδομένων στο Facebook. Χωρίς σημαντικές διαφορές στις μετρήσεις αναφορικά με την γνωριμία με ξένους, τη χρήση του Facebook για ενημέρωση και για χρήση για διασκέδαση. Μικρή διαφοροποίηση μεταξύ των ηλικιακών ομάδων αναφορικά με την παραμετροποίηση του Facebook για κοινωνική αλληλεπίδραση, με τους νέους να

το υλοποιούν περισσότερο από ότι οι μεγαλύτεροι. Ηλικιακές διαφορές στις Συμπεριφορές της ιδιώτικότητας και η επιρροή τους στην προστασία των προσωπικών δεδομένων στο Facebook. Οι μεγαλύτεροι σε ηλικία συμμετέχοντες στην επιρροή συμπεριφορών ιδιώτικότητας για τη χρήση μέτρων προστασίας έδειξαν μεγαλύτερη τάση από ότι οι άλλες δύο. Συγκριτικά αντίστοιχες συμπεριφορές μεταξύ των ηλικιακών ομάδων παρατηρήθηκε στο ερώτημα «ανησυχίες για του ιδίου τα προσωπικά δεδομένα» Συμπερασματικά τα ευρήματα ήταν: οι 65+ συμμετέχοντες ήταν λιγότερο πιθανό να αποκαλύψουν πληροφορίες και επίσης λιγότερο πιθανό να χρησιμοποιήσουν τα μέτρα προστασίας του Facebook. Αναφορικά με τη χρήση του Facebook: διαφορές παρατηρήθηκαν στην χρήση και στον σκοπό χρήσης του Facebook/ οι μεγαλύτεροι ενήλικες μικρότερα δίκτυα φίλων και επίσης λιγότερο πιθανό να χρησιμοποιήσουν το Facebook για κοινωνική αλληλεπίδραση. Αναφορικά με την διαδικτυακή παιδεία δεν βρέθηκαν σημαντικές διαφορές μεταξύ των ηλικιακών ομάδων. Αναφορικά με την πολυδιάστατη προσέγγιση της προστασίας τη ιδιώτικότητας και την λήψη μέτρων τα ευρήματα της έρευνας δηλώνουν ότι στους 65+ είναι πιο ισχυρή (Kezer et al., 2016).

#### 3.4.1.1.3 Κοινωνικά Δίκτυα και εκφοβισμός

**Οι Meter & Bauman, το 2015,** στις Η.Π.Α διερεύνησαν μεταξύ 1272 φοιτητών (μεταξύ 3ης και 8ης τάξης στις νοτιοδυτικές περιοχές των Η.Π.Α.) τα διαχρονικά αποτελέσματα της επικίνδυνης Διαδικτυακής συμπεριφοράς στη συμμετοχή σε Διαδικτυακό εκφοβισμό. Αποτελέσματα: Συμμετοχή σε Κοινωνικά Δίκτυα: Η έρευνα έδειξε ότι η συμμετοχή σε κοινωνικά Δίκτυα αυξάνει τις πιθανότητες της συμμετοχής σε διαδικτυακό εκφοβισμό. Επίσης ότι σε όσο περισσότερα κοινωνικά δίκτυα δραστηριοποιείται ο χρήστης στον χρόνο Τ1 (1ο δείγμα) περισσότερο ανέφεραν ότι διαμοίραζαν κωδικούς πρόσβασης στον Τ2 ( 2ο δείγμα). Διαμοιρασμός κωδικών πρόσβασης: Παρά το γεγονός ότι η αυξημένη συμμετοχή σε πολλά Κοινωνικά Δίκτυα ενέχει μεγαλύτερη αποκάλυψη Προσωπικών κωδικών πρόσβασης αυτό δεν σημαίνει αυτόματα και αυξημένο κίνδυνο σε φαινόμενα Διαδικτυακού εκφοβισμού όταν η αποκάλυψη των προσωπικών κωδικών γίνεται σε φίλους. Συμμετοχή σε Διαδικτυακό Εκφοβισμό: Επίσης η έρευνα έδειξε ότι όσοι συμμετείχαν ή ενεπλάκησαν σε φαινόμενα Διαδικτυακού εκφοβισμού στον χρόνο Τ1 τόσο λιγότερο αποκάλυπταν προσωπικούς κωδικούς στο δεύτερο δείγμα στο δεύτερο χρόνο Τ2. Αυτά τα αποτελέσματα δεν γενικεύονται σε άλλα δείγματα σε άλλες περιοχές (Meter & Bauman, 2015).

**Οι Sampasa-Kanyinga & Hamilton, 2015,** στον Καναδά ερεύνησαν την σχέση χρήσης Κοινωνικών Δικτύων με την εμφάνιση φαινομένων υποκειμένων σε Διαδικτυακό Εκφοβισμό, σε δείγμα συμμετεχόντων μαθητών Μέσης και Δευτεροβάθμιας εκπαίδευσης δείγμα 5478 μαθητών ηλικίας 11-20 Ετών. Αποτελέσματα: Υπήρξαν σημαντικές διαφορές στη χρήση των κοινωνικών Δικτύων συγκριτικά μεταξύ των φύλων ([F(4.75, 844.95) = 11.25, p < 0.001]) Οι γυναίκες ήταν πιθανότερο και για μεγαλύτερο χρονικό διάστημα να χρησιμοποιήσουν τα Κοινωνικά Δίκτυα σε σχέση με τους άνδρες. Οι νεότεροι φοιτητές χρησιμοποιούσαν τα Κοινωνικά Δίκτυα λιγότερες ώρες συγκριτικά με τους πιο μεγάλους σε ηλικία φοιτητές ([F(12.89, 2294.69) = 8.83, p < 0.001]). Η χρήση των Κοινωνικών Δικτύων ήταν αυξημένη σε όσους κάπνιζαν, έπιναν αλκοόλ και χρησιμοποιούσαν ουσίες-κάνναβη. Επικράτηση Εκφοβισμού ως θύμα με δημογραφικά και χαρακτηριστικά συμπεριφοράς. 19% των συμμετεχόντων ανέφεραν ότι έχουν υποστεί εκφοβισμό κατά την προηγούμενη περίοδο με μέση ηλικία τα 15 έτη. Η εμφάνιση του Διαδικτυακού Εκφοβισμού διέφερε σημαντικά ανάλογα με την τάξη φοίτησης ([F(4.49, 799.05) = 3.27, p < 0.01]). Μεγαλύτερη αναλογία υπήρξε στις τάξεις 8η και 9η από ότι στους φοιτούντες στην 12η τάξη. Η μέση εκπαίδευση των γονιών όσων είχαν αναφέρει εκφοβισμό δεν διέφερε σημαντικά από όσους δεν είχαν αναφέρει. Οι αναφέροντες εκφοβισμό ήταν κυρίως κορίτσια χαμηλής κοινωνικοοικονομικής κατάστασης, ήταν περισσότερο πιθανό να καπνίζουν και να κάνουν χρήση ουσιών – κάνναβης. Εκφοβισμό επίσης ανέφερε ένα ποσοστό περίπου 5% μη χρήστες Κοινωνικών Δικτύων. Περισσότερα περιστατικά Διαδικτυακού Εκφοβισμού αναφέρθηκαν στους συμμετέχοντες με περισσότερο χρόνο στα κοινωνικά Δίκτυα (Sampasa-Kanyinga & Hamilton, 2015).

#### 3.4.1.1.4 Κοινωνικά Δίκτυα και λοιποί Κίνδυνοι Γενικά

**Οι Mitchell & Ybarra το 2009** στις ΗΠΑ, εξετάζει του κινδύνους και τα οφέλη από την χρήση των Κοινωνικών Δικτύων στους εφήβους. Αιτίες που τα κοινωνικά Δίκτυα είναι πολύ δημοφιλή τους νέους: Τους επιτρέπουν την εξερεύνηση της ταυτότητας τους, την δημιουργία νέων φίλων, να ακουστεί η φωνή τους και η άποψή τους. Κίνδυνοι που μπορούν να προκύψουν: Τα κοινωνικά δίκτυα είναι χώροι που η εξωτερίκευση των νέων μπορεί να οδηγήσει στον κίνδυνο της Θυματοποίησης είτε με την μορφή της παρενόχλησης είτε με την σεξουαλική προσβολή, απομόνωση. Η αναζήτηση ιατρικής

πληροφόρησης και συμβουλής αποτελεί ακόμη ένα κίνδυνο των Κοινωνικών Δικτύων, είτε λανθασμένης είτε ανακριβούς. Οφέλη που προκύπτουν από την χρήση των Κοινωνικών Δικτύων: Συνεχή πρόσβαση στην πληροφορία σε ανώνυμα forum (θέματα υγείας – (1 στους 4 νέους ηλικίας 15-24 ετών έχουν αναζητήσει βοήθεια στο Διαδίκτυο για την κατάθλιψη με αντίστοιχα να είναι τα ποσοστά στους εφήβους που αναζήτησαν πληροφορίες για την βία, ναρκωτικά και αλκοόλ). Ευρήματα στα κοινωνικά Δίκτυα έδειξαν ότι στοχευμένες ενέργειες σε κοινωνικά Δίκτυα μπορούν να επηρεάσουν θετικά την νεανική συμπεριφορά. Έρευνες έδειξαν ότι με ένα σύντομο email σε ένα Κοινωνικό Δίκτυο είναι δυνατό και μπορεί να μειώσει τις σεξουαλικές αναφορές. Πιο συγκεκριμένα στην ομάδα στόχευσης από ένα ποσοστό 13,7% που εμφάνιζαν σεξουαλικές αναφορές στο προφίλ τους μειώθηκε στο 0%, συγκρινόμενο με το 5,3% της ομάδας ελέγχου. Τα αντίστοιχα ποσοστά για την μείωση ουσιών μεταξύ των ομάδων ελέγχου και παρέμβασης δεν εμφάνισαν ουσιώδεις διαφορές από τίς αρχικές (22% και 26% αντίστοιχα).Τα κοινωνικά δίκτυα προσφέρουν οφέλη αλλά και κινδύνους στους νέους. Έτσι είναι τα ίδια τα κοινωνικά δίκτυα μέσω των οποίων τόσο οι γονείς όσο και οι παιδίατροι ή ιατροί που μπορούν να απευθυνθούν σε αυτούς ώστε να μειωθούν οι κίνδυνοι (Mitchell & Ybarra, 2009).

**Οι Livingstone & Brake το 2010,** στο Ηνωμένο Βασίλειο, Αναζήτηση Συνεπειών και Κινδύνων στην διαδικασία της Κοινωνικής Δικτύωσης σε παιδιά και νέους. Ανασκόπηση ερευνών Θετικές Συνέπειες Κοινωνικής Δικτύωσης 1. Α. Έρευνα σε νέους 13-18 ετών για αναζήτηση κύκλου φίλων. 1. Β. Έρευνα στις Η.Π.Α. MySpace σε νέους ηλικίας 16+2. Κίνδυνοι 2. Α. έρευνα Η.Β: νέοι 9-19 ετών2. Β. έρευνα μεταξύ 2423 εχόντων λογαριασμό στο MySpace ηλικίας κάτω των 18 ετών 3. Α. Έρευνα στις Η.Π.Α 3. Β. Έρευνα στην Ιρλανδία σε παιδιά 10-12 ετών. 3. Γ. Έρευνα για την διαδικτυακή Παρενόχληση Αποτελέσματα Ερευνών 1. Α Συνέπειες κοινωνικής Δικτύωσης: Α. Ο μεγάλος κύκλος φίλων α. ενισχύει τους τα δίκτυα ασθενών δεσμών β. βοηθάει την υπερπήδηση την δυσκολίας της πρόσωπο με πρόσωπο επικοινωνίας αυτής της ηλικίας γ. Η επικοινωνία μέσω των κοινωνικών δικτύων γίνεται πιο ευέλικτη με δυνατότητα διαμοιρασμού απόψεων συμβουλών και υποστήριξης πιο εύκολη μεταξύ των παιδιών. Επιπλέον η κοινωνική Δικτύωση επιτρέπει στους νέους την αύξηση τόσο των τεχνικών όσο και των κοινωνικών δεξιοτήτων τους. 2. Α. Αποτελέσματα ερευνών για Κινδύνους. Α.57% παρακολούθησε πορνογραφικό υλικό, 31% έχει παρακολουθήσει βίαιο και ρατσιστικό περιεχόμενο. Επιπλέον ένα 31% έλαβε διαδικτυακά σχόλια σεξουαλικού περιεχομένου και ένα 28% έλαβε ανεπιθύμητο σεξουαλικού περιεχομένου υλικό. 1/3 δέχθηκε

διαδικτυακά εκφοβιστικά σχόλια και ένα 8% συναντήθηκε για πρώτη φορά με άγνωστο που γνώρισε διαδικτυακά. 2 Β. 57% ανάρτησε προσωπικές φωτογραφίες Διαδικτυακά, 16% ανάρτησε φωτογραφίες φίλων με μαγιό ή εσώρουχα, 16% ανέφερε πραγματικό όνομα, 18% συζήτησε θέματα κατανάλωσης αλκοόλ, 8% συζήτησε θέματα καπνίσματος, 2% συζήτησε θέματα μαριχουάνας 3. Α. Νέα αγόρια είναι ευκολότερο να αναρτήσουν ψευδείς πληροφορίες ενώ λίγο μεγαλύτεροι και κυρίως κορίτσια μπορούν να αποκαλύψουν περισσότερες και πιο λεπτομερείς προσωπικές πληροφορίες 3. Β. 49% παρείχε πρόσβαση σε πληροφορίες σχετικές με το σχολείο ένα 12% παρείχε το κινητό τους τηλέφωνο και ένα 8% την διεύθυνση κατοικίας. Υπάρχουν ενδείξεις ότι η αποκάλυψη προσωπικών πληροφοριών διευκολύνει κινδύνους στην επικοινωνία. 3. Γ. στην έρευνα αυτή του 2006 ένα 69% των μαθητών ανέφεραν ότι είχαν δεχθεί παρενόχληση κατά το προηγούμενο έτος, ενώ μόνο το 7% εξ αυτών δήλωσαν ότι είχαν δεχθεί μηνύματα ή ηλεκτρονικού ταχυδρομείου, παρενόχλησης μηνύματα. Μεγαλύτερα και περισσότερα φαινόμενα εκφοβισμού παρατηρούνται κυρίως στις ΗΠΑ. Αποδεδειγμένα πλεονεκτήματα από τη κοινωνική Δικτύωση σύμφωνα με το άρθρο αποτελούν η επικοινωνία και οι σχέσεις. Λιγότερο αποδεδειγμένα πλεονεκτήματα αποτελούν η εκμάθηση και η συμμετοχή -απόδειξη και για κάποιους κινδύνους. Ωστόσο χρειάζεται εντατικοποίηση στους δημιουργούντες πολιτική για τα παιδιά για να ενισχύσουν τα πλεονεκτήματα εις βάρος των κινδύνων (Livingstone & Brake, 2010).

**Οι Weir, Toolan, & Smeed, το 2011** στη Γλασκόβη Ιρλανδία, εξετάζουν εάν οι κίνδυνοι και απειλές που εμφανίζονται στα Κοινωνικά Δίκτυα, είναι νέα φαινόμενα. Αναφορά σε Κοινωνικά Δίκτυα και το Facebook, τα οποία αποκαλεί «walled gardens", καθώς παρέχουν την δυνατότητα στους χρήστες τους να τα προσαρμόζουν στις ανάγκες του κάθε ενός, τόσο του ψηφιακού κόσμου όσο και του κοινωνικού. Κίνδυνοι που αφορούν και προέρχονται από τις ρυθμίσεις του απορρήτου, κινδύνους που μπορεί να προέρθουν από τις εφαρμογές που χρησιμοποιεί το Facebook και οι χρήστες του ( π.χ. "likejacking" για να περιγράψει το κακόβουλο λογισμικό του να συνδεθείς σε ανύπαρκτη σύνδεση που αυτοχαρακτηρίζεται ως μια ιστοσελίδα που αρέσει στον ενεργό χρήση και που μέσω των φίλων του αποκτά πρόσβαση και σε άλλους). Αναφέρεται σε κινδύνους που μπορούν να πολλαπλασιαστούν μέσω της χρήσης των κοινωνικών δικτύων που υποβοηθούνται από την ύπαρξη των Κοινωνικών Δικτύων, π.χ. κοινοί κλέφτες που εξαιτίας των αναρτήσεων των χρηστών στο Facebook, γνωρίζουν ότι οι χρήστες λείπουν και με αυτό τον τρόπο διευκολύνεται η εγκληματική τους δραστηριότητα ή αντίστοιχα την χρησιμοποίηση των μέσων Κοινωνικής Δικτύωσης από τα όργανα της Τάξης, ως παγίδα για τους κοινούς

εγκληματίες. Αναφέρεται και σε κινδύνους, όπως identity theft. Διαχωρίζει τους κινδύνους σε «απειλές για το κοινό» και «απειλές κατά των χρηστών των κοινωνικών δικτύων». Το άρθρο συμπερασματικά κλείνει με το ότι όπως όλα τα μέσα της επικοινωνίας προσφέρουν ένα μηχανισμό που προβάλλει και το καλό αλλά και το προβληματικό. Οι απάτες ο εκφοβισμός η κλοπή δεδομένων ακόμη και η υποκίνηση διαδηλώσεων και εξεγέρσεων είναι φαινόμενα που ακολουθούν τα μέσα επικοινωνίας, δεν είναι κάτι νέο (Weir et al., 2011)

**Οι Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, & Yan Chen το 2011,** στις ΗΠΑ, εξετάζουν τους κινδύνους της ασφάλειας στα Κοινωνικά Δίκτυα τις οποίες κατηγοριοποιούν σε 4 κατηγορίες – Παραβιάσεις προσωπικής ζωής (privacy breaches), ιογενή μάρκετινγκ (viral marketing), Δομικές/ Διαρθρωτικές διαδικτυακές επιθέσεις (network structural attacks), Επιθέσεις κακόβουλου λογισμικού (malware attacks) Εστιάζουν σε κινδύνους αναφορικά με την παραβίαση της προσωπικής ζωής, τους αναπτύσσουν και επεξηγούν και επίσης εστιάζουν & όπου υπάρχουν, στους αμυντικούς μηχανισμούς. Ιογενή Μάρκετινγκ (Viral Marketing) Ανεπιθύμητα Μηνύματα σε Κοινωνικά Δίκτυα (Spam messages) (Hongyu Gao et al., 2011).

**Οι Vandoninck, d'Haenens, De Cock, & Donoso το 2012**, στο Βέλγιο ερευνά τον τρόπο με τον οποίο οι έφηβοι ηλικίας 14-19 ετών χρησιμοποιούν τα Κοινωνικά Δίκτυα αλλά και άλλες Διαδικτυακές εφαρμογές επικοινωνίας, και σε ποιον βαθμό είναι εκτεθειμένοι σε κινδύνους από τις διαδικτυακές επαφές τους που σχετίζονται με αυτές τις εφαρμογές αλλά και πως αντιμετωπίζουν/διαχειρίζονται αυτούς τους κινδύνους. Η έρευνα έγινε την περίοδο Φεβρουαρίου- Απριλίου 2009. Εννέα σχολεία συμμετείχαν στην έρευνα και 815 Φλαμανδοί μαθητές ηλικίας 14-19 ετών συμπλήρωσαν γραπτό ερωτηματολόγιο. Αποτελέσματα: Χρήση Κοινωνικών Δικτύων για διαμοιρασμό και συλλογή πληροφοριών. 38,3% Συχνά, 44% μερικές φορές, 17.7% ποτέ δεν εμπλέκεται σε τέτοιου τύπου χρήση των Κοινωνικών Δικτύων. Χρήση Κοινωνικών Δικτύων για δραστηριότητες Διασκέδασης: 16,1% Συχνά, 25% (1/4) του δείγματος μερικές φορές, 58,9% Δεν ενδιαφέρεται για τον συγκεκριμένο σκοπό χρήσης του Κοινωνικού Δικτύου. Άνθρωποι που γνωρίζουν έχουν λογαριασμό σε κοινωνικά Δίκτυα: 83,5% νέων ατόμων ανέφερε ως κίνητρο εγγραφής του σε κοινωνικό Δίκτυο, το γεγονός ότι άτομα που γνώριζαν διατηρούσαν λογαριασμό σε Κοινωνικά Δίκτυα. 62,5% των συμμετεχόντων στην έρευνα θεωρεί ως κίνητρο την γνωριμία με περισσότερα άτομα. Το κίνητρο είναι το ίδιο

σημαντικό για αγόρια και κορίτσια. Ως μοτίβο την προσωπική ανάπτυξη, μόνο ένα ποσοστό 12,9% συμπλήρωσε στο «έντονα συμφωνώ», κυρίως αγόρια μαθητές, τεχνικής και επαγγελματικής εκπαίδευσης. Παιδιά γονέων χαμηλότερης μορφωτικής εκπαίδευσης εγγράφονται σε κοινωνικά Δίκτυα με σκοπό την ατομική προώθηση και την εξεύρεση ραντεβού. Διαδικτυακοί Κίνδυνοι, Διαδικτυακή συνομιλία και email επαφές: 47.9% έχουν άγνωστους στις επαφές τους για διαδικτυακή συνομιλία με το αντίστοιχο ποσοστό τις επαφές αλληλογραφίας email να ανέρχεται στο 35.4%. Και επίσης το 1/3 έχει τακτική επικοινωνία με άτομα που δεν έχουν συναντήσει ποτέ. Κινδύνους επαφών όπως Σεξουαλική Παρενόχληση, όπως και ή συνάντηση με ξένους, είναι φαινόμενα επαναλαμβανόμενα που συμβαίνουν. 1/3 έχουν ήδη έρθει αντιμέτωποι με σεξουαλικής φύσεως θέματα σε συνομιλία και στο 11.7% των συμμετεχόντων, έρχονται σε τέτοιου τύπου θέματα και αυτό συμβαίνει πάνω από μία φορά το μήνα. Με τους εφήβους χαμηλής κοινωνικό οικονομικής κατάστασης, να λαμβάνουν τα περισσότερα σεξουαλικά μηνύματα στις συνομιλίες. Επαφή με Διαδικτυακή επαφή: 30% ηλικίας 18-19 ετών είχαν ήδη έρθει σε επαφή, αγόρια και παιδιά με χαμηλότερη ακαδημαϊκή επίδοση ($\chi 2 = 20.29$; $df = 4$; $p < .001$). Αρνητική επίδραση εξ αίτιας αυτού, θεώρησε μόνο ένα 8%. Η χρήση εργαλείων επικοινωνίας ( κυρίως μέσω άμεσου μηνύματος και μεταξύ συμμαθητών) για εκφοβισμό είναι γνωστά στις ηλικίες μεταξύ 15-19 ετών. 22.5% έχουν παραδεχθεί εκφοβισμό, 15% έχει αποτελέσει θύμα Δ. Ε. και σχεδόν τους μισούς να έχουν υπάρξει μάρτυρες Δ.Ε.. Ο Δ.Ε., είναι ένα φαινόμενο πιο κοινό στα αγόρια και σε εκείνους που προέρχονται από γονείς χαμηλής εκπαίδευσης. Τα συναισθήματα όσων έχουν εμπλακεί σε φαινόμενα Δ.Ε. ως θύτες/ δράστες: 20% αισθάνονται καλά, 27% αισθάνονται άσχημα και το 1/3 δεν έχουν ούτε καλά αλλά ούτε και κακά συναισθήματα. Οι μάρτυρες δεν έχουν ούτε καλά ούτε κακά συναισθήματα. Τα θύματα, αντίστοιχα, αισθάνονται άσχημα ενώ ένα ποσοστό του 30% των θυμάτων φαίνεται να είναι αδιάφορο, ως προς το ότι έχει διατελέσει, θύμα Δ.Ε. Η κακή γονική σχέση και η πρακτική του διαμοιρασμού προσωπικών πληροφοριών με αγνώστους φαίνεται να ενισχύεται εξαιτίας αυτής της κατάστασης. Το αντίστοιχο συμβαίνει και στην συνάντηση με ξένο από συνομιλία και όταν το Κοινωνικό Δίκτυο θεωρείται ως έξυπνη ευκαιρία. Η ισχυρή αυτοπεποίθηση επίσης οδηγεί στον διαμοιρασμό του κοινωνικού προφίλ του χρήστη. Οι μέτριου επιπέδου αυτοπεποίθησης συμμετέχοντες εμπλέκονται λιγότερα σε φαινόμενα Δ.Ε. (Vandoninck et al., 2012)

**Ephraim, το 2013,** στην Αφρική, Το άρθρο, εξετάζει την διάδοση και επέκταση των Μέσων Κοινωνικής Δικτύωσης στην Ήπειρο Αφρική/ χώρα και προτείνει μια μεθόδευση, προσέγγιση πολιτισμική σε μια προσπάθεια περιορισμού των φαινομένων διαδικτυακών εγκλημάτων και ταυτόχρονα ενίσχυσης μιας υπεύθυνης χρήσης των Μέσων κοινωνικής Δικτύωσης μεταξύ των νέων της Αφρικανικής Ηπείρου. Η πολιτισμική προσέγγιση συμπεριλαμβάνει ηθικά καθοδηγούμενες πρακτικές δρομολογούμενες α. από την οικογένεια, β. Το εκπαιδευτικό σύστημα, και τις κυβερνητικές υπηρεσίες. γ. Τους θρησκευτικούς οργανισμούς Δ. Τα Μέσα Μαζικής ενημέρωσης (Ephraim, 2013).

**Οι Hajli & Lin, το 2016** στις Η.Π.Α, εξετάζουν την ασφάλεια των κοινωνικών Μέσων Δικτύωσης (SNS), εξετάζοντας την επιρροή του αντιληπτού ελέγχου των πληροφοριών από τους χρήστες, και τις συμπεριφορές τους για την ανταλλαγή πληροφοριών. Έγινε έρευνα σε μεγάλο πανεπιστήμιο στις Βορειοδυτικές Ηνωμένες Πολιτείες. 500 συμμετέχοντες φοιτητές, έγκυρες 405. Αποτελέσματα: Η έρευνα απέδειξε ότι ο αντιληπτός έλεγχος μετριάζει τους αντιληπτούς κινδύνους της προσωπικής ζωής των χρηστών των Κοινωνικών Δικτύων (SNS), οι οποίοι με τη σειρά τους επηρεάζουν τις συμπεριφορές τους όσον αφορά την ανταλλαγή πληροφοριών. Η ανάλυση επίσης των δεδομένων έδειξε ότι στις γυναίκες ο αντιληπτός έλεγχος των πληροφοριών, επιδρά θετικότερα στην συμπεριφορά τους στον διαμοιρασμό πληροφοριών σε σχέση με την αντίστοιχη συμπεριφορά των ανδρών χρηστών Κοινωνικών Δικτύων (Hajli & Lin, 2016).

**Οι Montes-Vozmediano, García-Jiménez, & Menor-Sendra, 2018** στην Ισπανία, διερευνούν το οπτικοακουστικό υλικό που αναρτούν έφηβοι ή και άλλοι πράκτορες στο YouTube και τους κινδύνους που εγκυμονούν αυτά (και από την δημιουργία αλλά και από την κατανάλωσή τους) Αποτελέσματα: Συνθήκες Ευπάθειας Σε ένα ποσοστό 68,3%, των αναλυθέντων βίντεο, η ταυτότητα του εφήβου δημιουργού, ήταν προστατευμένη. Αποτελέσματα: Καθορισμός της ταυτότητας του Δημιουργού του βίντεο 25,3% άγνωστος, 20,3 % βίντεο δημιουργημένα από τα μέσα ενημέρωσης, 15,1% βίντεο δημιουργημένα από εφήβους, 8,8% βίντεο δημιουργημένα από δημόσια ιδρύματα προς ευαισθητοποίηση της κοινής γνώμης για διάφορα θέματα και τέλος 10,3% ενήλικες δημιουργοί ή επαγγελματίες, ανέβασαν λιγότερα βίντεο σε σχέση με τους εφήβους. Συνθήκες Ευπάθειας: Σε ένα ποσοστό 68,3%, των αναλυθέντων βίντεο, η ταυτότητα του εφήβου δημιουργού ήταν προστατευμένη. Η εμφάνιση παιδιών τόσο στα ιδιωτικά όσο και τα δημόσια βίντεο υπάρχει σε ένα μεγάλο ποσοστό της τάξης του 60,7 % στα ιδιωτικά

και 56,3% στα δημόσια, που η ταυτότητα των παιδιών, δεν προστατεύεται. Το ακριβώς αντίθετο συμβαίνει με τα βίντεο των μέσων ενημέρωσης με ένα 28% να σέβεται την ταυτότητα των παιδιών ( είτε με σκιά είτε με στρέβλωση της εικόνας του προσώπου). Το περιεχόμενο όμως των αναρτήσεων σε ένα ποσοστό 35,4% είναι ακατάλληλο για παιδιά. Ο χώρος υλοποίησης του βίντεο: στους Youtubers: (80%) βίντεο εφήβων σε ιδιωτικές τοποθεσίες 31,7%, ενώ σε δημόσιους χώρους 16,7%. Των Μέσων ενημέρωσης τα βίντεο στο μεγαλύτερο ποσοστό γίνονται σε δημόσιους χώρους. Δημιουργία και ευπάθεια: 26,67% των βίντεο των εφήβων αντιμετωπίζει με κάποιο τρόπο το θέμα του εκφοβισμού bullying, 21,67% ασχολείται με ναρκωτικά drugs, 13,33% με σεξουαλικού περιεχομένου θέματα. Σε αναρτήσεις των Youtubers το περιεχόμενο σεξουαλικής φύσης είναι 42,86%, 11,43% αντίστοιχα θέματα ναρκωτικών (drugs) και εγκυμοσύνης. Στων Μέσων Ενημέρωσης τα ποσοστά αυτά είναι 37,8% σεξουαλικού περιεχομένου, 23,17% θέματα αναφορικά με ερωτήσεις για τον εκφοβισμό και 18,29% για την εγκυμοσύνη (Montes-Vozmediano et al., 2018).

### 3.4.2 Ελλάδα Μελέτες έρευνες

#### 3.4.2.1 Διαδίκτυο Γενικά

##### 3.4.2.1.1 Εθισμός & Προβληματική Χρήση διαδικτύου.

Οι Tsitsika et al. 2009, ερευνούν την χρήση και κατάχρηση του Διαδικτύου (Internet), στους εφήβους στην Ελλάδα. Έγινε έρευνα. Συλλέχθηκαν δεδομένα σε περίοδο ενός έτους από 01/01/2007-01/01/2008. Τυχαίο δείγμα 953 ατόμων (n=953) σε δημόσια Γυμνάσια και Λύκεια στην Αθήνα. Συμμετέχοντες: Αγόρια 438, κορίτσια 499 με μέση ηλικία 15,21 έτη. 16 συμμετέχοντες δεν δήλωσαν φύλο και εξαιρέθηκαν της μελέτης. Αποτελέσματα Χαμηλή Χρήση Διαδικτύου (1-3ώρες εβδομαδιαίως). Στατιστικά δεν επιβεβαιώνεται η χαμηλή χρήση του Διαδικτύου, με την ηλικία, το φύλο, ή τον δείκτη μάζας σώματος. Σχετίζεται όμως με το ιστορικό χρήσης του Διαδικτύου και φαίνεται να προκύπτει ότι επιτυγχάνεται είτε από την κατοικία του χρήστη είτε από internet café. Η χαμηλή χρήση διαδικτύου στις γυναίκες γίνεται κυρίως για χρήση του ηλεκτρονικού ταχυδρομείου σε ποσοστό 46,4% και στους άνδρες αναφορικά με το παιχνίδι (gaming) σε ποσοστό 53,5%. Αναφορικά με την κλίμακα της Young για την προβληματική χρήση προκύπτει ότι η χαμηλή Χρήση του Διαδικτύου δεν σχετίζεται με τον εθισμό και φαίνεται ότι σχετίζεται

στις γυναίκες με την οριακή χρήση (BIU – Borderline Internet use). Μεσαία Χρήση Διαδικτύου. (4-10 ώρες εβδομαδιαίως). Η Μεσαία Χρήση του Διαδικτύου στατιστικά είναι ισχυρά συνδεδεμένη και με το φύλο αλλά και με το ιστορικό χρήσης του Διαδικτύου. Η πρόσβαση γίνεται μέσα από την οικία του χρήστη ή internet café. Η επισκεψιμότητα αφορά κυρίως ηλεκτρονικό ταχυδρομείο και δωμάτια συζήτησης (chat rooms). Οι άρρενες χρήστες επίσης χρησιμοποιούν το διαδίκτυο για αγορά αγαθών ή και σεξουαλική εκπαίδευση. Οι γυναίκες σε αυτή την κατηγορία χρησιμοποιούν το Διαδίκτυο για λόγους υπηρεσιών. Οριακή χρήση Διαδικτύου (BIU – Borderline Internet Use) βρέθηκε να είναι ισχυρά συνδεδεμένα με την Μεσαία Χρήση Διαδικτύου και στα δύο φύλα και σε υψηλά επίπεδα στους άρρενες χρήστες. Σε αυτή την κατηγορία των χρηστών παρατηρήθηκε εθισμός (AIU- Addictive Internet Use) σε ποσοστό 44,5% (n=4) και οι άρρενες ήταν διπλάσιοι συγκριτικά με τις γυναίκες χρήστες Διαδικτύου. Υψηλή Χρήση Διαδικτύου (11-20 ώρες εβδομαδιαίως). Αντίστροφα ανάλογη είναι η υψηλή Χρήση του διαδικτύου τόσο με το νεαρό της ηλικίας του χρήστη και με το θηλυκό φύλο. Ισχυρά συνδεδεμένη επίσης είναι με το ιστορικό χρήσης. Η πρόσβαση σε αυτή την κατηγορία γίνεται είτε μέσω της οικίας του χρήστη είτε μέσω των Internet cafe, με τις γυναίκες χρήστες να χρησιμοποιούν περισσότερο τα internet cafe. Τόσο οι άνδρες όσο και οι γυναίκες χρήστες χρησιμοποιούν το Διαδίκτυο για λόγους κοινωνικοποίησης, και αγορών. Σε αυτή την κατηγορία χρήσης του Διαδικτύου οι άνδρες είναι περισσότερο πιθανό να υιοθετήσουν παιχνίδια Διαδικτυακά συγκριτικά με τους μη Χρήστες. Όσον αφορά της YIAS, η Οριακή χρήση Διαδικτύου (BIU) είναι συνδεδεμένη σε αυτή την κατηγορία Χρήσης του Διαδικτύου με τους άνδρες. Κανένα περιστατικό Εθισμού δεν παρατηρήθηκε σε αυτή την κατηγορία Χρήσης του Διαδικτύου. Υπερβολική Χρήση Διαδικτύου ( >20 ωρών εβδομαδιαίως) Αρνητική συσχέτιση τόσο με το φύλο όσο και με τον Δείκτη Μάζας Σώματος. Πρόσβαση μέσω Της οικίας του Χρήστη ή και μέσω Internet cafe. Οι άνδρες Χρήστες σε αυτή την κατηγορία χρησιμοποιούν το Διαδίκτυο σε ποσοστό 95,8% για παιχνίδια διαδικτυακά ενώ οι γυναίκες αντίστοιχα για την χρήση ηλεκτρονικού ταχυδρομείου σε ποσοστό 87,5%. Και τα δύο φύλα σε αυτή την κατηγορία χρησιμοποιούν το Διαδίκτυο για σεξουαλική διαπαιδαγώγηση και αγορές. Οι άνδρες επίσης χρησιμοποιούν το Διαδίκτυο σε Δωμάτια συζήτησης και Διαδικτυακά Παιχνίδια ενώ αντίστοιχα οι γυναίκες για υπηρεσίες σε σύγκριση με την ομάδα ελέγχου. Αναφορικά με της YIAS μια σημαντική συσχέτιση παρατηρήθηκε μεταξύ της υπερβολικής Χρήσης του Διαδικτύου και της Οριακής Χρήσης (BIU -Borderline Internet Use) και στα δύο φύλα. Σε ποσοστό 55,5% (n=5) Εθισμού (AIU Addictive Internet Use) παρατηρήθηκε σε αυτή

την κατηγορία Χρήσης. Σε ποσοστό επίσης 10,4% οι Εθισμένοι ( AIU) ήταν άνδρες. (Tsitsika et al., 2009)

**Οι Frangos et al, το 2011** εξετάζουν την ύπαρξη «Προβληματικής χρήσης του Διαδικτύου (PIU) » σε Έλληνες φοιτητές σε πανεπιστημιακά ιδρύματα της Αττικής αλλά και της Βόρειας Ελλάδος, καθώς και τους παράγοντες κινδύνου στους οποίους μπορεί να οφείλεται η «Προβληματική Χρήση του Διαδικτύου». Παράγοντες όπως το φύλο, η ηλικία, η οικογενειακή κατάσταση η ακαδημαϊκή επίδοση, η χρήση σε ώρες εβδομαδιαίως του Διαδικτύου και λοιπούς παράγοντες όπως η χρήση αλκοόλ, καφέ τσιγάρα, εξετάσθηκαν. Αποτελέσματα: Σε Δημογραφικούς παράγοντες όπως το φύλο, οικογενειακή κατάσταση, κ.λ.π βρέθηκε συσχετισμός με την «προβληματική Χρήση Διαδικτύου (PIU)» ($p<0.0001$). Προβληματική Χρήση Διαδικτύου Ποσοστό σε άνδρες= 42,01% έναντι 27,7% σε γυναίκες. Η χρήση δε του Διαδικτύου αυτών των χρηστών αφορούν επισκέψεις σε "forums" δωμάτια συνομιλιών (chatting rooms), ιστολόγια (blogs) MSN Παιχνίδια (games) περισσότερο από τους μη «Προβληματικούς Διαδικτυακούς Χρήστες» όπως επίσης είναι πιθανότερο να καταναλώνουν αλκοόλ, να καπνίζουν και να έχουν περισσότερες προσωπικές εξαρτήσεις και συνήθειες σε ποσοστό 3φορές μεγαλύτερο από τους μη Προβληματικούς Διαδικτυακούς χρήστες. «Προβληματική Χρήση Διαδικτύου» Σε 2293 συμμετέχοντες στην έρευνα το 34,7% ανήκαν στην κατηγορία της «Προβληματικής Χρήσης Διαδικτύου» ("Διαδικτυακά Εθισμένοι" (Internet Addiction IA) = 12% Σε κίνδυνο (at risk) = 22,7%) (Frangos et al., 2011).

**Οι Kormas, Critselis, Janikian, Kafetzis, & Tsitsika, το 2011** ερευνούν τους καθοριστικούς παράγοντες για την Προβληματική και Δυνητικά Προβληματική Χρήση του Διαδικτύου (PIU – Problematic Internet Use) μεταξύ των εφήβων. Δευτερευόντως αξιολογεί τα ψυχοκοινωνικά χαρακτηριστικά και τις συνέπειες αναφορικά με την Προβληματική Χρήση του Διαδικτύου στα συμμετέχοντα της μελέτης άτομα. Έγινε έρευνα. Περίοδος συλλογής στοιχείων 01/01/2007-01/01/2008- 2 διαδοχικά εξάμηνα. Τυχαίο δείγμα 937 ατόμων (n = 937) φοιτούντων σε 20 δημόσια σχολεία (9η & 10η τάξη) στην Αθήνα, Ελλάδα. Εξ αυτών 438 αγόρια ( 46,7%) & 499 κορίτσια (53,3%). Εξ αυτών 71 άτομα (7,6%) δεν συμπλήρωσαν όλα τα δεδομένα στο τεστ Εθισμού της Young (YIAT-Young's Internet Addiction Test) και εξαιρέθηκαν των στατιστικών αναλύσεων. Έτσι το ποσοστό των απαντήσεων ανήλθε σε 92,4% εκ των 866 συμμετεχόντων (n=866). Αποτελέσματα Συνολική Ακατάλληλη Δυσπροσάρμοστη/ Χρήση Διαδικτύου

(maladaptive internet use (MIU)) Μεταξύ των συμμετεχόντων 20,9% (N=181 άτομα) Έφηβοι με Ακατάλληλη Χρήση Διαδικτύου. Δυνητική Προβληματική Χρήση Διαδικτύου (Potential problematic internet use (PIU)) Μεταξύ των συμμετεχόντων 19,4% (N=168) Με τα αγόρια να είναι κατά 2,77 φορές πιθανότερο να είναι Δυνητικά Προβληματικοί Χρήστες Διαδικτύου. Π.Χ.Δ και Φ.Χ.Δ δεν φαίνεται να παρουσιάζουν διαφορές σε ηλικία. Φτωχή ακαδημαϊκή βαθμολογία επίσης παρουσιάζουν περισσότερο σε σχέση με τους Φ.Χ.Δ. Αντίστοιχα αποτελέσματα αναφορικά με τους τόπους πρόσβασης, καφέ και το σπίτι αλλά και επισκεψιμότητα σε ιστοσελίδες για συλλογή σεξουαλικής φύσης πληροφοριών 2.43 φορές περισσότερο από ότι οι συνομήλικοι Φ.Χ.Δ. Η επισκεψιμότητα επίσης για παιχνίδια ήταν 1,86 φορές μεγαλύτερη από ότι οι Φ.Χ.Δ. Επίσης οι συμμετέχοντες με πιθανή Προβληματική Χ.Δ. είναι έως 2 φορές μεγαλύτερη να παρουσιάζουν ψυχοκοινωνική δυσλειτουργία σε σχέση με τους ομότιμους τους Φ.Χ.Δ. Προβληματική Χρήση Διαδικτύου (Problematic internet use (PIU))Μεταξύ των συμμετεχόντων 1.5% (N=13)7 φορές περισσότερες πιθανότητες να είναι αγόρια σε σχέση με τους συνομήλικους τους συμμετέχοντες και επίσης έως και 8 φορές περισσότερο να αναφέρουν >12 μήνες χρήσης Διαδικτύου. Πρόσβαση στο Διαδίκτυο, μέσω καφέ και σπιτιού πιο συχνά από ότι οι συνομήλικοί τους Φ.Χ.Δ. ($p = 0.018$) Και επίσης ισχυρά συσχετισμένοι με την επισκεψιμότητα για την συλλογή στοιχείων σεξουαλικού περιεχομένου ή δωμάτια συνομιλίας. Πολύ σημαντικό επίσης να αναφερθεί ότι η πλειονότητα των ατόμων Προβληματικής Χρήσης Διαδικτύου χρησιμοποιούν το Διαδίκτυο για διαδραστικά Διαδικτυακά παιχνίδια, χαρακτηριστικό που δεν διαφέρει σημαντικά από τους Φ.Χ.Δ. συνομηλίκους τους. Καθοριστικοί παράγοντες για Δυνητικά Προβληματική Χρήση και Προβληματικής Χρήσης Διαδικτύου Η υλοποιηθείσα ανάλυση (πολυεθνής διοικητικής παλινδρόμησης/multinomial, logistic regression analysis) έδειξε ο χρήστης διαδικτύου, άρρεν που χρησιμοποιεί το Διαδίκτυο για ανάκτηση πληροφοριών σεξουαλικής φύσης, που εμπλέκεται σε διαδραστικά Διαδικτυακά παιχνίδια, δωματίων συζητήσεων συνδέεται ανεξάρτητα με την Δυνητικά Προβληματική και την Προβληματική Χρήση Διαδικτύου (Kormas et al., 2011).

#### 3.4.2.1.2 Κίνδυνοι Εκφοβισμός Παρενόχληση και Κίνδυνοι Γενικά

**Οι Floros, Siomos, Fisoun, Dafouli, & Geroukalis το 2013,** ερεύνησαν το «επιδημιολογικό» φαινόμενο του Διαδικτυακού εκφοβισμού σε Ελληνικό περιβάλλον, τα συνέκριναν με προηγούμενα σχετικά δεδομένα, και καθόρισαν τους παραγόντες που επιδρούν στο φαινόμενο και τέλος πρότειναν μέτρα για τη καταπολέμηση του

φαινομένου. Έγινε έρευνα, μέρος ενός μεγαλύτερου ερευνητικού προγράμματος «Ιπποκράτης 2010» του οποίου εστίαση αποτελεί ο «online και offline εκφοβισμός» και οι συμπεριφορά των νέων στο νησί της Κω. Το δείγμα της έρευνας αποτελούν 2017 έφηβοι μαθητές, ηλικίας μεταξύ 12 – 19 ετών, και συμμετείχαν όλα τα 13 Δημόσια σχολεία της Κω – 7 Γυμνάσια & 6 Λύκεια- 1217 συμμετέχοντες. Στο ερώτημα για εάν έχουν υποστεί Διαδικτυακό Εκφοβισμό απάντησαν 1957 συμμετέχοντες (97%) και αντίστοιχα στο εάν έχει διαπράξει κανείς Διαδικτυακό Εκφοβισμό 1959 συμμετέχοντες. Τα κορίτσια αποτέλεσαν μεγαλύτερο στόχο Διαδικτυακού Εκφοβισμού - 341 κορίτσια υπήρξαν θύματα Διαδικτυακού Εκφοβισμού και ποσοστό 35,9% υπολογισθέν πάνω σε όλα τα κορίτσια. Αντίστοιχα στα αγόρια 212 αγόρια υπήρξαν θύματα Διαδικτυακού Εκφοβισμού και ποσοστό 21,2% αντίστοιχα υπολογισθέν πάνω σε όλα τα αγόρια. Αντίθετα τα ποσοστά στο εάν έχουν διατελέσει Διαδικτυακό Εκφοβισμό το ποσοστό στα αγόρια ήταν μεγαλύτερο ήτοι 204 αγόρια και ποσοστό 20,4% έναντι 80 κοριτσιών και ποσοστό 8,4%. Ηλικιακά τώρα οι έφηβοι που δέχθηκαν Διαδικτυακό Εκφοβισμό ήταν μεγαλύτεροι από εκείνους που δεν είχαν αντίστοιχη εμπειρία (μέση Ηλικία = 15,46 χρονών έναντι 14,94 χρόνων). Αντίστοιχα μεγαλύτεροι σε ηλικία ήταν και όσοι είχαν εκφοβίσει άλλα άτομα σε σχέση με όσους δεν είχαν (μέση Ηλικία = 15,26 χρονών έναντι 15,04 χρόνων). Επίσης οι ασκούντες Διαδικτυακό Εκφοβισμό ανήκαν σε χαμηλότερου οικονομικού εισοδήματος οικογένειες και αντίστοιχα ακόμη και προσωπικού επιδόματος/ εισοδήματος και αντίστοιχα η πιθανότητα να τελειώσουν το σχολείο ήταν μικρή. Συγκρίσεις για την ασφάλεια μεταξύ θυμάτων και μη και μεταξύ δραστών Διαδικτυακού Εκφοβισμού και μη έδειξε σημαντική διαφορά αναφορικά με τα μέτρα γονικής ασφάλειας. Η γονική φροντίδα τόσο η μητρική όσο και η πατρική συσχετίζεται με χαμηλότερα φαινόμενα τόσο εκφοβισμού όσο και εκφοβιστών/δραστών (Floros et al., 2013).

**Οι Antoniadou & Kokkinos, 2015** υλοποιούν μια ανασκόπηση της υπάρχουσας έρευνας (που έχει δημοσιευθεί σε επιστημονικά περιοδικά, ή που έχουν υλοποιηθεί στο πλαίσιο υλοποιημένων μεταπτυχιακών σπουδών) αναφορικά με τον Διαδικτυακό Εκφοβισμό σε Έλληνες νέους. Συμπληρωματικά στόχος της παρούσας έρευνας είναι η παρουσίαση Ελληνικών Φορέων και οργανισμών που σκοπό έχουν την ασφαλή χρήση των τεχνολογιών Πληροφορικής και Επικοινωνιών. Τέλος η παρουσίαση ασφαλών αποτελεσμάτων αναφορικά με τα υπάρχοντα περιστατικά Διαδικτυακού Εκφοβισμού στους Έλληνες Νέους. 1η έρευνα το 2005, Αποτελέσματα: 54% των συμμετεχόντων

ανέφεραν ότι είχαν υπάρξει θύματα 2η έρευνα το 2008 Αποτελέσματα: Αυτό-αναφερόμενος Διαδικτυακός Εκφοβισμός. Το 20,5% ανάφεραν ότι έχουν υποστεί Δ.Ε. και το ποσοστό Δ.Ε στο 15,2%. 3η έρευνα το 2008 η Επιτροπή Κοινωνικής Πολιτικής του Αριστοτελείου Πανεπιστημίου: Αποτελέσματα: Θύματα Δ.Ε ήταν 6%. Μεγαλύτερο ποσοστό θυμάτων Γυναίκες ενώ δράστες κυρίως Άνδρες. Μέσα παρενόχλησης κυρίως Δωμάτια συζητήσεων (chat rooms), Ιστότοποι Κοινωνικών Δικτύων (social Network Sites) & υπηρεσίες ανταλλαγής άμεσων μηνυμάτων. 4η το 2007, διεξαχθείσα έρευνα, από την Εφηβική Μονάδα Υγείας του Πανεπιστημίου Αθηνών Αποτελέσματα: 4,2% δήλωσαν ότι έχουν εκφοβισθεί και ότι έλαβαν απειλητικά και προσβλητικά μηνύματα. 5η. έρευνα διεξαχθείσα από το ίδιο τμήμα σε έφηβους στην Αθήνα το 2008, με σκοπό την χρήση του Διαδικτύου και σχετικές καταχρηστικές συμπεριφορές σχετικές με το ψυχολογικό προφίλ των συμμετεχόντων Αποτελέσματα: 315 συμμετέχοντες μαθητές σε Γυμνάσια. Το 5,8% ήταν θύματα από ότι αναφέρθηκε ως Διαδικτυακός Εκφοβισμός στην έρευνα. 6ο: Σχετικά στοιχεία αντλούνται επίσης από έρευνες που ο Διαδικτυακός Εκφοβισμός, δεν αποτελεί πρωταρχικό στόχο της σχετικής έρευνας (Antoniadou & Kokkinos, 2015).

