Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών: ***Ασφάλεια Υπολογιστών και Δικτύων***

Μεταπτυχιακή Διατριβή

Έρευνα για την αντιληπτή Ασφάλεια και Εμπιστοσύνη στα Μέσα Κοινωνικής Δικτύωσης και η επίδραση τους στα προσωπικά δεδομένα

Ανδρέου Γεώργιος

Επιβλέπων Καθηγητής
Ζαχαριάς Παναγιώτης

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Έρευνα για την αντιληπτή Ασφάλεια και Εμπιστοσύνη στα Μέσα Κοινωνικής Δικτύωσης και η επίδραση τους στα προσωπικά δεδομένα

Ανδρέου Γεώργιος

Επιβλέπων Καθηγητής
Ζαχαριάς Παναγιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην Ασφάλεια Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2019

Περίληψη

Αναμφισβήτητα η εποχή την οποία διανύουμε είναι αυτή της ψηφιακής επανάστασης με τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ) να αποτελούν το βασικό πυλώνα αυτής της επανάστασης. Σύμφωνα με τα στατιστικά στοιχεία που είναι διαθέσιμα περισσότεροι από 7.5 δισεκατομμύρια άνθρωποι (το 55% περίπου) σε όλο τον κόσμο έχουν πρόσβαση στον ψηφιακό αυτό κόσμο ενώ η αύξηση των χρηστών από το 2000 μέχρι σήμερα ξεπερνά το 890%.

Αφορμή για την παρούσα Διπλωματική εργασία ήταν οι προεδρικές εκλογές των ΗΠΑ το 2016 όπου η οσμή σκανδάλων και παρατυπιών να είναι κάτι παραπάνω από έντονη και βασικό εργαλείο στη χειραγώγηση των ψηφοφόρων ήταν τα Μέσα Κοινωνικής Δικτύωσης. Οι πολιτικοί πια σε όλο τον κόσμο αξιοποιούν στο έπακρο το προνομιακό χώρο που προσφέρουν τα ΜΚΔ και πλέον δημοσιοποιούν προσωπικά τους μηνύματα συμμετέχοντας στην ηλεκτρονική δημιουργία ενός πάζλ πληροφοριών και γεγονότων με συνοδοιπόρους τους ίδιους τους χρήστες. Μέσα από τα ΜΚΔ γίνεται μια αμφίδρομη επικοινωνία μεταξύ πολιτικών και πολιτών ανταλλάσοντας πληροφορίες και απόψεις.

Σκοπός αυτής της Διπλωματικής εργασίας είναι να αναδείξει τους κινδύνους που διατρέχουν οι χρήστες καθημερινά στα Μέσα Κοινωνικής Δικτύωσης καθώς ο ρόλος τους δεν είναι καθόλου σύμφωνος με τις επιθυμίες και τις απαιτήσεις των χρηστών. Γύρω από τα μέσα αυτά έχει στηθεί μια πολύ καλά οργανωμένη επιχείρηση χειραγώγησης των χρηστών από την απλή προώθηση προϊόντων μέχρι τον επηρεασμό της ψήφου σε τοπικές ή εθνικές εκλογές. Οι χρήστες αν και γνωρίζουν πια ότι οι προθέσεις των ΜΚΔ δεν είναι και τόσο αθώες εντούτοις κάνουν ελάχιστα για να διαφυλάξουν τα προσωπικά τους δεδομένα και τα δεδομένα φίλων τους με αποτέλεσμα να δίνουν απλόχερα στα ΜΚΔ προσωπικές πληροφορίες ή προτιμήσεις οι οποίες βέβαια αξιοποιούνται ανάλογα.

Summary

We are undoubtedly experiencing the digital revolution era with Social Media being the main pillar of this revolution. According to available statistics more than 7.5 billion people (around 55%) worldwide, have access to digital world while the increase in the number of users since 2000 up today is more than 890%.

Current Thesis came up from the fact that in US presidential elections in 2016 intense scandals and irregularities took place and Social Media were used as the basic tool to manipulate voters. Politicians nowadays around the world take advantage of Social Media to publicize personal messages and participate in the creation of a puzzle of information and facts along with the users. A two way communication between politicians and citizens takes place through Social Media by exchanging information and views.

The purpose of this thesis is to highlight the dangers that users face every day while using Social Media as their role is not at all consistent with the wishes and demands of users. A well-organized user manipulation business has been set up around Social Media, aiming to promote products or even influence voters in local or national elections. Although users are aware of the “not so innocent” intentions of Social Media, however they act poorly to safeguard their personal data and as a result they provide personal information or preferences to Social Media, which are of course used accordingly.

Περιεχόμενα σελ

Πρόλογος

Τα μέσα κοινωνικής δικτύωσης σήμερα έχουν αλλάξει το σκοπό για τον οποίο δημιουργηθήκαν. Η αρχική ιδέα της ύπαρξης τους ήταν να διαμοιράζουν απόψεις, ιδέες, εμπειρίες και να μπορεί κανείς μέσα από μια πολυπληθή βάση δεδομένων να βρει στοιχεία για ανθρώπους, φίλους, συμμαθητές με τους οποίους θα ήταν εξαιρετικά δύσκολη η επικοινωνία μαζί τους . Το Facebook κατά κύριο λόγο συντέλεσε στην ενίσχυση της κοινωνικοποίησης των ανθρώπων κάνοντας τους να εξωτερικεύσουν πληροφορίες, απόψεις, συναισθήματα σκέψεις και πολύ περισσότερα . Δυστυχώς όπως όμως συμβαίνει συχνά ο άνθρωπος έχει την τάση να περνά στο αντίθετο άκρο, αυτό της υπερέκθεσης κοινοποιώντας σε «φίλους» προσωπικές πληροφορίες, δικές του ή της οικογένειας του, φίλων του, και κάθε είδους προσωπικών προτιμήσεων. Τα ίδια τα ΜΚΔ βέβαια δεν άφησαν την ευκαιρία να πάει χαμένη και ουσιαστικά να καθοδηγήσουν τους χρήστες είτε σε προϊόντα (για τα οποία έχουν τεράστια κέρδη μέσω διαφήμισης), είτε δημοσιοποιούν ειδήσεις (οι οποίες απέχουν πολύ από το να είναι οι σημαντικότερες που απασχολούν την κοινή γνώμη), και τελικά μέσω του εξελιγμένου αλγόριθμου που χρησιμοποιούν να διαμορφώνουν ουσιαστικά το προφίλ των χρηστών.

Η ερώτηση που ακούγεται όλο και πιο συχνά στα χείλη των χρηστών του Facebook: Γιατί καθημερινά βλέπουμε ειδήσεις και ενημερώσεις για συγκεκριμένα θέματα ή από συγκεκριμένες σελίδες στη ροή τους; Η απάντηση είναι πιο απλή από ότι φανταζόμαστε. Αποκλειστικοί υπεύθυνοι είμαστε εμείς οι ίδιοι. Και το Facebook θα μας αποκαλύπτει πλέον αναλυτικά πως γίνεται αυτό, μέσα από τη νέα λειτουργία "Γιατί βλέπω αυτή την ανάρτηση;".

Στην πράξη, μέσα από τις καθημερινές τους δραστηριότητες, οι χρήστες του δημοφιλέστερου κοινωνικού δικτύου επηρεάζουν τον αλγόριθμο, στην ουσία "αυτοφακελώνονται" επιλέγοντας να επισκέπτονται συγκεκριμένες σελίδες, συγκεκριμένες πηγές ενημέρωσης, συγκεκριμένη θεματολογία. Όλα αυτά αναλύονται από τον αλγόριθμο που πρακτικά "σερβίρει" στους χρήστες αυτό που ακριβώς θέλουν να δουν, από εκεί που θέλουν να το δουν... Βλέπετε π.χ. όλη την ώρα βίντεο με χαριτωμένα σκυλάκια και γατάκια; Τότε αυτά θα έχουν πρώτο λόγο στη ροή σας. Συνηθίζετε να ενημερώνεστε από δυο - τρεις συγκεκριμένες σελίδες; Η πλειοψηφία από τα ειδησεογραφικά θέματα που εμφανίζονται στις ενημερώσεις σας είναι από εκεί.

Κεφάλαιο 1.
Εισαγωγή στα ΜΚΔ

Τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ) θεωρούνται οι τεχνολογίες και οι πρακτικές που χρησιμοποιούνται από τους χρήστες για να διαμοιράσουν απόψεις, ιδέες, εμπειρίες ή ακόμα και πολυμέσα (video εικόνα). Σαν σκοπό έχουν να κτίσουν κοινωνικές σχέσεις μεταξύ των χρηστών μέσα από τις σελίδες ΜΚΔ επιτρέποντας στους ανθρώπους να δημιουργούν προφίλ με τα οποία συνδέονται με άλλους ανθρώπους. Οι πιο γνωστές είναι το Facebook, Twitter, Youtube, Instagram, LinkedIn, Google+ κ.α.

Η χρήση των ΜΚΔ γίνεται με διάφορους τρόπους με τους οποίους οι χρήστες αλληλεπιδρούν ο ένας με τον άλλον σε απ' ευθείας σύνδεση (online) και περιλαμβάνει κατά κύριο λόγο δημιουργία και σχολιασμό σε blogs, διαμοιρασμό περιεχομένου ή επικοινωνία με φίλους μέσα από αυτά. Τα νέα μέλη που εντάσσονται στα μέσα αυτά δημιουργούν μια ηλεκτρονική σελίδα προφίλ κάνοντας τους να έρθουν σε επαφή μέσω email ή άμεσου μηνύματος (57: Kwak 2010:591-600).

Τα ΜΚΔ αποτελούν βασικό εργαλείο για την προώθηση προϊόντων και υπηρεσιών. Ένας τρόπος για να γίνει αυτό είναι δημιουργώντας οι επιχειρήσεις σελίδες θαυμαστών των προϊόντων τους στα ΜΚΔ. Οι εταιρείες μπορούν να τοποθετήσουν δημοσιεύσεις για κάποιο προϊόν (χρησιμοποιώντας βίντεο, μηνύματα, κουίζ κ.α.) σε σελίδες θαυμαστών. Οι χρήστες – πελάτες μπορούν να εκφράσουν την επιθυμία τους κάνοντας 'like' ή σχολιάζοντας μέσω 'comments' (46: Jansen 2009: 2169-2385) .

1.1 Κοινά χαρακτηριστικά των Μέσων Κοινωνικής Δικτύωσης

Τα ΜΚΔ κατά Mayfield (66: Mayfield 2008) παρουσιάζουν κάποια κοινά χαρακτηριστικά τα οποία μπορούμε να τα συνοψίσουμε ως ακολούθως:

Συμμετοχή(Participation)*:* Τα ΜΚΔ ενθαρρύνουν τη συμμετοχή των χρηστών σε αυτά μέσα από σχόλια likes κ.α.

Διαφάνεια(Opensses)*:* οι περισσότερες υπηρεσίες των ΜΚΔ είναι ανοικτές σε ανατροφοδότηση και συμμετοχή ενώ οι χρήστες σπάνια βρίσκουν εμπόδια στην πρόσβαση του περιεχομένου.

Συνομιλία (Conversation)*:* Σε αντίθεση με τα μέσα μαζικής ενημέρωσης τα ΜΚΔ αποτελούν μια αμφίδρομη επικοινωνία μεταξύ των χρηστών.

Κοινότητα(Community)*:* Τα ΜΚΔ παρέχουν εργαλεία για τη δημιουργία κοινοτήτων μέσα από τις οποίες οι χρήστες μοιράζονται κοινά ενδιαφέροντα ή απόψεις (αγάπη για τη φωτογραφία κ.α).

Συνεκτικότητα (Connectedness): Τα περισσότερα ΜΚΔ αναπτύσσουν μηχανισμούς συνεκτικότητας κάνοντας χρήση συνδέσεων με άλλες ιστοσελίδες, πόρους και ανθρώπους.

Είναι σημαντικό να αναφέρουμε ότι το Μάρτιο του 2008 η Διεθνής ομάδα Προστασίας των Προσωπικών δεδομένων των Τηλεπικοινωνιών (IWGDPT) εξέδωσε οδηγίες και συστάσεις για τις υπηρεσίες κοινωνικής δικτύωσης. Οι συστάσεις αυτές απευθύνονταν και στην Ελλάδα και αφορά τόσο τους χρήστες όσο και τα ίδια τα μέσα (46: Jansen 2009: 2169-2385).

1.2 *Προϋποθέσεις των ΜΚΔ*

Οι ίδιες οι υπηρεσίες κοινωνικής δικτύωσης θα πρέπει να έχουν τις εξής προϋποθέσεις:

1. Διαφανή και πλήρη πληροφόρηση των χρηστών σχετικά με την επεξεργασία και τη χρήση των προσωπικών τους δεδομένων. Η πληροφόρηση δεν πρέπει να αρκείται μόνο στο κείμενο όρων και προϋποθέσεων (“terms and conditions”) της πολιτικής απορρήτου του παρόχου αλλά και επιμέρους επιλογές όπως π.χ. στη δημιουργία άλμπουμ φωτογραφιών ώστε να ενημερώνεται ο χρήστης για πιθανούς κινδύνους από αυτή τη δημοσίευση. Θα πρέπει επίσης να ενημερώνουν τους χρήστες για όλους τους πιθανούς κινδύνους καθώς και να τους αποθαρρύνουν από τη δημοσιοποίηση προσωπικών δεδομένων τρίτων προσώπων καθώς και ενημέρωση για χρήση διαφημιστικών μηνυμάτων.

2. Παροχή ελέγχου των προφίλ των χρηστών από τους ίδιους ώστε να μην επιτρέπουν δεδομένα να δημοσιοποιηθούν χωρίς την έγκριση τους**.**

3. Ενεργοποίηση μηχανισμών διαχείρισης παραπόνων που υποβάλλονται από τους χρήστες, προβλέποντας και μέτρα, όπως κατάργηση λογαριασμών χρηστών που δεν συμμορφώνονται με τις απαιτήσεις για προσωπικά δεδομένα.

4. Δυνατότητα δημιουργίας ανώνυμων προφίλ από τους χρήστες.

1.3 Προϋποθέσεις των χρηστών των ΜΚΔ

Οι χρήστες από τη μεριά τους τώρα θα πρέπει:

1. Να είναι προσεκτικοί όταν δημοσιοποιούν προσωπικά δεδομένα καθώς αυτά αυτόματα είναι διαθέσιμα άμεσα από άγνωστο αριθμό χρηστών.

2. Να σέβονται την ιδιωτικότητα άλλων μη δημοσιοποιώντας προσωπικά δεδομένα τρίτων.

3. Να χρησιμοποιούν ρυθμίσεις φιλικές προς την ιδιωτικότητα , όπως: περιορισμό της διαθεσιμότητας των προσωπικών τους δεδομένων σε μηχανές αναζήτησης.

4. Να χρησιμοποιούν διαφορετικούς κωδικούς πρόσβασης από άλλους λογαριασμούς που διαθέτουν στο διαδίκτυο(web banking email κ.α.).

5. Να δείχνουν ιδιαίτερη προσοχή όταν τους ζητείται η συγκατάθεση τους για διάθεση προσωπικών δεδομένων σε διαφημιστικούς σκοπούς.

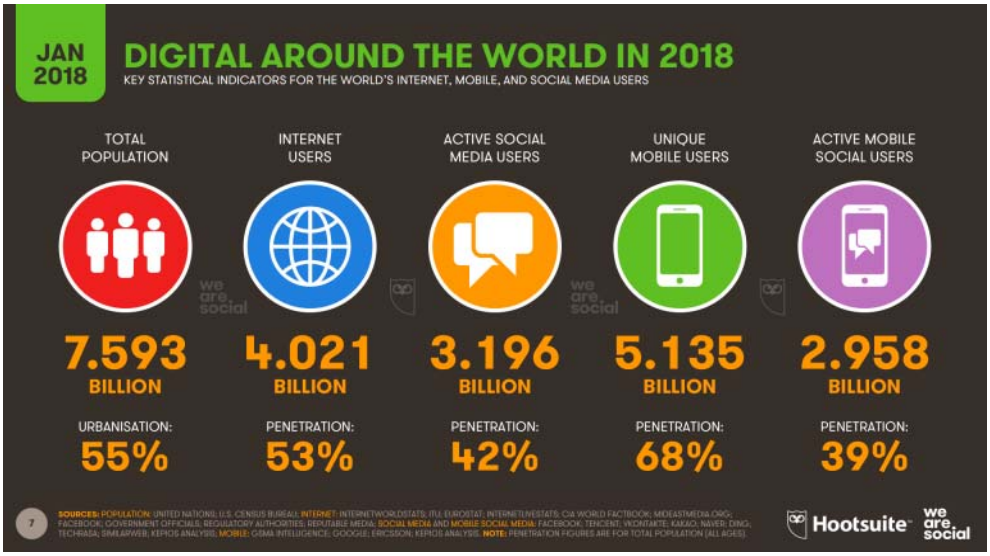
6. Δυνατότητα χρήσης ανωνύμων προφίλ σε περίπτωση που οι χρήστες δεν θέλουν να αποκαλύψουν καθόλου προσωπικές πληροφορίες.

Κεφάλαιο *2.* Ανταπόκριση χρηστών στα ΜΚΔ παγκοσμίως

Η καθημερινή χρήση των ΜΚΔ έχει απογειωθεί τα τελευταία χρόνια με κυριότερους εκπροσώπους το Facebook, Twitter και το LinkedIn. Η ραγδαία αυτή αύξηση απεικονίζεται στον παρακάτω πίνακα. Τα δεδομένα τα οποία ανταλλάσουν οι χρήστες είναι σε εξαιρετικά μεγάλες ποσότητες. Οι πάροχοι των ΜΚΔ λαμβάνουν τεράστια κέρδη από τη δημοσιοποίηση των δεδομένων των χρηστών σε τρίτους όπως διαφημιστικές εταιρείες ακαδημαϊκούς ερευνητές κ.α. (4: Amardeep 2018: 46-63)

2.1 Παντοδυναμία ΜΚΔ στο διαδίκτυο παγκοσμίως

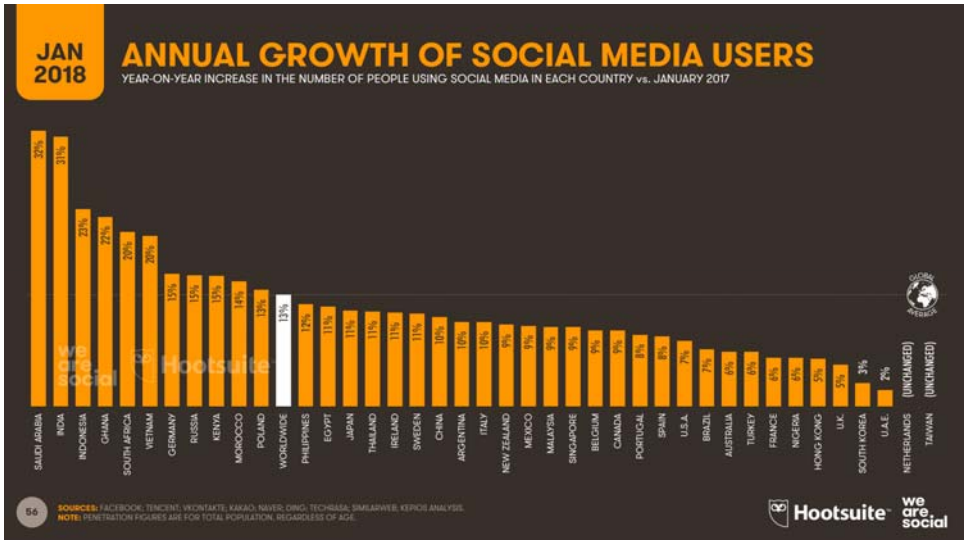
Στους παρακάτω πίνακες παρουσιάζονται στατιστικά δεδομένα σχετικά με την ραγδαία αύξηση των ΜΚΔ σε όλο το κόσμο. Συγκεκριμένα στον ακόλουθο πίνακα(Εικόνα 1) τα ΜΚΔ υποστηρίζονται από συνολικά 3.196 δις. χρηστών δηλαδή το 42% του πληθυσμού της γης (21: Chaffey 2018) .



Εικόνα 1

2.2 Ετήσια αύξηση των ΜΚΔ ανά χώρα

Στον ακόλουθο πίνακα (Εικόνα 2) παρουσιάζεται η ετήσια αύξηση που παρουσιάζουν τα ΜΚΔ ανά χώρα. Κατά μέσο όρο λοιπόν, η ετήσια αύξηση είναι 13% περίπου με τις μεγαλύτερες αυξήσεις να καταγράφονται σε Σαουδική Αραβία(32%) και Κίνα (31%)(21: Chaffey 2018).



Εικόνα 2

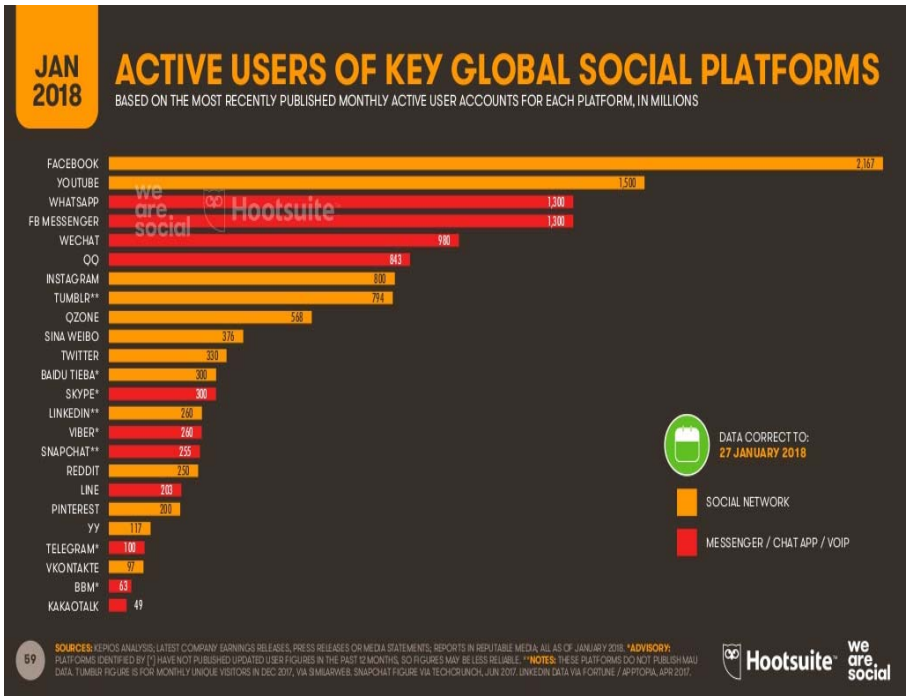
2.3 Μεταβολή των κυριότερων χαρακτηριστικών του Facebook μέσα στο 2018

Στον ακόλουθο πίνακα (Εικόνα 3) παρουσιάζεται η ετήσια αύξηση που παρουσίασαν για το 2018 τα πιο δημοφιλή χαρακτηριστικά του Facebook(21: Chaffey 2018).

Εικόνα 3

2.4 Facebook και ενεργοί χρήστες των δημοφιλέστερων ΜΚΔ

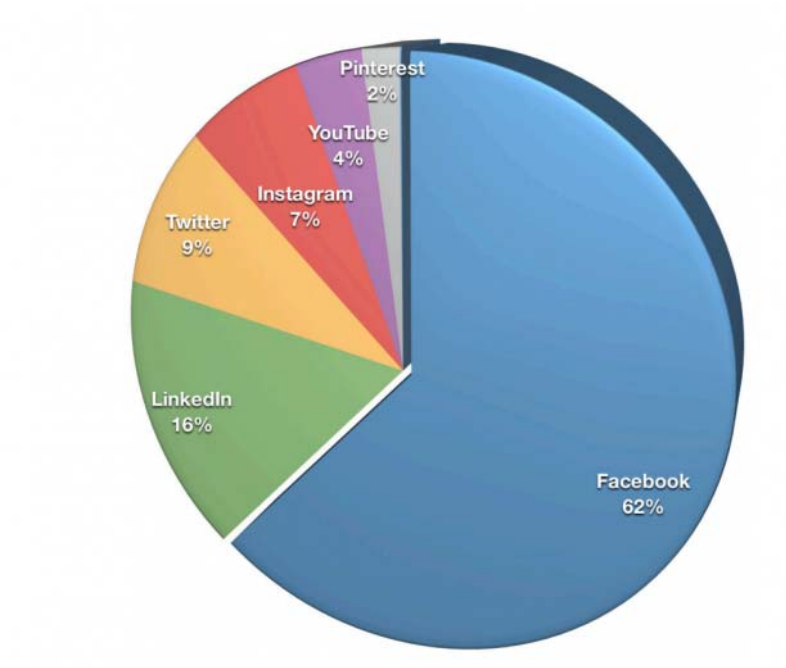
Στον ακόλουθο πίνακα (Εικόνα 4) παρουσιάζεται το πλήθος χρηστών που ακολουθούν πιο δημοφιλή ΜΚΔ. Όπως φαίνεται το Facebook κερδίζει με πολύ μεγάλη διαφορά ακολουθώντας το Youtube, whatsupp και Messenger(21: Chaffey 2018).



Εικόνα 4

2.5 Επιλογή των αγορών στα ΜΚΔ

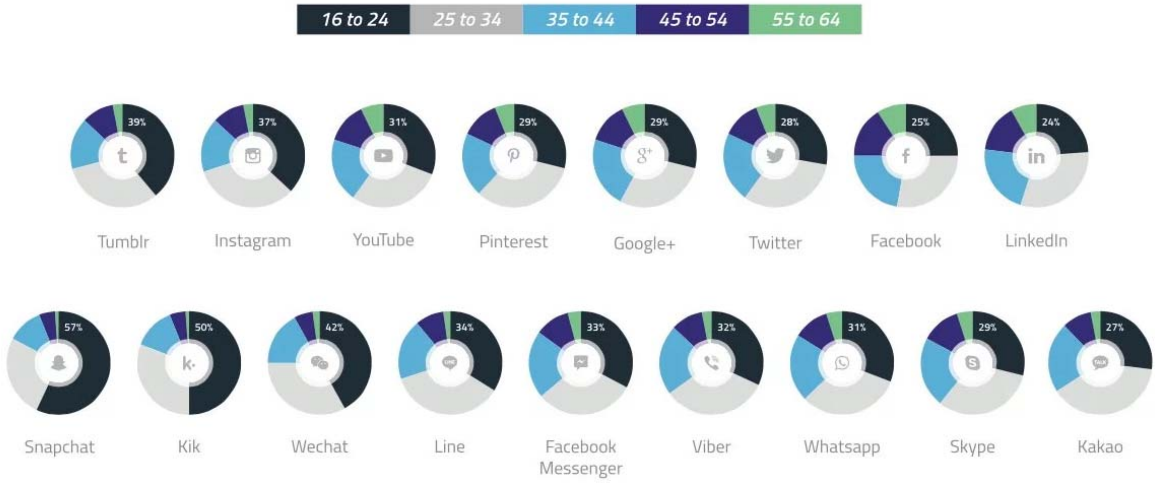
Στο επόμενο γράφημα (Εικόνα 5) παρουσιάζεται η σειρά με την οποία οι αγορές επιλέγουν να συνεργαστούν με τα διάφορα ΜΚΔ προκειμένου να διαφημίσουν τα προϊόντα τους. Και εδώ η παντοδυναμία του Facebook ξεχωρίζει με ποσοστό 62% και ακολουθεί με τεράστια διαφορά το LinkedIn και Twitter(21: Chaffey 2018).



Εικόνα 5

2.6 Ηλιακή κατανομή των ΜΚΔ

Στο παρακάτω γράφημα (Εικόνα 6) παρουσιάζεται η κατανομή των ΜΚΔ ανά ηλικία. Όπως παρατηρούμε οι μικρότερες ηλικίες έχουν προτίμηση περισσότερο στο Instagram και στο Snapchat σε αντίθεση με τις μεγαλύτερες ηλικίες που δείχνουν προτίμηση κυρίως σε Facebook και LinkedIn. Αυτό δείχνει και μια τάση γενικότερα κατά την οποία καταγράφεται σημαντική αποστροφή των νέων από το Facebook και προτίμηση τους στο Instagram κατά κύριο λόγο (για ανταλλαγή κυρίως περιεχομένων πολυμέσων) (65: Ma Mengyan 2017).

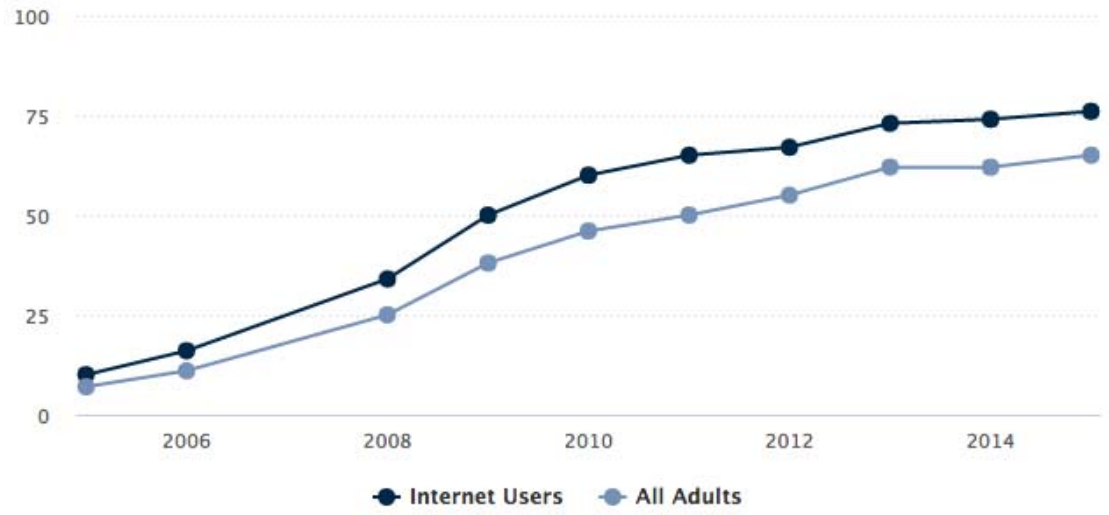


Εικόνα 6

Κεφάλαιο 3. Τα πιο γνωστά ΜΚΔ που χρησιμοποιούνται σήμερα

Το 2017, το Facebook είχε 1,94 δισεκατομμύρια μηνιαίους ενεργούς χρήστες και ήταν ο τρίτος ιστότοπος που επισκέπτεται περισσότερο το Διαδίκτυο(108: Zephoria2017). Το Twitter, από την άλλη, αξιώνει πάνω από 313 εκατομμύρια μηνιαίους ενεργούς χρήστες, οι οποίοι στέλνουν Tweets σε περισσότερες από 40 γλώσσες .

Στην ακόλουθη γραφική παράσταση (Εικόνα 7)αποτυπώνεται η μεταβολή των ενηλίκων Αμερικανών χρηστών τόσο του διαδικτύου όσο και των ΜΚΔ από το 2006 και μετά.

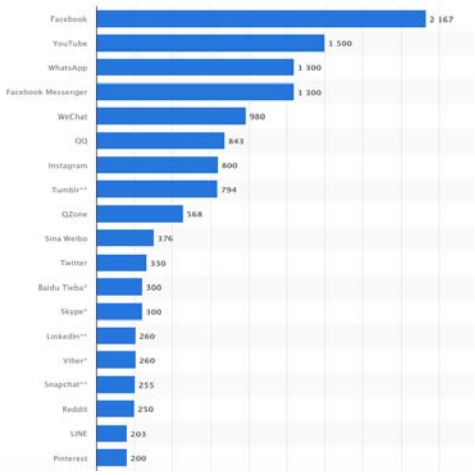


Εικόνα 7

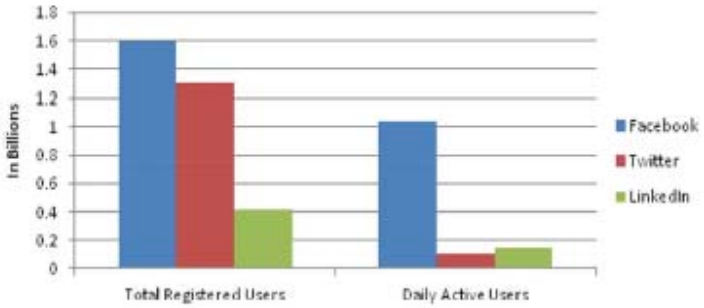
3.1 Facebook

Το Facebook είναι ένα κοινωνικό δίκτυο που λίγο πολύ κάνει λίγο από όλα. Είναι μια πλατφόρμα στην οποίο ο εκάστοτε χρήστης καλείτε να δημιουργήσει ένα διαδικτυακό προφίλ του εαυτού του εισάγοντας προσωπικά στοιχεία, και από αυτό μπορεί να διαμοιράζει πολυμέσα, κείμενο ή live video στους "φίλους" του, δηλαδή σε ανθρώπους στους οποίους έχει επιτρέψει να βλέπουν την δική του πληροφορία. Ο χρήστης έχει διαφόρους τρόπους με τους οποίους μπορεί να αλληλεπιδράσει με τους υπόλοιπους χρήστες. Μπορεί να το κάνει είτε μέσω προσωπικών μηνυμάτων (messaging),είτε μέσω σχολίων (comments) κάτω από τις κοινοποιήσεις ενός χρήστη (post), είτε αφήνοντας διάφορα διακριτικά, γνωστά και ως reactions κάτω από το εκάστοτε post του χρήστη. Επιπλέον το Facebook επιτρέπει την δημιουργία ομάδων μεταξύ χρηστών, όπως επίσης και την δημιουργία σελίδων επιχειρήσεων, οργανισμών, ατόμων κ.α. η οποίες μπορούν και ενημερώνουν τους χρήστες για τα τρέχοντα νέα ή να διαφημίσουν τα προϊόντα/υπηρεσίες τους. Το 2017 το Facebook ανακοίνωσε ότι θα εισάγει σύντομα τη δυνατότητα διακίνησης χρημάτων και πληρωμών μέσω της πλατφόρμας του, οπότε αναμένουμε περισσότερα. Το Facebook δικαίως μπορεί να χαρακτηριστεί ως ο βασιλιάς των κοινωνικών δικτύων με τους χρήστες του να είναι, σύμφωνα με αποτελέσματα έρευνας που έγιναν τον Ιανουάριο του 2017 να ανέρχονται σε 2.167 δισεκατομμύρια χρήστες, ενώ κατέχει το 18% του

μεριδίου της αγοράς (76: Nuha 2018: 351–356). Σύμφωνα με έρευνα που πραγματοποιήθηκε τον Νοέμβριο του 2016 από το Pew Research Center, το Facebook αποτελεί το πιο δημοφιλές κοινωνικό δίκτυο με τους περισσότερους χρήστες (Greenwood et al., 2016). Η ίδια έρευνα έδειξε ότι σχεδόν 8 στους 10 ενηλίκους (79%) που βρίσκονται συνδεδεμένοι στο διαδίκτυο, κάνουν χρήση του Facebook, με το μεγαλύτερο ποσοστό διείσδυσης να προέρχεται από μεγαλύτερους σε ηλικία ανθρώπους που αποφάσισαν να κάνουν λογαριασμό σε αυτό. Κοιτώντας με βάση το βιολογικό φύλο το 83% των Αμερικανών ανδρών κάνουν χρήση του σε σχέση με τις γυναίκες που το αντίστοιχο ποσοστό ανέρχεται στο 75% . Αξίζει να προσθέσουμε επίσης ότι και οι άλλες πλατφόρμες του Facebook, το Messenger που είναι για επικοινωνία μηνύματος και το Instagram (το οποίο εξαγοράστηκε από το Facebook) πάνε εξίσου καλά σε αριθμό χρηστών, με το Messenger να καταλαμβάνει την δεύτερη θέση (76: Nuha 2018: 351–356). Δεν φτάνει μόνο αυτό, το Facebook καταφέρνει να είναι το κοινωνικό δίκτυο το οποίο το 76% των χρηστών του το επισκέπτονται σε καθημερινή βάση αφήνοντας αρκετά πίσω όλα τα υπόλοιπα (76: Nuha 2018: 351–356). Έχοντας εκατομμύρια ανθρώπους εγγεγραμμένους και ενεργούς σε αυτό, το Facebook αποτελεί μια ξεχωριστή ευκαιρία για τις επιχειρήσεις να ενημερώσουν το κοινό τους για το brand τους, καθώς και να το αυξήσουν σε αριθμό και αν χτίσουν μια κοινότητα γύρω από αυτό.



Εικόνα 8



Εικόνα 9

3.2 Twitter

Το twitter είναι ένα κοινωνικό δίκτυο το οποίο ανήκει στην κατηγορία Microblogs. Μέσα από αυτό ο χρήστης μπορεί να κοινοποιήσει περιεχόμενο (εικόνα, κείμενο ή video) στους υπόλοιπους χρήστες του Twitter με τον μοναδικό περιορισμό, το κείμενό του να μην περιέχει περισσότερους από 140 χαρακτήρων. Εκμεταλλεύεται εκτενώς την χρήση των hashtags (λέξεις και χαρακτήρες ακολουθούμενοι από το σύμβολο # , λειτουργεί σαν αναγνωριστικό σε ορισμένα θέματα που σχολιάζουν οι χρήστες) προκειμένου να ενώσει όλους τους χρήστες που μιλάνε για το ίδιο θέμα εκείνη την στιγμή. Με την βοήθεια του, επιχειρήσεις μπορούν να επικοινωνούν και να ελέγχουν τα λεγόμενα των χρηστών όταν μιλάνε για αυτές. Αξίζει να προσθέσουμε επίσης ότι λόγο του όγκου της πληροφορίας τα tweets (έτσι ονομάζεται το περιεχόμενο που ανεβάζει ένας χρήστης σε αυτήν την πλατφόρμα) έχουν πολύ μικρή διάρκεια ζωής και μπορούν να χαθούν από την συνεχόμενη ροή άλλων εισερχόμενων tweet. Το Twitter απαριθμεί 330 εκατομμύρια χρήστες έως τον Ιανουάριο του 2018 (31: Epstein 2015). Σχεδόν το ένα τέταρτο των ενηλίκων, σύμφωνα με έρευνα του Pew Research Center, που χρησιμοποιούν το διαδίκτυο έχει λογαριασμό στο Twitter. Είναι ένα αρκετά δημοφιλές κοινωνικό δίκτυο σε άτομα νεότερη ηλικίας, ενώ παρατηρείτε ότι άτομα με υψηλότερο μορφωτικό επίπεδο έχουν μεγαλύτερη πιθανότητα να έχουν λογαριασμό σε αυτό (Greenwood et al., 2016).

3.3 Instagram

Το Instagram είναι ένα κοινωνικό δίκτυο στο οποίο οι χρήστες μοιράζονται πολυμέσα μεταξύ τους, και συγκεκριμένα βίντεο και εικόνες, ενώ το ίδιο, όπως και το Twitter κάνει εκτενή χρήση των hashtags προκείμενου να συγκεντρώσει τους χρήστες κάτω από μια κοινή θεματολογία. Επιτρέπει επίσης στους χρήστες να σχολιάσουν ή να αντιδράσουν (πιέζοντας την καρδούλα που υπάρχει, δηλώνοντας έτσι ότι τους αρέσει το συγκεκριμένο πολυμέσο) κάτω από ένα πολυμέσο, όπως και επίσης να αναζητήσουν πολυμέσα που τους αρέσουν. Το Instagram απαριθμεί 800 εκατομμύρια χρήστες έως τον Ιανουάριο του 2018 (114: Κουτσογιαννοπούλου 2013) κατατάσσοντάς το σε ένα από τα μεγαλύτερα κοινωνικά δίκτυα. Σχεδόν 1 στους 3 ενηλίκους (32%) που βρίσκονται συνδεδεμένοι στο διαδίκτυο, είναι εγγεγραμμένοι στο κοινωνικό δίκτυο του Instagram. Αξίζει αν σημειωθεί ότι το Instagram είναι αρκετά δημοφιλές σε νεότερες ηλικίες όπου παρατηρείτε ότι 6 στα 10 άτομα ηλικίας 18 έως 29 έχουν λογαριασμό σε αυτό. Επιπροσθέτως οι γυναίκες είναι περισσότερο πιθανό να έχουν λογαριασμό σε αυτό σε σχέση με τους άντρες. Το 38% των γυναικών που είναι συνδεδεμένες στο διαδίκτυο έχουν λογαριασμό στο Instagram σε αντίθεση με τους άντρες όπου το αντίστοιχο ποσοστό ανέρχεται στο 26%.

3.4 Youtube

Το Youtube είναι μια διαδικτυακή πλατφόρμα στην οποία οι χρήστες μπορούν να ανεβάζουν βίντεο. Κάθε χρήστης έχει την δυνατότητα όταν το επιθυμεί να δημιουργήσει τον δικό του χώρο που θα ανεβάζει τα βίντεο του το οποίο ονομάζεται κανάλι. Τα κανάλια μπορούν να ανήκουν είτε σε φυσικά πρόσωπα, είτε σε επιχειρήσεις οι οποίες προσπαθούν να διαφημίζουν τα προϊόντα τους μέσα από αυτά, δημιουργώντας ενίοτε διαδικτυακές εκπομπές για να ενισχύσουν το αίσθημα της κοινότητας και να προσελκύσουν περισσότερο κόσμο. Κάθε χρήστης πέρα της δυνατότητα να ανεβάζει κάποιο βίντεο, μπορεί να το σχολιάσει ή να επισημάνει αν αυτό του αρέσει ή όχι (αυτό γίνεται με την βοήθεια των like και unlike κουμπιών που έχει σαν επιλογές). Αξίζει να σημειώσουμε ότι οι χρήστες του μπορούν να το χρησιμοποιήσουν χωρίς να έχει κάνει κάποιου είδους έγγραφή σε αυτό. Σύμφωνα με το ίδιο το Youtube, οι χρήστες του ανέρχονται σε πάνω από 1.5 δισεκατομμύρια, το οποίο είναι σχεδόν το ένα τρίτο των ατόμων που βρίσκονται στο διαδίκτυο (76: Nuha 2018: 351–356).

3.5 Linked in

Το Linked in είναι ένα κοινωνικό δίκτυο το οποίο χρησιμοποιείτε και έχει δημιουργηθεί για επαγγελματικούς σκοπούς και είναι αρκετά δημοφιλές μεταξύ των απόφοιτων πανεπιστημίων και άτομα που έχουν υψηλό εισόδημα (Greenwood et al., 2016). Κάθε χρήστης που είναι εγγεγραμμένος σε αυτό έχει την δική του σελίδα προφίλ ή οποία δεν είναι κάτι άλλο από την ψηφιακή μορφή του βιογραφικό του. Αυτό βοηθάει τις εταιρίες ώστε να εντοπίζουν τα κατάλληλα άτομα για να στελεχώσουν τις επιχειρήσεις του, ενώ ταυτόχρονα το ίδιο το άτομο μπορεί να αναζητήσει ανοιχτές θέσεις εργασία στο πεδίο που επιθυμεί να εργαστεί. Επίσης, δίνεται η δυνατότητα στις επιχειρήσεις και στους χρήστες να αναρτούν νέα σχετικά με αυτούς, και να τα μοιράζονται με ακόλουθους ή τους φίλους τους αντίστοιχα. Η σελίδες των επιχειρήσεων στο Linked in είναι ένας χώρος στον οποίον οι εταιρίες μπορούν να μοιράζονται πληροφορίες σχετικά με αυτές, τα προϊόντα τους ή τις υπηρεσίες τους, τις ευκαιρίες εργασίας που προσφέρουν, καθώς και να τις γνώσεις τους σαν ειδικοί σχετικά με ένα αντικείμενο το οποίο γνωρίζουν. Το Linked in απαριθμεί 260 εκατομμύρια χρήστες έως τον Ιανουάριο του 2018 (31: Greenwood et al., 2018) και το χρησιμοποιεί το 29% των ατόμων που κάνουν χρήση του διαδικτύου (Greenwood et al., 2018). Το 50% των ατόμων που έχουν τελειώσει το πανεπιστήμιο έχουν λογαριασμό στο Linked in, σε αντίθεση με το 12% των ατόμων που έχουν τουλάχιστον απολυτήριο λυκείου (Greenwood et al., 2018).

3.6 Snapchat

Το Snapchat είναι ένα κοινωνικό δίκτυο σαν το Instagram, στο οποίο διαμοιράζεις δημόσια είτε με φίλους πολυμέσα (εικόνες και βίντεο). Η ιδιαιτερότητα του βρίσκεται στο γεγονός ότι οι αναρτήσεις σου παραμένουν σε αυτό ελάχιστα δευτερόλεπτα και μπορεί να τις δει μια μόνο φορά ένας χρήστης, εκτός και αν αποτελεί μέρος της "ιστορίας της ημέρας" σου όπου κάποιος μπορεί να δει αυτήν την ανάρτηση όσες φορές θέλει μέσα σε ένα εικοσιτετράωρο. Επίσης προσφέρεται και η δυνατότητα ανταλλαγής μηνυμάτων μεταξύ των χρηστών. Αξίζει να προσθέσουμε ότι σε σχέση με τα υπόλοιπα κοινωνικά δίκτυα που διερευνάμε το Snapchat δεν είναι διαθέσιμο σε σταθερούς ή φορητούς υπολογιστές, παρά μόνο σε κινητά και σε tablet. Στο Snapchat είναι το μοναδικό κοινωνικό δίκτυο το οποίο είχε τεράστια απότομη αύξηση στον αριθμό χρηστών από την ημερομηνία έναρξης του. Συγκεκριμένα το 2012 απαριθμούσε κοντά στα 10 εκατομμύρια χρήστες (Piwek & Joinson, 2016). Το 2015 ο αριθμός τους είχε φτάσει τα 100 εκατομμύρια (Piwek & Joinson, 2016), ενώ τον Ιανουάριο του 2018 το Snapchat απαριθμεί 255 εκατομμύρια χρήστες (31). Ένα ποσοστό 24% των χρηστών κάνουν χρήση εφαρμογών επικοινωνίας τα οποία διαγράφουν αυτόματα τα μηνύματα αφού τα στείλουν, μέσα και σε αυτή περιέχεται και το Snapchat.