**Οι Antoniadou, Kokkinos, & Markos, 2016,** εξετάζουν τα πιθανά κοινά σημεία, χαρακτηριστικά των συμμετεχόντων, στα δύο είδη εκφοβισμού - παραδοσιακού εκφοβισμού (bullying) και Διαδικτυακού εκφοβισμού (Cyber Bullying), μεταξύ 146 Ελλήνων Εφήβων μαθητών Γυμνασίου. Επίσης μελετούν εκείνα τα χαρακτηριστικά που μπορεί να χαρακτηρισθούν ως επικρατέστερα, σε όσους συμμετέχουν σε Δ.Ε. (Cyber Bullying). Αποτελέσματα: Οι μαθητές διαχωρίσθηκαν σε ομάδες ανάλογα με τον ρόλο που τους ανατέθηκε σε Διαδικτυακό ή Παραδοσιακό Εκφοβισμό. Μια δεύτερη ταξινόμηση ομαδοποίησε τους μαθητές σε ρόλους παραδοσιακός/ Διαδικτυακός εκφοβισμός/ θυματοποίησης, για να καθορισθούν εκείνοι οι μαθητές που συμμετείχαν με τον ίδιο ρόλο (του θύματος του δράστη ή) και στα δύο φαινόμενα , με τον αντίθετο ρόλο θύμα σε Δ.Ε και δράστης σε Παραδοσιακό εκφοβισμό και αντίστροφα σε μόνο ένα εκ των δύο φαινομένων και τέλος αυτοί που δεν συμμετείχαν σε κανένα φαινόμενο. Τα αποτελέσματα έδειξαν ότι 36 μαθητές (24,7% συμμετείχαν και στα δύο φαινόμενα με τον ίδιο ρόλο ( 2 μαθητές ως θύματα, 4 ως δράστες και 7 ως δράστες /θύματα), 22 μαθητές (15,1%), συμμετείχαν και στα δύο φαινόμενα με τον αντίθετο ρόλο και 75 μαθητές (51,4%), παρέμειναν αμέτοχοι. Προσωπικά χαρακτηριστικά: Οι δράστες τόσο του Δ.Ε. (Διαδικτυακού Εκφοβισμού) όσο και του Π.Ε. (Παραδοσιακού Εκφοβισμού), είχαν υψηλότερες βαθμολογίες σε σχέση με όσους παρέμειναν αμέτοχοι. Τόσο οι δράστες όσο

και τα θύματα στον Π.Ε. είχαν υψηλότερες βαθμολογίες στην αναζήτηση εμπειρίας και της Διαδικτυακής έλλειψης συγκράτησης/ Διαδικτυακών αναστολών σε σχέση με τους αμέτοχους. Αναφορικά με τις κοινωνικές δεξιότητες οι δράστες/θύματα είχαν υψηλότερες βαθμολογίες από τους αμέτοχους στην ισχυρογνωμοσύνη μόνο στην περίπτωση του Π.Ε/ Θυματοποίησης. Οι δράστες στον Δ.Ε. ανέφεραν περισσότερες διαφορετικές Διαδικτυακές δραστηριότητες από ότι οι αμέτοχοι. Οι μαθητές που συμμετείχαν ταυτόχρονα και στα δύο φαινόμενα και στους δύο ρόλους (είτε θύτης είτε θύμα) χρησιμοποιούσαν το Διαδίκτυο πιο συχνά, επέδειξαν υψηλότερες βαθμολογίες στον ισχυρισμό/ισχυρογνωμοσύνη. Αντίθετα οι αμέτοχοι επέδειξαν μικρότερη διαδικτυακή έλλειψη αυτοσυγκράτησης, διαδικτυακές δραστηριότητες και ψυχοπαθητικά χαρακτηριστικά .Η συμμετοχή σε όλα τα φαινόμενα Δ.Ε/ Θύτης /Θύμα, Π.Ε. Θύτης /Θύμα είναι θετικά συσχετισμένο με την έλλειψη αυτοσυγκράτησης στο Διαδίκτυο και ψυχοπαθητικά χαρακτηριστικά. Θετικά συσχετισμένα επίσης είναι και Δ.Ε. και ο Π.Ε. με διαδικτυακές δραστηριότητες, επιρρεπής στην πλήξη, (βαρεμάρα) και την ισχυρογνωμοσύνη. Ο Π.Ε. θετικά συσχετισμένος με την αναζήτηση εμπειριών, την έλλειψη αυτοσυγκράτησης (Antoniadou, Kokkinos, & Markos, 2016).

**Οι Gkiomisi, Gkrizioti, Gkiomisi, Anastasilakis, & Kardaras, 2017**, ερευνούν το φαινόμενο του Διαδικτυακού Εκφοβισμού σε 3 διαφορετικά Γυμνάσια της Χώρας καθώς και την αποτελεσματικότητα των προτεινόμενων μεθόδων. Αποτελέσματα: 666 συμμετέχοντες μαθητές Γυμνασίου (ηλικίας 14.2+/-0.9 έτη) 194 μαθητές Δημοσίου Σχολείου (29%) 246 μαθητές Πειραματικού σχολείου (37%), 226 μαθητές Ιδιωτικού Σχολείου (34%). Χρήση Διαδικτύου24-29% κάτω από 10 ετών, 83-85% από 12 ετών. Οι μαθητές του Δημοσίου σχολείου ξεκίνησαν να χρησιμοποιούν το Διαδίκτυο αργότερα από τους μαθητές των δύο άλλων σχολείων. Αποκάλυψη Προσωπικών στοιχείων: Οι μαθητές του Δημοσίου σχολείου ήταν πιο επιρρεπείς στην αποκάλυψη του ονόματός τους σε σχέση με τους μαθητές των 2 άλλων σχολείων αλλά ήταν στα αντίστοιχα επίπεδα τόσο στην ανάρτηση, δημοσίευση φωτογραφιών ($p<0.199$), ή προσωπικών στοιχείων ($p<0.384$). Ηλικία Χρήσης κινητού ή άλλης ηλεκτρονικής συσκευής: από τα 10 έτη 20-27.5% των μαθητών, 12 έτη 91-93%, με τους μαθητές του Ιδιωτικού Σχολείου να έχουν αποκτήσει κινητό τηλέφωνο νωρίτερα (($p<0.001$) και με χρήση κινητού από την ηλικία των 13 ετών. Διαδικτυακός Εκφοβισμός: 62,2% των συμμετεχόντων, ανέφερε προηγούμενη εμπειρία Δ.Ε μέσω ηλεκτρονικής συσκευής, με τους μαθητές του Δημοσίου Σχολείου να το έχουν αντιμετωπίσει συχνότερα από τους μαθητές των 2 άλλων σχολείων

(Δημόσιο Ιδιωτικό και Πειραματικό 71.1 έναντι 57.1 έναντι 59.8 %, p 0.008 & 74.6 έναντι 61.2 έναντι 55.1 %, p 0.002,αντίστοιχα). Ο Δράστης συνήθως ήταν ξένος. Σχόλια Δ.Ε. Επιρροές από τον Δ.Ε.: Ύπνος: 86,2-87% δεν αντιμετώπισε πρόβλημα. Συνήθειες φαγητού: 81.7-88.4% δεν αντιμετώπισε πρόβλημα. Τα ποσοστά ήταν ανεξάρτητα από τον τύπο του σχολείου. Κανένα σύμπτωμα, τους 6 προηγούμενους μήνες της έρευνας, δεν αντιμετώπισε η πλειονότητα των μαθητών και των 3 διαφορετικών τύπων σχολείων. Τα άτομα που δέχθηκαν Δ.Ε. και ανέφεραν ότι αντιμετώπισαν κάποιο σύμπτωμα δεν προέβησαν σε καμμιά ενέργεια, οι πλειονότητα εξ αυτών, λίγοι μόνο το ανέφεραν στους γονείς και μια μικρή μειονότητα έλαβε φαρμακευτική αγωγή ή ζήτησε ιατρική συμβουλή. Τα 2/3 των μαθητών που φοιτούσαν στο Ιδιωτικό και το Δημόσιο σχολείο δεν θα αναζητούσαν βοήθεια για τις αλλαγές στην συμπεριφορά τους εξαιτίας του Δ.Ε., ενώ το αντίστοιχο ποσοστό των μαθητών του Πειραματικού Σχολείου ήταν πολύ μικρότερο. Το 1/3 των μαθητών όλων των τύπων σχολείων, θα ζητούσαν βοήθεια από τους γονείς. Πολύ λιγότεροι θα αναζητούσαν βοήθεια από τον θεράποντα ιατρό του σχολείου ή τον αρμόδιο για θέματα Δ.Ε. Καθηγητή (Gkiomisi et al., 2017).

#### 3.4.2.2 Κοινωνικά Δίκτυα Κίνδυνοι

##### 3.4.2.2.1 Κίνδυνοι σε Προσωπική Ζωή

**Οι Giota & Kleftaras το 2013**, διερευνούν τα χαρακτηριστικά της προσωπικότητας που σχετίζονται με την προβληματική χρήση Κοινωνικών Δικτύων αλλά και συμπτώματα κατάθλιψης εξαιτίας της χρήσης τους. Έγινε έρευνα, με ένα δείγμα 163 ατόμων ηλικίας 18-34 ετών στην Θεσσαλία (κεντρική Ελλάδα), τυχαία επιλεχθέντων. Προβληματική χρήση Διαδικτύου και Κατάθλιψη: Η Ηλικία και το φύλο δεν έδειξαν σημαντική συσχέτιση με τη Προβληματική Χρήση Διαδικτύου και την κατάθλιψη. Οι γυναίκες σε σχέση με τους άνδρες ανέφεραν υψηλότερα επίπεδα Νευρωτισμού. Ο τόπος κατοικίας φάνηκε ωστόσο να σχετίζεται με τη Προβληματική Χρήση Κοινωνικών Δικτύων (SNS). Άτομα που κατοικούσαν σε αγροτικές περιοχές (πληθυσμό έως 1500 κατοίκους), εμφανίζουν υψηλότερη βαθμολογία στην Προβληματική Χρήση Κοινωνικών Δικτύων (SNS), σε σχέση με άτομα που κατοικούσαν σε άλλες περιοχές Προβληματική Χρήση Κοινωνικών Δικτύων ( SNS) και Χαρακτηριστικά της Προσωπικότητας του Χρήστη: Η Προβληματική Χρήση Κοινωνικών Δικτύων ήταν ισχυρά συσχετισμένη με συμπτώματα Κατάθλιψης, του Νευρωτισμού και της Τερπνότητας. Ο συσχετισμός της Προβληματικής Χρήσης Κοινωνικών Δικτύων, τόσο με την Εξωστρέφεια, την Ανοιχτότητα σε Εμπειρίες

όσο και με την Συνειδητότητα, δεν επιβεβαιώθηκε από τα αποτελέσματα (Giota & Kleftaras, 2013).

**Οι Kourouthanassis, Lekakos, & Gerakis, 2015,** διερευνούν το 2012, την επίδραση της αυτοπεποίθησης της προσωπικής εικόνας του χρήστη, και της εμπιστοσύνης, στην σχέση μεταξύ της ικανοποίησης και συνέχισης της χρήσης του Κοινωνικού Δικτύου. Ηλικίες: 233 άτομα μεταξύ 18-28 ετών (80,9%), 37 άτομα 29-35 ετών (12,8%) και 18 άτομα ηλικίας μεγαλύτερης των 36 ετών (6,3%). Τα αποτελέσματα έδειξαν ότι τόσο η αυτοπεποίθηση της προσωπικής εικόνας του χρήση όσο και η εμπιστοσύνη μετριάζουν την επίδραση της ικανοποίησης στην πρόθεση συνέχισης χρήσης του Κοινωνικού Δικτύου. Μια αντίληψη της αυτοπεποίθησης της προσωπικής εικόνας αλλά και εμπιστοσύνης σχεδόν πάντα θα οδηγούν σε μεγαλύτερα επίπεδα πρόθεσης χρήσης των Κοινωνικών Δικτύων, ακόμη και όταν οι ίδιοι οι χρήστες αναφέρουν χαμηλή ικανοποίηση από την παρεχόμενη υπηρεσία. Το αντίστοιχο συμβαίνει και στην περίπτωση της εμπιστοσύνης και της σχέσης μεταξύ ικανοποίησης και της πρόθεσης συνέχισης της χρήσης. Αναφορικά τώρα με την εμπιστοσύνη, οι νεότερες ηλικίες γενικά πιο εύκολα μπορούν να αποκαλύψουν προσωπικές πληροφορίες στα Κοινωνικά Δίκτυα σε σχέση με τους μεγαλύτερους σε ηλικία και αντίστοιχα χρησιμοποιούν λιγότερο τα εργαλεία για την προστασία των προσωπικών τους δεδομένων σε σχέση με τους ηλικιακά μεγαλύτερους (Kourouthanassis et al., 2015).

**Οι Tsiolka, Bergiannaki, Margariti, Malliori, & Papageorgiou, το 2017** διερεύνησε την Δυσλειτουργική συμπεριφορά στο Διαδίκτυο σε σχέση με χαρακτηριστικά της προσωπικότητας του ατόμου και πιο συγκεκριμένα του Νευρωτισμού και της εξωστρέφειας. Η μελέτη έγινε σε ενήλικες Έλληνες μέσω της διαδικασίας της συνέντευξης. Έγινε έρευνα. Συμμετέχοντες 1211 ενήλικες 18 ετών και πάνω, χρήστες διαδικτύου. Η επιλογή των συμμετεχόντων έγινε μέσω διαφόρων forums, κοινωνικά Δίκτυα και κυρίως το Facebook. Αποτελέσματα 1211 συμμετέχοντες 51,7% άνδρες μέσης ηλικίας 29,3 ετών (SD=9.8). Οι συμμετέχοντες σε ποσοστό 79,1% ήταν μόνοι. Ο μέσος χρόνος εκπαίδευσης ήταν τα 15.1 χρόνια (SD=5.5). Το 86,3% κατοικούσε σε πόλεις με πληθυσμό πάνω από 250000 κατοίκους. Ένα 24,6% εμφάνιζε μια κάποια χρόνια σωματική κατάσταση υγείας, ενώ ένα 6% είχε μια χρόνια ψυχική κατάσταση υγείας. Φάρμακο ελάμβανε ένα ποσοστό 13,8% και θεραπεία ψυχοτροπική ένα ποσοστό 4,45%. Διαδικτυακή Συμπεριφορά Εθισμού (Internet addiction Behavior/ IAB), 71,2% δεν έδειξε σημάδια, 21,1% έδειξε λίγα σημάδια, 7,5% βρισκόταν σε κίνδυνο, 0,3% έδειξε

Συμπεριφορά εθισμού. Συνολικά Δυσλειτουργική Συμπεριφορά είχε ένα 7,7% των συμμετεχόντων. Η Δυσλειτουργική Διαδικτυακή Συμπεριφορά στην ανάλυση που υλοποιήθηκε εμφανίζεται υψηλότερη σε άτομα με χρόνια ψυχική υγεία, σε άτομα που χρησιμοποιούν ψυχοτροπικά φάρμακα και χαμηλότερη σε άτομα που έχουν παιδιά. Αντίστοιχα σε όσους παρουσιάζουν υψηλή βαθμολογία στο Ερωτηματολόγιο του Νευρωτισμού υπήρξε θετική συσχέτιση με την ύπαρξη Διαδικτυακής Δυσλειτουργικής Συμπεριφοράς, ενώ το αντίθετο συμβαίνει με την υψηλή βαθμολογία στην εξωστρέφεια και την ύπαρξη Διαδικτυακής Δυσλειτουργίας. Τα αποτελέσματα της παρούσας έρευνας έχουν επιβεβαιωθεί και από άλλες μελέτες (τόσο το ότι η εξωστρέφεια δεν σχετίζεται με την Διαδικτυακή Δυσλειτουργία) αλλά επίσης ότι ο Νευρωτισμός έχει φαίνεται να αυξάνει σημαντικά τις πιθανότητες εθισμού στο Διαδίκτυο (Tsiolka et al., 2017).

## 3.5 Αιτιολόγηση Έρευνας/ (Προβληματική)

Η υπάρχουσα διεθνής βιβλιογραφία κυρίως εστιάζει σε θέματα κινδύνου όπως ο εκφοβισμός αλλά και σε συγκεκριμένες ηλικιακές ομάδες όπως αυτές των παιδιών και των νεαρών εφήβων (Ybarra et al., 2006), (DeMarco et al., 2017), (Kezer et al., 2016).
Παρά το γεγονός ότι αυτές οι ηλικιακές ομάδες είναι ευάλωτες και επιρρεπείς στον κίνδυνο, που είναι ταυτόχρονα φοβιστικό, τόσο για τους γονείς όσο και για τους εκπαιδευτικούς τους, εντούτοις υπάρχει εκτενής βιβλιογραφική έρευνα αναφορικά με αυτές τις ομάδες.
Η Εθνική Βιβλιογραφία αντίστοιχα εξετάζει κυρίως θέματα κινδύνων σχετικά με την Καταναγκαστική Χρήση Διαδικτύου (Tsitsika et al., 2009), (Tsitsika et al., 2014), (Kormas et al., 2011), αναζήτηση αιτιών χρήσης Ιστοσελίδων Κοινωνικής Δικτύωσης, και εκφοβισμού επίσης σε νεαρά άτομα και παιδιά κυρίως (Gkiomisi et al., 2017), (Antoniadou & Kokkinos, 2015). Η διερεύνηση άλλων κινδύνων σε ΙΚΔ στην Ελλάδα είναι πολύ περιορισμένη.

Σύμφωνα με τα δημοσιευμένα στατιστικά, οι χρήστες των Κοινωνικών Δικτύων το 2019 ανέρχονται στο 45% του παγκόσμιου πληθυσμού με περίπου 2.65 δισεκατομμύρια χρήστες. Το αντίστοιχο ποσοστό το 2010 ανέρχονταν περίπου σε 1 δισεκατομμύριο. Η αυξημένη χρήση συσκευών όπως τηλέφωνα, επιπλέον διευκολύνουν την διείσδυση της προσβασιμότητας στις ΙΚΔ, και όπως υποστηρίζεται οι φθηνές συσκευές (κινητά

τηλέφωνα), είναι ένας από τους λόγους της ανάπτυξης των Κοινωνικών Μέσων (Clement, 2019).

Η επέκταση όσο και ο πολλαπλασιασμός των Ιστοσελίδων Κοινωνικής Δικτύωσης και η διείσδυσή τους σε ολοένα και μεγαλύτερο μέρος του ενήλικου πληθυσμού, (όχι απαραίτητα μόνο του εθνικού αλλά και του παγκόσμιου, σχεδόν καθιστά αναγκαιότητα την διεξαγωγή της προταθείσας έρευνας, - το 2021 αναμένεται οι παγκόσμιοι χρήστες να ανέλθουν περίπου στα 3.1 δισεκατομμύρια. (Clement, 2019) ("infographic-information-technologies-2019—ELSTAT," n.d.) ("Η Ελλάδα με Αριθμούς—ELSTAT," n.d.).

Η πληθυσμιακή κατανομή του πληθυσμού της χώρας, και σύμφωνα με την απογραφή του 2011, αλλά και λοιπών εκτιμήσεων που δημοσιεύονται στον τύπο, ενισχύει την άποψη ότι ο πληθυσμός της Ελλάδας, τείνει να οδηγείται σε ποσοστά ενηλίκων υψηλότερα των παλαιότερων εποχών ("Στατιστικές—ELSTAT," n.d.) (Σαλούρου, 2015).

Ο σκοπός αυτής της πρότασης έρευνας είναι να καλύψει, το υπάρχον κενό στην υπάρχουσα βιβλιογραφία, αυτή της ανίχνευσης κινδύνων στις Ιστοσελίδες Κοινωνικής Δικτύωσης στον ενήλικο πληθυσμό.

## 3.6 Πώς η παρούσα μελέτη θα επεκτείνει την βιβλιογραφία

Η μελέτη της βιβλιογραφίας έδειξε ότι οι παγκόσμιοι χρήστες ΙΚΔ αυξάνονται με ταχείς ρυθμούς, οι δε κίνδυνοι είναι ένα φαινόμενο που αφορά κάθε πτυχή της ανθρώπινης δραστηριότητας. Η μέτρηση τόσο της διείσδυσης των ΙΚΔ στον ενήλικο πληθυσμό της χώρας, όσο και η μέτρηση των κινδύνων σε αυτές, μπορούν να αποτελέσουν εργαλεία (μέτρησης), που θα συνεισφέρουν στην ανάλυση των μοτίβων, που θα δώσουν τάσεις και ανωμαλίες, ή ακόμη και δυνατότητα συσχετισμού κινδύνων με πιθανές συνέπειες, που με την σειρά τους, να οδηγήσουν στην δημιουργία πρακτικών προστασίας. Όπως αναφέρουν οι Frye et all, (2012) «Πολλά πλεονεκτήματα προκύπτουν από την ικανότητα μέτρησης των απειλών με ακρίβεια και συνέπεια….. Σε συντομία μια καλή μέτρηση κινδύνου υποστηρίζει καλή διαχείριση κινδύνου» (Frye et al., 2012).

## 3.7 Ερευνητικά ερωτήματα

Όπως παρουσιάστηκε παραπάνω, η βιβλιογραφία, η σχετική με κινδύνους (εκτός του εθισμού), στην Ελλάδα, είναι περιορισμένη. Προκειμένου να καλυφθούν τα κενά η παρούσα έρευνα έχει στόχο να εξερευνήσει τα ερευνητικά ερωτήματα που ακολουθούν.

1. Ποιες είναι οι πιο δημοφιλείς (κυρίαρχες) Πλατφόρμες Κοινωνικών Δικτύων.
2. Ποιος ο βαθμός Διείσδυσης (χρήση) των Κοινωνικών Δικτύων στους χρήστες του Διαδικτύου.
3. Ποιοι είναι οι πλέον κοινοί κίνδυνοι στα Κοινωνικά Δίκτυα και οι παράγοντες έκθεσης.
4. Υπάρχει σχέση μεταξύ Κοινωνικό-δημογραφικών στοιχείων των χρηστών και συμπεριφορών (παραγόντων) που οδηγούν σε κίνδυνο?
5. Υπάρχει συσχετισμός μεταξύ Κοινωνικό-Δημογραφικών στοιχείων των χρηστών των ιστοσελίδων Κοινωνικών Δικτύων (φύλου, ηλικίας, μορφωτικού επιπέδου) και έκθεσης σε διαδικτυακούς κινδύνους?

# Κεφάλαιο 4

# Πειραματική Μέθοδος με Χρήση Ποσοτικής Έρευνας

## 4.1 Μεθοδολογία της Έρευνας

Η παρούσα έρευνα χρησιμοποιεί την ποσοτική μέθοδο για την συλλογή των δεδομένων, καθώς μέσω αυτών των δεδομένων και των αποτελεσμάτων τους, μπορούν να εξετασθούν οι παράγοντες της έκθεσης, πόσο ο χρήστης αντιλαμβάνεται, εάν και πόσο, εκτίθεται σε κινδύνους. Η έρευνα απευθύνεται σε ενήλικες από την ηλικία των 18 ετών, καθώς αυτές οι ηλικίες εξετάζονται λιγότερο σε σχέση με τα παιδιά και τους εφήβους (ομάδες οι οποίες θεωρούνται ότι είναι πιο επιρρεπείς στην έκθεση σε κινδύνους).

## 4.2 Δείγμα και Τόπος της Έρευνας

Μη τυχαίο Δείγμα πληθυσμού 4000 ατόμων κατά προσέγγιση. Συμμετέχοντες ενήλικες άνω των 18 ετών. Τόπος υλοποίησης της έρευνας, είναι η Ελλάδα.

Τα ερωτηματολόγια δημιουργήθηκαν μέσω της εφαρμογής της Google (Google forms) και διανεμήθηκαν με δύο διαφορετικούς τρόπους, **1.** μέσω της εφαρμογής Κοινωνικής Δικτύωσης Facebook και **2.** μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (Gmail) **1.** Η πρόσκληση προς τους «φίλους» του Facebook, έγινε με ανάρτηση της ερευνήτριας και ζητήθηκε από τους «φίλους» να το συμπληρώσουν αλλά επιπλέον, να το αναρτήσουν αντίστοιχα, όπως και να ζητήσουν από τους δικούς τους «φίλους» να το συμπληρώσουν - μέθοδος «χιονοστιβάδα/snowball. **2.** Μηνύματα Ηλεκτρονικού Ταχυδρομείου, εστάλησαν σε εργαζόμενους, σε μεγάλο δημόσιο Οργανισμό. Τόσο το κείμενο της ανάρτησης στο Facebook, όσο και το συνοδευτικό κείμενο του ηλεκτρονικού ταχυδρομείου προς τους υποψήφιους συμμετέχοντες, περιείχαν πληροφορίες περί της

διατήρησης της «ανωνυμίας» των συμμετεχόντων (και αναφορικά με την συμπλήρωση του ερωτηματολογίου όσο και για την συλλογή των δεδομένων).
Περίοδος υλοποίησης του Πιλοτικού 17/07/2019 – 20/07/2019
Περίοδος υλοποίησης της έρευνας 21/07/2019 - 23/09/2019.
Το ερωτηματολόγιο τελικά συμπλήρωσαν 432 άτομα εκ των οποίων οι 98 δεν διατηρούσαν λογαριασμό σε Ι.Κ.Δ. Η ανάλυση των δημογραφικών στοιχείων των συμμετεχόντων με πίνακες και γραφήματα παρατίθεται στο κεφάλαιο 5.

## 4.3 Πρόσβαση και άδειες

Για την αποστολή των ερωτηματολογίων στις ηλεκτρονικές διευθύνσεις αποδεκτών Μεγάλου Δημόσιου Οργανισμού, άδεια ζητήθηκε και αποκτήθηκε ηλεκτρονικά από την Διοίκηση του οργανισμού.

## 4.4 Εργαλεία, η διαθεσιμότητα και η εγκυρότητά τους

Η συλλογή των δεδομένων έγινε με την χρήση Ερωτηματολογίων.
Τα ερωτηματολόγια που χρησιμοποιήθηκαν είναι :

Η Χρήση των Ιστοσελίδων Κοινωνικής Δικτύωσης/ General Social Media Usage Subscale) μετρήθηκε με το σταθμισμένο υπό ερωτηματολόγιο (General Social Media Usage Subscale)» της «Κλίμακας Χρήσης Μέσων και Τεχνολογίας και Συμπεριφορών (Media and Technology Usage and Attitudes Scale – MTUAS)» (Rosen, Whaling, Carrier, Cheever, & Rokkum, 2013), 9 ερωτήσεων σε 10/θμη σε κλίμακα Likert από το 1= Ποτέ έως 10 Συνεχώς /Όλη την Ώρα
Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.60-0.85
Αξιοπιστία Ερωτηματολογίου Πιλοτικό Cronbach Alpha 0.861
Αξιοπιστία Ερωτηματολογίου έρευνας Cronbach Alpha 0.852
(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 12-20)
Για τις Πρακτικές Χρήσης Διαμοιρασμού Πληροφοριών σε Ιστοσελίδες Κοινωνικής Δικτύωσης (Personal Information Sharing Practices (PISP) χρησιμοποιήθηκε το Ερωτηματολόγιο του (Ball, Ramim, & Levy, 2015), με απαντήσεις Ναι/ Όχι

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 23-25)

Κλίμακα Αναστροφής Κινδύνου (Risk Averseness Scale). Μετρήθηκε με το ερωτηματολόγιο των Pan & Zinkhan (2006), (Fogel & Nehmad, 2009), 5 ερωτήσεων. Οι ερωτήσεις μετρώνται σε 5/θμη κλίμακα Likert από το 1 = Ισχυρά Διαφωνώ έως το 5 Ισχυρά Συμφωνώ. *Υψηλότερες βαθμολογίες υποδεικνύουν περισσότερο επικίνδυνες συμπεριφορές* (Fogel & Nehmad, 2009).

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.76

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.875

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.795

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 26-30)

Εμπιστοσύνη σε Εταιρείες ΙΚΔ (Trust) Μετρήθηκε με το ερωτηματολόγιο των Pan & Zinkhan (2006), (Fogel & Nehmad, 2009), 4 ερωτήσεων. Οι ερωτήσεις μετρώνται σε 5/θμη κλίμακα Likert από το 1 = Ισχυρά Διαφωνώ έως το 5 Ισχυρά Συμφωνώ.

*Υψηλότερες βαθμολογίες υποδεικνύουν ότι οι εταιρείες είναι πιο αξιόπιστες* (Fogel & Nehmad, 2009).

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.95

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.949

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.895

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 31-34)

Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο (Privacy Behavior Scale) Μετρήθηκε με το ερωτηματολόγιο των Buchanan, et al (2007) , (Fogel & Nehmad, 2009), 6 ερωτήσεων.

Οι ερωτήσεις μετρώνται σε 5/θμη κλίμακα Likert από το 1 = Ποτέ έως το 5 Πάντα. *Μεγαλύτερες βαθμολογίες υποδεικνύουν μεγαλύτερα επίπεδα συμπεριφοράς Ιδιωτικότητας / απορρήτου* (Fogel & Nehmad, 2009).

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.80

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.944

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.790

Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 35-40)

Ανησυχία για την Ιδιωτικότητα/ Απόρρητο (Privacy Concern Scale) Μετρήθηκε με το ερωτηματολόγιο των Dinev & Hart, (2004), (Fogel & Nehmad, 2009), 3 ερωτήσεων. Οι ερωτήσεις μετρώνται σε 5/θμη κλίμακα Likert από το 1 = Ισχυρά Διαφωνώ έως το 5 Ισχυρά Συμφωνώ.

*Οι υψηλότερες βαθμολογίες δείχνουν μεγαλύτερη ανησυχία για τις πληροφορίες που παρέχονται μέσω των ΙΚΔ* (Fogel & Nehmad, 2009).

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.92

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.763

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.916

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 41-43)

Αντιληπτός έλεγχος πληροφορίας (Perceived Control of Information). Μετρήθηκε με το ερωτηματολόγιο των Krasnova et al. (2010), (Hajli & Lin, 2016), 3 ερωτήσεων και μετρήθηκε σε 5/θμη κλίμακα από το 1 = Ισχυρά Διαφωνώ έως το 5 Ισχυρά Συμφωνώ.

*Οι υψηλότερες βαθμολογίες δείχνουν μεγαλύτερη ανησυχία για τον αντιληπτό έλεγχο των πληροφοριών που παρέχονται σε ΙΚΔ* (Fogel & Nehmad, 2009).

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.89

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.932

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.830

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 44-46)

Αποκάλυψη Προσωπικών πληροφοριών (Identity Information Disclosure Scale) Μετρήθηκε με το ερωτηματολόγιο του Stutzman, (2006), (Fogel & Nehmad, 2009), το οποίο περιέχει 2 υπό-ερωτηματολόγια 4 ερωτήσεων το κάθε ένα. Οι ερωτήσεις και των δύο υπό-ερωτηματολόγιων μετρήθηκαν με 5/θμη κλίμακα από το 1 = Ισχυρά Διαφωνώ έως το 5 Ισχυρά Συμφωνώ.

*Οι υψηλότερες βαθμολογίες υποδεικνύουν μικρότερη ανησυχία αναφορικά με την Αποκάλυψη Προσωπικών Πληροφοριών στις ΙΚΔ* (Fogel & Nehmad, 2009).

Υπό-ερωτηματολόγιο Α

Αξιοπιστία Αρχικού Ερωτηματολογίου Cronbach Alpha 0.82

Αξιοπιστία Ερωτηματολογίου Έρευνας Πιλοτικό Cronbach Alpha 0.813

Αξιοπιστία Ερωτηματολογίου Έρευνας Cronbach Alpha 0.736

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 47-50)

Υπό ερωτηματολόγιο Β

Καθώς η αξιοπιστία των δύο υπό-ερωτηματολογίων δεν είναι ίδια, (Cronbach Alpha 0.813 πρώτου υπό ερωτηματολογίου) ενώ το Cronbach Alpha του δεύτερου υπό-ερωτηματολογίου ήταν χαμηλό, οι ερωτήσεις (του δεύτερου υπό-ερωτηματολογίου 4 ερωτήσεων) αναλύθηκαν αυτόνομες.

(Ερωτήσεις σε Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα 51-54)

"Όλα τα ερωτηματολόγια μεταφράσθηκαν και προσαρμόσθηκαν στα Ελληνικά από την διεξάγουσα την έρευνα.

## 4.5 Διαδικασία Συγκέντρωσης Δεδομένων

Οι υποψήφιοι συμμετέχοντες συμπλήρωσαν το ερωτηματολόγιο (που δημιουργήθηκε με Google Forms), το οποίο είτε αναρτήθηκε στο Κοινωνικό Δίκτυο είτε απεστάλη με email και ενσωματωμένο σύνδεσμο (link). Ένα συνοδευτικό κείμενο ακολουθούσε την ανάρτηση ή το ηλεκτρονικό ταχυδρομείο, στο οποίο οι υποψήφιοι συμμετέχοντες ενημερώνονταν για τις λεπτομέρειες της έρευνας, (σκοπό, στόχο, τον υπεύθυνο διενέργειας της έρευνας κλπ.). Όλα τα δεδομένα συλλέχθηκαν ανώνυμα και διασφαλίσθηκε πλήρως, η ανωνυμία των συμμετεχόντων. Στους υποψήφιους συμμετέχοντες τονίσθηκε ότι και η συλλογή αλλά και η επεξεργασία των δεδομένων υλοποιούνται ανώνυμα. Όπου απαιτήθηκε έγκριση, ελήφθη. Η διενέργεια μιας έρευνας μέσω ερωτηματολογίων και της συλλογής των στοιχείων τους είναι εύχρηστη λύση, δεν απαιτείται κόστος (πέραν του χρόνου του ερευνητή), ο χρόνος συλλογής των δεδομένων είναι σχετικά μικρός και επιπλέον είναι ανώνυμα, που μπορεί ως παράγων να είναι θετικός, καθώς δεν εγείρονται θέματα από τους συμμετέχοντες δισταγμών που μπορεί να προκύψουν σε επώνυμες απαντήσεις. Η διαδικτυακή μορφή επιπλέον της έρευνας ειδικά στις περιπτώσεις που ερευνάται μια ίδιου τύπου έρευνα δεν αποτελεί μεροληπτικό παράγοντα.

## 4.6 Ανάλυση Δεδομένων

Για την επεξεργασία και ανάλυση των δεδομένων, στατιστικές αναλύσεις, την παραγωγή των πινάκων αποτελεσμάτων, των εικόνων και των γραφικών χρησιμοποιήθηκε το IBM SPSS v. 26 for iMac (το οποίο παρασχέθηκε από το ΑΠΚΥ).

Ανάλυση υλοποιήθηκε, για την εξέταση των παραγόντων του ερωτηματολογίου. Οι έλεγχοι συσχέτισης με Pearson r και Spearman's rho, όπως και τα αποτελέσματα των (test) Mann-Whitney ανεξάρτητων δειγμάτων παρατίθενται. Έλεγχοι One Way ANOVA υλοποιήθηκαν για τις μεταβλητές Risk Taking, Privacy Behavior, Perceived Control of Information, Identity Information Disclosure ως εξαρτημένες μεταβλητές και την ηλικία ως ανεξάρτητη μεταβλητή. Test Kruskal-Wallis για τις μεταβλητές Trust, ως εξαρτημένη μεταβλητή και ανεξάρτητη μεταβλητή το Μορφωτικό Επίπεδο. Επίσης Kruskal-Wallis test, χρησιμοποιήθηκε όπου κρίθηκε απαραίτητο για τον έλεγχο κατηγορικών μεταβλητών όπως στην «Αποκάλυψη Προσωπικών πληροφοριών – "Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο

διαδίκτυο και Μορφωτικό Επίπεδο, αλλά και στην Έκθεση σε κίνδυνο» και Φύλου. Σε όλους τους υπολογισμούς, τιμές του p κάτω του 0,05 θεωρήθηκαν σημαντικές.

Οι μεταβλητές που θα χρησιμοποιούνταν για τους ελέγχους υποθέσεων και συσχέτισης (correlation), ελέγχθηκαν ως προς την κανονικότητά τους (test for normality, Shapiro-Wilk test) και την ομοιογένεια διακύμανσης (Levene's test), όπου ήταν απαραίτητο προκειμένου να επιλεγεί το κατάλληλο test (παραμετρικό ή μη), για την συσχέτιση ή τον έλεγχο της Μηδενικής Υπόθεσης.

# Κεφάλαιο 5

# Αποτελέσματα

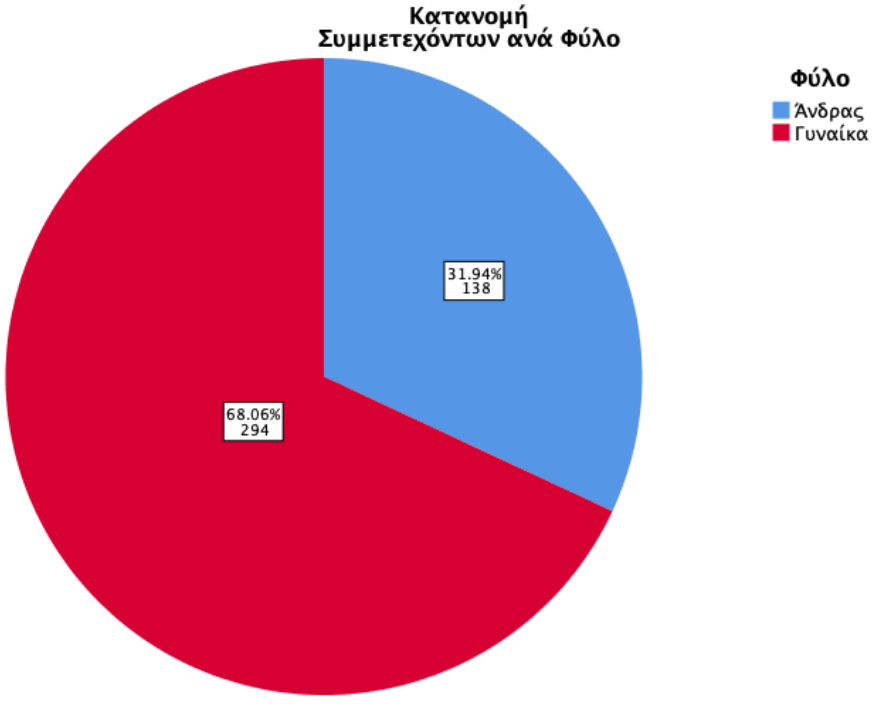
## 5.1 Περιγραφική Ανάλυση των δεδομένων

### 5.1.1 Φύλο Χρηστών Διαδικτύου

| | | Φύλο | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Άνδρας | 138 | 31.9 | 31.9 | 31.9 |
| | Γυναίκα | 294 | 68.1 | 68.1 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 1 Κατανομή Συμμετεχόντων ανά Φύλο*

Στον πίνακα 5.1.1 παρατίθεται η κατανομή του φύλου των συμμετεχόντων, από όπου και προκύπτει ότι οι γυναίκες του δείγματος είναι η πλειοψηφία σε ποσοστό 68,1% (απόλυτος αριθμός 294 γυναίκες) ενώ οι άνδρες είναι 31,9% (απόλυτος αριθμός 138).



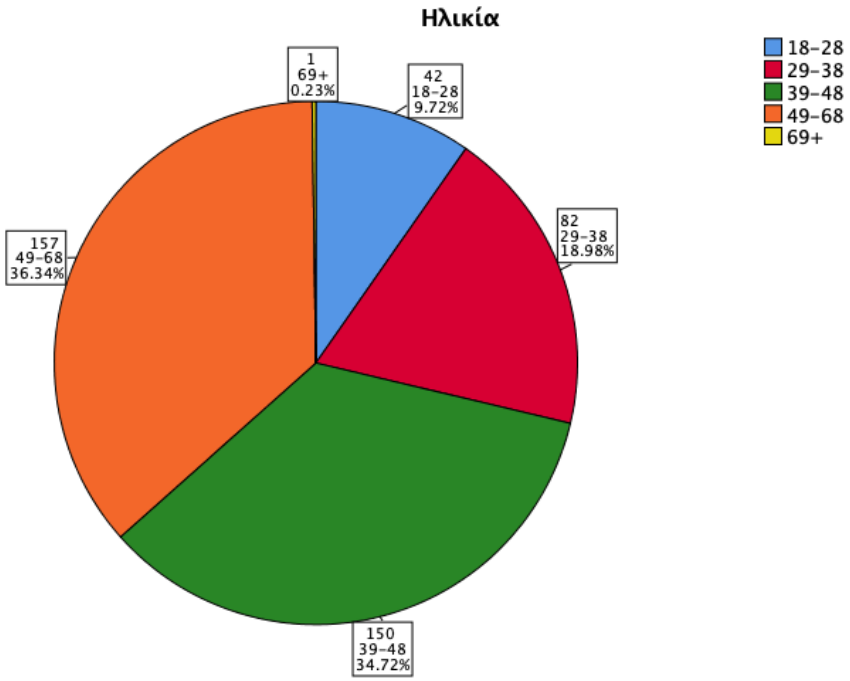
*Γράφημα: 1 Κατανομή Συμμετεχόντων ανά Φύλο*

### 5.1.2 Ηλικία Χρηστών Διαδικτύου

| Ηλικία | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | 18-28 | 42 | 9.7 | 9.7 | 9.7 |
| | 29-38 | 82 | 19.0 | 19.0 | 28.7 |
| | 39-48 | 150 | 34.7 | 34.7 | 63.4 |
| | 49-68 | 157 | 36.3 | 36.3 | 99.8 |
| | 69+ | 1 | .2 | .2 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 2 Συγκεντρωτικά Στοιχεία Κατανομής Ηλικιών*

Στον πίνακα 5.1.2 παρατίθεται η κατανομή των ηλικιών των συμμετεχόντων, από όπου και προκύπτει ότι το μεγαλύτερο ποσοστό συμμετεχόντων 36,3% (απόλυτος αριθμός 157 άτομα) ανήκουν στην ηλικιακή ομάδα των 49-68 ετών, και το αμέσως επόμενο ποσοστό 34,7% ( απόλυτος αριθμός 150 άτομα) στην ηλικιακή ομάδα 39-48 ετών. Ακολουθούν οι ηλικιακές ομάδες 29- 38 ετών σε ποσοστό 19% (απόλυτος αριθμός 82 άτομα), 18-28 ετών 9,7% (απόλυτος αριθμός 42 άτομα) και τέλος μόνο ένα άτομο στην ηλικιακή ομάδα των 69+ ποσοστό 0,2% .



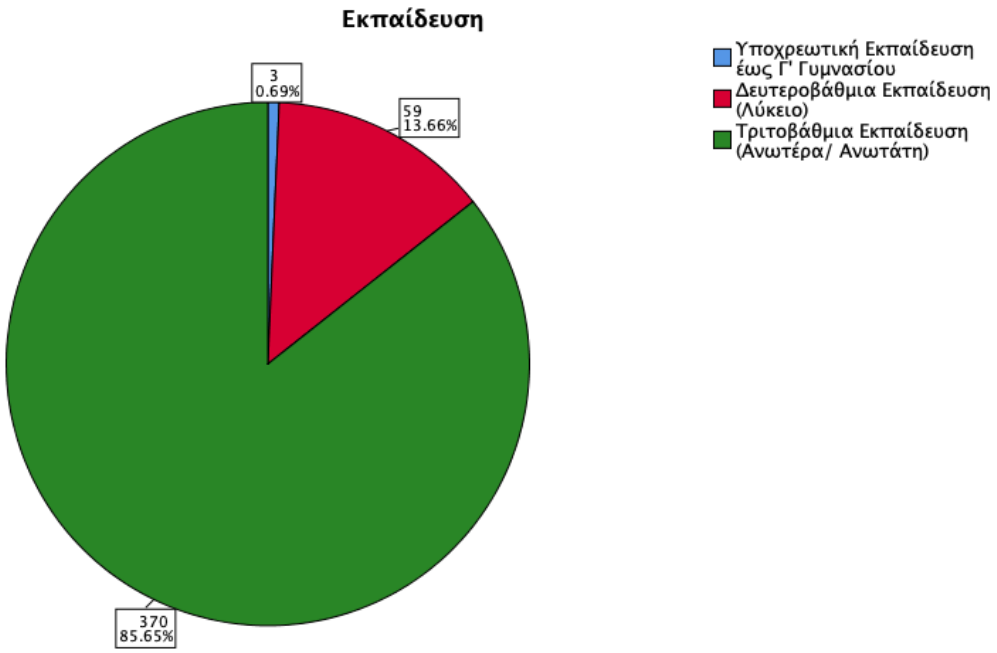

*Γράφημα: 2 Κατανομή Ηλικιών Συμμετεχόντων*

### 5.1.3 Εκπαίδευση Χρηστών Διαδικτύου

| Εκπαίδευση | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | 3 | .7 | .7 | .7 |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | 59 | 13.7 | 13.7 | 14.4 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | 370 | 85.6 | 85.6 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 3 Εκπαίδευση (Μορφωτικό Επίπεδο)*

Στον πίνακα 5.1.3 παρατίθεται η κατανομή της εκπαίδευσης των συμμετεχόντων, από όπου προκύπτει ότι το μεγαλύτερο ποσοστό των συμμετεχόντων 85,6% (απόλυτος αριθμός 370 άτομα) έχουν μορφωτικό επίπεδο τριτοβάθμιας εκπαίδευσης, Ανωτέρας ή Ανώτατης, το αμέσως επόμενο ποσοστό 13,7% (απόλυτος αριθμός 59 άτομα) έχουν μορφωτικό επίπεδο Δευτεροβάθμιας εκπαίδευσης και υπάρχει και ένα ποσοστό 0.7% (απόλυτος αριθμός 3 άτομα) που έχουν μορφωτικό επίπεδο Υποχρεωτικής εκπαίδευσης.




*Γράφημα: 3 Εκπαίδευση (Μορφωτικό Επίπεδο) Συμμετεχόντων*

### 5.1.4 Σύνδεση στο Διαδίκτυο

| Έχετε Μόνιμη Σύνδεση στο Διαδίκτυο? | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Ναι | 392 | 90.7 | 90.7 | 90.7 |
| | Όχι | 40 | 9.3 | 9.3 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 4 Στοιχεία Μόνιμης Σύνδεσης στο Διαδίκτυο*

Στον πίνακα 5.1.4 παρατίθενται τα στοιχεία της Μόνιμης Σύνδεσης στο Διαδίκτυο, από όπου προκύπτει ότι το μεγαλύτερο ποσοστό των συμμετεχόντων 90,74% (απόλυτος αριθμός 392 άτομα) διατηρεί μόνιμη σύνδεση Διαδικτύου, ενώ μόνο το 9,26% (απόλυτος αριθμός 40 άτομα) δεν διατηρεί.


*Γράφημα: 4 Στοιχεία Μόνιμης Σύνδεσης στο Διαδίκτυο*

### 5.1.5 Σύνδεση στο Διαδίκτυο από Σημείο Πρόσβασης

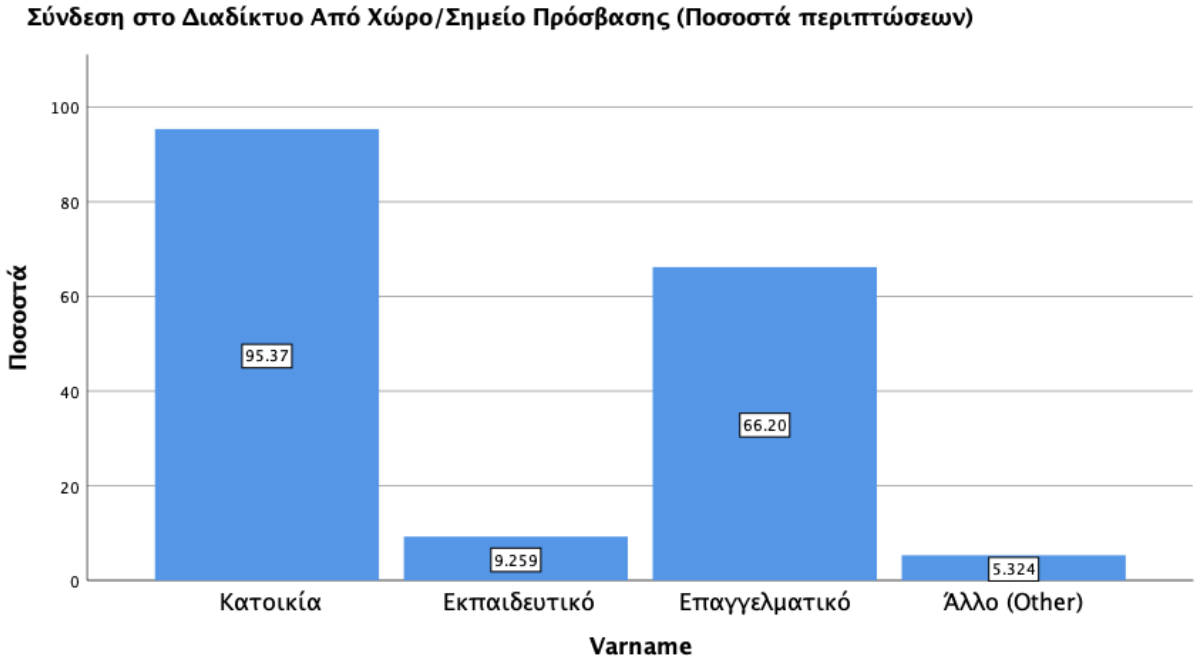
Στον Πίνακας: 5 & Γράφημα: 5 που ακολουθούν παρατίθενται στοιχεία αναφορικά με τον τόπο πρόσβασης των συμμετεχόντων στο Διαδίκτυο. Ένα 95,4% των συμμετεχόντων συνδέονται από το σπίτι, το αμέσως επόμενο ποσοστό 66,4%, αφορά την Σύνδεση από επαγγελματικό χώρο.

### 5.1.6 Σύνδεση στο Διαδίκτυο Από Σημείο Πρόσβασης

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| Σύνδεση στο Διαδίκτυο Από | Κατοικία | 412 | 54.1% | 95.4% |
| | Εκπαιδευτικό | 40 | 5.3% | 9.3% |
| | Επαγγελματικό | 286 | 37.6% | 66.2% |
| | Άλλο (Other) | 23 | 3.0% | 5.3% |
| Total | | 761 | 100.0% | 176.2% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 5 Σύνδεση στο Διαδίκτυο Από Χώρο*




*Γράφημα: 5 Σύνδεση στο Διαδίκτυο Από Χώρο Ποσοστά ανά Σημείο Πρόσβασης*

### 5.1.7 Σύνδεση στο Διαδίκτυο Μέσω (Συσκευών)

Σύμφωνα με τους Πίνακας: 6 & Γράφημα: 6 που ακολουθεί οι συμμετέχοντες χρησιμοποιούν (πολλαπλά και εναλλακτικά) όλα τα μέσα για την σύνδεσή τους στο Διαδίκτυο.

**Σύνοψη**

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Σύνδεση Μέσου | 432 | 100.0% | 0 | 0.0% | 432 | 100.0% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 6 Σύνοψη Συμμετεχόντων Σύνδεση Στο Διαδίκτυο Μέσω*

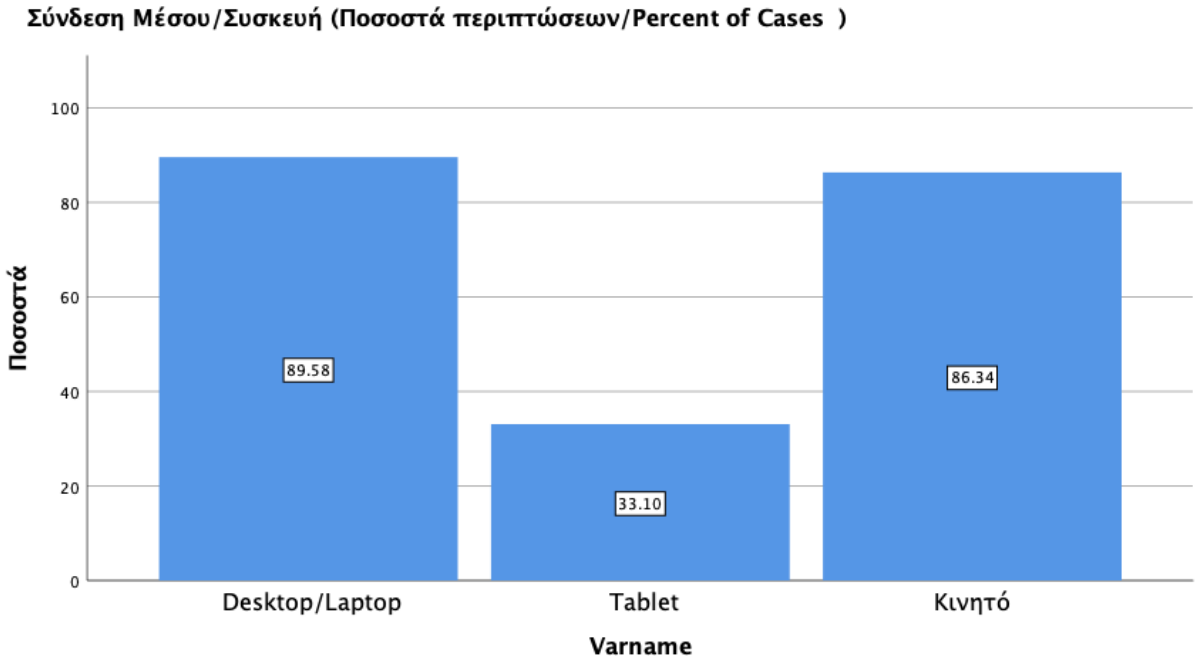
Στον Πίνακας: 7 & Γράφημα: 6 παρατίθενται στοιχεία αναφορικά με τα Μέσα (συσκευές) που χρησιμοποιούν οι Συμμετέχοντες για την Σύνδεσή τους στο Διαδίκτυο. Η σύνδεση στο Διαδίκτυο από Σταθερό ή Φορητό υπολογιστή φαίνεται να είναι μικρότερη συγκρινόμενη με τις δύο συσκευές κινητό και tablet που και τα δύο μαζί ανέρχονται σε 57,1%

**Σύνδεση Μέσου**

| | Responses | | Percent of Cases |
|---|---|---|---|
| | N | Percent | |
| Σύνδεση Μέσω Desktop/Laptop | 387 | 42.9% | 89.6% |
| Σύνδεση Μέσω Tablet | 143 | 15.8% | 33.1% |
| Σύνδεση Μέσω Κινητού | 373 | 41.3% | 86.3% |
| Total | 903 | 100.0% | 209.0% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 7 Σύνδεση Στο Διαδίκτυο Μέσου – ανά Μέσο*




*Γράφημα: 6 Σύνδεση Στο Διαδίκτυο Μέσου Πρόσβασης- Ποσοστά ανά Συσκευή*

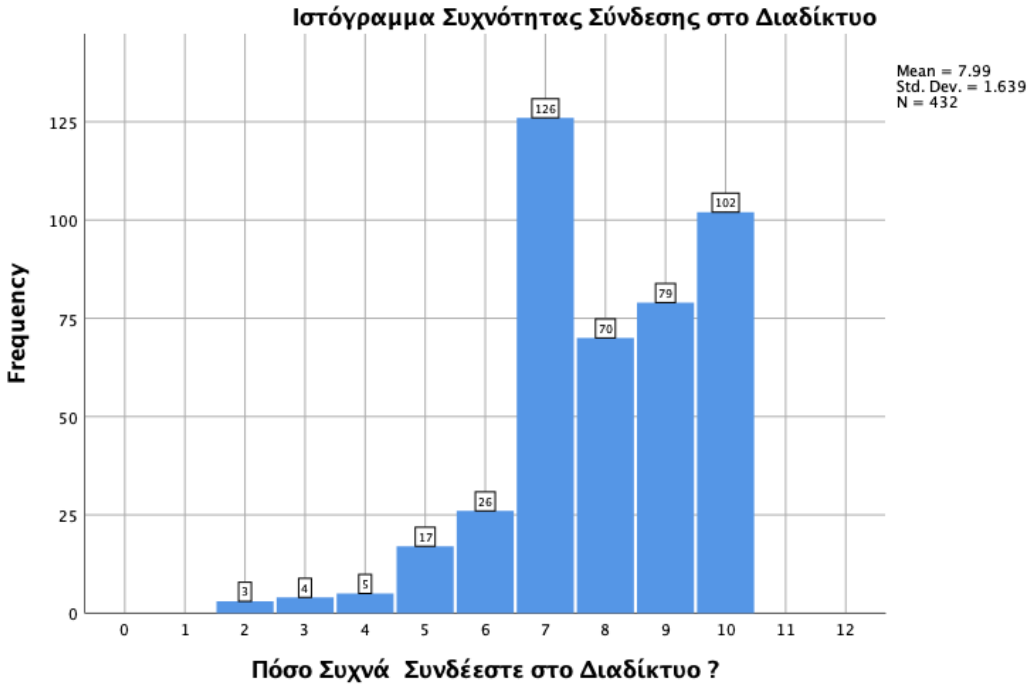
### 5.1.8 Συχνότητα Σύνδεσης στο Διαδίκτυο

| Πόσο Συχνά Συνδέεστε στο Διαδίκτυο ? | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 2 | 3 | .7 | .7 | .7 |
| | 3 | 4 | .9 | .9 | 1.6 |
| | 4 | 5 | 1.2 | 1.2 | 2.8 |
| | 5 | 17 | 3.9 | 3.9 | 6.7 |
| | 6 | 26 | 6.0 | 6.0 | 12.7 |
| | 7 | 126 | 29.2 | 29.2 | 41.9 |
| | 8 | 70 | 16.2 | 16.2 | 58.1 |
| | 9 | 79 | 18.3 | 18.3 | 76.4 |
| | 10 | 102 | 23.6 | 23.6 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 8 Συχνότητα Σύνδεσης στο Διαδίκτυο*

Στο Πίνακας: 8 & Γράφημα: 7 παρατίθενται τα ποσοστά (και οι απόλυτοι αριθμοί) της συχνότητας Σύνδεσης στο Διαδίκτυο των συμμετεχόντων. (Η κλίμακα σύνδεσης μετρά από το 1= Ποτέ, 2= Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7=Μερικές Φορές την Ημέρα, 8= Μια φορά την Ώρα, 9= Μερικές Φορές την Ώρα, 10=Όλη την Ώρα/ Συνεχώς) Από τον πίνακα προκύπτει ότι το μεγαλύτερο ποσοστό 29,2% (απόλυτος

αριθμός 126 άτομα) συνδέονται στο Διαδίκτυο Μερικές φορές την ημέρα (7), το επόμενο 23,6% (απόλυτος αριθμός 102 άτομα) Συνεχώς όλη την ώρα (10) και ακολουθούν με ποσοστό 18,3% (απόλυτος αριθμός 79 άτομα) Μερικές Φορές την Ημέρα (9), 16,2% (απόλυτος αριθμός 70 άτομα) Μια φορά την Ώρα (8). Μονοψήφια είναι τα ποσοστά τα των συμμετεχόντων που συνδέονται σπανιότερα στο Διαδίκτυο 6% (απόλυτος αριθμός 26 άτομα) Μια φορά την Ημέρα (6), 3,9% (απόλυτος αριθμός 17 άτομα) Μερικές Φορές την Εβδομάδα (5), 1,2% (απόλυτος αριθμός 5 άτομα) Μια φορά την Εβδομάδα (4), 0.9% (απόλυτος αριθμός 4 άτομα) Μερικές Φορές τον Μήνα( 3) και τέλος 0,7% (απόλυτος αριθμός 3 άτομα) Μία Φορά τον Μήνα (2).



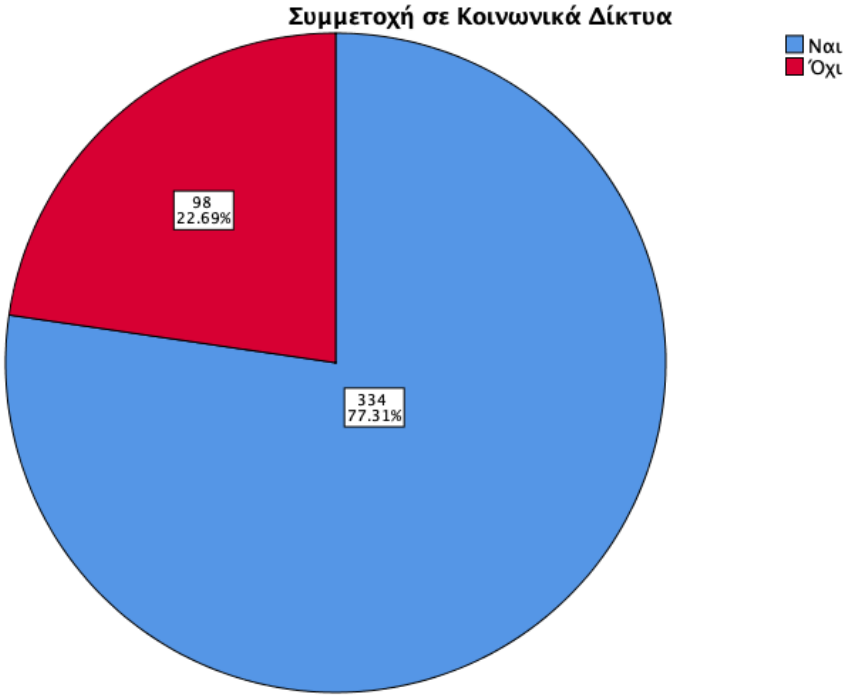

*Γράφημα: 7 Συχνότητα Σύνδεσης στο Διαδίκτυο*

### 5.1.9 Συμμετοχή σε Κοινωνικά Δίκτυα ( Διείσδυση στους Χρήστες Διαδικτύου)

| Συμμετέχετε σε Ιστοσελίδες Κοινωνικών Δικτύων? | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Ναι | 334 | 77.3 | 77.3 | 77.3 |
| | Όχι | 98 | 22.7 | 22.7 | 100.0 |
| | Total | 432 | 100.0 | 100.0 | |

*Πίνακας: 9 Συμμετοχή Σε Κοινωνικά Δίκτυα*

Στον Πίνακας: 9 & Γράφημα: 8 παρατίθεται το ποσοστό των συμμετεχόντων σε Κοινωνικά Δίκτυα, από όπου προκύπτει ότι το μεγαλύτερο ποσοστό των συμμετεχόντων 77,3% (απόλυτος αριθμός 334 άτομα) συμμετέχει σε Ιστοσελίδες Κοινωνικής Δικτύωσης ενώ ένα ποσοστό 22,7% (απόλυτος αριθμός 98), δεν συμμετέχει.




*Γράφημα: 8 Συμμετοχή Σε Κοινωνικά Δίκτυα – Ποσοστά συμμετεχόντων*

Καθώς οι μη έχοντες λογαριασμό σε Ιστοσελίδα Κοινωνικής Δικτύωσης, 98 άτομα συνολικά από τους 432 συμμετέχοντες, υπέβαλαν το ερωτηματολόγιο, μετά την συγκεκριμένη ερώτηση, για τις υπόλοιπες (και σχετικές με τα Κοινωνικά Δίκτυα ερωτήσεις), εξαιρέθηκαν από την ανάλυση των αποτελεσμάτων. Έτσι η ανάλυση αφορά μόνο τα 334 άτομα τελικά που διατηρούν λογαριασμό σε Ιστοσελίδες Κοινωνικής Δικτύωσης.

### 5.1.10 Συμμετοχή σε Κοινωνικά Δίκτυα ανά Ιστοσελίδα Κοινωνικής Δικτύωσης

**Σύνοψη**

| | Cases | | |
|---|---|---|---|
| | Valid | Missing | Total |

| | N | Percent | N | Percent | N | Percent |
|---|---|---|---|---|---|---|
| Συμμετοχή σε Κοινωνικά Δίκτυα | 334 | 100.0% | 0 | 0.0% | 334 | 100.0% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 10 Συμμετοχή σε Κοινωνικά Δίκτυα*

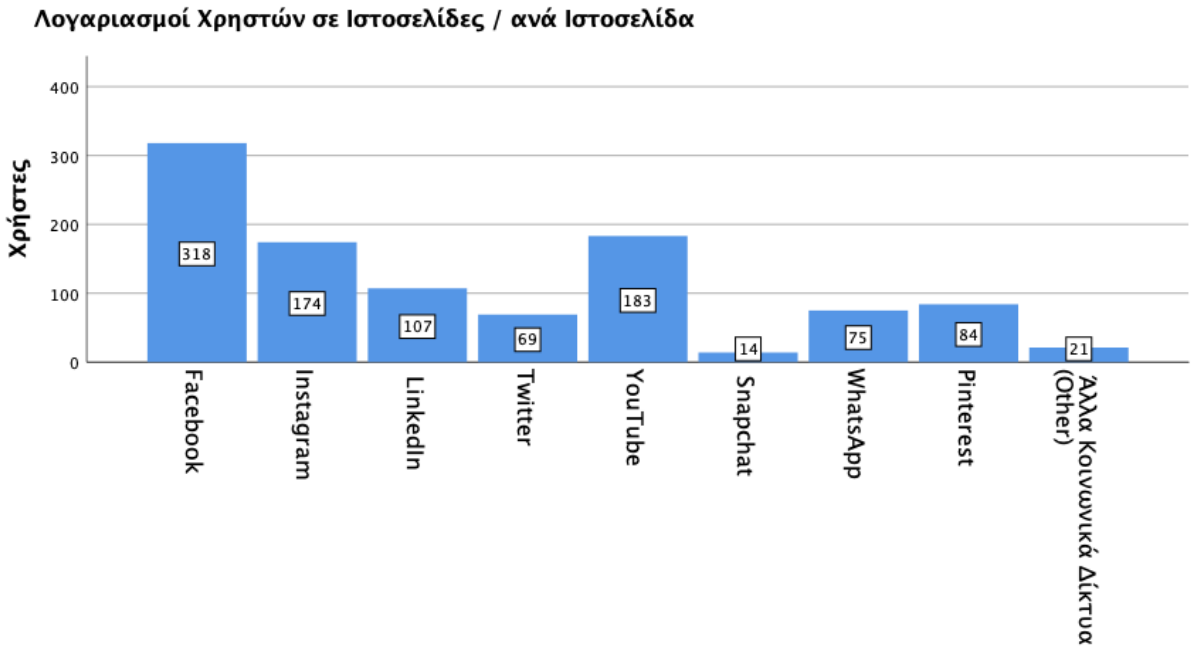
Σύμφωνα με τους Πίνακας: 10 Πίνακας: 11 & Γράφημα: 9, φαίνεται ότι οι χρήστες σε ένα ποσοστό 95,2%, διατηρούν λογαριασμό στο Facebook, με το αμέσως επόμενο ποσοστό να είναι ένα 54,8% και αφορά το YouTube. Οι αριθμοί των λογαριασμών δεν συμφωνούν με τους χρήστες καθώς αποτυπώνεται το σύνολο των λογαριασμών ανά χρήστη.

**Λογαριασμοί Χρηστών/ανά Ιστοσελίδα**

| Varname | | Responses N | Responses Percent | Percent of Cases |
|---|---|---|---|---|
| Λογαριασμοί ανά Ιστοσελίδα [a] | Χρήστης Facebook | 318 | 30.4% | 95.2% |
| | Χρήστης Instagram | 174 | 16.7% | 52.1% |
| | Χρήστης LinkedIn | 107 | 10.2% | 32.0% |
| | Χρήστης Twitter | 69 | 6.6% | 20.7% |
| | Χρήστης YouTube | 183 | 17.5% | 54.8% |
| | Χρήστης Snapchat | 14 | 1.3% | 4.2% |
| | Χρήστης WhatsApp | 75 | 7.2% | 22.5% |
| | Χρήστης Pinterest | 84 | 8.0% | 25.1% |
| | Χρήστες Άλλων Κοινωνικών Δικτύων (Other) | 21 | 2.0% | 6.3% |
| Total | | 1045 | 100.0% | 312.9% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 11 Λογαριασμοί Χρηστών ανά Ιστοσελίδα*




*Γράφημα: 9 Λογαριασμοί Χρηστών Ανά Ιστοσελίδα Bar*

### 5.1.11 Πόσοι λογαριασμοί ανά συμμετέχοντα σε Ιστοσελίδες.

Οι Συμμετέχοντες σε Ιστοσελίδες Κοινωνικής Δικτύωσης, σύμφωνα με τα στοιχεία που παρατίθενται στον Πίνακας: 12& Πίνακας: 13 & Γράφημα: 10 φαίνεται ανά περίπτωση να διατηρούν από ένα (1 λογαριασμό) έως και εννέα (9) διαφορετικούς λογαριασμούς. Το μεγαλύτερο ποσοστό των συμμετεχόντων διατηρεί λογαριασμό σε δύο (2) διαφορετικές ΙΚΔ σε ποσοστό 27,2% και 91 άτομα, ενώ υπάρχει και ένας συμμετέχων, ο οποίος διατηρεί λογαριασμό σε εννέα (9) Ιστοσελίδες Κοινωνικής Δικτύωσης.

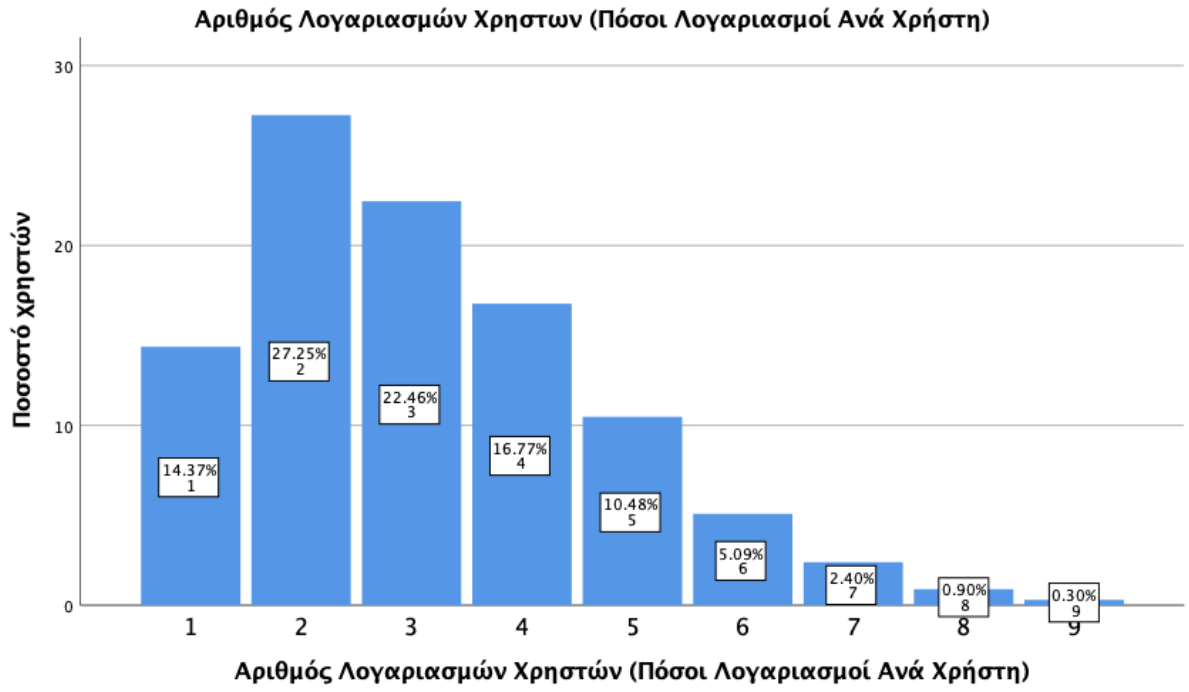
**Σύνοψη**

| | N | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|
| Αριθμός Λογαριασμών Χρηστών (Πόσοι Λογαριασμοί Ανά Χρήστη) | 334 | 1 | 9 | 3.13 | 1.612 |
| Valid N (listwise) | 334 | | | | |

*Πίνακας: 12 Πόσοι Λογαριασμοί ανά Χρήστη*

| Αριθμός Λογαριασμών Χρηστών (Πόσοι Λογαριασμοί Ανά Χρήστη) | | | | | |
|---|---|---|---|---|---|
| | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | 1 | 48 | 14.4 | 14.4 | 14.4 |
| | 2 | 91 | 27.2 | 27.2 | 41.6 |
| | 3 | 75 | 22.5 | 22.5 | 64.1 |
| | 4 | 56 | 16.8 | 16.8 | 80.8 |
| | 5 | 35 | 10.5 | 10.5 | 91.3 |
| | 6 | 17 | 5.1 | 5.1 | 96.4 |
| | 7 | 8 | 2.4 | 2.4 | 98.8 |
| | 8 | 3 | .9 | .9 | 99.7 |
| | 9 | 1 | .3 | .3 | 100.0 |
| | Total | 334 | 100.0 | 100.0 | |

*Πίνακας: 13 Αριθμός Λογαριασμών ανά Χρήστη*




*Γράφημα: 10 Ποσοστά Χρηστών και αριθμός Λογαριασμών*

### 5.1.12 Λόγοι Χρήσης Ιστοσελίδων Κοινωνικής Δικτύωσης

Οι λόγοι χρήσης των ΙΚΔ αποτυπώνονται στους Πίνακας: 14, Πίνακας: 15 & Γράφημα: 11, οι οποίοι φαίνεται να αφορούν στο μεγαλύτερο μέρος των περιπτώσεων “Ενημέρωση & Επικοινωνία με φίλους” και ο αμέσως επόμενος λόγος είναι η Διασκέδαση. Και στο σημείο αυτό καθώς είναι πολλαπλή επιλογή οι περιπτώσεις είναι περισσότερες.

**Σύνοψη**

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $LogosXrisisKoinonikonDiktyon[a] | 334 | 100.0% | 0 | 0.0% | 334 | 100.0% |

a. Dichotomy group tabulated at value 1.

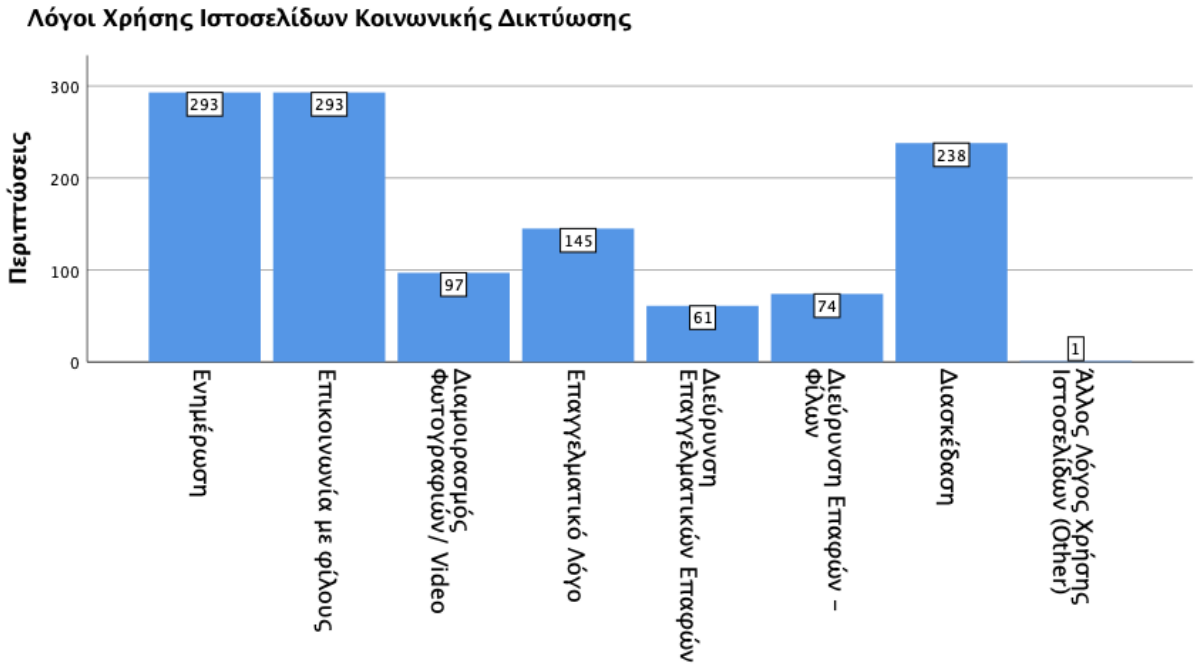
*Πίνακας: 14 Λόγοι Χρήσης Ιστοσελίδων Κοινωνικών Δικτύων – Χρήστες*

**Λόγοι Χρήσης Ιστοσελίδων Κοινωνικής Δικτύωσης**

| | | Responses | | Percent of Cases |
|---|---|---|---|---|
| | | N | Percent | |
| $LogosXrisisKoinonikonDiktyon[a] | Ενημέρωση | 293 | 24.4% | 87.7% |
| | Επικοινωνία με φίλους | 293 | 24.4% | 87.7% |
| | Διαμοιρασμός Φωτογραφιών/ Video | 97 | 8.1% | 29.0% |
| | Επαγγελματικό Λόγο | 145 | 12.1% | 43.4% |
| | Διεύρυνση Επαγγελματικών Επαφών | 61 | 5.1% | 18.3% |
| | Διεύρυνση Επαφών - Φίλων | 74 | 6.2% | 22.2% |
| | Διασκέδαση | 238 | 19.8% | 71.3% |
| | Άλλος Λόγος Χρήσης Ιστοσελίδων (Other) | 1 | 0.1% | 0.3% |
| Total | | 1202 | 100.0% | 359.9% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 15 Λόγοι Χρήσης Κοινωνικών Δικτύων (Πολλαπλή επιλογή) Σύνολα Περιπτώσεων*




*Γράφημα: 11 Λόγοι Χρήσης Κοινωνικών Δικτύων – Περιπτώσεις ανά Λόγο*

### 5.1.13 Συχνότητα Σύνδεσης σε Ιστοσελίδες Κοινωνικής Δικτύωσης

Στον Πίνακας: 16 & Γράφημα: 12 παρατίθενται τα περιγραφικά στατιστικά στοιχεία της Συνδεσιμότητας των Χρηστών ανά ΙΚΔ από τα οποία προκύπτει ότι με βάση τον Μέσο Όρο οι συμμετέχοντες στο Facebook φαίνεται να συνδέονται περισσότερο από κάθε άλλη ΙΚΔ, με την αμέσως επόμενη  το YouTube και να ακολουθεί το Instagram με σχεδόν τον μισό δαπανηθέντα χρόνο των χρηστών στο Facebook.

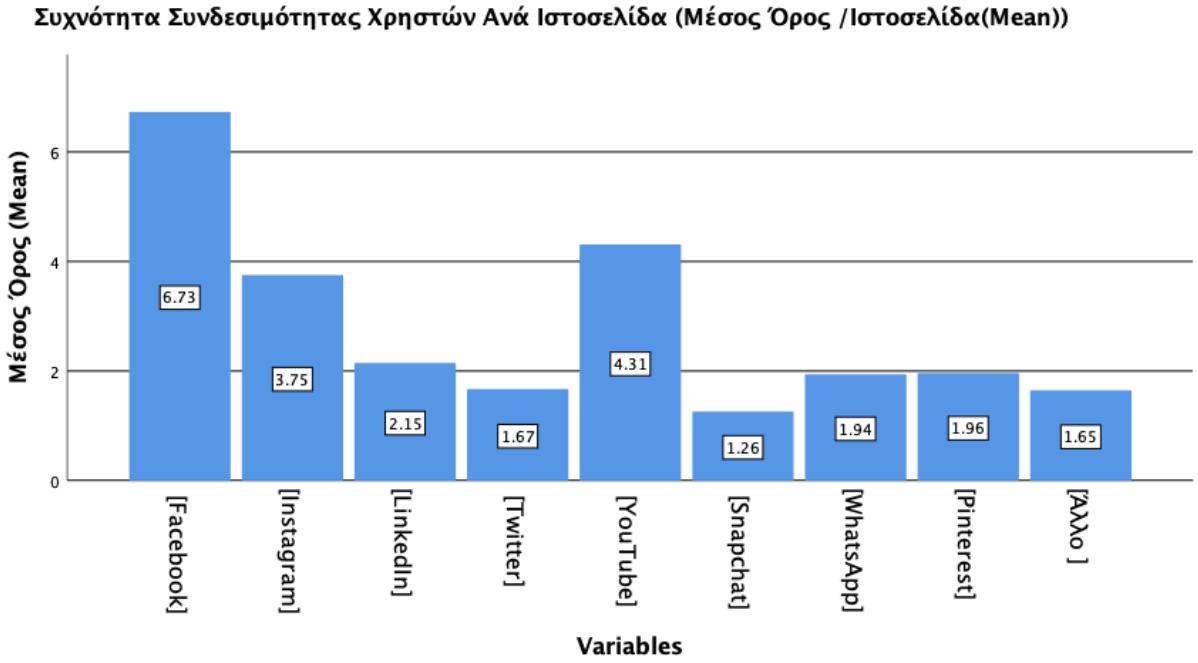
**Descriptive Statistics**

| | N | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Facebook] | 334 | 1 | 10 | 6.73 | 2.155 |

| | | | | | |
|---|---|---|---|---|---|
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Instagram] | 334 | 1 | 10 | 3.75 | 2.994 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [LinkedIn] | 334 | 1 | 10 | 2.15 | 2.007 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Twitter] | 334 | 1 | 10 | 1.67 | 1.657 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [YouTube] | 334 | 1 | 10 | 4.31 | 2.630 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Snapchat] | 334 | 1 | 9 | 1.26 | 1.049 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [WhatsApp] | 334 | 1 | 10 | 1.94 | 2.002 |

| | | | | | |
|---|---|---|---|---|---|
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Pinterest] | 334 | 1 | 10 | 1.96 | 1.768 |
| Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε? [Άλλο] | 334 | 1 | 10 | 1.65 | 1.793 |
| Valid N (listwise) | 334 | | | | |

*Πίνακας: 16 Συχνότητα Σύνδεσης Χρηστών Ανά ΙΚΔ*




*Γράφημα: 12 Μέσος Όρος Συνδεσιμότητας / ΙΚΔ Χρηστών*

### 5.1.14 Χρήση Ιστοσελίδων Κοινωνικής Δικτύωσης (SNS Usage Scale)

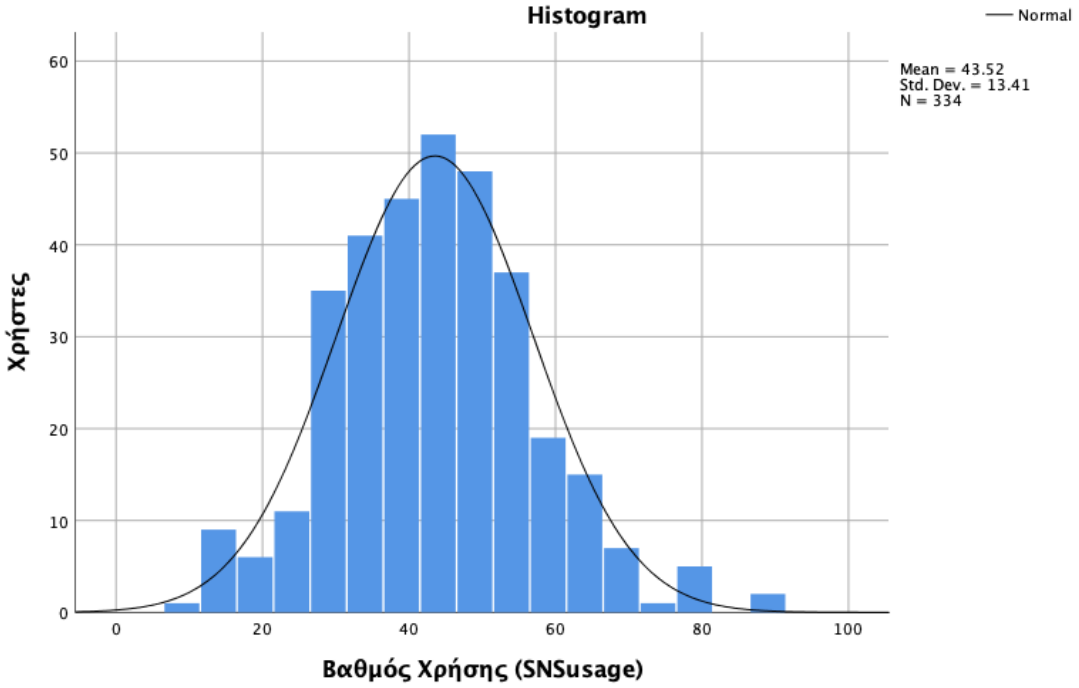
Στον Πίνακας: 17 παρατίθενται τα στοιχεία αναφορικά με τον βαθμό χρήσης των ΙΚΔ των συμμετεχόντων χρηστών και στο Γράφημα: 13 αποτυπώνεται το Ιστόγραμμα της κατανομής (Κανονική Κατανομή).

**Descriptive Statistics**

| | N | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Βαθμός Χρήσης ΙΚΔ | 334 | 9 | 90 | 43.52 | 13.410 |
| Valid N (listwise) | 334 | | | | |

*Πίνακας: 17 Βαθμός Χρήσης ΙΚΔ Χρηστών*




*Γράφημα: 13 Βαθμός Χρήσης ΙΚΔ*

### 5.1.15 Κίνδυνοι σε Κοινωνικά Δίκτυα – Αντίληψη Κινδύνων

**Σύνοψη**

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| $GnosiKindynon[a] | 334 | 100.0% | 0 | 0.0% | 334 | 100.0% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 18 Οι πιο Κοινοί Κίνδυνοι- Γνώση Κινδύνων*

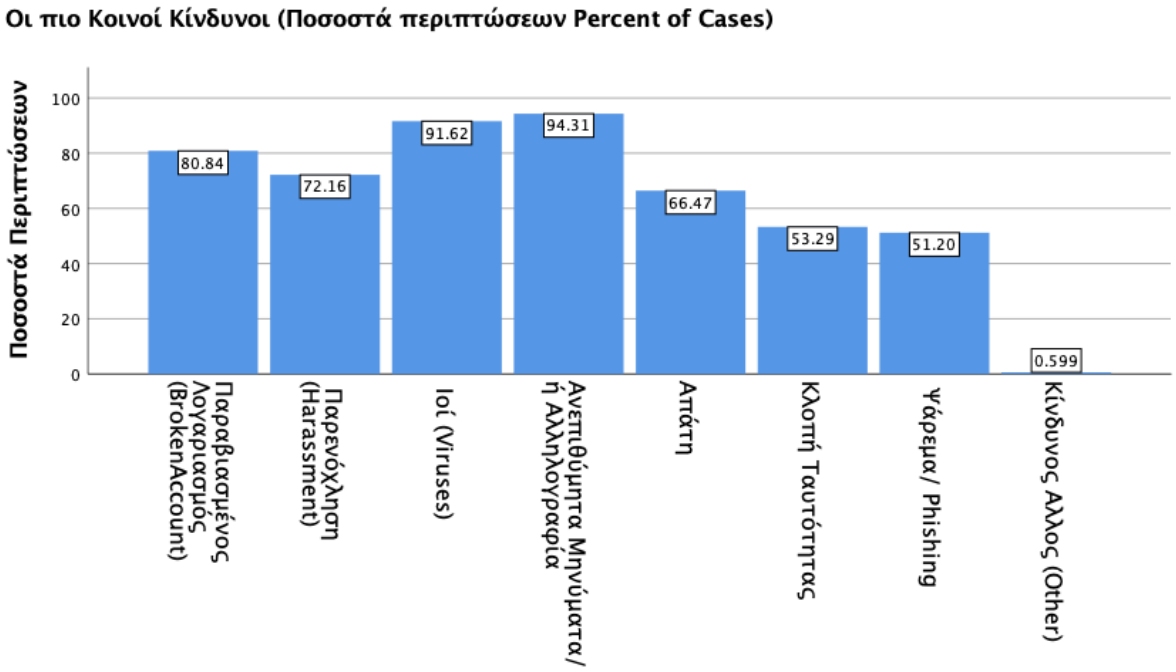
Από τα στοιχεία που παρατίθενται στους Πίνακας: 18 & Πίνακας: 19 και στο αντίστοιχο Γράφημα: 14, προκύπτει ότι οι χρήστες στην πλειοψηφία τους γνωρίζουν τους παρατιθέμενους κινδύνους. Τα ποσοστά αντίληψης (γνώσης) κινδύνων όπως οι ιοί και τα ανεπιθύμητα μηνύματα ξεπερνούν το 90%. Μικρότερα ωστόσο ποσοστά εμφανίζουν κίνδυνοι όπως το Ψάρεμα/Phishing και η κλοπή ταυτότητας που πάντως ξεπερνούν σε

ποσοστά το 50%. Που υποδηλώνει ότι οι χρήστες είναι ενήμεροι. Και στο σημείο αυτό καθώς είναι πολλαπλή επιλογή οι περιπτώσεις είναι περισσότερες

| Αντίληψη Κινδύνων (Συχνότητες) | | | | |
|---|---|---|---|---|
| | | Responses | | Percent of Cases |
| | | N | Percent | |
| $GnosiKindynon[a] | Παραβιασμένος Λογαριασμός (Broken Account) | 270 | 15.8% | 80.8% |
| | Παρενόχληση (Harassment) | 241 | 14.1% | 72.2% |
| | Ιοί (Viruses) | 306 | 17.9% | 91.6% |
| | Ανεπιθύμητα Μηνύματα/ ή Αλληλογραφία | 315 | 18.5% | 94.3% |
| | Απάτη | 222 | 13.0% | 66.5% |
| | Κλοπή Ταυτότητας | 178 | 10.4% | 53.3% |
| | Ψάρεμα/ Phishing | 171 | 10.0% | 51.2% |
| | Κίνδυνος Άλλος (Other) | 2 | 0.1% | 0.6% |
| Total | | 1705 | 100.0% | 510.5% |

a. Dichotomy group tabulated at value 1.

*Πίνακας: 19 Οι πιο Κοινοί Κίνδυνοι _ Συχνότητες*




*Γράφημα: 14 Κοινοί Κίνδυνοι - Ποσοστά περιπτώσεων*

### 5.1.16 Έκθεση σε Κίνδυνο

Στον Πίνακας: 20 & Πίνακας: 21 & Γράφημα: 15 παρατίθενται τα στοιχεία της έκθεσης σε κίνδυνο των συμμετεχόντων. Το μεγαλύτερο μέρος των συμμετεχόντων φαίνεται να έχει έρθει αντιμέτωπος με κάποιον κίνδυνο, με το μεγαλύτερο ποσοστό 26,6% των συμμετεχόντων να έχει αντιμετωπίσει τουλάχιστον 2 κινδύνους στην αλληλεπίδρασή του στις ΙΚΔ που συμμετέχει. Το αμέσως μεγαλύτερο ποσοστό 21,3% είναι αυτό που αφορά 3 διαφορετικούς κινδύνους. Το ποσοστό που δεν έχει έρθει ποτέ αντιμέτωπο με κάποιον κίνδυνο ανέρχεται στο 11,7%.