3.7 Μετάβασή από το Web 1.0 στο Web 2.0 και ο δρόμος προς το Web 4.0

Η τεράστια εξέλιξη των ΜΚΔ αλλά και γενικότερα του διαδικτύου παγκοσμίως οφείλεται ως ένα μεγάλο βαθμό στην εξέλιξη του παγκόσμιου ιστού. Αυτή η τεράστια αλλαγή στην υφή, στην δομή και στην ανάπτυξη του Παγκόσμιου Ιστού (Web) απογείωσε τη χρήση των ΜΚΔ.

Στα μέσα της δεκαετίας του ΄90 η δημοτικότητα του Παγκόσμιου Ιστού (Web 1.0) εκτοξεύτηκε στα ύψη ανοίγοντας νέους διαύλους διαμοιρασμού πληροφοριών μεταξύ των ανθρώπων παγκοσμίως. Παρά το γεγονός ότι επρόκειτο για κάτι αναμφίβολα πρωτοπόρο κάτι έμοιαζε να απουσιάζει. Το Web 1.0 επέτρεπε μία μονόδρομη επικοινωνία μέσω στατικών ιστοσελίδων (99: Thackeray 2009: 338–343) και παρουσίαζε παντελή έλλειψη διαδραστικότητας και άμεσης επικοινωνίας μεταξύ των χρηστών. Ήταν μοιραίο λοιπόν κάποια χρόνια αργότερα να αντικατασταθεί.

Ο όρος web 2.0 ορίστηκε επίσημα το 2004 από τον Dale Dougherty, αντιπρόεδρο του O'Reilly Media, σε μια συνάντηση brainstorming συνεδρίων μεταξύ του O'Reilly και του MediaLive International . Ο Tim O'Reilly ορίζει το web 2.0 στον ιστότοπο του ως εξής: "Το Web 2.0 είναι η επιχειρηματική επανάσταση στη βιομηχανία υπολογιστών που

προκαλείται από τη μετάβαση στο διαδίκτυο ως πλατφόρμα και μια προσπάθεια κατανόησης των κανόνων επιτυχίας σε αυτή τη νέα πλατφόρμα. Στην κορυφή αυτών είναι τα εξής: Δημιουργήστε εφαρμογές που αξιοποιούν τα εφέ του δικτύου για να βελτιώσετε τη λειτουργία τους και να χρησιμοποιηθούν από περισσότερους ανθρώπους.

Το ακριβές νόημα του όρου γίνεται αντιληπτό από τον ορισμό που δίνεται στον ελληνικό ιστότοπο της Wikipedia «το Web 2.0 (**Ιστός 2.0**), και χρησιμοποιείται για να περιγράψει τη νέα γενιά του Παγκόσμιου Ιστού η οποία βασίζεται στην όλο και μεγαλύτερη δυνατότητα των χρηστών του Διαδικτύου να μοιράζονται πληροφορίες και να συνεργάζονται online. Αυτή η νέα γενιά είναι μια δυναμική διαδικτυακή πλατφόρμα στην οποία μπορούν να αλληλεπιδρούν χρήστες χωρίς εξειδικευμένες γνώσεις σε θέματα υπολογιστών και δικτύων.»

Τα βασικά χαρακτηριστικά του Web 2.0 είναι (68: Miller 2005):

- ελευθερία των δεδομένων
- συμμετοχή
- επικοινωνία
- ανάμειξη
- κτίσιμο εμπιστοσύνης
- διευκόλυνση της κοινωνίας

Οι βασικές διαφορές Web 1.0 και Web 2. 0 απεικονίζονται στον παρακάτω πίνακα (Εικόνα 10) (3: Al-Qurishi 2018: 743-753) .

Web 1.0	Web 2.0
Reading	Reading/Writing
Companies	Communities
Client-Server	Peer to Peer
HTML, Portals	XML, RSS
Taxonomy	Tags
Owning	Sharing
IPOs	Trade sales
Netscape	Google
Web forms	Web applications
Screen scraping	APIs
Dialup	Broadband
Hardware costs	Bandwidth costs
Lectures	Conversation
Advertising	Word of mouth
Services sold over the web	Web services
Information portals	Platforms

Εικόνα 10

Ο John Markoff των New York Times πρότεινε το web 3.0 ως τρίτη γενιά του ιστού το 2006 (93: Spivack 2019). Η βασική ιδέα του web 3.0 είναι να ορίσει δομή δεδομένων και να τα συνδέσει ώστε να γίνει πιο αποτελεσματική η ανακάλυψη, η αυτοματοποίηση, η ενσωμάτωση και η επαναχρησιμοποίηση σε διάφορες εφαρμογές. Το Web 3.0 προσπαθεί

να συνδέσει, να ενσωματώσει και να αναλύσει δεδομένα από διάφορα σύνολα δεδομένων για να αποκτήσει νέα ροή πληροφοριών. Είναι σε θέση να βελτιώσει τη διαχείριση δεδομένων, τη στήριξη της προσβασιμότητας κινητών μέσων, την προσομοίωση της δημιουργικότητας και την καινοτομία, την ενθάρρυνση των παραγόντων της παγκοσμιοποίησης, τη βελτίωση της ικανοποίησης των πελατών και να βοηθήσει να επιτευχθεί καλύτερη συνεργασία στον κοινωνικό ιστό. Το Web 3.0 είναι επίσης γνωστό ως σημασιολογικός ιστός. Ο σημασιολογικός ιστός δημιουργήθηκε από τον Tim Berners-Lee,εφευρέτης του Παγκόσμιου Ιστού.

Το Web 4.0 εξακολουθεί να είναι μια ιδέα σε εξέλιξη και δεν υπάρχει ακριβής ορισμός του πώς θα είναι. Το Web 4.0 είναι επίσης γνωστό ως συμβιωτικός ιστός. Το όνειρο πίσω από το συμβιωτικό ιστό είναι η αλληλεπίδραση μεταξύ ανθρώπων και μηχανών σε συμβίωση. Θα είναι δυνατή η κατασκευή περισσότερων και ισχυρότερων διεπαφών όπως οι ελεγχόμενες από το μυαλό διεπαφές, χρησιμοποιώντας το web 4.0. Με απλά λόγια, οι μηχανές θα είναι έξυπνες κατά την ανάγνωση των περιεχομένων του ιστού, και θα αντιδρούσαν με τη μορφή εκτέλεσης αποφασίζοντας τι να εκτελέσει πρώτα για να φορτώσει γρήγορα τις ιστοσελίδες με ανώτερη ποιότητα και απόδοση ώστε να οικοδομηθούν διεπαφές εντολών (2: Aghaei 2012).

3.8 Κατηγοριοποίηση των ΜΚΔ

Μια πιο περιεκτική κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης καταγράφεται στο άρθρο “Social Media and Distance Education”, (109: Zhang 2010) σύμφωνα με τον οποίο τα Social Media διακρίνονται στις παρακάτω βασικές κατηγορίες :

1. Κοινωνικά δίκτυα ή σελίδες κοινωνικής δικτύωσης (social networks) :Facebook

2. Μέσα κοινωνικής σελιδοσήμανσης (social bookmarking) : Digg, delicious

3. Ιστοσελίδες συνεργατικής συγγραφής (collaborative authoring) :Wikipedia, Google Docs.

4. Ιστοσελίδες ανταλλαγής πολυμέσων (multimedia sharing): YouTube, Instagram, Flickr

5. Ιστολόγια (blogs- micro blogging): Blogger, Word Press, Twitter

6. Διαδικτυακές τηλεδιασκέψεις (Web conferencing):WebEx, GoToMeeting, DimDim.

Ίσως περισσότερο από όλους τους άλλους τύπους ηλεκτρονικών εφαρμογών, τα Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ) έχουν αποκτήσει σημαντικό ρόλο στην πραγματική ζωή: οι εταιρείες προωθούν τις νέες τάσεις τους στο Facebook και το Twitter δημιουργώντας likes και shares , οι εργοδότες ελέγχουν τα προφίλ των υποψηφίων για εργασία σε

Facebook, LinkedIn και Twitter (81: Protalinski 2012), οι αστυνομικές και δικαστικές αρχές συλλέγουν στοιχεία από τα ΜΚΔ για την επίλυση εγκληματικών υποθέσεων και άλλων σοβαρών αδικημάτων (42: Heather 2012). Ταυτόχρονα οι δραστηριότητες σε διαδικτυακές κοινωνικές πλατφόρμες αλλάζουν τα πολιτικά καθεστώτα (37: Gilad 2011:1375-1405) και αλλοιώνουν τα αποτελέσματα των εκλογών (80: Prashant 2013).

Το Facebook είναι αυτό, που παρουσιάζει ιδιαίτερο ενδιαφέρον για τους μελετητές της επικοινωνίας, διότι ενσωματώνει μια ποικιλία επιστημονικών ευρημάτων σχετικών με την κοινωνική ωφελιμότητα των νέων τεχνολογιών και κυρίως των ψηφιακών και διαδικτυακών εφαρμογών (88: Rosen 2014) .

3.9 Υπηρεσίες που παρέχουν τα ΜΚΔ

Οι εν λόγω ιστότοποι δίνουν τη δυνατότητα στους ανθρώπους να φτιάξουν τις δικές τους ιστοσελίδες και μετά να συνδέονται με φίλους, να μοιράζονται περιεχόμενο και να επικοινωνούν. Οι πιο γνωστές υπηρεσίες που παρέχουν τα ΜΚΔ είναι:

Blogs

Ενδεχομένως από τα πιο γνωστά μέσα κοινωνικής δικτύωσης, τα blogs (ή ιστολόγια) είναι διαδικτυακά «έντυπα» ημερολογιακού χαρακτήρα, όπου προβάλλονται τα πιο πρόσφατα κείμενα.

Wikis

Πρόκειται για ιστότοπους που αντιμετωπίζονται ως κοινόχρηστα έγγραφα ή βάσεις δεδομένων: επιτρέπουν την προσθήκη περιεχομένου ή την επεξεργασία των ήδη υπαρχουσών πληροφοριών. Ο πιο γνωστός ιστότοπος είναι η διαδικτυακή εγκυκλοπαίδεια Wikipedia, με περισσότερα από 2 εκατομμύρια κείμενα.

Podcasts

Αρχεία ήχου και εικόνας που είναι διαθέσιμοι διάμεσου συνδρομής σε εταιρείες, όπως είναι η Apple με το iTunes.

Fora

Είναι χώροι για διαδικτυακή συζήτηση, συχνά γύρω από συγκεκριμένα θέματα και ενδιαφέροντα. Τα φόρουμ έχουν ενταχθεί στην κατηγορία των μέσων κοινωνικής

δικτύωσης και αποτελούν ένα ισχυρό και δημοφιλές στοιχείο των διαδικτυακών κοινοτήτων.

Κοινότητες περιεχομένου

Είναι οι κοινότητες οι οποίες οργανώνουν και μοιράζονται συγκεκριμένα είδη περιεχομένου. Οι πιο δημοφιλείς ως τάση είναι αυτές που περιέχουν φωτογραφίες (Flickr), συνδέσμους (del.icio.us) και βίντεο(YouTube).

Microblogging

Η κοινωνική δικτύωση που συνδυάζει πολύ μικρού μεγέθους blogs, τα οποία ανανεώνονται όποτε θέλει ο ενδιαφερόμενος χρήστης, και διανέμεται διαμέσου του διαδικτύου ή του κινητού τηλεφώνου. Το Twitter είναι το σημείο αναφοράς-ηγέτης σε αυτή την κατηγορία.

Τα κοινωνικά δίκτυα είναι τα κανάλια μέσα από τα οποία τα άτομα μπορούν να αλληλεπιδράσουν μεταξύ τους. Τα εν λόγω δίκτυα επιτρέπουν στα άτομα να δομήσουν μια σειρά από δράσεις: 1) να διαμορφώσουν ένα δημόσιο ή ημι-δημόσιο προφίλ μέσα σε ένα οριοθετημένο σύστημα, 2) να διαρθρώσουν μια λίστα άλλων χρηστών με τους οποίους μοιράζονται μια σύνδεση, και 3) να δουν και να διασταυρώσουν τη λίστα των συνδέσεών τους με αυτήν που έχουν δημιουργήσει άλλοι μέσα στο σύστημα (19: Boyd 2007: 210-230).

Κεφάλαιο 4. 0

Πλεονεκτήματα και μειονεκτήματα της χρήσης ΜΚΔ

Τα ΜΚΔ δείχνουν την offline ζωή των χρηστών, online. Είναι μια εξαίρεση της επικοινωνίας δια στόματος. Τα social media είναι μια online πλατφόρμα όπου οι άνθρωποι χρησιμοποιούν για να χτίσουν κοινωνικά δίκτυα ή κοινωνικές σχέσεις με άλλους ανθρώπους με τους οποίους μοιράζονται παρόμοια προσωπικά ή επαγγελματικά ενδιαφέροντα, δραστηριότητες, υπόβαθρο ή συνδέσεις πραγματικότητας. Σε πολλές

περιπτώσεις όπου οι πληροφορίες διακινούνται ανώνυμα στα κοινωνικά δίκτυα για λόγους ασφαλείας, υπόκεινται σε αλλοίωση από χρήστη σε χρήστη. Οι τεχνικές ανωνυμοποίησης είναι καλές στον εντοπισμό και την εξάλειψη του κινδύνου αποκάλυψης τους, όμως δεν προστατεύουν τα ίδια τα δεδομένα(73: Nettleton 2016:87-105).

Σύμφωνα με τον Hamza Khan (53a: Khan2012) διακρίνονται τα παρακάτω οφέλη από την χρήση των μέσων κοινωνικής δικτύωσης:

 Επιτρέπουν την άμεση αλληλεπίδραση μεταξύ των χρηστών.

 Επιτρέπουν την αστραπιαία μετάδοση των γεγονότων.

 Συμβάλλουν στην διάχυση της γνώσης.

 Καλύπτουν την βασικά ανάγκη των ανθρώπων να μοιραστούν πράγματα, σκέψεις και απόψεις.

 Παρέχουν την δυνατότητα δημιουργίας δεσμών με πολύ μεγάλο αριθμό ατόμων παγκοσμίως, από διαφορετικές χώρες, κοινωνίες, πολιτισμούς και με διαφορετικές συνήθειες και χαρακτηριστικά.

 Παρέχουν την δυνατότητα αναζήτησης και ανεύρεσης περιεχομένου (φωτογραφιών, βίντεο κλπ) στο οποίο οι χρήστες δε θα μπορούσαν να έχουν πρόσβαση με διαφορετικό τρόπο (π.χ. από έντυπα μέσα).

 Παρέχουν την δυνατότητα άμεσης ενημέρωσης για οτιδήποτε συμβαίνει στον κόσμο την ίδια στιγμή.

 Παρέχουν την δυνατότητα εύκολης πρόσβασης σε ψυχαγωγικό περιεχόμενο, από το σπίτι,.

 Διευκολύνουν την ανοικτή επικοινωνία, που οδηγεί σε αυξημένη ανακάλυψη πληροφοριών.

 Επιτρέπουν στους εργαζόμενους να συζητήσουν τις ιδέες, να ποστάρουν νέα, να κάνουν ερωτήσεις και να μοιραστούν links συνδέσεις.

 Παρέχουν την ευκαιρία να διευρυνθούν οι επιχειρηματικές επαφές.

 Στοχεύουν σε ένα ευρύ κοινό, καθιστώντας το ένα χρήσιμο και αποτελεσματικό εργαλείο για τις προσλήψεις.

 Βελτιώνουν την επιχειρηματική φήμη και πελατεία με ελάχιστη χρήση της διαφήμισης.

 Επεκτείνουν την έρευνα της αγοράς, υλοποιεί εκστρατείες μάρκετινγκ, παρέχει επικοινωνίες και κατευθύνει τα ενδιαφερόμενα άτομα σε συγκεκριμένες ιστοσελίδες.

Στον αντίποδα υπάρχουν ερευνητές όπως οι Weir (103: Weir 2011:38-43) που υποστηρίζουν πως τα νέα μέσα κοινωνικής δικτύωσης αποτελούν «παλιό κρασί σε καινούρια μπουκάλια» αφού τα μειονεκτήματα και οι κίνδυνοι που υπήρχαν στα

παραδοσιακά μέσα και στις προσωπικές σχέσεις των ανθρώπων εξακολουθούν να υπάρχουν ίσως και να πληθαίνουν.
Τα μειονεκτήματα και οι κίνδυνοι που προκύπτουν είναι:
 Η υπερβολική χρήση οδηγεί σε εθισμό.

 Η επιβλαβής έκθεση της προσωπικής ζωής των χρηστών.

 Κλοπή προσωπικών δεδομένων.

 Καταπάτηση της ιδιωτικότητας.

 Απαλοιφή διαπροσωπικών σχέσεων δια ζώσης.

 Σπατάλη χρόνου.

 Trolling. Αναφέρεται στην κακή χρήση των μέσων κοινωνικής δικτύωσης για συναισθηματική κακοποίηση που επιτυγχάνεται για παράδειγμα με δυσμενή σχόλια για να προκαλέσουν τον θυμό ή την λύπη κάποιου.

 Cyber- Bullying. Αναφέρεται στον διαδικτυακό εκφοβισμό των χρηστών που μπορεί να οδηγήσει σε συναισθηματικό τραυματισμό. Σύμφωνα με έρευνα (complete Social Media guide) το 39% των χρηστών των μέσων κοινωνικής δικτύωσης αναφέρει πως έχει πέσει θύμα εκφοβισμού.

 Βομβαρδισμός πληροφοριών διαφημιστικών μηνυμάτων.

 Μετάδοση επιλεγμένων πληροφοριών με σκοπό την χειραγώγηση της κοινής γνώμης.

 Η χρήση των νέων μέσων κοινωνικής δικτύωσης δίνει τη δυνατότητα στους hackers για να διαπράξουν απάτη και να ξεκινήσουν επιθέσεις ιών.

 Τα ΜΚΔ αυξάνουν τον κίνδυνο των ατόμων που πέφτουν θύματα ηλεκτρονικών απατών που φαίνονται γνήσιες, με αποτέλεσμα την κλοπή προσωπικών δεδομένων.

 Σε επιχειρησιακό επίπεδο, μπορεί να οδηγήσουν σε αρνητικά σχόλια τους υπαλλήλους μιας επιχείρησης σχετικά με την εταιρεία ή να επιφέρουν νομικές συνέπειες, αν οι εργαζόμενοι χρησιμοποιούν αυτές τις ιστοσελίδες για να προβάλλουν παράνομο ή προσβλητικό υλικό.

 Η χρήση των ΜΚΔ καλλιεργεί τον εγωισμό και τον ναρκισσισμό. Τα κοινωνικά δίκτυα βομβαρδίζουν τους χρήστες οδηγώντας τους σε υπερκατανάλωση άχρηστων πληροφοριών καλλιεργώντας έτσι ένα υπερτροφικό Εγώ.

4.1 ΜΚΔ και ενημέρωση

Οι σύγχρονες ανησυχίες, ότι το Διαδίκτυο μπορεί να οδηγήσει σε πολιτική απάθεια,

βασίζονται σε προτάσεις ότι οι άνθρωποι θα χρησιμοποιούν το Διαδίκτυο για λόγους ψυχαγωγίας αντί για κατανάλωση ειδήσεων. Ωστόσο, τι γίνεται αν κάποιος σκοντάψει στις ειδήσεις κατά την πλοήγηση στο Διαδίκτυο; Αυτή η περιστασιακή έκθεση σε ειδήσεις μέσω του διαδικτύου είναι χρήσιμη για την προώθηση της πολιτικής δέσμευσης των πολιτών. Το σημαντικότερο είναι ότι ο ρόλος της ενημέρωσης μέσω ΜΚΔ συμβάλλει στη διευκόλυνση της ηλεκτρονικής πολιτικής συμμετοχής των πολιτών , γεγονός που υποδηλώνει ότι η περιστασιακή έκθεση ειδήσεων μπορεί να αυξήσει τα υπάρχοντα κενά στην πολιτική συμμετοχή μεταξύ των ανθρώπων που προτιμούν ειδήσεις και των ανθρώπων που προτιμούν την online ψυχαγωγία (107: Yonghwan 2013:2607-2614). Έτσι λοιπόν, με την πάροδο των χρόνων τα ΜΚΔ έχουν ενσωματώσει λειτουργίες newsfeed μέσα από τις οποίες παρέχουν μια συνολική ενημέρωση ακολουθώντας μια χρονική ακολουθία μιμούμενοι τα παραδοσιακά μέσα μαζικής ενημέρωσης. Η προσθήκη αυτή διευκόλυνε τους χρήστες να έχουν άμεση πρόσβαση στο τι συμβαίνει γύρω τους επαναπροσδιορίζοντας τον ρόλο της ενημέρωσης σε πραγματικό χρόνο. Οι χρήστες – πολίτες έχουν την δυνατότητα να μοιράζονται πληροφορίες με οποιοδήποτε αριθμό συνομηλίκων δικτυακά μέσω των ΜΚΔ (32: Eytan 2012: 519-528). Τώρα πια οι χρήστες των ΜΚΔ δεν ανταλλάσουν μόνο φωτογραφίες, μηνύματα και οτιδήποτε ξέραμε ως σήμερα αλλά και ειδήσεις , ανησυχίες, πολιτικές εξελίξεις κ.α. . Η ενημέρωση των χρηστών μέσα από τα ΜΚΔ έχει αυξηθεί τόσο πολύ ώστε να θεωρείται ότι οι νέοι σε ηλικίες 18 – 30 ενημερώνονται πολύ περισσότερο από τα newsfeed του Facebook ή του Twitter παρά από τους New York Times (67: Messing 2012). Καθώς όμως όλο και περισσότεροι επιλέγουν ενημέρωση μέσω των ΜΚΔ υπάρχουν έντονες ανησυχίες για το κατά πόσο οι ειδήσεις που τροφοδοτούν καθημερινά τα ΜΚΔ συμβαδίζουν με τα παραδοσιακά μέσα μαζικής ενημέρωσης. Έρευνα σχετικά με ειδήσεις που έχουν διαμοιραστεί περισσότερο μέσω emails στην σελίδα των New York Times έδειξε ότι η είδηση δεν ήταν κατ' ανάγκη το πρωτοσέλιδο της εφημερίδας αλλά ιστορίες που αφορούν κάποιο συναισθηματικό αντικείμενο ή κάποια χρήσιμα στοιχεία(13: Berger 2012: 192-205). Έτσι, εξαιτίας της συνεχόμενης ροής ειδήσεων μέσω των ΜΚΔ η οποία γίνεται σε πραγματικό χρόνο, οι χρήστες ενδιαφέρονται περισσότερο για γεγονότα που εξελίσσονται άμεσα από ειδήσεις που απαιτούν συνεχή παρακολούθηση της επικαιρότητας. Μια έκθεση από το Ινστιτούτο του Reuters αναφορικά με τη μελέτη της δημοσιογραφίας δείχνει ότι οι ειδήσεις που διαμοιράζονται πιο συχνά στο Twitter ήταν ή ιδιαιτέρως συγκλονιστικές, αναφερόμενες σε καταστροφές ή θανάτους, είτε αστείες ή έστω περίεργες (74: Newman 2011).

Πολλές φορές μια διαστρέβλωση της πραγματικότητας στα ΜΚΔ μπορεί να επιφέρει μεγάλη ζημία τόσο σε οικονομικό όσο και κοινωνικό επίπεδο. Για παράδειγμα τον Απρίλιο του 2013 ο δείκτης Standard &Poor' s υποχώρησε 0,9%, το οποίο μεταφράζεται σε απώλεια των μετοχών της τάξης των 130 δις. $ λόγω ενός ψευδούς tweet από το λογαριασμό του Associated Press Twitter για το οποίο ενημέρωνε τα εκατομμύρια των

ακολούθων ότι ο Πρόεδρος της Αμερικής είχε τραυματιστεί σε έκρηξη στο Λευκό οίκο. Παρά το γεγονός ότι η είδηση διαψεύστηκε άμεσα το κακό είχε ήδη γίνει (bogus terror tweet sparks shares blip. Financial times) (18: Bradshaw 2013). Τέτοιου είδους ειδήσεις είχαν προβλεφθεί πολύ νωρίτερα καθώς ερευνητές θεωρούσαν ότι μελλοντικά το διαδίκτυο δεν θα χρησιμοποιείται μόνο για ενημέρωση αλλά και για διασπορά ψευδών ειδήσεων (9: Ayres 1999:132-143).

4.2 ΜΚΔ και ψυχική υγεία

Τον κώδωνα του κινδύνου κρούουν οι ειδικοί για τις επιπτώσεις των social media στην ψυχική μας υγεία καθώς, τα πορίσματά της έρευνάς τους έδειξαν ότι, όσοι σερφάρουν επί ώρες στα ΜΚΔ, κινδυνεύουν από μοναξιά και κατάθλιψη. Σύμφωνα με έρευνα του Πανεπιστημίου της Πενσιλβάνια που διεξήχθη σε δείγμα 143 ατόμων, ηλικίας 18-22 ετών, ο χρόνος που πρέπει να αφιερώνουμε στα social media για να κρατάμε σε ισορροπία την πνευματική μας υγεία, πρέπει να είναι μετρημένος: μόλις μισή ώρα. Οι ειδικοί για πρώτη φορά αποδεικνύουν επιστημονικά ότι, όσο περισσότερο χρόνο αφιερώνουμε στο Facebook και το Instagram, τόσο περισσότερο κινδυνεύουμε να εμφανίσουμε αρνητικά συναισθήματα. Στην έρευνά τους, οι Αμερικανοί επιστήμονες έλαβαν υπόψη το αίσθημα του φόβου, του άγχους, της κατάθλιψης και της μοναξιάς. Διαπίστωσαν πως, όσο περισσότερο ασχολείται κανείς με τα social media, τόσο πιο πολύ αισθάνεται φόβο, μοναξιά και άγχος. Αυτές οι επιδράσεις ήταν ιδιαίτερα έντονες για τους ανθρώπους που είχαν καταθλιπτικές τάσεις. «Τα ευρήματά μας υποδηλώνουν ότι, ο περιορισμός της χρήσης των social media σε περίπου 30 λεπτά την ημέρα, μπορεί να οδηγήσει σε σημαντική βελτίωση της ψυχικής υγείας», επισημαίνουν οι ερευνητές. «Ελάχιστες μελέτες έχουν επιχειρήσει να αποδείξουν ότι η χρήση των μέσων κοινωνικής δικτύωσης βλάπτει την ψυχική υγεία των χρηστών» ,υποστήριξε η επικεφαλής της μελέτης, ερευνήτρια του Πανεπιστημίου της Πενσιλβάνια, Μελίσα Χαντ. Η έρευνα των Αμερικανών επιστημόνων δημοσιεύτηκε στην επιθεώρηση «Journal of Social and Clinical Psychology» (113: Αγγελίνη 2018).

Επειδή οι χρήστες των ΜΚΔ συνδέονται συνήθως με φίλους, οικογένειες και γνωστούς, μια κοινή αντίληψη είναι ότι αυτά παρέχουν ασφαλέστερο ιδιωτικό περιβάλλον στο Διαδίκτυο για διαδικτυακή επικοινωνία (24: Cutillo 2009: 94–101).

Στην πραγματικότητα, ωστόσο, τα ΜΚΔ έχουν αυξήσει το ρίσκο της προστασίας της ιδιωτικής ζωής εξαιτίας της διαθεσιμότητας του τεράστιου όγκου προσωπικών δεδομένων

των χριστών που δεν θα είχαν εκτεθεί μέχρι τώρα. Το πιο σημαντικό όμως είναι ότι τα ΜΚΔ εκθέτουν τώρα πληροφορίες από πολλές κοινωνικές οντότητες - για παράδειγμα, προσωπικές πληροφορίες με τη χρήση του Facebook και επαγγελματική δραστηριότητα στο LinkedIn - οι οποίες, συγκεντρωτικά, οδηγούν σε δυσάρεστα αποτελέσματα λόγω της υπερ - έκθεσης πληροφοριών (75: Nissenbaum 2011: 32-48).

Σχετικά με τις κοινωνικές προεκτάσεις που αφορά το ζήτημα της ασφάλειας στα μέσα κοινωνικής δικτύωσης σε μια η μελέτη με τίτλο «Ιδιωτικότητα εναντίων ασφάλειας στο διαδίκτυο» γίνεται λόγος για τους αυστηρότερους κανόνες που έχουν θεσπιστεί και αφορούν τα προσωπικά δεδομένα(στην Ευρώπη είναι η θέσπιση του GDPR). Θα πρέπει λοιπόν να επιλέξουμε ανάμεσα στην οικειότητα και την ασφάλεια. Υπάρχει βέβαια η πιθανότητα να μην υποστηρίξουμε την ιδιωτικότητα. Ο Harry Lewis (Harvard University) πιστεύει ότι αυτό θα είναι η απώλεια της κοινωνίας θεωρώντας ότι όσο περισσότερο εκτιθέμεθα από πολύ μικρή ηλικία τόσο περισσότερο πιέζουμε τους εαυτούς μας ή πιεζόμαστε από τους γονείς μας στην «κοινωνική συμμόρφωση». Ο Jonathan Shaw (Harvard University) πιστεύει ότι με την απώλεια της ιδιωτικότητας απειλείται το πνεύμα της ανθρώπινης προόδου μέσω του κοινωνικού πειραματισμού. Άρα λοιπόν, συνεχίζει η μελέτη, η οικειότητα και η ασφάλεια πρέπει να προσφέρονται στους χρήστες με το ίδιο μέτρο (90: Şerbu 2015: 73-76).

4.3 Κίνδυνοι – Απειλές στα ΜΚΔ

Τα στατιστικά στοιχεία που αφορούν την Ελλάδα είναι ιδιαίτερα ανησυχητικά. Το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου του Ιδρύματος Τεχνολογίας και Έρευνας (είναι επίσημος εκπρόσωπος στην Ελλάδα των Πανευρωπαϊκών Οργανισμών INSAFE / INHOPE) στην ανασκόπηση που εκδόθηκε το 2017 κατέγραψε 34.590 καταγγελίες οι οποίες είχαν πραγματοποιηθεί στην τελευταία 15ετία, με τα τελευταία 5 χρόνια να κυμαίνονται κατά μέσο όρο στις 4.000 σε ετήσια βάση. Από αυτές οι 13.000 κρίθηκαν από τους νομικούς του κέντρου ότι έχουν εγκληματικό υπόβαθρο και προωθήθηκαν είτε στις αρμόδιες ελληνικές αρχές (Δίωξη ηλεκτρονικού εγκλήματος) είτε στις ευρωπαϊκές (Europol). Οι περισσότερες καταγγελίες που δέχτηκε η γραμμή αφορούν σε περιστατικά παραβίασης προσωπικών δεδομένων και επικοινωνιών (39%). Ακολουθούν τα εγκλήματα παιδικής κακοποίησης (21%), που είναι και το κύριο αντικείμενο των Ανοιχτών Γραμμών Καταγγελιών του INHOPE και οι διαδικτυακές οικονομικές απάτες (21%). Στην τρίτη θέση έρχονται τα περιστατικά ρητορικής μίσους και εκφοβισμού (14%) και ακολουθούν τα περιστατικά βίας

και απειλών στο διαδίκτυο. Τα παραπάνω στατιστικά αποτυπώνονται στον παρακάτω πίνακα (116: Safeline 2017:10 –11).

Εικόνα 11

Σταθερά ανοδική τάση καθ' όλη την 15ετή διάρκεια λειτουργίας της SafeLine καταγράφεται στα καταγγελθέντα περιστατικά εγκλημάτων παιδικής κακοποίησης. Ιδιαίτερα τα έτη 2016, 2017 οι εν λόγω καταγγελίες ξεπέρασαν κάθε προηγούμενο στην Ελλάδα επιβεβαιώνοντας την αύξηση των περιστατικών που παρατηρείται σε όλο τον κόσμο, μέσα από τα στατιστικά στοιχεία του INHOPE. Διαπιστώνεται μάλιστα ότι όσο μικραίνει ο μέσος όρος ηλικίας των παιδιών που έχουν πρόσβαση στις νέες τεχνολογίες, τόσο το πρόβλημα γιγαντώνεται.

Εικόνα 12

Το Νοέμβριο του 2013 αποκαλύφθηκε η μεγαλύτερη παραβίαση ως τότε προσωπικών δεδομένων σε πάνω από 2 εκατομμύρια λογαριασμούς χρηστών σε Facebook, Google, Twitter, Yahoo, Linked In κ.α. Η παραβίαση αφορούσε σε πάνω από 93.000 ιστοσελίδες και προέρχονταν από server της Ολλανδίας.

318,000 λογαριασμούς Facebook

70,000 000 λογαριασμούς Gmail, Google+ και YouTube

60,000 000 λογαριασμούς Yahoo

22,000 000 λογαριασμούς Twitter

9,000 λογαριασμούς Odnoklassniki (ένα ευρείας χρήσης Ρώσικο δίκτυο)

8,000 λογαριασμούς ADP(ADP-Αμερικάνικη εταιρεία επενδύσεων και υπηρεσιών μισθοδοσίας)

8,000 λογαριασμούς LinkedIn

Η υποκλοπή αποδόθηκε στη χρήση κακόβουλου λογισμικού τύπου Δούρειου Ίππου όπου εγκαταστάθηκε στους υπολογιστές των χρηστών επιτρέποντας την υποκλοπή usernames και passwords για πάνω από ένα μήνα.(79: Pagliery 2013).

Το Facebook ανακοίνωσε ότι στο εξάμηνο Απριλίου-Σεπτεμβρίου 2018 διέγραψε περισσότερους από ενάμισι δισεκατομμύριο ψευδείς (fake) και κακόβουλους λογαριασμούς, έναντι 1,3 δισεκατομμυρίου που είχε απενεργοποιήσει στο αμέσως προηγούμενο εξάμηνο. Οι περισσότεροι λογαριασμοί είχαν κίνητρα οικονομικής κερδοσκοπίας μάλλον παρά παραπληροφόρησης. Η θετική ανακοίνωση έρχεται την αμέσως επόμενη μέρα μετά την τρομερά αρνητική δημοσιότητα που, για μια ακόμη φορά, είχε το Facebook διεθνώς, μετά από το αποκαλυπτικό δημοσίευμα των "Τάιμς της Νέας Υόρκης" για τις "σκοτεινές" τακτικές στο πεδίο των δημοσίων σχέσεων, στις οποίες κατέφυγε το Facebook με στόχο να απαξιώσει τους επικριτές του, τους οποίους προσπάθησε να παρουσιάσει τεχνηέντως ακόμη και ως πράκτορες του Τζορτζ Σόρος (87: Romm *2018*).

4.4 Εμπλοκή των ΜΚΔ στην πολιτική

Βασιζόμενοι στην εξέγερση στην πλατεία Tahrir της Αιγύπτου το 2011 γίνεται κατανοητό το πόσο σημαντικό ρόλο παίζουν πλέον τα ΜΚΔ στην ανταλλαγή ή και διαμόρφωση ιδεών, απόψεων και γενικότερα στο να γίνονται οι πολίτες πιο ενεργοί (ή μήπως όχι;)(105: Wilson 2012: 363–379). Η εξέγερση αυτή είναι ορόσημο για τα ΜΚΔ καθώς αυτά χρησιμοποιήθηκαν ως δημοκρατικό εργαλείο ενός λαού που μέχρι τότε δεν είχε φωνή ώστε να οργανώσει εξεγέρσεις και διαμαρτυρίες οι οποίες συντέλεσαν στις πολιτικές εξελίξεις της χώρας.

Στις τελευταίες Αμερικανικές εκλογές η CIA έχει βάσιμες υποψίες ότι υπήρχε Ρωσικός δάκτυλος σε σωρεία ηλεκτρονικών μηνυμάτων, ψευδών ειδήσεων και διαρροή των προσωπικών μηνυμάτων της αντιπάλου του Trump, Clinton. Τον Αύγουστο του 2015, ο γνωστός ερευνητικός ψυχολόγος Robert Epstein (AmericanInstituteforBehavioralResearchandTechnology) δημοσίευσε ένα άρθρο με τίτλο «How Google Could Rigthe 2016 Election» (Πώς η Google μπορεί να χειραγωγήσει τις εκλογές, χωρίς κανένας να πάρει είδηση;). Προειδοποιούσε ότι ο νέος πρόεδρος της Αμερικής (προεδρικές 2016) θα κρινόταν όχι μόνο από τις τηλεμαχίες, αλλά και από τις κρυφές αποφάσεις της Google, τις οποίες μόνο κάποιοι εξειδικευμένοι ερευνητές, όπως τον Epstein, αντιλαμβάνονται. Σύμφωνα με έρευνα του ίδιου, η Google έχει συγκεντρώσει τεράστια δύναμη για έλεγχο της κοινής γνώμης (εκλογών). Ως γνωστό, Google είναι ένας μηχανισμός με τη βοήθεια του οποίου κάποιος μπορεί να κάνει έρευνα στο διαδίκτυο. Η

σειρά κατάταξης των απαντήσεων καθορίζεται από τον αλγόριθμο. Δηλαδή, αν κάποιος ζητήσει πληροφορίες για τον Σωκράτη και υπάρχουν έστω 1000 ιστότοποι που αναφέρονται στον Σωκράτη, η κατάταξη στη σειρά ακολουθεί τις οδηγίες του προγράμματος (αλγόριθμος). Ο Robert Epstein έχει κάμει ειδικά πειράματα μαζί με τον Ronald E. Robertson για να αποδείξει ότι ο αλγόριθμος της ερευνητικής μηχανής της Google έχει τη δυνατότητα να μεταθέσει τις επιλογές των ψηφοφόρων, χωρίς να το αντιλαμβάνονται, από 20-80%.
Με δεδομένο ότι πολλές εκλογές κερδίζονται με μικρή διαφορά, αυτό επιτρέπει στην Google να επηρεάσει τις εκλογές οπουδήποτε στον κόσμο (30: Epstein 2015: 4512 – 4521).

Στις Ηνωμένες Πολιτείες περίπου μισές προεδρικές εκλογές έχουν κριθεί με διαφορά κάτω του 7.6%, μέσα στο φάσμα επηρεασμού της Google. Οι προγραμματιστές της Google μπορούν να αλλάξουν τον αλγόριθμο αλλάζοντας τα κριτήρια επιλογής (τα οποία δεν αποκαλύπτονται ποτέ), χωρίς τη γνώση των προϊσταμένων της εταιρείας, χειραγωγώντας έτσι τον κόσμο. Αυτές οι προσαρμογές επηρεάζουν όλο και περισσότερο τον τρόπο που σκεφτόμαστε και συνεπαγόμενα που ψηφίζουμε. Οι ερευνητές ονόμασαν το φαινόμενο SEME (Search Engine Manipulation Effect) που είναι μια από τις μεγαλύτερες συμπεριφορικές επιδράσεις που υπήρξαν ποτέ. Στην ολοκληρωμένη μελέτη, που δημοσιεύτηκε στο Proceeding of the National Academy of Sciences (PNAS), συμπεριλαμβάνονται τα αποτελέσματα πέντε πειραμάτων με τη συμμετοχή 4,500 ανθρώπων σε δυο διαφορετικές χώρες. Η έρευνα αποδεικνύει ότι η Google έχει τη δυνατότητα να επηρεάσει ψηφοφόρους. Στο πείραμα μετά από μόνο μια στημένη «έρευνα» με μεροληπτική κατάταξη, ο αριθμός των ατόμων που ευνόησε έναν υποψήφιο αυξήθηκε από 37-63%. Με συνεχείς μεροληπτικές κατατάξεις το ποσοστό αυξάνεται περισσότερο (30). Να σημειωθεί ότι σε περιόδους εκλογών ο αριθμός των ακολούθων σε ένα υποψήφιο πρόεδρο μπορεί να αυξηθεί πάνω από εκατό χιλιάδες τη μέρα.

Σε μια έρευνα που διεξήχθη μόλις το 2011 αναδεικνύει το πρόβλημα της πρόβλεψης πολιτικής ταυτότητας των χρηστών μέσα από τα κοινωνικά δίκτυα και συγκεκριμένα από το twitter. Έτσι με βάση σχόλια και hashtags των χρηστών μπορεί εύκολα να εξαχθούν συμπεράσματα για τα πολιτικά τους πιστεύω. Συγκεκριμένα στις εκλογές που έγιναν το 2010 σε ένα δείγμα 1000 ψηφοφόρων η επιτυχία της πρόβλεψης άγγιξε το 91%. Σε παρόμοια έρευνα πάλι μέσα από τους χρήστες του twitter μέσα από τα στοιχεία που αναρτούν οι χρήστες μπορεί να εξαχθούν συμπεράσματα για την προσωπικότητα του κάθε χρήστη(22: Conover 2011:*192-199*), (39: Golbeck 2011: 149 – 156).

Μια ειδική Επιτροπή εννέα κυβερνήσεων από όλο τον κόσμο συνεδρίασε στο Βρετανικό Κοινοβούλιο, ελπίζοντας να λάβει απαντήσεις από τον ιδρυτή του Facebook για τη διάδοση ψευδών ειδήσεων στην πλατφόρμα του**.** Ήταν οπλισμένοι με εκρηκτικές νέες πληροφορίες, για μια σειρά από έγγραφα που ελήφθησαν από βρετανούς νομοθέτες που τεκμηρίωναν ότι η ομάδα του Zuckerberg είχε ειδοποιηθεί ήδη από το 2014 σχετικά με το πόσο έχει

κλιμακωθεί η συλλογή δεδομένων από τους Ρώσους. Στα έγγραφα αυτά υπήρχαν αποδείξεις ότι ένας μηχανικός του Facebook είχε προειδοποιήσει τη διοίκηση το 2014, ότι η Ρωσία συλλέγει καθημερινά τρία δισεκατομμύρια πακέτα δεδομένων από τους χρήστες του Facebook. Η συγκεκριμένη επιτροπή δεν αποτέλεσε τη μοναδική προσπάθεια να πραγματοποιηθεί μία συνάντηση πρόσωπο με πρόσωπο με τους μεγαλύτερους φορείς λήψης αποφάσεων στη Silicon Valley (78: Olson 2018).

Έναν κώδικα ορθής πρακτικής σε επίπεδο Ε.Ε. για την αντιμετώπιση της παραπληροφόρησης μέσω του Διαδικτύου προωθεί η Ευρώπη. Πρόκειται για ένα μόνο από τα μέτρα που δρομολογεί η Ε.Ε. και ανακοινώθηκαν με στόχο την καταπολέμηση της online παραπληροφόρησης. Η Ευρωπαϊκή Επιτροπή ορίζει ως παραπληροφόρηση τις "*αποδεδειγμένα ψευδείς ή παραπλανητικές πληροφορίες που δημιουργούνται, παρουσιάζονται και διαδίδονται για οικονομικό όφελος ή για τη σκόπιμη παραπλάνηση του κοινού και που ενδέχεται να βλάψουν το κοινό συμφέρον*". Στην τελευταία έρευνα του Ευρωβαρομέτρου, το 83% όσων απάντησαν δήλωσαν ότι οι ψευδείς ειδήσεις συνιστούν κίνδυνο για τη δημοκρατία. Στο μεταξύ, σύμφωνα με έρευνα του Κοινού Κέντρου Ερευνών, τα δύο τρίτα των καταναλωτών διαδικτυακών ειδήσεων προτιμούν να έχουν πρόσβαση σε αυτές από πλατφόρμες, που λειτουργούν με αλγόριθμους, όπως είναι οι μηχανές αναζήτησης και οι φορείς συγκέντρωσης ειδήσεων, καθώς και μέσω των ιστοτόπων των μέσων κοινωνικής δικτύωσης. Προκειμένου να αντιμετωπιστούν οι υφιστάμενες ανησυχίες, η Επιτροπή προτείνει σειρά μέτρων για την αντιμετώπιση της παραπληροφόρησης. Στα μέτρα αυτά περιλαμβάνεται ένας "Κώδικας ορθής πρακτικής για την παραπληροφόρηση". Έως τον Ιούλιο 2018 και ως πρώτο βήμα, οι διαδικτυακές πλατφόρμες θα πρέπει να αναπτύξουν και να ακολουθούν κοινό κώδικα ορθής πρακτικής προκειμένου να εξασφαλίζουν διαφάνεια σχετικά με το χρηματοδοτούμενο με χορηγία περιεχόμενο, ιδίως την πολιτική διαφήμιση, καθώς και να περιορίζουν τις επιλογές στόχευσης για την πολιτική διαφήμιση και να μειώνουν τα έσοδα των διακινητών παραπληροφόρησης. Επίσης, θα πρέπει να παρέχουν σαφέστερες πληροφορίες σχετικά με τη λειτουργία των αλγορίθμων και να δίνουν τη δυνατότητα επαλήθευσης από τρίτους, αλλά και να καθιερώσουν μέτρα για τον εντοπισμό και το κλείσιμο των πλαστών λογαριασμών και την αντιμετώπιση των αυτοματοποιημένων προγραμμάτων.(118: Ευρωπαϊκή Ένωση 2019)

4.5 Συνέπειες από «κακή» χρήση των ΜΚΔ

Η ανεπιθύμητη αποκάλυψη των πληροφοριών των χρηστών σε συνδυασμό με την ασυμφωνία που προκαλείται από τα ίδια τα ΜΚΔ μεταξύ των επαγγελματικών και των προσωπικών πτυχών της ζωής των χρηστών επιτρέπουν περιστατικά με άσχημες

συνέπειες. Τα μέσα ενημέρωσης κάλυψαν μερικά από αυτά, όπως στην περίπτωση ενός δασκάλου που ανεστάλη η επαγγελματική του ιδιότητα για ανάρτηση φωτογραφιών με πυροβόλα όπλα (26: Dam 2009)ή υπάλληλος απολύθηκε επειδή σχολιάζοντας, συνέκρινε τον μισθό της με εκείνο του αφεντικού της (25: DailyMail 2011). Με τη δουλειά της «πλήρωσε» επίσης μια μαθηματικός στη Βρετανία λόγω κάποιων τολμηρών φωτογραφιών που είχε αναρτήσει στο Facebook πριν να προσληφθεί από λύκειο στο Μπέρμιγχαμ. Οι επίμαχες φωτογραφίες είχαν αναρτηθεί το 2013 (86: Ridler 2018). Και τα τρία περιστατικά είχαν αναρτηθεί στο Facebook. Τέλος μια καθηγήτρια σε γυμνάσιο στις ΗΠΑ έχασε τη δουλειά της όταν μία γυμνή φωτογραφία που είχε στείλει παλιότερα στο σύντροφό της, έφτασε στα χέρια μαθητή της μέσω ΜΚΔ.