**Descriptive Statistics**

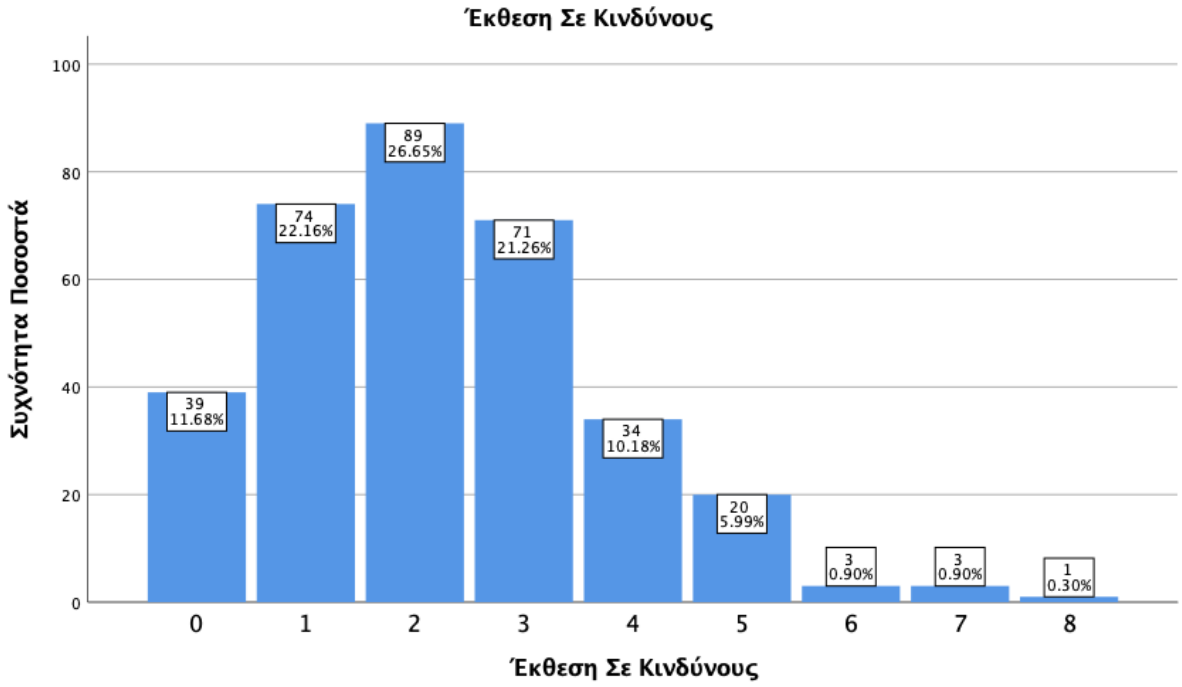
| | N | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|
| Έκθεση Σε Κινδύνους | 334 | 0 | 8 | 2.24 | 1.508 |
| Valid N (listwise) | 334 | | | | |

*Πίνακας: 20 Έκθεση σε Κίνδυνο Μέσος Όρος*

**Έκθεση Σε Κινδύνους**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 0 | 39 | 11.7 | 11.7 | 11.7 |
| | 1 | 74 | 22.2 | 22.2 | 33.8 |
| | 2 | 89 | 26.6 | 26.6 | 60.5 |
| | 3 | 71 | 21.3 | 21.3 | 81.7 |
| | 4 | 34 | 10.2 | 10.2 | 91.9 |
| | 5 | 20 | 6.0 | 6.0 | 97.9 |
| | 6 | 3 | .9 | .9 | 98.8 |
| | 7 | 3 | .9 | .9 | 99.7 |
| | 8 | 1 | .3 | .3 | 100.0 |
| | Total | 334 | 100.0 | 100.0 | |

*Πίνακας: 21 Έκθεση σε Κινδύνους (0 κανένας- & 8 κίνδυνοι)*



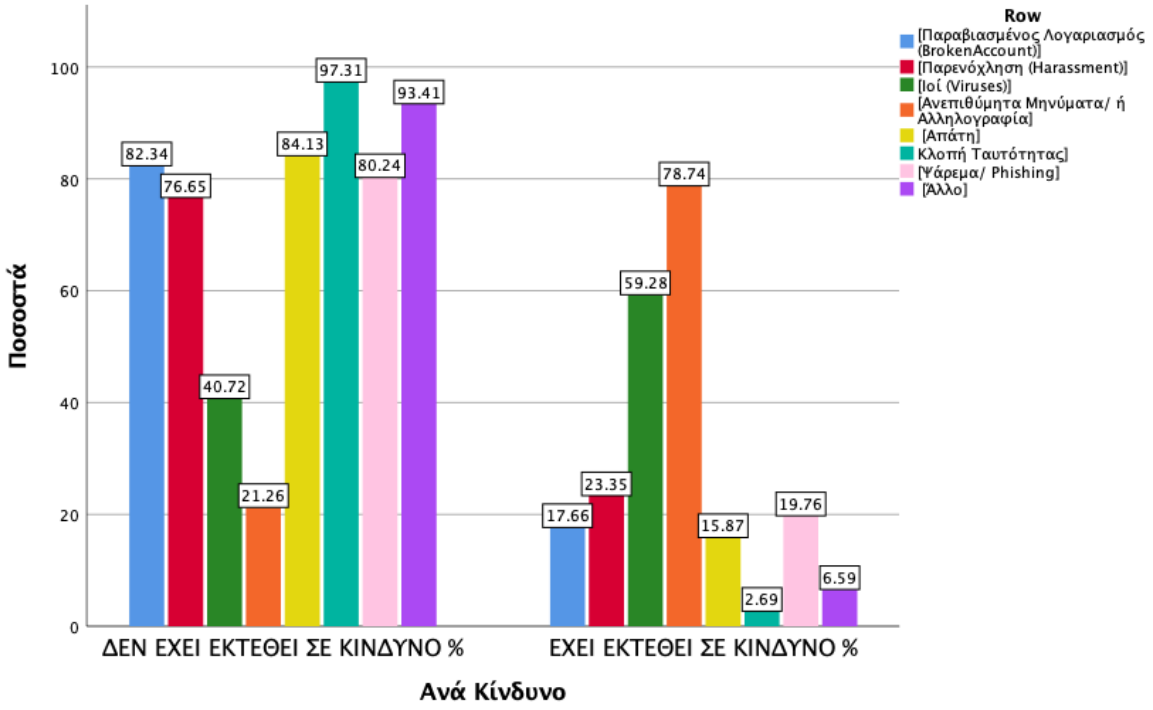

*Γράφημα: 15 Έκθεση σε Κινδύνους*

Στον Πίνακας: 22 & Πίνακας: 20 & Γράφημα: 16 που ακολουθούν παρατίθενται στοιχεία σύμφωνα με τις απαντήσεις των συμμετεχόντων αναφορικά με τους κινδύνους με τους οποίους έχουν έρθει αντιμέτωποι. Τα ποσοστά εμφανίζονται ανά κίνδυνο. Το μεγαλύτερο ποσοστό 78,7% έχει αντιμετωπίσει τον κίνδυνο των ανεπιθύμητων μηνυμάτων και το αμέσως επόμενο ποσοστό 59,3% αναφέρεται σε ιούς. Αρκετά υψηλό ωστόσο εμφανίζεται και το ποσοστό 23,4% της Παρενόχλησης.

| | ΟΧΙ<br>Row N % | ΝΑΙ<br>Row N % |
|---|---|---|
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Παραβιασμένος Λογαριασμός (Broken Account)] | 82.3% | 17.7% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Παρενόχληση (Harassment)] | 76.6% | 23.4% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Ιοί (Viruses)] | 40.7% | 59.3% |

| | | |
|---|---|---|
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Ανεπιθύμητα Μηνύματα/ ή Αλληλογραφία] | 21.3% | 78.7% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Απάτη] | 84.1% | 15.9% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Κλοπή Ταυτότητας] | 97.3% | 2.7% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Ψάρεμα/ Phishing] | 80.2% | 19.8% |
| Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους? [Άλλο] | 93.4% | 6.6% |

*Πίνακας: 22 Έκθεση Συμμετεχόντων σε Κίνδυνο/Κίνδυνο*




*Γράφημα: 16 Έκθεση σε Κίνδυνο/ανά Κίνδυνο Ναι Όχι*

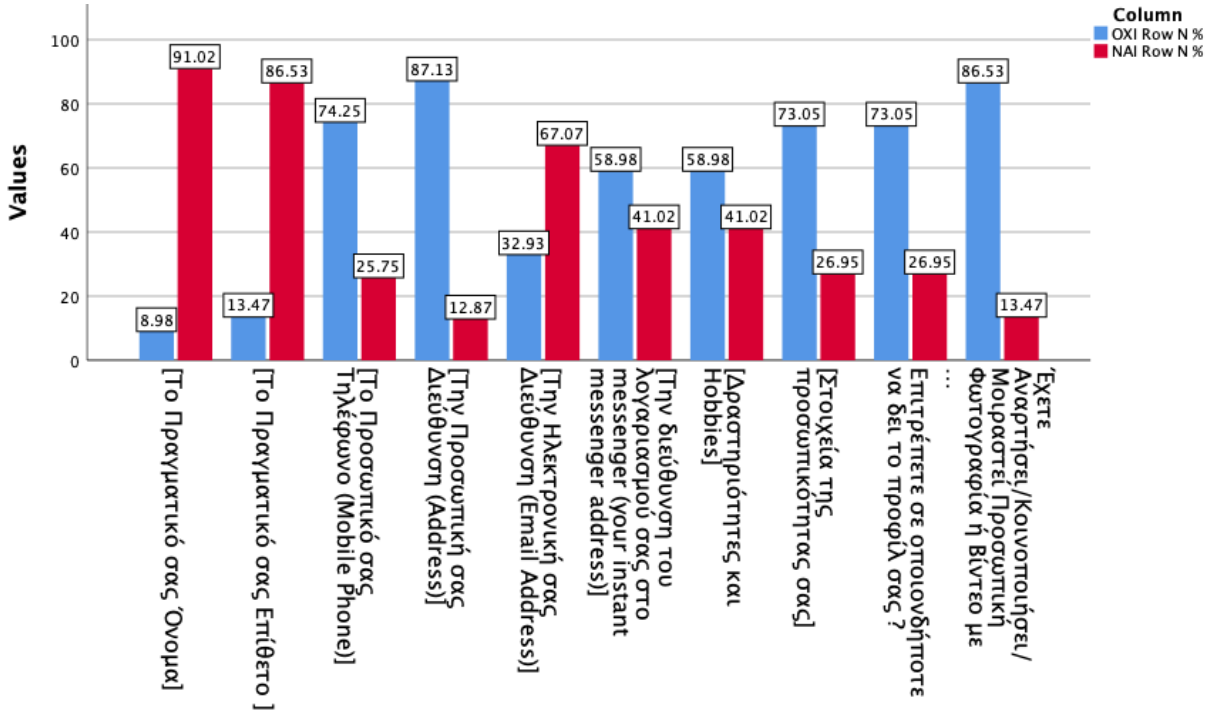
### 5.1.17 Πρακτικές Χρήσης Διαμοιρασμού Πληροφοριών σε Ιστοσελίδες Κοινωνικής Δικτύωσης (Personal Information Sharing Practices (PISP)

Στον Πίνακας: 23 & Γράφημα: 17 παρατίθενται στοιχεία Προσωπικών Πληροφοριών που οι συμμετέχοντες αποκαλύπτουν στις ΙΚΔ. Τα ποσοστά των αποκαλυπτομένων προσωπικών πληροφοριών είναι πολύ μεγάλα. Το πραγματικό τους Όνομα και Επίθετο αποκαλύπτουν ένα 91% των συμμετεχόντων και 86,5% αντίστοιχα. Ενδιαφέρον επίσης παρουσιάζει ότι ένα ποσοστό της τάξης του 25,7% ενσωματώνει και τον αριθμό του Κινητό του τηλεφώνου.

| | ΟΧΙ<br>Row N % | ΝΑΙ<br>Row N % |
|---|---|---|
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Το Πραγματικό σας Όνομα] | 9.0% | 91.0% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Το Πραγματικό σας Επίθετο ] | 13.5% | 86.5% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Το Προσωπικό σας Τηλέφωνο (Mobile Phone)] | 74.3% | 25.7% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Την Προσωπική σας Διεύθυνση (Address)] | 87.1% | 12.9% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Την Ηλεκτρονική σας Διεύθυνση (Email Address)] | 32.9% | 67.1% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Την διεύθυνση του λογαριασμού σας στο messenger (your instant messenger address)] | 59.0% | 41.0% |

| | | |
|---|---|---|
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Δραστηριότητες και Hobbies] | 59.0% | 41.0% |
| Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε? [Στοιχεία της προσωπικότητας σας] | 73.1% | 26.9% |
| Επιτρέπετε σε οποιονδήποτε να δει το προφίλ σας ? | 73.1% | 26.9% |
| Έχετε Αναρτήσει/Κοινοποιήσει/ Μοιραστεί Προσωπική Φωτογραφία ή Βίντεο με άτομα που δεν γνωρίζετε? | 86.5% | 13.5% |

*Πίνακας: 23 Πρακτικές Χρήσης Διαμοιρασμού Προσωπικών Πληροφοριών*




*Γράφημα: 17 Διαμοιρασμός Προσωπικών Πληροφοριών σε ΙΚΔ ΝΑΙ-ΟΧΙ*

### 5.1.18 Συμπεριφορές Χρηστών ΙΚΔ σε Κοινωνικά Δίκτυα ( Παράγοντες Έκθεσης)

Στον Πίνακας: 24 παρατίθενται στοιχεία αναφορικά με τις συμπεριφορές των χρηστών στις ΙΚΔ

| Descriptive Statistics | | | | | |
|---|---|---|---|---|---|
| | N | Minimum | Maximum | Mean | Std. Deviation |
| Risk Averseness Total | 334 | 5 | 25 | 15.41 | 3.912 |
| Trust Total | 334 | 4 | 20 | 8.89 | 3.378 |

| | | | | | |
|---|---|---|---|---|---|
| Privacy Behavior scale Total | 334 | 6 | 30 | 20.15 | 5.388 |
| Privacy Concern Scale Total | 334 | 3 | 15 | 11.49 | 2.577 |
| Perceived Control of Information Total | 334 | 3 | 15 | 8.84 | 2.890 |
| Identity Information Disclosure Scale Total | 334 | 4 | 20 | 12.88 | 3.360 |
| Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | 334 | 1 | 5 | 4.50 | .859 |
| Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | 334 | 1 | 5 | 4.16 | .966 |
| Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | 334 | 1 | 5 | 2.25 | 1.176 |
| Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | 334 | 1 | 5 | 2.36 | 1.116 |
| Valid N (listwise) | 334 | | | | |

*Πίνακας: 24 Συμπεριφορές Χρηστών ΙΚΔ*

Στον Πίνακας: 25 παρατίθενται στοιχεία σχετικά με τις συμπεριφορές στις ΙΚΔ μεταξύ ανδρών και γυναικών των συμμετεχόντων. Παρατηρείται ότι οι Μέσοι Όροι μεταξύ των δύο διαφορετικών φύλων παρουσιάζουν μικρές διαφορές μεταξύ τους.

**Report**

| Φύλο | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Άνδρας | | | Γυναίκα | | | Total | | |
| Mean | N | Std. Deviation | Mean | N | Std. Deviation | Mean | N | Std. Deviation |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Risk Averseness Total | 15.45 | 110 | 4.146 | 15.39 | 224 | 3.802 | 15.41 | 334 | 3.912 |
| Trust Total | 8.79 | 110 | 3.527 | 8.94 | 224 | 3.309 | 8.89 | 334 | 3.378 |
| Privacy Behavior scale Total | 20.60 | 110 | 5.607 | 19.93 | 224 | 5.276 | 20.15 | 334 | 5.388 |
| Privacy Concern Scale Total | 11.18 | 110 | 2.984 | 11.63 | 224 | 2.345 | 11.49 | 334 | 2.577 |
| Perceived Control of Information Total | 8.43 | 110 | 3.117 | 9.05 | 224 | 2.757 | 8.84 | 334 | 2.890 |
| Identity Information Disclosure Scale Total | 12.99 | 110 | 3.264 | 12.83 | 224 | 3.413 | 12.88 | 334 | 3.360 |
| Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | 4.39 | 110 | .920 | 4.55 | 224 | .824 | 4.50 | 334 | .859 |
| Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | 3.98 | 110 | 1.049 | 4.25 | 224 | .912 | 4.16 | 334 | .966 |
| Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | 2.35 | 110 | 1.169 | 2.21 | 224 | 1.180 | 2.25 | 334 | 1.176 |
| Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | 2.21 | 110 | 1.076 | 2.43 | 224 | 1.130 | 2.36 | 334 | 1.116 |

*Πίνακας: 25 Συμπεριφορές Χρηστών σε ΙΚΔ ανά φύλο*

## 5.2 Επαγωγική Ανάλυση που Αναφέρεται σε Ερωτήματα/ Υποθέσεις

Στην διαδικασία της επαγωγικής ανάλυσης, θα ελεγχθεί η συσχέτιση των διάφορων μεταβλητών και θα ελεγχθούν τα επιμέρους ερευνητικά ερωτήματα, με την χρήση του εκάστοτε κατάλληλου test συσχέτισης (Pearson ή Spearman) ανάλογα με τις μεταβλητές. Επίσης θα ελεγχθεί και ο συσχετισμός των διαφορών, μεταξύ των διαφόρων ομάδων των συμμετεχόντων – Φύλο, Ηλικία, Μορφωτικό Επίπεδο, συσχετιζόμενα με τα χαρακτηριστικά συμπεριφορές (παράγοντες) που μετρήθηκαν με αντίστοιχα test για τον εντοπισμό πιθανής αιτιότητας και επίσης σε σχέση με την έκθεση σε Κίνδυνο.

### 5.2.1 Έλεγχος Συσχέτισης (Correlation) Test Pearson ή Spearman

Σε περιπτώσεις μεταβλητών, που είναι συνεχείς, διαστήματος ή λόγου, ή στην περίπτωση της μιας συνεχούς και της άλλης διχοτομικής (ΝΑΙ-ΟΧΙ, 1 – 2 κ.α.), χρησιμοποιούμε δείκτη Pearson. Προϋποθέσεις: Για την κάθε κατηγορία της διχοτομικής μεταβλητής να υπάρχει α. Κανονική Κατανομή και β. Ομοιογένεια Διακύμανσης. Για τον έλεγχο της ομοιογένειας διακύμανσης μπορεί να χρησιμοποιηθεί το Levene's test.
Στην περίπτωση συνεχούς μεταβλητής και κατηγορικής μεταβλητής ή όταν δεν υπάρχει κανονική κατανομή τότε χρησιμοποιείται το test Spearman Rho.

### 5.2.2 Συσχετισμοί Pearson (r) & Spearman's Rho ($r_s$) ανά μεταβλητή

#### 5.2.2.1 Συμπεριφορές Χρηστών σε ΙΚΔ - Συσχετισμοί

##### 5.2.2.1.1 Ανάληψη Κινδύνου Risk Taking

**Ερευνητικό Ερώτημα:** Η Ανάληψη Κινδύνου "Risk Averseness" στις ΙΚΔ σχετίζεται με το Φύλο.
Η μεταβλητή "Risk Averseness" ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Tests of Normality

Πίνακας: 75 & Γράφημα: 18 & Γράφημα: 19 & Γράφημα: 20 & Γράφημα: 21 Κεφάλαιο 5.3).

**Correlations**

| | | Risk Averseness Total | Φύλο |
|---|---|---|---|
| Risk Averseness Total | Pearson Correlation | 1 | -.008 |
| | Sig. (2-tailed) | | .885 |
| | N | 334 | 334 |
| Φύλο | Pearson Correlation | -.008 | 1 |
| | Sig. (2-tailed) | .885 | |
| | N | 334 | 334 |

*Πίνακας: 26 Pearson correlation Risk Averseness & Φύλο*

Τα αποτελέσματα ελέγχου Pearson's r έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Risk Averseness και Φύλο(r = -0,008, p = 0,885).

**Ερευνητικό Ερώτημα:** Η Ανάληψη Κινδύνου "Risk Averseness" στις ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Risk Averseness Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Risk Averseness Total | Correlation Coefficient | 1.000 | -.110* |
| | | Sig. (2-tailed) | . | .044 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | -.110* | 1.000 |
| | | Sig. (2-tailed) | .044 | . |
| | | N | 334 | 334 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Πίνακας: 27 Risk Averseness & Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Risk Averseness και ηλικία ($r_s$ = -0,110*, p =0,44)

**Ερευνητικό Ερώτημα:** Η Ανάληψη Κινδύνου "Risk Averseness" στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο.

| Correlations | | | | |
|---|---|---|---|---|
| | | | Risk Averseness Total | Εκπαίδευση |
| Spearman's rho | Risk Averseness Total | Correlation Coefficient | 1.000 | -.077 |
| | | Sig. (2-tailed) | . | .162 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.077 | 1.000 |
| | | Sig. (2-tailed) | .162 | . |
| | | N | 334 | 334 |

*Πίνακας: 28 Risk Averseness & Εκπαίδευση/ Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Risk Averseness και Μορφωτικό Επίπεδο (rs = -0,77, p =0,162).

#### 5.2.2.1.2 Εμπιστοσύνη "Trust"

**Ερευνητικό Ερώτημα:** Η Εμπιστοσύνη/Trust στις Εταιρείες ΙΚΔ σχετίζεται με το Φύλο Η μεταβλητή "Trust " ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 77 & Γράφημα: 26 & Γράφημα: 27, Κεφάλαιο 5.3).

| Correlations | | | | |
|---|---|---|---|---|
| | | | Trust Total | Φύλο (Αριθμός) |
| Spearman's rho | Trust Total | Correlation Coefficient | 1.000 | .024 |
| | | Sig. (2-tailed) | . | .656 |
| | | N | 334 | 334 |
| | Φύλο (Αριθμός) | Correlation Coefficient | .024 | 1.000 |
| | | Sig. (2-tailed) | .656 | . |
| | | N | 334 | 334 |

*Πίνακας: 29 Spearman's Rho Correlation Trust & Φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Εμπιστοσύνη "Trust" και Φύλο ($r_s$ = 0,024, p =0,656).

**Ερευνητικό Ερώτημα:** Η Εμπιστοσύνη/Trust στις Εταιρείες ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Trust Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Trust Total | Correlation Coefficient | 1.000 | .023 |
| | | Sig. (2-tailed) | . | .680 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .023 | 1.000 |
| | | Sig. (2-tailed) | .680 | . |
| | | N | 334 | 334 |

*Πίνακας: 30 Spearman's Rho Correlation Trust & Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Εμπιστοσύνη "Trust" και Ηλικία ($r_s$ = 0,023, p =0,680).

**Ερευνητικό Ερώτημα:** Η Εμπιστοσύνη/Trust στις Εταιρείες ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο

**Correlations**

| | | | Trust Total | Εκπαίδευση (Αριθμός) |
|---|---|---|---|---|
| Spearman's rho | Trust Total | Correlation Coefficient | 1.000 | -.109* |
| | | Sig. (2-tailed) | . | .047 |
| | | N | 334 | 334 |
| | Εκπαίδευση (Αριθμός) | Correlation Coefficient | -.109* | 1.000 |
| | | Sig. (2-tailed) | .047 | . |
| | | N | 334 | 334 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Πίνακας: 31 Spearman's Rho Correlation Trust & Εκπαίδευση/Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Trust και Μορφωτικό Επίπεδο ($r_s$ = -0,109*, p =0,047)

#### 5.2.2.1.3 Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior"

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior στις ΙΚΔ σχετίζεται με το Φύλο

Η μεταβλητή "Privacy Behavior " ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 79 & Γράφημα: 31 & Γράφημα: 32 & Γράφημα: 33 & Γράφημα: 34, Κεφάλαιο 5.3).

**Correlations**

| | | Privacy Behavior scale Total | Φύλο |
|---|---|---|---|
| Privacy Behavior scale Total | Pearson Correlation | 1 | -.058 |
| | Sig. (2-tailed) | | .288 |
| | N | 334 | 334 |
| Φύλο | Pearson Correlation | -.058 | 1 |
| | Sig. (2-tailed) | .288 | |
| | N | 334 | 334 |

*Πίνακας: 32 Pearson's Correlation Privacy Behavior και Φύλο*

Τα αποτελέσματα ελέγχου Pearson's r έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Privacy Behavior και Φύλο (r = -0,058, p =0,288).

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior" στις ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Privacy Behavior scale Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Privacy Behavior scale Total | Correlation Coefficient | 1.000 | .261** |
| | | Sig. (2-tailed) | . | .000 |
| | | N | 334 | 334 |

| | | | | |
|---|---|---|---|---|
| | Ηλικία | Correlation Coefficient | .261** | 1.000 |
| | | Sig. (2-tailed) | .000 | . |
| | | N | 334 | 334 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | |

*Πίνακας: 33 Pearson's Correlation Privacy Behavior& Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Privacy Behavior και Ηλικία ($r_s$ = -0,0261**, p < 0,01)

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior" στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο.

**Correlations**

| | | | Privacy Behavior scale Total | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Privacy Behavior scale Total | Correlation Coefficient | 1.000 | -.044 |
| | | Sig. (2-tailed) | . | .421 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.044 | 1.000 |
| | | Sig. (2-tailed) | .421 | . |
| | | N | 334 | 334 |

*Πίνακας: 34 Spearman's Rho Correlation Privacy Behavior και Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Privacy Behavior και Μορφωτικό Επίπεδο ($r_s$ = -0,044, p = 0,421).

#### 5.2.2.1.4 Ανησυχία για την Ιδιωτικότητα/Απόρρητο "Privacy Concern"

**Ερευνητικό Ερώτημα :** Η Συμπεριφορά "Privacy Concern" στις ΙΚΔ σχετίζεται με το Φύλο.

Η μεταβλητή "Privacy Concern " ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 81 & Γράφημα: 39 & Γράφημα: 40 & Γράφημα: 41 & Γράφημα: 42, Κεφάλαιο 5.3).

**Correlations**

| | | | Privacy Concern Scale Total | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Privacy Concern Scale Total | Correlation Coefficient | 1.000 | .055 |
| | | Sig. (2-tailed) | . | .316 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | .055 | 1.000 |
| | | Sig. (2-tailed) | .316 | . |
| | | N | 334 | 334 |

*Πίνακας: 35 Spearman's Rho Correlation Privacy Concern Scale και Φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Privacy Concern και Φύλο ($r_s$ = 0,055, p <=0,316).

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Privacy Concern" στις ΙΚΔ σχετίζεται με την Ηλικία.

**Correlations**

| | | | Privacy Concern Scale Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Privacy Concern Scale Total | Correlation Coefficient | 1.000 | .106 |
| | | Sig. (2-tailed) | . | .052 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .106 | 1.000 |
| | | Sig. (2-tailed) | .052 | . |
| | | N | 334 | 334 |

*Πίνακας: 36 Spearman's Correlation Privacy Concern και Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Privacy Concern και Ηλικία ($r_s$ = 0,106, p = 0,052).

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Privacy Concern" στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο.

**Correlations**

| | | | Privacy Concern Scale Total | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Privacy Concern Scale Total | Correlation Coefficient | 1.000 | .043 |
| | | Sig. (2-tailed) | . | .435 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | .043 | 1.000 |
| | | Sig. (2-tailed) | .435 | . |
| | | N | 334 | 334 |

*Πίνακας: 37 Spearman Rho Correlation Privacy Concern & Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Privacy Concern Scale και Εκπαίδευση / Μορφωτικό Επίπεδο ($r_s$ = 0,043 p =0,435).

#### 5.2.2.1.5 Αντιληπτός Έλεγχος της Πληροφορίας "Perceived Control of Information"

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Perceived Control of Information" στις ΙΚΔ σχετίζεται με το Φύλο.

Η μεταβλητή "Perceived Control of Information» ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 82 & Γράφημα: 43 & Γράφημα: 44 & Γράφημα: 45 & Γράφημα: 46, Κεφάλαιο 5.3).

**Correlations**

| | | | Perceived Control of Information Total | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Perceived Control of Information Total | Correlation Coefficient | 1.000 | .080 |
| | | Sig. (2-tailed) | . | .145 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | .080 | 1.000 |
| | | Sig. (2-tailed) | .145 | . |
| | | N | 334 | 334 |

*Πίνακας: 38 Spearman's Correlation Perceived Control of Information & Φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Perceived Control of Information και Φύλο ($r_s$ = 0,80, p =0,145)

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Perceived Control of Information" στις ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Perceived Control of Information Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Perceived Control of Information Total | Correlation Coefficient | 1.000 | .027 |
| | | Sig. (2-tailed) | . | .629 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .027 | 1.000 |
| | | Sig. (2-tailed) | .629 | . |
| | | N | 334 | 334 |

*Πίνακας: 39 Spearman's Rho Correlation Perceived Control of Information & Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Perceived Control Of Information και Ηλικία ($r_s$ = 0,027, p =0,0629).

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Perceived Control of Information" στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο

**Correlations**

| | | | Perceived Control of Information Total | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Perceived Control of Information Total | Correlation Coefficient | 1.000 | -.129* |
| | | Sig. (2-tailed) | . | .019 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.129* | 1.000 |
| | | Sig. (2-tailed) | .019 | . |
| | | N | 334 | 334 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Πίνακας: 40 Spearman's Rho Correlation Perceived Control of Information & Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Perceived Control of Information και Εκπαίδευση / Μορφωτικό Επίπεδο (rs = -0,129, p = 0,019)

#### 5.2.2.1.6 Αποκάλυψη Προσωπικών πληροφοριών "Identity Information Disclosure"

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Identity Information Disclosure" στις ΙΚΔ σχετίζεται με το Φύλο

Η μεταβλητή "Identity Information Disclosure" ελέγχθηκε ως προς την κανονικότητα και ως προς το φύλο και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 84 & Γράφημα: 53 & Γράφημα: 54 & Γράφημα: 55 & Γράφημα: 56, Κεφάλαιο 5.3).

**Correlations**

| | | Identity Information Disclosure Scale Total | Φύλο |
|---|---|---|---|
| Identity Information Disclosure Scale Total | Pearson Correlation | 1 | -.022 |
| | Sig. (2-tailed) | | .682 |
| | N | 334 | 334 |
| Φύλο | Pearson Correlation | -.022 | 1 |
| | Sig. (2-tailed) | .682 | |
| | N | 334 | 334 |

*Πίνακας: 41 Pearson's r Correlation Identity Information Disclosure & Φύλο*

Τα αποτελέσματα ελέγχου Pearson's r έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Identity Information Disclosure και Φύλο (r = -0,022, p =0,682) .

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Identity Information Disclosure" στις ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Identity Information Disclosure Scale Total | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Identity Information Disclosure Scale Total | Correlation Coefficient | 1.000 | .174** |
| | | Sig. (2-tailed) | . | .001 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .174** | 1.000 |
| | | Sig. (2-tailed) | .001 | . |
| | | N | 334 | 334 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | |

*Πίνακας: 42 Spearman's Rho Correlation Identity Information Disclosure & Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Identity Information Disclosure και Ηλικία ($r_s$ = 0,174**., p = 0,001)

**Ερευνητικό Ερώτημα:** Η Συμπεριφορά "Identity Information Disclosure" στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο

**Correlations**

| | | | Identity Information Disclosure Scale Total | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Identity Information Disclosure Scale Total | Correlation Coefficient | 1.000 | -.071 |
| | | Sig. (2-tailed) | . | .193 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.071 | 1.000 |
| | | Sig. (2-tailed) | .193 | . |
| | | N | 334 | 334 |

*Πίνακας: 43 Spearman's Rho Correlation Identity Information Disclosure & Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Identity Information Disclosure και Εκπαίδευση/ Μορφωτικό Επίπεδο ($r_s$ =-0,071, p = 0,193)

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» στις ΙΚΔ σχετίζεται με το Φύλο.

**Correlations**

| | | | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Correlation Coefficient | 1.000 | .095 |
| | | Sig. (2-tailed) | . | .082 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | .095 | 1.000 |
| | | Sig. (2-tailed) | .082 | . |
| | | N | 334 | 334 |

*Πίνακας: 44 Spearman's Correlation «Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου» & Φύλο*

Τα αποτελέσματα ελέγχου Spearman's έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» και Φύλο ($r_s$= 0,095, p =0,082)

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» στις ΙΚΔ σχετίζεται με την Ηλικία.

**Correlations**

| | | | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Correlation Coefficient | 1.000 | .034 |
| | | Sig. (2-tailed) | . | .536 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .034 | 1.000 |
| | | Sig. (2-tailed) | .536 | . |
| | | N | 334 | 334 |

*Πίνακας: 45 Spearman's Rho Correlation «Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου» & Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι <u>δεν υπάρχει στατιστικά σημαντική συσχέτιση</u> μεταξύ των μεταβλητών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» και Ηλικίας ($r_s$=0,034 p =0,536)

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο.

**Correlations**

| | | | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου | Correlation Coefficient | 1.000 | -.019 |

| | | | |
|---|---|---|---|
| | Sig. (2-tailed) | . | .735 |
| | N | 334 | 334 |
| Εκπαίδευση | Correlation Coefficient | -.019 | 1.000 |
| | Sig. (2-tailed) | .735 | . |
| | N | 334 | 334 |

*Πίνακας: 46 Spearman's Rho Correlation «Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου» & Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Είναι σημαντικό για μένα να προστατεύω τις πληροφορίες τις σχετικές με την ταυτότητά μου» και Εκπαίδευση / Μορφωτικό Επίπεδο ($r_s$ = -0,019, p = 0,735)

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» στις ΙΚΔ σχετίζεται με το Φύλο.

**Correlations**

| | | | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Correlation Coefficient | 1.000 | .119* |
| | | Sig. (2-tailed) | . | .029 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | .119* | 1.000 |
| | | Sig. (2-tailed) | .029 | . |
| | | N | 334 | 334 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Πίνακας: 47 Spearman's Correlation «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Φύλο.*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Φύλο ($r_s$ =0,119*, p =0,029).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» στις ΙΚΔ σχετίζεται με την Ηλικία.

**Correlations**

| | | | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Correlation Coefficient | 1.000 | .040 |
| | | Sig. (2-tailed) | . | .462 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .040 | 1.000 |
| | | Sig. (2-tailed) | .462 | . |
| | | N | 334 | 334 |

*Πίνακας: 48 Spearman's Rho Correlation ««Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Ηλικία (r = 0,040, p =0,462).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» σχετίζεται με το Μορφωτικό Επίπεδο

**Correlations**

| | | | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Correlation Coefficient | 1.000 | -.003 |
| | | Sig. (2-tailed) | . | .952 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.003 | 1.000 |
| | | Sig. (2-tailed) | .952 | . |
| | | N | 334 | 334 |

*Πίνακας: 49 Spearman's Rho Correlation ««Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Εκπαίδευση/ Μορφωτικό επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Ανησυχώ για τις συνέπειες διαμοιρασμού/ Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» και Εκπαίδευση / Μορφωτικό Επίπεδο ($r_s$ = -0,003, p = 0,952).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» σχετίζεται με το Φύλο

**Correlations**

| | | | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Correlation Coefficient | 1.000 | -.064 |
| | | Sig. (2-tailed) | . | .241 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | -.064 | 1.000 |
| | | Sig. (2-tailed) | .241 | . |
| | | N | 334 | 334 |

*Πίνακας: 50 Spearman's Correlation "Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και Φύλο ($r_s$ = -0,064, p = 0,241).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» σχετίζεται με την Ηλικία

| **Correlations** |
|---|

| | | | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Correlation Coefficient | 1.000 | -.010 |
| | | Sig. (2-tailed) | . | .852 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | -.010 | 1.000 |
| | | Sig. (2-tailed) | .852 | . |
| | | N | 334 | 334 |

*Πίνακας: 51 Spearman's rho Correlation "Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και Ηλικία (rs = -0,010, p =0,852).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» σχετίζεται με το Μορφωτικό Επίπεδο

**Correlations**

| | | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Εκπαίδευση |
|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Spearman's rho | Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον. | Correlation Coefficient | 1.000 | -.075 |
| | | Sig. (2-tailed) | . | .172 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.075 | 1.000 |
| | | Sig. (2-tailed) | .172 | . |
| | | N | 334 | 334 |

*Πίνακας: 52 Spearman's rho Correlation "Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και Εκπαίδευση / Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με την ταυτότητά μου διαδικτυακά (online) στο μέλλον» και Εκπαίδευση/ Μορφωτικό Επίπεδο ($r_s$ = -0,075, p =0,172).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» σχετίζεται με το Φύλο.

**Correlations**

| | | | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Correlation Coefficient | 1.000 | .089 |
| | | Sig. (2-tailed) | . | .106 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | .089 | 1.000 |
| | | Sig. (2-tailed) | .106 | . |
| | | N | 334 | 334 |

*Πίνακας: 53 Spearman's Correlation «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο»» και φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» και Φύλο (r = 0,089, p =0,106).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» σχετίζεται με την Ηλικία.

**Correlations**

| | | | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Correlation Coefficient | 1.000 | .080 |
| | | Sig. (2-tailed) | . | .145 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | .080 | 1.000 |
| | | Sig. (2-tailed) | .145 | . |
| | | N | 334 | 334 |

*Πίνακας: 54 Spearman's rho Correlation «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» και ηλικία*

Τα αποτελέσματα ελέγχου Spearman Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» και Ηλικία ($r_s$ = 0,080, p = 0,145).

**Ερευνητικό Ερώτημα:** Η Αποκάλυψη Προσωπικών πληροφοριών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» σχετίζεται με το Μορφωτικό Επίπεδο.

**Correlations**

| | | | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Εκπαίδευση |
|---|---|---|---|---|
| Spearman's rho | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Correlation Coefficient | 1.000 | -.111* |
| | | Sig. (2-tailed) | . | .043 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.111* | 1.000 |
| | | Sig. (2-tailed) | .043 | . |
| | | N | 334 | 334 |

*. Correlation is significant at the 0.05 level (2-tailed).

*Πίνακας: 55 Spearman's Rho Correlation «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» και Εκπαίδευση/ Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν **ότι υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» και Εκπαίδευση / Μορφωτικό Επίπεδο ($r_s$ =-0, 111*, p = 0,043).

### 5.2.2.2 Έκθεση σε Κίνδυνο Συσχετισμοί

**Ερευνητικό Ερώτημα:** Η Έκθεση σε Κίνδυνο στις ΙΚΔ σχετίζεται με το Φύλο

**Correlations**

| | | | Έκθεση Σε Κινδύνους | Φύλο |
|---|---|---|---|---|
| Spearman's rho | Έκθεση Σε Κινδύνους | Correlation Coefficient | 1.000 | -.209** |

| | | | | |
|---|---|---|---|---|
| | | Sig. (2-tailed) | . | .000 |
| | | N | 334 | 334 |
| | Φύλο | Correlation Coefficient | -.209** | 1.000 |
| | | Sig. (2-tailed) | .000 | . |
| | | N | 334 | 334 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | |

*Πίνακας: 56 Έκθεση σε Κίνδυνο – Φύλο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι **υπάρχει στατιστικά σημαντική συσχέτιση** μεταξύ των μεταβλητών Έκθεση σε Κίνδυνο και Φύλο (rs = -0,209*, p <0,01).

**Ερευνητικό Ερώτημα:** Η Έκθεση σε Κίνδυνο στις ΙΚΔ σχετίζεται με την Ηλικία

**Correlations**

| | | | Έκθεση Σε Κινδύνους | Ηλικία |
|---|---|---|---|---|
| Spearman's rho | Έκθεση Σε Κινδύνους | Correlation Coefficient | 1.000 | -.037 |
| | | Sig. (2-tailed) | . | .496 |
| | | N | 334 | 334 |
| | Ηλικία | Correlation Coefficient | -.037 | 1.000 |
| | | Sig. (2-tailed) | .496 | . |
| | | N | 334 | 334 |

*Πίνακας: 57 Έκθεση σε Κίνδυνο - Ηλικία*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν <u>ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση</u> μεταξύ των μεταβλητών Έκθεση σε Κίνδυνο και Ηλικία ($r_s$ = -0,037 p = 0,496).

**Ερευνητικό Ερώτημα:** Η Έκθεση σε Κίνδυνο στις ΙΚΔ σχετίζεται με το Μορφωτικό Επίπεδο.

**Correlations**

| | Έκθεση Σε Κινδύνους | Εκπαίδευση |
|---|---|---|

| | | | | |
|---|---|---|---|---|
| Spearman's rho | Έκθεση Σε Κινδύνους | Correlation Coefficient | 1.000 | -.015 |
| | | Sig. (2-tailed) | . | .784 |
| | | N | 334 | 334 |
| | Εκπαίδευση | Correlation Coefficient | -.015 | 1.000 |
| | | Sig. (2-tailed) | .784 | . |
| | | N | 334 | 334 |

*Πίνακας: 58 Έκθεση σε Κίνδυνο - Εκπαίδευση/Μορφωτικό Επίπεδο*

Τα αποτελέσματα ελέγχου Spearman's Rho έδειξαν ότι δεν υπάρχει στατιστικά σημαντική συσχέτιση μεταξύ των μεταβλητών Έκθεση σε Κίνδυνο και Εκπαίδευση / Μορφωτικό Επίπεδο (rs = -0,015, p =0,784)

### 5.2.3 Έλεγχος ερευνητικών ερωτημάτων με χρήση test (μέσων όρων)

Η μέτρηση των test αυτών έχει στόχο τον έλεγχο απόδοσης δύο καταστάσεων. Γίνεται για να διαπιστωθούν τυχόν διαφορές μεταξύ δύο ομάδων ως προς ένα χαρακτηριστικό ή να ελεγχθεί ένα δείγμα με δύο διαφορετικές μετρήσεις. Παράδειγμα, μπορεί να αποτελεί Η «Συμπεριφορά Ανάληψης Ρίσκου μεταξύ Ανδρών και Γυναικών».

Παραδοχές: Για την χρήση του T-test πρέπει:

1. Η μία μεταβλητή - μετρήσεις του δείγματος- να είναι σε συνεχή κλίμακα.
2. Η δεύτερη μεταβλητή να είναι διχοτομική, όπως το φύλο.
3. Η μεταβλητή κλίμακας (συνεχής μεταβλητή) να παρουσιάζει περίπου κανονική κατανομή για την κάθε κατηγορία της διχοτομικής μεταβλητής που ελέγχεται με το test Kolmogorov-Smirnov (N>30) ή Shapiro-Wilk test (N<30) (ή το q-q plot).
4. Η συνεχής μεταβλητή να παρουσιάζει ομοιογένεια διακύμανσης, για κάθε κατηγορία της διχοτομικής μεταβλητής, που ελέγχεται με Levene's test.
5. Οι μετρήσεις να είναι ανεξάρτητες- κάθε υποκείμενο να συμμετέχει μια φορά.
6. Η στατιστική σημαντικότητα ορίζεται στο 0,05.

Στην περίπτωση μιας συνεχούς μεταβλητής και μιας κατηγορικής η οποία περιέχει περισσότερες από 3 ομάδες (και με κανονικότητα που δεν αποκλίνει) τότε για τον έλεγχο χρησιμοποιείται το test One Way-ANOVA.

Στις υπόλοιπες περιπτώσεις χρησιμοποιούνται μη-παραμετρικά test (Mann-Whitney ή Kruskal-Wallis), ανάλογα με το είδος των μεταβλητών – (μεταβλητές με μη κανονική κατανομή ή κατηγορικές-), και τον αριθμό των μεταβλητών, στις περιπτώσεις, της μιας κατηγορικής μεταβλητής. Στη παρούσα εργασία σε έλεγχο με test (t test ή άλλα μη παραμετρικά test) υλοποιήθηκε (εξετάσθηκε), σε όσες μεταβλητές παρουσίασαν **«στατιστικά σημαντική συσχέτιση»** στα test "Pearson" ή "Spearman" (υπό-κεφάλαιο 5.2.2)

### 5.2.3.1 Συμπεριφορές Χρηστών ΙΚΔ- Σχέσεις Test

#### 5.2.3.1.1 Διαφορά στην συμπεριφορά Ανάληψης Ρίσκου στις ΙΚΔ ανάλογα με την ηλικία.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με την ηλικία στην συμπεριφορά Ανάληψης Ρίσκου/"Risk Taking".

Με βάση το παραπάνω ερευνητικό ερώτημα μπορεί να διατυπωθεί η κάτωθι μηδενική υπόθεση η οποία θα επαληθευθεί (ελεγχθεί εάν αληθεύει) με το κατάλληλο test.

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ των διαφορετικών ηλικιών των συμμετεχόντων αναφορικά με την συμπεριφορά Ανάληψης Ρίσκου Risk Taking στις ΙΚΔ.*

Η μεταβλητή "Risk Averseness" ελέγχθηκε ως προς την κανονικότητα και ως προς την ηλικία και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Tests of Normality Πίνακας: 76 & Q-Q plots Γράφημα: 22 & Γράφημα: 23 & Γράφημα: 24 & Γράφημα: 25 κεφάλαιο 5.3).

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το test One Way-ANOVA.

**ANOVA**

Risk Averseness Total

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 40.826 | 4 | 10.207 | .664 | .617 |
| Within Groups | 5055.979 | 329 | 15.368 | | |
| Total | 5096.805 | 333 | | | |

*Πίνακας: 59 Ανάληψη Ρίσκου – Ηλικία One Way ANOVA*

Τα αποτελέσματα της ανάλυσης διακύμανσης ενός παράγοντα (ANOVA) έδειξαν ότι ηλικιακή ομάδα ενός χρήστη **δεν** επιδρά με στατιστικά σημαντικό τρόπο (F[4,329] =

0,664, p=0,617, ) συμπεραίνουμε ότι δεν υπάρχει διαφορά Μεταξύ Ανδρών και Γυναικών στην ανάληψη ρίσκου.

#### 5.2.3.1.2 Διαφορά στην συμπεριφορά Εμπιστοσύνη"Trust" ανάλογα με την Εκπαίδευση/ Μορφωτικό Επίπεδο.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά μεταξύ του Μορφωτικού Επιπέδου των συμμετεχόντων αναφορικά με την Συμπεριφορά Εμπιστοσύνη/Trust.

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ του Μορφωτικού Επιπέδου των συμμετεχόντων και στην συμπεριφορά αναφορικά με την Εμπιστοσύνη "Trust" στις ΙΚΔ.*

Η μεταβλητή Εμπιστοσύνη "Trust" ελέγχθηκε ως προς την κανονικότητα, ως προς το Μορφωτικό Επίπεδο και ευρέθη ότι αποκλίνει από την κανονική κατανομή (Βλέπε & Πίνακας: 78 & Γράφημα: 28 & Γράφημα: 29 & Γράφημα: 30 κεφάλαιο 5.3).

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το μη παραμετρικό test "Kruskal-Wallis".

**Ranks**

| | Εκπαίδευση | N | Mean Rank |
|---|---|---|---|
| Trust Total | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | 2 | 175.75 |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | 45 | 194.22 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | 287 | 163.25 |
| | Total | 334 | |

*Πίνακας: 60 Test Kruskal-Wallis Κατάταξη Εκπαίδευση/ Μορφωτικό Επίπεδο & Εμπιστοσύνη "Trust"*

| **Independent-Samples Kruskal-Wallis Test Summary** | |
|---|---|
| Total N | 334 |
| Test Statistic | 4.063[a,b] |
| Degree of Freedom | 2 |
| Asymptotic Sig.(2-sided test) | .131 |

a. The test statistic is adjusted for ties.
b. Multiple comparisons are not performed because the overall test does not show significant differences across samples.

*Πίνακας: 61 Αποτελέσματα Kruskal- Wallis test Μορφωτικό Επίπεδο & Trust*

Οι μέσοι όροι των κατατάξεων Kruskal-Wallis για τις κατηγορίες μορφωτικού επιπέδου των συμμετεχόντων στις ΙΚΔ είναι: για το επίπεδο Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου 175,75, για το επίπεδο Δευτεροβάθμια Εκπαίδευση 194,22 και για το επίπεδο Τριτοβάθμια Εκπαίδευση 163,25. Το test Kruskal-Wallis έδειξε ότι **δεν** υπάρχουν στατιστικά σημαντικές διαφορές (t= 4,063, df= 2, p= 0,131) μεταξύ των κατηγοριών μορφωτικού επιπέδου των συμμετεχόντων στις ΙΚΔ αναφορικά με την Εμπιστοσύνη "Trust".

#### 5.2.3.1.3 Διαφορά στην συμπεριφορά για την Ιδιωτικότητα "Privacy Behavior" ανάλογα με την ηλικία.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με την ηλικία στη "Συμπεριφορά για την Ιδιωτικότητα"

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ των διαφορετικών ηλικιών αναφορικά με την συμπεριφορά για την Ιδιωτικότητα /Privacy Behavior***.**

Η μεταβλητή "Privacy Behavior" ελέγχθηκε ως προς την κανονικότητα και ως προς την ηλικία και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 80 & Q-Q plots Γράφημα: 35 & Γράφημα: 36 & Γράφημα: 37& Γράφημα: 38 κεφάλαιο 5.3)

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το test One Way-ANOVA με εξαίρεση της κατηγορίας 69+ καθώς αποτελούσε σταθερά στο test κανονικότητας (Πίνακας: 79 ***Privacy Behavior scale Total is constant when Ηλικία = 69+. It has been omitted)*

**ANOVA**

Privacy Behavior scale Total

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 716.286 | 3 | 238.762 | 8.827 | .000 |
| Within Groups | 8899.612 | 329 | 27.050 | | |
| Total | 9615.898 | 332 | | | |

*Πίνακας: 62 One Way-ANOVA Privacy Behavior & Ηλικία*

**Multiple Comparisons**

Dependent Variable: Privacy Behavior scale Total

Bonferroni

| (I) Ηλικία | (J) Ηλικία | | Sig. | 95% Confidence Interval |
|---|---|---|---|---|

| | | Mean Difference (I-J) | Std. Error | | Lower Bound | Upper Bound |
|---|---|---|---|---|---|---|
| 18-28 | 29-38 | -1.219 | 1.055 | 1.000 | -4.02 | 1.58 |
| | 39-48 | -1.977 | .979 | .265 | -4.58 | .62 |
| | 49-68 | -4.304* | .993 | .000 | -6.94 | -1.67 |
| 29-38 | 18-28 | 1.219 | 1.055 | 1.000 | -1.58 | 4.02 |
| | 39-48 | -.759 | .780 | 1.000 | -2.83 | 1.31 |
| | 49-68 | -3.085* | .798 | .001 | -5.20 | -.97 |
| 39-48 | 18-28 | 1.977 | .979 | .265 | -.62 | 4.58 |
| | 29-38 | .759 | .780 | 1.000 | -1.31 | 2.83 |
| | 49-68 | -2.326* | .695 | .005 | -4.17 | -.48 |
| 49-68 | 18-28 | 4.304* | .993 | .000 | 1.67 | 6.94 |
| | 29-38 | 3.085* | .798 | .001 | .97 | 5.20 |
| | 39-48 | 2.326* | .695 | .005 | .48 | 4.17 |

*. The mean difference is significant at the 0.05 level.

*Πίνακας: 63 Bonferroni Πίνακας Privacy behavior & Ηλικίες*

Τα αποτελέσματα της ανάλυσης διακύμανσης ενός παράγοντα (ANOVA) έδειξαν ότι η ηλικιακή ομάδα ενός χρήστη **επιδρά** με στατιστικά σημαντικό τρόπο (F[3,329]=8,827,p=0.00 $\eta^2$=0,074) μεταξύ των ηλικιών, αναφορικά με την συμπεριφορά για την Ιδιωτικότητα. Το μέγεθος της επίδρασης ωστόσο είναι μικρό $\eta^2$=0,074. Οι αναλύσεις Bonferroni post hoc test έδειξαν ότι υπάρχει στατιστικά σημαντική (p<0,005) διαφορά ανάμεσα στις ηλικιακές ομάδες 18-28 ετών και 49-68 και μεταξύ των ηλικιών 29-38 ετών και 49-68 ετών, ενώ είναι οριακή p=0,05 η διαφορά ανάμεσα στις ομάδες 39-48 ετών και 49-68 ετών.

#### 5.2.3.1.4 Διαφορά στην συμπεριφορά για τον Αντιληπτό έλεγχο πληροφορίας ανάλογα με το Μορφωτικό Επίπεδο των συμμετεχόντων.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με το Μορφωτικό Επίπεδο στην συμπεριφορά για τον Αντιληπτό έλεγχο πληροφορίας.

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ Του Μορφωτικού Επιπέδου των Χρηστών αναφορικά με την συμπεριφορά Αντιληπτός Έλεγχος της Πληροφορίας/Perceived Control of Information*

Η μεταβλητή "Perceived Control Of Information" ελέγχθηκε ως προς την κανονικότητα και ως προς την Μορφωτικό Επίπεδο και ευρέθη ότι δεν αποκλίνει από την κανονική

κατανομή (Βλέπε  Πίνακας: 83 & Γράφημα: 47 & Γράφημα: 48 & Γράφημα: 49 & Γράφημα: 50 & Γράφημα: 51 & Γράφημα: 52 Κεφάλαιο 5.3).