4.6 Κίνδυνοι των ΜΚΔ για τις επιχειρήσεις και τους εργαζόμενους

Στις επιχειρήσεις από την άλλη ο αντίκτυπος της διαρροής ευαίσθητων πληροφοριών μπορεί να οδηγήσει σε μια σειρά οργανωτικών επιπτώσεων, συμπεριλαμβανομένης της απώλειας ανταγωνιστικού πλεονεκτήματος, απώλειας φήμης, απώλειας εισοδήματος και απώλειας ευκαιριών, ειδικά όταν οι πελάτες είναι ευαίσθητοι σε παραβιάσεις πληροφοριών (8: Atif 2014: 27 – 39).

Η διαρροή ευαίσθητων πληροφοριών σε οργανισμούς είναι ένας σημαντικός και αυξανόμενος κίνδυνος ασφαλείας γενικότερα. Οι ευαίσθητες πληροφορίες μπορεί να περιλαμβάνουν εμπορικά μυστικά, πνευματική ιδιοκτησία, επιχειρηματικές στρατηγικές, λεπτομέρειες σχετικά με προϊόντα ή υπηρεσίες και ακόμη και εμπιστευτικές πληροφορίες εργαζομένων και πελατών. Ο παρακάτω πίνακας (Εικόνα 13) απεικονίζει τις βασικές λειτουργίες των τοποθεσιών των ΜΚΔ και τους σχετικούς κινδύνους διαρροής σε οργανισμούς (76).

OSN Functions	Potential Security Risks	Potential Impacts to Organisations
Post information / update status	Users may inadvertently disclose sensitive information through OSN posts/updates as access to OSN is by anyone, anywhere, anytime, using any devices	Unauthorized access or deduction of information of value from inadvertent disclosures
Friend Requests	Carelessness in accepting friend requests increases risk of adding untrusted users	Monitoring of organisational targets and social engineering attacks to progress an impending attack
Upload photos and videos	Photo albums and videos may inadvertently disclose sensitive information	Photos and videos may contain sensitive information resulting in a range of impacts
Third party applications and links to external sites	Third party content may contain malware or links that enable inadvertent disclosure	Use of compromised client platforms to further an impending attack

Εικόνα 13

Τα ΜΚΔ είναι παρόμοια με ένα "διαπερατό σωλήνα" καθώς έχουν σχεδιαστεί έτσι ώστε οι επικοινωνίες μεταξύ του αποστολέα και των παραληπτών να είναι ορατές και σε άλλα μέρη. Η διαρροή μέσω των ΜΚΔ είναι (1) στιγμιαία, καθώς είναι διαθέσιμη στο κοινό αμέσως μετά την δημοσιοποίηση, (2) πανταχού παρούσα, καθώς είναι παγκοσμίως προσπελάσιμη σε χιλιάδες δημογραφικά στοιχεία και (3) επίμονη σε αυτό που αρχειοθετείται σε διαχρονικότητα . Αυτά τα χαρακτηριστικά παρακινούν τους τελικούς χρήστες να συνεργαστούν με τα ΜΚΔ αλλά δημιουργούν επίσης ευκαιρίες για διαρροή πληροφοριών. Ορίζουμε τη διαρροή πληροφοριών ως "παραβίαση της εμπιστευτικότητας των πληροφοριών, που κατά κανόνα προέρχονται από το προσωπικό μέσα σε έναν οργανισμό και συνήθως οδηγούν στην αποκάλυψη εσωτερικών πληροφοριών ..." σε όλα τα οργανωτικά όρια (26).

4.7 Άγνοια κινδύνου

Τα ίδια τα κοινωνικά δίκτυα εκ προθέσεως (π.χ. χρήση στο Facebook Beacon: μια ιδιότητα που έχει προστεθεί στο Facebook τα τελευταία χρόνια με σκοπό να παρέχονται διαφημιστικά μηνύματα στην κύρια πλατφόρμα ανάλογα με τις επιθυμίες των χρηστών (104: wikipedia 2009) (28: Dwyer 2011:58-63)) ή ακούσια (π.χ. δημοσιεύοντας ανώνυμα προσωπικά δεδομένα τα οποία από- ανωνυμοποιούνται και χρησιμοποιούνται σε επιθέσεις ώστε να παραβιαστεί το απόρρητο των χρηστών (72: Narayanan 2011: 1825-1834). Επιπλέον, ο μεγάλος όγκος δεδομένων προσωπικού χαρακτήρα που αποκαλύφθηκε είτε από άγνοια των χρηστών είτε λόγω της αποτυχίας των ΜΚΔ να παρέχουν εξελιγμένα εργαλεία προστασίας προσωπικών δεδομένων, έχουν προσελκύσει εταιρείες (π.χ. GNIP) οι οποίες συγκεντρώνουν και πωλούν δεδομένα προσωπικού χαρακτήρα του χρήστη(52: Kayes 2015). Επιπλέον, φύση των ΜΚΔ που τα καθιστά έμπιστα στους χρήστες, έχει καταστεί αποτελεσματικός μηχανισμός για την εξάπλωση ανεπιθύμητων μηνυμάτων, κακόβουλων προγραμμάτων, και επιθέσεων ηλεκτρονικού ψαρέματος (phishing). Οι μηχανισμοί αυτοί εκκινούν ένα ευρύ φάσμα επιθέσεων, δημιουργώντας ψεύτικα προφίλ, χρησιμοποιώντας κλοπές διαπιστευτηρίων λογαριασμού που πωλούνται στην μαύρη αγορά (94: Staff 2010) ή αναπτύσσοντας αυτοματοποιημένα κοινωνικά ρομπότ (102: Wagner 2012: 41-48). Τη θέση του για την Οδηγία σχετικά με την καταπολέμηση της απάτης και της πλαστογραφίας(phishing, skimming), που αφορούν τα μέσα πληρωμής πλην των μετρητών, ενέκρινε στις 9 Μαρτίου 2018 το Ευρωπαϊκό Συμβούλιο. (117: Ευρωκοινοβούλιο , 2019)

Οι χρήστες λοιπόν πολλές φορές είναι πρόθυμοι να κοινοποιήσουν προσωπικές πληροφορίες όπως φωτογραφίες, video, αριθμούς τηλεφώνων κ.α. μερικές φορές επίσης δέχονται αιτήματα φιλίας από αγνώστους οι οποίοι προσποιούμενοι τους φίλους μπορεί να είναι hackers. Υπολογίζεται ότι καθημερινά διακινούνται περίπου 1,8 δισεκατομμύρια φωτογραφίες την ημέρα (54: Knibbs 2014). Έτσι, μέσα από τις προσωπικές πληροφορίες που έχουμε δημοσιοποιήσει μπορεί ο επιτιθέμενος να καταφέρει να διεισδύσει στα προσωπικά μας στοιχεία. Επίσης στην πλειονότητα τους οι χρήστες εμφανίζονται με τα πλήρη στοιχεία του ονόματος τους πράγμα που οδηγεί πολύ εύκολα, και με την τεχνολογία που υπάρχει σήμερα, να αποκαλυφτούν πλήθος προσωπικών πληροφοριών των χρηστών όπως σε ποιο σχολείο έχουν φοιτήσει, χώρο εργασίας, επάγγελμα και άλλες δραστηριότητες που αφορούν την πραγματική ζωή. Παράλληλα πολλοί χρήστες αποκαλύπτουν την διεύθυνση του ηλεκτρονικού τους ταχυδρομείου που μπορεί να οδηγήσει εύκολα σε επιθέσεις τύπου ψαρέματος για να αποσπάσουν πληροφορίες προσωπικές, οικονομικές κ.α. Ένα επίσης σημαντικό εύρημα αυτής της μελέτης είναι ότι το ανδρικό φύλο αποκαλύπτει πολύ ευκολότερα προσωπικά δεδομένα απ' ότι το γυναικείο λόγω κυρίως έλλειψης ή μη του φόβου (98: Taraszow 2010: 81–101) . Μια άλλη πολύ σημαντική πτυχή της ασφάλειας των μέσων κοινωνικής δικτύωσης η οποία δημοσιεύτηκε από το Πανεπιστήμιο Ισλαμικών σπουδών της Μαλαισίας αφορά στην αθρόα, και χωρίς κανένα έλεγχο, κοινοποίηση πληροφοριών σχετικά με τον εργασιακό χώρο εργαζομένων

οι οποίοι δημοσιεύουν με μεγάλη ευκολία σημαντικά στοιχεία επιχειρήσεων (οικονομικά, ατομικά κ.α) δίνοντας την δυνατότητα σε κακόβουλους πολύ εύκολα να συλλέγουν πληροφορίες για την επιχείρηση. Πολλές φορές η δημοσίευση αυτή είναι εν ήδη αστεϊσμού χωρίς βεβαίως να αλλάζει το αποτέλεσμα. (77: Nuha 2011).

Πολλές φορές επίσης με την πρόφαση της διασκέδασης μας ζητούνται πληροφορίες, εκτός από την εργασία μας, άλλες, που σχετίζονται με δεδομένα τραπεζικών λογαριασμών ή κωδικούς. Οι εταιρείες που χρησιμοποιούν τεχνικές third-party, πολλές φορές σε συνεργασία με τους παρόχους των μέσων κοινωνικής δικτύωσης ανταλλάσουν πληροφορίες χρηστών – πελατών με στόχο την προώθηση προϊόντων, τη διαφήμιση ή και την προώθηση τους σε κρατικές υπηρεσίες . Οι απειλές των χρηστών των μέσων κοινωνικής δικτύωσης μπορούν να χωριστούν σε τρεις κατηγορίες:

Κλασσικές απειλές : αφορούν επιθέσεις, απάτες μέσω internet,επιθέσεις με κακόβουλο λογισμικό, επιθέσεις ψαρέματος (phishing) καθώς και επιθέσεις στη βάση δεδομένων (sql attacks).

Απειλές Νέου τύπου: Σε αυτή την κατηγορία ανήκουν επιθέσεις τύπου Clickjacking όπου γίνεται παράνομη καταγραφή των κλικ που εκτελούνται είτε με το ποντίκι είτε με το πληκτρολόγιο. Άλλος τύπος είναι τα Socialbots για τα οποία θα αναφερθούμε παρακάνω.

Απειλές με χρήση ψεύτικου προφίλ: είναι η χρήση ψεύτικων προφίλ για άμεση διοχέτευση smap μηνυμάτων με στόχο χρήστες – φίλους (μέσω αιτημάτων φιλίας) η χρήστες φίλων φίλων. Τα ΜΚΔ έχουν μηχανισμούς να αντιμετωπίσουν τέτοιες απειλές πιστοποιώντας και επικυρώνοντας τους χρήστες ώστε να είναι μοναδικοί. Μια άλλη απειλή που εντάσσεται σε αυτή την κατηγορία είναι η διαρροή τοποθεσίας και πληροφοριών στην οποία οι χρήστες είναι πρόθυμοι να μοιραστούν πληροφορίες οι οποίες είναι χρήσιμες από εταιρείες για έλεγχο υποψηφίων είτε κακόβουλων με σκοπό να βλάψουν τους χρήστες, καθώς και θέσεις στις οποίες βρίσκονται ή διαμένουν άμεσα(δήλωση στο προφίλ τόπο διαμονής) ή έμμεσα με φωτογραφίες, video κ.α. Επιθέσεις εφήβων: Καθώς αυξάνει η χρήση των ΜΚΔ από άτομα που βρίσκονται σε εφηβική ηλικία εντείνεται ένα νέο είδος επίθεσης όπως είναι το bullying και grooming. Το δικτυακό bullying έχει πολλές κατηγορίες όπως δυσφήμηση, παρενόχληση, κοροϊδία σε εξωτερικούς χώρους, πρόκληση φόβου μέσω μηνυμάτων. Το blooming είναι η προσπάθεια αποπλάνησης ανηλίκων από ενήλικες (112: Zhivago 2016: 914 –925).

Το 2009, το Φόρουμ Secure Enterprise 2.0 εντόπισε οκτώ κύριες απειλές (Perez, 2009; Chi, 2011): ανεπαρκείς έλεγχοι επαλήθευσης ταυτότητας, cross site scripting (αναφερόμαστε στην εκμετάλλευση διάφορων ευπαθειών (vulnerabilities) υπολογιστικών

συστημάτων με εισαγωγή κώδικα HTML ή Javascript σε κάποιο ιστοχώρο.), cross site request forgery(είναι ένας τύπος κακόβουλης εκμετάλλευσης ενός ιστότοπου όπου μεταδίδονται μη εξουσιοδοτημένες εντολές από έναν χρήστη που εμπιστεύεται η εφαρμογή ιστού, απειλή ψαρέματος, διαρροή πληροφοριών, injection flow (επιτρέπει στους επιτιθέμενους να αναμεταδίδουν κακόβουλο κώδικα μέσω μιας εφαρμογής σε άλλο σύστημα), απειλή ακεραιότητας πληροφοριών πλαστογράφηση, διαρροή πληροφοριών, fault injection, ακεραιότητα πληροφοριών και ανεπαρκής αντι-αυτοματισμός (Ανεπαρκής αντι-αυτοματοποίηση είναι όταν ένας ιστότοπος επιτρέπει σε έναν εισβολέα να αυτοματοποιήσει μια διαδικασία που πρέπει να εκτελείται μόνο χειροκίνητα).

4.8 Κατηγοριοποίηση απειλών

Παρακάτω (Εικόνα 14) παρουσιάζεται ένας συγκριτικός πίνακας των πιο γνωστών απειλών σε συνδυασμό με τη συχνότητα εμφάνισης τους.

Measure	Impact on user	Effectiveness of server side protection mechanism	Effectiveness of user side protection mechanism	Threat to data privacy	Threat to data integrity
Identity theft	Average to high	Poor	Poor	Yes	Yes
Spam attack	Small	Strong	Poor	No	No
Malware	High	Medium	Medium	Yes	Yes
Sybil attack	Average	Strong	Poor	No	Yes
Social phishing	High	Poor	Strong	Yes	Yes
Impersonation	High	Poor	Poor	Yes	Yes
Hijacking	High	Poor	Poor	Yes	Yes
Fake requests	Small	Poor	Strong	Yes	No
Image retrieval and analysis	Average to high	Medium	Medium	Yes	No

Εικόνα 14

Κλοπή ταυτότητας

Αυτό αναφέρεται στην πλαστοπροσωπία σε πραγματικό χρόνο του νόμιμου χρήστη. Ο εισβολέας παίρνει τον έλεγχο του προφίλ του θύματος και είναι σε θέση να έρθει σε επαφή με άλλους πραγματικούς χρήστες στους οποίους ανήκει το προφίλ .

Επίθεση μέσω spam

Εδώ, ο επιτιθέμενος είναι σε θέση να γνωρίζει λεπτομέρειες της επικοινωνίας του χρήστη και είναι σε θέση να στείλει ανεπιθύμητα δεδομένα. Οι λεπτομέρειες επικοινωνίας δεν είναι τόσο δύσκολο να αποκτηθούν, μπορούν να εξαχθούν από τα προφίλ του νόμιμου χρήστη.

Επιθέσεις κακόβουλου λογισμικού

Γίνονται πολύ συνηθισμένοι μεταξύ των ιστοτόπων κοινωνικής δικτύωσης. Οι επιτιθέμενοι στέλνουν κακόβουλο λογισμικό σε μορφή script στον νόμιμο χρήστη. Κάνοντας κλικ στην κακόβουλη διεύθυνση URL μπορεί να εγκατασταθεί κακόβουλο λογισμικό στις συσκευές εισβολέων ή μπορεί να οδηγήσει σε έναν ψεύτικο ιστότοπο ο οποίος επιχειρεί να κλέψει σημαντικές προσωπικές πληροφορίες από το χρήστη-στόχο.

Επιθέσεις Sybil

Τα ψεύτικα προφίλ αποτελούν τις βάσεις για τις επιθέσεις Sybil, οι οποίες μπορεί να βλάψουν την καλή λειτουργία των ΜΚΔ, μπορούν να χρησιμοποιηθούν για τη διανομή ανεπιθύμητων πληροφοριών ή κακόβουλου λογισμικού μέσω του δικτύου. Για να αποφευχθούν αυτές οι επιθέσεις, οι μηχανισμοί ελέγχου ταυτότητας του χρήστη θα πρέπει να είναι ισχυροί.

Κοινωνικό ψάρεμα

Αναφέρεται στην επίθεση στην οποία ο επιτιθέμενος σκοπεύει να αποκτήσει ευαίσθητες πληροφορίες από έναν χρήστη-στόχο μέσω ενός ψεύτικου ιστότοπου που φαίνεται να είναι πραγματικός ή υποδυόμενος κάποιον που το θύμα γνωρίζει και εμπιστεύεται. Αυτές οι επιθέσεις μπορούν να μειωθούν σημαντικά εάν οι χρήστες γνωρίζουν και εξετάζουν προσεκτικά τα δεδομένα που λαμβάνουν.

Προσωποποίηση

Εδώ ο στόχος του επιτιθέμενου είναι να δημιουργήσει ψεύτικο προφίλ για να υποδυθεί με επιτυχία έναν πραγματικό χρήστη. Αυτή η επίθεση εξαρτάται σε μεγάλο βαθμό από τις τεχνικές επαλήθευσης ταυτότητας που αντιμετωπίζουν οι χρήστες κατά την εγγραφή για

να δημιουργήσουν νέο λογαριασμό. Αυτές οι επιθέσεις μπορούν να προκαλέσουν σοβαρή ζημιά στον στόχο που υποδύονται.

Πειρατεία

Αναφέρεται στην απόκτηση ελέγχου επί του προφίλ κάποιου άλλου. Ο εισβολέας επιτυγχάνει την εισβολή ενός νόμιμου προφίλ αν είναι σε θέση να σπάσει τον κωδικό πρόσβασης σύνδεσης του λογαριασμού του. Οι αδύναμοι κωδικοί πρόσβασης είναι επομένως μια κακή επιλογή καθώς αυξάνουν την απειλή. Τέτοιοι κωδικοί πρόσβασης μπορούν να αποκτηθούν από επιθέσεις με λεξικό (dictionary attacks). Οι ισχυροί κωδικοί πρόσβασης και η συχνή αλλαγή τους είναι μια καλή πρακτική.

Ψεύτικα αιτήματα

Ο εισβολέας στέλνει ψεύτικο αίτημα με το δικό του προφίλ, ώστε να διευρύνει το δίκτυό του. Εάν οι χρήστες αποδέχονται ψευδή αιτήματα, δίνουν στον εισβολέα περισσότερα προνόμια και μπορούν να λάβουν περισσότερες πληροφορίες από τα προφίλ θυμάτων. Η πρόληψη των πλαστών αιτημάτων δεν είναι εφικτή, οπότε οι χρήστες πρέπει να είναι πιο υπεύθυνοι στα ΜΚΔ.

Ανάκτηση και ανάλυση εικόνων

Ο επιτιθέμενος χρησιμοποιεί διάφορα λογισμικά αναγνώρισης προσώπου και εικόνας για να βρει περισσότερες πληροφορίες σχετικά με τον στόχο και τα στοιχεία του προφίλ του. Δεν επηρεάζει μόνο τον στόχο, αλλά και τους φίλους και την οικογένειά του. Αυτές οι επιθέσεις αποσκοπούν στη συγκέντρωση βίντεο κλπ. από το στόχο.

4.9 Κίνητρα επιθέσεων

Τα κίνητρα των κακόβουλων που πραγματοποιούν τέτοιες ενέργειες ποικίλουν. Τα βασικά είναι:

Εκδίκηση / Συναίσθημα

Οι δυσαρεστημένοι χρήστες ή ακόμη και ένας υπάλληλος ενός οργανισμού μπορούν να επιχειρήσουν επιθέσεις στα ΜΚΔ εξαιτίας του θυμού, της διαφωνίας τους ή οποιασδήποτε μορφής εκδίκησης. Αυτοί οι τύποι hacker επιδιώκουν να καταστρέψουν τη φήμη ενός οργανισμού παρεμποδίζοντας τις υπηρεσίες του . Λόγω αυτού του είδους επιθέσεων ένας οργανισμός μπορεί να υποστεί μεγάλες οικονομικές απώλειες.

Οικονομικά οφέλη

Αυτός είναι ο πιο σημαντικός και κοινός λόγος επίθεσης στα κοινωνικά μέσα. Οι κυβερνοεγκληματίες αποκτούν τις ευαίσθητες πληροφορίες σχετικά με τραπεζικούς λογαριασμούς των χρηστών με σκοπό το οικονομικό όφελος. Μπορεί να περιλαμβάνει κλοπή επιχειρηματικών πληροφοριών από άλλη αντίπαλη εταιρεία.

Ψυχαγωγία

Μερικοί hackers απολαμβάνουν τη συναρπαστική εμπειρία της πειρατείας στα κοινωνικά μέσα. Εκτελούν επίθεση για να επιβεβαιώσουν τις ικανότητές τους ή την αξιοπιστία τους στους συναδέλφους τους. Το κάνουν για ψυχαγωγικούς λόγους χωρίς να περιμένουν κανένα οικονομικό ή πολιτικό κέρδος.

Πειρατεία για το καλό της επιχείρησης

Οι περισσότερες επιχειρήσεις δεν αισθάνονται ασφάλεια στον κυβερνοχώρο σε θέματα πειρατείας, συνεπώς υπάρχει μεγάλη ζήτηση θωράκισης των επιχειρήσεων. Ο καλύτερος τρόπος είναι η προσέλκυση hackers και ειδικών στον κυβερνοχώρο για να αντιμετωπίσουν τους ίδιους. Είναι πιο εύκολο να νικήσουμε έναν εγκληματία αν έχουμε ένα πρόσωπο από την πλευρά μας, που μπορεί να σκέφτεται και να λειτουργεί με τον ίδιο τρόπο όπως αυτός. Χαρακτηριστικό παράδειγμα είναι τα penetration tests που διεξάγουν οι επιχειρήσεις με σκοπό να βρουν, αν υπάρχουν, ανοικτοί δίαυλοι που να μπορούν να εισχωρήσουν κακόβουλοι.

Ακτιβισμός

Είναι η χρήση υπολογιστών και δικτύων υπολογιστών για την προώθηση των πολιτικών στόχων, κυρίως της ελευθερίας του λόγου, των ανθρώπινων δικαιώματων και την ηθική των πληροφοριών. Αυτό περιλαμβάνει επίσης και τις απόψεις μιας πολιτικής κοινότητας ή θρησκείας, για να οργανώσουν διαμαρτυρίες που υποστηρίζουν τις πολιτικές / θρησκευτικές πεποιθήσεις τους. Περιλαμβάνει επίσης τον βανδαλισμό των διαφόρων ιστοτόπων με πολιτικά / θρησκευτικά μηνύματα.

Κυβερνοκατασκοπεία

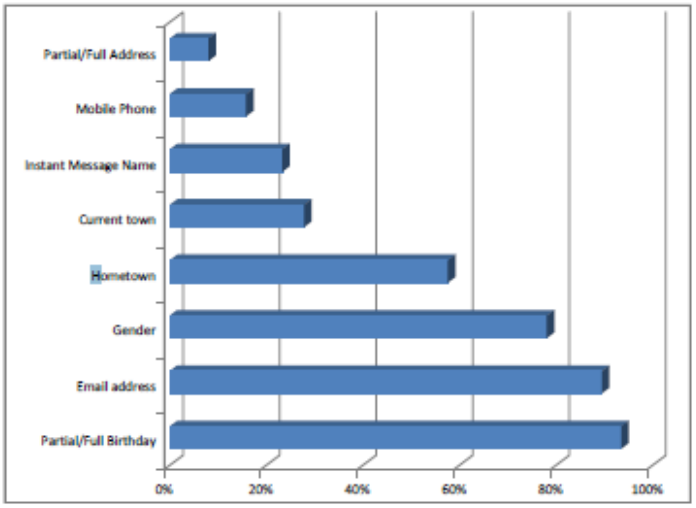
Οδηγεί στην κλοπή εμπιστευτικών πληροφοριών σχετικά με τα κοινωνικά μέσα. Περιλαμβάνει τη λήψη προσωπικών πληροφοριών χωρίς την άδεια του ιδιοκτήτη των πληροφοριών από ιδιώτες, ανταγωνιστές ή ακόμα και από άλλη χώρα. Οι επιθέσεις αυτές γίνονται με τη βοήθεια διαφόρων τεχνικών hacking και κακόβουλου λογισμικού.

Κυβερνοπόλεμος

Πρόκειται για πολιτικές επιθέσεις που βασίζονται στο διαδίκτυο και σε συστήματα πληροφόρησης και πληροφοριών που χρησιμοποιούν κοινωνικά μέσα. Ο στόχος αυτών των επιθέσεων περιλαμβάνει κυρίως κυβερνητικούς ιστότοπους για να παρακωλύσουν την επικοινωνία τους, την οικονομική σταθερότητα και πολλά άλλα πράγματα που επικεντρώνονται κυρίως στην κακή λειτουργία της κυβέρνησης άλλης χώρας. Είναι βασικά ένας πόλεμος που διεξάγεται μέσα από το δωμάτιο, παρά στο πεδίο (112).

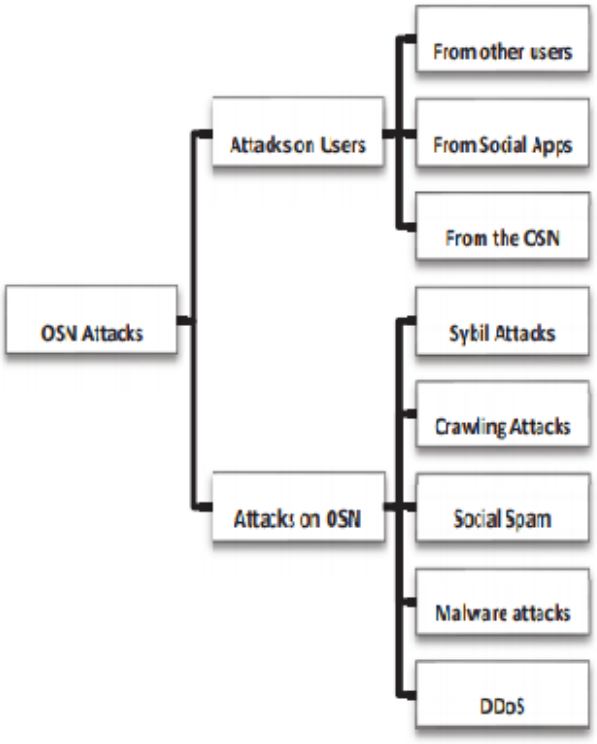
4.10 Κίνδυνοι από φίλους φίλων

Μια πολλή σημαντική παράμετρος την οποία θα πρέπει να έχουν όλοι οι χρήστες υπ' όψιν τους, είναι η προσκλήσεις που δεχόμαστε από «φίλους» φίλων. Έτσι, αν και πολλές φορές, έχουμε αντίληψη για την ιδιωτικότητα και την εμπιστοσύνη, δεχόμαστε με ευκολία τέτοιου είδους αιτήματα φιλίας με αποτελέσματα πολλές φορές δυσάρεστα καθώς ο «φίλος» φίλου μπορεί να είναι κακόβουλος. Τα προφίλ λοιπόν των χρηστών, πολλές φορές περιέχουν πληθώρα πληροφοριών με προσωπικά στοιχεία. Στο παρακάτω γράφημα (Εικόνα 15) αποτυπώνεται η εικόνα των φίλων που έχουν γίνει αποδεκτοί μέσα από τα προφίλ των χρηστών (71: Nagle 2009: 212-218).



Εικόνα 15

Έμμεσα λοιπόν, αυτό μεταφράζεται, ότι οι χρήστες είναι εξασφαλισμένοι ότι θα μπορούν να συνεχίζουν την ανταλλαγή δεδομένων μέσω των ΜΚΔ θεωρώντας ότι δεν υπάρχει κίνδυνος να είναι θύματα επιθέσεων ή κακόβουλων ενεργειών. Στο ακόλουθο σχήμα φαίνεται αυτή η κατηγοριοποίηση. Στο ακόλουθο σχήμα (Εικόνα 16) αποτυπώνονται οι κυριότερες μορφές επιθέσεων (50: Kader 2016:20-27).



Εικόνα 16

Οι επιθέσεις σε χρήστες αφορούν ένα μικρό αριθμό τυχαίων ή συγκεκριμένων χρηστών. Υπάρχουν διάφοροι τύποι επίθεσης με βάση τον επιτιθέμενο όπως: Επίθεση από άλλους χρήστες, επίθεση από εφαρμογή των ΜΚΔ, επίθεση από το ΜΚΔ. Οι επιθέσεις στα ΜΚΔ είναι: επιθέσεις που απευθύνονται στους παρόχους ΜΚΔ απειλώντας την παροχή της συγκεκριμένης υπηρεσίας όπως επιθέσεις τύπου Crawling, Social spam, DDoS ή επίθεση με κακόβουλο λογισμικό. Έτσι λοιπόν οι χρήστες είναι πολλαπλά εκτεθειμένοι. Αρχικά μια εφαρμογή μπορεί να είναι μολυσμένη με κάποιο ιό με σκοπό τη συλλογή δεδομένων για ανεπιθύμητη χρήση. Για να γίνει κατανοητό αυτό το BBC δημιούργησε μία κακόβουλη εφαρμογή η οποία μπορούσε να συλλέξει μια τεράστια ποσότητα δεδομένων από χρήστες σε μόλις 3 ώρες (51: Kayes 2015). Δεύτερον οι ίδιοι οι προγραμματιστές παραβιάζοντας την πολιτική απορρήτου μπορούν να ελέγχουν τα δεδομένα των χρηστών. Οι πολιτικές απορρήτου υποτίθεται ότι απαγορεύουν την κατάχρηση πληροφοριών από χρήστες. Αυτό όμως δεν τηρείται πάντα καθώς στην εφαρμογή του Facebook “Top friends” επέτρεπε στην καθένα να δει ημερομηνία γέννησης, φύλο και το κοινωνικό προφίλ των χρηστών ενώ επέτρεπε και όλες τις επιθέσεις που αναφέραμε για τα ΜΚΔ.

Μια άλλη μορφή εξαπάτησης είναι τα socialbots. Τα socialbots είναι αυτοματοποιημένα μηνύματα (tweets) ή χρησιμοποιούνται για να υποστηρίξουν μια άποψη λειτουργώντας σαν ομάδα ή σαν ένας ανύπαρκτος λογαριασμός. Σε έρευνα που έγινε χρησιμοποιώντας ως εργαλείο το facebook και με τη χρήση socialbots σε πολύ μεγάλη κλίμακα διαπιστώθηκαν τα εξής: 1) Το ποσοστό διείσδυσης στους χρήστες αγγίζει το 80%. 2) Ανάλογα με την πολιτική απορρήτου μια επιτυχημένη διείσδυση μπορεί να έχει ως αποτέλεσμα να παραβιαστούν προσωπικά δεδομένα των χρηστών. 3) Πρακτικά οι μηχανισμοί ασφαλείας του Facebook όπως είναι το Facebook Immune System αδυνατεί να ανιχνεύσει ή να σταματήσει μιας μεγάλης κλίμακας socialbots. (17: Boshmaf 2011: 93-102);(16: Boshmaf 2013: 556 - 578)

Σε μια άλλη μελέτη σχετικά με τα socialbots εκφράστηκε η απορία αν οι άνθρωποι είναι διατεθειμένοι να δημοσιοποιήσουν πληροφορίες γύρω από το χώρο εργασίας τους. Στην έρευνα αυτή λοιπόν που διεξήχθη σε δύο οργανισμούς χρησιμοποιώντας socialbots και ως εργαλείο και πάλι το facebook διαπιστώθηκε ότι αυτά είναι ικανά να διεισδύσουν σε λογαριασμούς εργαζομένων – χρηστών. Με την έρευνα αυτή ανακαλύφτηκε ένα άλλο

13,55% επιπλέον προσωπικό (δεν είχε σχέση με ΜΚΔ) και ένα ποσοστό 18,29% είναι πρόθυμα να δημοσιοποιήσουν περισσότερα links πληροφοριών της εταιρείας τα οποία δεν ήταν δημοσιοποιημένα (29: **Aviad** 2012:7–12).

Κεφάλαιο_5 . Ιδιωτικότητα

Σύμφωνα με τον Beldad υπάρχουν δύο κατηγορίες προσωπικών πληροφοριών οι οποίες εκτίθενται στα ΜΚΔ. Οι στατικές όπως όνομα, ηλικία, ημερομηνία γέννησης κ.α. και οι μη στατικές όπως καθημερινές δραστηριότητες, σκέψεις για ένα ζήτημα, φωτογραφίες κ.α. (16) .

Για να γίνει αντιληπτό του πόσο σημαντικό είναι η διατήρηση της ιδιωτικότητας μας και της προστασίας των δεδομένων προσωπικού χαρακτήρα, από το 2006, το Ευρωπαϊκό συμβούλιο, έχει επισήμως θεσπίσει την 28η Ιανουαρίου ως ημέρα προστασίας των δεδομένων με σκοπό την ευαισθητοποίηση των πολιτών στα θέματα αυτά. Είναι γνωστή ως "Convention 108". Η συνθήκη αυτή έχει υπογραφεί από περισσότερες από 50 χώρες σε όλο τον κόσμο (23: COUNCIL OF EUROPE 2019).

Από την άλλη ο ιδρυτής του Facebook, Mark Zuckerberg, πιστεύει ότι η ιδιωτικότητα δεν αποτελεί πλέον κοινωνικό κανόνα, καθώς οι διαδικτυακοί χρήστες έχουν συνηθίσει να μοιράζονται τις πληροφορίες τους στο διαδίκτυο, με αποτέλεσμα τα επίπεδα προσδοκίας για την προστασία της ιδιωτικής ζωής να είναι χαμηλότερα (47: Johnson 2010) .

Οι χρήστες πρέπει να αποφασίσουν μεταξύ της αποκάλυψης ή μη προσωπικών πληροφοριών. Για το λόγο αυτό οι χρήστες πρέπει να έχουν τις αντίστοιχες δεξιότητες, με άλλα λόγια, πρέπει να έχουν ηλεκτρονική παιδεία ώστε να μπορούν να κάνουν τις απαραίτητες ρυθμίσεις στην πολιτική απορρήτου. Σε ένα ηλεκτρονικό ερωτηματολόγιο με 630 χρήστες Facebook, διαπιστώσαμε ότι οι άνθρωποι που περνούν περισσότερο χρόνο στο Facebook και έχουν αλλάξει τις ρυθμίσεις απορρήτου πιο συχνά αναφέρουν ότι έχουν περισσότερη ηλεκτρονική παιδεία για την προστασία της ιδιωτικής τους ζωής. Τα άτομα με μεγαλύτερη παιδεία στον τομέα της ιδιωτικής ζωής, με τη σειρά τους αισθάνονται πιο ασφαλή στο Facebook και εφαρμόζοντας παρόμοιους κανόνες προστασίας της ιδιωτικής τους ζωής. Η έρευνα καταλήγουμε στο συμπέρασμα ότι η εμπειρία του Διαδικτύου οδηγεί σε μεγαλύτερη ηλεκτρονική παιδεία για την προστασία και της ιδιωτικής ζωής, γεγονός που προάγει μια πιο επιφυλακτική συμπεριφορά απορρήτου στα ΜΚΔ (11: Bartsch 2016:147-154) .

Σε ένα συμπόσιο για την ασφάλεια και την ιδιωτικότητα που έγινε το 2012 μια επιστημονική επιτροπή της IEEE συνέταξε μια αναφορά που αναφερόταν στην έλλειψη αυτών των χαρακτηριστικών. Συγκεκριμένα η επιτροπή μελέτησε την περίπτωση 8 μεγάλων sites, μεταξύ αυτών το Facebook και το PayPal, που χρησιμοποιούν SSO (Single Sign on) για την αυθεντικοποίηση εισόδου (δηλαδή η καταχώρηση ενός username και password). Συγκεκριμένα μελέτησαν τη ροή δεδομένων προς τα sites μέσα από browsers και χρησιμοποιώντας έναν αλγόριθμο κατέληξαν στο συμπέρασμα ότι υπάρχουν πολλά τρωτά σημεία στα οποία μπορεί κάποιος να τα εκμεταλλευτεί κακόβουλα και να εισχωρήσει στο σύστημα σαν χρήστης – θύμα. Η μελέτη καταλήγει ότι το μέλλον προμηνύεται ιδιαίτερα ανησυχητικό χρησιμοποιώντας τεχνικές SSO και προτρέπει για μεγαλύτερης κλίμακας έρευνα. (101: Wang 2012).

Μια άλλη πολύ σημαντική πτυχή του κίνδυνου της απώλειας της ιδιωτικότητας είναι ο εντοπισμός θέσης. Έρευνα που έκανε το **Associated Press** οδήγησε στο συμπέρασμα ότι ακόμη κι αν κάποιος απενεργοποιήσει τον εντοπισμό τοποθεσίας στις εφαρμογές της **Google** που τρέχουν σε συσκευές **Android** και **iPhones**, η Google συνεχίζει τον εντοπισμό της τοποθεσίας του. Αν και δεν είναι λίγες οι φορές που ακούει κανείς περί παραβίασης προσωπικών δεδομένων, δύσκολα μπορεί να κατανοήσει πώς αυτό επηρεάζει την καθημερινότητα του. Έχοντας κάποιος στα χέρια του ένα «έξυπνο κινητό», δεν μπορεί να συνειδητοποιήσει απόλυτα ότι προσφέρει κυριολεκτικά στο πιάτο όλες τις προσωπικές πληροφορίες του. Ακόμα πιο δύσκολα μπορεί να κατανοήσει, πόσο πολύ αυτές αξίζουν. Ενεργοποιώντας την εύρεση κινητού ή την παρακολούθηση της γεωγραφικής θέσης του (tracking) για να κάνει τη ζωή του πιο εύκολη, βρίσκοντας ένα κοντινό μαγαζί ή επιλέγοντας την πλοήγηση, ώστε να φτάσει στον προορισμό του, ουσιαστικά βρίσκεται απόλυτα εκτεθειμένος. Αυτό τουλάχιστον καταγγέλλουν επτά ευρωπαϊκές χώρες, μεταξύ αυτών και η Ελλάδα. Συγκεκριμένα, οργανώσεις καταναλωτών της Ολλανδίας, της Σουηδίας, της Τσεχίας, της Πολωνίας, της Νορβηγίας, της Σλοβενίας και της Ελλάδας στοχοποιούν τη Google, κατηγορώντας την ότι «χρησιμοποιεί αυτά τα δεδομένα για μια ευρεία γκάμα σκοπών, μεταξύ άλλων για στοχευμένη διαφήμιση, χωρίς όμως να ενημερώνει τους χρήστες με σαφήνεια τί σημαίνει αυτό όσον αφορά τα προσωπικά δεδομένα τους». Το τέλειο παράδειγμα είναι όταν εκφράζετε τις επιλογές σας, διαβάζετε τις προτιμήσεις και αποφασίζετε ότι δεν θέλετε να εισάγετε τοποθεσία, αλλά κάποια εταιρεία μπορεί ακόμα να σας εντοπίσει. Αυτό ξεπερνάει τις λογικές προσδοκίες των ανθρώπων», λέει η Φρέντερικ Καλτχάινερ, εκπρόσωπος των οργανώσεων «Data Privacy Lead» και «Privacy International».Μεταξύ άλλων, το Associated Press βρήκε ότι η Google κρατά την τοποθεσία σας όταν ανοίγετε την εφαρμογή Google Maps, ακόμη κι αν έχετε τον εντοπισμό τοποθεσίας απενεργοποιημένο. (7: Associated Press : 2018)

5.1 Προϋποθέσεις διασφάλισης προσωπικού απορρήτου

Τα ιδανικά ΜΚΔ θα πρέπει να πληροί τις ακόλουθες απαιτήσεις απορρήτου:

1. **Εμπιστευτικότητα από άκρο σε άκρο**: Όλες οι ανταλλαγές δεδομένων πρέπει να είναι εμπιστευτικές και μόνο ο αποστολέας και ο παραλήπτης πρέπει να έχουν πρόσβαση στα δεδομένα.

2. **Προστασία προσωπικών δεδομένων***:* Οι προσωπικές πληροφορίες ενός χρήστη δεν πρέπει να αποκαλύπτονται σε κανέναν εκτός από εκείνες που ρητά αναφέρει ο χρήστης.

3. **Έλεγχος πρόσβασης**: Οι χρήστες θα πρέπει να είναι σε θέση να διαχειρίζονται τα στοιχεία ελέγχου πρόσβασης και τα χαρακτηριστικά των προφίλ τους. Θα πρέπει επίσης να επιτρέπεται στους χρήστες να χορηγούν άδεια σε άλλον χρήστη ή σε ομάδα χρηστών.

4. **Έλεγχος ταυτότητας**: Για να ικανοποιηθούν οι προηγούμενες απαιτήσεις, ο παραλήπτης ενός μηνύματος θα πρέπει να είναι σε θέση να πιστοποιεί τον αποστολέα του μηνύματος.

5. **Ακεραιότητα δεδομένων**: Για κάθε ανταλλασσόμενο μήνυμα, είτε πρόκειται για απάντηση είτε για εκπλήρωση κάποιου αιτήματος, πρέπει να διεξαχθεί έλεγχος ταυτότητας προέλευσης και τροποποίησης.

6.**Διαθεσιμότητα**: Τα δημόσια δεδομένα πρέπει να είναι πάντα διαθέσιμα και όλα τα μηνύματα πρέπει να παραδίδονται έγκαιρα(84: Rathor 2013: 59 – 65).

5.2 Παράγοντες αντιστάθμισης σε σχέση με την ιδιωτική ζωή

Οι μέθοδοι ελέγχου πρόσβασης σε πολλά ΜΚΔ είναι πολύ αδύναμες. Υπάρχει ανάγκη να επιτευχθεί αντιστάθμιση μεταξύ της ιδιωτικής ζωής και των ακόλουθων παραγόντων :

1. **Αναζήτηση Κοινωνικού Δικτύου:** Να αποκρύπτονται όλες τις πληροφορίες του προφίλ ενός χρήστη, αλλά να επιτρέπονται η χρήση με κοινωνική αναζήτηση. Η ίδια περίπτωση είναι για το πέρασμα του προφίλ του φίλου.

2. **Αλληλεπίδραση κοινωνικού δικτύου:** Υπάρχει κίνδυνος της ιδιωτικής ζωής μέσω κοινών φίλων. Μέσω πληροφοριών χρηστών, όπως για παράδειγμα το όνομα του σχολείου , τα ενδιαφέροντα κ.λπ., μπορεί να εκτίθενται μέσω του προφίλ των φίλων τους.

3. **Εξόρυξη Δεδομένων:** Τα δεδομένα ΜΚΔ μπορούν να μελετηθούν για την ανάλυση κοινωνικών συμπεριφορών . Η αφαίρεση ιδιωτικών δεδομένων , μειώνει την ακρίβεια του αποτελέσματος (49: Jordaan 2017:90 – 96).

5.3 Ανησυχία των χρηστών

Σε αντίθεση με αυτή την πεποίθηση, πρόσφατη μελέτη που πραγματοποίησε ομάδα ερευνητών έδειξε ότι τα άτομα που εγκατέλειψαν το Facebook το κάνουν επειδή ανησυχούν για την ιδιωτικότητά τους. Στην πραγματικότητα, τα αποτελέσματά τους έδειξαν ότι τα προβλήματα προστασίας της ιδιωτικής ζωής υπερβαίνουν τα προφανή πλεονεκτήματα του Facebook και ότι αυτές οι ανησυχίες οδήγησαν τελικά αυτά τα άτομα να εγκαταλείψουν το Facebook (95: Stieger 2013) . Αυτή η συμπεριφορά θα πρέπει να είναι ιδιαίτερα σημαντική για το Facebook ως πλατφόρμα, λαμβάνοντας υπόψη την αναφερθείσα πτώση των χρηστών τα τελευταία χρόνια, ειδικά στις ανεπτυγμένες χώρες (35: Garside 2013) .

Μια άλλη οπτική σε σχέση με την (μη) διαφύλαξη της ιδιωτικότητα προτάσσει το Facebook καθώς όταν συνδέεται ένας χρήστης για πρώτη φορά, ενημερώνει το δίκτυο για το ποιος είναι, και εκείνο σου "λέει" ποιους άλλους χρήστες είναι πιθανό να γνωρίζεις στον ψηφιακό κόσμο. Ωστόσο, ο αλγόριθμος του Facebook ξεπερνά κάθε ανθρώπινη λειτουργία γνωριμίας. Τα αποτελέσματα του αλγορίθμου που σχετίζεται με το περίφημο "People You May Know" είναι καθόλου μα καθόλου προβλέψιμα ή αναμενόμενα. Πίσω από το προφίλ που "χτίζει" κανείς, λειτουργεί εν αγνοία του ένα δεύτερο, "σκιώδες προφίλ" που δημιουργείται από το inbox και την κινητικότητα στα smartphones του κάθε χρήστη, αλλά και από τις σελίδες που επισκέπτεται οι οποίες είναι σε σύνδεση με λειτουργίες του Facebook. Οι πληροφορίες που εντάσσονται στην κατηγορία των "Shadow contact information" είναι μια νέα λειτουργία του Facebook την οποία ο περισσότερος κόσμος αγνοεί μιας και το Facebook δεν έκριναν πως ήταν αναγκαίο να ενημερώσουν για κάτι τέτοιο, μέχρι σήμερα (43: Hill 2018).