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το test One Way-ANOVA

**ANOVA**

Perceived Control of Information Total

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 58.088 | 2 | 29.044 | 3.529 | .030 |
| Within Groups | 2723.816 | 331 | 8.229 | | |
| Total | 2781.904 | 333 | | | |

*Πίνακας: 64 One Way_ANOVA Αντιληπτός έλεγχος Πληροφορίας και Μορφωτικό Επίπεδο*

**Multiple Comparisons**

Dependent Variable:  Perceived Control of Information Total

Bonferroni

| (I) Εκπαίδευση | (J) Εκπαίδευση | Mean Difference (I-J) | Std. Error | Sig. | 95% Confidence Interval Lower Bound | 95% Confidence Interval Upper Bound |
|---|---|---|---|---|---|---|
| Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | 3.511 | 2.073 | .274 | -1.48 | 8.50 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | 4.286 | 2.035 | .108 | -.61 | 9.18 |
| Δευτεροβάθμια Εκπαίδευση (Λύκειο) | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | -3.511 | 2.073 | .274 | -8.50 | 1.48 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | .775 | .460 | .279 | -.33 | 1.88 |
| Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | -4.286 | 2.035 | .108 | -9.18 | .61 |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | -.775 | .460 | .279 | -1.88 | .33 |

*Πίνακας: 65 Bonferroni Tests Perceived Control of Information &Μορφωτικό Επίπεδο*

Τα αποτελέσματα της ανάλυσης διακύμανσης ενός παράγοντα (ANOVA) έδειξαν ότι το μορφωτικό επίπεδο ενός χρήστη **επιδρά** με στατιστικά σημαντικό τρόπο (F[2,331]=3,529, p=0,030 $\eta^2$=0,020) στον Αντιληπτό "Έλεγχο της πληροφορίας. Ωστόσο το μέγεθος της επίδρασης είναι μικρό $\eta^2$=0,020. Οι αναλύσεις Bonferroni post hoc test έδειξαν ότι **δεν υπάρχει στατιστικά σημαντική** (p<0,005) διαφορά ανάμεσα σε κανένα ζεύγος ομάδων μορφωτικού επιπέδου.

#### 5.2.3.1.5 Διαφορά στην συμπεριφορά Αποκάλυψη Προσωπικών Πληροφοριών/Identity Information Disclosure" ανάλογα με την Ηλικία.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με την Ηλικία στην συμπεριφορά αποκάλυψης Προσωπικών πληροφοριών.

**H₀:** *Δεν υπάρχει διαφορά μεταξύ ηλικίας αναφορικά με την συμπεριφορά Αποκάλυψης Προσωπικών Πληροφοριών /Identity Information Disclosure*

Η μεταβλητή "Identity Information Disclosure" ελέγχθηκε ως προς την κανονικότητα και ως προς την ηλικία και ευρέθη ότι δεν αποκλίνει από την κανονική κατανομή (Βλέπε Πίνακας: 85 & Γράφημα: 57 & Γράφημα: 58 & Γράφημα: 59 & Γράφημα: 60, Κεφάλαιο 5.3).

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το test One Way-ANOVA ANOVA με εξαίρεση της κατηγορίας 69+ καθώς αποτελούσε σταθερά στο test κανονικότητας (Πίνακας: 83Πίνακας: 79 ***Privacy Behavior scale Total is constant when Ηλικία = 69+. It has been omitted).*

**ANOVA**

Identity Information Disclosure Scale Total

| | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Between Groups | 160.476 | 3 | 53.492 | 4.890 | .002 |
| Within Groups | 3599.187 | 329 | 10.940 | | |
| Total | 3759.664 | 332 | | | |

*Πίνακας: 66 One Way-ANOVA και Ηλικία*

**Multiple Comparisons**

Dependent Variable: Identity Information Disclosure Scale Total

Bonferroni

| (I) Ηλικία | (J) Ηλικία | Std. Error | Sig. | 95% Confidence Interval |
|---|---|---|---|---|

| | | Mean Difference (I-J) | | | Lower Bound | Upper Bound |
|---|---|---|---|---|---|---|
| 18-28 | 29-38 | .059 | .671 | 1.000 | -1.72 | 1.84 |
| | 39-48 | -1.239 | .623 | .285 | -2.89 | .41 |
| | 49-68 | -1.601 | .632 | .070 | -3.28 | .08 |
| 29-38 | 18-28 | -.059 | .671 | 1.000 | -1.84 | 1.72 |
| | 39-48 | -1.298 | .496 | .056 | -2.61 | .02 |
| | 49-68 | -1.660* | .507 | .007 | -3.01 | -.31 |
| 39-48 | 18-28 | 1.239 | .623 | .285 | -.41 | 2.89 |
| | 29-38 | 1.298 | .496 | .056 | -.02 | 2.61 |
| | 49-68 | -.362 | .442 | 1.000 | -1.53 | .81 |
| 49-68 | 18-28 | 1.601 | .632 | .070 | -.08 | 3.28 |
| | 29-38 | 1.660* | .507 | .007 | .31 | 3.01 |
| | 39-48 | .362 | .442 | 1.000 | -.81 | 1.53 |

*. The mean difference is significant at the 0.05 level.

*Πίνακας: 67 Bonferroni Test Identity Information Disclosure & Ηλικίες*

Τα αποτελέσματα της ανάλυσης διακύμανσης ενός παράγοντα (ANOVA) έδειξαν ότι η ηλικιακή ομάδα ενός χρήστη **επιδρά** με στατιστικά σημαντικό τρόπο (F[3,329]=4,890, p=0,02, $\eta^2$=0,042), ωστόσο το μέγεθος της επίδρασης είναι μικρό $\eta^2$ =0.042. Οι αναλύσεις Bonferroni post hoc test έδειξαν ότι δεν υπάρχει στατιστικά σημαντική διαφορά μεταξύ ηλικιακών ομάδων 18-28 και 39-48 (p=0,285) και μεταξύ ηλικιακών ομάδων 18-28 & 49-68 (p=0,070). Υπάρχει οριακά στατιστικά σημαντική (p<0,056) διαφορά ανάμεσα στις ηλικιακές ομάδες 29-38 ετών και 39-48 ετών. Ωστόσο υπάρχει αρκετά στατιστικά σημαντική διαφορά μεταξύ ηλικιακών ομάδων 29-38 & 49-68 (p=0,007).

#### 5.2.3.1.6 Διαφορά στην συμπεριφορά Αποκάλυψη Προσωπικών Πληροφοριών/Identity Information Disclosure «Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» ανάλογα με το Φύλο.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με το φύλο στην συμπεριφορά αποκάλυψης Προσωπικών πληροφοριών "Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου"

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ ανδρών και γυναικών αναφορικά με την συμπεριφορά Αποκάλυψης Προσωπικών Πληροφοριών /Identity Information Disclosure "Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου"*

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το μη παραμετρικό test Mann Whitney.

| Ranks | | | | |
|---|---|---|---|---|
| | Φύλο | N | Mean Rank | Sum of Ranks |
| Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. | Άνδρας | 110 | 152.25 | 16747.50 |
| | Γυναίκα | 224 | 174.99 | 39197.50 |
| | Total | 334 | | |

*Πίνακας: 68 Mann-Whitney Αποκάλυψη Προσωπικών Πληροφοριών «Ανησυχώ....» & Φύλου Κατάταξη*

| Test Statistics[a] | |
|---|---|
| | Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου. |
| Mann-Whitney U | 10642.500 |
| Wilcoxon W | 16747.500 |
| Z | -2.175 |
| Asymp. Sig. (2-tailed) | .030 |
| a. Grouping Variable: Φύλο | |

*Πίνακας: 69 Mann- Whitney Test Αποκάλυψη Προσωπικών Πληροφοριών «Ανησυχώ....» & Φύλου*

Η μέση κατάταξη στις ομάδες «Άνδρας» και «Γυναίκα» ήταν αντίστοιχα 152,25 και 174,99. Τα αποτελέσματα του ελέγχου κατάταξης Mann-Whitney έδειξαν ότι **υπάρχει** στατιστικά σημαντική διαφορά μεταξύ Ανδρών και Γυναικών χρηστών αναφορικά με την συμπεριφορά «Αποκάλυψης Προσωπικών πληροφοριών "Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» (Mann-Whitney t = 10642.50, $n_1$=110, $n_2$=224, p<0,05). Που σημαίνει ότι η διαφορά φύλου συνδέεται με την Ανησυχία για τις Συνέπειες από την Αποκάλυψη πληροφοριών σχετικών με την ταυτότητα του χρήστη.

### 5.2.3.1.7 Διαφορά στην συμπεριφορά Αποκάλυψη Προσωπικών Πληροφοριών/Identity Information Disclosure «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο" ανάλογα με την Εκπαίδευση / Μορφωτικό Επίπεδο.

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά ανάλογα με το Μορφωτικό Επίπεδο στην Συμπεριφορά Αποκάλυψης Προσωπικών πληροφοριών – "Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο"

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ Μορφωτικού Επιπέδου (των Συμμετεχόντων Χρηστών ΙΚΔ) αναφορικά με την συμπεριφορά Αποκάλυψης Προσωπικών Πληροφοριών /Identity Information Disclosure "Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο"*.

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το μη παραμετρικό test Kruskal-Wallis.

**Ranks**

| | Εκπαίδευση | N | Mean Rank |
|---|---|---|---|
| Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | 2 | 316.00 |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | 45 | 186.68 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | 287 | 163.46 |
| | Total | 334 | |

*Πίνακας: 70 Kruskal-Wallis "Πιστεύω.... & Εκπαίδευση*

**Test Statistics[a,b]**

| | Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο. |
|---|---|
| Kruskal-Wallis H | 7.543 |
| df | 2 |
| Asymp. Sig. | .023 |

a. Kruskal Wallis Test
b. Grouping Variable: Εκπαίδευση

*Πίνακας: 71 Αποτελέσματα Kruskal-Wallis "Αποκάλυψη Προσωπικών Πληροφοριών «Πιστεύω... & Εκπαίδευση»*

**Pairwise Comparisons of Εκπαίδευση**

| Sample 1-Sample 2 | Test Statistic | Std. Error | Std. Test Statistic | Sig. | Adj. Sig.[a] |
|---|---|---|---|---|---|
| Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη)- Δευτεροβάθμια Εκπαίδευση (Λύκειο) | 23.220 | 14.923 | 1.556 | .120 | .359 |
| Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη)- Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | 152.542 | 66.043 | 2.310 | .021 | .063 |
| Δευτεροβάθμια Εκπαίδευση (Λύκειο)- Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | 129.322 | 67.260 | 1.923 | .055 | .164 |

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.

Asymptotic significances (2-sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

*Πίνακας: 72 Συγκρίσεις μεταξύ ομάδων διαφορετικού Μορφωτικού Επιπέδου*

Οι μέσοι όροι των κατατάξεων Kruskal-Wallis για τις κατηγορίες μορφωτικού επιπέδου των συμμετεχόντων στις ΙΚΔ είναι: για το επίπεδο Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου 316,00 για το επίπεδο Δευτεροβάθμια Εκπαίδευση 186,68 και για το επίπεδο Τριτοβάθμια Εκπαίδευση 163,46. Το test Kruskal-Wallis έδειξε ότι **υπάρχουν στατιστικά σημαντικές διαφορές** (t= 7,543, df= 2, p= 0,023) μεταξύ των κατηγοριών μορφωτικού επιπέδου των συμμετεχόντων στις ΙΚΔ αναφορικά με την συμπεριφορά Αποκάλυψης Προσωπικών Πληροφοριών /Identity Information Disclosure "Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο». Οι αναλύσεις Bonferroni post hoc έδειξαν ότι υπάρχει στατιστικά σημαντική διαφορά μεταξύ Μορφωτικού Επίπεδου (t=2,31, p<0,05) της Τριτοβάθμιας Εκπαίδευσης

και υποχρεωτικής Εκπαίδευσης, ενώ οριακή στατιστική διαφορά μεταξύ Μορφωτικού Επίπεδου της Δευτεροβάθμιας Εκπαίδευσης και Υποχρεωτικής Εκπαίδευσης (p=0,055) ενώ **δεν** βρέθηκε στατιστικά σημαντική διαφορά (p= 0,120) μεταξύ επιπέδων Εκπαίδευσης Τριτοβάθμιας και Δευτεροβάθμιας.

### 5.2.3.2 Έκθεση σε Κίνδυνο Σχέσεις Test

**Ερευνητικό Ερώτημα:** Υπάρχει διαφορά στην Έκθεση σε Κίνδυνο σε ΙΚΔ σε σχέση με το Φύλο.

Με βάση το παραπάνω ερευνητικό ερώτημα μπορεί να διατυπωθεί η κάτωθι μηδενική υπόθεση η οποία θα επαληθευθεί (ελεγχθεί εάν αληθεύει), με το κατάλληλο test.

**$H_0$:** *Δεν υπάρχει διαφορά μεταξύ των φύλων «Άνδρας» και «Γυναίκα» αναφορικά με την Έκθεση σε Κίνδυνο στις ΙΚΔ.*

Για τον έλεγχο της μηδενικής υπόθεσης θα χρησιμοποιηθεί το μη παραμετρικό test Mann-Whitney U.

**Ranks**

| | Φύλο | N | Mean Rank | Sum of Ranks |
|---|---|---|---|---|
| Έκθεση Σε Κινδύνους | Άνδρας | 110 | 195.68 | 21524.50 |
| | Γυναίκα | 224 | 153.66 | 34420.50 |
| | Total | 334 | | |

*Πίνακας: 73 Mann-Whitney Έκθεση σε Κίνδυνο και φύλο Κατάταξη*

**Test Statistics[a]**

| | Έκθεση Σε Κινδύνους |
|---|---|
| Mann-Whitney U | 9220.500 |
| Wilcoxon W | 34420.500 |
| Z | -3.819 |
| Asymp. Sig. (2-tailed) | .000 |

a. Grouping Variable: Φύλο

*Πίνακας: 74 Mann Whitney Test Έκθεση σε Κίνδυνο και φύλο*

Η μέση κατάταξη στις ομάδες «Άνδρας» και «Γυναίκα» ήταν αντίστοιχα 195,68 και 153,66. Τα αποτελέσματα του ελέγχου κατάταξης έδειξαν ότι **υπάρχει** στατιστικά σημαντική διαφορά μεταξύ Ανδρών και Γυναικών χρηστών αναφορικά με την «Έκθεση

σε Κίνδυνο» (Mann-Whitney t = 9220,50, $n_1$=110, $n_2$=224, p<0,05). Αυτό έχει ως αποτέλεσμα ότι Άνδρες και Γυναίκες εκτίθενται διαφορετικά στον κίνδυνο σε ΙΚΔ.

## 5.3 Πίνακες και Σχήματα

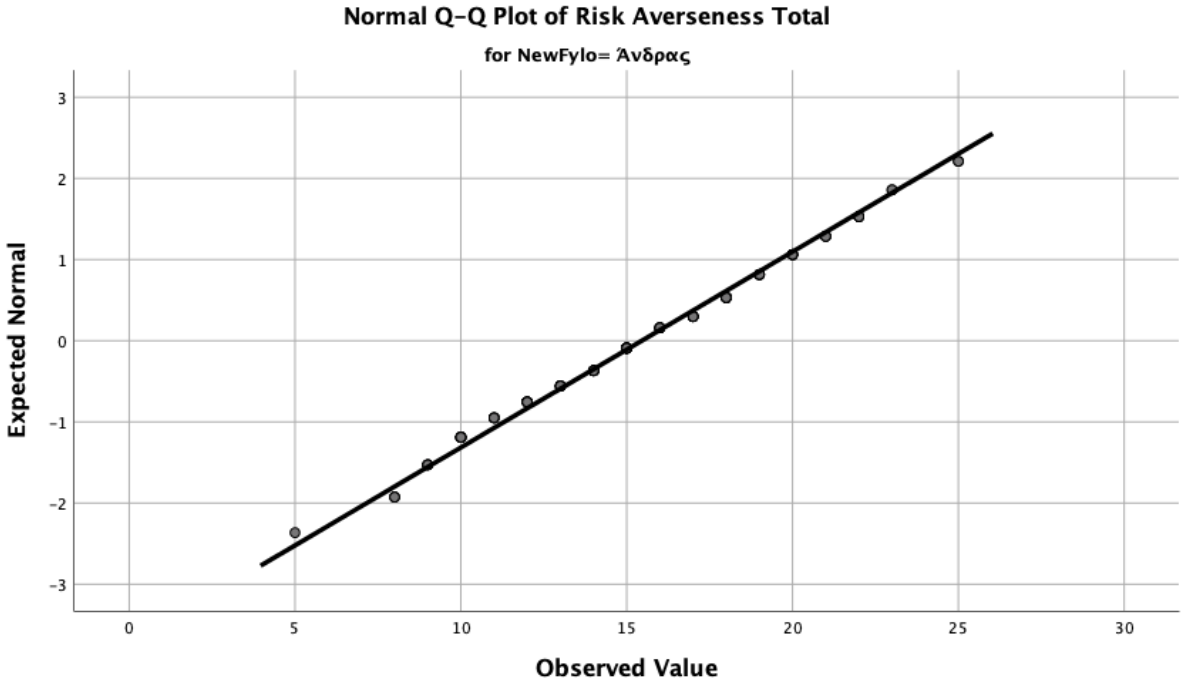
### Έλεγχος Κανονικότητας Risk Averseness & Φύλο

**Tests of Normality**

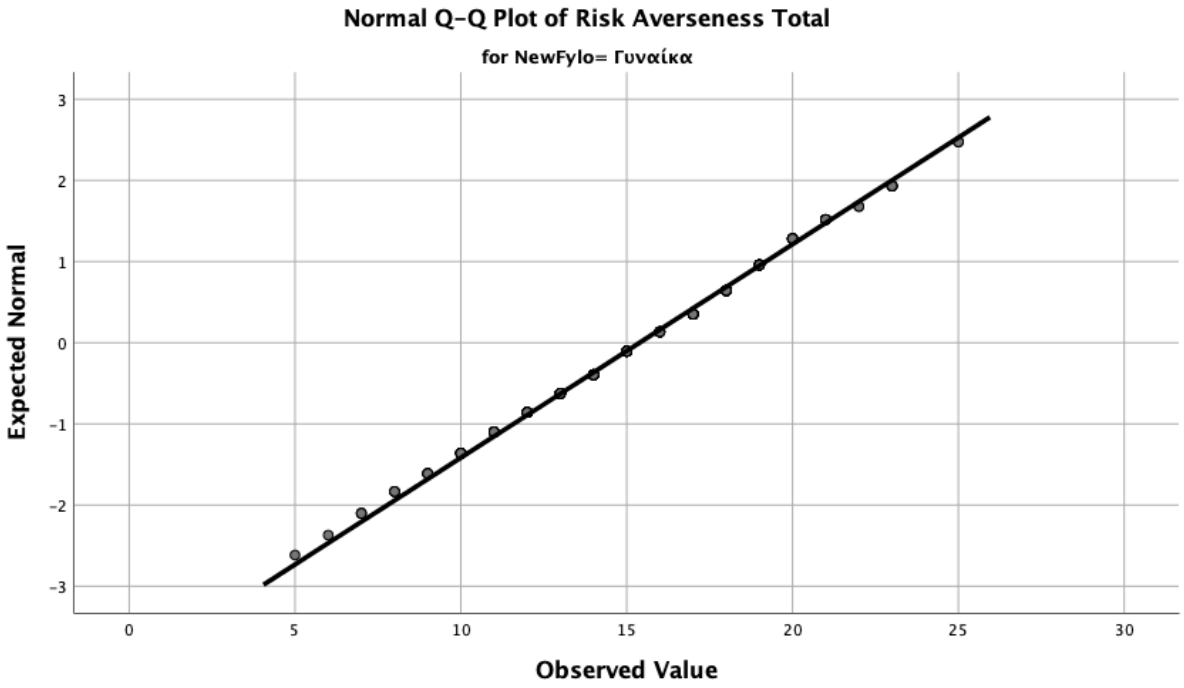
| | Φύλο | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | | Statistic | df | Sig. | Statistic | df | Sig. |
| Risk Averseness Total | Άνδρας | .085 | 110 | .049 | .986 | 110 | .332 |
| | Γυναίκα | .084 | 224 | .001 | .990 | 224 | .115 |

a. Lilliefors Significance Correction

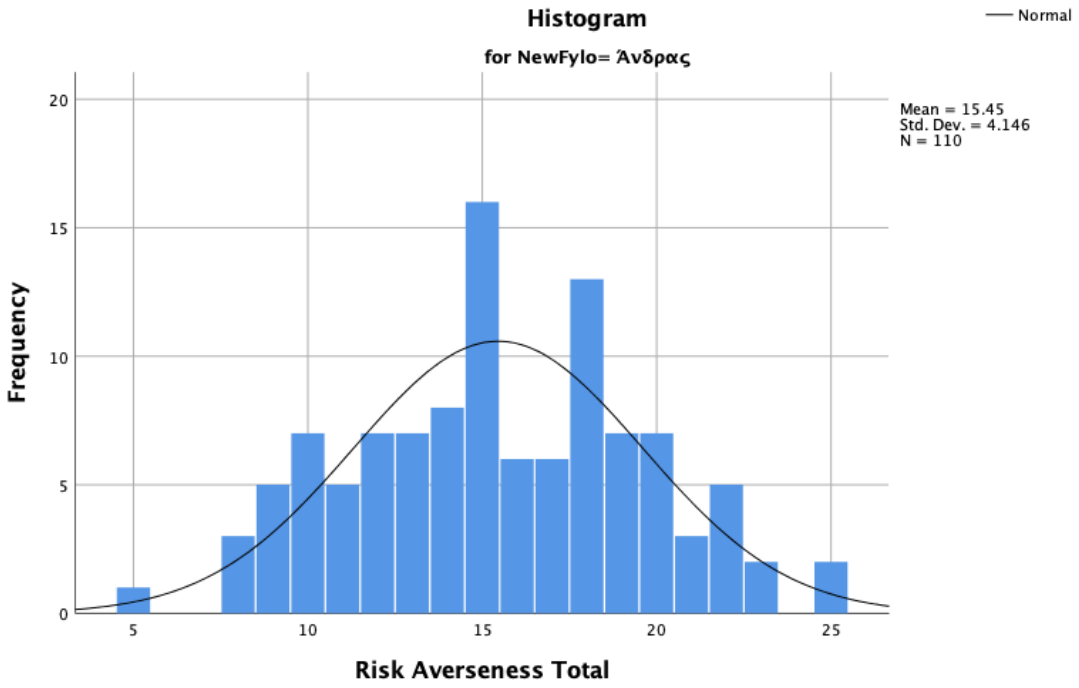
*Πίνακας: 75 Test Κανονικότητας Risk Averseness & Φύλο*



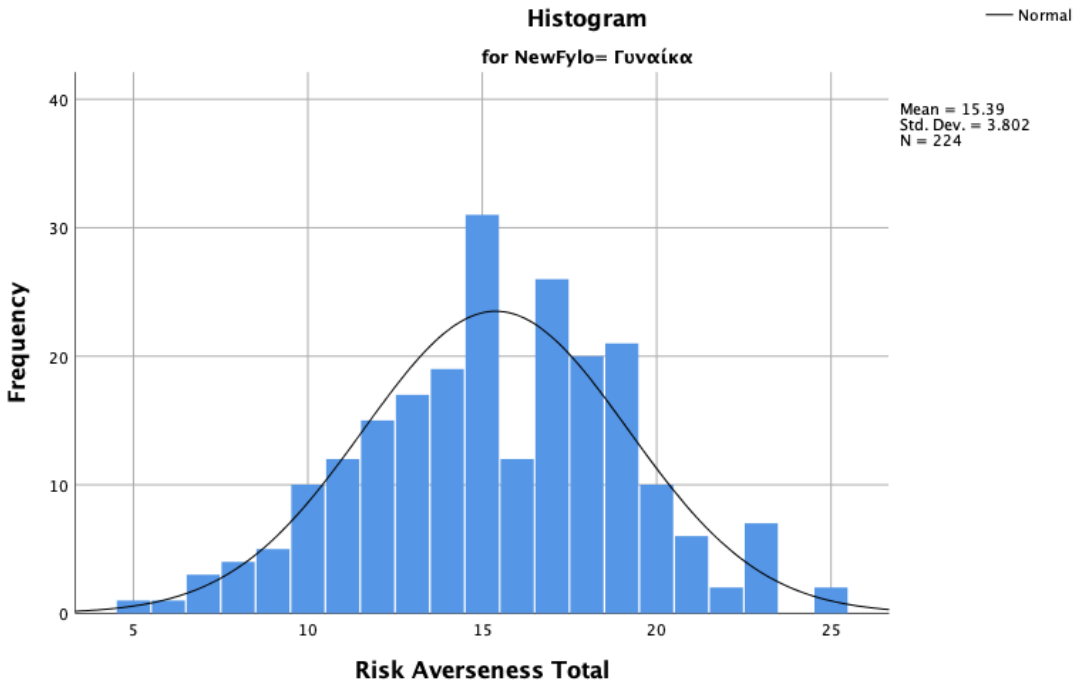

*Γράφημα: 18 Q-Q Plot Risk Averseness & Φύλο Άνδρας*




*Γράφημα: 19 Q-Q Plot Risk Averseness & Φύλο Γυναίκα*




*Γράφημα: 20 Ιστόγραμμα Risk Averseness & Φύλο 'Ανδρας*




*Γράφημα: 21 Ιστόγραμμα Risk Averseness & Φύλο Γυναίκα*

## Έλεγχος Κανονικότητας Risk Averseness & Ηλικία

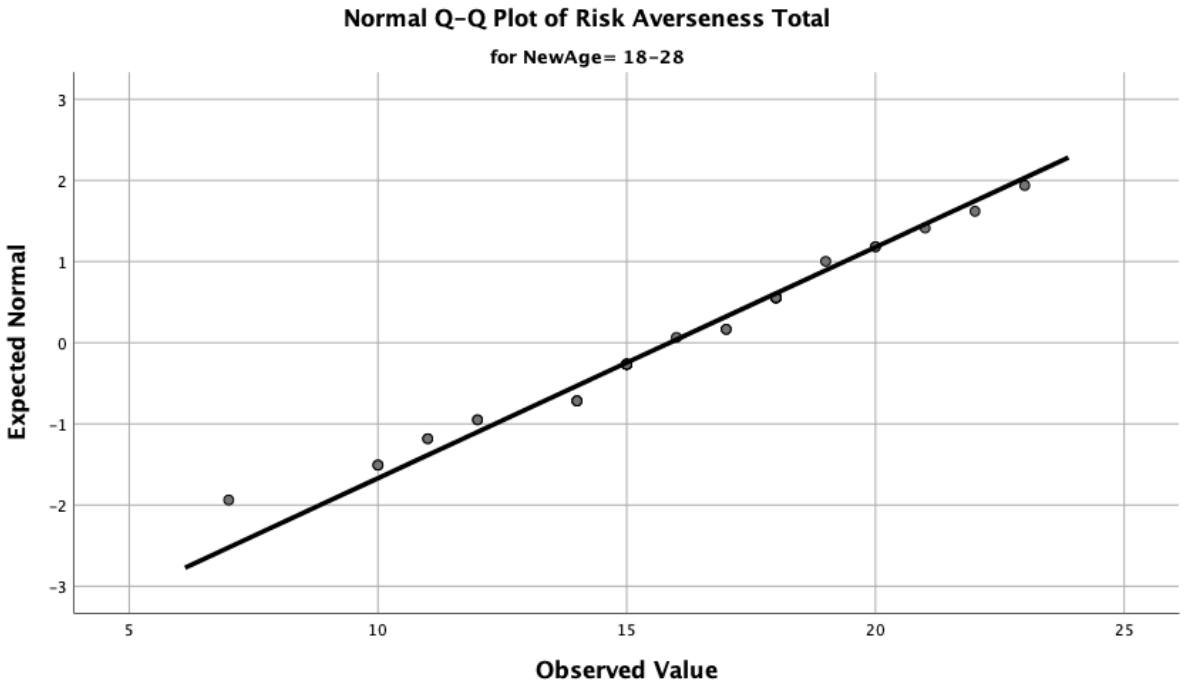
**Tests of Normality[b]**

| | Ηλικία | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | | Statistic | df | Sig. | Statistic | df | Sig. |
| Risk Averseness Total | 18-28 | .134 | 37 | .093 | .967 | 37 | .335 |
| | 29-38 | .136 | 71 | .002 | .953 | 71 | .010 |
| | 39-48 | .082 | 119 | .046 | .989 | 119 | .445 |
| | 49-68 | .107 | 106 | .004 | .980 | 106 | .113 |

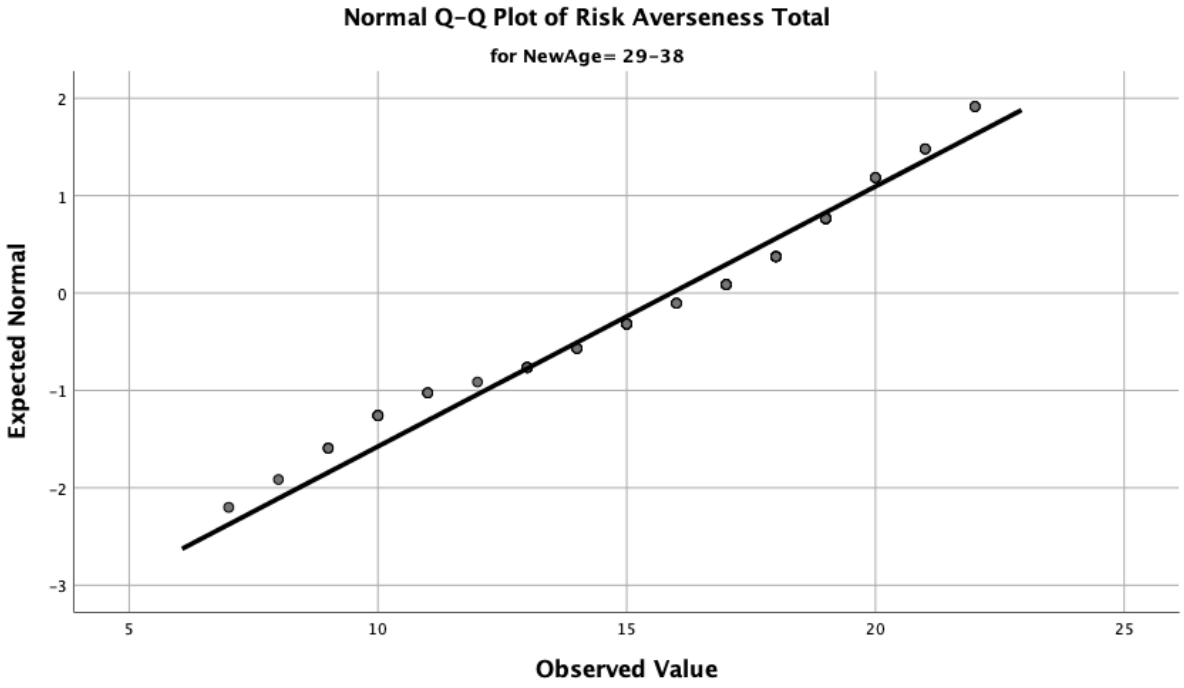
a. Lilliefors Significance Correction

b. Risk Averseness Total is constant when Ηλικία = 69+. It has been omitted.

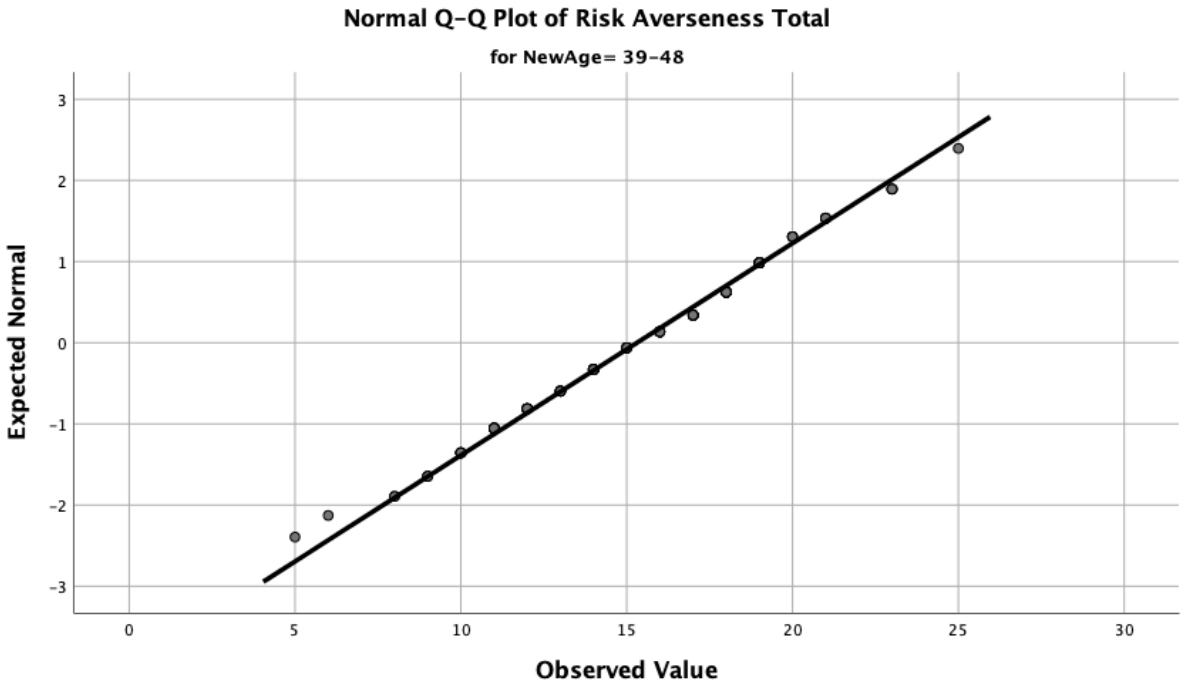
*Πίνακας: 76 Test Κανονικότητας Risk Averseness & Ηλικία*



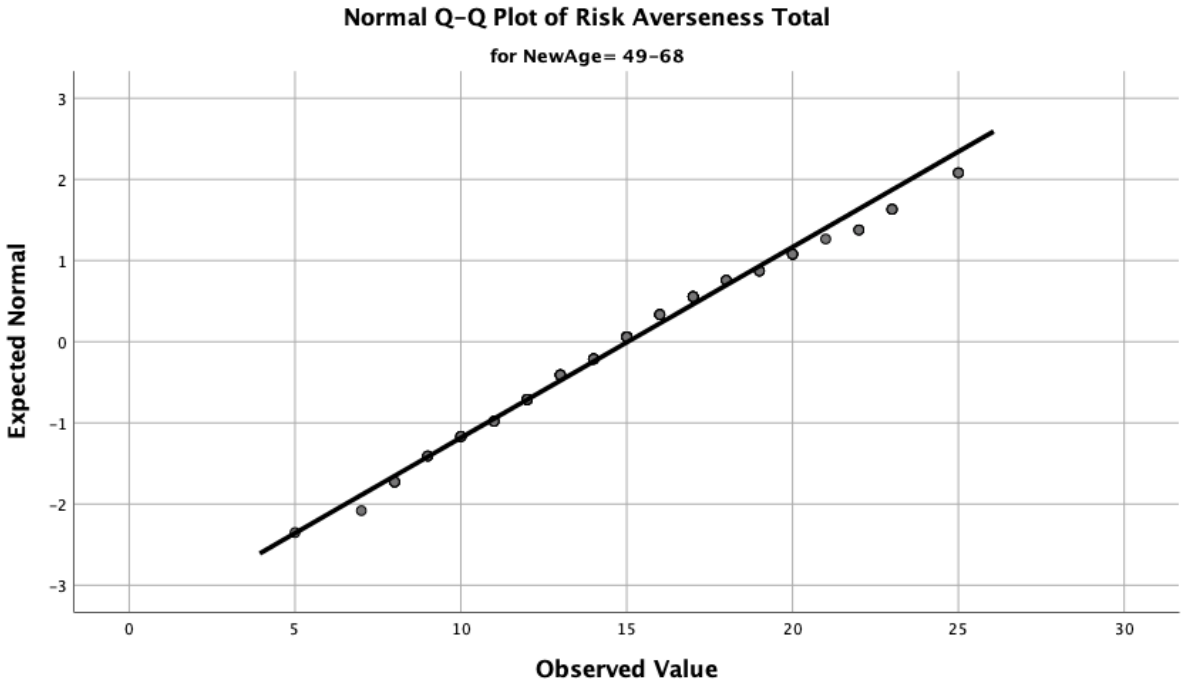

*Γράφημα: 22 Q-Q Plot Risk Averseness Ηλικία 18-28*




*Γράφημα: 23 Q-Q Plot Risk Averseness Ηλικία 29-38*




*Γράφημα: 24 Q-Q Plot Risk Averseness Ηλικία 39-48*




*Γράφημα: 25 Q-Q Plot Risk Averseness Ηλικία 49-68*

## Έλεγχος Κανονικότητας Εμπιστοσύνη "Trust" και Φύλο

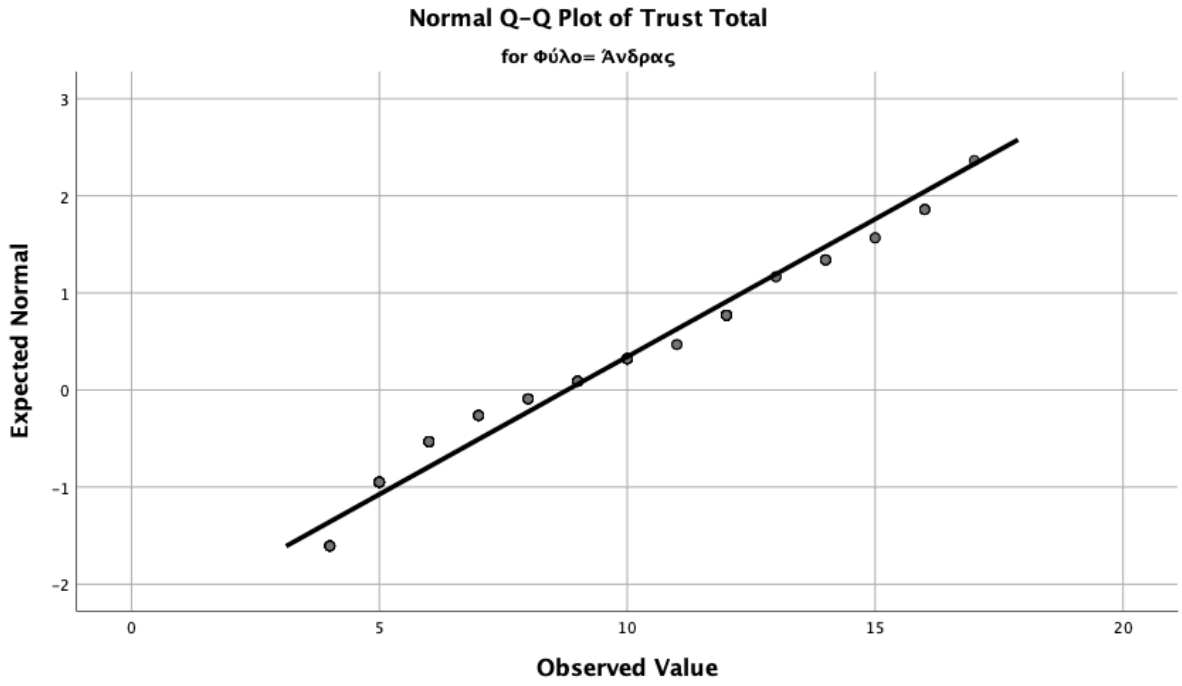
**Tests of Normality**

| | | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | Φύλο | Statistic | df | Sig. | Statistic | df | Sig. |

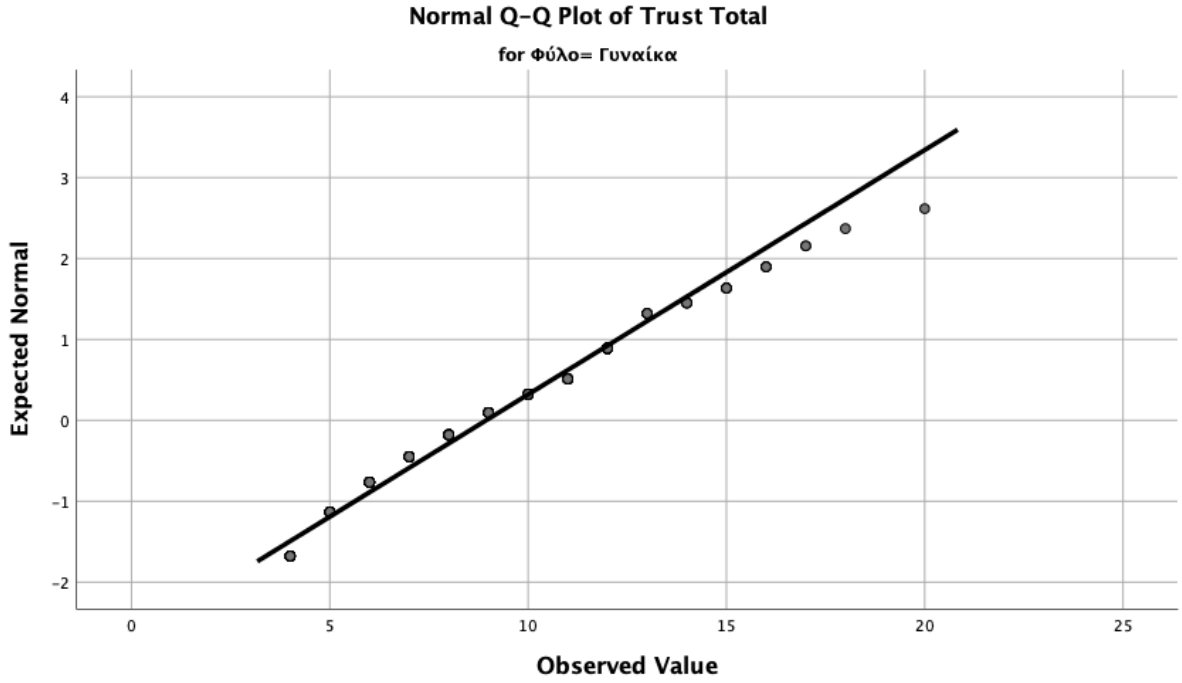
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Trust Total | Άνδρας | .140 | 110 | .000 | .934 | 110 | .000 |
| | Γυναίκα | .096 | 224 | .000 | .957 | 224 | .000 |

a. Lilliefors Significance Correction

*Πίνακας: 77 Test Κανονικότητας Εμπιστοσύνη Trust και Φύλο*




*Γράφημα: 26 Q-Q Plot Εμπιστοσύνη Trust & Φύλο Άνδρας*




*Γράφημα: 27 Q-Q Plot Εμπιστοσύνη Trust & Φύλο Γυναίκα*

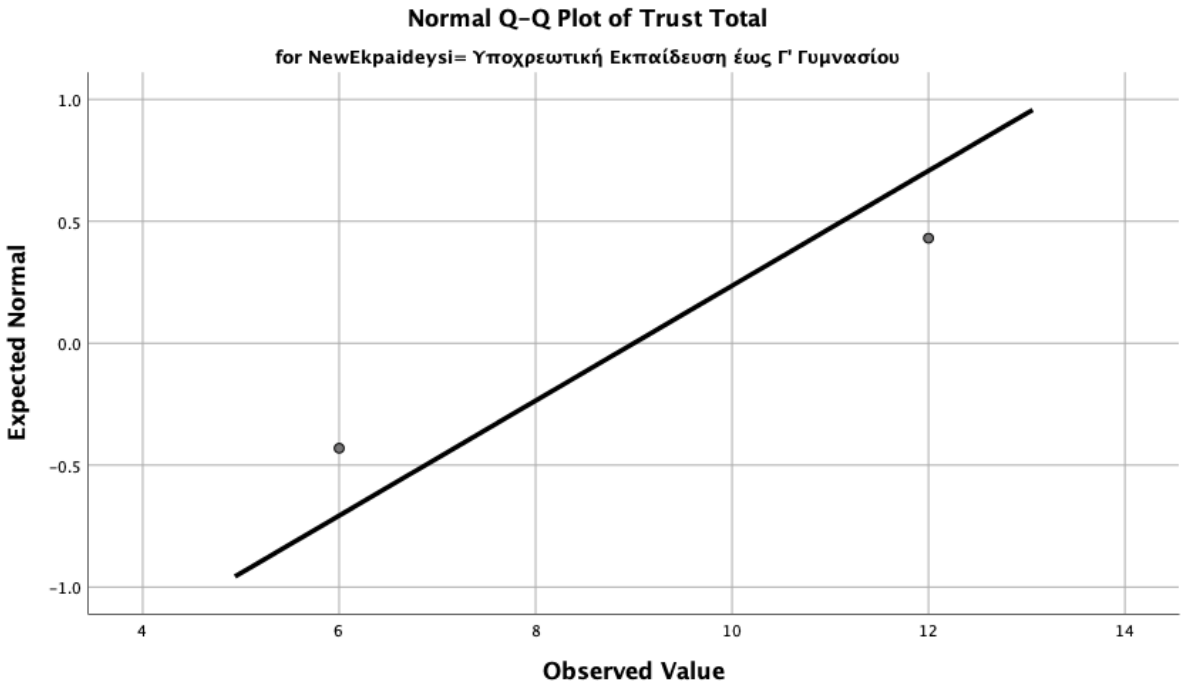
Έλεγχος Κανονικότητας «Εμπιστοσύνη "Trust" και Εκπαίδευση/ Μορφωτικό Επίπεδο.