Σημειώνεται επίσης πως ο ιδρυτής του Facebook ενδέχεται να βρεθεί ενώπιον δικαστηρίου καθώς ο ομοσπονδιακός δικαστής των Ηνωμένων Πολιτειών αποφάσισε ότι θα πρέπει να ασκηθεί αγωγή εις βάρος του μέσου κοινωνικής δικτύωσης, καθώς το τελευταίο έκανε

παράνομη χρήση της διαδικασίας αναγνώρισης προσώπου (face tagging) στις φωτογραφίες των χρηστών, χωρίς την άδεια τους (40: Griffin *2018*).

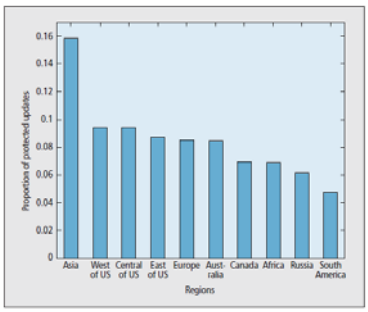
Η Ευρωπαϊκή ένωση είναι πολύ θορυβημένη από τις κινήσεις του Facebook. Συγκεκριμένα ο Βρετανός επικεφαλής της Επιτροπής που ερευνά σε βάθος τις δραστηριότητες του Facebook στην Ευρώπη αιτιολόγησε την απόφασή του να δημοσιοποιήσει απόρρητα email λέγοντας ότι το ενδιαφέρον του κοινού είναι τεράστιο αφενός, ενώ τα εν λόγω email εγείρουν μεγάλα ερωτηματικά για το πως διαχειρίζεται η εταιρεία τα προσωπικά δεδομένα των χρηστών, πως εκμεταλλεύεται την κυρίαρχη θέση της στην αγορά, αλλά και τον τρόπο με τον οποίο συνεργάζεται με τους δημιουργούς εφαρμογών.
Στις 250 σελίδες των κειμένων που δόθηκαν στη δημοσιότητα μαθαίνουμε πράγματα ικανά να εξοργίσουν και τον πιο "ορκισμένο" φανατικό χρήστη του Facebook.
- Αν νομίζατε ότι το Facebook σταμάτησε να διαμοιράζει τα προσωπικά δεδομένα σας μετά την αναβάθμιση της περιόδου 2014-15 απατάσθε. Μπορεί να άλλαξε μεν τις πολιτικές του για το θέμα, συνέχισε ωστόσο να μοιράζεται μέρος των προσωπικών δεδομένων με εταιρείες όπως το Netflix.
- Ξέρει πολύ καλά τι κάνει όταν μοιράζεται τα προσωπικά μας δεδομένα και το κάνει με πλήρη επίγνωση. Και απλώς τα στελέχη του δεν νοιάζονταν καν για τον ξεσηκωμό που θα προκαλούσε μία τέτοια αποκάλυψη.
- Κάποια στιγμή τα στελέχη του σκέφτηκαν ακόμη και να προχωρήσουν σε πώληση των προσωπικών δεδομένων των χρηστών, με ... διαφημιστικά ανταλλάγματα.
- Σε μία περίπτωση αναβάθμισης της εφαρμογής για το Android, προσπάθησε πολύ συνειδητά να κρύψει το γεγονός ότι ο σχεδιασμός επέτρεπε την καταγραφή των κλήσεων και των μηνυμάτων των χρηστών (91: *S*loane 2018).

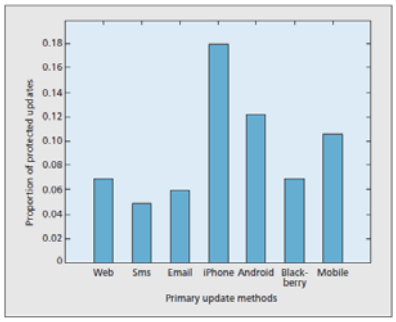
Σύμφωνα με δημοσίευμα των New York Times, νέες αποκαλύψεις έχουν προκύψει καθώς το Facebook επέτρεψε στη μηχανή αναζήτησης της Microsoft να βλέπει τα ονόματα σχεδόν όλων των φίλων των χρηστών του Facebook χωρίς τη συγκατάθεσή τους, ενώ έδωσε και τη δυνατότητα σε Netflix και Spotify να διαβάζουν τα προσωπικά μηνύματα των χρηστών. Στην περίπτωση του Spotify, η εταιρεία συνδέθηκε με τα παράθυρα συνομιλίας χρηστών για να στείλει τραγούδια στους φίλους τους.
Ακόμη, επέτρεψε στην Amazon να αποκτήσει ονόματα χρηστών και πληροφορίες επικοινωνίας μέσω των φίλων τους, και έδωσε ακόμη πρόσβαση στη Yahoo να διαβάζει τις αναρτήσεις φίλων χρηστών, παρά τις δημόσιες ανακοινώσεις της εταιρείας ότι είχε σταματήσει τον διαμοιρασμό.
Συνολικά εμπλέκονται 150 εταιρείες με τα προσωπικά δεδομένα να διαμοιράζονται χωρίς τη συγκατάθεση των εμπλεκομένων.
Οι δημοσιογράφοι των Times μίλησαν με 50 πρώην υπαλλήλους της Facebook και κρατικούς αξιωματούχους. Παράλληλα, είχαν πρόσβαση σε 270 σελίδες απόρρητων εγγράφων. Ανάμεσα δε στις εταιρείες που είχαν άδεια πρόσβασης σε ευαίσθητα δεδομένα,

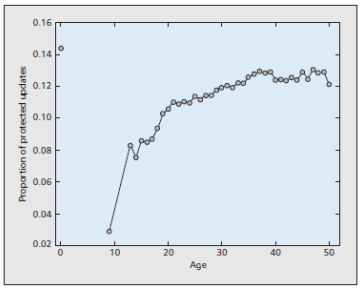
ακόμη και προσωπικά μηνύματα, φέρεται να είναι και η Royal Bank of Canada. Το δημοσίευμα αναφέρει πως ακόμη και "κλειδωμένα" thread συζητήσεων, "ξεκλείδωναν" για χάρη των εταιρειών.
Σημειώνεται πως από πέρυσι είναι γνωστό πως οι εταιρείες Sony, Amazon και Microsoft, είχαν πρόσβαση σε διευθύνσεις email χρηστών, μέσω των λογαριασμών των φίλων τους στην πλατφόρμα κοινωνικής δικτύωσης.
Οι συμφωνίες περιελάμβαναν και 60 κατασκευαστές smartphones, συμπεριλαμβανομένης της Apple και της Huawei. Η Apple, σύμφωνα με τα ίδια στοιχεία, μπορούσε να "δει" επαφές και καταχωρίσεις χρηστών, ακόμη κι αν ήταν "ιδιωτικές". Επίσης, χωρίς να "ζητά" από τον χρήστη δεδομένα, μπορούσε να τα καταγράφει και να τα καταχωρεί.
Ακόμη, το Facebook εμφάνιζε ως "προτεινόμενους φίλους", χρήστες των οποίων τα στοιχεία είχαν καταχωρηθεί σε άλλους κολοσσούς με τους οποίους "συνεργάστηκε" στο σκάνδαλο που φέρνουν στη δημοσιότητα οι New York Times (44: Jackson 2018).

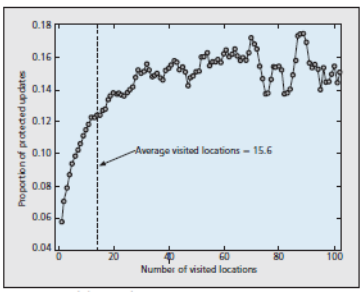
5.4 Έρευνες σχετικά με την ιδιωτικότητα

Ένα ερώτημα που προκύπτει είναι αν όλοι οι άνθρωποι στον κόσμο εμφανίζουν κοινά χαρακτηριστικά σε σχέση με την αντίληψη που έχουν για τους της ιδιωτικότητας, της εμπιστοσύνης ή της ασφάλειας. Σε έρευνα λοιπόν που διεξήχθη σε δείγμα 75.000 ανθρώπων και διήρκεσε 21 μήνες ανέδειξε ότι οι άνθρωποι αντιλαμβάνονται διαφορετικά τα παραπάνω χαρακτηριστικά ανάλογα με το φύλο την ηλικία, την χώρα καταγωγής αλλά και το κοινωνικό – πνευματικό υπόβαθρο του καθενός. Έτσι για παράδειγμα οι κάτοικοι ασιατικών χωρών δείχνουν μεγαλύτερη σπουδή για την ασφάλεια, ενώ εν γένει άνθρωποι μεγαλύτερης ηλικίας δείχνουν μεγάλη προσοχή σε θέματα ιδιωτικότητας σε σχέση με τους νέους. Διαφορές παρατηρούνται επίσης και ανάλογα με το μέσο που χρησιμοποιούν(υπολογιστής ή κινητό) ή και το είδος του λειτουργικού(ios ή android κ.α. Όλα τα παραπάνω αποτυπώνονται στα παρακάτω γραφήματα (Εικόνα 17) (60: Li 2010:20–25).









Εικόνα 17

Τα ψηφιακά μας δεδομένα τα οποία έχουμε αποθηκευμένα στα ΜΚΔ μπορούν να χρησιμοποιηθούν ώστε να εξαχθούν συμπεράσματα σχετικά με το φύλο ή την ηλικία μας, τον σεξουαλικό μας προσανατολισμό, την εθνικότητα μας, τις πολιτικές ή θρησκευτικές μας πεποιθήσεις, αλλά και άλλα χαρακτηριστικά της προσωπικότητας μας, της νοημοσύνης της ευτυχίας μας. Αυτά προκύπτουν από σχετική έρευνα που έγινε σε δείγμα 58.000 εθελοντών οι οποίοι παρείχαν τα likes τους ως στοιχείο προς ανάλυση σε μια έρευνα. Το μοντέλο που επεξεργάστηκε τα στοιχεία αυτά έδειξε ότι με ακρίβεια 88% μπορεί να διακρίνει σεξουαλικές προτιμήσεις (ετεροφυλία ή ομοφυλοφιλία), 95% καταγωγή και σε ποσοστό 85% πολιτικές πεποιθήσεις. Η έρευνα καταλήγει στο ότι μπορούν να εξαχθούν συμπεράσματα εξίσου όχι μόνο από likes αλλά και από το ιστορικό ή τα στοιχεία αναζήτησης στο διαδίκτυο. Επίσης τα χαρακτηριστικά τα οποία μπορούν να προβλεφθούν έχουν να κάνουν και σε προτιμήσεις σε προϊόντα (55: Kosinski: 2013) .

Σε μια άλλη έρευνα μελετήθηκε το πρόβλημα της χρήσης τοποθεσιών στα ΜΚΔ. Η έρευνα έδειξε ότι σε ποσοστό 56,3 % μπορεί να προβλεφτεί ο τόπος κατοικίας των χρηστών μέσα από σύγκριση παρόμοιων θέσεων των φίλων των χρηστών. Ακόμα, χαρακτηριστικά τα οποία πιθανόν δεν αποκαλύπτουμε, όπως για παράδειγμα ηλικία ή ημερομηνία γέννησης, μπορεί μέσα από τον κατάλογο των φίλων να προβλεφτεί και μάλιστα με ακρίβεια που ξεπερνά το 94% (58: Labitzke 2013:13-24) .

Μια άλλη οπτική γύρω από την ασφάλεια και ιδιωτικότητα δίνει μια μελέτη στην οποία τίθεται ένα ερώτημα – υπόθεση ίσως και διαπίστωση ότι καθώς η τεχνολογία μετατοπίζει όλο και μεγαλύτερο μέρος της κοινωνικοποίησης και της διαχείρισης σχέσεων στο διαδίκτυο, οι άνθρωποι ίσως αναπτύσσουν απόψεις περί ιδιωτικότητας οι οποίες να μη

θεωρούνται τόσο αυστηρές (45: James 2015:893-908) . Αυτή η άποψη ταυτίζεται με την πεποίθηση του ιδρυτή του Face book (35).

Κεφάλαιο 6.Third- party

Σε μια πολύ σημαντική έρευνα απασχολεί το ζήτημα των προσωπικών δεδομένων που διακινούνται αλλά δεν αφορά μόνο τα πρόσωπα αυτά αλλά και τρίτους. Για παράδειγμα μια φωτογραφία παιδιών σε μια γιορτή η οποία εκτίθεται στα ΜΚΔ δεν αφορά μόνο αυτόν που την προώθησε αλλά και τα υπόλοιπα παιδιά που βρίσκονται στην κοινή αυτή φωτογραφία. Ειδικά ορίζεται η έννοια της αντίληψης του "κοινού κινδύνου" ο οποίος αποτελείται από δύο συστατικά: την αυστηρότητα των πληροφοριών που εκθέτουν οι άλλοι και την ευαισθησία των άλλων σε πληροφορίες που εκτίθενται από τους χρήστες των ΜΚΔ (97: Tabitha 2017: 851-865).

Ένα πολύ ενδιαφέρον στοιχείο που πρέπει να δοθεί ιδιαίτερη προσοχή είναι η νομοθεσία των ΗΠΑ σχετικά με την καταχώρηση δεδομένων σε third – party επιχειρήσεις. Οι επιχειρήσεις αυτές, σύμφωνα με τον κανόνα 34 των Ομοσπονδιακών Κανόνων Πολιτικής Δικονομίας, είναι υποχρεωμένες να διατηρούν τα αρχεία που συλλέγουν από τα κοινωνικά μέσα, συμπεριλαμβανομένων των μεταδεδομένων και του σχετικού περιεχομένου των συνδέσμων , μπορούν να ζητήσουν για να πάρουν στην κατοχή τους "οποιαδήποτε καθορισμένα έγγραφα ή ηλεκτρονικά αποθηκευμένες πληροφορίες που αποθηκεύονται σε οποιοδήποτε μέσο από το οποίο μπορούν να ληφθούν πληροφορίες είτε άμεσα είτε, εάν είναι απαραίτητο, μετά από μετάφραση από το ανταποκρινόμενο μέρος ". Ένας άλλος κανόνας από τον Ομοσπονδιακό Κανόνα της Πολιτικής Δικονομίας, είναι ο κανόνας 26, ο οποίος απαιτεί όλες οι πληροφορίες που μπορούν να εντοπιστούν να "πρέπει να διατηρηθούν και να παραχθούν, εφόσον ζητηθεί από τον αντίδικο, οπότε είναι σαφές ότι υπάρχει νόμιμο καθήκον να διατηρούνται τα αρχεία κοινωνικών μέσων" (92: Smallwood 2014:119 -120).

Επιπρόσθετα οι Third – party εφαρμογές μπορούν να δώσουν πρόσβαση σε ένα μεγάλο πλήθος δεδομένων των χρηστών. Σε μια μελέτη των Felt & Evans (33: Felt 2008) έδειξε ότι σε 150 εφαρμογές ήταν απαραίτητα μόνο το όνομα, οι φίλοι και το δίκτυο για να αποκτήσει κάποιος πρόσβαση. Ωστόσο το 91% των εφαρμογών των ΜΚΔ έχει πρόσβαση σε δεδομένα τα οποία δεν είναι χρήσιμα για τη λειτουργία των εφαρμογών αυτών (1: Abdukader 2016: 20-27) .

Μια άλλη οπτική παρουσιάζεται σε έρευνα στην οποία αναδεικνύεται ο θετικός ρόλος των ΜΚΔ καθώς μέσα από εφαρμογές third – parties μπορούν να ολοκληρωθούν ταχύτερα κάποιες ειδικές εργασίες περισσότερο αποδοτικά. Έτσι λοιπόν αφού επιλυθούν προβλήματα ασφαλείας και διαφύλαξης της ιδιωτικότητας θα πρέπει οι χρήστες να ενθαρρύνονται προς αυτή την κατεύθυνση μέσω κινήτρων και ανταμοιβής (100: Wang 2018: 15–27) .

Σε έρευνα που διενεργήθηκε σε δείγμα 260 ατόμων σχετικά με την ασφάλεια και ιδιωτικότητα που νιώθουν σε σχέση με το Facebook διαπιστώθηκε ότι αν και λαμβάνουν μέτρα σε ποσοστό 95% σε μη «φιλικά» πρόσωπα υπάρχει ένα ποσοστό 16,5% το οποίο έχει κάνει ανάρτηση τουλάχιστον μια φορά κάτι για το οποίο νιώθουν άβολα με συγκεκριμένους φίλους – οι οποίοι είχαν την δυνατότητα να δουν τη συγκεκριμένη ανάρτηση – και ένα ποσοστό 37% το οποίο εξέφρασε γενικότερες ανησυχίες με την ανάρτηση ή διακίνηση πληροφοριών με φίλους. Η έρευνα καταλήγει σε ένα πολύ σημαντικό συμπέρασμα: αν και οι χρήστες χρησιμοποιώντας τα διάφορα εργαλεία καταφέρνουν σε μεγάλο βαθμό να διασφαλίσουν την ιδιωτικότητά τους σε σχέση με το άγνωστο κοινό, εντούτοις δεν συμβαίνει το ίδιο με μέλη – φίλους οι οποίοι δυναμικά γίνονται ακατάλληλο κοινό για αναρτήσεις (48: Johnson 2012) .

Κεφάλαιο_7.Πολιτικές απορρήτου

Η ρύθμιση της πολιτικής απορρήτου είναι μια πολύ πολύπλοκη υπόθεση ακόμα και γι' αυτούς που έχουν ειδική κατάρτιση ως διαχειριστές υπολογιστικών συστημάτων (63: Madejski 2012). Κάποιοι επιστήμονες θεωρούν μάλιστα ότι ανάλογα με τις ρυθμίσεις απορρήτου και την γνώση που αποκτούν οι χρήστες με τον καιρό για τα ΜΚΔ διαφοροποιεί τις απόψεις σχετικά με την εμπιστοσύνη και τον εθισμό σε αυτά(59: Lankton 2012). Η πολιτική απορρήτου είναι ένα πολύπλοκο ζήτημα. Δεν είναι τυχαίο όταν τον Μάιο του 2010 η ηλεκτρονική σελίδα του CNN έκανε ένα λογοπαίγνιο για το ποιο κείμενο είναι μεγαλύτερο: το Σύνταγμα των ΗΠΑ ή η πολιτική απορρήτου του Facebook; Η απάντηση είναι το δεύτερο όσο αστείο και αν ακούγεται. Το Facebook έχει πάνω από 400 εκατομμύρια χρήστες (σήμερα είναι πάνω από 2,2 δισεκατομμύρια σε όλο τον κόσμο) εκ των οποίων οι μισοί συνδέονται καθημερινά αφιερώνοντας χρόνο δισεκατομμύρια λεπτά στο site κάθε μήνα. Η πολιτική απορρήτου έχει αναθεωρηθεί προς όφελος των χρηστών ώστε να είναι πιο ασφαλείς. Στην προσπάθεια λοιπόν οι χρήστες να κρατήσουν τα προσωπικά τους δεδομένα μακριά από την κοινή θέα στην πραγματικότητα γίνονται περισσότερο δημόσια εξ' ορισμού. Τώρα μοιράζονται μέσω τρίτων (Third parties). Στη νέα αυτή πολιτική απορρήτου, συνεχίζει το άρθρο, αν κάποιος χρήστης θέλει να αποκλείσει την

πλήρη αποκάλυψη προσωπικών δεδομένων θα πρέπει να κάνει κλικ σε περισσότερα από 50 κουμπιά τα οποία στη συνέχεια απαιτούν συνολικά 170 επιλογών. Το "Κέντρο βοήθειας" του Facebook είναι διαθέσιμο για να βοηθήσει τους χρήστες, αλλά η καταμέτρηση λέξεων για τις Συχνές Ερωτήσεις σχετικά με την προστασία της ιδιωτικής ζωής προσθέτει περισσότερες από 45.000 λέξεις. Αυτό δείχνει λοιπόν πόσο σύνθετο (αν και όχι τυχαία) είναι η προσωπική ρύθμιση απορρήτου. Ο μοναδικός τρόπος έκθεσης είναι η ολική διαγραφή προσωπικών δεδομένων (14: BILTON 2010).

Οι ίδιοι οι προγραμματιστές παραβιάζοντας την πολιτική απορρήτου μπορούν να ελέγχουν τα δεδομένα των χρηστών. Οι πολιτικές απορρήτου υποτίθεται ότι απαγορεύουν την κατάχρηση πληροφοριών από χρήστες. Αυτό όμως δεν τηρείται πάντα καθώς στην εφαρμογή του Facebook "Top friends" επέτρεπε στην καθένα να δει ημερομηνία γέννησης, φύλο και το κοινωνικό προφίλ των χρηστών ενώ επέτρεπε και όλες τις επιθέσεις που αναφέραμε για τα ΜΚΔ.

Σε μια εμπειρική έρευνα που διεξήγαγε το πανεπιστήμιο Κολούμπια σε δείγμα 65 φοιτητών αποδείχτηκε ότι σε όλες τις περιπτώσεις υπήρξε τουλάχιστον μια παραβίαση στον λογαριασμό τους με αποτέλεσμα είτε να αποκαλυφθεί κάτι το οποίο ο χρήστης ήθελε να μείνει ιδιωτικό ή κάτι που ήθελε να μοιραστεί με άλλους χρήστες έγινε ιδιωτικό. Η έρευνα καταδεικνύει ότι το σημαντικότερο πρόβλημα είναι η ρύθμιση απορρήτου. Αυτό οφείλεται τόσο στους χρήστες που δεν δίνουν την απαιτουμένη σημασία σε αυτό αλλά και στο ίδιο το Facebook που προσεγγίζει λανθασμένα το πρόβλημα χωρίς να δείχνει διάθεση να βοηθήσει τους χρήστες σε αυτό (64: Madejski 2011).

7.1 Παραδείγματα παραβίασης απορρήτου

Πολύ συχνά οι χρήστες των ΜΚΔ αντιμετωπίζουν ιδιαίτερες δυσκολίες στο να ξεχωρίσουν την ιδιωτική από την επαγγελματική ζωή με αποτέλεσμα να μοιράζονται επαγγελματικές πληροφορίες σε προσωπικούς λογαριασμούς των ΜΚΔ. Έτσι για παράδειγμα στρατιώτης του Ισραηλινού στρατού αποκάλυψε το 2009 επιχείρηση μέσω Facebook. Ομοίως ένας Αμερικάνος το 2010, μέλος της επιτροπής ελέγχου για το Ιράκ εξέθεσε την αποστολή και ολόκληρο το ταξίδι καταγράφοντας με το κινητό του σημεία της Βαγδάτης τα οποία επισκεπτόταν. Αυτό λοιπόν καταδεικνύει μια άλλη πολύ σημαντική πτυχή των ΜΚΔ όπου οι χρήστες πολλές φορές αποκαλύπτουν πληροφορίες ή μυστικά από την επαγγελματική τους ιδιότητα τα οποία μπορεί να τύχουν εκμετάλλευσης από πολλούς αποδέκτες. Θα ήταν

χρήσιμο λοιπόν να δούμε ποιοι παράγοντες επηρεάζουν τους εργαζομένους στο να αποκαλύπτουν πληροφορίες της επιχείρησης. Μεταξύ αυτών είναι η ύπαρξη ενός εντύπου που αφορά στην πολιτική απορρήτου της κάθε επιχείρησης και κατά πόσο αυτό είναι κατανοητό και εις γνώσιν από όλο το προσωπικό καθώς και η γνώση γύρω από την ασφάλεια και τους κινδύνους της απώλειας αυτής. Έτσι θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί σε πληροφορίες που αφορούν κόστη, τιμές, κερδοφορία, μέθοδοι παραγωγής, προϊόντα υπό ανάπτυξη και γενικά σε οτιδήποτε έχει να κάνει με τη στρατηγική της επιχείρησης (70: Molok 2011).

Αν και οι ρυθμίσεις απορρήτου είναι γνωστές στο ευρύ κοινό η συντριπτική πλειοψηφία των χρηστών διατηρεί τις αρχικές - βασικές ρυθμίσεις απορρήτου χωρίς να κάνει εξατομικευμένη ρύθμιση. Σε έρευνα λοιπόν του πανεπιστημίου του Τορίνο γύρω από τις επιπτώσεις της αποκάλυψης προσωπικών δεδομένων αναδεικνύει ότι το καλύτερο όπλο για την προστασία των δεδομένων είναι οι χρήστες μεταξύ τους. Έτσι με τη συμπεριφορά τους, μην δημοσιεύοντας προσωπικά στοιχεία δικά τους ή λογαριασμών φίλων τους είναι η καλύτερη προστασία της ιδιωτικότητας (15: Bioglio 2017, 28 – 37) .

Κεφάλαιο 8 .Θέματα που αφορούν τα ίδια τα μέσα

Μια άλλη πολύ ενδιαφέρουσα έρευνα έδειξε ότι ακόμα και αν οι χρήστες των ΜΚΔ έχουν λάβει τα μέτρα τους για την προστασία προσωπικών δεδομένων εφαρμόζοντας αυστηρούς ελέγχους απορρήτου, εντούτοις τα ίδια τα ΜΚΔ εγγενώς λόγω αδυναμιών τους μπορούν να αποκαλύψουν πληροφορίες. Ως παράδειγμα η εν λόγο έρευνα φέρνει την περίπτωση δυο χρηστών – φίλων στο Facebook: του Bob και της Alice. Αν η Alice, αν και είναι φίλη με τον Bob, δεν του επιτρέπει να έχει πλήρη πρόσβαση στον κατάλογο των φίλων της εφαρμόζοντας πολιτικές απορρήτου τότε χρησιμοποιώντας μια υπηρεσία του Facebook που λέγεται " Άτομα που ίσως γνωρίζεται" δίνει τη δυνατότητα στον Bob να έχει πλήρη πρόσβαση στον κατάλογο των φίλων της Alice την οποία δεν είχε αρχικά. Έτσι έμμεσα λόγω αδυναμίας του ΜΚΔ ο χρήστης αποκτά πρόσβαση σε δεδομένα για τα οποία δεν έχει πρόσβαση αρχικά (61: Li 2014: 239–254).

Σε όλες τις μελέτες σχετικά μια το απόρρητο και την ιδιωτικότητα δίνεται έμφαση στη συμπεριφορά και τις ανησυχίες των χρηστών, τις πρακτικές και τις ειδοποιήσεις των μέσων καθώς και τους κανονισμούς και τις δηλώσεις σχετικά με αυτό. Δεν γίνεται ποτέ αναφορά λοιπόν για τις απόψεις των διαχειριστών των μέσων σχετικά με το απόρρητο και την ιδιωτικότητα. Σε έρευνα λοιπόν σχετικά με αυτό το ζήτημα έδειξε ότι οι διαχειριστές των μέσων μοιράζονται τις ανησυχίες των χρηστών αναφέρουν ότι οι δικοί τους ιστότοποι δεν παραβιάζουν το ιδιωτικό απόρρητο ενώ τους παρακινούν να παρέχουν προσωπικές πληροφορίες. Η έρευνα έδειξε ότι όσο νεώτεροι είναι οι διαχειριστές των μέσων τόσο λιγότερη ανησυχία εξέφραζαν αλλά ενεργούσαν όλο και περισσότερο για την προστασία της ιδιωτικής ζωής των χρηστών (38: Ginosar 2017: 948-957) .

Οι πάροχοι λοιπόν των ΜΚΔ ενθαρρύνουν τους χρήστες στην ανταλλαγή όλο περισσότερων πληροφοριών μεταξύ τους έτσι ώστε ο τζίρος τους ο οποίος σε μεγάλο βαθμό εξαρτάται από την κοινωνική αλληλεπίδραση των χρηστών αυξάνεται. Σήμερα υπολογίζεται ότι οι χρήστες των ΜΚΔ έχουν κατά μέσο όρο 228 φίλους και συνδέονται σε αυτά 118 λεπτά ημερησίως. Καθώς προστίθενται όλο και περισσότεροι φίλοι στους λογαριασμούς των χρηστών αναδεικνύεται ως πρόβλημα η διαφορετική οπτική που έχουν οι χρήστες μεταξύ τους ως προς την αποκάλυψη πληροφοριών. Για παράδειγμα φωτογραφίες που δείχνουν μια παρέα νεαρών που ξεφαντώνουν σε ένα πάρτι να είναι ευχάριστες για τους συνομήλικους τους, όχι όμως και για τον προπονητή τους σε κάποιο άθλημα ο οποίος διαμορφώνει διαφορετική εικόνα για αυτούς (62: Liu 2018: 1005-1023) . Όσον αφορά την Ελλάδα, όπως προκύπτει από έρευνα της Focus Bari, 4 στα 5 Ελληνόπουλα ηλικίας 5 έως 12 ετών χρησιμοποιούν το Διαδίκτυο. Σημαντικά υψηλότερη διείσδυση στο 89,3% παρατηρείται στα παιδιά 10-12 ετών. Η μέση ημερήσια χρήση του Διαδικτύου στην Ελλάδα είναι 3,1 ώρες, με το 67,7% των Ελλήνων να συνδέεται καθημερινά στο Διαδίκτυο από το κινητό (119: ΣΕΠΑ,2019).

Τα ΜΚΔ πολλές φορές εμφανίζουν ένα παράδοξο: ενώ από τη μια θεωρούν ότι οι χρήστες έχουν τον έλεγχο, και άρα την ευθύνη της ιδιωτικότητας τους για τις πληροφορίες που ανταλλάσσουν με άλλους χρήστες, από την άλλη όσο περισσότερα δεδομένα ανταλλάσσονται τόσο περισσότεροι χρήστες γίνονται μέλη των ΜΚΔ (5: Andrerson 2013: 51 - 60).

Στην περίπτωση του twitter για τους χρήστες που δεν μπορούν να προσελκύσουν άλλους followers με φυσικό τρόπο υπάρχει μια ολόκληρη αγορά με ψεύτικα –πληρωμένα μέλη – followers ενώ υπάρχουν και πυραμίδες με ψεύτικα profils για προσέλκυση νέων μελών (Sybils) (96: Stringhini 2013).

Τα ΜΚΔ αμφισβητούν την έννοια του “προσωπικού χώρου” εννοώντας προσωπικά και ιδιωτικά δεδομένα γίνονται δημόσια με υπαιτιότητα του χρήστη. Για να είμαστε πιο

ακριβείς όπως ισχυρίζονται οι Royer, Deuker and Rannenberg "η έννοια της ιδιωτικότητας έχει μετακινηθεί από κάτι στατικό το οποίο επηρεάζει μόνο αυτή σε μια δυναμική διαδικασία ελέγχου των ορίων που λειτουργεί ανάμεσα στο υποκείμενο και σε αυτό που το περιβάλλει(83: Rannenberg 2009). Αυτό περιπλέκει πολύ τη νομοθεσία γύρω από την προστασία απορρήτου. Μέχρι σήμερα , η νομοθεσία περί απορρήτου προστατεύει το δικαίωμα να ζει κάποιος ειρηνικά και από την άδικη μεταχείριση των προσωπικών δεδομένων που διέπει τη δημοσίευση των προσωπικών δεδομένων στο πλαίσιο στο οποίο αυτή πραγματοποιείται με τη συγκατάθεση των πολιτών. Από την άποψη αυτή, δύο θέματα ξεχωρίζουν ξεκάθαρα: οι γνώστες της ψηφιακής τεχνολογίας , που γεννήθηκαν και μεγάλωσαν σε υπολογιστικό περιβάλλον, έχουν λιγότερη συνείδηση του κινδύνου της ιδιωτική τους ζωής από εκείνους που έρχονται ως ενήλικες στον κόσμο του Διαδικτύου (82: Ragnedda 2013: 43 – 48).

Η Ευρωπαϊκή Επιτροπή θέτει ακόμα μία φορά στο στόχαστρό της τους αμερικανικούς κολοσσούς υψηλής τεχνολογίας και κοινωνικής δικτύωσης Facebook και Twitter, και τους επικρίνει για ολιγωρία στην προστασία των χρηστών. Σύμφωνα με τους Financial Times, εκπρόσωποι της αρμόδιας διεύθυνσης της Κομισιόν προειδοποίησαν τους δύο ομίλους ότι δεν ενημερώνουν με επάρκεια και σαφήνεια τους χρήστες σχετικά με το πότε αποσύρουν περιεχόμενο και πότε διαγράφουν λογαριασμούς από τις πλατφόρμες τους. Κι αυτό σημαίνει πως αν ένας χρήστης κάνει μια ανάρτηση και χωρίς προειδοποίηση και βάσιμη αιτιολογία το Facebook την αποσύρει, τότε παραβιάζει την ευρωπαϊκή νομοθεσία για την προστασία των καταναλωτών. Πέρυσι τον Μάρτιο, η Ευρωπαϊκή Επιτροπή έδωσε εντολή στις προαναφερθείσες πλατφόρμες κοινωνικής δικτύωσης αλλά και στην Google+ να αλλάξουν τους όρους και τις προϋποθέσεις που ισχύουν όταν οι χρήστες αναφέρουν περιστατικά απάτης (αγορές, ψευδείς λογαριασμούς κ.λπ.). Αλλιώς η Κομισιόν έχει το δικαίωμα να προσφύγει στη Δικαιοσύνη κατά των ομίλων και να ζητήσει να διευκρινιστούν οι όροι, βάσει των οποίων αποσύρουν επίμαχο περιεχόμενο. (53b: Khan 2018)

Κεφάλαιο 9.Προσωπικά Δεδομένα – Νομοθεσία

9.1 Γενικά για το GDPR

Από τις 25 Μαΐου του 2018 εφαρμόζεται και στην Ελλάδα ο νέος κανονισμός 679/2016 του Ευρωπαϊκού Κοινοβουλίου σε θέματα προστασίας των ατόμων για την επεξεργασία προσωπικών δεδομένων = General Data Protection Regulation (GDPR) (αντικατάσταση της Οδηγίας 95/46/ΕΚ). Τα νέα στοιχεία που περιέχει αυτός ο κανονισμός αφορούν την ενίσχυση της προστασίας προσωπικών δεδομένων, την εναρμόνιση βασικών κανόνων, την άμεση εφαρμογή σε όλα τα κράτη μέλη το Μάιο του 2018 καταργώντας όλες τις εθνικές νομοθεσίες. Ο νέος αυτός κανονισμός εφαρμόζεται άμεσα (χωρίς να χρειάζεται ψήφιση σε εθνικό επίπεδο), με αποτέλεσμα να υπάρχει μεγαλύτερος βαθμός εναρμόνισης με όλα τα κράτη μέλη (με την Οδηγία 95/46/ΕΚ υπήρχε δυνατότητα διαφοροποίησης).

9.2Βασικές αλλαγές στο νέο νόμο προστασίας δεδομένων προσωπικού χαρακτήρα

Σύμφωνα με το άρ. 2 του ν. 2472/1997 ως Προσωπικά δεδομένα (ή Δεδομένα προσωπικού χαρακτήρα) θεωρούνται κάθε πληροφορία (άμεση ή έμμεση) που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη. Δεν λογίζονται ως προσωπικά δεδομένα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία. Στην πράξη, προσωπικά δεδομένα είναι τα δεδομένα που

αφορούν ένα πρόσωπο και συνδέονται με την ταυτότητά του, όπως για παράδειγμα: το όνομά μας, η διεύθυνσή μας (ταχυδρομική αλλά και ηλεκτρονική – email), το τηλέφωνό μας, τα ενδιαφέροντά μας, οι απόψεις μας, η εικόνα μας (φωτογραφία/video). Επίσης το ψευδώνυμό μας (nickname) σε μία διαδικτυακή υπηρεσία, ακόμα και αν δεν παραπέμπει στο πραγματικό μας ονοματεπώνυμο ,τη IP διεύθυνση του υπολογιστή μας από τον οποίο «σερφάρουμε» δηλαδή κάθε δεδομένο από το οποίο υπάρχει πιθανότητα/περίπτωση να αναγνωριστούμε .

Κάποια προσωπικά δεδομένα χρήζουν ακόμα μεγαλύτερης προστασίας, γιατί εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας όπως ευαίσθητα δεδομένα(τα δεδομένα που αφορούν σε –φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, υγεία, κοινωνική πρόνοια, ερωτική ζωή, ποινικές διώξεις ή καταδίκες, στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις. Τα ευαίσθητα αυτά δεδομένα αποκαλούνται πλέον «προσωπικά δεδομένα ειδικών κατηγοριών». Σε αυτή την κατηγορία ανήκουν πλέον και τα γενετικά δεδομένα βιομετρικά δεδομένα, εφόσον χρησιμοποιούνται για την ταυτοποίηση ατόμου.

Στον GDPR τίθενται σαφείς προϋποθέσεις για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών τότε αν πρόκειται για συγκατάθεση παιδιού θα πρέπει αυτό να είναι τουλάχιστον 16 χρονών (άρ. 8 του GDPR).
◦ Εάν το παιδί είναι ηλικίας κάτω των 16 ετών, η επεξεργασία αυτή είναι σύννομη μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού. Ο υπεύθυνος επεξεργασίας των δεδομένων κοινωνικού χαρακτήρα οφείλει να καταβάλλει εύλογες προσπάθειες για να επαληθεύσει στις περιπτώσεις αυτές ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία. Τα κράτη μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία δεν είναι κάτω από τα 13 έτη.

Σύμφωνα με το άρθρο 17 το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος
επεξεργασίας υποχρεούται να τα διαγράψει χωρίς αδικαιολόγητη καθυστέρηση (εφόσον πληρούται σύνολο προϋποθέσεων). Αυτό σημαίνει ότι, αν ένας οργανισμός έχει δημοσιοποιήσει (νομίμως) προσωπικά δεδομένα και το υποκείμενο των δεδομένων ασκεί σε αυτόν το δικαίωμα στη λήθη, τότε ο οργανισμός οφείλει να φροντίσει να ενημερώσει όσους αναπαρήγαγαν τη δημοσιοποίηση/ανάρτηση ότι πρέπει επίσης να τα διαγράψουν. Με αυτόν τον τρόπο ενισχύεται το δικαίωμα των πολιτών να ζητήσουν διαγραφή των δεδομένων τους, ιδίως δε σε περιπτώσεις αναρτήσεων /δημοσιοποιήσεων. (115: Λιμνιώτης 2018)

Κεφάλαιο 10.Ενδεικτικές Λύσεις

Σε μια άλλη προσέγγιση προτείνεται ως λύση η όσο το δυνατό λιγότερη δημοσίευση προσωπικών πληροφοριών. Σε αυτό το συμπέρασμα κατέληξε η έρευνα ύστερα από επεξεργασία ενός μοντέλου κατά το οποίο μπορεί κάποιος να αντλήσει πληροφορίες για τους χρήστες γνωρίζοντας μόνο τις μουσικές προτιμήσεις των χρηστών (20: CHaabane 2012) .

Τα ΜΚΔ έχουν μια συγκεντρωτική τακτική σύμφωνα με την οποία συλλέγουν πλήθος πληροφοριών για το προφίλ του κάθε χρήστη (συνήθειες, προτιμήσεις, ενδιαφέροντα) ώστε οι διάφορες εταιρείες οι οποίες έχουν συμβόλαια με τα ΜΚΔ να στοχοποιούν πολύ εύκολα τους χρήστες – καταναλωτές. Αυτό κάνει τους χρήστες των ΜΚΔ να μην θεωρούνται ουσιαστικά πελάτες των εταιρειών αυτών αλλά τα ίδια τα προϊόντα (10: Bahri 2018:18 -25) . Εκτός όμως από αυτό, και η ροή των δεδομένων από έναν φίλο στο ΜΚΔ και μετά στον άλλο φίλο, δημιουργεί προβλήματα, όχι μόνο από κακόβουλους (εσωτερικούς και εξωτερικούς) αλλά και από το ίδιο το ΜΚΔ αλλά και από υπηρεσίες third- party. Η Υπηρεσίας Εθνικής Ασφάλειας (NSA) των ΗΠΑ δείχνουν με σαφήνεια τον τρόπο με τον οποίο τα πρακτορεία συγκέντρωσαν τις πληροφορίες των χρηστών αξιοποιώντας τις αδυναμίες της πλατφόρμας ασφαλείας του Facebook . Η λύση που έχει προταθεί είναι η αποκεντρωμένη διαχείριση των χρηστών DOSN (Decentralized Online Social Networks) χρησιμοποιώντας τεχνικές P2P. Οι Diaspora και Friendica είναι οι πιο διάσημες πλατφόρμα DOSNs με πάνω από 670.000 χρήστες και βασίζονται σε δίκτυα ανεξάρτητων διακομιστών που διαχειρίζονται οι χρήστες (27: De Salve 2018 : 154 – 176).

Κάποιες από τις λύσεις που προτείνονται είναι:

Μια ομάδα μελετητών του IEEE συστήνει 8 κανόνες που είναι απαραίτητοι για την προστασία των χρηστών. Αυτοί είναι : 1. Απομάκρυνση προσωπικών πληροφοριών που δεν είναι χρήσιμες 2. Σωστή ρύθμιση ασφάλειας και ιδιωτικότητας 3. Δεν δεχόμαστε αιτήματα φιλίας από αγνώστους 4. Εγκατάσταση λογισμικού ασφαλείας στον Η/Υ 5. Απομάκρυνση εφαρμογών με τρίτα μέρη (Third party) 6. Μη δημοσιοποίηση θέσης 7. Μην εμπιστεύεσαι τους «φίλους» από τα μέσα κοινωνικής δικτύωσης 8. Οι γονείς θα πρέπει να παρακολουθούν την δραστηριότητα των παιδιών τους(34: Fire 2014).

Σε μια άλλη μελέτη σχετικά με την ταχύτατη εξάπλωση των μέσων κοινωνικής δικτύωσης κάνει σαφή διαχωρισμό στην ασφάλεια και την ιδιωτική ζωή. Η ασφάλεια τίθεται σε κίνδυνο όταν ένας κακόβουλος αποκτά μη εξουσιοδοτημένη πρόσβαση σε ένα προστατευόμενο κώδικα ή στην γλώσσα προγραμματισμού ενός ιστότοπου. Τα ζητήματα

ιδιωτικού απορρήτου, τα οποία αφορούν την αδικαιολόγητη πρόσβαση σε ιδιωτικές πληροφορίες, δεν πρέπει απαραιτήτως να συνεπάγονται παραβιάσεις στην ασφάλεια. Κάποιος, μπορεί να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες, απλώς παρακολουθώντας τον κωδικό πρόσβασης μας. Συχνά όμως οι δύο τύποι αυτοί παραβιάσεων συχνά αλληλοσυνδέονται στα κοινωνικά δίκτυα, καθώς παραβιάζοντας το δίκτυο ασφαλείας ενός ιστότοπου μπορείς να αποκτήσεις πρόσβαση σε προσωπικές πληροφορίες οποιουδήποτε χρήστη. Ωστόσο η πιθανή βλάβη σε ένα μεμονωμένο χρήστη προέρχεται από το πόσο αυτός ασχολείται με τα ιστότοπους κοινωνικής δικτύωσης καθώς και με την ποσότητα των προσωπικών δεδομένων που είναι πρόθυμος να μοιραστεί. Η λύση που προτείνεται είναι ένας μετρητής κινδύνου (Security Master) για την ελαχιστοποίηση του κόστους και του μετριασμού του κινδύνου σε ένα επιθυμητό επίπεδο το οποίο μπορούμε να ρυθμίσουμε ανταποκρινόμενο στις αυξημένες ανάγκες των σημερινών δεδομένων. (89: Sahinoglu 2012: 163-169).

Σε ΜΚΔ που τρέχουν σε κινητά οι πληροφορίες των φίλων καθώς και τοποθεσίες αποθηκεύονται σε δύο ξεχωριστούς servers. Οι servers οι οποίοι αποθηκεύουν αυτά τα δεδομένα είναι οι Social Network Server (SNS) and Location Based Server (LBS) και να χρησιμοποιούν πρωτόκολλα κρυπτογράφησης για να παρέχουν την υπηρεσία κατανομής θέσης μεταξύ φίλων και ξένων. Ωστόσο, αυτή η κατανεμημένη αρχιτεκτονική συνεπάγεται μεγάλο κόστος επικοινωνίας μεταξύ SNS και LBS, καθώς και μεγάλο φορτίο αποθήκευσης. Για να ξεπεραστούν τα παραπάνω προβλήματα προτείνεται ένα κεντρικό σύστημα διαμοιρασμού θέσης που προστατεύει την ιδιωτική ζωή, το οποίο ονομάζεται CenLocShare χρησιμοποιώντας μόνο έναν server (LSSNS) (Location-storing Social Network Server). Αυτός χρησιμοποιεί ψεύτικες θέσεις και ειδικά πρωτόκολλα χαρτογράφησης μεταξύ LSSNS και δικτύων κινητής ώστε να επιτυγχάνεται μεγαλύτερη ασφάλεια και ιδιωτικότητα μεταξύ φίλων και όχι μόνο (106: Xiaoa 2017) .

Μια άλλη λύση που προτείνεται από τον Yi Liu είναι “Attribute-based handshake protocol for mobile healthcare social networks” και δίνει μια λύση στο πρόβλημα του πρωτοκόλλου κινητής επικοινωνίας στα δίκτυα ιατρικής περίθαλψης εισάγοντας τον όρο “attribute-based handshake” (ABH). Χρησιμοποιώντας το ABH, οι χρήστες στο κοινωνικό δίκτυο κινητής επικοινωνίας ιατρικής περίθαλψης μπορούν να κάνουν χειραψία (*Three-Way Handshake*: χρησιμοποιείται στα πρωτόκολλα tcp/ip για να ξεκινήσει η επικοινωνία μεταξύ client και server) για να πιστοποιήσουν το ένα το άλλο και να αποκτήσουν ένα κοινό κλειδί συνόδου χωρίς να εκθέσουν την ιδιωτική τους ζωή όταν τα χαρακτηριστικά τους πληρούν τις κοινωνικές ανάγκες μεταξύ τους (41: Hao 2018:873-880) .