**Tests of Normality**

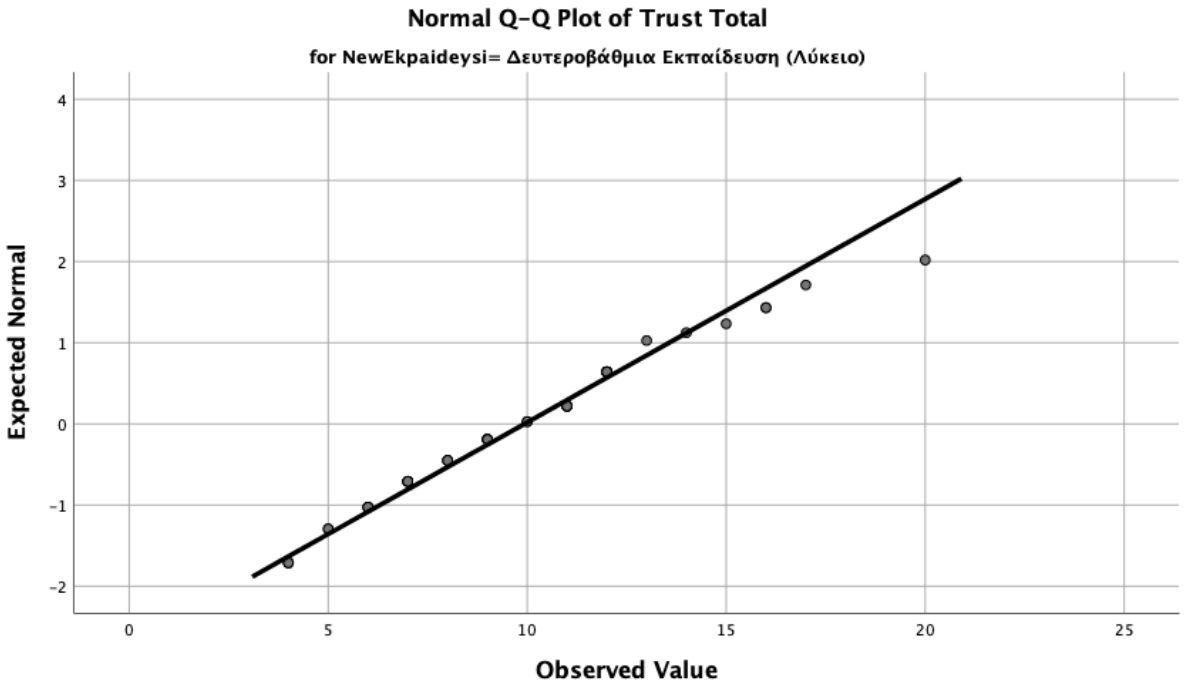
| | Εκπαίδευση | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | | Statistic | df | Sig. | Statistic | df | Sig. |
| Trust Total | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | .260 | 2 | . | | | |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | .129 | 45 | .058 | .964 | 45 | .179 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | .115 | 287 | .000 | .949 | 287 | .000 |

a. Lilliefors Significance Correction

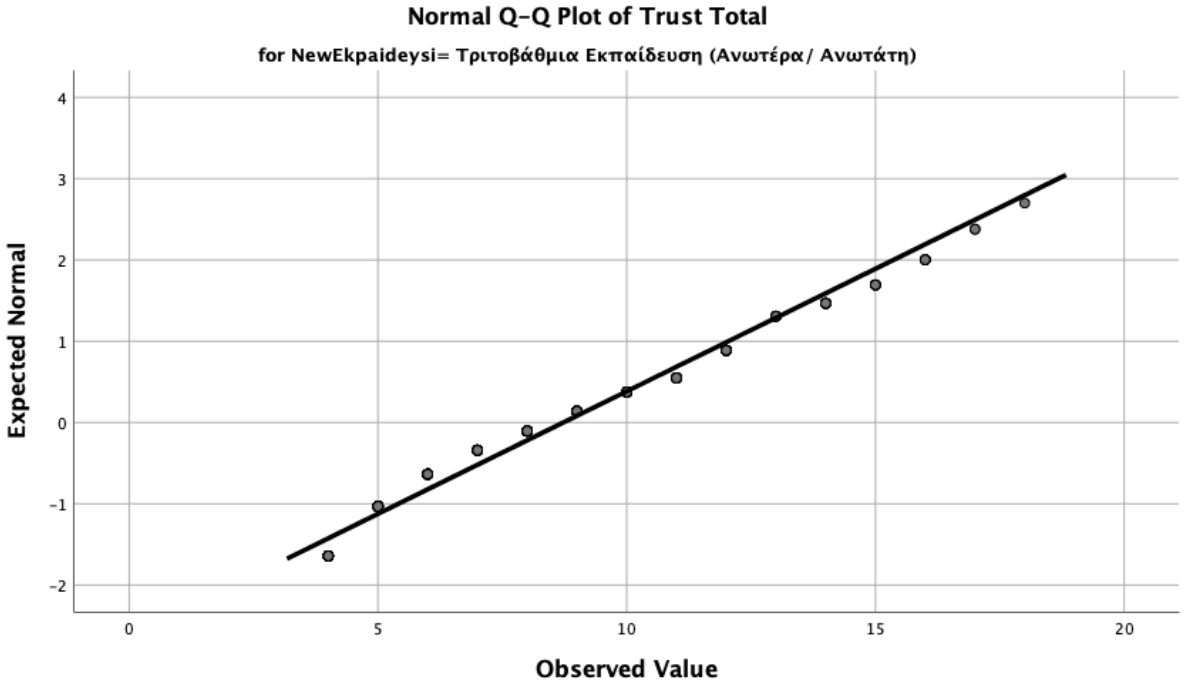
*Πίνακας: 78 Test Κανονικότητας Trust / Εκπαίδευση*




*Γράφημα: 28 Q-Q Plot Εμπιστοσύνη (Trust) Υποχρεωτική Εκπαίδευση*




*Γράφημα: 29 Q-Q Plot Εμπιστοσύνη (Trust) - Δευτεροβάθμια Εκπαίδευση*




*Γράφημα: 30 Q-Q Plot Εμπιστοσύνη (Trust) - Τριτοβάθμια Εκπαίδευση*

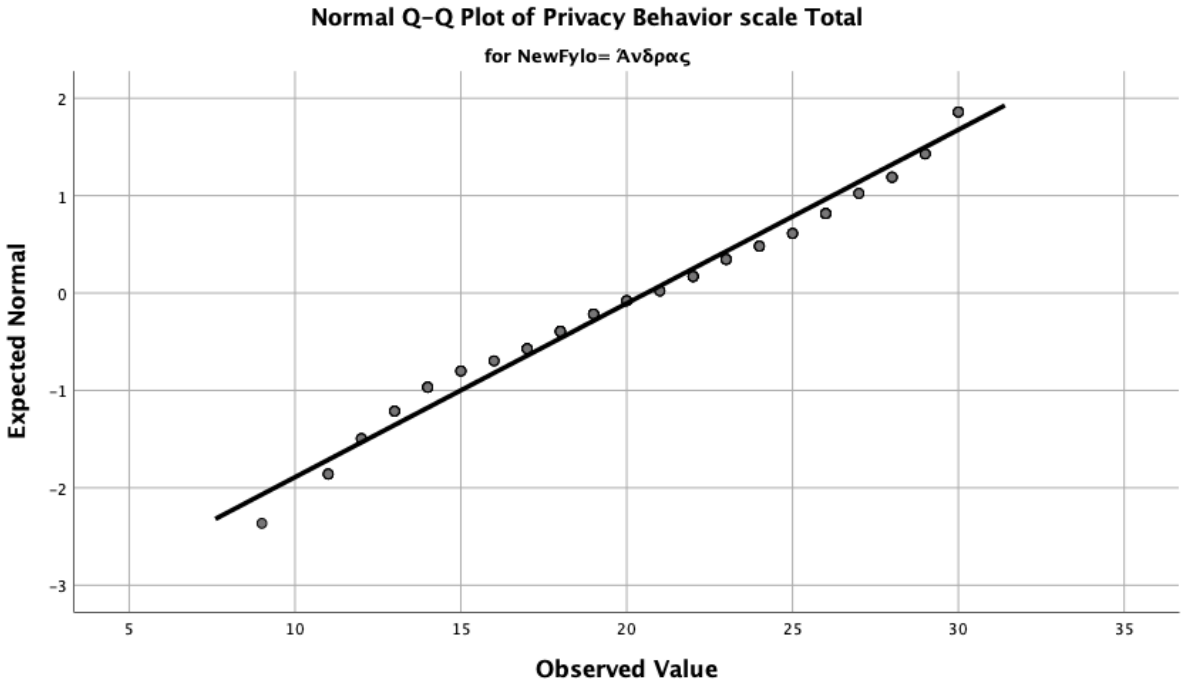
## Έλεγχος Κανονικότητας Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior" & Φύλο

### Tests of Normality

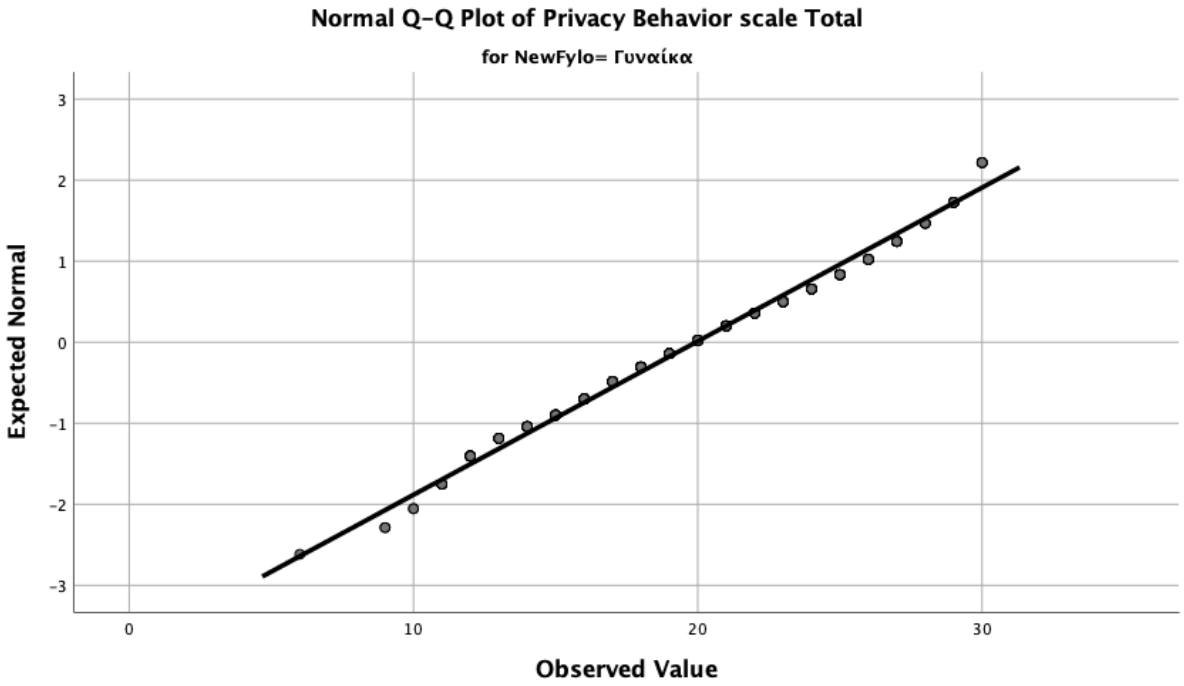
| | | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | Φύλο | Statistic | df | Sig. | Statistic | df | Sig. |
| Privacy Behavior scale Total | Άνδρας | .078 | 110 | .099 | .965 | 110 | .005 |
| | Γυναίκα | .061 | 224 | .043 | .982 | 224 | .006 |

a. Lilliefors Significance Correction

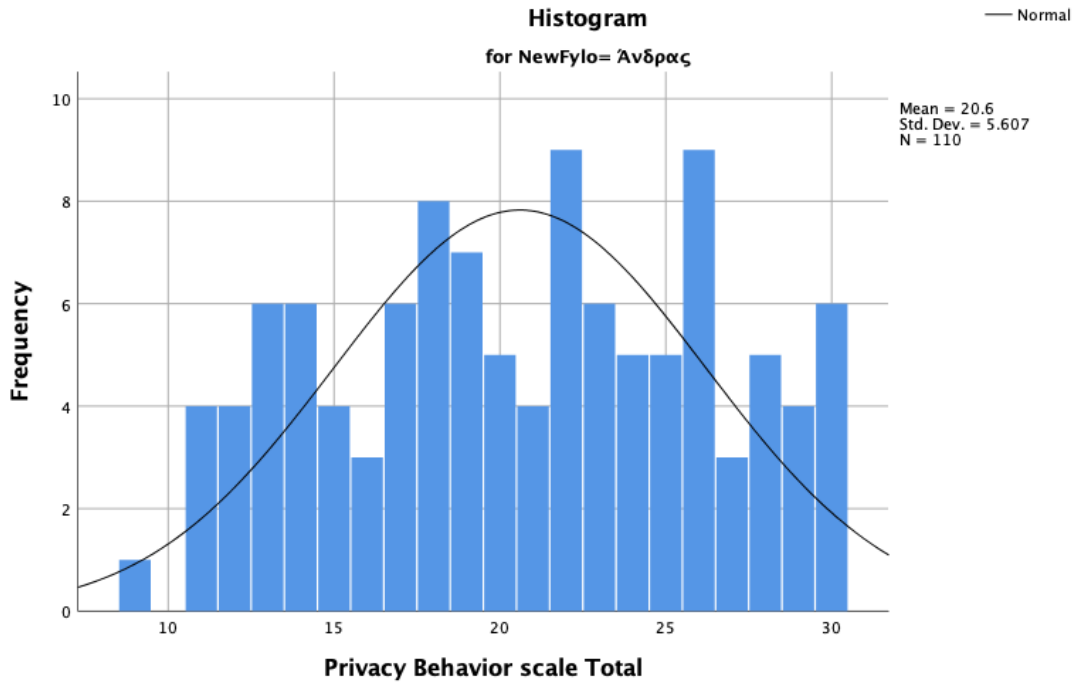
*Πίνακας: 79 Test Κανονικότητας Privacy Behavior (Συμπεριφορά για την Ιδιωτικότητα) & Φύλο*



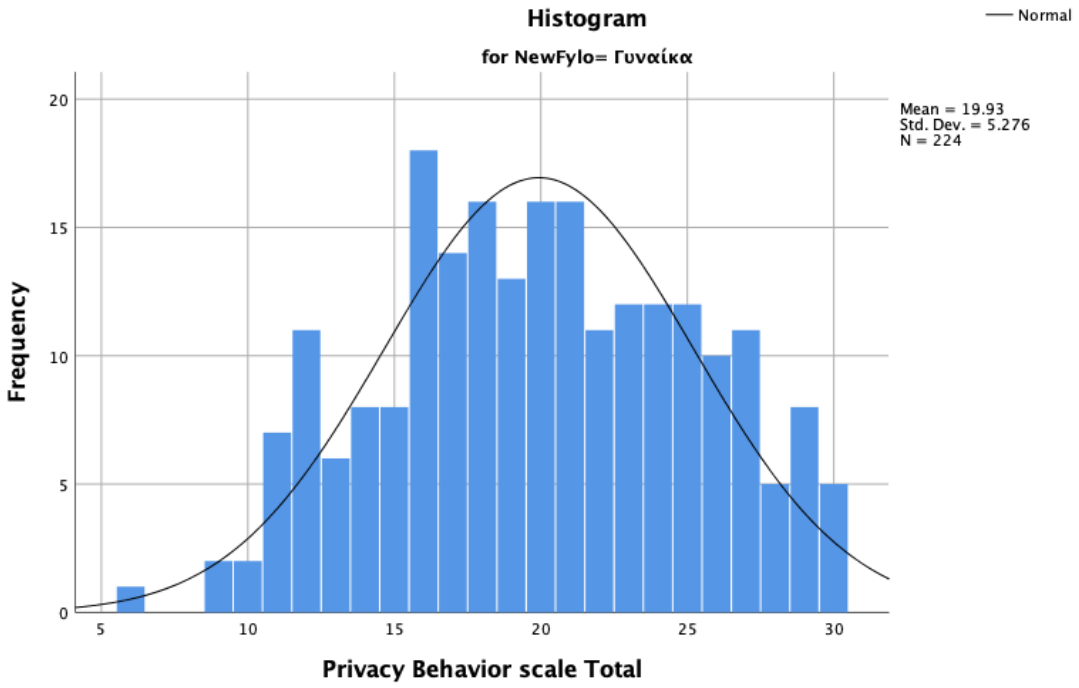

*Γράφημα: 31 Q-Q Plot Privacy Behavior και Φύλο Άνδρας*




*Γράφημα: 32 Q-Q Plot Privacy Behavior και Φύλο Γυναίκα*




*Γράφημα: 33 Ιστόγραμμα Privacy Behavior & Φύλο Άνδρας*




*Γράφημα: 34 Ιστόγραμμα Privacy Behavior & Φύλο Γυναίκα*

## Έλεγχος Κανονικότητας Συμπεριφορά για την Ιδιωτικότητα/Απόρρητο "Privacy Behavior" & την Ηλικία

**Tests of Normality [c]**

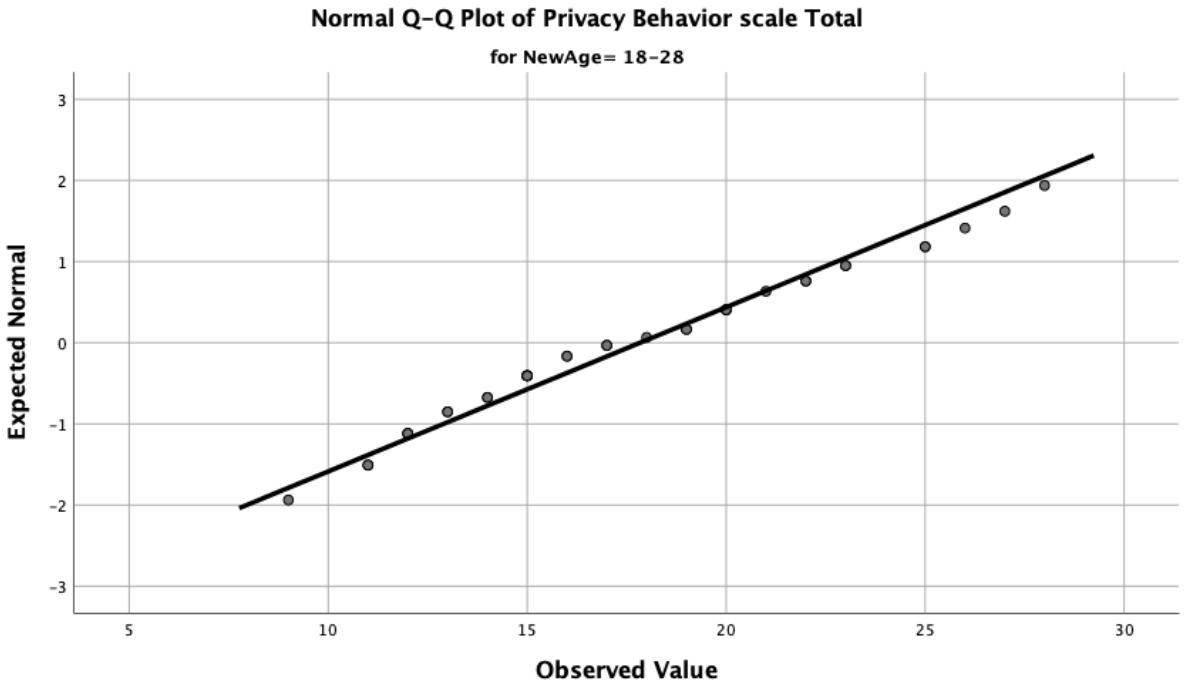
| | | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | Ηλικία | Statistic | df | Sig. | Statistic | df | Sig. |
| Privacy Behavior scale Total | 18-28 | .123 | 37 | .176 | .968 | 37 | .362 |
| | 29-38 | .121 | 71 | .012 | .968 | 71 | .067 |
| | 39-48 | .071 | 119 | .200* | .980 | 119 | .070 |
| | 49-68 | .094 | 106 | .023 | .962 | 106 | .004 |

*. This is a lower bound of the true significance.

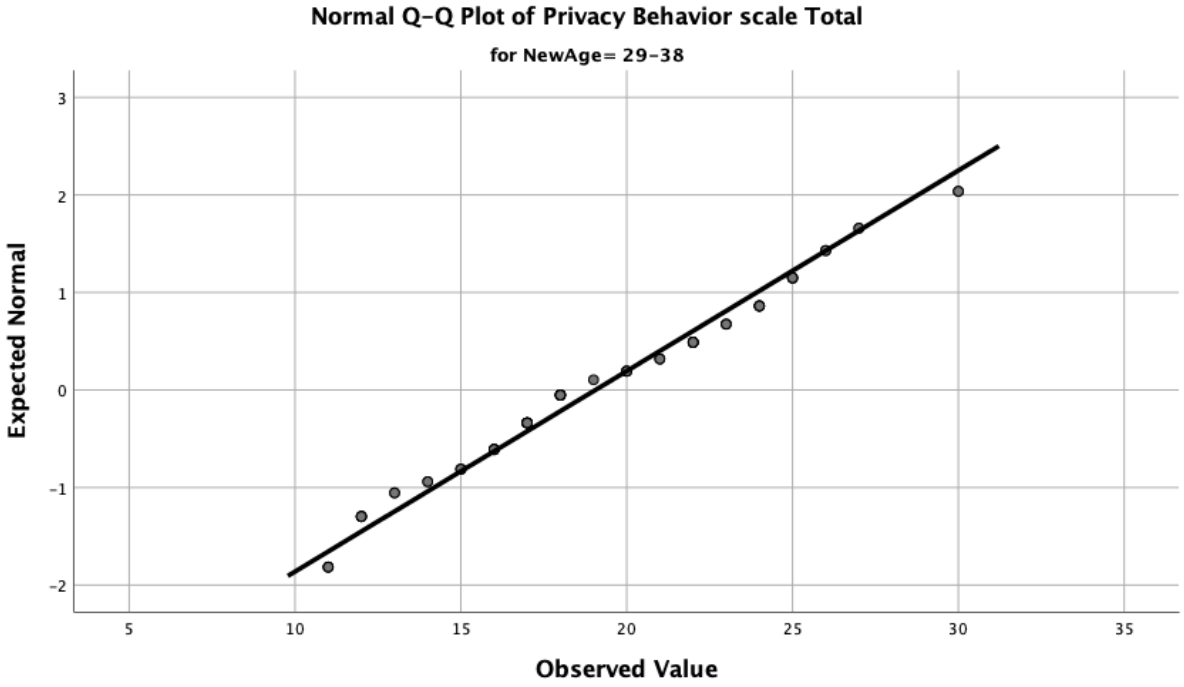
a. Lilliefors Significance Correction

c. Privacy Behavior scale Total is constant when Ηλικία = 69+. It has been omitted.

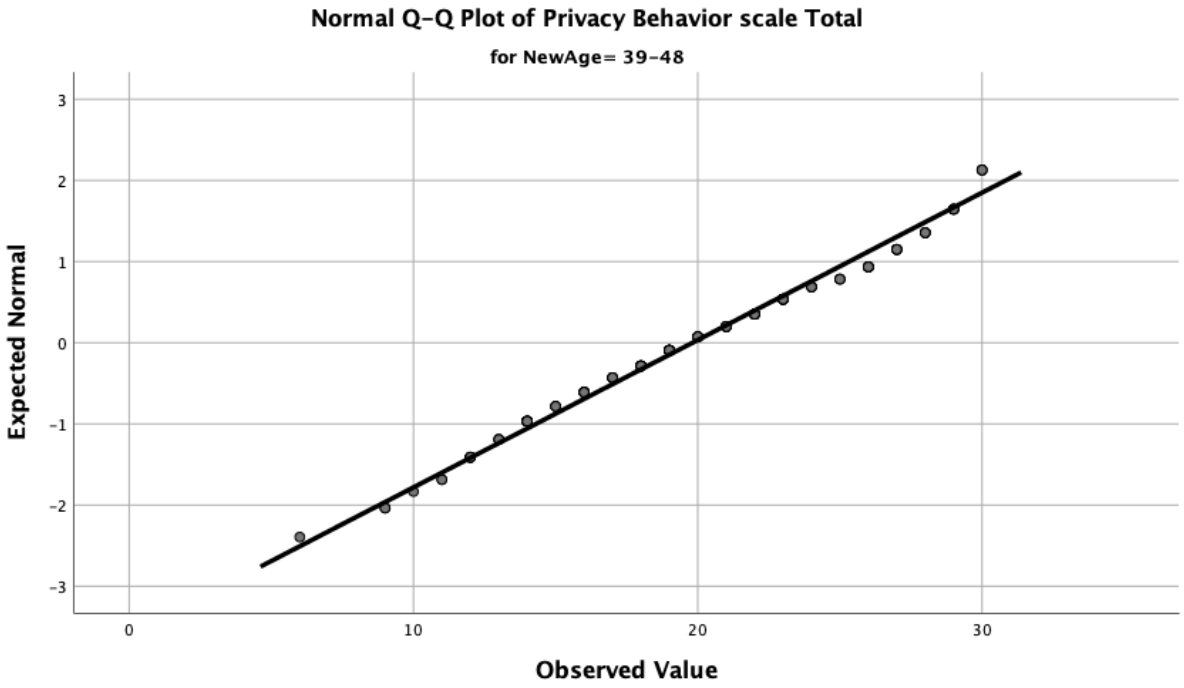
*Πίνακας: 80 Privacy Behavior & Ηλικία Test Κανονικότητας*



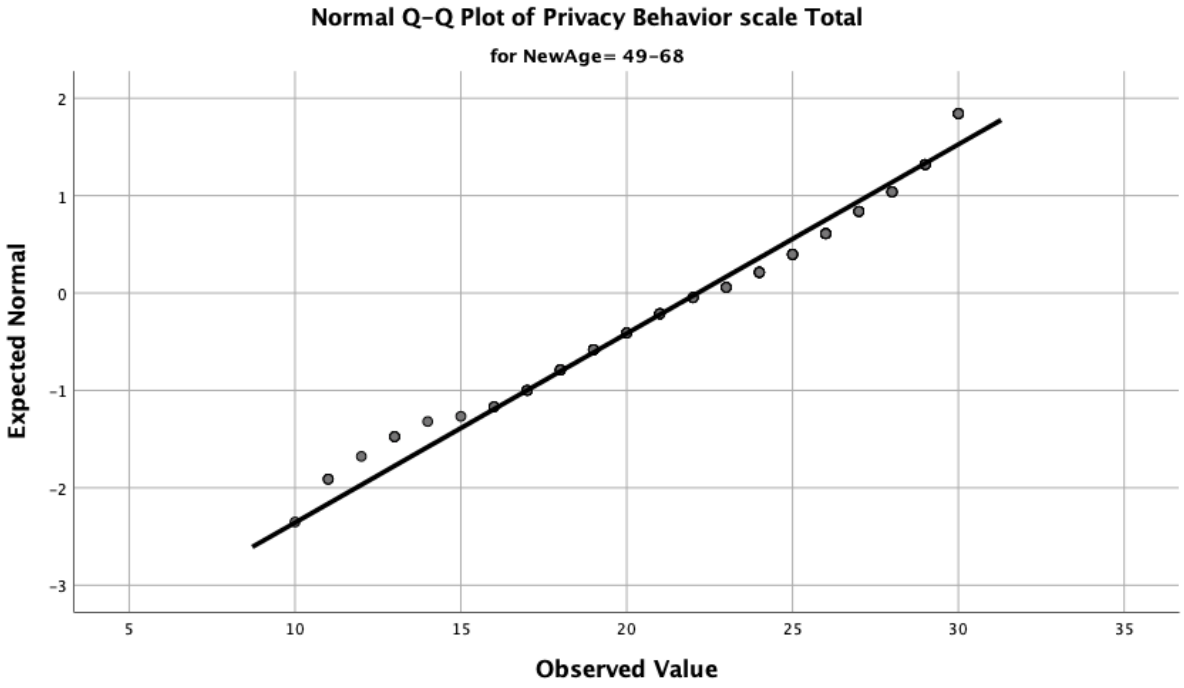

*Γράφημα: 35 Privacy Behavior & Ηλικία 18-28 Q-Q Plot*




*Γράφημα: 36 Privacy Behavior & Ηλικία 29 -38 Q-Q Plot*




*Γράφημα: 37 Privacy Behavior & Ηλικία 39 -48 Q-Q Plot*




*Γράφημα: 38 Privacy Behavior & Ηλικία 49-68 Q-Q Plot*

**Έλεγχος Κανονικότητας Συμπεριφορά Ανησυχία για την Ιδιωτικότητα/Απόρρητο "Privacy Concern"**

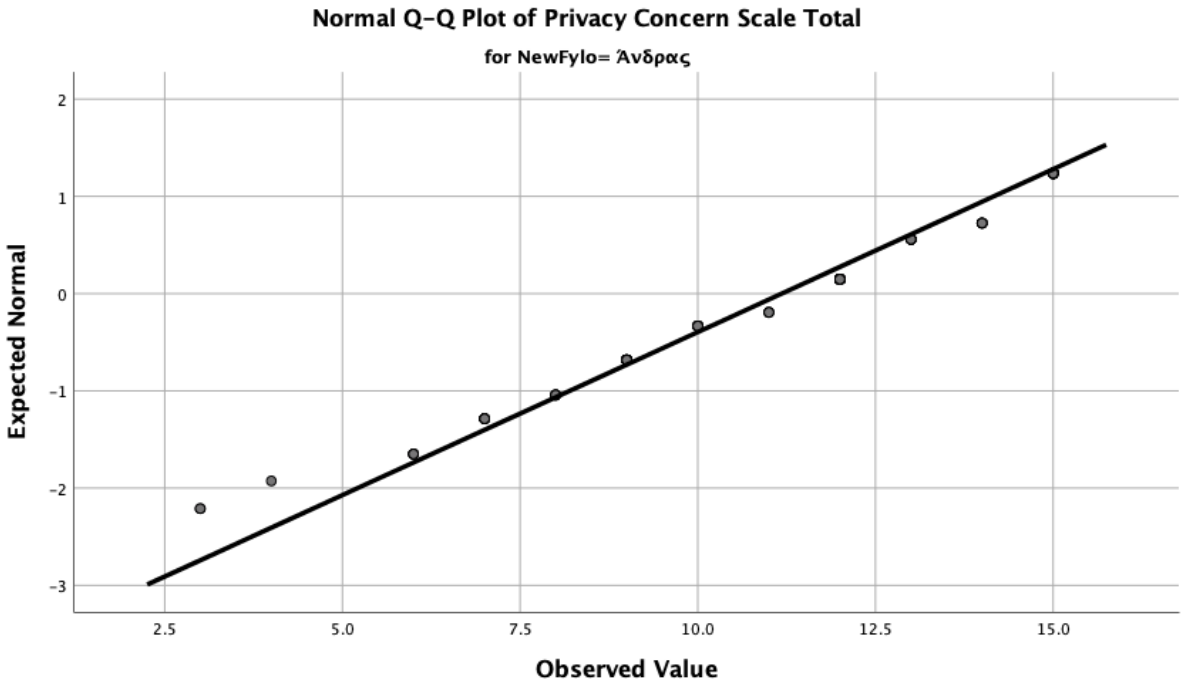
**Tests of Normality**

| | Φύλο | Kolmogorov-Smirnov[a] | Shapiro-Wilk |
|---|---|---|---|

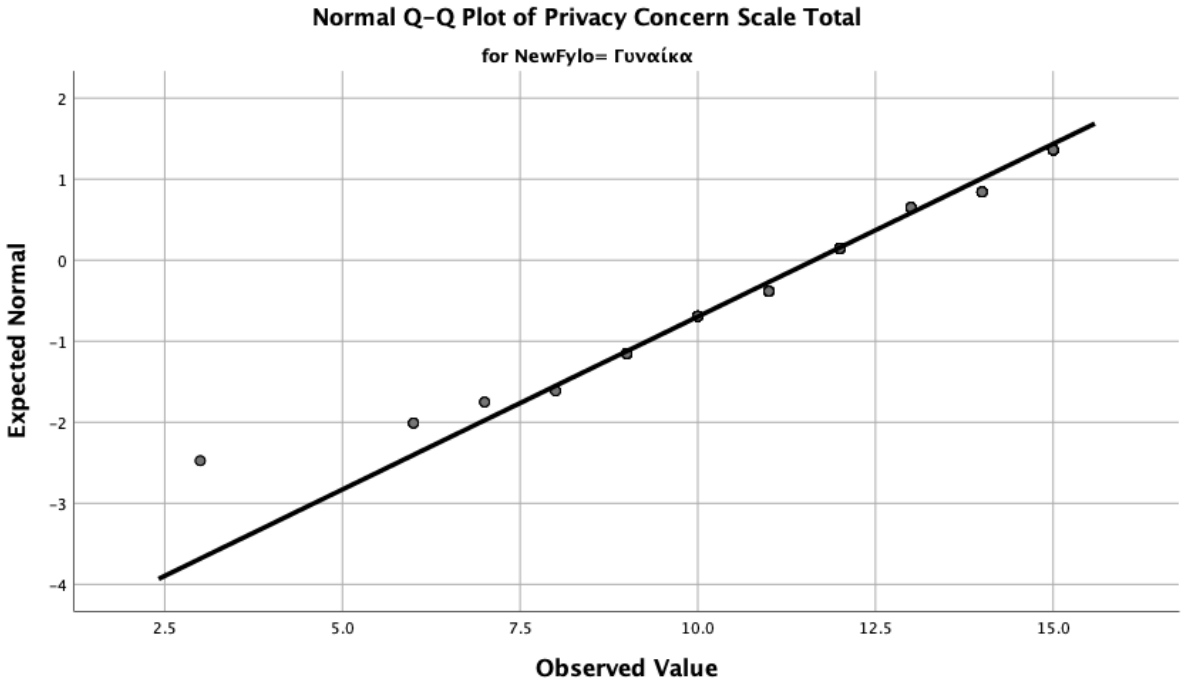
| | | Statistic | df | Sig. | Statistic | df | Sig. |
|---|---|---|---|---|---|---|---|
| Privacy Concern Scale Total | Άνδρας | .172 | 110 | .000 | .927 | 110 | .000 |
| | Γυναίκα | .160 | 224 | .000 | .926 | 224 | .000 |

a. Lilliefors Significance Correction

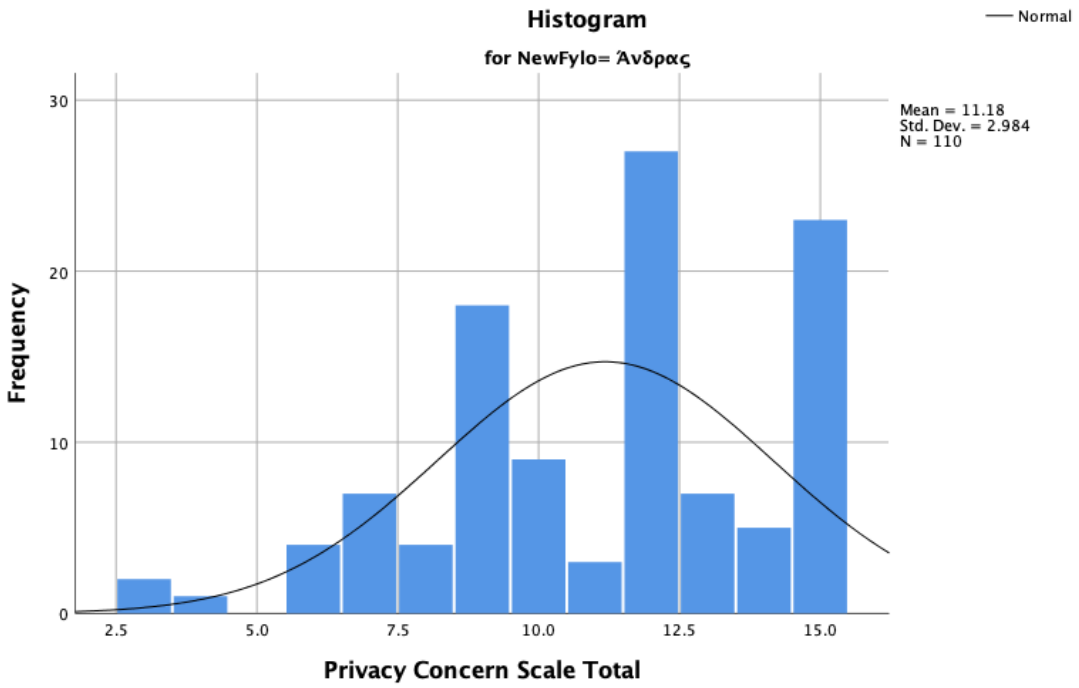
*Πίνακας: 81 Test Κανονικότητας Privacy Concern & Φύλο*



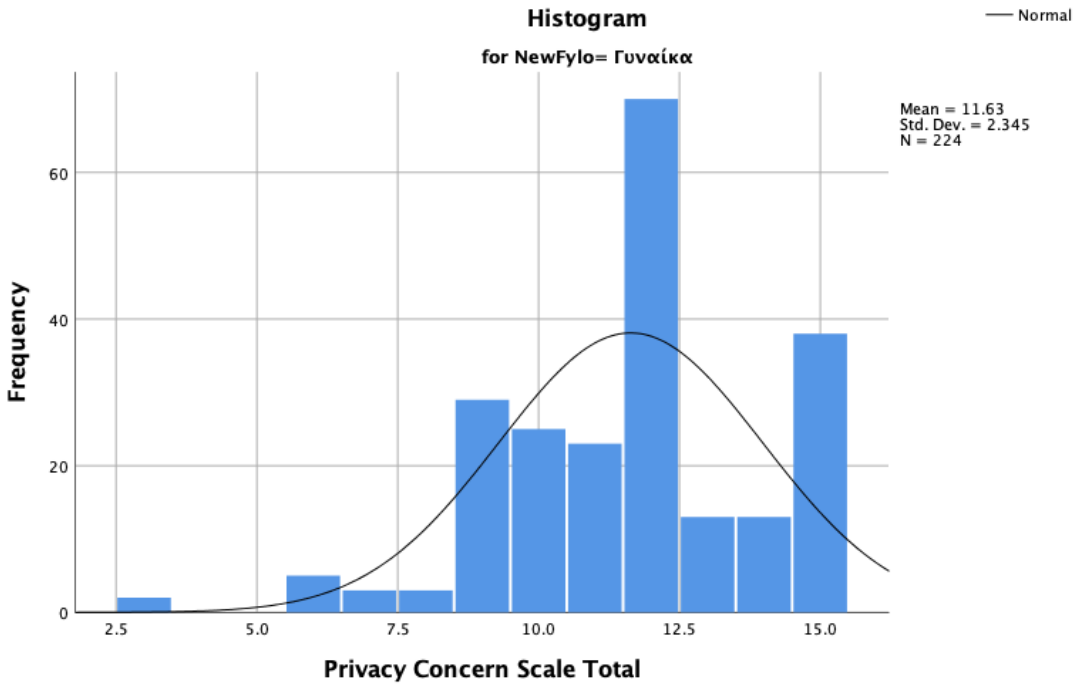

*Γράφημα: 39 Q-Q plot Privacy Concern & Φύλο Άνδρας*




*Γράφημα: 40 Q-Q plot Privacy Concern & Φύλο Γυναίκα*




*Γράφημα: 41 Ιστόγραμμα Privacy Concern & Φύλο Άνδρας*




*Γράφημα: 42 Ιστόγραμμα Privacy Concern & Φύλο*

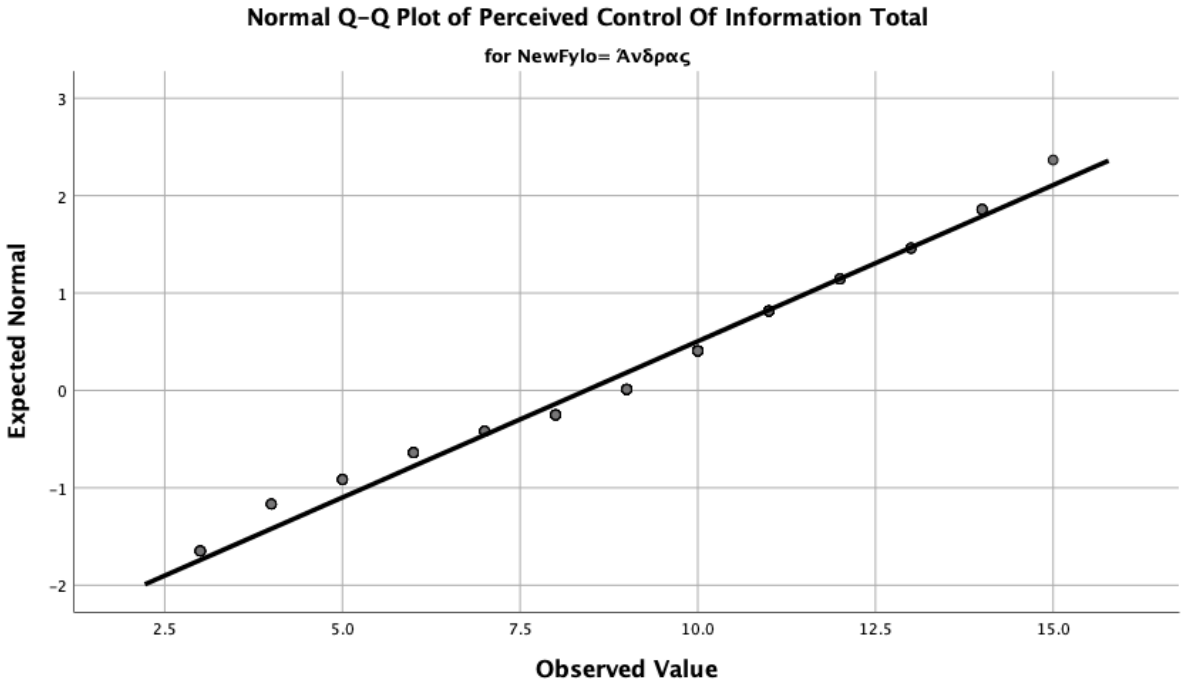
## Έλεγχος Κανονικότητας Perceived Control Of Information & Φύλο

### Tests of Normality

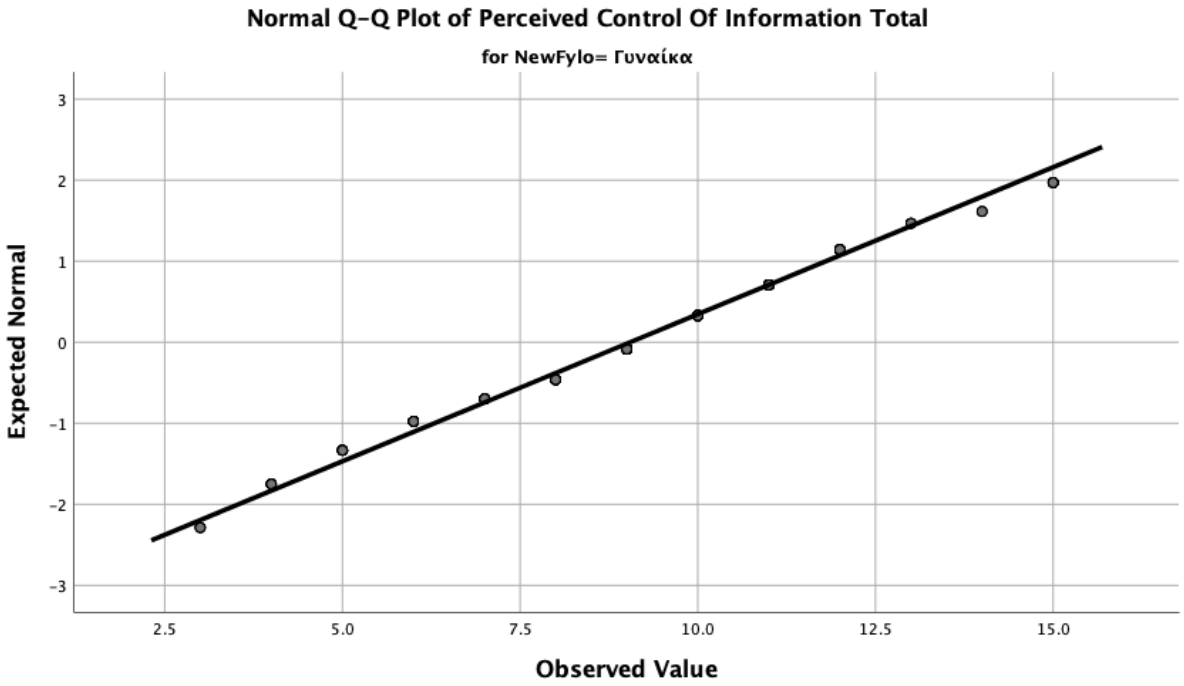
| | Φύλο | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | | Statistic | df | Sig. | Statistic | df | Sig. |
| Perceived Control of Information Total | Άνδρας | .137 | 110 | .000 | .958 | 110 | .001 |
| | Γυναίκα | .127 | 224 | .000 | .973 | 224 | .000 |

a. Lilliefors Significance Correction

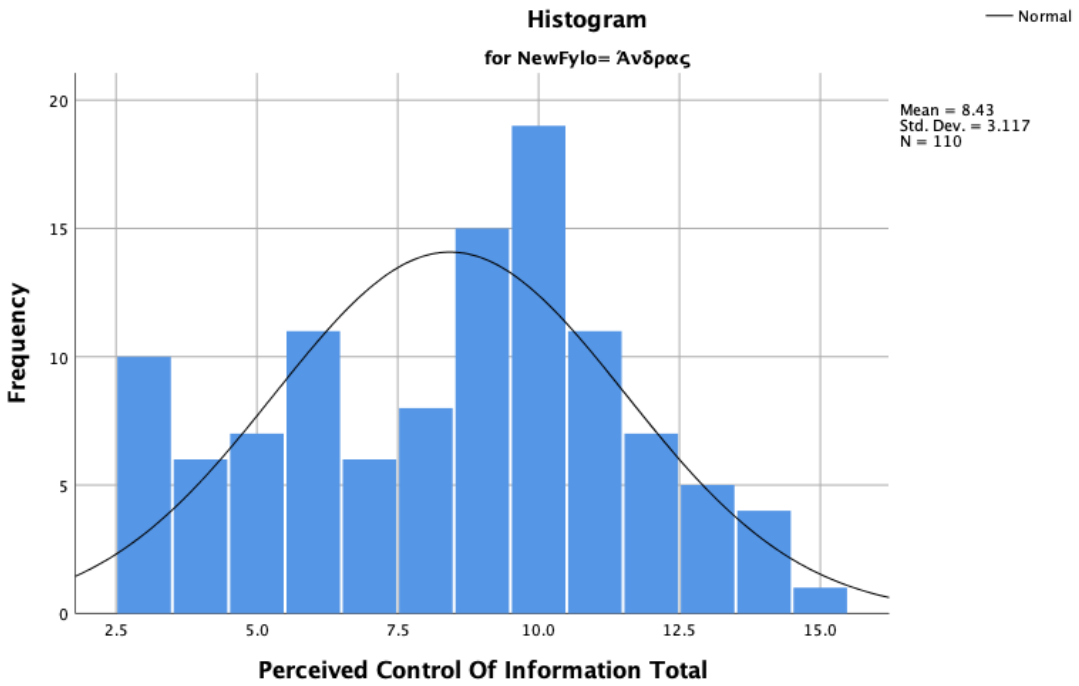
*Πίνακας: 82 Test Κανονικότητας Perceived Control of Information & Φύλο*



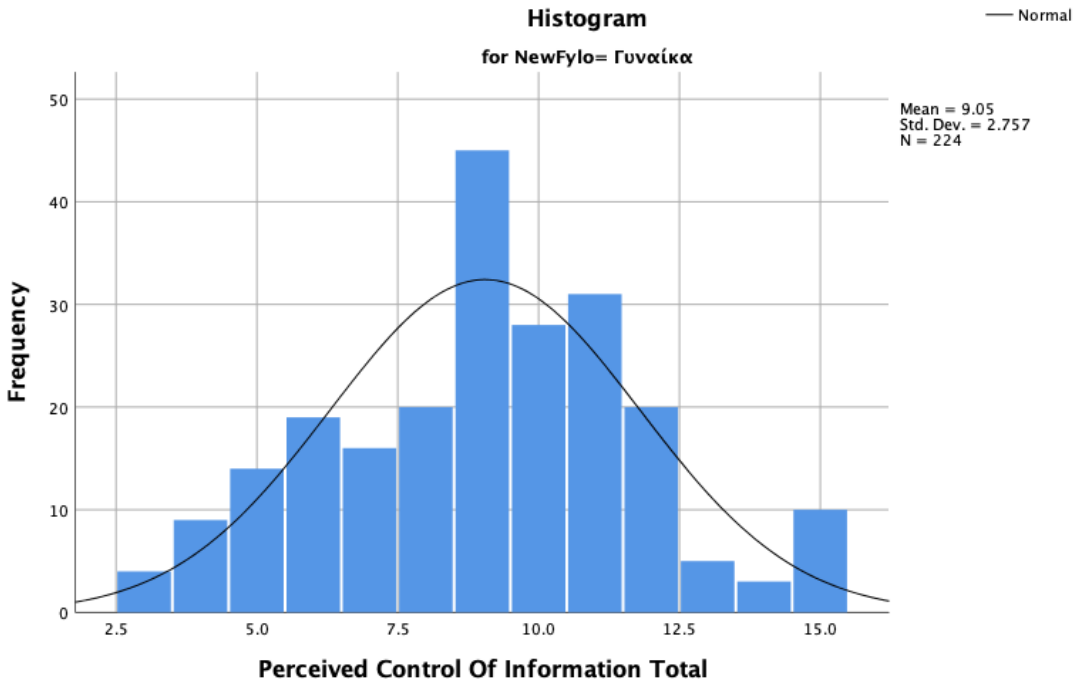

*Γράφημα: 43 Q-Q Plot Perceived Control of Information & Φύλο Άνδρας*




*Γράφημα: 44 Q-Q Plot Perceived Control of Information & Φύλο Γυναίκα*




*Γράφημα: 45 Ιστόγραμμα Perceived Control of Information & Φύλο Άνδρας*




*Γράφημα: 46 Ιστόγραμμα Perceived Control of Information & Φύλο Γυναίκα*

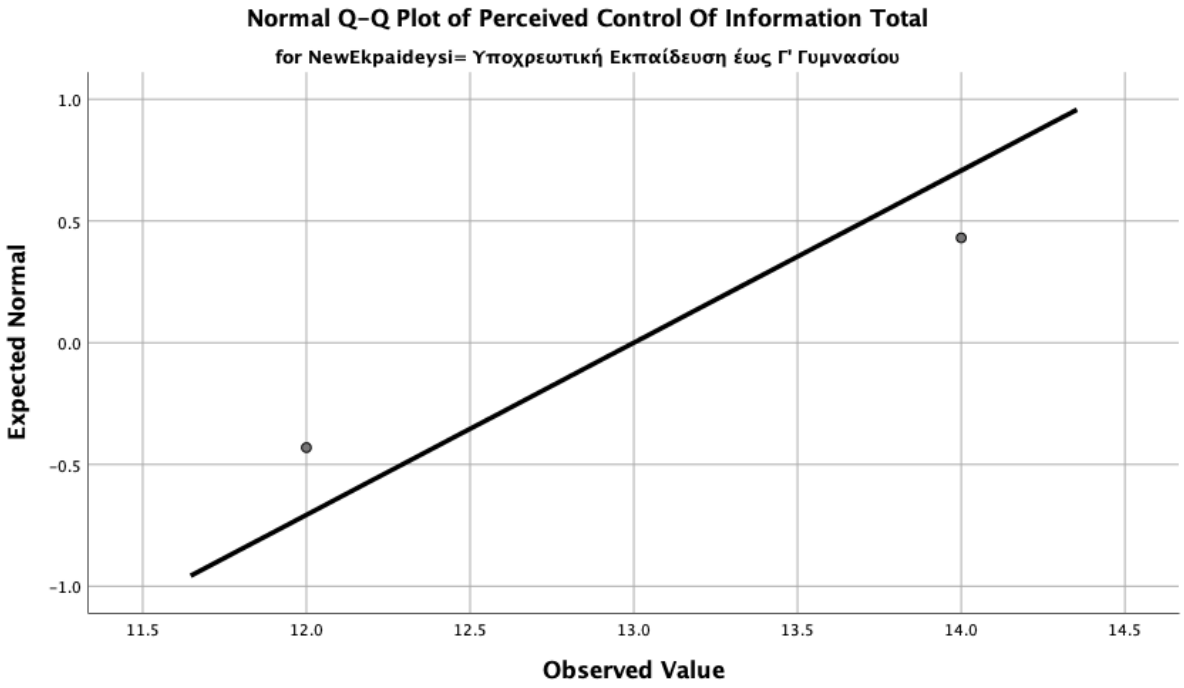
**Έλεγχος κανονικότητας «Αντιληπτός Έλεγχος Πληροφορίας» & Εκπαίδευση/ Μορφωτικό Επίπεδο.**