Μια άλλη λύση προτείνεται για συστήματα που υποστηρίζουν εντοπισμό θέσης (location-based services -LBSs). Οι υπάρχουσες λύσεις που χρησιμοποιούνται μεταξύ των χρηστών και του παρόχου υπηρεσιών εντοπισμού θέσης (LSP) λαμβάνουν ως δεδομένη την αξιοπιστία αυτού. Έτσι η εμπιστοσύνη στον πάροχο υπηρεσιών εντοπισμού θέσης μπορεί να εγκυμονεί κινδύνους για την ασφάλεια των χρηστών. Η τεχνική που εφαρμόζεται ως σήμερα παρουσιάζεται στο σχήμα

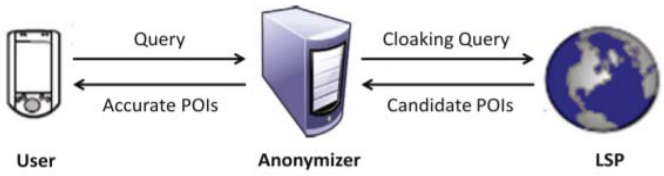


Fig. 1. A typical TTP architecture.

Προτείνεται λοιπόν μια λύση όπου ενισχύεται η ιδιωτικότητα της θέσης στους LBSs. Η προτεινόμενη λύση λοιπόν βασίζεται στο ομοιόμορφο δίκτυο και υιοθετεί τόσο την συμμετρική κρυπτογράφηση (OPSE) όσο και την τεχνική ανωνυμίας. Έτσι, ο server που χρησιμοποιείται για την ανωνυμοποίηση δεν γνωρίζει τίποτα σχετικά με την πραγματική τοποθεσία ενός χρήστη, και μπορεί να εφαρμόσει απλές λειτουργίες αντιστοίχισης και σύγκρισης. Στο παρακάτω σχήμα παρουσιάζεται η λύση που προτείνεται (111: Zhang 2018: 881-892) .

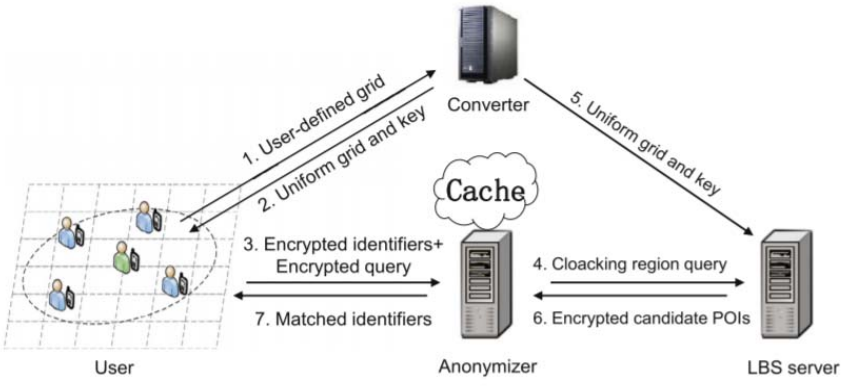


Fig. 2. UGC architecture.

Μια άλλη μελέτη, βασιζόμενη σε τεχνικές στενογραφίας προτείνει μια λύση κατά την οποία οι επικοινωνίες μεταξύ των χρηστών είναι εντελώς μη ανιχνεύσιμες το οποίο διασφαλίζει

ότι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να διαβάσουν ή να ανεβάσουν μηνύματα στα ΜΚΔ (12: Beato 2014) .

Μια άλλη προσέγγιση για τα πλαστά προφίλ χρηστών (Sybil) προτείνεται ώστε να βελτιστοποιηθούν με νέα δεδομένα, με στόχο τη βελτίωση των στρατηγικών κατά των συνεχώς εξελισσόμενων φορέων Sybil. Εισάγεται λοιπόν ένα σύστημα πρόβλεψης που μπορεί να αξιοποιηθεί για το πρόβλημα των επιθέσεων Sybil στο Twitter. Το προτεινόμενο σύστημα περιλαμβάνει τρεις ενσωματωμένες ενότητες, δηλαδή μια ενότητα συλλογής δεδομένων, έναν μηχανισμό εξαγωγής χαρακτηριστικών και ένα μοντέλο βαθιάς παλινδρόμησης. Όλες αυτές οι ενότητες λειτουργούν σε συστηματική μορφή για να αναλύσουν και να αξιολογήσουν τα προφίλ των χρηστών στο Twitter. Το προτεινόμενο μοντέλο φαίνεται να προσφέρει αυτό το είδος βελτιστοποίησης και έχει αποδειχθεί ότι παρέχει ακρίβεια έως 86% όταν τροφοδοτείται με ύποπτα δεδομένα (3: Al-Qurishi 2018: 743-753) .

Για την προστασία της ιδιωτικής ζωής των χρηστών, τα κοινωνικά δίκτυα πρέπει να ανώνυμα. Ωστόσο, οι υπάρχοντες αλγόριθμοι ανωνυμοποίησης στα κοινωνικά δίκτυα πολλές φορές αποδεικνύονται ανεπαρκής. Επομένως, πρέπει αναπτυχθεί ένας αποτελεσματικός αλγόριθμος ανωνυμίας για την προστασία της ιδιωτικής ζωής του χρήστη. Έτσι προτείνουμε ένα νέο μοντέλο ανωνυμοποίησης , το οποίο ενσωματώνει την επανα-κρυπτογράφηση ενδιάμεσου (proxy) με τις τεχνικές αναζήτησης λέξεων-κλειδιών, για την αντιμετώπιση του ζητήματος της ανωνυμοποίησης . Στο προτεινόμενο σύστημα δεν μπορεί μόνο να προστατευτεί η αυθεντικότητα των χρηστών, αλλά διατηρεί την πλήρη χρησιμότητα του κοινωνικού δικτύου. Εκτεταμένα πειράματα σε μεγάλα σε κοινωνικά δίκτυα επιβεβαιώνουν την αποτελεσματικότητα και την αποτελεσματικότητα του σχεδίου αυτού(110: Zhang 2017: 227-238) .

Μια άλλη πρόταση στηρίζεται στη δημιουργία λιστών ελέγχου πρόσβασης και τη χρήση τους για φωτογραφίες, αρχεία multimedia και στοιχεία από την κίνηση στο δίκτυο. Αυτές οι λίστες παρέχουν στους προγραμματιστές εφαρμογών το απαραίτητο μέσο για να δοθεί στον χρήστη περισσότερος έλεγχος των δεδομένων του στα online κοινωνικά δίκτυα και μεγαλύτερη διαφάνεια για το ποιος μπορεί να έχει πρόσβαση στα δεδομένα αυτά (85: Berger 2010).

Ο Hamza Al Aghaei πρότεινε ένα πλαίσιο ασφάλειας των ΜΚΔ για την προστασία του περιεχομένου πολυμέσων από διαφορετικούς τύπους παράνομης χρήσης και επιθέσεων με

την εφαρμογή δύο ανώνυμων βάσεων δεδομένων με αλγόριθμο RSA και τεχνική CAPTCHA στο διακομιστώ (6: Al Aghaei 2012)

Οι M. Linked και B. Ayres πρότειναν μια προσέγγιση η υποδομή της οποίας είναι βασισμένη στην πολιτική απορρήτου , με τη βοήθεια ενός ΜΚΔ σχεδιασμένου σε γλώσσα PHP, επιτρέποντας: 1. Οι χρήστες να εκφράζουν τις προτιμήσεις τους όσον αφορά το απόρρητο σε σχέση με το ποιος μπορεί να έχει πρόσβαση στα δεδομένα τους και για ποιο σκοπό.2. Υποστήριξη του παρόχου δεδομένων για την επιβολή των προτιμήσεων απορρήτου των χρηστών και την υποστήριξη πρόσθετων μοντέλων πρόσβασης. 3. Διαχείριση προβλημάτων απορρήτου και πρόσβαση σε δεδομένα στο ΜΚΔ (69: Bahri 2012: *59-65*).
Ο Deuker Al και άλλοι εξέτασαν τις πολιτικές απορρήτου του Facebook και πρότεινε ένα πλαίσιο με ορισμένες νέες πολιτικές απορρήτου για ισχυροποίηση και ενίσχυση των υφιστάμενων πολιτικών, εφαρμόζοντας μόνο τρεις πολιτικές σε ένα πρωτότυπο Facebook σημειώνοντας ότι απαιτείται πολλή έρευνα ακόμα να γίνει σε αυτό το πεδίο (56: Al 2014:129–133) .

Η Al Bahri πρότεινε ένα νέο πλαίσιο στο οποίο ένας χρήστης έχει τη δυνατότητα να δημιουργεί πολλαπλά προφίλ και στοχεύει στη μείωση των κινδύνων παραβίασης της ιδιωτικής ζωής δίνοντας στον χρήστη πιο διαισθητικούς τρόπους για να διαχειριστεί τους προσωπικούς και κοινωνικούς του κύκλους και να ελέγξει ποιος αποκτά πρόσβαση σε ποιο τύπο δεδομένων (36: Bahri 2015: 187 – 199).

Κεφάλαιο 11. Εμπειρική Μελέτη

11.1 Επιλογή Constructs προς στατιστική ανάλυση

Η **ασφάλεια** (security) στα ΜΚΔ αποτελεί θεμέλιο λίθο και σχετίζεται συγκεκριμένα με την ασφάλεια των υπολογιστών, την ασφάλεια των δεδομένων, την ακεραιότητα, τη διαθεσιμότητα και άλλα ευρύτερα πεδία του πλαισίου ασφάλειας πληροφοριών και είναι ουσιαστικά η προστασία από μη εξουσιοδοτημένη πρόσβαση, χρήση, μετατροπή ή καταστροφή. Οι χρήστες των ΜΚΔ φοβούνται ότι θα χάσουν τα δεδομένα τους και τα ίδια τα ΜΚΔ φοβούνται τις οικονομικές απώλειες που συνδέονται με τυχόν κακή δημοσιότητα και διάρρηξη.

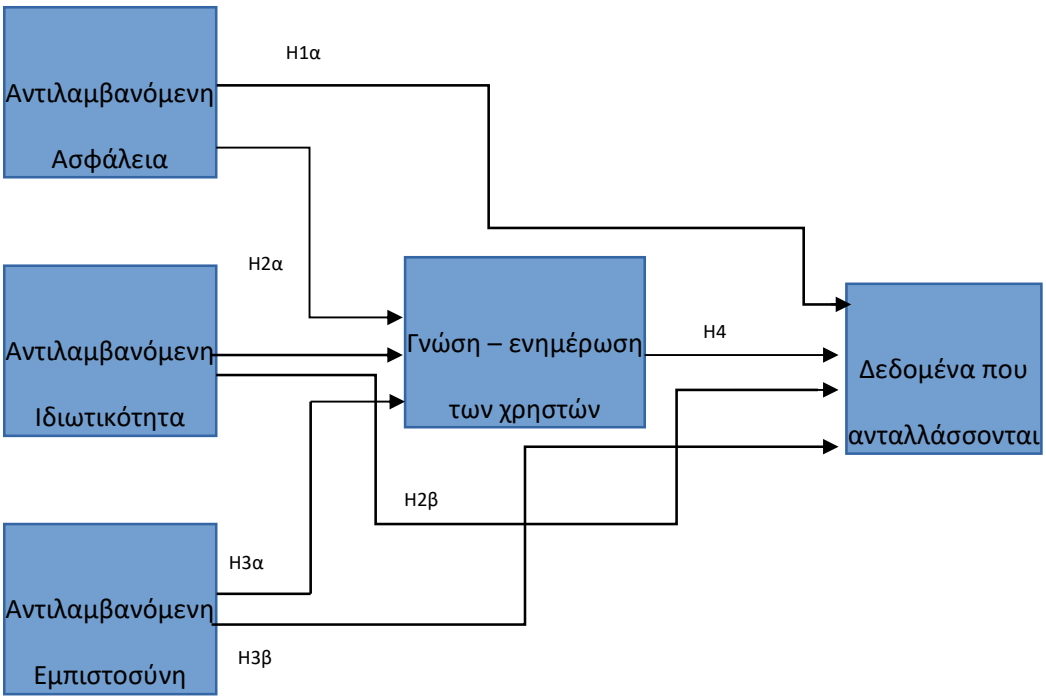
Όπως μπορούμε όλοι να καταλάβουμε, και σαν χρήστες ΜΚΔ, η ασφάλεια είναι ένα πολύ σημαντικό θέμα για την καθημερινή μας ενασχόληση με τα ΜΚΔ και γι' αυτό η ασφάλεια θα είναι η **1η sub construct** μας στην εργασία.

Η **ιδιωτικότητα** (privacy) είναι ένα σοβαρό ζήτημα στο ηλεκτρονικό εμπόριο, ανεξάρτητα από την πηγή που εξετάζει κανείς. Ο Culnan υποστήριξε ότι οι ανησυχίες για την προστασία της ιδιωτικής ζωής είναι ένας κρίσιμος λόγος για τον οποίο οι άνθρωποι δεν πηγαίνουν στο διαδίκτυο και παρέχουν ψευδείς πληροφορίες ηλεκτρονικά. Ο συνδυασμός των τρεχουσών επιχειρηματικών πρακτικών των ΜΚΔ, των φόβων των χρηστών και της πίεσης των μέσων ενημέρωσης συνδυάστηκε για να καταστήσει την ιδιωτικότητα ως ένα ισχυρό πρόβλημα για τα ΜΚΔ. Ορισμένοι θεωρούν ότι η ιδιωτική ζωή αποτελεί θεμελιώδες δικαίωμα, ενώ άλλοι θεωρούν ότι είναι εμπορεύσιμο είδος.

Και η ιδιωτικότητα θα αποτελέσει την **2η subconstruct** μας λόγω της σημαντικότητας της για τον χρήστη.

Τέλος οι απειλές και οι κινδύνου που υφίστανται οι χρήστες ΜΚΔ τόσο σε προσωπικό αλλά και σε επαγγελματικό επίπεδο τους καθιστά απρόθυμους στη διατήρηση ή ενημέρωση των λογαριασμών τους στα ΜΚΔ. Οι περιπτώσεις ουκ ολίγες και τα ίδια τα μέσα πολλές φορές δεν λαμβάνουν εκ των προτέρων μέτρα για να διασκεδάσουν τις ανησυχίες και τους φόβους των χρηστών. Ψεύτικα προφίλ, fake ειδήσεις αλλά και αιτήματα φιλίας – παγίδες είναι συχνό φαινόμενο. Άρα η εμπιστοσύνη των χρηστών στα ΜΚΔ θα αποτελέσει την **3η subconstruct** η οποία είναι πολύ σημαντική για τους χρήστες.

11.2 Προτάσεις – Υποθέσεις - Μεταβλητές



Προτάσεις

Π1α. Η αντιλαμβανόμενη ασφάλεια σχετίζεται θετικά με την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
Π2α. Η αντιλαμβανόμενη Ιδιωτικότητα σχετίζεται θετικά με την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.

Π1β. Η αντιλαμβανόμενη Ασφάλεια σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Π2β. Η αντιλαμβανόμενη Ιδιωτικότητα σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Π3α. Η αντιλαμβανόμενη Εμπιστοσύνη σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Π3β. Η εμπιστοσύνη σχετίζεται θετικά με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
Π4. Τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι το αποτέλεσμα της γνώσης – ενημέρωσης των χρηστών γύρω από αυτά.
Π5α. Η θετική σκέψη ανάμεσα στην αντίληψη περί ιδιωτικότητας σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι ισχυρότερη στις μεγαλύτερες ηλικίες.
Π5β. Η θετική σκέψη ανάμεσα στην αντίληψη περί εμπιστοσύνης σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι ισχυρότερη στις μεγαλύτερες ηλικίες.
Π6. Η αποδοχή στο αίτημα φιλίας από αγνώστους είναι διαφορετικό για άνδρες και γυναίκες.
Π7. Η διασφάλιση απορρήτου των προσωπικών δεδομένων είναι διαφορετική για χρήστες δευτεροβάθμιας από τριτοβάθμιας εκπαίδευσης.
Π8. Η άποψη ότι τα ΜΚΔ είναι ασφαλή είναι διαφορετική για άνδρες και γυναίκες.

Εξαρτημένες μεταβλητές (Dependent Variables)

D1. Γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
D2. Δεδομένα που ανταλλάσσονται στα ΜΚΔ με ή χωρίς τη θέληση των χρηστών

Ανεξάρτητες μεταβλητές (Independent Variables)

I1. Η αντιλαμβανόμενη Ασφάλεια
I2. Η αντιλαμβανόμενη Ιδιωτικότητα
I3. Η αντιλαμβανόμενη Εμπιστοσύνη

Μηδενικές Υποθέσεις

Ηο1α. Η αντιλαμβανόμενη ασφάλεια δεν σχετίζεται με την γνώση – ενημέρωση των χρηστών .
Ηο2α. Η αντιλαμβανόμενη Ιδιωτικότητα δεν σχετίζεται με την γνώση – ενημέρωση των χρηστών.

Ηο1β. Η αντιλαμβανόμενη Ασφάλεια δεν έχει καμία επίδραση στην ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Ηοβ. Η αντιλαμβανόμενη Ιδιωτικότητα δεν έχει καμία επίδραση στην ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Η03α. Η αντιλαμβανόμενη Εμπιστοσύνη δεν έχει καμία επίδραση στην ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Ηο3β. Η εμπιστοσύνη δεν σχετίζεται με την γνώση – ενημέρωση των χρηστών.
Ηο4.Τα δεδομένα που ανταλλάσσονται στα ΜΚΔ δεν είναι το αποτέλεσμα της γνώσης – ενημέρωσης των χρηστών γύρω από αυτά.
Ηο5α. Η θετική σκέψη ανάμεσα στην αντίληψη περί ιδιωτικότητας σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ δεν είναι ισχυρότερη στις μεγαλύτερες ηλικίες.
Ηο5β. Η θετική σκέψη ανάμεσα στην αντίληψη περί εμπιστοσύνης σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ δεν είναι ισχυρότερη στις μεγαλύτερες ηλικίες.
Ηο6: Η αποδοχή στο αίτημα φιλίας από αγνώστους είναι ίδια για άνδρες και γυναίκες.
Ηο7: Η διασφάλιση απορρήτου των προσωπικών δεδομένων είναι ίδια για χρήστες δευτεροβάθμιας και τριτοβάθμιας εκπαίδευσης.
Ηο8: Η άποψη ότι τα ΜΚΔ είναι ασφαλή είναι ίδια για άνδρες και γυναίκες.

Υποθέσεις

Η1α. Τα μέτρα που λαμβάνονται για τη μη παραβίαση (μη πρόσβαση) στα προσωπικά μας δεδομένα (= αντιλαμβανόμενη ασφάλεια) σχετίζεται θετικά με την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
Η2α. Η συχνότητα (ή ο βαθμός) με τον οποίο αποκαλύπτουμε προσωπικές πληροφορίες (= αντιλαμβανόμενη Ιδιωτικότητα) σχετίζεται θετικά με την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
Η1β. Τα μέτρα που λαμβάνονται για τη μη παραβίαση (μη πρόσβαση) στα προσωπικά μας δεδομένα (= αντιλαμβανόμενη ασφάλεια) σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Η2β. Η συχνότητα με την οποία αποκαλύπτουμε προσωπικές πληροφορίες (= αντιλαμβανόμενη Ιδιωτικότητα) σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Η3α. Η προθυμία να ανταλλάσουμε δεδομένα με φίλους ή μη (αποδοχή αιτημάτων φιλίας από γνωστούς ή μη) (= αντιλαμβανόμενη Εμπιστοσύνη) σχετίζεται θετικά με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.
Η3β. Η προθυμία να ανταλλάσουμε δεδομένα με φίλους ή μη (αποδοχή αιτημάτων φιλίας από γνωστούς ή μη) (= αντιλαμβανόμενη Εμπιστοσύνη) σχετίζεται θετικά με την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.
Η4. Τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι το αποτέλεσμα της γνώσης – ενημέρωσης των χρηστών γύρω από αυτά.

Η5α. Η θετική σκέψη ανάμεσα στην αντίληψη περί ιδιωτικότητας σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι ισχυρότερη στις μικρότερες ηλικίες.
Η5β. Η θετική σκέψη ανάμεσα στην αντίληψη περί εμπιστοσύνης σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι ισχυρότερη στις μικρότερες ηλικίες.
Η6: Η αποδοχή στο αίτημα φιλίας από αγνώστους είναι διαφορετική μεταξύ ανδρών και γυναικών.

Η7: Η διασφάλιση απορρήτου των προσωπικών δεδομένων είναι διαφορετική μεταξύ χρηστών επιπέδου σπουδών δευτεροβάθμιας με τριτοβάθμια εκπαίδευση.
Η8: Η άποψη ότι τα ΜΚΔ είναι ασφαλή είναι διαφορετική μεταξύ ανδρών και γυναικών.

Δεδομένα που ανταλλάσσονται στα ΜΚΔ

Σύνδεση υποθέσεων με ερευνητικά ερωτήματα

Η1α>>Ε15,Ε16,Ε17,Ε18

Η1β>> Ε16

Η2α>>Ε19,Ε20,Ε21,Ε22,Ε27

Η2β>> Ε22,Ε23,Ε28,Ε29

Η3α >>Ε8,Ε11,Ε12,Ε13

Η3β>>Ε9, Ε10, Ε12,Ε14

Η4>>Ε12,Ε22,Ε23,Ε25

Η5α>>Ε24

Η5β>>Ε14

Η6>>Ε1,Ε10

Η7>>Ε19,Ε20,Ε3

Η8>>Ε16,Ε1

Κεφάλαιο 12.Αποτελέσματα ερωτηματολογίου – Στατιστική Ανάλυση

12.1 Πίνακες και γραφήματα ερωτηματολογίου

Γενικές ερωτήσεις

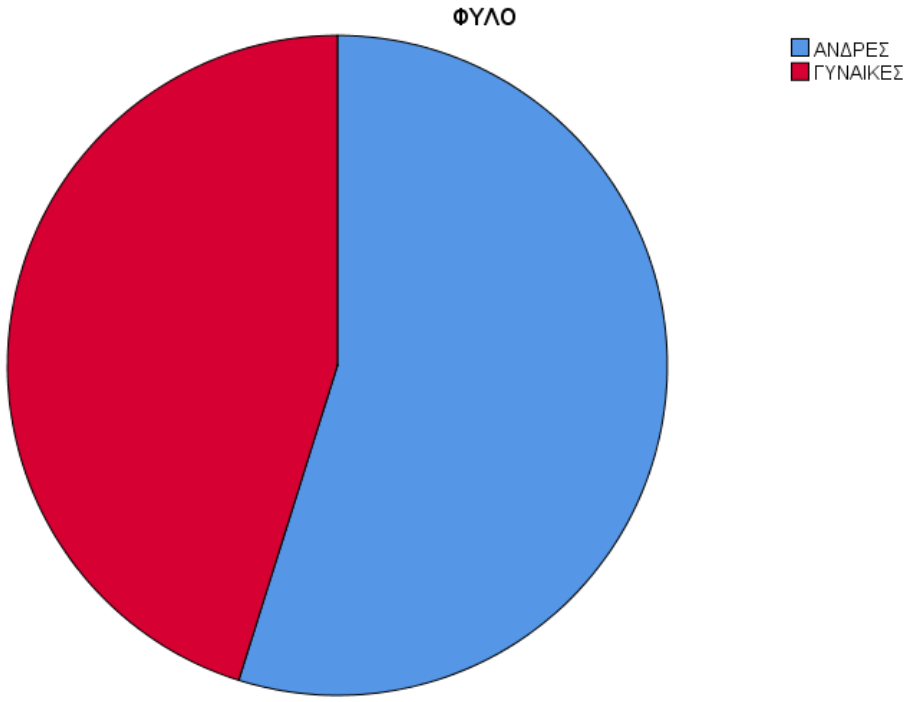
- **Φύλο:**

Στον πίνακα 1 παρουσιάζεται αριθμητικά και ποσοστιαία το φύλο των ερωτηθέντων. Παρατηρούμε ότι περίπου το 55% των ερωτηθέντων ήταν άντρες και το 45% γυναίκες. Τα συγκεκριμένα ποσοστά αυτά απεικονίζονται γραφικά στο διάγραμμα 1

Πίνακας 1:

ΦΥΛΟ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΑΝΔΡΕΣ	34	54,8	54,8	54,8
	ΓΥΝΑΙΚΕΣ	28	45,2	45,2	100,0
	Total	62	100,0	100,0	

Διάγραμμα 1:



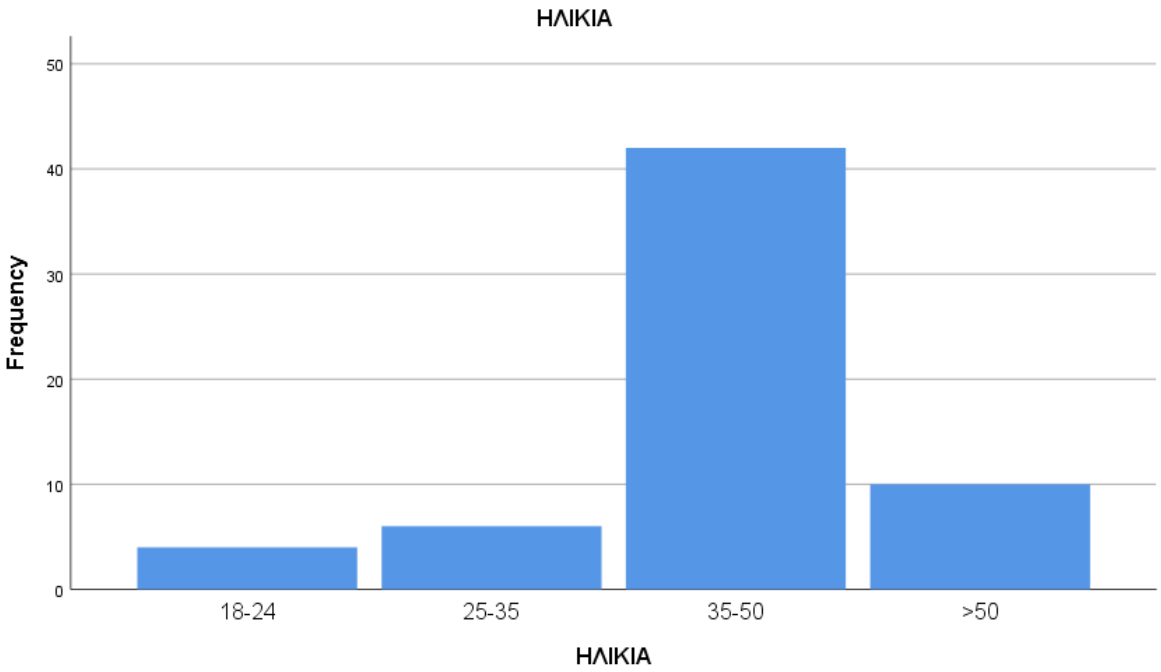
2. Ηλικία:

Όσον αφορά την ηλικία του δείγματος, στον Πίνακα 2 παρουσιάζεται η συχνότητα και το ποσοστό των ατόμων που ανήκουν στην κάθε ηλικιακή κατηγορία. Παρατηρούμε ότι το μεγαλύτερο ποσοστό συγκεντρώνεται στις ηλικίες 35-50 (67,7%). Η κατανομή συχνότητας της μεταβλητής απεικονίζεται στο Διάγραμμα 2.

Πίνακας 2:

ΗΛΙΚΙΑ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	4	6,5	6,5	6,5
	25-35	6	9,7	9,7	16,1
	35-50	42	67,7	67,7	83,9
	>50	10	16,1	16,1	100,0
	Total	62	100,0	100,0	



Διάγραμμα 2:

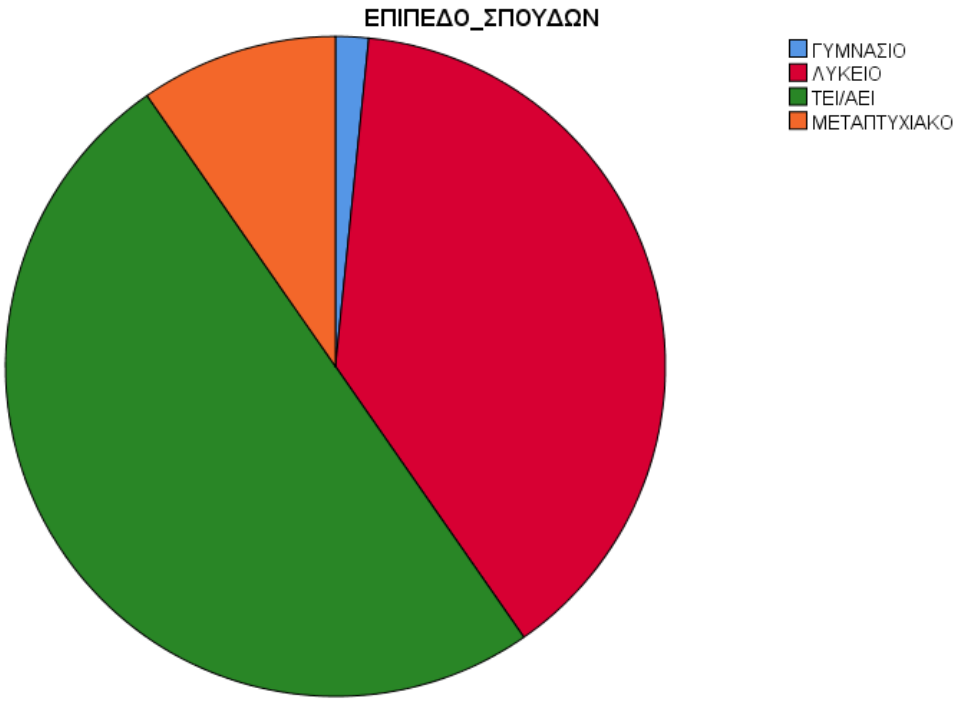
3. Μορφωτικό Επίπεδο:

Στον Πίνακα 3 παρουσιάζεται αναλυτικά το μορφωτικό επίπεδο των ερωτηθέντων. Παρατηρούμε ότι το μεγαλύτερο ποσοστό ~ 50% των ερωτηθέντων είναι απόφοιτοι τριτοβάθμιας εκπαίδευσης. Το μορφωτικό επίπεδο απεικονίζετε στο Διάγραμμα 3.

Πίνακας 3:

ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΓΥΜΝΑΣΙΟ	1	1,6	1,6	1,6
	ΛΥΚΕΙΟ	24	38,7	38,7	40,3
	ΤΕΙ/ΑΕΙ	31	50,0	50,0	90,3
	ΜΕΤΑΠΤΥΧΙΑΚΟ	6	9,7	9,7	100,0
	Total	62	100,0	100,0	

Διάγραμμα 3:



4. Λογαριασμοί χρηστών:

Στον πίνακα 4 απεικονίζονται οι λογαριασμοί που έχει ό κάθε χρήστης στα ΜΚΔ. Όπως παρατηρούμε το Facebook είναι αυτό με τις περισσότερες προτιμήσεις χρηστών με ποσοστό 42% περίπου.

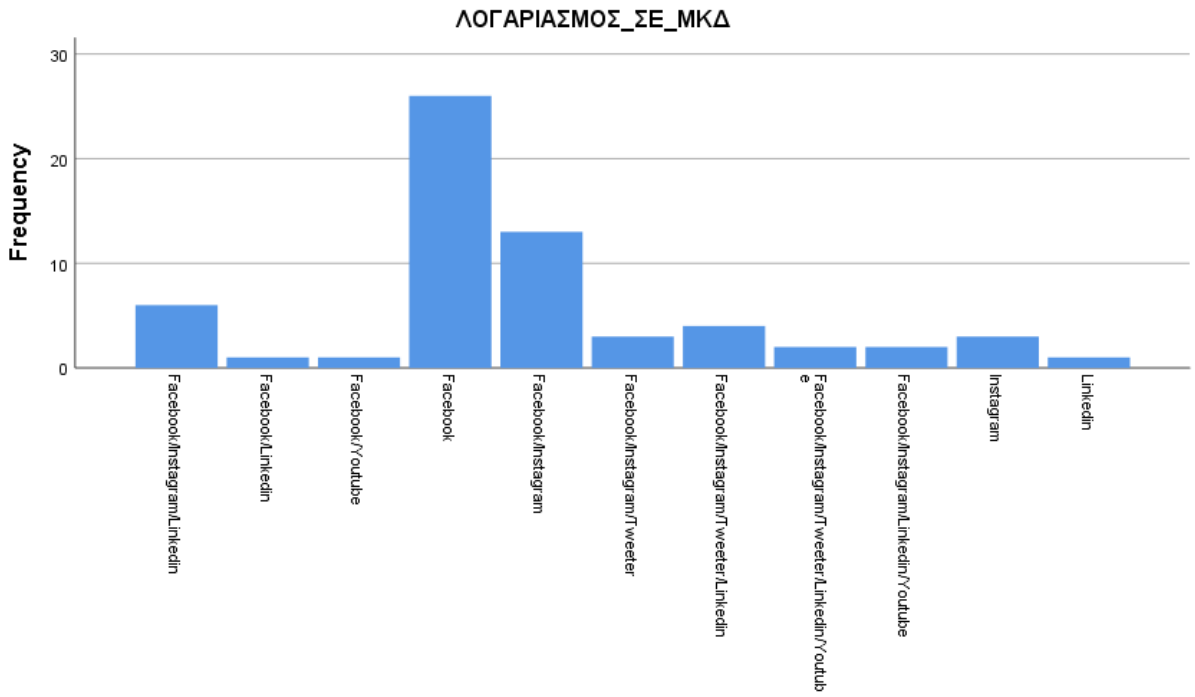
Πίνακας 3:

ΛΟΓΑΡΙΑΣΜΟΣ_ΣΕ_ΜΚΔ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Facebook/Instagram/Linkedin	6	9,7	9,7	9,7
	Facebook/Linkedin	1	1,6	1,6	11,3
	Facebook/Youtube	1	1,6	1,6	12,9
	Facebook	26	41,9	41,9	54,8
	Facebook/Instagram	13	21	21	75,8
	Facebook/Instagram/Tweeter	3	4,8	4,8	80,6
	Facebook/Instagram/Tweeter/Linkedin	4	6,5	6,5	87,1
	Facebook/Instagram/Tweeter/LinkedIn/YouTube	2	3,2	3,2	90,3
	Facebook/Instagram/LinkedIn/Youtube	2	3,2	3,2	93,5
	Instagram	3	4,8	4,8	98,4
	LinkedIn	1	1,6	1,6	100
	Total	62	100	100	

Στο διάγραμμα 4 απεικονίζονται οι προτιμήσεις χρηστών

Διάγραμμα 4



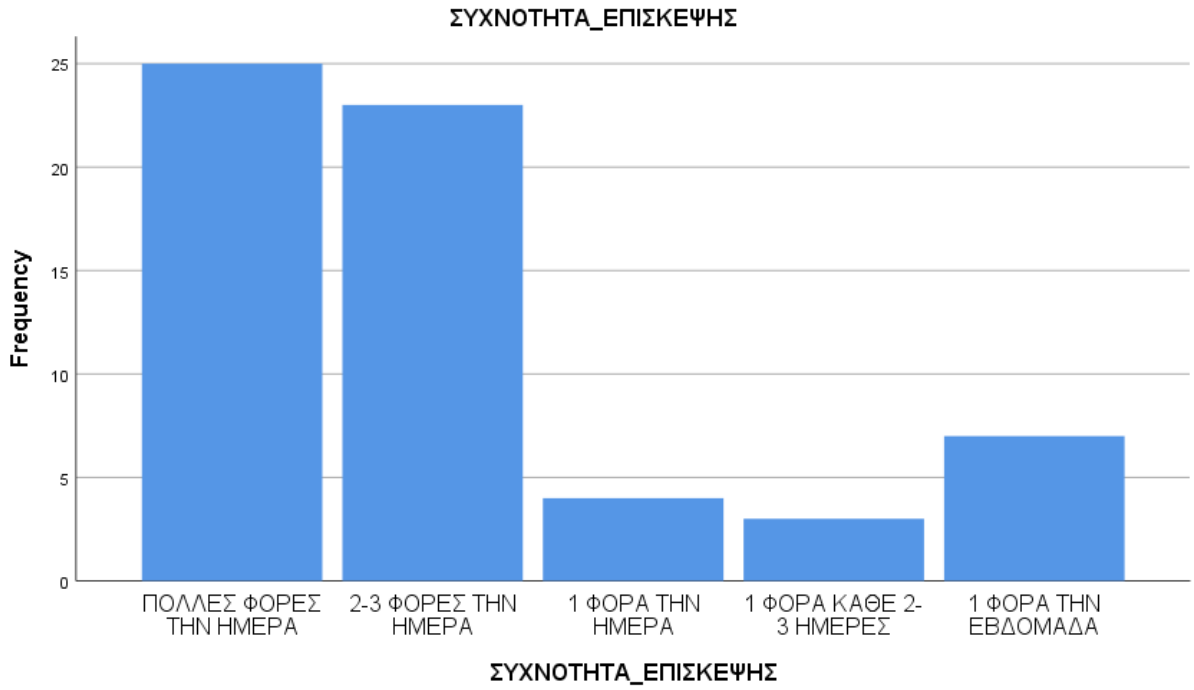
5. Συχνότητα επίσκεψης

Στον παρακάτω πίνακα (***Πίνακας 5***) παρουσιάζεται η συχνότητα επίσκεψης των χρηστών στα ΜΚΔ στα οποία οι χρήστες έχουν λογαριασμούς. Το μεγαλύτερο ποσοστό κατέχουν οι χρήστες που επισκέπτονται τα ΜΚΔ 2-3 φορές την ημέρα (37,1%). Στο διάγραμμα 5παρατίθεται η απεικόνιση του πίνακα 5.

Πίνακας 5

ΣΥΧΝΟΤΗΤΑ_ΕΠΙΣΚΕΨΗΣ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΟΛΛΕΣ ΦΟΡΕΣ ΤΗΝ ΗΜΕΡΑ	25	40,3	40,3	40,3
	2-3 ΦΟΡΕΣ ΤΗΝ ΗΜΕΡΑ	23	37,1	37,1	77,4
	1 ΦΟΡΑ ΤΗΝ ΗΜΕΡΑ	4	6,5	6,5	83,9
	1 ΦΟΡΑ ΚΑΘΕ 2-3 ΗΜΕΡΕΣ	3	4,8	4,8	88,7
	1 ΦΟΡΑ ΤΗΝ ΕΒΔΟΜΑΔΑ	7	11,3	11,3	100,0
	Total	62	100,0	100,0	



Διάγραμμα 5

6. Χρόνος επίσκεψης

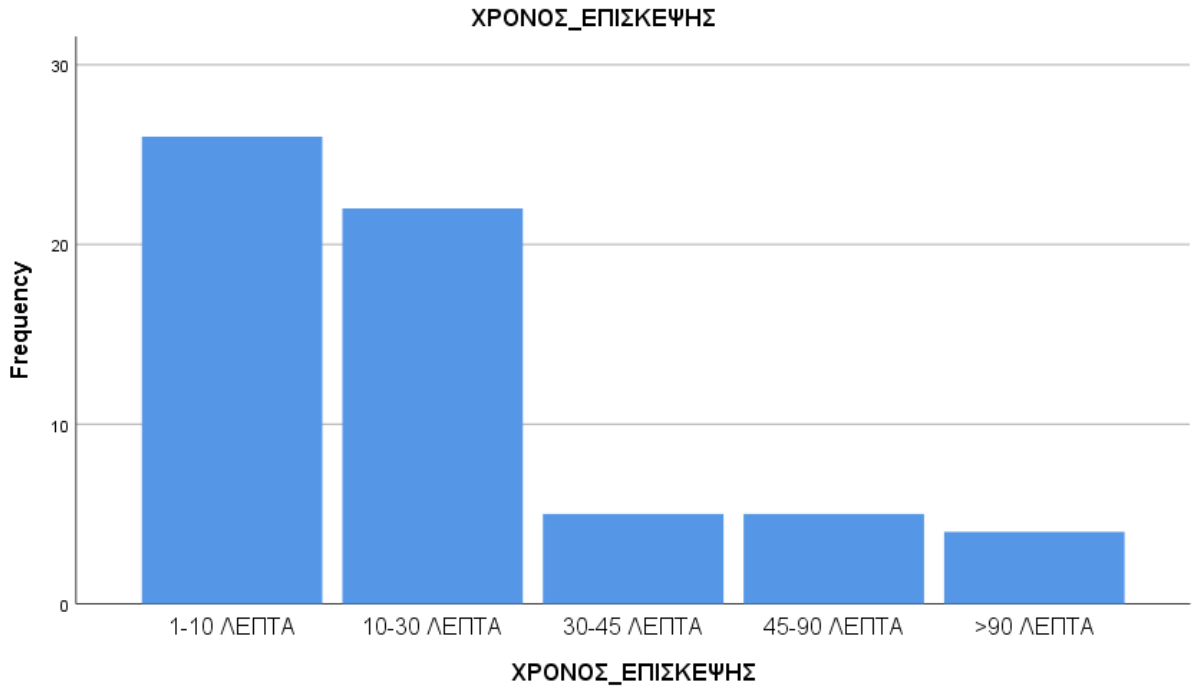
Στον πίνακα 6 παρουσιάζεται ο χρόνος επίσκεψης των χρηστών με το μεγαλύτερο ποσοστό (35,5%) να εμφανίζει η επιλογή 10 – 30 λεπτά ημερησίως.

Πίνακας 6

ΧΡΟΝΟΣ_ΕΠΙΣΚΕΨΗΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-10 ΛΕΠΤΑ	26	41,9	41,9	41,9
	10-30 ΛΕΠΤΑ	22	35,5	35,5	77,4
	30-45 ΛΕΠΤΑ	5	8,1	8,1	85,5
	45-90 ΛΕΠΤΑ	5	8,1	8,1	93,5
	>90 ΛΕΠΤΑ	4	6,5	6,5	100,0
	Total	62	100,0	100,0	

Στο διάγραμμα 6 απεικονίζεται ο χρόνος επίσκεψης των χρηστών.

Διάγραμμα 6



7. Λόγος επίσκεψης

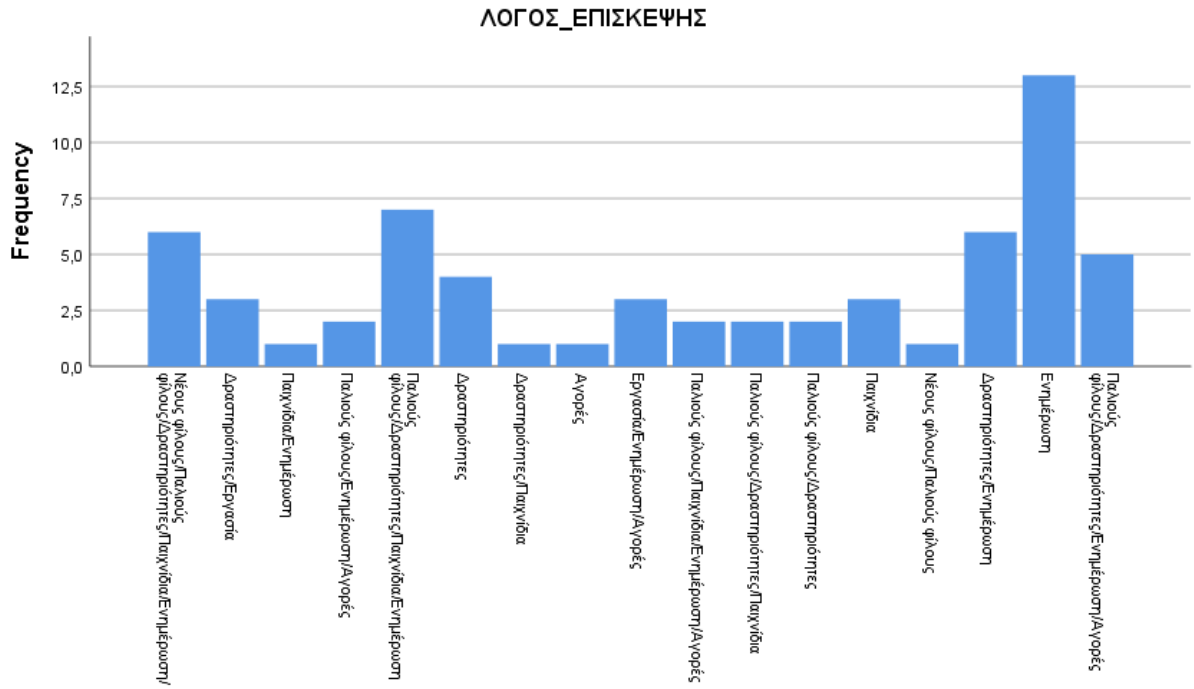
Στον πίνακα 7 παρουσιάζονται οι λόγοι για τους οποίους οι χρήστες επισκέπτονται τα ΜΚΔ με το μεγαλύτερο ποσοστό να αφορά την ενημέρωση (21%).