**Tests of Normality**

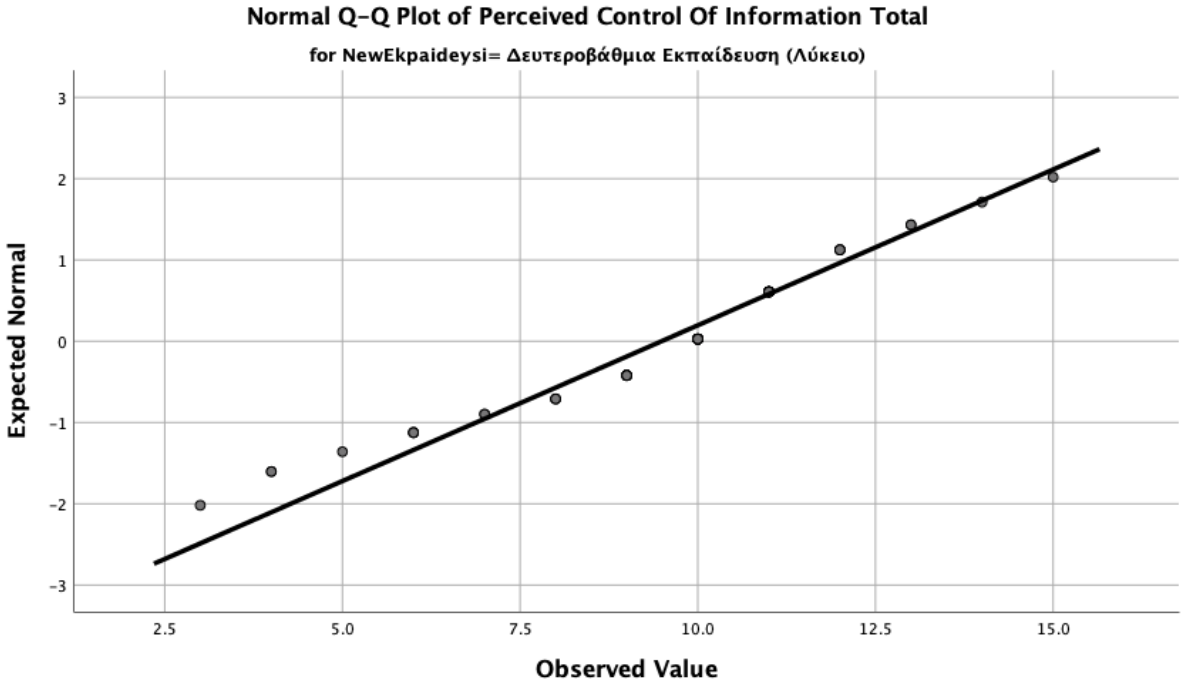
| | Εκπαίδευση | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | | Statistic | df | Sig. | Statistic | df | Sig. |
| Perceived Control of Information Total | Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου | .260 | 2 | . | | | |
| | Δευτεροβάθμια Εκπαίδευση (Λύκειο) | .178 | 45 | .001 | .948 | 45 | .042 |
| | Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη) | .128 | 287 | .000 | .973 | 287 | .000 |

a. Lilliefors Significance Correction

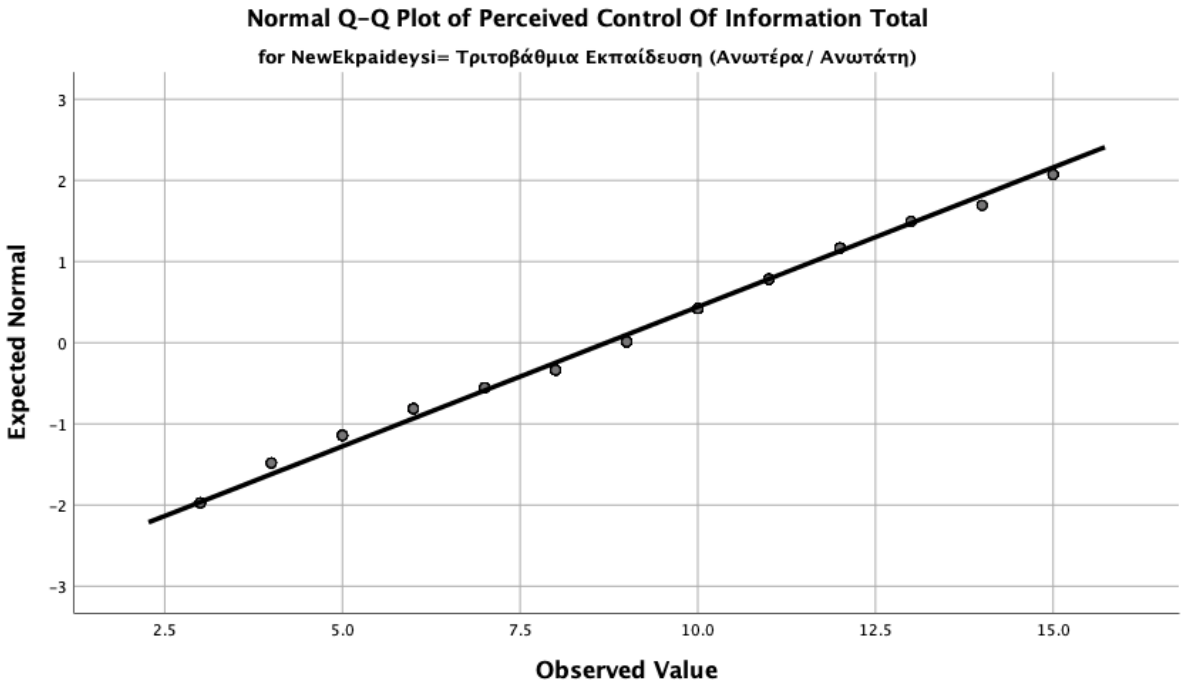
*Πίνακας: 83 Test Κανονικότητας Perceived Control of Information & Εκπαίδευση/ Μορφωτικό Επίπεδο*



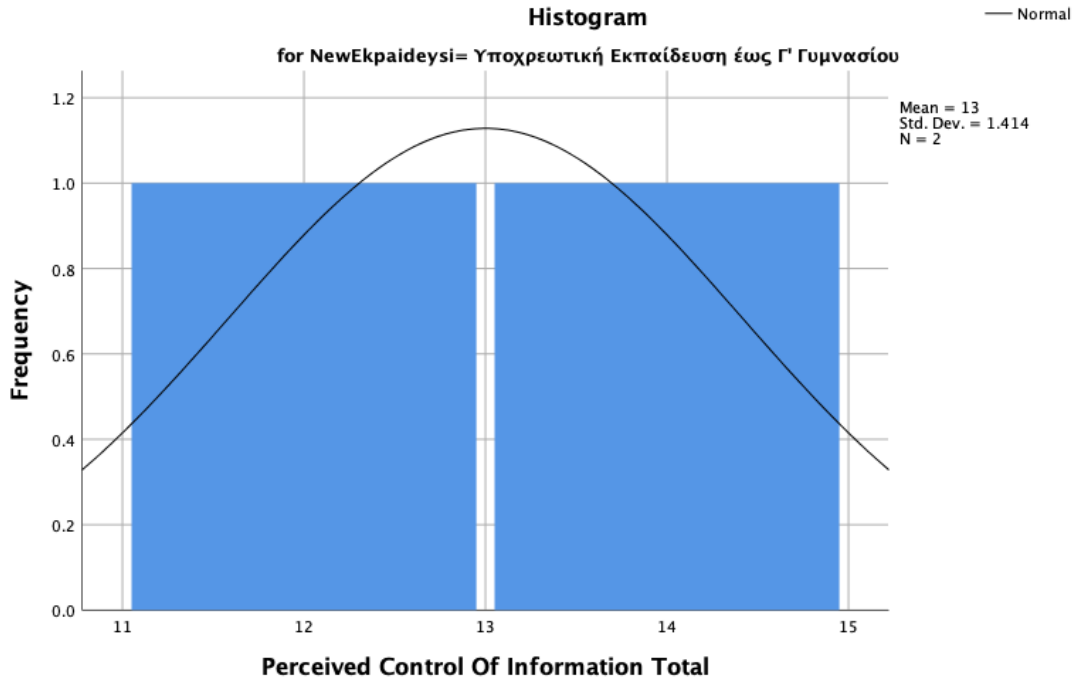

*Γράφημα: 47 Q-Q Plot Perceived Control of Information & Εκπαίδευση Υποχρεωτική*



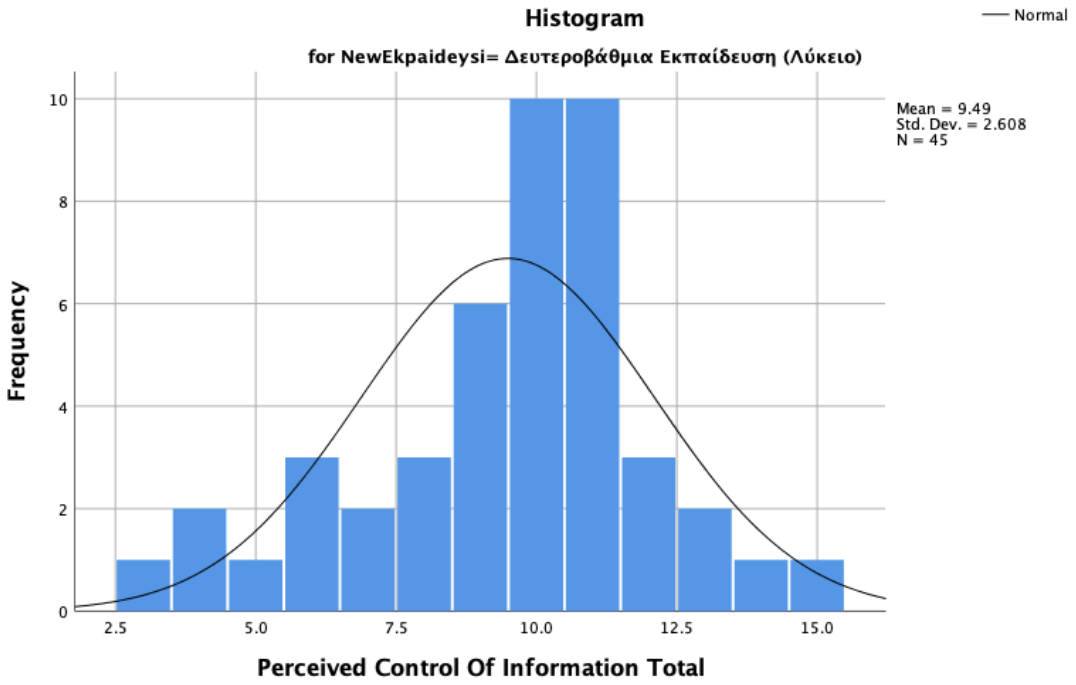

*Γράφημα: 48 Q-Q Plot Perceived Control of Information & Εκπαίδευση Δευτεροβάθμια*



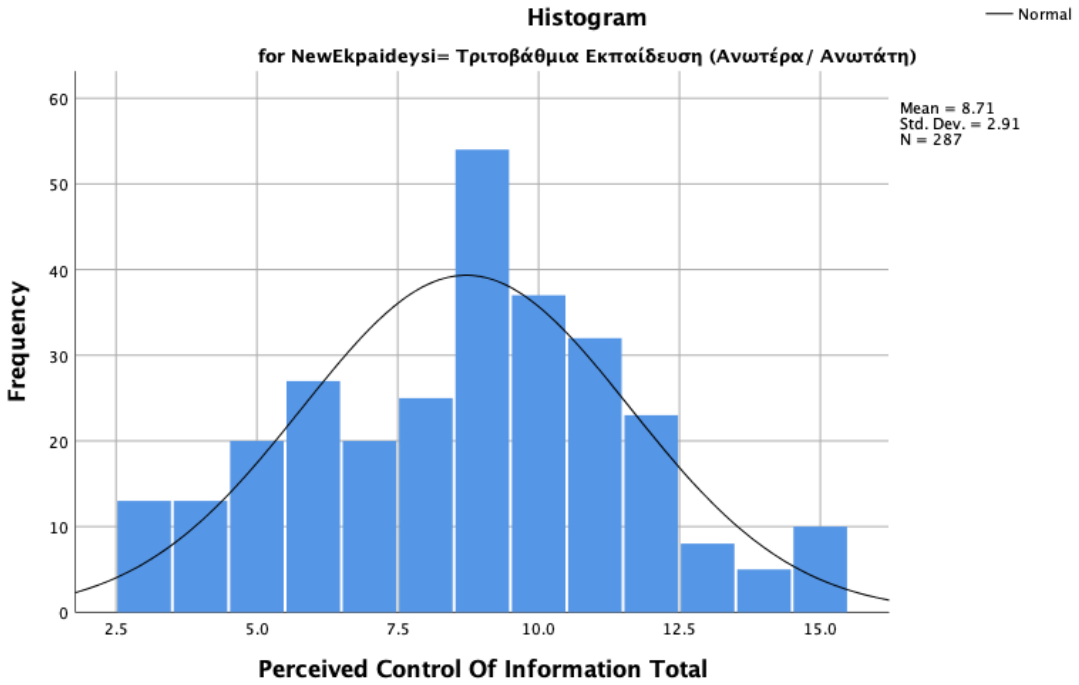

*Γράφημα: 49 Q-Q Plot Perceived Control of Information & Εκπαίδευση Τριτοβάθμια*




*Γράφημα: 50 Ιστόγραμμα Perceived Control of Information Εκπαίδευση Υποχρεωτική*




*Γράφημα: 51 Ιστόγραμμα Perceived Control of Information Εκπαίδευση Δευτεροβάθμια*




*Γράφημα: 52 Ιστόγραμμα Perceived Control of Information & Εκπαίδευση Τριτοβάθμια*

**Έλεγχος Κανονικότητας «Αποκάλυψη Προσωπικών Πληροφοριών" Identity Information Disclosure» & Φύλο**

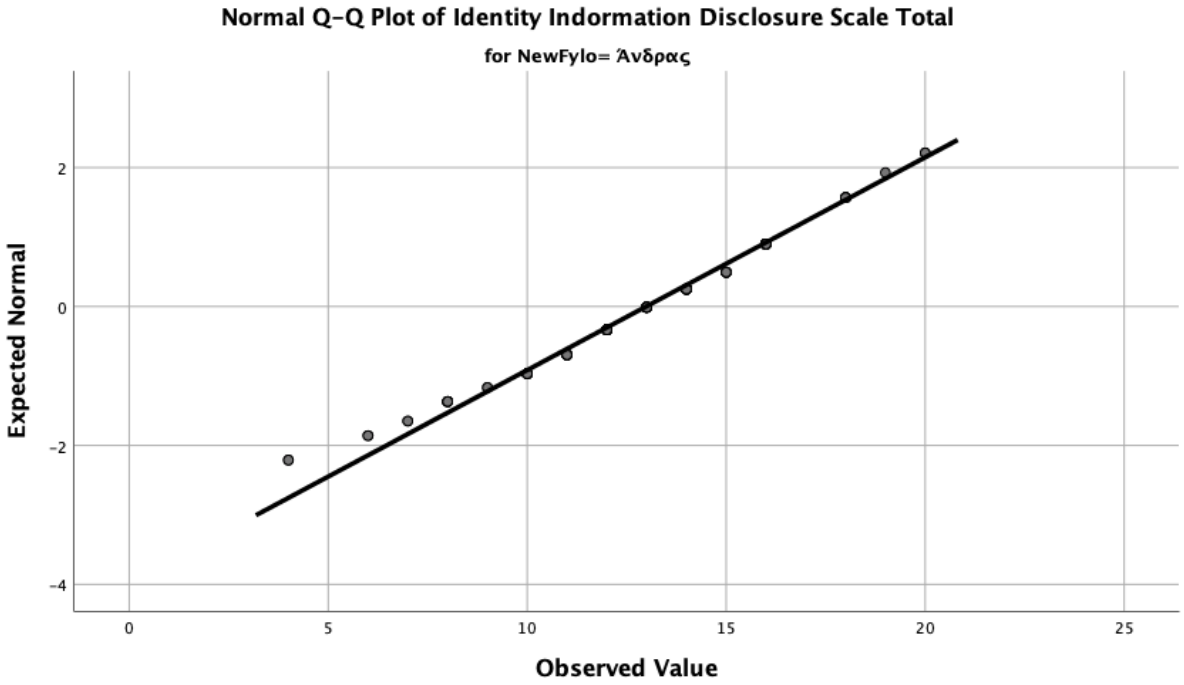
**Tests of Normality**

| | Φύλο | Kolmogorov-Smirnov[a] | Shapiro-Wilk |
|---|---|---|---|

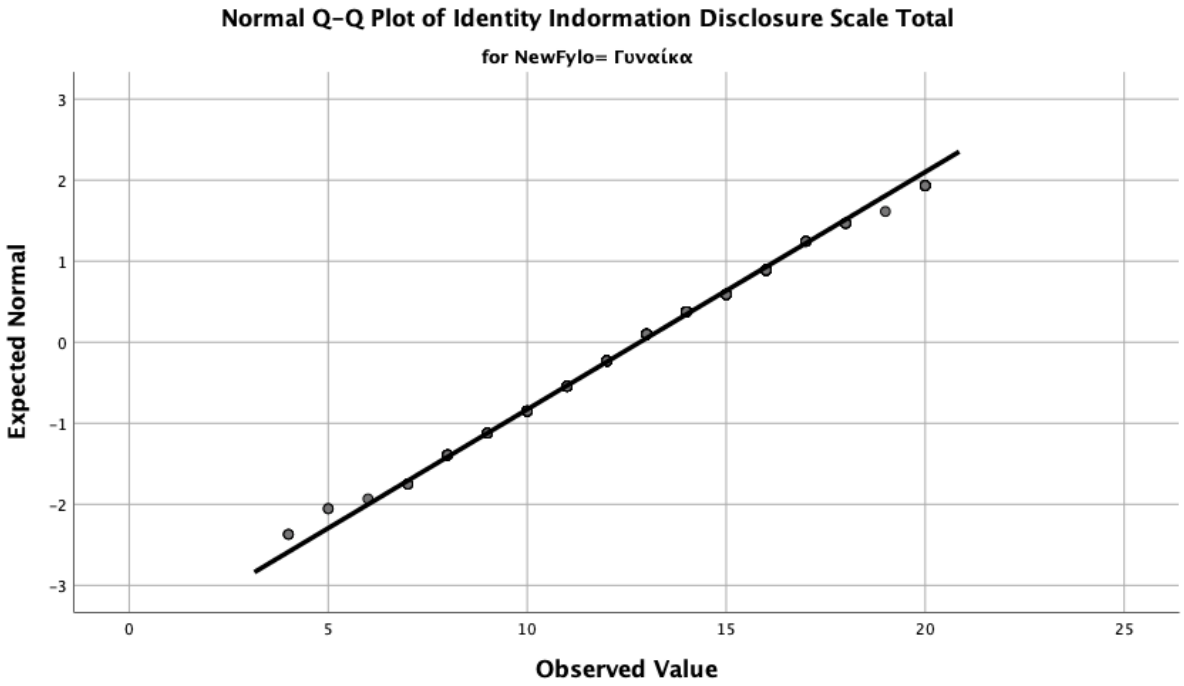
| | | Statistic | df | Sig. | Statistic | df | Sig. |
|---|---|---|---|---|---|---|---|
| Identity Information Disclosure Scale Total | Άνδρας | .104 | 110 | .006 | .971 | 110 | .016 |
| | Γυναίκα | .083 | 224 | .001 | .982 | 224 | .006 |

a. Lilliefors Significance Correction

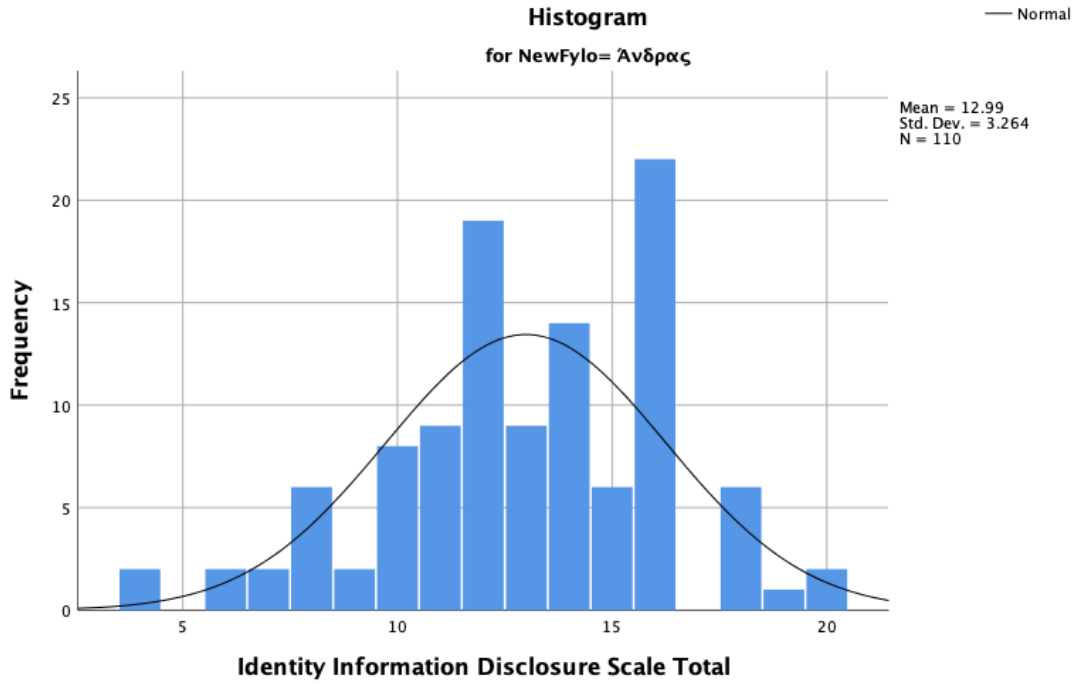
*Πίνακας: 84 Test Κανονικότητας Identity Information Disclosure & Φύλο*



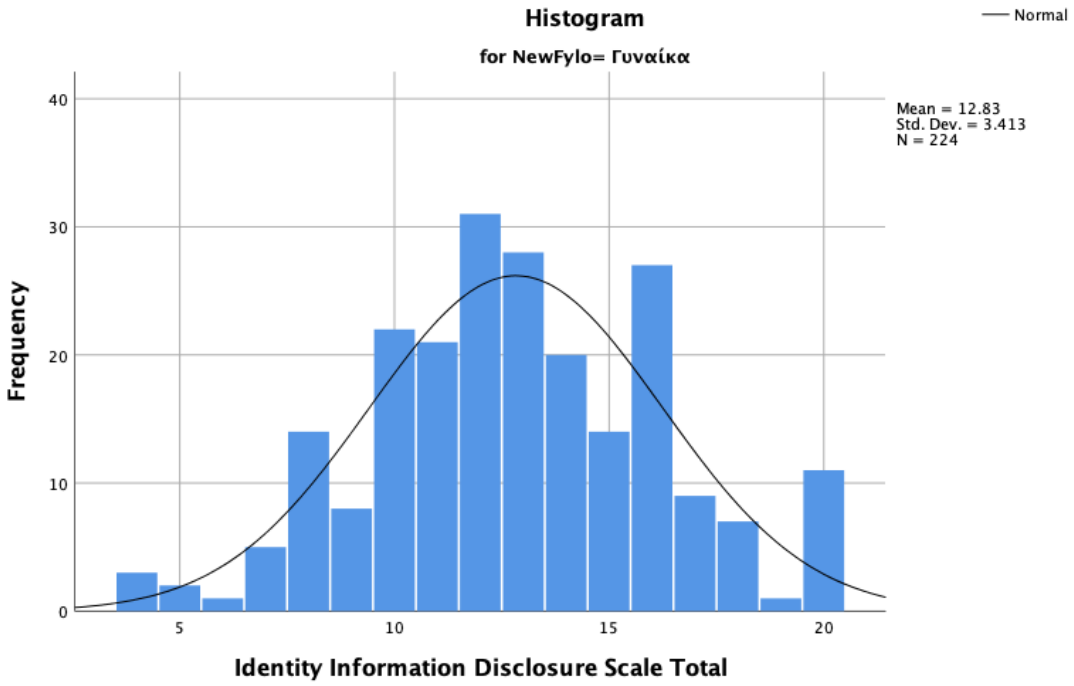

*Γράφημα: 53 Q-Q Plot Identity Information Disclosure & φύλο Άνδρας*




*Γράφημα: 54 Q-Q Plot Identity Information Disclosure & φύλο Γυναίκα*




*Γράφημα: 55 Ιστόγραμμα Identity Information Disclosure & φύλο Άνδρας*




*Γράφημα: 56 Ιστόγραμμα Identity Information Disclosure & φύλο Γυναίκα*

**Έλεγχος Κανονικότητας «Αποκάλυψη Προσωπικών Πληροφοριών "Identity Information Disclosure» & Ηλικία**

**Tests of Normality [c]**

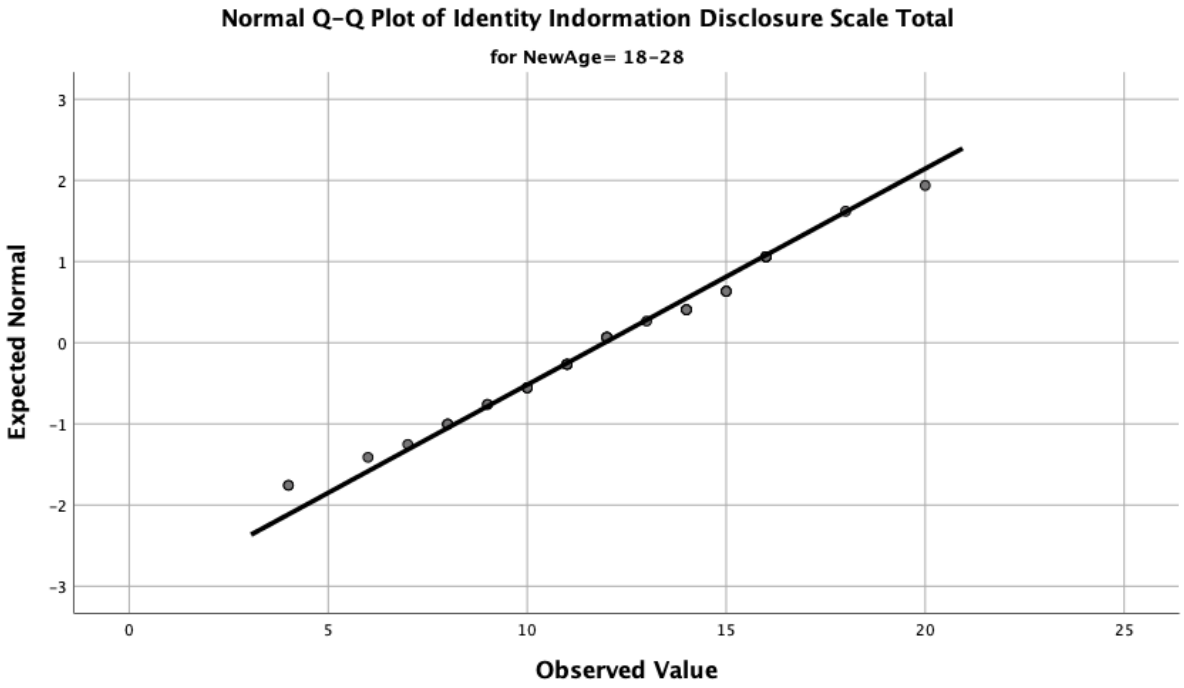
| | | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|---|
| | Ηλικία | Statistic | df | Sig. | Statistic | df | Sig. |
| Identity Information Disclosure Scale Total | 18-28 | .089 | 37 | .200* | .976 | 37 | .584 |
| | 29-38 | .077 | 71 | .200* | .981 | 71 | .369 |
| | 39-48 | .103 | 119 | .003 | .965 | 119 | .004 |
| | 49-68 | .090 | 106 | .034 | .971 | 106 | .022 |

*. This is a lower bound of the true significance.

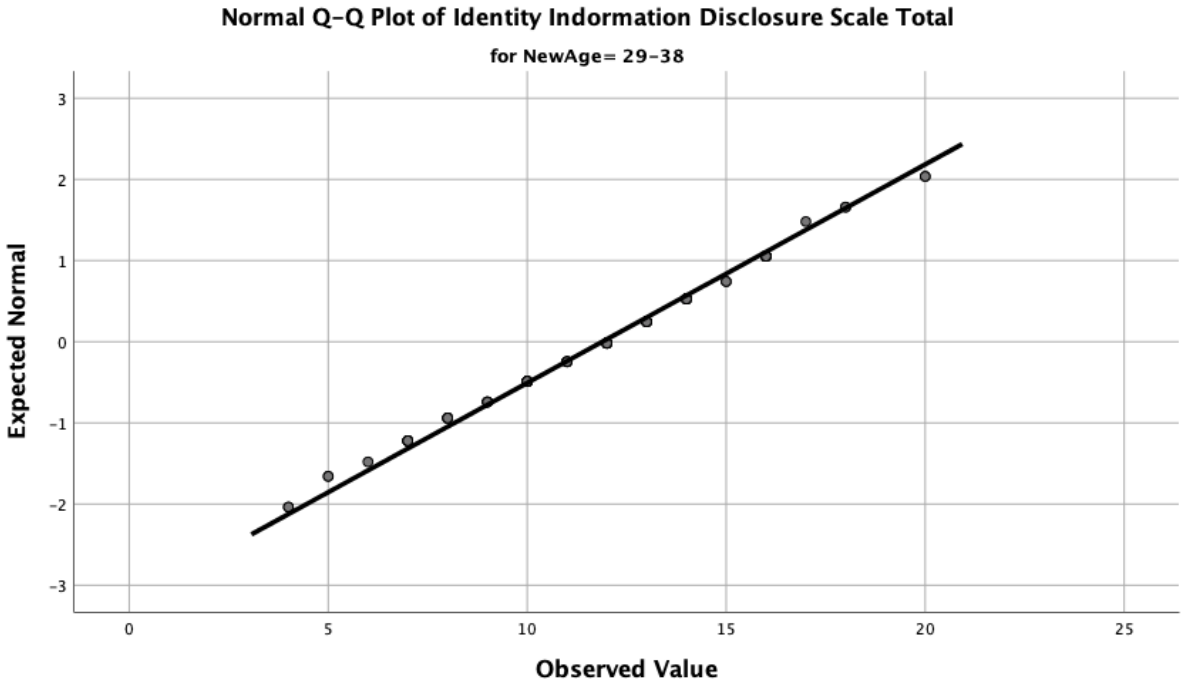
a. Lilliefors Significance Correction

c. Identity Information Disclosure Scale Total is constant when Ηλικία = 69+. It has been omitted.

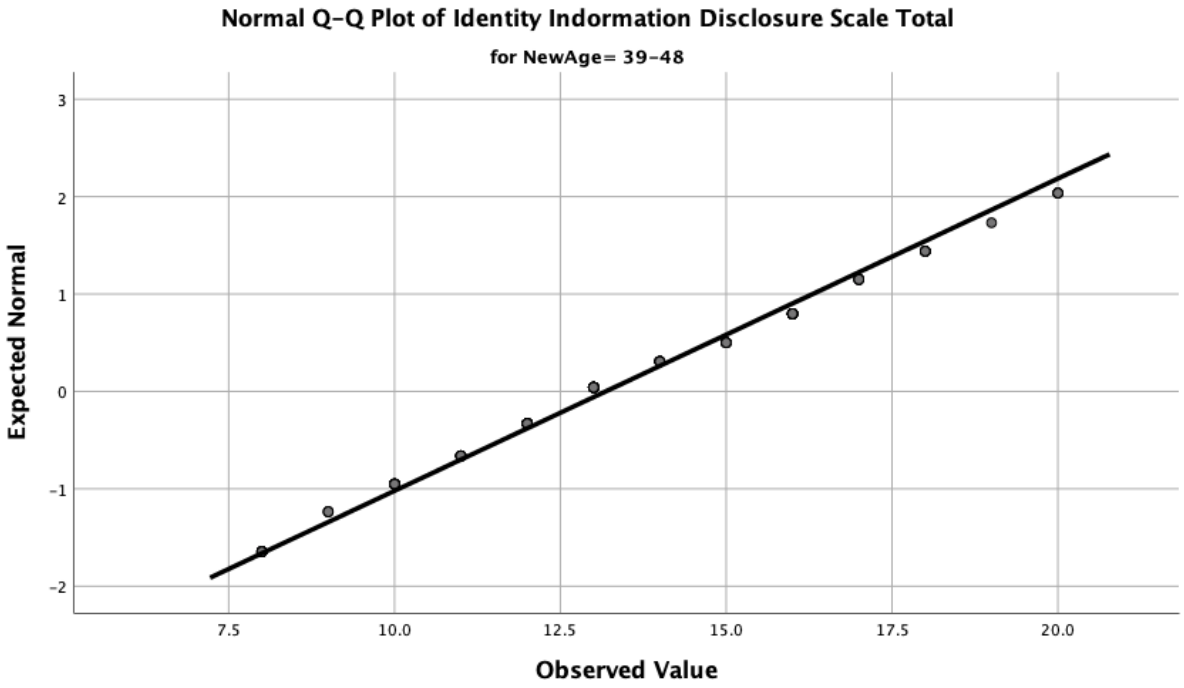
*Πίνακας: 85 Test Κανονικότητας Identity Information Disclosure & Ηλικία*



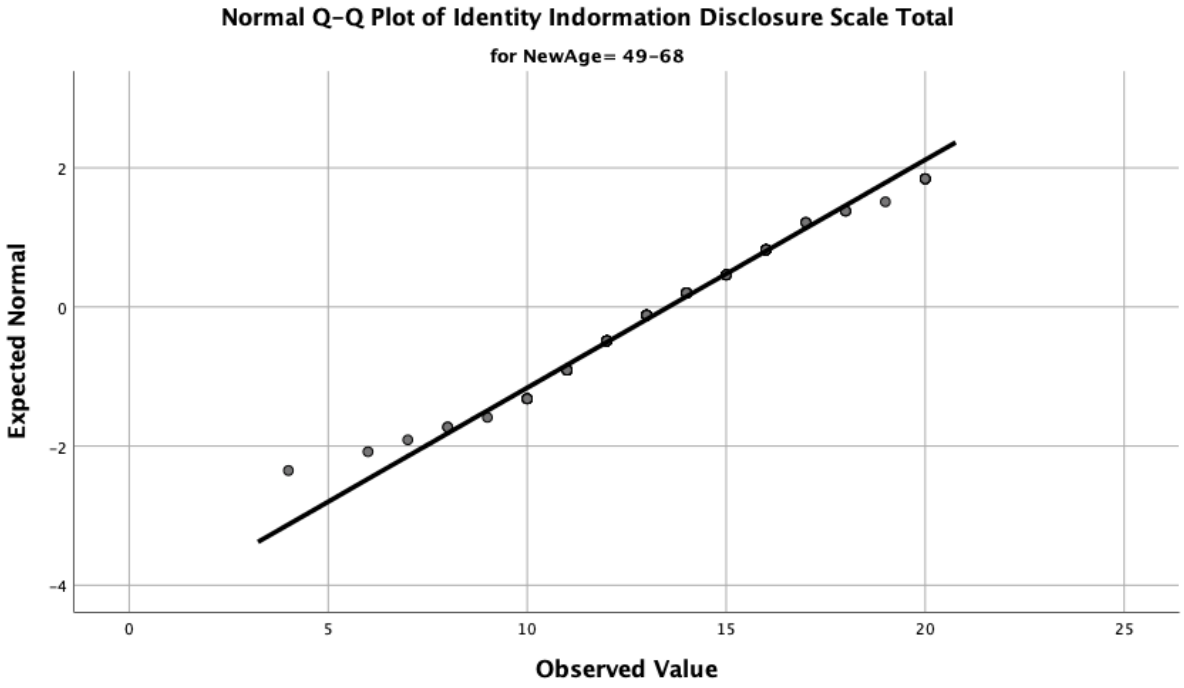

*Γράφημα: 57 Q-Q Plot Identity Information Disclosure & Ηλικία 18-28*




*Γράφημα: 58 Q-Q Plot Identity Information Disclosure & Ηλικία 29-38*




*Γράφημα: 59 Q-Q Plot Identity Information Disclosure & Ηλικία 39-48*




*Γράφημα: 60 Q-Q Plot Identity Information Disclosure & Ηλικία 49-68*

# Κεφάλαιο 6
# Συμπεράσματα

## 6.1 Περίληψη Σημαντικών Αποτελεσμάτων

Τα αποτελέσματα που προέκυψαν από την έρευνα και τους ελέγχους που υλοποιήθηκαν, παρατίθενται κατωτέρω:

1. Οι πιο δημοφιλείς πλατφόρμες: Η πιο δημοφιλής πλατφόρμα Κοινωνικής Δικτύωσης είναι το Facebook το οποίο συγκεντρώνει την προτίμηση των Ενηλίκων συμμετεχόντων χρηστών σε ποσοστό 95,2%, δεύτερη πιο δημοφιλής πλατφόρμα είναι το YouTube που συγκεντρώνει ποσοστό συμμετοχής 54,8%, τρίτο είναι το Instagram με ποσοστό συμμετοχής 52,1%, τέταρτο το LinkedIn με ποσοστό 32% και πέμπτο το Pinterest με ποσοστό 25,1%. Οι υπόλοιπες ΙΚΔ ακολουθούν με μικρότερα ποσοστά.
2. Οι έχοντες λογαριασμό σε ΙΚΔ αποτελούν το 77,3% των συμμετεχόντων ενώ το 22,7% δεν συμμετέχει σε ΙΚΔ (απέχει).
3. Οι κίνδυνοι που εξετάσθηκαν φαίνεται να είναι στο σύνολό τους γνωστοί στους συμμετέχοντες. Τα ανεπιθύμητα μηνύματα είναι πρώτα στην λίστα της αντίληψης κινδύνων με ποσοστό εμφάνισης 94,3%, ακολουθούν οι Ιοί, οι οποίοι βρίσκονται στην αντίληψη των χρηστών σε ποσοστά 91,6%, ο Παραβιασμένος λογαριασμός σε ποσοστό 80,8% και η Παρενόχληση με 72,2%. Κίνδυνοι όπως οι Απάτες βρίσκονται στο 66,5%, ενώ το Ψάρεμα (Phishing) αλλά και η Κλοπή ταυτότητας βρίσκονται στην αντίληψη των χρηστών σε ποσοστά που ξεπερνούν το 50%. Το γεγονός αυτό υποδηλώνει ότι, οι Χρήστες των ΙΚΔ είναι ενήμεροι για τους κινδύνους με τους οποίους μπορεί να έρθουν αντιμέτωποι, κατά την αλληλεπίδρασή τους στις ΙΚΔ στις οποίες συμμετέχουν.
4. Μεταξύ των παραγόντων - συμπεριφορών που επιδεικνύουν οι συμμετέχοντες (n=334) κατά την αλληλεπίδρασή τους στις ΙΚΔ, μεγαλύτερους μέσους όρους εμφανίζουν η Ιδιωτικότητα/ Απόρρητο (mean 20,15 & SD 5,378), η Ανάληψη Ρίσκου (mean 15,41 & SD 3,912) και η Αποκάλυψη Προσωπικών Πληροφοριών

(mean 12,88 & SD 3,360) μεταξύ των διαφορετικών παραγόντων - συμπεριφορών που εξετάσθηκαν.

5. Συμπεριφορές Χρηστών σε ΙΚΔ Σχέσεις

Οι έλεγχοι που διενεργήθηκαν στο κεφάλαιο 5.2.3 υπέδειξαν μερικές σημαντικές σχέσεις μεταξύ συμπεριφορών που επιδεικνύουν οι Χρήστες των ΙΚΔ κατά την αλληλεπίδρασή τους. Τα αποτελέσματα της έρευνας έδειξαν ότι **δεν** σχετίζονται οι συμπεριφορές αναφορικά με την **Ανάληψη Κινδύνου, Εμπιστοσύνη/Trust** σε Εταιρείες ΙΚΔ, όπως και η **Ανησυχία για την Ιδιωτικότητα Privacy Concern** με το φύλο, την ηλικία και το Μορφωτικό Επίπεδο.
Ωστόσο εντοπίσθηκαν οι κάτωθι σχέσεις:

- Η Συμπεριφορά για την Ιδιωτικότητα "Privacy Behavior" σχετίζεται με την ηλικία.
- Η Αποκάλυψη Προσωπικών Πληροφοριών Identity Information Disclosure σχετίζεται με την ηλικία.
- Στις επιμέρους ερωτήσεις για την Αποκάλυψη προσωπικών Πληροφοριών προκύπτει ότι στην ερώτηση «Ανησυχώ για τις συνέπειες διαμοιρασμού/Κοινής χρήσης πληροφοριών σχετικές με την ταυτότητά μου» σχετίζεται με το φύλο και τέλος
- Στην Αποκάλυψη Προσωπικών «Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο» σχετίζεται με το Μορφωτικό Επίπεδο.

6. **Έκθεση σε Κίνδυνο και Σχέσεις**

- Η Έκθεση σε Κίνδυνο σχετίζεται με το φύλο.
- Η Έκθεση σε Κίνδυνο δεν σχετίζεται με την ηλικία
- Η Έκθεση σε Κίνδυνο δεν σχετίζεται με το Μορφωτικό Επίπεδο

## 6.2 Σχέση των Αποτελεσμάτων με τις Υπάρχουσες Μελέτες

Όσον αφορά την Ελληνική Πραγματικότητα, τα αποτελέσματα της παρούσας μελέτης, δεν είναι δυνατόν να συγκριθούν με άλλες παρόμοιες καθώς δεν έχουν εντοπισθεί άλλες σχετικές με το θέμα μελέτες. Εντοπίσθηκε ωστόσο μια έρευνα, υλοποιηθείσα από τους Fogel & Nehmad (ΗΠΑ 2009), στην οποία κάποιες μετρήσεις και αποτελέσματα των ελεγχθέντων χαρακτηριστικών μπορούν να συγκριθούν με την παρούσα έρευνα.

Οι Fogel & Nehmad διαπίστωσαν, στις συγκρίσεις μεταξύ Ανδρών και Γυναικών αναφορικά με την ανάληψη κινδύνου, εμπιστοσύνης και ιδιωτικότητας, ότι οι άνδρες εμφάνισαν μεγαλύτερη βαθμολογία, ενώ αντίστοιχα οι γυναίκες επέδειξαν μεγαλύτερη ανησυχία για την αποκάλυψη προσωπικών στοιχείων και αποκάλυψαν λιγότερα προσωπικά στοιχεία σε σχέση με τους άνδρες. Τα αποτελέσματα της παρούσας έρευνας είναι αντίστοιχα σε κάποια εκ των μετρηθέντων συμπεριφορών. Υπάρχει συμφωνία σε κάποια από τα αποτελέσματα των μετρήσεων. Ανάληψη Κινδύνου και Ιδιωτικότητα οι Μέσοι Όροι (mean) των Ανδρών είναι μεγαλύτεροι από τις αντίστοιχες των γυναικών, Ανάληψη Κινδύνου (Άνδρες mean 15,45 Sd 4,146, Γυναίκες mean 15,41 Sd 3,912) & Ιδιωτικότητα (Άνδρες mean 20,6 Sd 5,607, Γυναίκες mean 20.15 Sd 5.388). Αντίστοιχα είναι και τα αποτελέσματα για την Ανησυχία για την Ιδιωτικότητα (Άνδρες mean 11,18 Sd 2,984, Γυναίκες mean 11,49 Sd 2,577). Αναφορικά με την Εμπιστοσύνη, οι μετρήσεις στην παρούσα έρευνα είναι αντίστροφες της έρευνας των Fogel & Nehmad με τους Μέσους Όρους των Γυναικών να είναι μεγαλύτερες από αυτές των ανδρών (Γυναίκες mean 8,89 Sd 3.378, Άνδρες mean 8,79 Sd 3,527,). Για τα αποτελέσματα της παρούσας έρευνας, βλέπε Πίνακας: 25) (Fogel & Nehmad, 2009).

## 6.3 Περιορισμοί της Μελέτης

Περιορισμό της παρούσας μελέτης θα μπορούσε να αποτελεί το θέμα της συμμετοχής των γυναικών, καθώς το δείγμα του πληθυσμού των γυναικών είναι μεγαλύτερο από αυτό των ανδρών. Οι γυναίκες ωστόσο, υποστηρίζεται από τους Kimbrough et al. (2013), συμμετέχουν περισσότερο στα Κοινωνικά Δίκτυα συγκριτικά με τους άνδρες, το οποίο επίσης υποστηρίζεται και σε άλλα ευρήματα (Alnjadat, Hmaidi, Samha, Kilani, & Hasswan, 2019)(Hargittai, 2007) (Madden & Zickuhr, 2011). Αν και αυτή η διαφορά, σύμφωνα με τελευταίες έρευνες στις ΗΠΑ, τείνει να εξαλειφθεί (Madden & Zickuhr, 2011), έχει επιπλέον υποστηριχθεί, ότι οι γυναίκες συμμετέχουν σε περισσότερες έρευνες (Kimbrough et al., 2013) (Branley & Covey, 2018). Άλλος περιορισμός που θα μπορούσε να υπάρχει είναι αυτός της υπό-αντιπροσώπευσης συμμετεχόντων στην ηλικιακή ομάδα των 69+ ετών. Καθώς όμως η διείσδυση της τεχνολογίας σε αυτές τις ηλικίες είναι

μικρότερη, πιθανά η σχετική διερεύνηση, να αποτελέσει πεδίο για περαιτέρω έρευνα (Smith & Anderson, 2018) (Anderson & Perrin, 2017).

## 6.4 Περιοχές Μελλοντικής Έρευνας

Η μελέτη αυτή προσεγγίζει το θέμα των κινδύνων σε Ενήλικες χρήστες ΙΚΔ. Θα μπορούσε ωστόσο το θέμα αυτό (η διερεύνηση κινδύνων σε ΙΚΔ) μελλοντικά να ερευνηθεί συγκριτικά μεταξύ χρηστών ΙΚΔ και μη χρηστών ΙΚΔ (απλών χρηστών Διαδικτύου), όπως επίσης να συμπεριλάβει και τις πιθανές επιπτώσεις και πως αυτές επηρεάζουν όσους εκτίθενται σε κινδύνους.

## 6.5 Συμπέρασμα / Επίλογος

Η έκθεση σε κινδύνους στις Ιστοσελίδες Κοινωνικής Δικτύωσης σύμφωνα με τα αποτελέσματα της παρούσας έρευνας συσχετίζεται με το φύλο.
Επίσης η Ιδιωτικότητα/“Privacy Behavior” και η Αποκάλυψη Προσωπικών Πληροφοριών/“Identity Information Disclosure” συσχετίζονται με την ηλικία και σε επιμέρους ερωτήσεις αναφορικά με την Αποκάλυψη Πληροφοριών και με το φύλο και το Μορφωτικό Επίπεδο.

# Παράρτημα Α

# Ερωτηματολόγιο



## Ερωτηματολόγιο Ανίχνευσης Κινδύνων σε Κοινωνικά Δίκτυα

Η παρούσα έρευνα υλοποιείται στο πλαίσιο της Μεταπτυχιακής Διατριβής μου στο Ανοικτό Πανεπιστήμιο Κύπρου και στο Πρόγραμμα Σπουδών "Κοινωνικά Πληροφοριακά Συστήματα".

Με το παρόν ερωτηματολόγιο καλείστε να συμμετέχετε στην έρευνα αναφορικά με τους κινδύνους που ελλοχεύουν στις Ιστοσελίδες Κοινωνικής Δικτύωσης.
Το ερωτηματολόγιο απαρτίζεται από 3 τμήματα. Ένα τμήμα αναφέρεται στα Κοινωνικο-Δημογραφικά χαρακτηριστικά των συμμετεχόντων, ένα τμήμα αναφέρεται στην Χρήση του Διαδικτύου και των Ιστοσελίδων Κοινωνικής Δικτύωσης (διαδικτυακές συνήθειες των συμμετεχόντων) και ένα τμήμα που στόχο έχει τον εντοπισμό των κοινών κινδύνων που ελλοχεύουν στα Κοινωνικά Δίκτυα, τις πρακτικές που εφαρμόζουν οι συμμετέχοντες στην αλληλεπίδρασή τους με αυτά, καθώς και την αντίληψη που διατηρούν οι συμμετέχοντες αναφορικά με την ύπαρξη κινδύνων.

Παρακαλείστε να το συμπληρώσετε με ειλικρίνεια. Τα δεδομένα θα επεξεργαστούν ανώνυμα και τα αποτελέσματα αυτά θα χρησιμοποιηθούν αποκλειστικά για τις ανάγκες συγγραφής της διατριβής μου.

Ο χρόνος που χρειάζεται για να απαντήσετε το ερωτηματολόγιο είναι περίπου 15 λεπτά.

Ευχαριστώ προκαταβολικά για τον χρόνο σας και εκτιμώ ιδιαίτερα την βοήθειά σας!

Ελένη Στρατηγοπούλου

* Required

## Κοινωνικό-Δημογραφικά Στοιχεία

1. **Φύλο** *
   *Mark only one oval.*
   - ◯ Γυναίκα
   - ◯ Άνδρας

2. **Ηλικία** *
   *Mark only one oval.*
   - ◯ 18-28
   - ◯ 29-38
   - ◯ 39-48
   - ◯ 49-68
   - ◯ 69+

3. **Εκπαίδευση** *
*Mark only one oval.*

- ◯ Υποχρεωτική Εκπαίδευση έως Γ' Γυμνασίου
- ◯ Δευτεροβάθμια Εκπαίδευση (Λύκειο)
- ◯ Τριτοβάθμια Εκπαίδευση (Ανωτέρα/ Ανωτάτη)

## Στοιχεία Διαδικτύου και Μέσων Κοινωνικής Δικτύωσης

4. **Έχετε Μόνιμη Σύνδεση στο Διαδίκτυο?** *
*Mark only one oval.*

- ◯ Ναι
- ◯ Όχι

5. **Σύνδεση στο Διαδίκτυο από:** *
(Δυνατότητα πολλαπλής Επιλογής - Παρακαλώ Επιλέξτε ένα ή περισσότερα )
*Check all that apply.*

- ☐ Κατοικία
- ☐ Εκπαιδευτικό
- ☐ Επαγγελματικό
- ☐ Other: _____

6. **Σύνδεση στο Διαδίκτυο Μέσω:** *
(Δυνατότητα Πολλαπλής Επιλογής - Παρακαλώ Επιλέξτε ένα ή περισσότερα)
*Check all that apply.*

- ☐ Υπολογιστή (Desktop) / Φορητό Υπολογιστή (Laptop)
- ☐ Tablet
- ☐ Κινητό (SmartPhone)

7. **Πόσο Συχνά Συνδέεστε στο Διαδίκτυο ?** *
Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

8. **Συμμετέχετε σε Ιστοσελίδες Κοινωνικών Δικτύων?** *
   *Mark only one oval.*

   - ◯ Ναι *Skip to question 9.*
   - ◯ Όχι *Stop filling out this form.*

## Συμμετοχή Σε Κοινωνικά Δίκτυα

9. **Σε ποιες από τις ακόλουθες Ιστοσελίδες Κοινωνικής Δικτύωσης Διατηρείτε Λογαριασμό?** *
   (Δυνατότητα Πολλαπλής Επιλογής- Παρακαλώ Επιλέξτε όσα Χρειάζεται)
   *Check all that apply.*

   - ☐ Facebook
   - ☐ Instagram
   - ☐ LinkedIn
   - ☐ Twitter
   - ☐ YouTube
   - ☐ Snapchat
   - ☐ WhatsApp
   - ☐ Pinterest
   - ☐ Other: _____

10. **Για ποιο Λόγο Χρησιμοποιείτε τις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *
    (Δυνατότητα Πολλαπλής Επιλογής- Παρακαλώ Επιλέξτε έναν ή περισσότερους λόγους)
    *Check all that apply.*

    - ☐ Επαγγελματικό Λόγο
    - ☐ Ενημέρωση
    - ☐ Διασκέδαση
    - ☐ Επικοινωνία με φίλους
    - ☐ Διαμοιρασμός Φωτογραφιών/ Video
    - ☐ Διεύρυνση Επαφών - Φίλων
    - ☐ Διεύρυνση Επαγγελματικών Επαφών
    - ☐ Other: _____

11. **Πόσο Συχνά Συνδέεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης που Συμμετέχετε?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μία φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval per row.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Facebook | | | | | | | | | | |
| Instagram | | | | | | | | | | |
| LinkedIn | | | | | | | | | | |
| Twitter | | | | | | | | | | |
| YouTube | | | | | | | | | | |
| Snapchat | | | | | | | | | | |
| WhatsApp | | | | | | | | | | |
| Pinterest | | | | | | | | | | |
| Άλλο | | | | | | | | | | |

## Χρήση Ιστοσελίδων Κοινωνικής Δικτύωσης

Κλίμακα Χρήσης Ιστοσελίδων Κοινωνικής Δικτύωσης - (SNS Usage Scale)

12. **Πόσο Συχνά Ελέγχετε τις Ιστοσελίδες Κοινωνικής Δικτύωσης στις οποίες Συμμετέχετε / Διατηρείτε Λογαριασμό?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | | | | | | | | | | | Όλη την Ώρα/ Συνεχώς |

13. **Πόσο Συχνά Ελέγχετε τις Ιστοσελίδες Κοινωνικής Δικτύωσης στις οποίες Συμμετέχετε / Διατηρείτε Λογαριασμό από το Κινητό (smartphone)?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | | | | | | | | | | | Όλη την Ώρα / Συνεχώς |

14. **Πόσο Συχνά Ελέγχετε τις Ιστοσελίδες Κοινωνικής Δικτύωσης στην Δουλειά ή στο Εκπαιδευτικό Ίδρυμα στο οποίο φοιτάτε?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

15. **Πόσο συχνά Δημοσιεύετε Ενημέρωση του Προφίλ σας (status update) στις Ιστοσελίδες Κοινωνικής Δικτύωσης ?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

16. **Πόσο Συχνά κάνετε Ανάρτηση Φωτογραφίας στις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

17. **Πόσο Συχνά Περιηγείστε Προφίλ και Φωτογραφίες στις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *

Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

18. **Πόσο Συχνά Διαβάζετε Αναρτήσεις (posts) στις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *
Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την ώρα/ Συνεχώς |

19. **Πόσο Συχνά Σχολιάζετε Ανάρτηση (post) ή Φωτογραφία στις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *
Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

20. **Πόσο Συχνά κάνετε like σε ανάρτηση (post) ή φωτογραφία στις Ιστοσελίδες Κοινωνικής Δικτύωσης?** *
Κλίμακα 1= Ποτέ, 2 = Μία Φορά τον Μήνα, 3= Μερικές Φορές τον Μήνα, 4= Μια φορά την Εβδομάδα, 5= Μερικές Φορές την Εβδομάδα, 6= Μια φορά την Ημέρα, 7= Μερικές Φορές την Ημέρα, 8 = Μια φορά την Ώρα, 9 = Μερικές Φορές την Ώρα, 10 = Όλη την Ώρα/ Συνεχώς
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | ◯ | Όλη την Ώρα / Συνεχώς |

## Κίνδυνοι στις Ιστοσελίδες Κοινωνικής Δικτύωσης

Παρακαλώ να επιλέξετε έναν ή περισσότερους / Δυνατότητα Πολλαπλής Επιλογής.

21. **Ποιους από τους Κάτωθι Κινδύνους Γνωρίζετε?** *
*Check all that apply.*

- [ ] Παραβιασμένος Λογαριασμός (BrokenAccount)
- [ ] Παρενόχληση (Harassment)
- [ ] Ιοί (Viruses)
- [ ] Ανεπιθύμητα Μηνύματα/ ή Αλληλογραφία
- [ ] Απάτη
- [ ] Κλοπή Ταυτότητας
- [ ] Ψάρεμα/ Phishing
- [ ] Other: _____

22. **Έχετε Βρεθεί Αντιμέτωπος/η με κάποιον Κίνδυνο κατά την Αλληλεπίδρασή σας και εάν ναι με ποιον από τους Παρατιθέμενους?** *
*Mark only one oval per row.*

| | Ναι | Όχι |
|---|---|---|
| Παραβιασμένος Λογαριασμός (BrokenAccount) | ◯ | ◯ |
| Παρενόχληση (Harassment) | ◯ | ◯ |
| Ιοί (Viruses) | ◯ | ◯ |
| Ανεπιθύμητα Μηνύματα/ ή Αλληλογραφία | ◯ | ◯ |
| Απάτη | ◯ | ◯ |
| Κλοπή Ταυτότητας | ◯ | ◯ |
| Ψάρεμα/ Phishing | ◯ | ◯ |
| Άλλο | ◯ | ◯ |

Απαντήστε στις παρακάτω δηλώσεις με Ναι ή Όχι, σχετικά με τις προσωπικές πληροφορίες που μοιράζεστε στις Ιστοσελίδες Κοινωνικής Δικτύωσης (Πρακτικές Κοινής Χρήσης Προσωπικών Πληροφοριών)

23. **Έχετε Συμπεριλάβει κάποια από τις παρακάτω Προσωπικές Πληροφορίες στο Προφίλ σας στο/στα Κοινωνικά Δίκτυα στα οποία Αλληλεπιδράτε?** *
*Mark only one oval per row.*

| | Ναι | Όχι |
|---|---|---|
| Το Πραγματικό σας Όνομα | ◯ | ◯ |
| Το Πραγματικό σας Επίθετο | ◯ | ◯ |
| Το Προσωπικό σας Τηλέφωνο (Mobile Phone) | ◯ | ◯ |
| Την Προσωπική σας Διεύθυνση (Address) | ◯ | ◯ |
| Την Ηλεκτρονική σας Διεύθυνση (Email Address) | ◯ | ◯ |
| Την διεύθυνση του λογαριασμού σας στο messenger (your instant messenger address) | ◯ | ◯ |
| Δραστηριότητες και Hobbies | ◯ | ◯ |
| Στοιχεία της προσωπικότητας σας | ◯ | ◯ |

24. **Επιτρέπετε σε οποιονδήποτε να δει το προφίλ σας ?** *
*Mark only one oval.*

◯ Ναι
◯ Όχι

25. **Έχετε Αναρτήσει/Κοινοποιήσει/ Μοιραστεί Προσωπική Φωτογραφία ή Βίντεο με άτομα που δεν γνωρίζετε?** *
*Mark only one oval.*

◯ Ναι
◯ Όχι

Στις ακόλουθες δηλώσεις παρακαλώ να απαντήσετε εάν Διαφωνείτε ή Συμφωνείτε σε μια κλίμακα από το 1-5
όπου το 1 ισοδυναμεί με Διαφωνώ Ισχυρά, 2 = Διαφωνώ Λίγο, 3 = Ούτε Διαφωνώ ούτε Συμφωνώ, 4 = Συμφωνώ Λίγο και το 5 με το Συμφωνώ Ισχυρά (Κίνδυνοι / Αντίληψη Risk Averseness scale)

26. **Για να αποκτήσεις υψηλά κέρδη στις επιχειρήσεις, πρέπει να αναλάβεις υψηλό ρίσκο.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

27. **Εάν υπάρχει μεγάλη πιθανότητα ανταμοιβής, θα αναλάβω υψηλά ρίσκα.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

28. **Η λογική ανάληψη ρίσκου (κινδύνου) είναι μία από τις σημαντικότερες διοικητικές δεξιότητες.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

29. **Εάν υπάρχει μεγάλη ευκαιρία να πολλαπλασιάσω τα κέρδη μου, θα επενδύσω τα χρήματά μου ακόμη και σε μετοχές μιας εντελώς νέας και αβέβαιης επιχείρησης.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

30. **Για να επιτευχθεί κάτι στη ζωή, ο οποιοσδήποτε πρέπει να αναλάβει ρίσκα.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

Στις ακόλουθες δηλώσεις παρακαλώ να απαντήσετε εάν Διαφωνείτε ή Συμφωνείτε σε μια κλίμακα από το 1-5
όπου το 1 ισοδυναμεί με Διαφωνώ Ισχυρά, 2 = Διαφωνώ Λίγο, 3 = Ούτε Διαφωνώ ούτε Συμφωνώ, 4 = Συμφωνώ Λίγο και το 5 με το Συμφωνώ Ισχυρά (Trust/Εμπιστοσύνη σε Ε.Ι.Κ.Δ)

31. **Οι Εταιρείες των Ιστοσελίδων Κοινωνικής Δικτύωσης είναι αξιόπιστες** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

32. **Μπορώ να βασίζομαι στις Εταιρείες Κοινωνικής Δικτύωσης για να προστατεύσω τα προσωπικά μου δεδομένα.**
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

33. **Μπορώ να βασίζομαι στο ότι οι Εταιρείες των Ιστοσελίδων Κοινωνικής Δικτύωσης μπορούν να προστατεύσουν τα Προσωπικά Δεδομένα των χρηστών τους από μη εξουσιοδοτημένη χρήση.**
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

34. **Μπορώ να βασίζομαι ότι οι Εταιρείες των Ιστοσελίδων Κοινωνικής Δικτύωσης μπορούν να τηρούν τις υποσχέσεις τους.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

Παρακαλώ απαντήστε στις κάτωθι δηλώσεις σε κλίμακα από το 1 έως το 5,
όπου το 1 ισοδυναμεί με το Ποτέ, 2= Σπάνια, 3= Μερικές Φορές, 4= Συχνά και το 5 που ισοδυναμεί με το Πάντα (Privacy Behavior scale)

35. **Καταστρέφετε (Shred) /Καίτε τα προσωπικά σας έγγραφα όταν τα απορρίπτετε?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

36. **Κρύβετε τον προσωπικό σας Αριθμό (Pin) της Χρεωστικής κάρτας σας όταν χρησιμοποιείτε ταμειακές μηχανές / πραγματοποιείτε αγορές?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

37. **Δημιουργείτε λογαριασμό/ Εγγράφεστε μόνο σε ιστοσελίδες που έχουν πολιτική απορρήτου?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

38. **Διαβάζετε την Πολιτική Απορρήτου (privacy policy) των Ιστοσελίδων που επισκέπτεστε πριν καταχωρήσετε τις προσωπικές σας πληροφορίες?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

39. **Ελέγχετε εάν υπάρχει Πιστοποίηση Ασφάλειας Προσωπικών Δεδομένων (Privacy certification) στις Ιστοσελίδες, πριν καταχωρήσετε τις προσωπικές σας πληροφορίες?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

40. **Διαβάζετε πλήρως τις άδειες Χρήσης (License Agreement) πριν συμφωνήσετε με αυτές?** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Ποτέ | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Πάντα |

Στις ακόλουθες δηλώσεις παρακαλώ να απαντήσετε εάν Διαφωνείτε ή Συμφωνείτε σε μια κλίμακα από το 1-5
όπου το 1 ισοδυναμεί με Διαφωνώ Ισχυρά, 2 = Διαφωνώ Λίγο, 3 = Ούτε Διαφωνώ ούτε Συμφωνώ, 4 = Συμφωνώ Λίγο και το 5 με το Συμφωνώ Ισχυρά (Privacy Concern Scale)

41. **Ανησυχώ ότι οι πληροφορίες που υποβάλλω στις Ιστοσελίδες Κοινωνικής Δικτύωσης μπορούν να χρησιμοποιηθούν κατά λάθος.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Συμφωνώ Ισχυρά |

42. **Ανησυχώ ότι οι πληροφορίες που υποβάλλω στις Ιστοσελίδες Κοινωνικής Δικτύωσης μπορούν να χρησιμοποιηθούν με τρόπο που δεν προέβλεψα.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | 5 =Συμφωνώ Ισχυρά |

43. **Ανησυχώ με την υποβολή πληροφοριών στις Ιστοσελίδες Κοινωνικής Δικτύωσης, καθώς δεν γνωρίζω με ποιον τρόπο μπορούν να χρησιμοποιηθούν από άλλους/ ή τρίτους.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| 1= Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | 5 = Συμφωνώ Ισχυρά |

Στις ακόλουθες δηλώσεις παρακαλώ να απαντήσετε εάν Διαφωνείτε ή Συμφωνείτε σε μια κλίμακα από το 1-5
όπου το 1 ισοδυναμεί με Διαφωνώ Ισχυρά, 2 = Διαφωνώ Λίγο, 3 = Ούτε Διαφωνώ ούτε Συμφωνώ, 4 = Συμφωνώ Λίγο και το 5 με το Συμφωνώ Ισχυρά ( Perceived Control of Information scale & Identity Information Disclosure Scale)

44. **Αισθάνομαι ότι έχω τον έλεγχο των πληροφοριών που παρέχω στις Ιστοσελίδες Κοινωνικής Δικτύωσης.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

45. **Η ρύθμιση απορρήτου μου επιτρέπει να έχω πλήρη έλεγχο στις πληροφορίες που παρέχω στις Ιστοσελίδες Κοινωνικής Δικτύωσης.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

46. **Έχω τον έλεγχο του ποιος μπορεί να δει τις πληροφορίες μου στις Ιστοσελίδες Κοινωνικής Δικτύωσης.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

47. **Είμαι εντάξει με τους φίλους που έχουν πρόσβαση στο προφίλ μου στις Ιστοσελίδες Κοινωνικής Δικτύωσης** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

48. **Είμαι εντάξει με την οικογένεια να έχει πρόσβαση στο προφίλ μου στις Ιστοσελίδες Κοινωνικής Δικτύωσης** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

49. **Είμαι εντάξει με τους συναδέλφους/ συμφοιτητές που έχουν πρόσβαση στο προφίλ μου στις Ιστοσελίδες Κοινωνικής Δικτύωσης** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

50. **Είμαι εντάξει με τους ξένους που έχουν πρόσβαση στο προφίλ μου στις Ιστοσελίδες Κοινωνικής Δικτύωσης** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

51. **Είναι σημαντικό για μένα να προστατεύω πληροφορίες σχετικές με την ταυτότητά μου** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

52. **Ανησυχώ για τις συνέπειες διαμοιρασμού/ κοινής χρήσης πληροφοριών σχετικές με την ταυτότητα μου.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

53. **Είναι πιθανό να μοιραστώ πληροφορίες σχετικές με τη ταυτότητά μου διαδικτυακά (online) στο μέλλον.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

54. **Πιστεύω ότι οι πληροφορίες οι σχετικές με την ταυτότητά μου είναι καλά προστατευμένες στο διαδίκτυο.** *
*Mark only one oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Διαφωνώ Ισχυρά | ◯ | ◯ | ◯ | ◯ | ◯ | Συμφωνώ Ισχυρά |

# Βιβλιογραφία


300+ Terrifying Cybercrime & Cybersecurity Statistics [2019 EDITION]. (2019, May 13). Retrieved October 8, 2019, from Comparitech website: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

A Brief History of Snapchat | Adsoup. (n.d.). Retrieved October 20, 2019, from https://adsoup.com/a-brief-history-of-snapchat/

A. Obiniyi, A., Oyelade, O. N., & Obiniyi, P. (2014). Social Network and Security Issues: Mitigating Threat through Reliable Security Model. *International Journal of Computer Applications*, *103*(9), 1–7.

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In G. Danezis & P. Golle (Eds.), *Privacy Enhancing Technologies* (pp. 36–58). Springer Berlin Heidelberg.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model. *Communications of the Association for Information Systems*, *41*, 62–96. https://doi.org/10.17705/1CAIS.04104

Alhabash, S., & Ma, M. (2017). *A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students?* -. https://doi.org/10.1177/2056305117691544

Alnjadat, R., Hmaidi, M. M., Samha, T. E., Kilani, M. M., & Hasswan, A. M. (2019). Gender variations in social media usage and academic performance among the students of University of Sharjah. *Journal of Taibah University Medical Sciences*, *14*(4), 390–394. https://doi.org/10.1016/j.jtumed.2019.05.002

Anderson, M., & Perrin, A. (2017, May 17). Tech Adoption Climbs Among Older Americans. Retrieved November 21, 2019, from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2017/05/17/tech-adoption-climbs-among-older-adults/

Andreassen, C. S. (2015). Online Social Network Site Addiction: A Comprehensive Review. *Current Addiction Reports*, *2*(2), 175–184. https://doi.org/10.1007/s40429-015-0056-9

Antoniadou, N., & Kokkinos, C. M. (2015). A review of research on cyber-bullying in Greece. *International Journal of Adolescence and Youth*, *20*(2), 185–201. https://doi.org/10.1080/02673843.2013.778207

Antoniadou, N., Kokkinos, C. M., & Markos, A. (2016). Possible common correlates between bullying and cyber-bullying among adolescents. *Posibles Correlatos Comunes Entre El Acoso y El Ciberacoso En Adolescentes (Spanish; Castilian)*, *22*, 27–38. https://doi.org/10.1016/j.pse.2016.01.003

Aro, J. (2016). The cyberspace war: Propaganda and trolling as warfare tools. *European View*, *15*(1), 121–132. https://doi.org/10.1007/s12290-016-0395-5

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, *8*, 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). *Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems*. *3*(1), 28.

Bányai, F., Zsila, Á., Király, O., Maraz, A., Elekes, Z., Griffiths, M. D., … Demetrovics, Z. (2017). Problematic Social Media Use: Results from a Large-Scale Nationally Representative Adolescent Sample. *Plos One*, *12*(1), e0169839–e0169839. https://doi.org/10.1371/journal.pone.0169839

Barabasi, A.-L. (2012). *Network Science by Albert-László Barabási*. Retrieved from http://networksciencebook.com/

Benedickt, M. (ed ). (1991). Cyberspace: First Steps. *The MIT Press, Cambridge, MA and London, UK*. Retrieved from http://papers.cumincad.org/cgi-bin/works/Show?_id=4eed

Beran, T., & Li, Q. (2005). Cyber-Harassment: A Study of a New Method for an Old Behavior. *Journal of Educational Computing Research*, *32*(3), 265–277.

Bernstein, P. L. (1996). *Against the Gods: The Remarkable Story of Risk*. A&C Black Publishers Ltd.

Boholm, Å., & Corvellec, H. (2011). A relational theory of risk. *Journal of Risk Research*, *14*(2), 175–190. https://doi.org/10.1080/13669877.2010.515313

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Branley, D. B., & Covey, J. (2018). Risky behavior via social media: The role of reasoned and social reactive pathways. *Computers in Human Behavior*, *78*, 183–191. https://doi.org/10.1016/j.chb.2017.09.036

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Christofides, E., Muise, A., & Desmarais, S. (2012a). Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults. *Social Psychological and Personality Science*, *3*. https://doi.org/10.1177/1948550611408619

Christofides, E., Muise, A., & Desmarais, S. (2012b). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research*, *27*(6), 714–731. https://doi.org/10.1177/0743558411432635

Citron, D., & Franks, M. (2014). Criminalizing Revenge Porn. *Faculty Scholarship*. Retrieved from https://digitalcommons.law.umaryland.edu/fac_pubs/1420

Clement, J. (2019, August 14). Number of social media users worldwide 2010-2021. Retrieved November 20, 2019, from Statista website: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Collins, B. S., & Mansell, R. (2004, June 10). Cyber trust and crime prevention: A synthesis of the state-of-the-art science reviews [Monograph]. Retrieved September 23, 2019, from http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/index.html

Collins, K., Tessler, H., Harrigan, K., Dixon, M., & Fugelsang, J. (2012). Sound in Electronic Gambling Machines: A Review of the Literature and its Relevance to Game Sound. In *Game Sound Technology and Player Interaction: Concepts and Developments*. https://doi.org/10.4018/978-1-61692-828-5.ch001

Company Info | Facebook Newsroom. (n.d.). Retrieved May 18, 2018, from https://newsroom.fb.com/company-info/

Cooper, P. G. (2019). Social Media. In *Salem Press Encyclopedia*. Salem Press.

Cyberbullying (for Parents)—KidsHealth. (n.d.). Retrieved October 24, 2019, from https://kidshealth.org/en/parents/cyberbullying.html

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Definition of BLOG. (n.d.). Retrieved October 22, 2019, from https://www.merriam-webster.com/dictionary/blog

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x

DeMarco, J. N., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M., … Bifulco, A. (2017). Digital Dangers and Cyber-Victimisation: A Study of European Adolescent Online Risky Behaviour for Sexual Exploitation. *Clinical Neuropsychiatry*, *14*(1), 104–112.

Denney, D. (2005). *Risk and Society*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=251302&site=eds-live

Derks, D., Fischer, A. H., & Bos, A. E. R. (2008). The role of emotion in computer-mediated communication: A review. *Computers in Human Behavior*, *24*(3), 766–785. https://doi.org/10.1016/j.chb.2007.04.004

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Diomidous, M., Chardalias, K., Magita, A., Koutonias, P., Panagiotopoulou, P., & Mantas, J. (2016). Social and Psychological Effects of the Internet Use. *Acta Informatica Medica*, *24*(1), 66–68. https://doi.org/10.5455/aim.2016.24.66-68

Dodge, M., & Kitchin, R. (2003). *Mapping Cyberspace*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=96104&site=eds-live

Eder, P. F. (2012). A History of the Internet and the Digital Future. *World Future Review (World Future Society)*, *4*(1), 105–108.

Edosomwan, S., Prakasan, S. K., Kouame, D., Watson, J., & Seymour, T. (2011). *The History of Social Media and its Impact on Business*. *16*(3), 14.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Ephraim, P. E. (2013). African youths and the dangers of social networking: A culture-centered approach to using social media. *Ethics & Information Technology*, *15*(4), 275–284. https://doi.org/10.1007/s10676-013-9333-2

Eudaimonia. (2017, January 26). How Instagram Started. Retrieved October 20, 2019, from Medium website: https://medium.com/@obtaineudaimonia/how-instagram-started-8b907b98a767

Facebook users worldwide 2019. (n.d.). Retrieved October 23, 2019, from Statista website: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys Tutorials*, *16*(4), 2019–2036. https://doi.org/10.1109/COMST.2014.2321628

Flickr Company History: Before Instagram Lived Flickr. (n.d.). Retrieved October 20, 2019, from SEO Web Marketing Internet and Social Media News website: http://www.seowebmarketing.co.uk/flickr-company-history/

Floros, G. D., Siomos, K. E., Fisoun, V., Dafouli, E., & Geroukalis, D. (2013). Adolescent online cyberbullying in Greece: The impact of parental online security practices, bonding, and online impulsiveness. *Journal of School Health*, (6), 445.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Fox, N. (1999). PostModern reflections on risk' "hazards" and lifechoices. In M. Douglas (Ed.), *Risk and Sociocultural theory:new directions and perspectives* (p. 212). Cambridge University Press.

Frangos, C. C., Frangos, C. C., & Sotiropoulos, I. (2011). Problematic Internet Use Among Greek University Students: An Ordinal Logistic Regression with Risk Factors of Negative Psychological Beliefs, Pornographic Sites, and Online Games. *CyberPsychology, Behavior & Social Networking*, *14*(1/2), 51–58. https://doi.org/10.1089/cyber.2009.0306

Frewer, L. J., Howard, C., & Shepherd, R. (1998). Understanding public attitudes to technology. *Journal of Risk Research*, *1*(3), 221–235. https://doi.org/10.1080/136698798377141

Frye, J. N., Veitch, C. K., Mateski, M. E., Michalski, J. T., Harris, J. M., Trevino, C. M., & Maruoka, S. (2012). *Cyber threat metrics.* (No. SAND2012-2427, 1039394). https://doi.org/10.2172/1039394

Giota, K. G., & Kleftaras, G. (2013). The role of personality and depression in problematic use of social networking sites in Greece. *Cyberpsychology*, *7*(3), 1–10. https://doi.org/10.5817/CP2013-3-6

Gkiomisi, A., Gkrizioti, M., Gkiomisi, A., Anastasilakis, D. A., & Kardaras, P. (2017). Cyberbullying Among Greek High School Adolescents. *Indian Journal Of Pediatrics*, *84*(5), 364–368. https://doi.org/10.1007/s12098-016-2256-2

González-Bailón, S. (2018, April 4). Want to change Facebook? Don't delete your account—use it for good. Retrieved November 22, 2019, from Quartz website: https://qz.com/1244750/the-delete-facebook-movement-is-ultimately-self-defeating/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Gregersen, E. (n.d.). LinkedIn | Overview, History, & Facts. Retrieved October 19, 2019, from Encyclopedia Britannica website: https://www.britannica.com/topic/LinkedIn

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111.

Hargittai, E. (2007). Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication*, *13*(1), 276–297. https://doi.org/10.1111/j.1083-6101.2007.00396.x

Hayes, B. (2000). *GRAPH THEORY IN PRACTICE: PART I*. *88*(1), 6.

Hilbert, M. (2016). Big Data for Development: A Review of Promises and Challenges. *Development Policy Review*, *34*(1), 135–174. https://doi.org/10.1111/dpr.12142

Hilgartner. (1992). The Social Construction of Risk Objects: Or, How to Pry Open Networks of Risk. Retrieved August 23, 2019, from ResearchGate website: https://www.researchgate.net/publication/257732287_The_Social_Construction_of_Risk_Objects_Or_How_to_Pry_Open_Networks_of_Risk

Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, & Yan Chen. (2011). Security Issues in Online Social Networks. *IEEE Internet Computing, Internet Computing, IEEE, IEEE Internet Comput.*, (4), 56. https://doi.org/10.1109/MIC.2011.50

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys Tutorials*, *17*(4), 2242–2270. https://doi.org/10.1109/COMST.2015.2457491

Houghton, D. J., & Joinson, A. N. (2010). Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services*, *28*(1–2), 74–94. https://doi.org/10.1080/15228831003770775

Hwang, H., & Kim, K.-O. (2015). Social media as a tool for social movements: The effect of social media use and social capital on intention to participate in social movements. *International Journal of Consumer Studies*, *39*(5), 478–488. https://doi.org/10.1111/ijcs.12221

infographic-information-technologies-2019—ELSTAT. (n.d.). Retrieved November 22, 2019, from https://www.statistics.gr/el/infographic-information-technologies-2019

Jaeger, C. W. (2012). CYBER-TRACKING: INTERPRETING A FIVE LEVEL MODEL OF BEHAVIOR IN CYBERSPACE. *Wdsinet.Org/Annual_Meetings/2012_Proceedings/Papers/Paper251.Pdf*, 2.

Jowitt, T. (2017, November 3). Tales In Tech History: Myspace. Retrieved October 19, 2019, from Silicon UK website: https://www.silicon.co.uk/e-marketing/socialmedia/tales-tech-history-myspace-224241

Kaplan M. Andreas, & Haenlein Michael. (2009). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons (2010)*, *53*, 59–68. https://doi.org/doi:10.1016/j.bushor.2009.09.003

Kapoor, T. (n.d.). *Pros and Cons of Social Networking*. Retrieved from http://www.academia.edu/619443/Pros_and_Cons_of_Social_Networking

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, *10*(1), 52–71. https://doi.org/10.5817/CP2016-1-2

Kimbrough, A., Guadagno, R., & Janeann Dill, D. der P. (2013). *Gender differences in mediated communication: Women connect more than do men*. Retrieved from https://www.academia.edu/19260090/Gender_differences_in_mediated_communication_Women_connect_more_than_do_men

Kleinberg, J. (2008). The Convergence of Social and Technological Networks. *Commun. ACM*, *51*(11), 66–72. https://doi.org/10.1145/1400214.1400232

Kormas, G., Critselis, E., Janikian, M., Kafetzis, D., & Tsitsika, A. (2011). Risk factors and psychosocial characteristics of potential problematic and problematic internet use among adolescents: A cross-sectional study. *BMC Public Health*, *11*, 595–595. https://doi.org/10.1186/1471-2458-11-595

Kourouthanassis, P., Lekakos, G., & Gerakis, V. (2015). Should I stay or should I go? The moderating effect of self-image congruity and trust on social networking continued use. *Behaviour & Information Technology*, *34*(2), 190–203. https://doi.org/10.1080/0144929X.2014.948489

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kraut, R., & Burke, M. (2015). Internet use and psychological well-being: Effects of activity and audience. *Communications of the ACM*, *58*(12), 94–100. https://doi.org/10.1145/2739043

Kuss, D. J., & Griffiths, M. D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environmental Research & Public Health*, *14*(3), 311. https://doi.org/10.3390/ijerph14030311

Lee, Y.-H., Ko, C.-H., & Chou, C. (2015). Re-visiting internet addiction among Taiwanese students: A cross-sectional comparison of students' expectations, online gaming, and online social interaction. *Journal Of Abnormal Child Psychology*, *43*(3), 589–599. https://doi.org/10.1007/s10802-014-9915-4

Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. *EURASIP Journal on Wireless Communications and Networking*, *2009*(1), 692654. https://doi.org/10.1155/2009/692654

Livingstone, S., & Brake, D. R. (2010). On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. *Children & Society*, *24*(1), 75–83. https://doi.org/10.1111/j.1099-0860.2009.00243.x

Loon, J. van. (2002). *Risk and Technological Culture: Towards a Sociology of Virulence*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=83193&site=eds-live

Lucchi, N. (2015). Internet–Based Communication: Rights, Risks and Opportunities. *European Journal of Risk Regulation*, *6*(1), 121–128. https://doi.org/10.1017/S1867299X00004347

Lupton, D., & Tulloch, J. (2002a). `Risk is Part of Your Life': Risk Epistemologies Among a Group of Australians. *Sociology*, *36*(2), 317–334. https://doi.org/10.1177/0038038502036002005

Lupton, D., & Tulloch, J. (2002b). "Life would be pretty dull without risk": Voluntary risk-taking and its pleasures. *Health, Risk & Society*, *4*(2), 113–124. https://doi.org/10.1080/13698570220137015

MacArthur, A. (2019, July 1). The History of Twitter You Didn't Know. Retrieved October 20, 2019, from Lifewire website: https://www.lifewire.com/history-of-twitter-3288854

Madden, M., & Zickuhr, K. (2011, August 26). 65% of online adults use social networking sites. Retrieved November 22, 2019, from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2011/08/26/65-of-online-adults-use-social-networking-sites/

Marzano, G., Lubkina, V., & Truskovska, Z. (2013). Cyberspace's threats: A pedagogical perspective on Internet addiction, violence and abuse. *Pedagogia Oggi*.

McAlinden, A.-M. (2012). *"Grooming" and the Sexual Abuse of Children: Institutional, Internet, and Familial Dimensions*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=520109&site=eds-live&authtype=ip,athens

Meter, D. J., & Bauman, S. (2015). When Sharing Is a Bad Idea: The Effects of Online Social Network Engagement and Sharing Passwords with Friends on Cyberbullying Involvement. *Cyberpsychology, Behavior And Social Networking*, *18*(8), 437–442. https://doi.org/10.1089/cyber.2015.0081

Mitchell, K. J., & Ybarra, M. (2009). Social networking sites: Finding a balance between their risks and benefits. *Archives Of Pediatrics & Adolescent Medicine*, *163*(1), 87–89. https://doi.org/10.1001/archpediatrics.2008.534

Montes-Vozmediano, M., García-Jiménez, A., & Menor-Sendra, J. (2018). Teen Videos on YouTube: Features and Digital Vulnerabilities. *Comunicar: Media Education Research Journal*, *26*(54), 61–69. (Grupo Comunicar Ediciones. Marina 8, Atico B - 21001 Huelva, Spain. Tel: 34-959-248480; e-mail: info@grupocomunicar.com; Web site: https://www.revistacomunicar.com/).

Oweis, N. E., Alrababa, M. A., Oweis, W. G., Owais, S. S., & Alansari, M. (2014). A survey of Internet security risk over social networks. *2014 6th International Conference on Computer Science and Information Technology (CSIT)*, 1–4. https://doi.org/10.1109/CSIT.2014.6805970

Öztürk, C., Bektas, M., Ayar, D., Özgüven Öztornacı, B., & Yağcı, D. (2015). Association of Personality Traits and Risk of Internet Addiction in Adolescents. *Asian Nursing Research*, *9*(2), 120–124. https://doi.org/10.1016/j.anr.2015.01.001

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331–338. https://doi.org/10.1016/j.jretai.2006.08.006

Petter, B., Henrik, B., Martikainen, M., & Lehner, O. M. (2019). Cybercrime in a Business World: Behavioral Perspectives. *ACRN Oxford Journal of Finance & Risk Perspectives*, *8*, 98–110.

Ponte, C., Simões, J. A., & Jorge, A. (2013). Do questions matter on children's answers about internet risk and safety? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *7*(1). https://doi.org/10.5817/CP2013-1-2

PRIVACY | meaning in the Cambridge English Dictionary. (n.d.). Retrieved October 25, 2019, from https://dictionary.cambridge.org/dictionary/english/privacy

Rain, O., & Lorents, P. (2010, April). Cyberspace: Definition and Implications - ProQuest. Retrieved September 27, 2019, from https://search.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?pq-origsite=gscholar&cbl=396500

Rangwala, M. (2017, May 12). The evolution of social media over the last 2 decades. Retrieved October 20, 2019, from YourStory.com website: https://yourstory.com/2017/05/evolution-of-social-media

Rasmussen, J., & Ihlen, Ø. (2017). Risk, Crisis, and Social Media: A systematic review of seven years' research. *NORDICOM Review*, *38*(2), 1–17. https://doi.org/10.1515/nor-2017-0393

Remaining Safe and Avoiding Dangers Online: A Social Media Q&A with Kimberly Mitchell. (2010). *Prevention Researcher*, *17*(5), 7–9. (Integrated Research Services, Inc. 66 Club Road Suite 370, Eugene, OR 97401. Tel: 800-929-2955; Fax: 541-683-2621; Web site: http://www.tpronline.org).

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, *1*(1), 49–71. https://doi.org/10.1080/136698798377321

Rosen, L. D., Whaling, K., Carrier, L. M., Cheever, N. A., & Rokkum, J. (2013). The Media and Technology Usage and Attitudes Scale: An empirical investigation. *Computers in Human Behavior*, *29*(6), 2501–2511. https://doi.org/10.1016/j.chb.2013.06.006

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior. *Journal of Social Psychology*, *154*(4), 352–369. https://doi.org/10.1080/00224545.2014.914881

Safeline. (n.d.). Στατιστικά στοιχεία Safeline για το 2015—Ασφάλεια στο Διαδίκτυο. Retrieved October 23, 2019, from https://internet-safety.sch.gr/index.php/articles/parents/item/378-στατιστικά-στοιχεία-safeline-για-το-2015

Sampasa-Kanyinga, H., & Hamilton, H. A. (2015). Use of Social Networking Sites and Risk of Cyberbullying Victimization: A Population-Level Study of Adolescents. *Cyberpsychology, Behavior And Social Networking*, *18*(12), 704–710. https://doi.org/10.1089/cyber.2015.0145

Schulz, A., Bergen, E., Schuhmann, P., Hoyer, J., & Santtila, P. (2015). Online Sexual Solicitation of Minors: How Often and between Whom Does It Occur? *Journal of Research in Crime and Delinquency*, *ahead of print*. https://doi.org/10.1177/0022427815599426

Sheldon, J. (2012). State of the Art: Attackers and Targets in Cyberspace | Journal of Military and Strategic Studies. *Journal of Military and Strategic Studies*, *Vol 14*(No 2 (2012)). Retrieved from https://journalhosting.ucalgary.ca/index.php/jmss/article/view/58029

Slovic, P. (1993). Perceived Risk, Trust, and Democracy. *Risk Analysis*, *13*(6), 675–682. https://doi.org/10.1111/j.1539-6924.1993.tb01329.x

Smith, A., & Anderson, M. (2018, March 1). Social Media Use 2018: Demographics and Statistics. Retrieved November 21, 2019, from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/

Snap shares skyrocket on first earnings beat with revived user growth. (n.d.). Retrieved October 20, 2019, from TechCrunch website: http://social.techcrunch.com/2018/02/06/snap-inc-earnings-q4-2017/

Social Media and Our Privacy. (2016). Retrieved November 22, 2019, from Futurism website: https://vocal.media/futurism/social-media-and-our-privacy

SOCIAL NETWORKING | meaning in the Cambridge English Dictionary. (n.d.). Retrieved October 18, 2019, from https://dictionary.cambridge.org/dictionary/english/social-networking

Stalans, L. J., & Finn, M. A. (2016). Understanding How the Internet Facilitates Crime and Deviance. *Victims & Offenders*, *11*(4), 501–508. https://doi.org/10.1080/15564886.2016.1211404

Statistics. (n.d.). Retrieved May 31, 2018, from Cyberbullying Research Center website: https://cyberbullying.org/statistics

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *In IDMAa and IMS Code Conference*, *3*.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Tarinidis I., K., Baglanea, P., Danilans, D., Rokis, M., Elisa, D., & Marques, J. (n.d.). *Risk, Trust and Privacy Issues on Internet Social Network Communities*. 21.

Taylor-Gooby, P., & Zinn, J. (2006). *Risk in Social Science*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=e000bww&AN=191297&site=eds-live

Terrell, K. (2015, June 16). The History of Social Media: Social Networking Evolution! Retrieved October 19, 2019, from History Cooperative website: https://historycooperative.org/the-history-of-social-media/

The history of YouTube. (2016, May 9). Retrieved October 20, 2019, from Phrasee website: https://phrasee.co/the-history-of-youtube/

Theohary, C. A. (2018). *Defense Primer: Cyberspace Operations*. 2.

Theohary, C. A., & Harrington, A. I. (2015). Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities. In *Cyberspace Threat Landscape*. Retrieved from http://eds.a.ebscohost.com/eds/ebookviewer/ebook/ZTAyMG13d19fOTg2NjY5X19BTg2?sid=842cfc77-2f1e-428b-a721-63f9f48f85c5@sdc-v-sessmgr01&vid=5&format=EB&rid=1

Today's social network sites: An analysis of emerging security risks and their counter measures. (2017). *2017 International Conference on Communication Technologies (ComTech), Communication*

*Technologies (ComTech), 2017 International Conference On*, 143. https://doi.org/10.1109/COMTECH.2017.8065764

Todd, H. K., Dave Gershgorn, Sarah. (2018, March 29). The Cambridge Analytica scandal is wildly confusing. This timeline will help. Retrieved November 22, 2019, from Quartz website: https://qz.com/1240039/the-cambridge-analytica-scandal-is-confusing-this-timeline-will-help/

Tsiolka, E., Bergiannaki, I. D., Margariti, M., Malliori, M., & Papageorgiou, C. (2017). Dysfunctional internet behaviour symptoms in association with personality traits. *Psychiatrike = Psychiatriki*, *28*(3), 211–218. https://doi.org/10.22365/jpsych.2017.283.211

Tsitsika, A., Critselis, E., Kormas, G., Filippopoulou, A., Tounissidou, D., Freskou, A., … Kafetzis, D. (2009). Internet use and misuse: A multivariate regression analysis of the predictive factors of internet use among Greek adolescents. *European Journal Of Pediatrics*, *168*(6), 655–665. https://doi.org/10.1007/s00431-008-0811-1

Tsitsika, A., Janikian, M., Schoenmakers, T. M., Tzavela, E. C., Olafsson, K., Wójcik, S., … Richardson, C. (2014). Internet addictive behavior in adolescence: A cross-sectional study in seven European countries. *Cyberpsychology, Behavior And Social Networking*, *17*(8), 528–535. https://doi.org/10.1089/cyber.2013.0382

Turel, O., & Serenko, A. (2012). The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems*, *21*(5), 512–528. https://doi.org/10.1057/ejis.2012.1

Vadza, K. (2011). Cyber Crime & its Categories. *Indian Journal of Applied Research*, *3*, 130–133. https://doi.org/10.15373/2249555X/MAY2013/39

Vandoninck, S., d'Haenens, L., De Cock, R., & Donoso, V. (2012). Social Networking Sites and Contact Risks among Flemish Youth. *Childhood: A Global Journal of Child Research*, *19*(1), 69–85. (SAGE Publications. 2455 Teller Road, Thousand Oaks, CA 91320. Tel: 800-818-7243; Tel: 805-499-9774; Fax: 800-583-2665; e-mail: journals@sagepub.com; Web site: http://sagepub.com).

Walker, K. N., MacBride, A., & Vachon, M. L. S. (1977). Social support networks and the crisis of bereavement. *Social Science & Medicine (1967)*, *11*(1), 35–41. https://doi.org/10.1016/0037-7856(77)90143-3

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

Weber, E. U. (2001). Risk: Empirical Studies on Decision and Choice. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 13347–13351). https://doi.org/10.1016/B0-08-043076-7/00634-3

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, *16*(2), 38–43. https://doi.org/10.1016/j.istr.2011.09.008

What is a Podcast? - Definition from Techopedia. (n.d.). Retrieved October 22, 2019, from Techopedia.com website: https://www.techopedia.com/definition/5546/podcast

What is Media? - Definition from Techopedia. (n.d.). Retrieved October 22, 2019, from Techopedia.com website: https://www.techopedia.com/definition/1098/media

What is Socware | IGI Global. (n.d.). Retrieved October 24, 2019, from https://www.igi-global.com/dictionary/auditing-defense-against-xss-worms-in-online-social-network-based-web-applications/54784

Williams, K., Boyd, A., Densten, S., Chin, R., Diamond, D., & Morgenthaler, C. (2009). *Social Networking Privacy Behaviors and Risks*.

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A Review of Facebook Research in the Social Sciences. *Perspectives on Psychological Science*, *7*(3), 203–220. https://doi.org/10.1177/1745691612442904

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining Characteristics and Associated Distress Related to Internet Harassment: Findings From the Second Youth Internet Safety Survey. *Pediatrics*, *118*(4), e1169–e1177. https://doi.org/10.1542/peds.2006-0815

Yeo, G. (2013). Trust and context in cyberspace. *Archives and Records*, *34*(2), 214–234. https://doi.org/10.1080/23257962.2013.825207

Yisa, V. L., Osho, O., & Soje, I. (2016). *Online Social Networks: A Survey of Usage and Risks Experience among University Students in North-Central Nigeria*. 5.

Young, Kimberly S. (1996, August 15). *INTERNET ADDICTION: THE EMERGENCE OF A NEW CLINICAL DISORDER*. *Vol. 1 No. 3.*, pages 237-24. Retrieved from https://pdfs.semanticscholar.org/04b3/09af262cf2643daa93a34c1ba177cd6e7a85.pdf

Zhang, N. (andy, Wang, C. (alex, & Xu, Y. (2011). *PRIVACY IN ONLINE SOCIAL NETWORKS Completed Research Paper*.

Η Ελλάδα με Αριθμούς—ELSTAT. (n.d.). Retrieved November 22, 2019, from https://www.statistics.gr/greece-in-figures

Σαλούρου, Ρ. (2015, September 19). Ετοιμη να εκραγεί η δημογραφική βόμβα, τ | Kathimerini. Retrieved November 20, 2019, from https://www.kathimerini.gr/831452/article/oikonomia/ellhnikh-oikonomia/etoimh-na-ekragei-h-dhmografikh-vomva

Στατιστικές—ELSTAT. (n.d.). Retrieved November 20, 2019, from https://www.statistics.gr/el/statistics/-/publication/SAM07/-

Χρήστος Κατσάνος. (2017). *ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΜΠΕΙΡΙΚΗΣ ΕΡΕΥΝΑΣ (ΚΠΣ513) Γνωστικό Αντικείμενο 4: Προετοιμασίες για έρευνα*.

# Κατάλογος Εικόνων

# Κατάλογος Πινάκων

# Κατάλογος Γραφημάτων