Πίνακας 7

ΛΟΓΟΣ_ΕΠΙΣΚΕΨΗΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Νέους φίλους/Παλιούς φίλους/Δραστηριότητες/Παιχνίδια/Ενημέρωση/	6	9.7	9.7	9.7
	Δραστηριότητες/Εργασία	3	4.8	4.8	14.5
	Παιχνίδια/Ενημέρωση	1	1.6	1.6	16.1
	Παλιούς φίλους/Ενημέρωση/Αγορές	2	3.2	3.2	19.4
	Παλιούς φίλους/Δραστηριότητες/Παιχνίδια/Ενημέρωση	7	11.3	11.3	30.6
	Δραστηριότητες	4	6.5	6.5	37.1
	Δραστηριότητες/Παιχνίδια	1	1.6	1.6	38.7
	Αγορές	1	1.6	1.6	40.3
	Εργασία/Ενημέρωση/Αγορές	3	4.8	4.8	45.2
	Παλιούς φίλους/Παιχνίδια/Ενημέρωση/Αγορές	2	3.2	3.2	48.4
	Παλιούς φίλους/Δραστηριότητες/Παιχνίδια	2	3.2	3.2	51.6
	Παλιούς φίλους/Δραστηριότητες	2	3.2	3.2	54.8
	Παιχνίδια	3	4.8	4.8	59.7
	Νέους φίλους/Παλιούς φίλους	1	1.6	1.6	61.3
	Δραστηριότητες/Ενημέρωση	6	9.7	9.7	71.0
	Ενημέρωση	13	21.0	21.0	91.9
	Παλιούς φίλους/Δραστηριότητες/Ενημέρωση/Αγορές	5	8.1	8.1	100.0
	Total	62	100.0	100.0	

Στο διάγραμμα που ακολουθεί απεικονίζονται οι λόγοι επίσκεψης

Διάγραμμα 7



Εμπιστευτικότητα (Trust)

8. Ποια από τα παρακάτω στοιχεία που έχετε δώσει στα ΜΚΔ είναι πραγματικά:

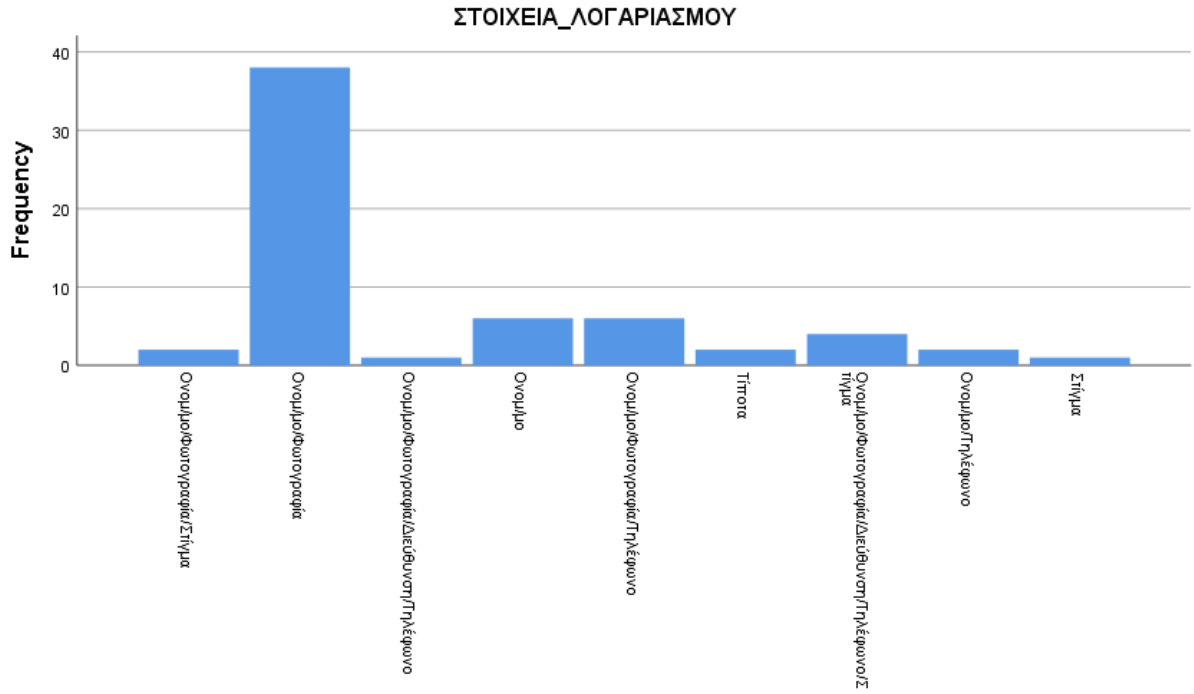
Στο παρακάτω διάγραμμα παρουσιάζονται τα στοιχεία τα οποία έχουν διαθέσει οι χρήστες στα ΜΚΔ και όπως είναι φυσικό το μεγαλύτερο ποσοστό χρηστών έχει διαθέσει ονοματεπώνυμο και φωτογραφία.

Πίνακας 8

ΣΤΟΙΧΕΙΑ_ΛΟΓΑΡΙΑΣΜΟΥ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ονομ/μο/Φωτογραφία/Στίγμα	2	3,2	3,2	3,2
	Ονομ/μο/Φωτογραφία	38	61,3	61,3	64,5
	Ονομ/μο/Φωτογραφία/Διεύθυνση/Τηλέφωνο	1	1,6	1,6	66,1
	Ονομ/μο	6	9,7	9,7	75,8
	Ονομ/μο/Φωτογραφία/Τηλέφωνο	6	9,7	9,7	85,5
	Τίποτα	2	3,2	3,2	88,7
	Ονομ/μο/Φωτογραφία/Διεύθυνση/Τηλέφωνο/Στίγμα	4	6,5	6,5	95,2
	Ονομ/μο/Τηλέφωνο	2	3,2	3,2	98,4
	Στίγμα	1	1,6	1,6	100,0
	Total	62	100,0	100,0	

Στο διάγραμμα 8 γίνεται απεικόνιση του διαγράμματος 8

Διάγραμμα 8



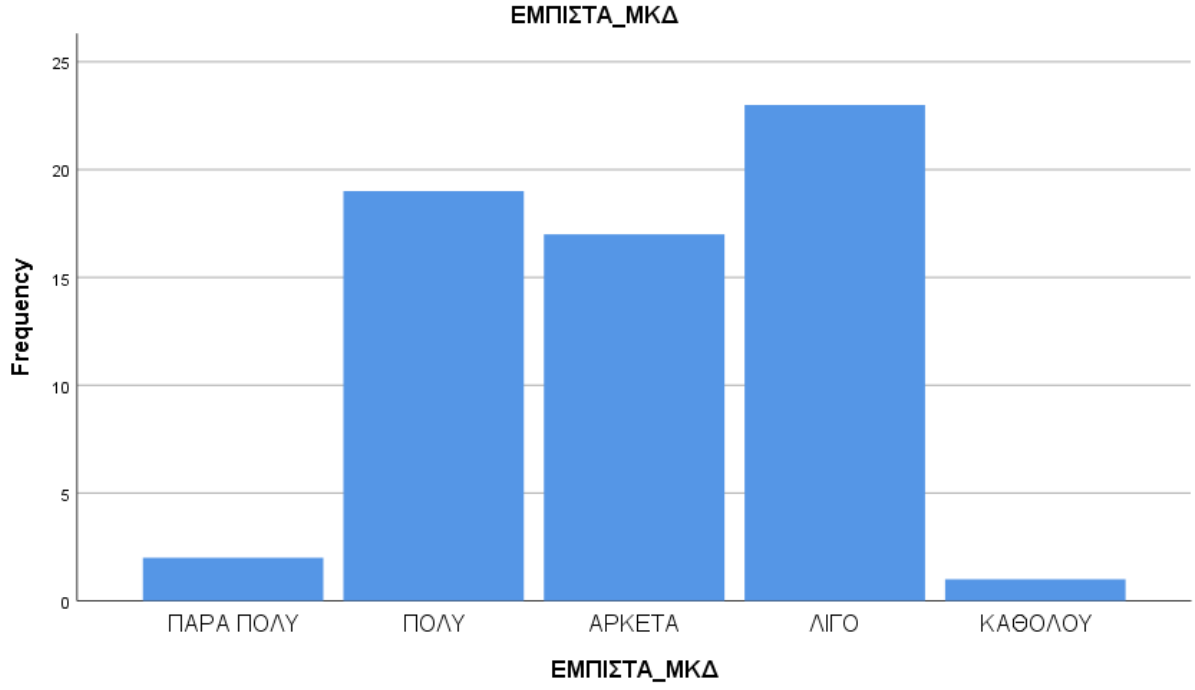
<u>9. Θεωρείτε τα ΜΚΔ έμπιστα στην ανταλλαγή πληροφοριών με φίλους ή μη</u>;

Στον παρακάτω πίνακα (Πίνακας 9) παρουσιάζεται η άποψη των χρηστών σχετικά με το κατά πόσο έμπιστα θεωρούν τα ΜΚΔ. Οι απόψεις παρουσιάζουν ιδιαίτερο ενδιαφέρον καθώς τρεις τελείως διαφορετικές απαντήσεις κατέχουν παρόμοια ποσοστά. Τα ποσοστά αυτά απεικονίζονται στο διάγραμμα 9.

Πίνακας 9

ΕΜΠΙΣΤΑ_ΜΚΔ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	2	3,2	3,2	3,2
	ΠΟΛΥ	19	30,6	30,6	33,9
	ΑΡΚΕΤΑ	17	27,4	27,4	61,3
	ΛΙΓΟ	23	37,1	37,1	98,4
	ΚΑΘΟΛΟΥ	1	1,6	1,6	100,0
	Total	62	100,0	100,0	

Διάγραμμα 9



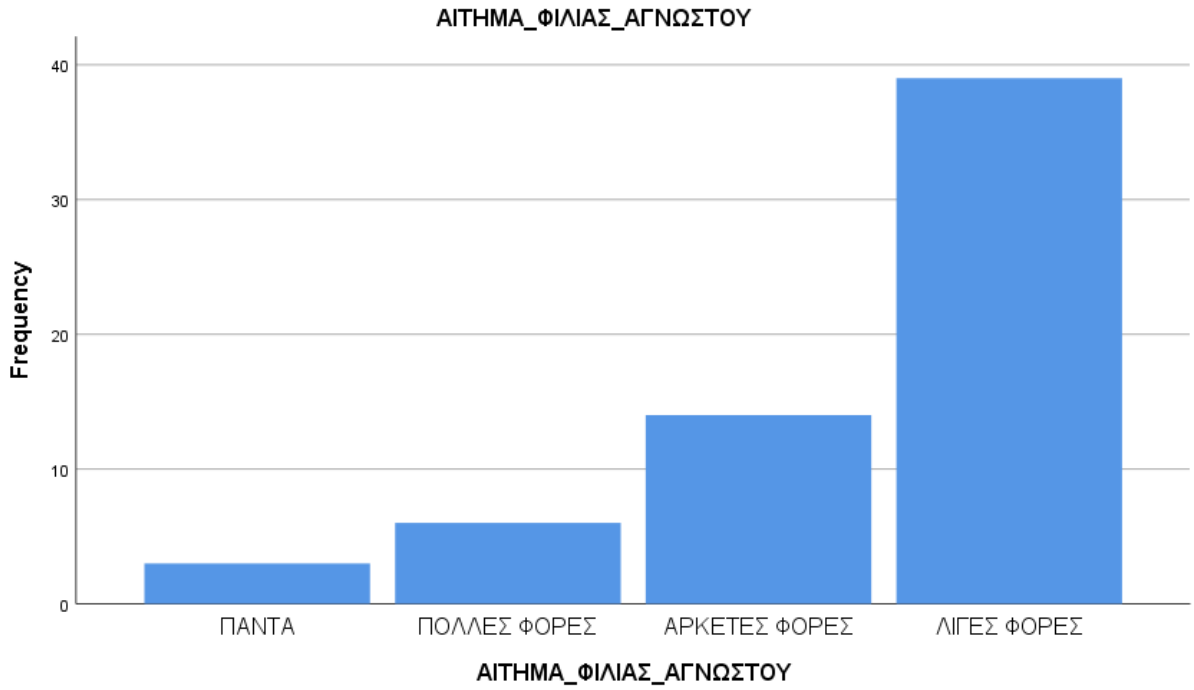
10. Θα κάνατε φίλο κάποιον που σας κάνει αίτημα φιλίας χωρίς να τον γνωρίζεται;

Στον παρακάτω πίνακα φαίνεται η άποψη των χρηστών σχετικά με το αν θα έκαναν κάποιον άγνωστο "φίλο" ο οποίος θα τους έκανε αίτημα φιλίας. Το μεγαλύτερο ποσοστό αφορά λίγες φορές (39%). Τα ποσοστά αυτά απεικονίζονται στο διάγραμμα 10.

Πίνακας 10

ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΝΤΑ	3	4,8	4,8	4,8
	ΠΟΛΛΕΣ ΦΟΡΕΣ	6	9,7	9,7	14,5
	ΑΡΚΕΤΕΣ ΦΟΡΕΣ	14	22,6	22,6	37,1
	ΛΙΓΕΣ ΦΟΡΕΣ	39	62,9	62,9	100,0
	Total	62	100,0	100,0	

Διάγραμμα 10



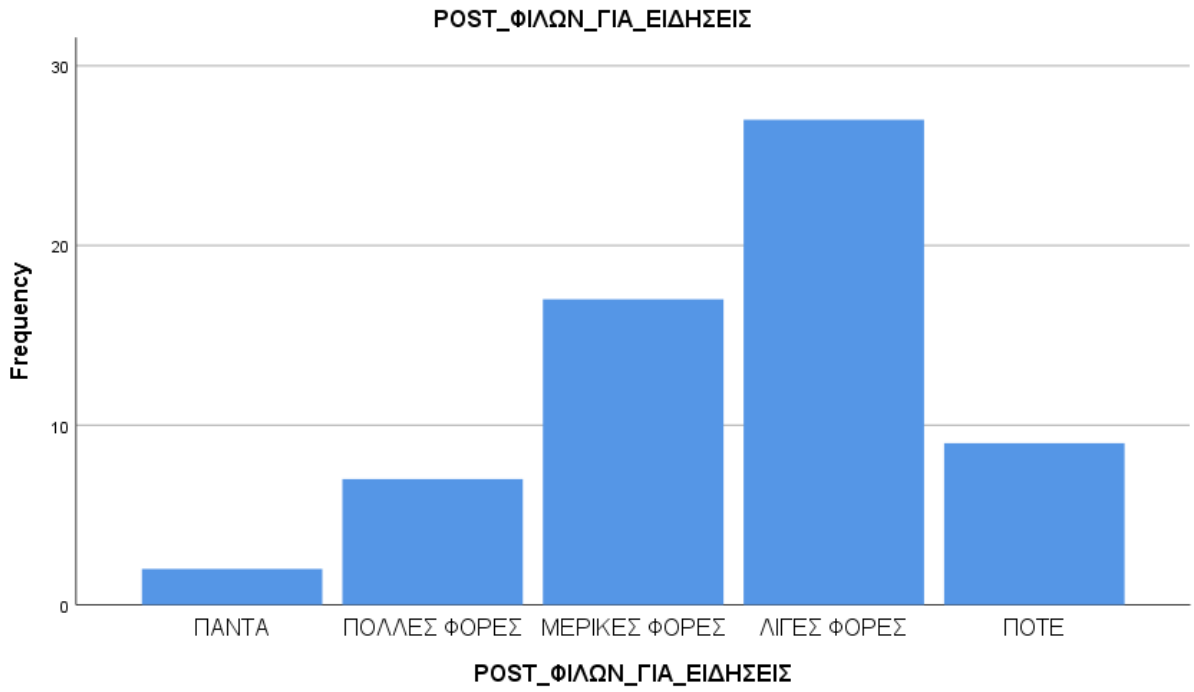
<u>11. Εμπιστεύεστε τα post των φίλων σας στα ΜΚΔ όταν μοιράζονται ειδήσεις στα κοινωνικά δίκτυα;</u>

Στον πίνακα και στο διάγραμμα 11 παρουσιάζεται και απεικονίζεται αντίστοιχα η άποψη των χρηστών για το αν και κατά πόσο εμπιστεύονται ειδήσεις από post φίλων τους. Η άποψη που υπερισχύει είναι λίγες φορές.

Πίνακας 11

POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΝΤΑ	2	3,2	3,2	3,2
	ΠΟΛΛΕΣ ΦΟΡΕΣ	7	11,3	11,3	14,5
	ΜΕΡΙΚΕΣ ΦΟΡΕΣ	17	27,4	27,4	41,9
	ΛΙΓΕΣ ΦΟΡΕΣ	27	43,5	43,5	85,5
	ΠΟΤΕ	9	14,5	14,5	100,0
	Total	62	100,0	100,0	

Διάγραμμα 11



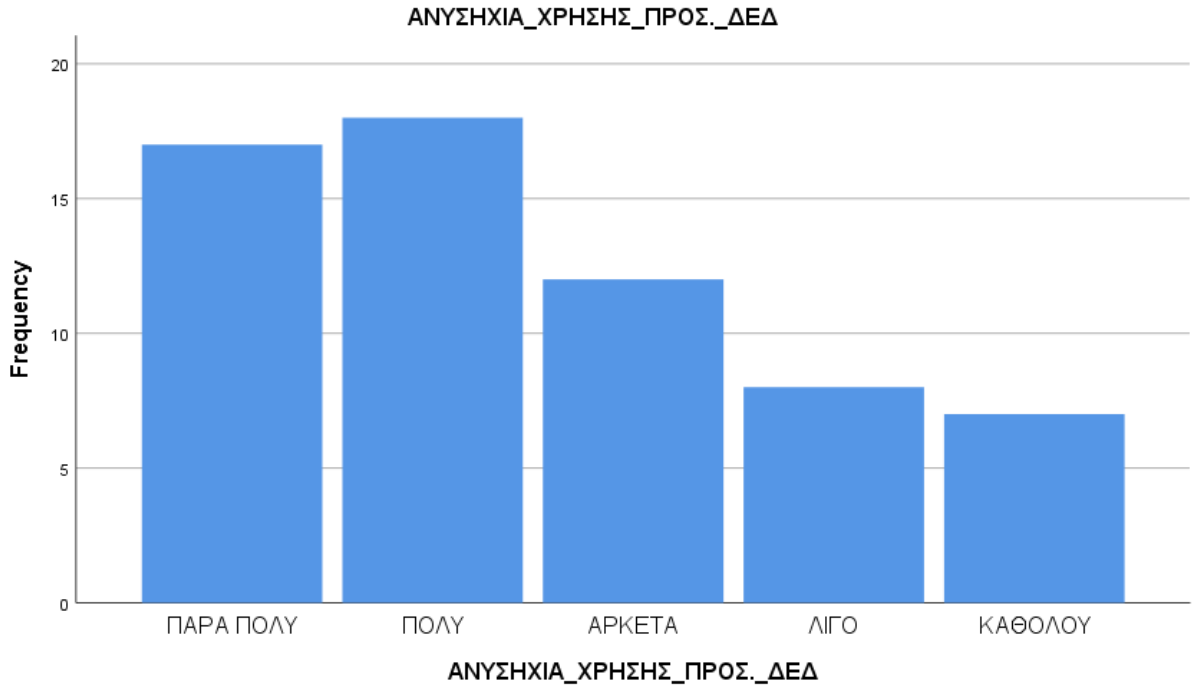
12. Σας ανησυχεί το γεγονός ότι τα ίδια τα ΜΚΔ μπορεί να χρησιμοποιούν προσωπικά σας στοιχεία;

Στον πίνακα και στο διάγραμμα 12 παρουσιάζεται και απεικονίζεται αντίστοιχα η άποψη των χρηστών για το κατά πόσο ανησυχούν οι χρήστες από το γεγονός της χρήσης των προσωπικών τους στοιχείων από τα ίδια τα ΜΚΔ προς όφελος τρίτων (π.χ. διαφημιστικές εταιρείες) . Η ανησυχία των ερωτηθέντων είναι έκδηλη και φτάνει σε αθροιστικό ποσοστό το 75% (από πάρα πολύ μέχρι αρκετά).

Πίνακας 12

ΑΝΥΣΗΧΙΑ_ΧΡΗΣΗΣ_ΠΡΟΣ._ΔΕΔ

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	17	27,4	27,4	27,4
	ΠΟΛΥ	18	29,0	29,0	56,5
	ΑΡΚΕΤΑ	12	19,4	19,4	75,8
	ΛΙΓΟ	8	12,9	12,9	88,7
	ΚΑΘΟΛΟΥ	7	11,3	11,3	100,0
	Total	62	100,0	100,0	



Διάγραμμα 12

<u>13. Πόσο συχνά διαβάζετε ειδήσεις από τα ΜΚΔ;</u>

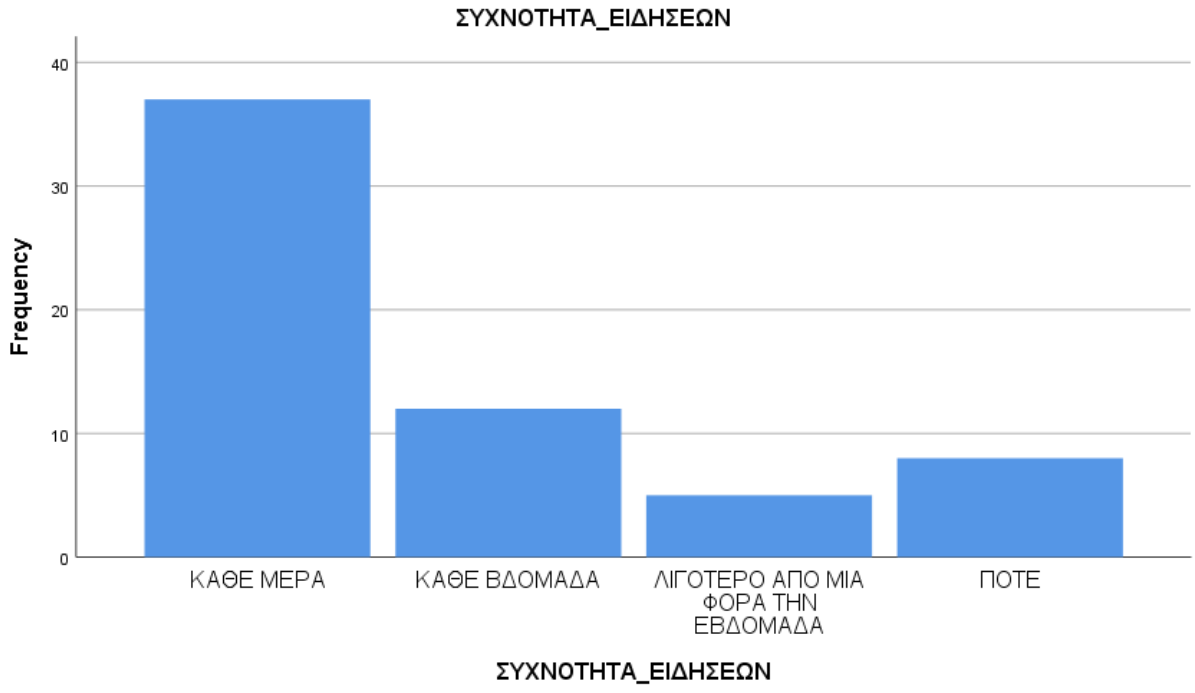
Στον παρακάτω πίνακα παρουσιάζεται η ξεκάθαρη προτίμηση των χρηστών να ενημερώνονται καθημερινά από τα ΜΚΔ σε ποσοστό 59,7%.

Πίνακας 13

ΣΥΧΝΟΤΗΤΑ_ΕΙΔΗΣΕΩΝ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΚΑΘΕ ΜΕΡΑ	37	59,7	59,7	59,7
	ΚΑΘΕ ΒΔΟΜΑΔΑ	12	19,4	19,4	79,0
	ΛΙΓΟΤΕΡΟ ΑΠΟ ΜΙΑ ΦΟΡΑ ΤΗΝ ΕΒΔΟΜΑΔΑ	5	8,1	8,1	87,1
	ΠΟΤΕ	8	12,9	12,9	100,0
	Total	62	100,0	100,0	

Η ίδια προτίμηση απεικονίζεται στο διάγραμμα 13

Διάγραμμα 13



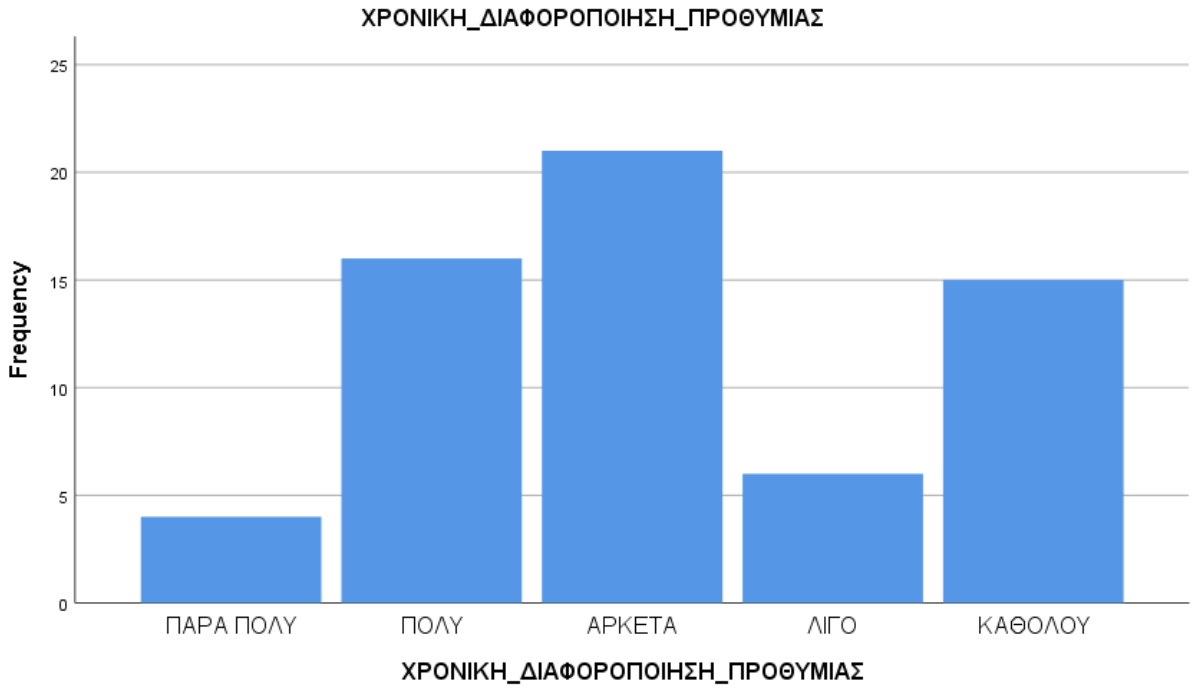
14. Με την πάροδο του χρόνου διαφοροποιείται η προθυμία σας να ανταλλάσσεται προσωπικά ή μη δεδομένα στα ΜΚΔ;

Στον παρακάτω πίνακα εκφράζεται η άποψη αν και κατά πόσο οι χρήστες με την πάροδο του χρόνου διαφοροποιούνται ως προς την ανταλλαγή προσωπικών ή μη δεδομένων. Οι προτιμήσεις πολύ και αρκετά συγκεντρώνουν μαζί ποσοστό 37%. Στο Διάγραμμα 14 παρουσιάζεται η παραπάνω προθυμία.

Πίνακας 14

ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	4	6,5	6,5	6,5
	ΠΟΛΥ	16	25,8	25,8	32,3
	ΑΡΚΕΤΑ	21	33,9	33,9	66,1
	ΛΙΓΟ	6	9,7	9,7	75,8
	ΚΑΘΟΛΟΥ	15	24,2	24,2	100,0
	Total	62	100,0	100,0	

Διάγραμμα 14



Ασφάλεια (Security)

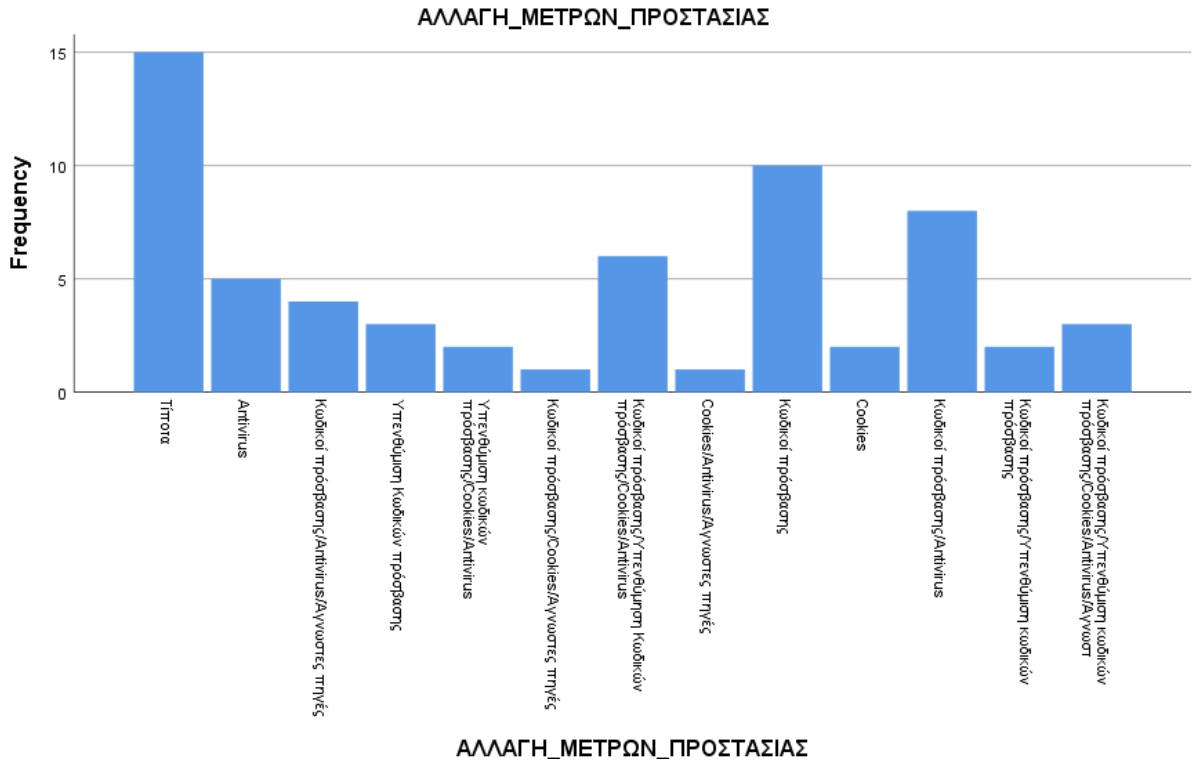
15. **Λαμβάνετε μέτρα προστασίας των προσωπικών σας λογαριασμών στα ΜΚΔ; Αν ναι ποιά από τα ακόλουθα εφαρμόζετε;**

Στον παρακάτω πίνακα παρουσιάζονται τα μέτρα που λαμβάνει ο κάθε χρήστης για τη προστασία των προσωπικών του λογαριασμών. Δυστυχώς ένας στους τέσσερις περίπου δεν εφαρμόζει κανένα μέτρο. Στο διάγραμμα 15 απεικονίζονται τα παραπάνω μέτρα.

Πίνακας 15

ΑΛΛΑΓΗ_ΜΕΤΡΩΝ_ΠΡΟΣΤΑΣΙΑΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Τίποτα	15	24.2	24.2	24.2
	Antivirus	5	8.1	8.1	32.3
	Κωδικοί πρόσβασης/Antivirus/Άγνωστες πηγές	4	6.5	6.5	38.7
	Υπενθύμιση Κωδικών πρόσβασης	3	4.8	4.8	43.5
	Υπενθύμιση κωδικών πρόσβασης/Cookies/Antivirus	2	3.2	3.2	46.8
	Κωδικοί πρόσβασης/Cookies/Άγνωστες πηγές	1	1.6	1.6	48.4
	Κωδικοί πρόσβασης/Υπενθύμηση Κωδικών πρόσβασης/Cookies/Antivirus	6	9.7	9.7	58.1
	Cookies/Antivirus/Άγνωστες πηγές	1	1.6	1.6	59.7
	Κωδικοί πρόσβασης	10	16.1	16.1	75.8
	Cookies	2	3.2	3.2	79.0
	Κωδικοί πρόσβασης/Antivirus	8	12.9	12.9	91.9
	Κωδικοί πρόσβασης/Υπενθύμιση κωδικών πρόσβασης	2	3.2	3.2	95.2
	Κωδικοί πρόσβασης/Υπενθύμιση κωδικών πρόσβασης/Cookies/Antivirus/Άγνωστ	3	4.8	4.8	100.0
	Total	62	100.0	100.0	

Διάγραμμα 15



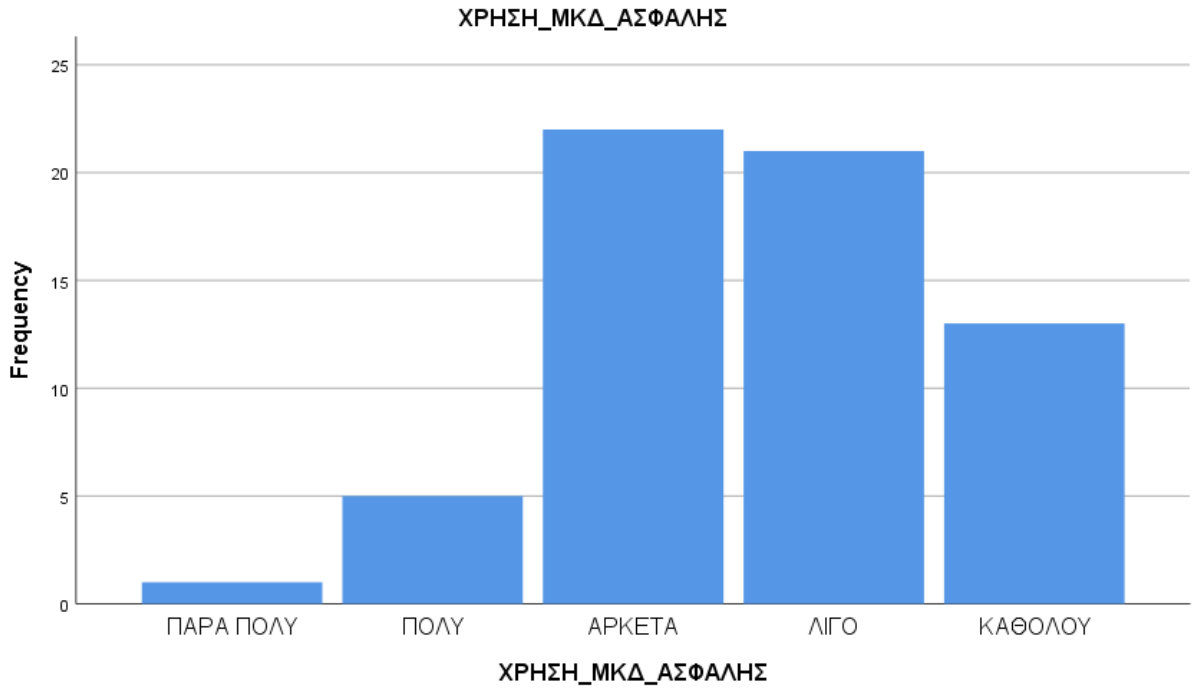
16.Η χρήση των ΜΚΔ είναι ασφαλής;

Στον πίνακα και στο διάγραμμα 16 παρουσιάζεται και απεικονίζεται αντίστοιχα η άποψη των χρηστών για το κατά πόσο θεωρούν οι χρήστες τα ΜΚΔ ασφαλή. Η άποψη που κυριαρχεί είναι αρκετά σε ποσοστό 35,5% ενώ η άποψη λίγο ακολουθεί με ποσοστό 33,9%

Πίνακας 16

ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	1	1,6	1,6	1,6
	ΠΟΛΥ	5	8,1	8,1	9,7
	ΑΡΚΕΤΑ	22	35,5	35,5	45,2
	ΛΙΓΟ	21	33,9	33,9	79,0
	ΚΑΘΟΛΟΥ	13	21,0	21,0	100,0
	Total	62	100,0	100,0	

Διάγραμμα 16



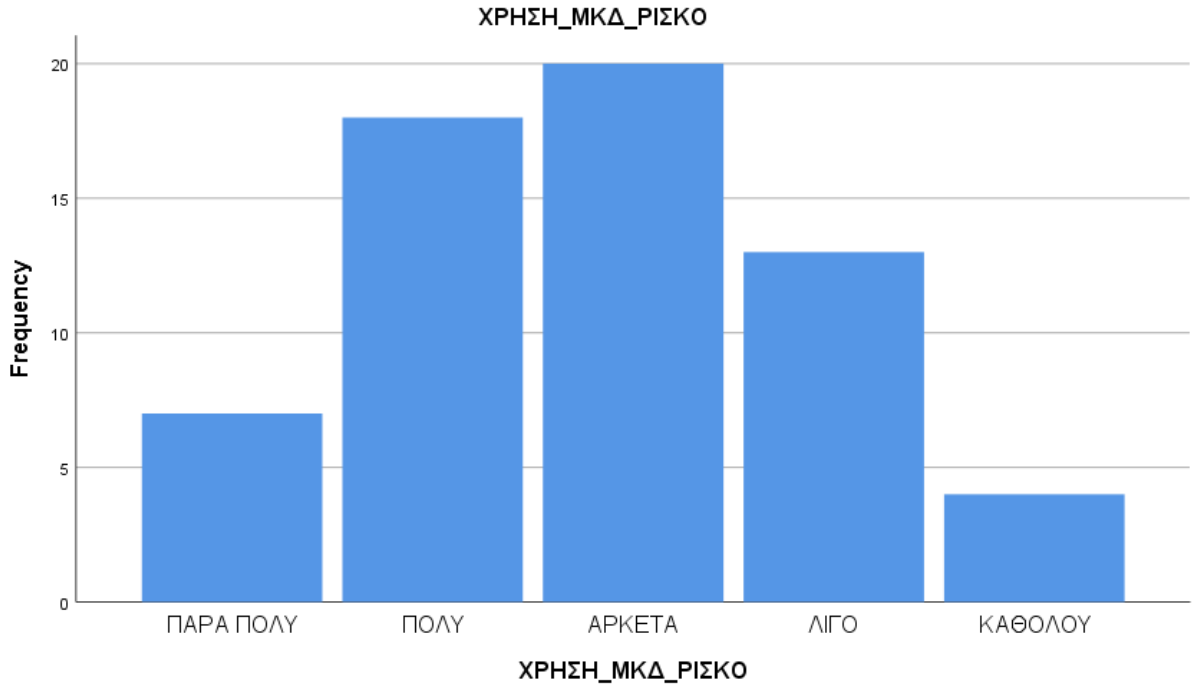
17. Η επικοινωνία στα ΜΚΔ εμπεριέχει ρίσκο;

Στον πίνακα και στο διάγραμμα 17 παρουσιάζεται και απεικονίζεται αντίστοιχα η άποψη των χρηστών για το κατά πόσο θεωρούν οι χρήστες ότι παίρνουν ρίσκο ανταλλάσοντας δεδομένα στα ΜΚΔ. Οι απόψεις αρκετά και πολύ κατέχουν ποσοστά 20% και 18% αντίστοιχα.

Πίνακας 17

ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	7	11,3	11,3	11,3
	ΠΟΛΥ	18	29,0	29,0	40,3
	ΑΡΚΕΤΑ	20	32,3	32,3	72,6
	ΛΙΓΟ	13	21,0	21,0	93,5
	ΚΑΘΟΛΟΥ	4	6,5	6,5	100,0
	Total	62	100,0	100,0	

Διάγραμμα 17



<u>18. Είστε ενημερωμένοι με τους κινδύνους που ελλοχεύουν στα ΜΚΔ;</u>

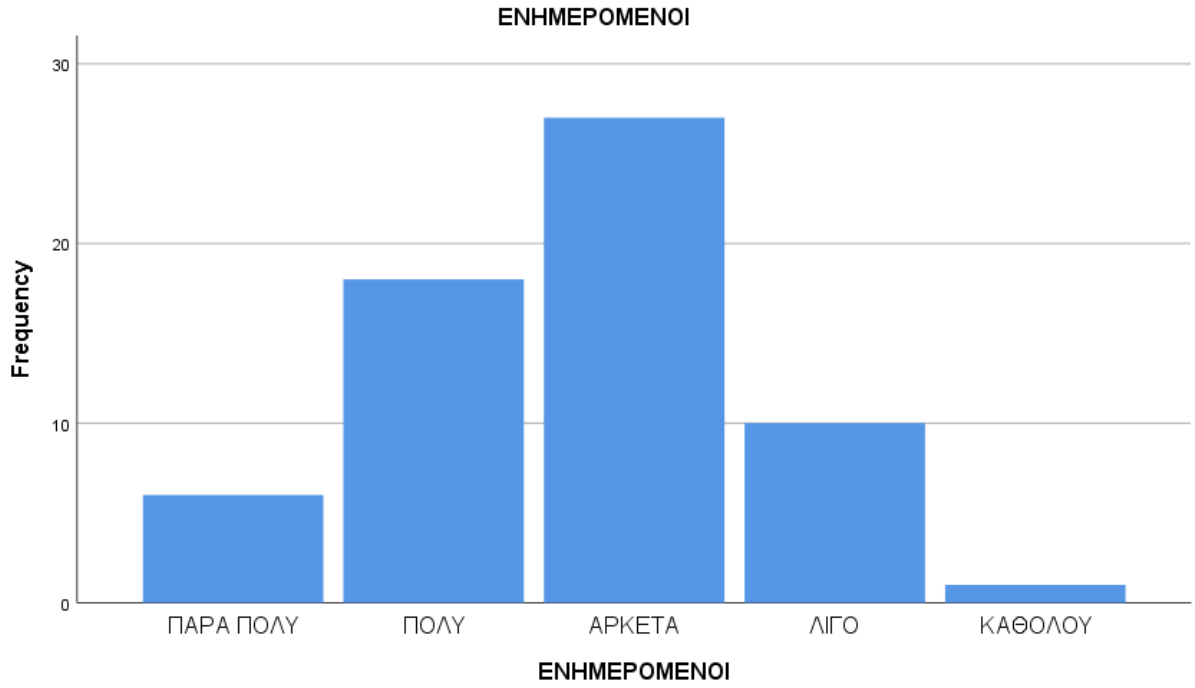
Στον πίνακα 18 παρουσιάζεται η άποψη για το κατά πόσο οι χρήστες θεωρούν τον εαυτό τους ενημερωμένο σχετικά με τους κινδύνους που ελλοχεύουν στα ΜΚΔ. Ένα πολύ μεγάλο ποσοστό της τάξης του 43,5% απάντησε αρκετά.

Πίνακας 18

ΕΝΗΜΕΡΟΜΕΝΟΙ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	6	9,7	9,7	9,7
	ΠΟΛΥ	18	29,0	29,0	38,7
	ΑΡΚΕΤΑ	27	43,5	43,5	82,3
	ΛΙΓΟ	10	16,1	16,1	98,4
	ΚΑΘΟΛΟΥ	1	1,6	1,6	100,0
	Total	62	100,0	100,0	

Στο παρακάτω διάγραμμα παρουσιάζεται η θεώρηση των χρηστών σχετικά με τη γνώση των κινδύνων στα ΜΚΔ.

Διάγραμμα 18



Ιδιωτικότητα (Privacy)

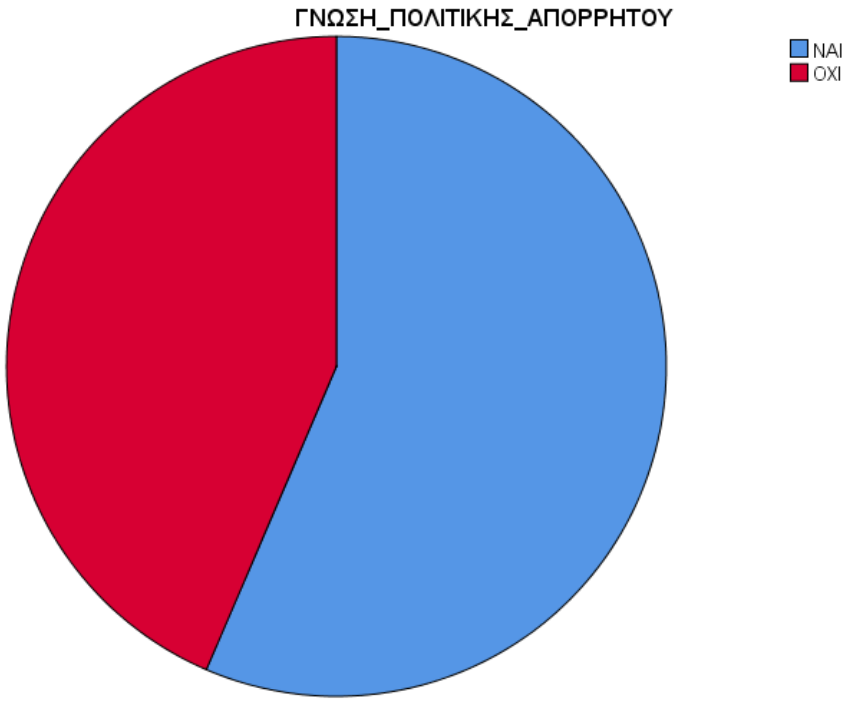
19. Γνωρίζετε για την πολιτική απορρήτου των ΜΚΔ;

Στον Πίνακα και στο διάγραμμα 19 αντίστοιχα παρουσιάζεται η γνώση ή μη της πολιτικής απορρήτου στα ΜΚΔ. Εντύπωση προκαλεί ότι ένα ποσοστό 43,5% δεν γνωρίζει για την πολιτική απορρήτου.

Πίνακας 19

ΓΝΩΣΗ_ΠΟΛΙΤΙΚΗΣ_ΑΠΟΡΡΗΤΟΥ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	NAI	35	56,5	56,5	56,5
	OXI	27	43,5	43,5	100,0
	Total	62	100,0	100,0	

Διάγραμμα 19



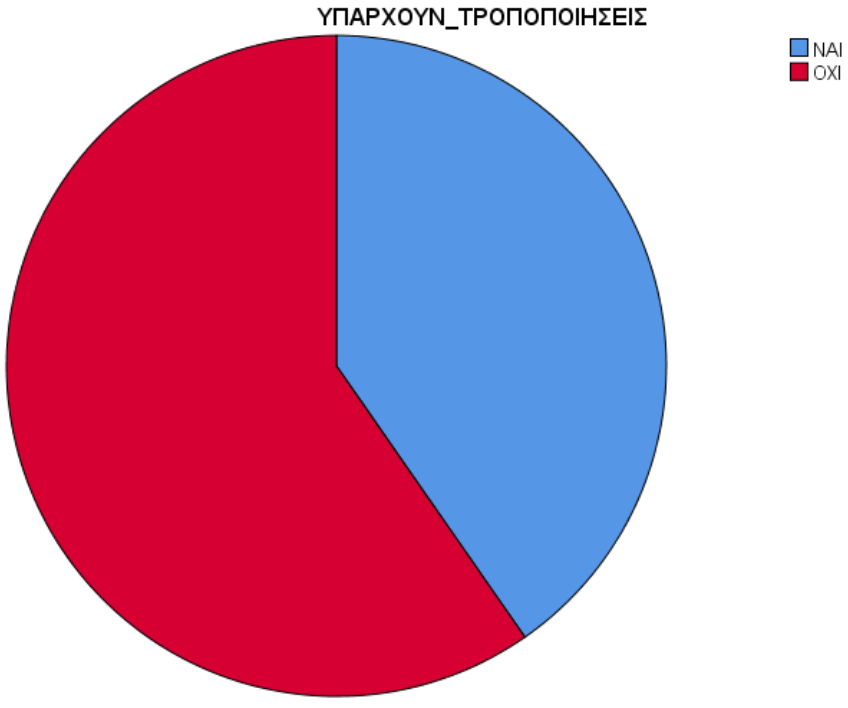
20. Έχετε κάνει τροποποιήσεις στις βασικές ρυθμίσεις απορρήτου

Στον παρακάτω πίνακα και στο ακόλουθο διάγραμμα παρουσιάζονται αντίστοιχα οι απαντήσεις των χρηστών σχετικά με το αν έχουν κάνει αλλαγές στις βασικές ρυθμίσεις απορρήτου. Ένα σημαντικό ποσοστό 59,7% δεν έχει κάνει αλλαγές.

Πίνακας 20

ΥΠΑΡΧΟΥΝ_ΤΡΟΠΟΠΟΙΗΣΕΙΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	NAI	25	40,3	40,3	40,3
	OXI	37	59,7	59,7	100,0
	Total	62	100,0	100,0	

Διάγραμμα 20



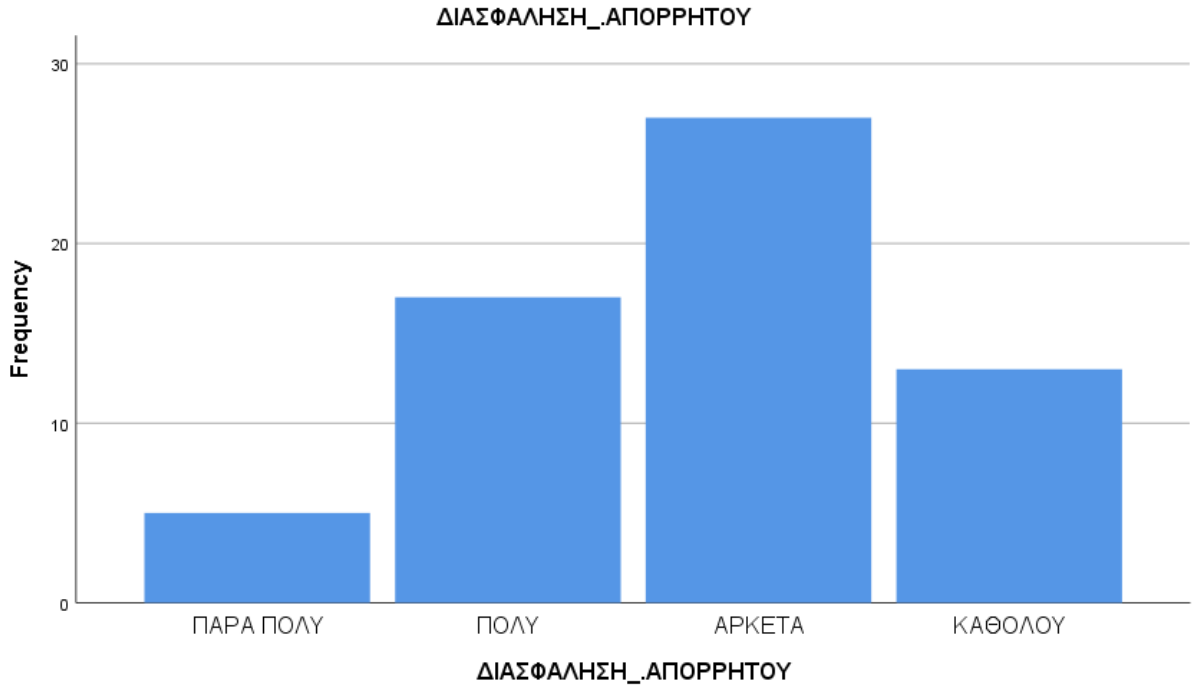
<u>21. Διασφαλίζεται το απόρρητο των προσωπικών σας δεδομένων;</u>

Στον παρακάτω πίνακα και στο διάγραμμα που ακολουθεί παρουσιάζονται οι απαντήσεις των χρηστών για το εάν θεωρούν ότι διασφαλίζεται το απόρρητο στα προσωπικά δεδομένα τους.

Πίνακας 21

ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	5	8,1	8,1	8,1
	ΠΟΛΥ	17	27,4	27,4	35,5
	ΑΡΚΕΤΑ	27	43,5	43,5	79,0
	ΚΑΘΟΛΟΥ	13	21,0	21,0	100,0
	Total	62	100,0	100,0	

Διάγραμμα 21



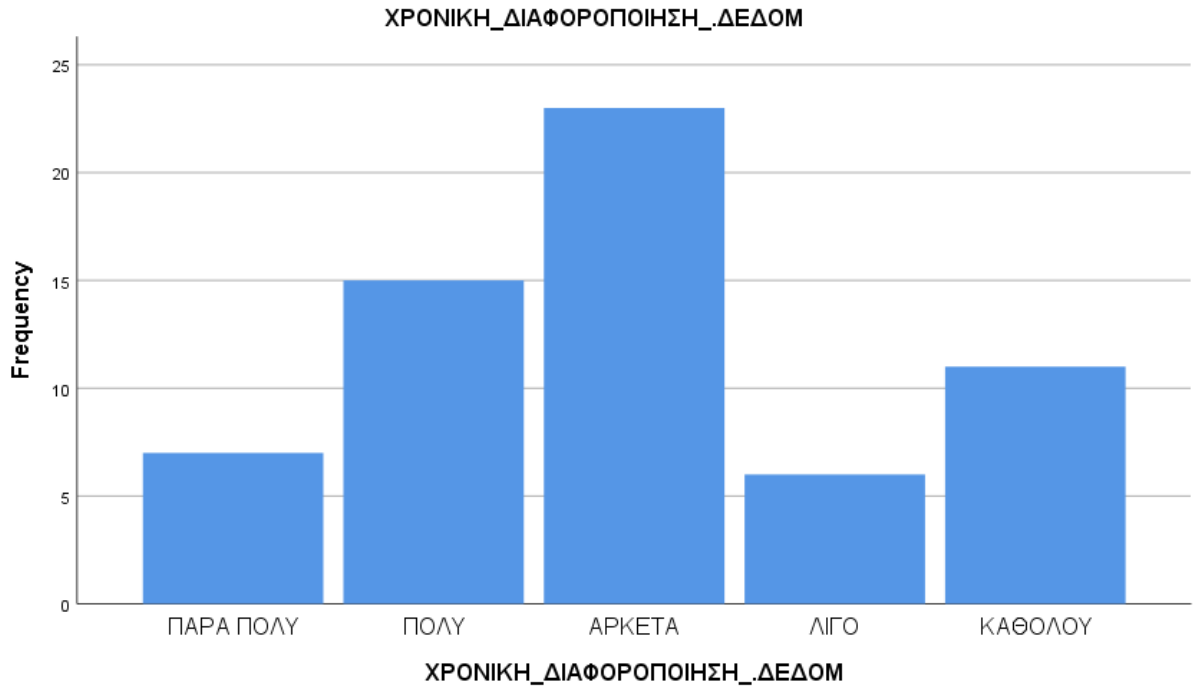
22. Με την πάροδο του χρόνου έχει διαφοροποιηθεί η άποψη σας γύρω από τα προσωπικά δεδομένα και της προστασίας τους;

Στον παρακάτω πίνακα και στο διάγραμμα που ακολουθεί παρουσιάζονται οι απαντήσεις των χρηστών σχετικά με το εάν διαφοροποιείται η άποψη τους χρονικά για τα προσωπικά δεδομένα. Ένα ποσοστό 38% απάντησε συνολικά πολύ και αρκετά πράγμα που δείχνει ότι οι χρήστες με την εμπειρία που αποκτούν αλλάζουν άποψη για την διάθεση των προσωπικών τους δεδομένων.

Πίνακας 22

ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_.ΔΕΔΟΜ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	7	11,3	11,3	11,3
	ΠΟΛΥ	15	24,2	24,2	35,5
	ΑΡΚΕΤΑ	23	37,1	37,1	72,6
	ΛΙΓΟ	6	9,7	9,7	82,3
	ΚΑΘΟΛΟΥ	11	17,7	17,7	100,0
	Total	62	100,0	100,0	

Διάγραμμα 22



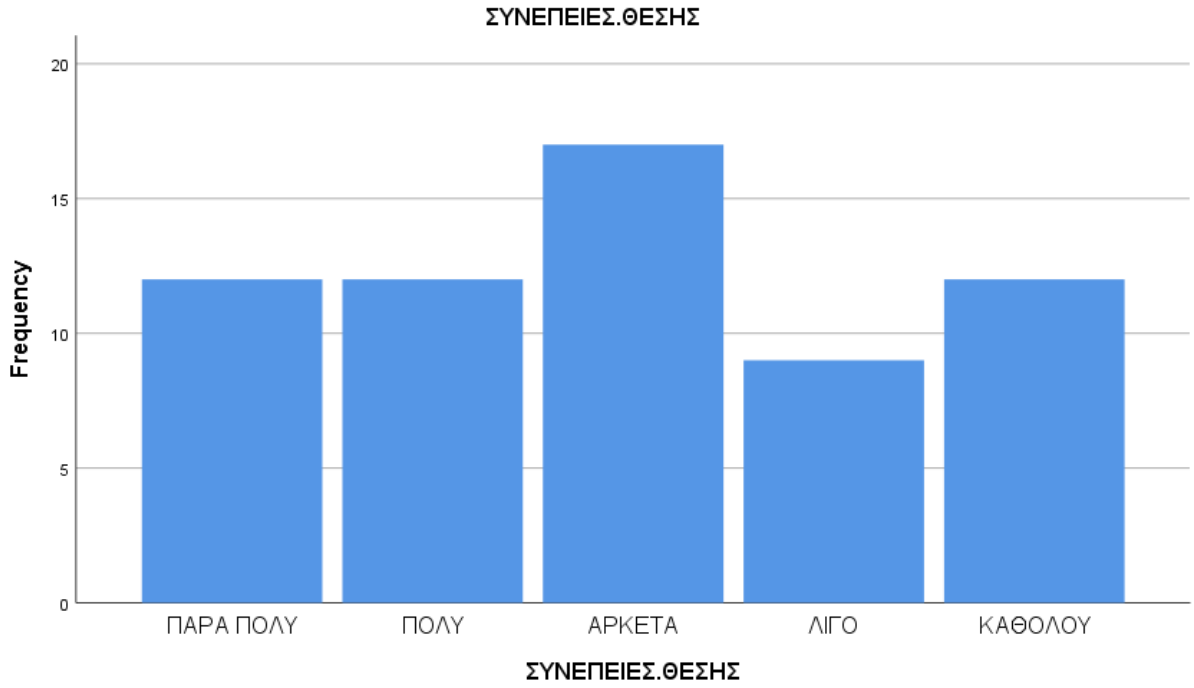
23. Γνωρίζετε τις συνέπειες δημοσιοποίησης της θέσης στην οποία βρίσκεστε:

Στον παρακάτω πίνακα και στο διάγραμμα που ακολουθεί παρουσιάζονται οι απαντήσεις των χρηστών σχετικά με το εάν οι χρήστες θεωρούν ότι υπάρχουν συνέπειες από τη δημοσιοποίηση της θέσης τους. Οι χρήστες απάντησαν και στις πέντε επιλογές με παρόμοια ποσοστά εξαιρώντας την απάντηση 'αρκετά' η οποία είχε λίγο μεγαλύτερο ποσοστό.

Πίνακας 23

ΣΥΝΕΠΕΙΕΣ.ΘΕΣΗΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	12	19,4	19,4	19,4
	ΠΟΛΥ	12	19,4	19,4	38,7
	ΑΡΚΕΤΑ	17	27,4	27,4	66,1
	ΛΙΓΟ	9	14,5	14,5	80,6
	ΚΑΘΟΛΟΥ	12	19,4	19,4	100,0
	Total	62	100,0	100,0	

Διάγραμμα 23



Γνώση ενημέρωσης των χρηστών (user awareness)

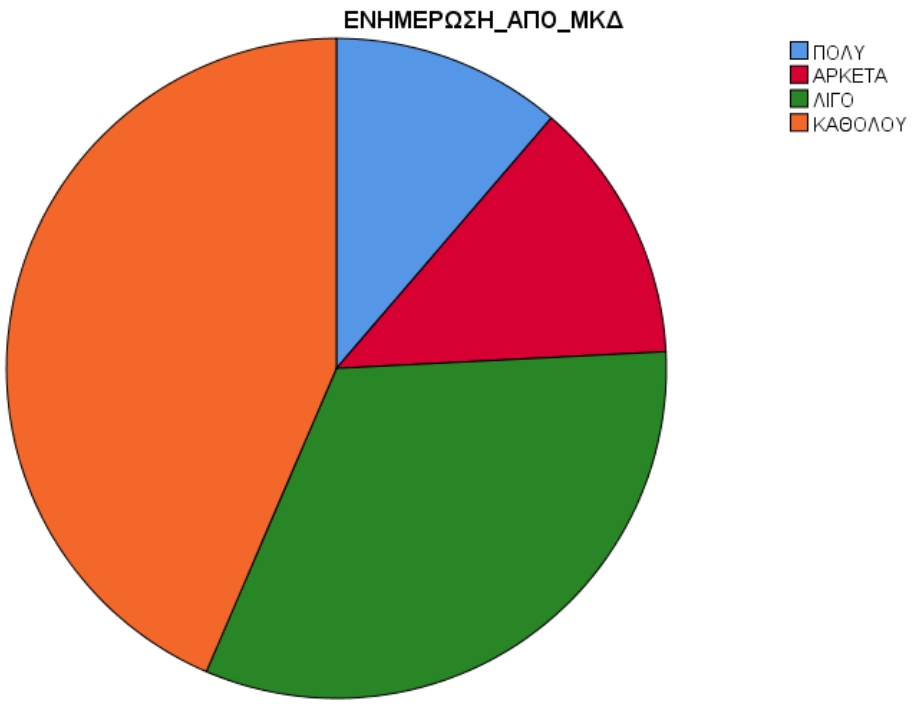
24. Θεωρείτε ότι τα ΜΚΔ ενημερώνουν επαρκώς τους χρήστες για τις πιθανές επιπτώσεις της διάθεσης των προσωπικών τους δεδομένων;

Στον παρακάτω πίνακα και στο διάγραμμα που ακολουθεί παρουσιάζονται οι απαντήσεις των χρηστών σχετικά με το εάν οι χρήστες θεωρούν ότι τα ίδια τα ΜΚΔ ενημερώνουν επαρκώς τους χρήστες τους για πιθανές επιπτώσεις της διάθεσης των προσωπικών τους δεδομένων. Η πλειοψηφία των χρηστών απάντησε καθόλου σε ποσοστό 43,5%.

Πίνακας 24

ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΟΛΥ	7	11,3	11,3	11,3
	ΑΡΚΕΤΑ	8	12,9	12,9	24,2
	ΛΙΓΟ	20	32,3	32,3	56,5
	ΚΑΘΟΛΟΥ	27	43,5	43,5	100,0
	Total	62	100,0	100,0	

Διάγραμμα 24



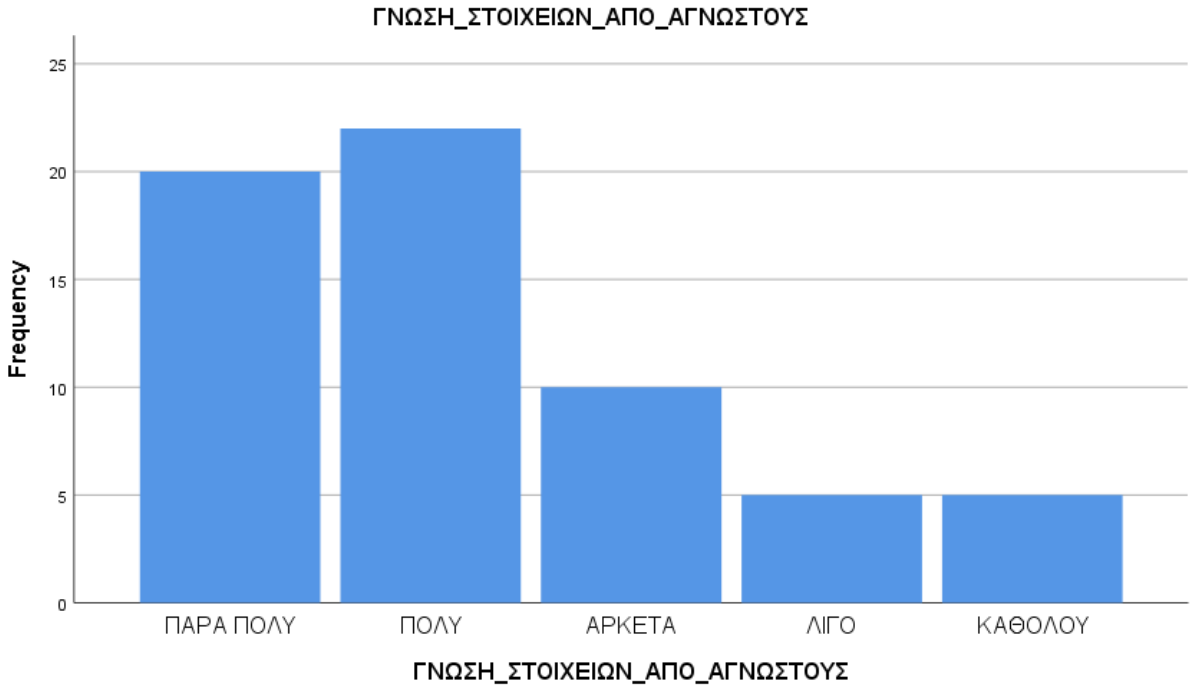
25. Σας ενοχλεί εάν κάποιος που δεν γνωρίζετε μπορεί να βρει τα προσωπικά σας στοιχεία στην σελίδα κοινωνικής δικτύωσης ;

Στην παραπάνω ερώτηση οι χρήστες απάντησαν με συντριπτική πλειοψηφία ότι τους ενοχλεί πολύ (35,5%) ή πάρα πολύ (32,5%). Αυτά παρουσιάζονται στον ακόλουθο πίνακα και στο γράφημα που ακολουθεί αντίστοιχα.

Πίνακας 25

ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	20	32,3	32,3	32,3
	ΠΟΛΥ	22	35,5	35,5	67,7
	ΑΡΚΕΤΑ	10	16,1	16,1	83,9
	ΛΙΓΟ	5	8,1	8,1	91,9
	ΚΑΘΟΛΟΥ	5	8,1	8,1	100,0
	Total	62	100,0	100,0	

Γράφημα 25



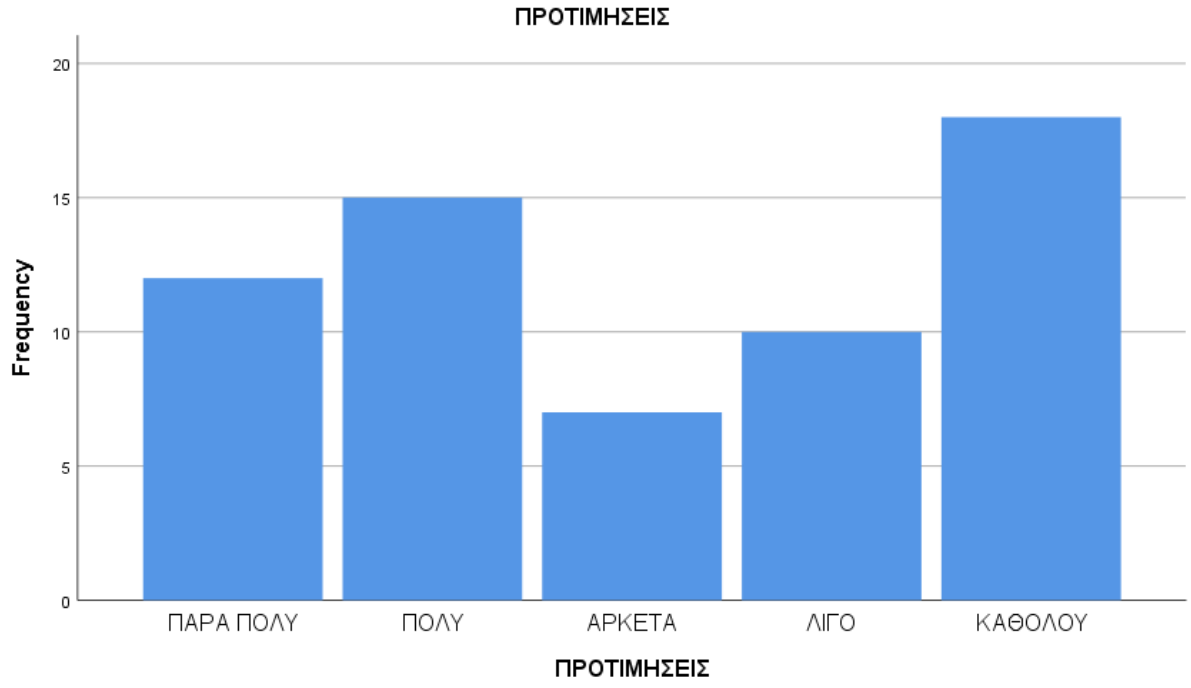
<u>26. Σας ενοχλεί αν κάποιος θα μπορούσε να διαπιστώσει τις προτιμήσεις σας σχετικά με τη μουσική, το διάβασμα, τις ταινίες , ακόμα και τις πολιτικές πεποιθήσεις από το προφίλ ή τα post που κάνετε στα ΜΚΔ</u>

Στην παραπάνω ερώτηση οι χρήστες απάντησαν με μικρή πλειοψηφία ότι δεν ενοχλούνται από το αν κάποιος μπορεί να βρει τις παραπάνω προτιμήσεις σε ποσοστό 29%. Αυτά παρουσιάζονται στον ακόλουθο πίνακα και στο γράφημα που ακολουθεί αντίστοιχα.

Πίνακας 26

ΠΡΟΤΙΜΗΣΕΙΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	12	19,4	19,4	19,4
	ΠΟΛΥ	15	24,2	24,2	43,5
	ΑΡΚΕΤΑ	7	11,3	11,3	54,8
	ΛΙΓΟ	10	16,1	16,1	71,0
	ΚΑΘΟΛΟΥ	18	29,0	29,0	100,0
	Total	62	100,0	100,0	

Διάγραμμα 26



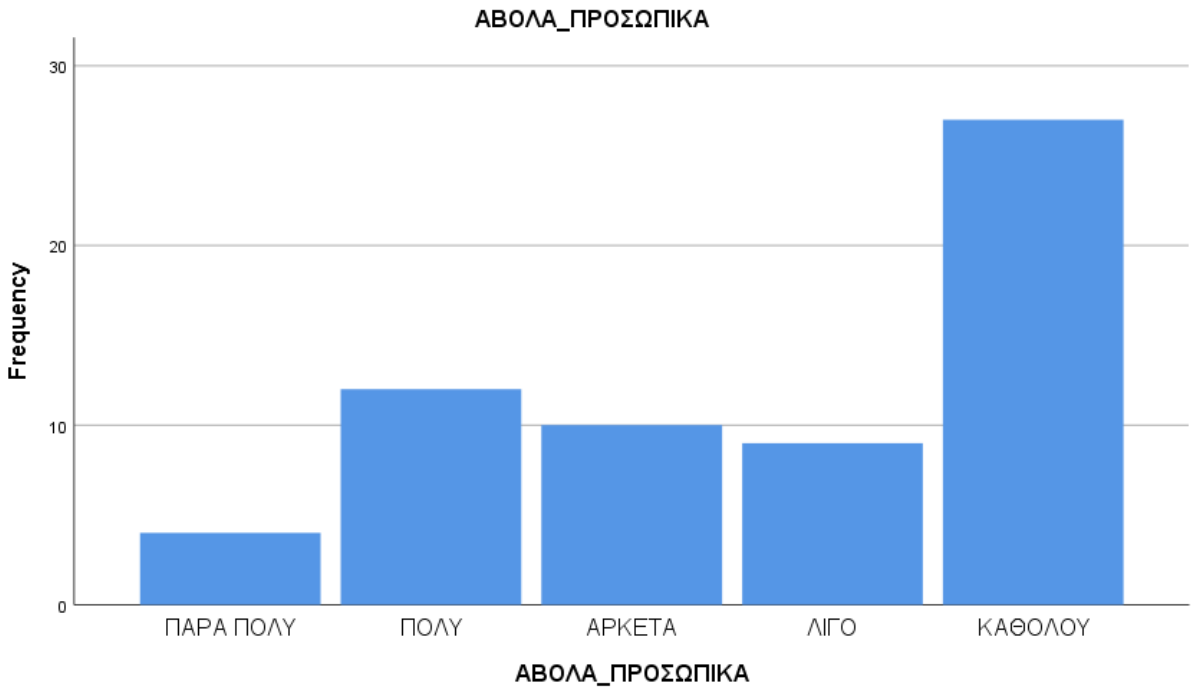
27.Νιώθετε άβολα όταν μοιράζεστε προσωπικές πληροφορίες στα ΜΚΔ

Στην παραπάνω ερώτηση οι χρήστες απάντησαν στο ερώτημα αν νιώθουν άβολα όταν μοιράζονται τα προσωπικά τους δεδομένα. Η συνηθέστερη απάντηση ήταν καθόλου σε ποσοστό 43,5%.

Πίνακας 27

ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	4	6,5	6,5	6,5
	ΠΟΛΥ	12	19,4	19,4	25,8
	ΑΡΚΕΤΑ	10	16,1	16,1	41,9
	ΛΙΓΟ	9	14,5	14,5	56,5
	ΚΑΘΟΛΟΥ	27	43,5	43,5	100
	Total	62	100	100	

Διάγραμμα 27



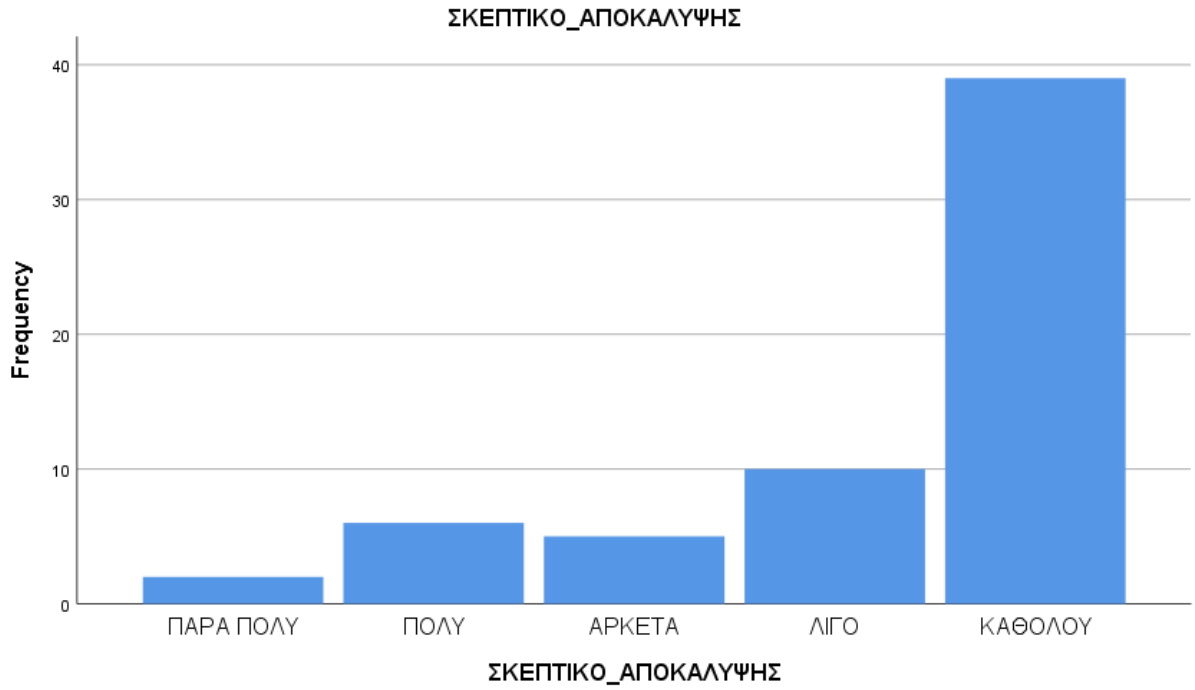
28. Αποκαλύπτετε προσωπικές πληροφορίες με το σκεπτικό ότι το κάνουν όλοι αυτό;

Στην παραπάνω ερώτηση οι χρήστες απάντησαν στο ερώτημα αν αποκαλύπτουν προσωπικές πληροφορίες με το σκεπτικό ότι οι περισσότεροι χρήστες κάνουν το ίδιο.

Πίνακας 28

ΣΚΕΠΤΙΚΟ_ΑΠΟΚΑΛΥΨΗΣ					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ΠΑΡΑ ΠΟΛΥ	2	3,2	3,2	3,2
	ΠΟΛΥ	6	9,7	9,7	12,9
	ΑΡΚΕΤΑ	5	8,1	8,1	21,0
	ΛΙΓΟ	10	16,1	16,1	37,1
	ΚΑΘΟΛΟΥ	39	62,9	62,9	100,0
	Total	62	100,0	100,0	

Διάγραμμα 28



12.2 Έλεγχοι καταλληλότητας ερωτηματολογίου

Στην συνέχεια, αυτό που πρέπει να δείξουμε είναι ότι το ερωτηματολόγιο μας είναι κατάλληλο για αυτά που θέλουμε να μετρήσουμε. Για να το δείξουμε αυτό χρησιμοποιήσαμε την Ανάλυση παραγόντων (Factor Analysis).

Και το SPSS μας δίνει τα αποτελέσματα στο φύλλο output σε πίνακες. Τα αποτελέσματα λοιπόν φαίνονται στους πίνακες 29:

Εγκυρότητα ερωτηματολογίου

Πίνακας 29

Descriptive Statistics

	Mean	Std. Deviation	Analysis N
ΗΛΙΚΙΑ	3,94	,721	62
ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ	2,68	,672	62
ΕΜΠΙΣΤΑ_ΜΚΔ	4,47	3,793	62
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	4,44	,861	62
POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ	3,55	,986	62
ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	3,19	1,252	62
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	3,65	,960	62
ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	2,82	1,094	62
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	3,77	,876	62
ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	4,08	1,013	62
ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	2,24	1,224	62

Στον ακόλουθο πίνακα λαμβάνουμε τη σχέση ανάμεσα στις ερωτήσεις

Πίνακας 30

		ΗΛΙΚΙΑ	ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ	ΕΜΠΙΣΤΑ_ΜΚΔ	ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ	ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ
Correlation	ΗΛΙΚΙΑ	1	-0,044	0,035	-0,007	0,097	0,068	0,132	-0,098	0,158	0,187	0,092
	ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ	-0,044	1	-0,191	0,105	-0,1	-0,1	-0,18	0,01	-0,181	-0,033	-0,203
	ΕΜΠΙΣΤΑ_ΜΚΔ	0,035	-0,191	1	-0,048	0,263	0,001	0,046	0,056	0,146	0,156	-0,064
	ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	-0,007	0,105	-0,048	1	0,158	-0,034	0,131	-0,352	0,263	-0,003	-0,382
	POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ	0,097	-0,1	0,263	0,158	1	0,125	0,244	-0,167	0,203	0,135	-0,03
	ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	0,068	-0,1	0,001	-0,034	0,125	1	-0,133	-0,034	-0,094	-0,051	-0,01
	ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	0,132	-0,18	0,046	0,131	0,244	-0,133	1	-0,326	0,371	0,165	-0,177
	ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	-0,098	0,01	0,056	-0,352	-0,167	-0,034	-0,326	1	-0,436	-0,061	0,192
	ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	0,158	-0,181	0,146	0,263	0,203	-0,094	0,371	-0,436	1	0,279	-0,254
	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	0,187	-0,033	0,156	-0,003	0,135	-0,051	0,165	-0,061	0,279	1	-0,122
	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	0,092	-0,203	-0,064	-0,382	-0,03	-0,01	-0,177	0,192	-0,254	-0,122	1

Πίνακας 31: μας δείχνει την KMO μέτρηση

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,606
Bartlett's Test of Sphericity	Approx. Chi-Square	81,404
	df	55
	Sig.	,012

Ξέρουμε ότι αν η KMO μέτρηση έχει τιμή μεγαλύτερη από 0,5 τότε η ανάλυση παραγόντων είναι κατάλληλη για τα δεδομένα μας. Από τον πίνακα 31, μπορούμε να δούμε ότι η KMO μέτρηση για το ερωτηματολόγιο μας και τις ερωτήσεις που μετρούν την construct και τις subconstructs μας είναι ίση με 0,606. Η τιμή αυτή είναι αρκετά καλή.

Επίσης, ξέρουμε ότι το Bartlett's test εξετάζει τη μηδενική υπόθεση ο Correlation-matrix να είναι μοναδιαίος, δηλαδή οι συσχετίσεις να είναι 0. Εμείς παρατηρούμε ότι το Sig. στον πίνακα 31είναι μικρότερο από το 0,5. Άρα, υπάρχουν σημαντικές συσχετίσεις.

Ο πίνακας 32 μας δείχνει την συμμετοχικότητα των μεταβλητών

Πίνακας 32

Communalities		
	Initial	Extraction
ΗΛΙΚΙΑ	1,000	,743
ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ	1,000	,699
ΕΜΠΙΣΤΑ_ΜΚΔ	1,000	,729
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	1,000	,605
POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ	1,000	,517
ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	1,000	,797
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	1,000	,569
ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	1,000	,651
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	1,000	,624
ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	1,000	,667
ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	1,000	,664
Extraction Method: Principal Component Analysis.		

Η συμμετοχικότητα (communality) είναι το ποσό της διασποράς μιας μεταβλητής που εξηγείται από όλους μαζί τους παράγοντες και είναι αυτή που μας δείχνει την αξιοπιστία μιας μεταβλητής. Μεταβλητές με μικρή συμμετοχικότητα ίσως να πρέπει να αφαιρεθούν από το μοντέλο ανάλυσης παραγόντων διότι το μοντέλο αυτό δεν είναι αρκετά καλό γι' αυτές και χάνεται πολλή πληροφορία με τη μείωση των διαστάσεων.

Από τον πίνακα 32 όμως βλέπουμε ότι η συμμετοχικότητα των ερωτήσεων/μεταβλητών μας είναι αρκετά ψηλή και άρα δεν είναι απαραίτητο να αφαιρέσουμε καμία από το μοντέλο.

Ο Πίνακας 33 μας δείχνει τις ιδιοτιμές του πίνακα

Πίνακας 33

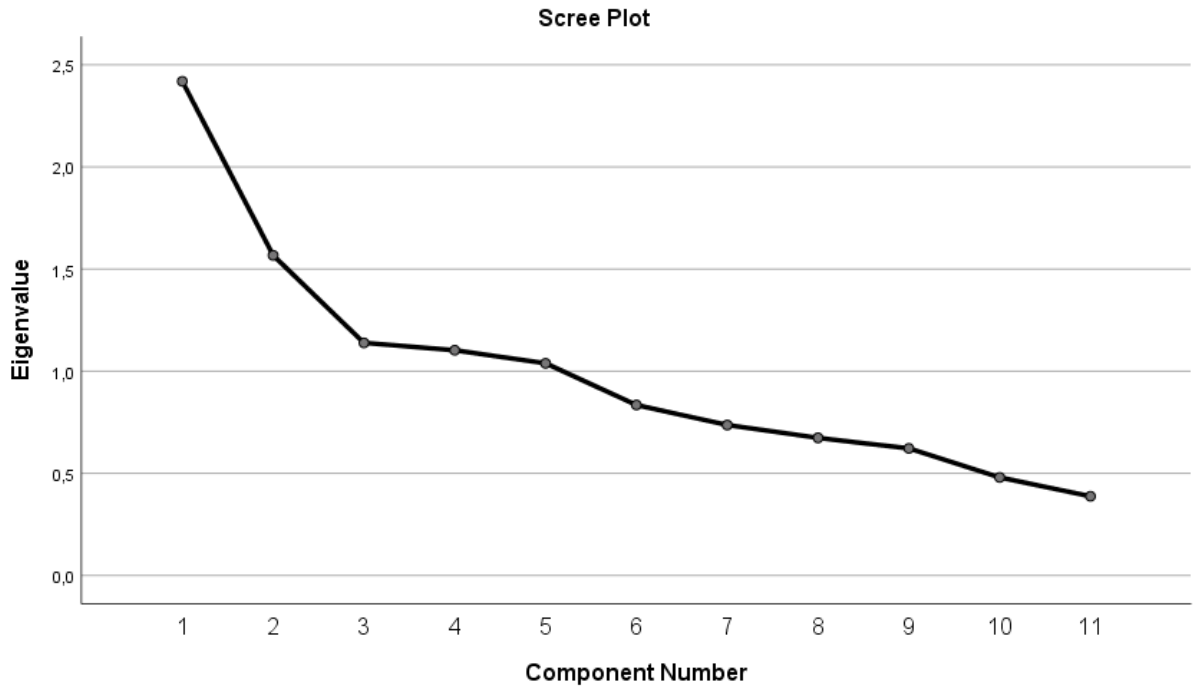
Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,419	21,992	21,992	2,419	21,992	21,992	2,042	18,562	18,562
2	1,567	14,247	36,239	1,567	14,247	36,239	1,517	13,789	32,350
3	1,139	10,352	46,591	1,139	10,352	46,591	1,371	12,460	44,811
4	1,102	10,022	56,613	1,102	10,022	56,613	1,201	10,922	55,732
5	1,039	9,441	66,055	1,039	9,441	66,055	1,135	10,322	66,055
6	,835	7,586	73,641						
7	,736	6,694	80,335						
8	,674	6,123	86,458						
9	,622	5,654	92,112						
10	,480	4,364	96,477						
11	,388	3,523	100,000						

Extraction Method: Principal Component Analysis.

Οι ιδιοτιμές (eigenvalues) παριστούν την συνολική διασπορά του συνόλου των δεδομένων που εξηγείται από κάθε παράγοντα, δηλαδή δείχνει την σπουδαιότητα του κάθε παράγοντα. Μεγάλη ιδιοτιμή σημαίνει ότι ο παράγοντας είναι σημαντικός. Τι σημαίνει όμως μεγάλη; Χρειαζόμαστε ένα κριτήριο. Σ' αυτό λοιπόν το σημείο θα μας βοηθήσει το ακόλουθο γράφημα.

Γράφημα 1: screen plot



Το γράφημα αυτό μας δείχνει στον κατακόρυφο άξονα τις ιδιοτιμές προς τον παράγοντα με τον οποίο συνδέεται στον οριζόντιο άξονα. Με άλλα λόγια, το γράφημα 1 δείχνει καθαρά την σχετική σπουδαιότητα κάθε παράγοντα. Το σημείο στο οποίο αρχίζει η καμπύλη του γραφήματος να φθίνει απότομα αποτελεί κριτήριο για την επιλογή των σημαντικών παραγόντων.

Το σημείο αυτό στο δικό μας γράφημα είναι το σημείο που αντιστοιχεί στο componet 5. Δηλαδή, οι σημαντικότεροι παράγοντες είναι οι πρώτοι 5 παράγοντες. Άρα οι πιο σημαντικοί παράγοντες όπως προκύπτει από το παραπάνω γράφημα είναι (εκτός της ηλικίας και του επιπέδου σπουδών) η άποψη ή μη για το αν τα ΜΚΔ θεωρούνται έμπιστα, η αποδοχή ή όχι αιτήματος φιλίας από

αγνώστους και το κατά πόσο οι χρήστες εμπιστεύονται τα post των φίλων τους που σχετίζονται με ειδήσεις.Και επειδή οι παράγοντες ερμηνεύονται δύσκολα και κάποιες μεταβλητές έχουν πολλούς παράγοντες, το SPSS βγάζει τον πιο κάτω πίνακα για τους 5 πιο σημαντικούς παράγοντες.

Στον Πίνακας 34 βλέπουμε ποιους από τους 5 σημαντικούς παράγοντες έχει κάθε μεταβλητή

Πίνακας 34

Component Matrix[a]					
	Component				
	1	2	3	4	5
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	,766				
ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	-,652				
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	,637				
POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ	,468		,407		
ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ		-,626			,481
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	,517	-,526			
ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	-,459	,517		-,405	
ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ			,797		
ΕΜΠΙΣΤΑ_ΜΚΔ		,490		,636	
ΗΛΙΚΙΑ					,633
ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ					,468
Extraction Method: Principal Component Analysis.					
a. 5 components extracted.					

Και ακολούθως, το SPSS κάνει περιστροφή παραγόντων που είναι τεχνική μετασχηματισμού του πίνακα 34 για την ευκολότερη ερμηνεία των παραγόντων. Υπάρχουν 2 τύποι περιστροφής, η ορθογώνια και η πλάγια περιστροφή και επιλέγουμε τον κατάλληλο τύπου στηριζόμενοι στις γνώσεις μας για τους παράγοντες και στο πρόβλημα.

Εμείς από την αρχή διαλέξαμε την ορθογώνια περιστροφή και πιο συγκεκριμένα την Varimax, η οποία προσπαθεί να φορτώσει λιγότερες μεταβλητές στον κάθε παράγοντα. Ο μετασχηματισμένος πίνακας είναι ο πιο κάτω:

Πίνακας 35

Rotated Component Matrix[a]

	Component				
	1	2	3	4	5
ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	-,731				
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	,714				
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	,709				
ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ		-,771			
ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ		,650			
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	,427	,612			
ΕΜΠΙΣΤΑ_ΜΚΔ			,851		
POST_ΦΙΛΩΝ_ΓΙΑ_ΕΙΔΗΣΕΙΣ			,531		
ΗΛΙΚΙΑ				,781	
ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ				,688	
ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ					,882

Από τον πίνακα 33 που παρουσιάζεται λίγο πιο πάνω μπορούμε να δούμε ότι οι 5 παράγοντες συνολικά εξηγούν το 66,055% της συνολικής διασποράς, ποσοστό που είναι σχετικά καλό. Μετά την περιστροφή, τα ποσοστά για τον κάθε παράγοντα αλλάζουν όμως το άθροισμα των ποσοστών παραμένει το ίδιο.

Και τελικά το SPSS μας βγάζει ακόμα ένα πίνακα και ένα τρισδιάστατο γράφημα πάνω στα οποία φαίνονται οι παράγοντες και η μεταξύ τους σχέση.

Πίνακας 36

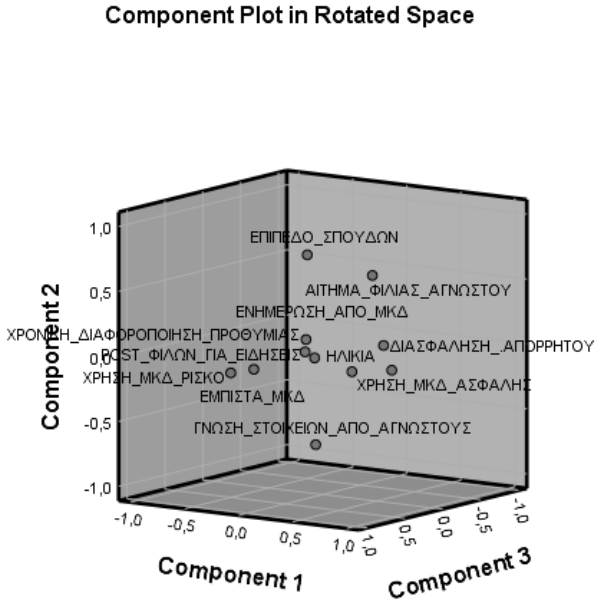
Component Transformation Matrix

Component	1	2	3	4	5
1	,848	,334	,318	,260	,035
2	-,006	-,766	,539	,325	,133
3	-,062	,149	,210	-,364	,893
4	-,411	,434	,737	-,079	-,306
5	-,330	,302	-,148	,829	,300

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

<u>Γράφημα 2:</u> το τρισδιάστατο αυτό γράφημα μας δείχνει τους 3 από τους 5 σημαντικούς μας παράγοντες και τη μεταξύ τους σχέση (φυσικά δε μπορούμε να φτιάξουμε γράφημα με 5 διαστάσεις ώστε να δείχνει όλους τους παράγοντες μας)



12.3 Έλεγχος υποθέσεων

Στη συνέχεια θα πραγματοποιήσουμε έλεγχο υποθέσεων στα ερευνητικά ερωτήματα τα οποία έχουμε διατυπώσει στην ενότητα 11.2 Προτάσεις - Υποθέσεις - Μεταβλητές. Τα υποθετικά ερωτήματα από το H1 - H5b αφορούν correlation tests ενώ από H6 - H8 αφορούν t- tests. Θα ξεκινήσουμε πρώτα με τα t-tests οπότε έχουμε:

Το πρώτο T-test αφορά την αποδοχή ή όχι αιτήματος φιλίας από αγνώστους(H6). Αυτό έχει διαφορετική απήχηση σε άνδρες και γυναίκες και τα διαγράμματα που ακολουθούν το πιστοποιούν.

Πίνακας 37

Group Statistics					
	ΦΥΛΟ	N	Mean	Std. Deviation	Std. Error Mean
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	ΑΝΔΡΕΣ	34	4.12	1.008	.173
	ΓΥΝΑΙΚΕΣ	28	4.82	.390	.074

Αρχικά διαπιστώνουμε ότι οι μέσες τιμές του αιτήματος φιλίας από αγνώστους για άνδρες (4,12% ±0,17) είναι μικρότερο από των γυναικών (4,82% ± 0,07).

Από τον πίνακα μπορούμε να δούμε ότι στο Levene's Test for Equality of valiances, το sig ισούται με 0,00. Η τιμή αυτή είναι μικρότερη από 0,05 και άρα οι διασπορές των δύο πληθυσμών έχουν διαφορά και θεωρούνται άνισες. Στο t-test Equal variances not assumed ελέγχουμε τις μέσες τιμές υποθέτοντας άνισες διασπορές. Και οι δύο αυτές τιμές είναι μικρότερη από 0,05 95% CI για τη διαφορά μ1 - μ2 = (1,082, -0,325). Επομένως το υποθετικό ερώτημα Η6 επαληθεύεται.

T- tests

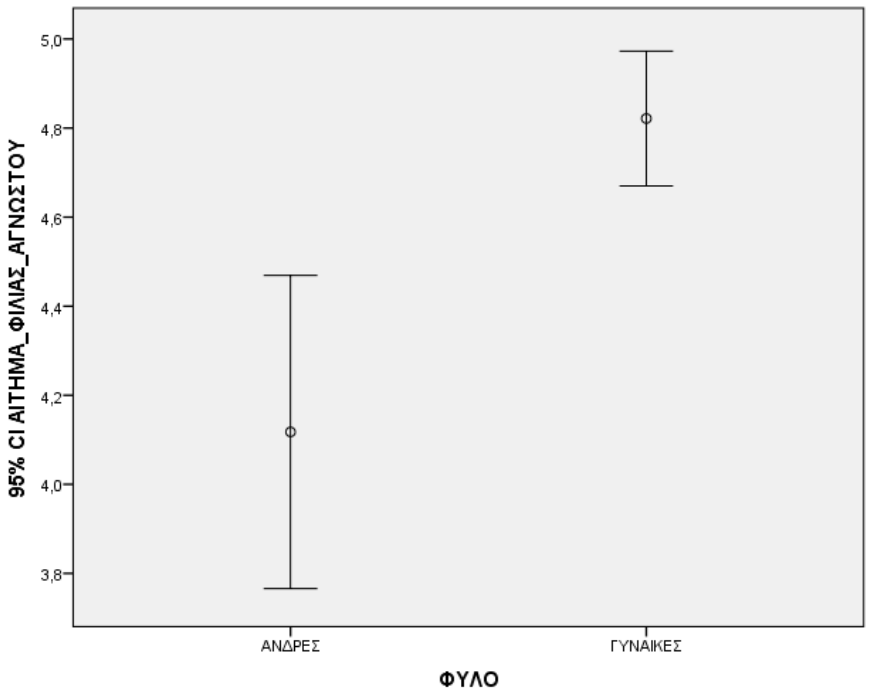
1.

Πίνακας 38

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ΑΙΤΗΜΑ_ΦΙΛΙΑΣ_ΑΓΝΩΣΤΟΥ	Equal variances assumed	22.562	.000	-3.482	60	.001	-.704	.202	-1.108	-.299
	Equal variances not assumed			-3.745	44.300	.001	-.704	.188	-1.082	-.325

Το παρακάτω γράφημα μας δείχνει ότι τα σημεία δεν καλύπτονται μεταξύ τους.



Το δεύτερο T-test αφορά τη διασφάλιση απορρήτου για δευτεροβάθμια και τριτοβάθμια εκπαίδευση. Στην ενότητα 11.2 αποτελεί το υποθετικό ερώτημα Η7.

Πίνακας 39

.

Group Statistics					
	ΕΠΙΠΕΔΟ_ΣΠΟΥΔΩΝ	N	Mean	Std. Deviation	Std. Error Mean
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	ΔΕΥΤΕΡΟΒΑΘΜΙΑ ΕΚΠΑΙΔΕΥΣΗ	37	3.68	.944	.155
	ΤΡΙΤΟΒΑΘΜΙΑ ΕΚΠΑΙΔΕΥΣΗ	25	3.92	.759	.152

Πίνακας40

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	Equal variances assumed	4.515	.038	-1.078	60	.285	-.244	.227	-.698	.209
	Equal variances not assumed			-1.125	58.083	.265	-.244	.217	-.679	.190

Αρχικά διαπιστώνουμε ότι οι μέσες τιμές της διασφάλισης απορρήτου για τελειόφοιτους δευτεροβάθμιας εκπαίδευσης (3,68% ±0,94) είναι μικρότερο από αυτή των τελειόφοιτων τριτοβάθμιας εκπαίδευσης (3,92% ± 0,76).

Από τον πίνακα μπορούμε να δούμε ότι στο Levene's Test for Equality of valiances, το sig ισούται με 0,038. Η τιμή αυτή είναι μικρότερη από 0,05 και άρα οι διασπορές των δύο πληθυσμών έχουν διαφορά και θεωρούνται άνισες. Στο t- Equal variances not assumed ελέγχουμε τις μέσες τιμές υποθέτοντας άνισες διασπορές για τη διαφορά μ1 - μ2 = (-0,68, 0,19). Άρα ισχύει η υπόθεση ότι η διασφάλιση απορρήτου των προσωπικών δεδομένων είναι διαφορετική για χρήστες δευτεροβάθμιας από τριτοβάθμιας εκπαίδευσης.

3.Το τρίτο t-test αφορά την υπόθεση της χρήσης των ΜΚΔ ασφαλή για άνδρες και γυναίκες. Το υποθετικό αυτό ερώτημα είναι το Η8 σύμφωνα με την ενότητα 11.2

Πίνακας 41

Group Statistics

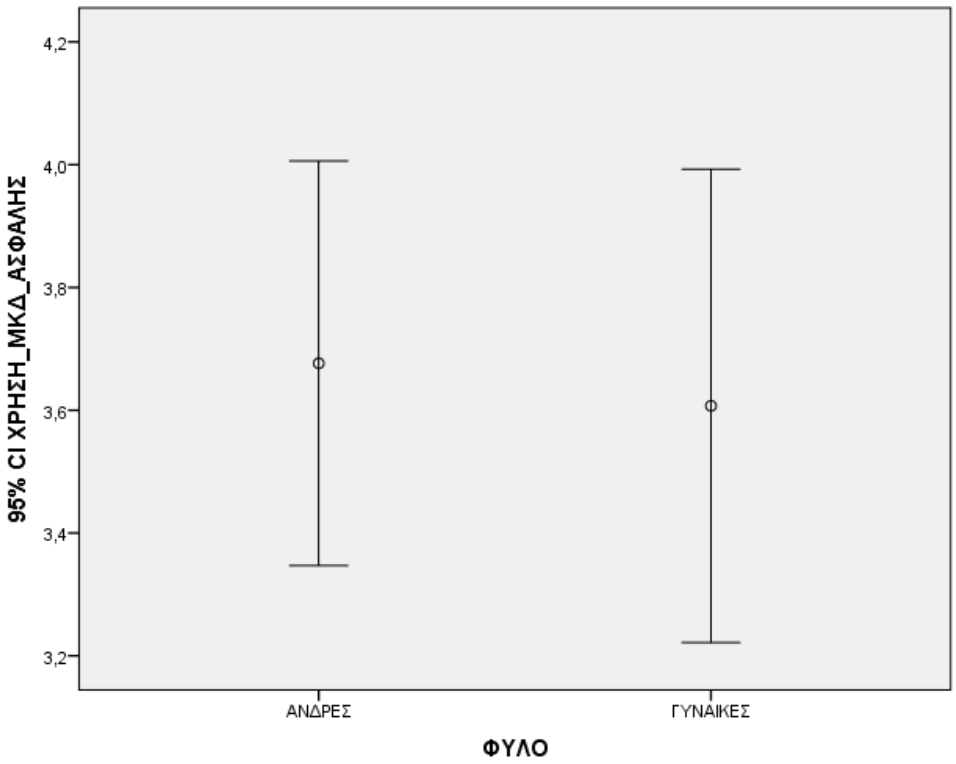
	ΦΥΛΟ	N	Mean	Std. Deviation	Std. Error Mean
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	ΑΝΔΡΕΣ	34	3.68	.945	.162
	ΓΥΝΑΙΚΕΣ	28	3.61	.994	.188

Πίνακας 42

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	Equal variances assumed	.728	.397	.281	60	.780	.069	.247	-.424	.563
	Equal variances not assumed			.279	56.515	.781	.069	.248	-.427	.566

Οι μέσες τιμές εμφανίζουν πολύ μικρή απόκλιση (3,68 για άνδρες και 3,61 για γυναίκες).

Από τον πίνακα μπορούμε να δούμε ότι στο Levene's Test for Equality of valiances, το sig ισούται με 0,397>0,05 και άρα οι διασπορές των δύο πληθυσμών έχουν δεν έχουν διαφορά και θεωρούνται ίσες. Στο t-test Equal variances assumed ελέγχουμε τις μέσες τιμές υποθέτοντας ίσες διασπορές οπότε το αποτέλεσμα είναι να δεχτούμε την μηδενική υπόθεση ότι δηλαδή η άποψη για το εάν είναι ασφαλή τα ΜΚΔ είναι ίδια για άνδρες και γυναίκες.



Το παραπάνω γράφημα μας δείχνει ότι τα σημεία καλύπτονται απόλυτα αν λάβουμε υπόψη μας και το σφάλμα τους.

12.4 Correlation Tests

Ανατρέχοντας πίσω στις αρχικές υποθέσεις μας στην ενότητα 11.2 είχαμε διατυπώσει την υπόθεση για το εάν η αντιλαμβανόμενη Εμπιστοσύνη σχετίζεται με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ (Η3α). Κάνοντας το παρακάτω Correlation test (Πίνακας 43) διαπιστώνουμε ότι δεν υπάρχουν σημαντικές συσχετίσεις που να ενισχύουν αυτή την υπόθεση. Επομένως θα θεωρήσουμε ως σωστή τη μηδενική υπόθεση ότι δηλαδή η εμπιστοσύνη δεν σχετίζεται με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.

Πίνακας 43

Correlations

			ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	ΕΜΠΙΣΤΑ_ΜΚΔ
Kendall's tau_b	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	Correlation Coefficient	1,000	-,130	,191
		Sig. (2-tailed)	.	,233	,086
		N	62	62	62
	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	Correlation Coefficient	-,130	1,000	-,173
		Sig. (2-tailed)	,233	.	,112
		N	62	62	62
	ΕΜΠΙΣΤΑ_ΜΚΔ	Correlation Coefficient	,191	-,173	1,000
		Sig. (2-tailed)	,086	,112	.
		N	62	62	62

2. Η δεύτερη υπόθεση αφορά το εάν η αντιλαμβανόμενη ασφάλεια σχετίζεται με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ(Η1α). Όπως προκύπτει από το παρακάτω correlation test (Πίνακας 44) και σε αυτή την περίπτωση δεν παρατηρούνται

σημαντικές συσχετίσεις και γι' αυτό θα θεωρήσουμε και πάλι σωστή την μηδενική υπόθεση ότι δηλαδή η ασφάλεια δεν σχετίζεται με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ.

Πίνακας 44

relations						
			ΕΝΗΜΕΡΟΜΕΝΟΙ	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ
Kendall's tau_b	ΕΝΗΜΕΡΟΜΕΝΟΙ	Correlation Coefficient	1,000	,190	-,096	,206
		Sig. (2-tailed)	.	,085	,376	,060
		N	62	62	62	62
	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	Correlation Coefficient	,190	1,000	-,130	,142
		Sig. (2-tailed)	,085	.	,233	,197
		N	62	62	62	62
	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	Correlation Coefficient	-,096	-,130	1,000	-,176
		Sig. (2-tailed)	,376	,233	.	,104
		N	62	62	62	62
	ΧΡΗΣΗ_ΜΚΔ_ΑΣΦΑΛΗΣ	Correlation Coefficient	,206	,142	-,176	1,000
		Sig. (2-tailed)	,060	,197	,104	.
		N	62	62	62	62

Πίνακας 45

Correlations						
			ΕΝΗΜΕΡΟΜΕΝΟΙ	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ
Kendall's tau_b	ΕΝΗΜΕΡΟΜΕΝΟΙ	Correlation Coefficient	1,000	,190	-,096	,113
		Sig. (2-tailed)	.	,085	,376	,306
		N	62	62	62	62
	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	Correlation Coefficient	,190	1,000	-,130	,255*
		Sig. (2-tailed)	,085	.	,233	,021
		N	62	62	62	62
	ΓΝΩΣΗ_ΣΤΟΙΧΕΙΩΝ_ΑΠΟ_ΑΓΝΩΣΤΟΥΣ	Correlation Coefficient	-,096	-,130	1,000	-,227*
		Sig. (2-tailed)	,376	,233	.	,037
		N	62	62	62	62
	ΔΙΑΣΦΑΛΗΣΗ_.ΑΠΟΡΡΗΤΟΥ	Correlation Coefficient	,113	,255*	-,227*	1,000
		Sig. (2-tailed)	,306	,021	,037	.
		N	62	62	62	62

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

3. Η τρίτη υπόθεση αναφέρεται στο εάν η αντιλαμβανόμενη Ιδιωτικότητα σχετίζεται με την ανταλλαγή προσωπικών ή μη δεδομένων στα ΜΚΔ(Η2α). Από το παραπάνω

Correlation test (Πίνακας 45)διαπιστώνεται ότι υπάρχουν συσχετίσεις σχετικά με αυτή την υπόθεση. Συγκεκριμένα η διασφάλιση απορρήτου σχετίζεται θετικά με την ενημέρωση που παρέχουν τα ίδια τα μέσα κοινωνικής δικτύωσης στους χρήστες τους ενώ υπάρχει αρνητική συσχέτιση της διασφάλισης απορρήτου ως προς τη διάθεση των προσωπικών δεδομένων των χρηστών σε άγνωστους (μη φίλους) μέσα από τα ΜΚΔ.

4. Η τέταρτη υπόθεση αφορά τη σχέση εμπιστοσύνης σε σχέση με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ(Η3β). Όπως διαπιστώνεται από το παρακάτω test (Πίνακας 46) δεν παρατηρούνται στατιστικές συσχετίσεις με αποτέλεσμα να δεχτούμε τη μηδενική υπόθεση ότι δηλαδή η εμπιστοσύνης δεν σχετίζεται με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.

Πίνακας 46

Correlations				
			ΕΜΠΙΣΤΑ_ΜΚΔ	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ
Kendall's tau_b	ΕΜΠΙΣΤΑ_ΜΚΔ	Correlation Coefficient	1,000	,191
		Sig. (2-tailed)	.	,086
		N	62	62
	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	Correlation Coefficient	,191	1,000
		Sig. (2-tailed)	,086	.
		N	62	62

Πίνακας 47

Correlations					
			ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ	ΣΚΕΠΤΙΚΟ_ΑΠΟΚΑΛΥΨΗΣ	ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ
Kendall's tau_b	ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ	Correlation Coefficient	1,000	-,126*	,002
		Sig. (2-tailed)	.	,245	,984
		N	62	62	62
	ΣΚΕΠΤΙΚΟ_ΑΠΟΚΑΛΥΨΗΣ	Correlation Coefficient	-,126*	1,000	,047
		Sig. (2-tailed)	,245	.	,663
		N	62	62	62
	ΧΡΗΣΗ_ΜΚΔ_ΡΙΣΚΟ	Correlation Coefficient	,002	,047	1,000
		Sig. (2-tailed)	,984	,663	.
		N	62	62	62
*. Correlation is significant at the 0.05 level (2-tailed).					

5. Η πέμπτη υπόθεση αφορά τη σχέση ασφάλειας σε σχέση με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ(Η1β). Το παραπάνω test (Πίνακας 47) έδειξε μια αρνητική συσχέτιση ανάμεσα στο σκεπτικό αποκάλυψης των προσωπικών δεδομένων και στην αίσθηση που έχουν οι χρήστες όταν μοιράζονται αυτά.

6. Η έκτη υπόθεση έχει να κάνει με την Ιδιωτικότητα σε σχέση με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ(Η2β). Και σε αυτή την υπόθεση (Πίνακας 48) δεν υπήρξαν σημαντικές συσχετίσεις επομένως θα κρατήσουμε τη μηδενική υπόθεση ότι δηλαδή η Ιδιωτικότητα δεν σχετίζεται με

την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ.

Πίνακας 48

Correlations				
			ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ
Kendall's tau_b	ΕΝΗΜΕΡΩΣΗ_ΑΠΟ_ΜΚΔ	Correlation Coefficient	1,000	,017
		Sig. (2-tailed)	.	,875
		N	62	62
	ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ	Correlation Coefficient	,017	1,000
		Sig. (2-tailed)	,875	.
		N	62	62

7. Η έβδομη υπόθεση έχει να κάνει με την ενημέρωση των χρηστών σε σχέση με την ανησυχία γύρω από την γνώση – ενημέρωση των χρηστών γύρω από τους κινδύνους που διέπει η χρήση των ΜΚΔ(Η4). Σε αυτή την υπόθεση (Πίνακας 49) υπάρχει μια θετική συσχέτιση οπότε μπορούμε να θεωρήσουμε τα δεδομένα που ανταλλάσσονται στα ΜΚΔ είναι το αποτέλεσμα της γνώσης – ενημέρωσης των χρηστών γύρω από αυτά.

Πίνακας 49

Correlations				
			ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ	ΣΚΕΠΤΙΚΟ_ΑΠΟΚΑΛΥΨΗΣ
Kendall's tau_b	ΑΒΟΛΑ_ΠΡΟΣΩΠΙΚΑ	Correlation Coefficient	1,000	,017*
		Sig. (2-tailed)	.	,875
		N	62	62
	ΣΚΕΠΤΙΚΟ_ΑΠΟΚΑΛΥΨΗΣ	Correlation Coefficient	,017*	1,000
		Sig. (2-tailed)	,875	.
		N	62	62
*. Correlation is significant at the 0.05 level (2-tailed).				

Η επόμενη υπόθεση έχει να κάνει με την αντίληψη περί ιδιωτικότητας σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ και είναι ισχυρότερη στις μικρότερες ηλικίες(Η5α). Όπως προκύπτει από τον παραπάνω πίνακα δεν παρατηρούνται στατιστικές συσχετίσεις με αποτέλεσμα να δεχτούμε τη μηδενική υπόθεση ότι η ιδιωτικότητα σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ δεν εξαρτάται από την ηλικία.

Πίνακας 50

Correlations				
			ΓΝΩΣΗ_ΠΟΛΙΤΙΚΗΣ_ΑΠΟΡΡΗΤΟΥ	ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ
Kendall's tau_b	ΓΝΩΣΗ_ΠΟΛΙΤΙΚΗΣ_ΑΠΟΡΡΗΤΟΥ	Correlation Coefficient	1,000	-,089
		Sig. (2-tailed)	.	,444
		N	62	62
	ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	Correlation Coefficient	-,089	1,000
		Sig. (2-tailed)	,444	.
		N	62	62

Η τελευταία υπόθεση αφορά στην αντίληψη περί εμπιστοσύνης σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ διαφοροποιείται ανάλογα με την ηλικία (Η5β). Όπως προκύπτει από τον παρακάτω πίνακα δεν παρατηρούνται στατιστικές συσχετίσεις με αποτέλεσμα να δεχτούμε τη μηδενική υπόθεση ότι η αντίληψη περί εμπιστοσύνης σε σχέση με τα δεδομένα που ανταλλάσσονται στα ΜΚΔ δεν διαφοροποιείται ανάλογα με την ηλικία.

Πίνακας 51

Correlations				
			ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	ΕΜΠΙΣΤΑ_ΜΚΔ
Kendall's tau_b	ΧΡΟΝΙΚΗ_ΔΙΑΦΟΡΟΠΟΙΗΣΗ_ΠΡΟΘΥΜΙΑΣ	Correlation Coefficient	1,000	,062
		Sig. (2-tailed)	.	,566
		N	62	62
	ΕΜΠΙΣΤΑ_ΜΚΔ	Correlation Coefficient	,062	1,000
		Sig. (2-tailed)	,566	.
		N	62	62

Επίλογος

Η εξάπλωση του διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης επιβεβαιώνεται από πλήθος στατιστικών στοιχείων. Αξιοσημείωτο είναι το γεγονός της διάχυτης ανησυχίας που επικρατεί για την ιδιωτικότητα των χρηστών παρά την αυξημένη συμμετοχή τους, μια διαπίστωση που μοιάζει εκ πρώτης όψης αντιφατική. Εντούτοις, καταδεικνύει την ανάγκη εκπαίδευσης των χρηστών σε συνεχή βάση, έτσι ώστε να διαμορφωθεί τελικά μια συγκεκριμένη συμπεριφορά – κουλτούρα ως προς τη συμμετοχή στα Μέσα Κοινωνικής Δικτύωσης. Με παράλληλη απόδοση σεβασμού στην ιδιωτικότητα των χρηστών.

Ιδιωτικότητα και προσωπικά δεδομένα είναι έννοιες άρρηκτα συνδεδεμένες και η σύνδεση τους αυτή προκύπτει από την αυξανόμενη ζήτηση προσωπικών πληροφοριών στην καθημερινότητα.

Η Ευρωπαϊκή Ένωση από τη μεριά της διαμόρφωσε ένα σαφές και αυστηρό πλαίσιο γύρω από τα ζητήματα που άπτονται της ιδιωτικότητας και της διαφύλαξης των προσωπικών δεδομένων των χρηστών μέσω του νέου κανονισμού GDPR. Για πρώτη φορά τα προσωπικά δεδομένα αποκτούν τόσο μεγάλη σημασία, ενώ κάποια από αυτά χρήζουν ακόμα μεγαλύτερης προστασίας, γιατί εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας όπως ευαίσθητα δεδομένα(τα δεδομένα που αφορούν σε –φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, υγεία, κοινωνική πρόνοια, ερωτική ζωή, ποινικές διώξεις ή καταδίκες, στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις. Τα ευαίσθητα αυτά δεδομένα αποκαλούνται πλέον «προσωπικά δεδομένα ειδικών κατηγοριών. Επίσης για πρώτη φορά το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση. Όμως επειδή δεν μπορεί να παραβλεφθεί ο δυναμικός χαρακτήρας της διαδικασίας ανάπτυξης και εφαρμογής της τεχνολογίας και κατ΄ επέκταση των ΜΚΔ, απαιτείται μια συνεχή διαδικασία δυναμικής προσαρμογής στα νέα δεδομένα που επιβάλλει η τεχνολογία

Βασικό πρόβλημα της λειτουργίας των ΜΚΔ αποτελεί η έλλειψη προτυποποίησης των μηχανισμών προστασίας της ιδιωτικότητας, με την ανάγκη ύπαρξης προτύπων ή τουλάχιστον κοινής γραμμής αντιμετώπισης να αποτελεί βασικό ζητούμενο. Εντούτοις η δημιουργία, καθιέρωση και θέσπιση ενός παγκόσμιας εμβέλειας ρυθμιστικού εργαλείου δυσχεραίνει κατά πολύ αφενός για τεχνολογικούς λόγους (π.χ. συμβατότητας) και αφετέρου εξαιτίας των κανόνων λειτουργίας της ίδιας της αγοράς.

Όσον αφορά την ασφάλεια που παρέχουν τα ΜΚΔ όπως διατυπώθηκε στην ανάλυση οι μηχανισμοί ασφάλειας των μέσων είναι ελλείπεις με αποτέλεσμα οι χρήστες να είναι εκτεθειμένοι σε κίνδυνο υποκλοπής των δεδομένων τους. Οι hackers έχουν βρει ένα νέο πεδίο δράσης το οποίο δεν είναι άλλο από τα ΜΚΔ. Περιπτώσεις υποκλοπής προσωπικών δεδομένων με οικονομικό όφελος (π.χ. εκβιασμοί) είναι πολύ συχνοί τα τελευταία χρόνια. Οι χρήστες από τη μεριά τους, αν και νοιώθουν ότι παίρνουν ρίσκο διατηρώντας λογαριασμούς στα ΜΚΔ, και ενώ δηλώνουν ότι είναι ενήμεροι των κινδύνων που διέπουν τα μέσα, στην πλειοψηφία τους δεν λαμβάνουν κανένα μέτρο για την προστασία τους. Οι κωδικοί που χρησιμοποιούν για να αυθεντικοποιήσουν την είσοδο τους σε κάποιο ΜΚΔ δεν είναι ισχυροί στην πλειοψηφία τους και δεν αλλάζουν σχεδόν ποτέ καθώς επιλέγουν την απομνημόνευση αντί της χειροκίνητης πληκτρολόγησης. Το πρόβλημα βέβαια είναι ακόμα πιο πολύπλοκο, καθώς δεν παίζει ρόλο μόνο εμείς πόσο διασφαλίζουμε τους λογαριασμούς μας, αλλά και οι φίλοι μας πρέπει να κάνουν το ίδιο όταν μοιραζόμαστε κοινά προσωπικά δεδομένα.

Από την άλλη, η πολιτική απορρήτου, αν και σε κάποιους είναι οικεία ως έννοια, δεν κάνουν αλλαγές ώστε να προστατευτούν, παραμένοντας στις αρχικές ρυθμίσεις οι οποίες λειτουργούν προς όφελος των κοινωνικών δικτύων αφήνοντας πολλή προσωπική πληροφορία εκτεθειμένη. Το οξύμωρο βέβαια, είναι ότι ενοχλούνται όταν κάποιος άγνωστος έχει πρόσβαση στα προσωπικά τους δεδομένα τα οποία οι ίδιοι δεν προστατεύουν. Βέβαια όπως έχουμε αναφέρει, αν και η πολιτική απορρήτου ειδικά στην περίπτωση του Facebook, έχει αλλάξει ριζικά προς το καλύτερο και έχει απλοποιηθεί σε μεγάλο βαθμό, εντούτοις για τους χρήστες δεν είναι ακόμα και τόσο εύκολο να κάνουν αλλαγές. Βέβαια όπως έχουμε αναφέρει ένα σημαντικό στοιχείο που θα πρέπει να έχουν οι χρήστες κατά νου είναι οι φίλοι φίλων οι οποίοι μπορούν να αποκτήσουν πρόσβαση στα προσωπικά μας δεδομένα χωρίς να τους έχουμε δώσει αυτή την άδεια.

Σχετικά με την εμπιστοσύνη στα ΜΚΔ οι απόψεις των χρηστών είναι διφορούμενες. Βέβαια τα παραδείγματα που έχουν παρατεθεί κάθε άλλο ενισχύουν την άποψη της εμπιστοσύνης. Και αυτό και πάλι έρχεται σε αντιπαράθεση με την καθολική άποψη των χρηστών ότι τα ίδια τα μέσα δεν ενημερώνουν τους χρήστες για το αν και που διαθέτουν τα προσωπικά τους δεδομένα. Υπάρχει ολόκληρη αγορά όπου τα ΜΚΔ εμπορεύονται ευαίσθητα προσωπικά δεδομένα. Όπως αναφέραμε και στον πρόλογο δεν είναι τυχαίο το γεγονός ότι αν δείξουμε ενδιαφέρον για μια κατηγορία προϊόντων ή μια δραστηριότητα στη συνέχεια βομβαρδιζόμαστε από διαφημιστικά μηνύματα. Κάποιος έχει δώσει πληροφορίες για να λαμβάνουμε αυτά τα μηνύματα. Κάποιος που έχει πρόσβαση στο λογαριασμό μας και το κάνει εντελώς κυνικά χωρίς να δίνει λογαριασμό σε εμάς τους χρήστες για τις πράξεις αυτές.

Ένα άλλο πεδίο στο οποίο δείξαμε ιδιαίτερη σπουδή ήταν αυτό της ενημέρωσης το οποίο σχετίζεται άμεσα με την εμπιστοσύνη. Όπως αποδείχτηκε (και από τις απαντήσεις στο ερωτηματολόγιο) οι χρήστες σχεδόν καθημερινά και αποκλειστικά επιλέγουν να ενημερώνονται για πολιτικά και όχι μόνο θέματα από τα ΜΚΔ. Τα παραδοσιακά μέσα ενημέρωσης που είναι κατά κύριο λόγο οι εφημερίδες έχουν υποστεί ένα τεράστιο πλήγμα από τα ΜΚΔ καθώς όλο και περισσότεροι χρήστες επιλέγουν να ενημερώνονται πλέον από αυτά. Είναι όμως η ενημέρωση τους αντικειμενική; Αυτό εμπεριέχει ένα σοβαρό κίνδυνο καθώς η ιεράρχηση των ειδήσεων δεν σχετίζεται με τη σπουδαιότητα τους με αποτέλεσμα να "σερβίρεται" στους χρήστες αυτό που θέλουν να δουν περισσότερο.

Το πιο σημαντικό κομμάτι ίσως απ' όλα όσα έχουμε αναφέρει είναι η εμπλοκή των ΜΚΔ στην πολιτική και η προσπάθεια χειραγώγησης των πολιτών. Τα παραδείγματα που έχουν παρατεθεί είναι ενδεικτικά στο να κατανοήσουμε ότι στην εποχή μας ο τρόπος που διεξάγεται η πολιτική έχει αλλάξει ριζικά. Τα ΜΚΔ παίζουν καθοριστικό ρόλο στην ανάπτυξη πολιτικής και συχνά γίνεται το κύριο εργαλείο ανάπτυξης της. Τα μηνύματα που

ανταλλάσουν πολιτικοί, ακόμη και αρχηγοί κρατών, είναι στοιχεία άσκησης πολιτικής. Σήμερα είναι πολύ πιο απλό για κάποιο πολιτικό πρόσωπο να κοινοποιήσει ένα μήνυμα από το να κάνει μια δήλωση.

Βέβαια τα ΜΚΔ με την κατάλληλη χρήση τους από τους πολίτες μπορούν να λειτουργήσουν σαν μοχλός αλλαγής και αμφισβήτησης της εκάστοτε εξουσίας φέρνοντας ουσιαστικές αλλαγές. Παραδείγματα τέτοια όπως έχουμε αναφέρει υπάρχουν πολλά από τη Μέση Ανατολή μέχρι τις χώρες της Βόρειας Αφρικής όπου με την αρωγή των κοινωνικών μέσων και του διαδικτύου οι πολίτες κατάφεραν να ανατρέψουν καθεστώτα. Τα πολιτικά και κοινωνικά κινήματα, οι επαναστάσεις αλλά και οι λαϊκές εξεγέρσεις που εκδηλώθηκαν σε όλο το κόσμο έρχονται να επιβεβαιώσουν την πολιτική ισχύ που κατέχουν τα κοινωνικά μέσα και το διαδίκτυο γενικότερα, καθώς κατάφεραν να συμβάλουν τόσο στον επαναπροσδιορισμό της πολιτικής κουλτούρας όσο και της συγκρότησης διεθνών σχέσεων.

Από την άλλη τα ίδια τα μέσα και ο τρόπος που αυτά χρησιμοποιούνται από τους χρήστες έπαιξαν σημαντικό ρόλο στο παρελθόν σε εκλογικές αναμετρήσεις κυρίως των Ηνωμένων Πολιτειών με την ανάδειξη προέδρων οι οποίοι είτε κατάλαβαν από νωρίς τη δύναμη των μέσων (περίπτωση Ομπάμα) είτε λειτούργησαν παρασκηνιακά με όχι και τόσο θεμιτά μέσα στην προσπάθεια εκλογής τους (περίπτωση Τραμπ).

Ένα σημαντικό στοιχείο, που είναι και το αισιόδοξο μήνυμα της έρευνας αυτής είναι ότι με την πάροδο του χρόνου, κυρίως οι μεγαλύτεροι ηλικιακά χρήστες, διαφοροποιούν τις απόψεις γύρω από τα ΜΚΔ. Αυτό σημαίνει ότι οι χρήστες ενημερώνονται περισσότερο και προσπαθούν να προστατέψουν την ιδιωτικότητα τους και τα προσωπικά τους δεδομένα περισσότερο απ' ότι παλαιότερα. Οι χρήστες γίνονται πιο καχύποπτοι ως προς το ρόλο που παίζουν τα μέσα στις ζωές μας.

Καταλήγοντας αναφέρουμε πάλι τους 8 παράγοντες που προτείνει η IEEE ώστε να είμαστε όσο το δυνατό περισσότερο προστατευμένοι στους κίνδυνους που κρύβονται (ή και όχι) στα ΜΚΔ αυτοί είναι:1. Απομάκρυνση προσωπικών πληροφοριών που δεν είναι χρήσιμες 2. Σωστή ρύθμιση ασφάλειας και ιδιωτικότητας 3. Δεν δεχόμαστε αιτήματα φιλίας από αγνώστους 4. Εγκατάσταση λογισμικού ασφαλείας στον Η/Υ 5. Απομάκρυνση εφαρμογών με τρίτα μέρη (Third party) 6. Μη δημοσιοποίηση θέσης 7. Μην εμπιστεύεσαι τους «φίλους» από τα μέσα κοινωνικής δικτύωσης 8. Οι γονείς θα πρέπει να παρακολουθούν την δραστηριότητα των παιδιών τους.

Τα Μέσα Κοινωνικής Δικτύωσης είναι η επανάσταση των τελευταίων χρόνων. Με τη αέναη ενημέρωση και γνώση των χρηστών μπορούμε να επωφεληθούμε από τα πλεονεκτήματα που αυτά κατέχουν και να περιορίσουμε ή εξαλείψουμε τα μειονεκτήματα τους. **It's up to us!**

Παράρτημα

Ερωτηματολόγιο

Γενικές ερωτήσεις - Προφίλ χρηστών

Ε1) Φύλο: α) άνδρας β)γυναίκα

Ε2)Ηλικία : α)<18 β)18-24 γ)25-35 δ)35 -50 ε)>50

Ε3)Επίπεδο σπουδών : α) γυμνάσιο β) λύκειο γ) ΤΕΙ/ΑΕΙ δ)Μεταπτυχιακό

Ε4) Σε ποιο ΜΚΔ έχετε λογαριασμό; α) Facebook b)Instagram γ)Tweeter δ)Linkedin ε)Youtube

Ε5)Πόσο συχνά επισκέπτεστε τα ΜΚΔ α)Πολλές φορές την ημέρα β)2-3 φορές την ημέρα γ)1 φορά την ημέρα δ)1 φορά κάθε 2-3 ημέρες ε)1 φορά την εβδομάδα (Avner Levin, 2008)

Ε6) Πόσο χρόνο αφιερώνετε κάθε φορά που επισκέπτεστε κάποιο ΜΚΔ ; (Avner Levin, 2008)

α) 1-10 λεπτά β) 10-30 λεπτά γ)30 -45 λεπτά δ)45 - 90 λεπτά ε)>90 λεπτά

Ε7) Χρησιμοποιείται τα ΜΚΔ για: α) νέες γνωριμίες β) να βρείτε παλιούς φίλους γ) να ενημερώνεστε για τις δραστηριότητες των φίλων σας δ) να παίζετε παιχνίδια ε) προσφορά και ζήτηση εργασίας στ) ενημέρωση ζ) αγορές η) άλλο (Nair, March 2017)

Εμπιστοσύνη (Trust):

Ε8)Ποια από τα παρακάτω στοιχεία που έχετε δώσει στα ΜΚΔ είναι πραγματικά: α) όνομα β) φωτογραφία γ) διεύθυνση δ) τηλέφωνο ε) σημείο που βρίσκομαι (Avner Levin, 2008)

Ε9)Θεωρείτε τα ΜΚΔ έμπιστα στην ανταλλαγή πληροφοριών με φίλους ή μη; (Song, 2011)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε10)Θα κάνατε φίλο κάποιον που σας κάνει αίτημα φιλίας χωρίς να τον γνωρίζεται; (Avner Levin, 2008)

α)πάντα β)πολλές φορές γ) αρκετές δ) λίγες ε) καθόλου

Ε11)Εμπιστεύεστε τα post των φίλων σας στα ΜΚΔ όταν μοιράζονται ειδήσεις στα κοινωνικά δίκτυα; (Janice C. Sipior, 2013)

α)πάντα β)πολλές φορές γ) αρκετά δ)λίγο ε) καθόλου

Ε12) Σας ανησυχεί το γεγονός ότι τα ίδια τα ΜΚΔ μπορεί να χρησιμοποιούν προσωπικά σας στοιχεία προς όφελος τους ή προς τρίτους ; (Krasnova Hanna, 2010)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε13)Πόσο συχνά διαβάζεται ειδήσεις από τα ΜΚΔ; α) κάθε μέρα β) κάθε βδομάδα γ) λιγότερο από μια φορά τη βδομάδα δ) ποτέ (Avner Levin, 2008)

Ε14) Με την πάροδο του χρόνου διαφοροποιείται η προθυμία σας να ανταλλάσσεται προσωπικά ή μη δεδομένα στα ΜΚΔ; Το ίδιο ισχύει και με τους φίλους σας; (YOUN, 2009)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου 2) α)ναι β) όχι (α, β, γ, δ-->1)

Ασφάλεια (Security):

Ε15) Λαμβάνεται μέτρα προστασίας των προσωπικών σας λογαριασμών στα ΜΚΔ; Αν ναι ποιά από τα ακόλουθα εφαρμόζετε; α)αλλαγή username passwords β)απενεργοποίηση υπενθύμισης/ απομνημόνευσης κωδικών πρόσβασης γ)φραγή αναδυόμενων παραθύρων (Cookies) δ)χρήση αντιβιοτικών ε) λήψη αρχείων από άγνωστες πηγές (Song, 2011)

Ε16)Η χρήση των ΜΚΔ είναι ασφαλής; (Song, 2011)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε17)Γενικά, η επικοινωνία στα ΜΚΔ εμπεριέχει ρίσκο; (Song, 2011)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε18) Θεωρείτε ότι είστε ενημερωμένοι με τους κινδύνους που ελλοχεύουν στα ΜΚΔ; (Rütten)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ιδιωτικότητα (Privacy):

Ε19)Γνωρίζεται για την πολιτική απορρήτου των ΜΚΔ; Πόσο δύσκολο σας είναι να βρείτε και να χρησιμοποιήσετε τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης; (Avner Levin, 2008
α)πάντα β)πολλές φορές γ) αρκετές δ) λίγες ε) καθόλου
Ε20)Έχετε κάνει τροποποιήσεις στις βασικές ρυθμίσεις απορρήτου ή είναι οι βασικές; Πόσο συχνά κάνετε αλλαγές στις ρυθμίσεις απορρήτου; (Michel Netter, 2013)
α)πάντα β)πολλές φορές γ) αρκετές δ) λίγες ε) καθόλου
Ε21)Πιστεύεται ότι διασφαλίζεται το απόρρητο των προσωπικών σας δεδομένων; (Janice C. Sipior, 2013)
α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε22) Με την πάροδο του χρόνου έχει διαφοροποιηθεί η άποψη σας γύρω από τα προσωπικά δεδομένα και της προστασίας τους; (YOUN, 2009)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε23) Γνωρίζετε τις συνέπειες δημοσιοποίησης της θέσης στην οποία βρίσκεστε;

Γνώση ενημέρωσης των χρηστών (user awareness)

Ε24) Θεωρείται ότι τα ΜΚΔ ενημερώνουν επαρκώς τους χρήστες για τις πιθανές επιπτώσεις της διάθεσης των προσωπικών τους δεδομένων; (Krasnova Hanna, 2010)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε25) Σας ενοχλεί εάν κάποιος που δεν γνωρίζετε μπορεί να βρει τα προσωπικά σας στοιχεία στην σελίδα κοινωνικής δικτύωσης ; (Krasnova Hanna, 2010)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε26) Σας ενοχλεί αν κάποιος θα μπορούσε να διαπιστώσει τις προτιμήσεις σας σχετικά με τη μουσική, το διάβασμα, τις ταινίες , ακόμα και τις πολιτικές πεποιθήσεις από το προφίλ ή τα post που κάνετε στα ΜΚΔ; (Avner Levin, 2008)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Δεδομένα που ανταλλάσσονται (Information Sharing)

Ε27)Νιώθετε άβολα όταν μοιράζεστε προσωπικές πληροφορίες στα ΜΚΔ; (Dhami, 2015)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου

Ε28)Αποκαλύπτετε προσωπικές πληροφορίες με το σκεπτικό ότι το κάνουν όλοι αυτό; (Dhami, 2015)

α)πάρα πολύ β) πολύ γ) αρκετά δ)λίγο ε) καθόλου (Dhami, 2015)

Βιβλιογραφία ερωτηματολογίου

1.Avner Levin Mary Foster, Bettina West, Mary Jo Nicholson, Tony Hernandez, Wendy Cukier The Next Digital Divide:Online Social Network Privacy [Report]. - [s.l.] : Ryerson University Ted Rogers School of Management Privacy and Cyber Crime Institute, 2008.

2.Dhami Ashish Gupta and Anil Measuring the impact of security,trust and privacy in information sharing: A study on social networking sites [Report]. - [s.l.] : Spinger, 2015.

3.Janice C. Sipior Burke T. Ward,Regina Connolly,Labhras MacGabhann Privacy in Online Social Networking: Applying a Privacy Calculus Model [Conference] // Pacific Asia Conference on Information Systems. - [s.l.] : AIS Electronic Library, 2013.

4.Krasnova Hanna Kolesnikova Elena, Günther Oliver LEVERAGING TRUST AND PRIVACY CONCERNS IN ONLINE SOCIAL NETWORKS: AN EMPIRICAL STUDY [Conference] // 18th European Conference on Information Systems. - [s.l.] : Scholarone, 2010.

5.Michel Netter Moritz Riesner, Michael Weber, Günther Pernul Privacy Settings in Online Social Networks - Preferences, Perception, and Reality [Conference] // 46th Hawaii International Conference on System Sciences. - [s.l.] : IEEE, 2013.

6.Nair Mr. K Sanal Security and privacy issues: Does association has role to play? [Report]. - [s.l.] : Research Gate, March 2017.

7.Rütten Laura Facebook user perceptions of privacy and security on Facebook, between Millennials' and Non-Millennials' [Report]. - [s.l.] : University of Twente.

8.Song Ki Jung Lee and Il-Yeol Modeling and Analyzing User Behavior of Privacy Management on Online Social Network [Conference] // 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing. - Philadelphia, PA, USA : IEEE, 2011.

9.YOUN SEOUNMI Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents [Report]. - [s.l.] : Wiley online library, 2009.

Βιβλιογραφία

Ξένη Βιβλιογραφία

1**. Abdukader H., E. Elabd, W. Ead, 2016 ,** volume 82 pages 20 – 27**,** *Protecting Online Social Networks Profiles by Hiding Sensitive Data Attributes,* ELSEVIER.

2. **Aghaei Sareh, Nematbakhsh Ali, Hadi Khosravi Farsani,** 2012, Vol.3, No.1**,** *EVOLUTION OF THE WORLD WIDE WEB: FROM WEB 1.0 TO WEB 4.0 ,* International Journal of Web & Semantic Technology (IJWesT)

3 . Al-Qurishi Muhammad, Majed Alrubaian, Sk Md Mizanur Rahman, AtifAlamriac, 2018, Pages 743-753, *A prediction system of Sybil attack in social network using deep-regression model,* ELSEVIER

4.Amardeep Singh, **Divya Barsal, Sanjeev Sofat ,**2018, pages 46-63, *What about Privacy of My OSN Data,* Taylor Francis Online.

5. Andrerson J., F. Stajano,*2013, Volume: 11, Issue****:3,*** *Pages: 51 - 60* ***,*** *Must social networking conflict with privacy?****,*** *IEEE.*

6. Al Shayeji Mohammad H., Ghufran A. Al Shiridah, and M. D. Samrajesh, 2012, *Vol. 3, No. 6, A Secure Framework for Multimedia Protection in Social Media Networks, International Journal of Innovation, Management and Technology.*

7.*The Associated Press,2018 ,* *AP Exclusive: Google tracks your movements, like it or not,* https://apnews.com/828aefab64d4411bac257a07c1af0ecb [7/4/2019]

8.Atif Ahmad, **Rachelle Bosua, Rens Scheepers,**2014, volume 42 pages 27 – 39, Protecting organization competitive advantage: A knowledge leakage perspective. In *Compures & Security,* Elsevier.

9. Ayres, Jeffrey M., 1999, pages 132-143, *From the Streets to the Internet: The Cyber-Diffusion of Contention,* RESEARCH GATE.

10. Bahri L., B. Carminati, E. Ferrari, 2018, Volume 6 pages 18 -25**,** *Decentalized privacy preserving services for Online Social Networks,* ELSEVIER.

11. M. Bartsch, T. Dienlin, 2016, Volume 56 Pages 147-154, *Control your Facebook: An analysis of online privacy literacy,* Elsevier.

12.Beato Filipe, Filipe Beato , Kasper B. Rasmussen, 2014, *Undetectable communication: The Online Social Networks case,* IEEE.

13.**Berger Jonah, Milkman Katherine ,** 2012, Vol. 49, No. 2, pp. 192-205, *What Makes Online Content Viral?* , JMR.

14.**BILTON NICK,** 2010, *Price of Facebook Privacy? Start Clicking,* https://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html, [18/12/2018].

15.Bioglio L., R. Pensa, 2017, volume 108, pages 28 – 37, *Impact of Neighbors on the Privacy of Individuals in Online Social Networks,* ELSEVIER.

16. **Boshmaf Yazen, Muslukov Ildar, K. Beznosov, Matei Ripeanu,** 2013, Volume 57 Issue 2 pages 556 - 578, *Design and Analysis of a Social Botnet, ELSEVIER.*

17.Boshmaf Yazan, l. M., 2011, Pages 93-102, *The Socialbot Network: When Bots Socialize for Fame and Money,* ACM.

18. Bradshaw Tim, Arash Massoudi, Kara Scannel*l,23/04/2013, Bogus terror tweet sparks shares blip*, The Financial Times Limited, [26/01/2019].

19.Boyd Danah, Nicole Ellison, 2007, Volume13 Issue 1Pages 210-230, *Social Network Sites: Definition, History, and scholarship*, Wiley Online Library.

20.**CHaabane A., G. Acs, M. Kaafar,** 2012**,** *You Are What You Like!Information Leakage Through Users Interests, INRIA France*.

21.Chaffey Dave, 2018, Our compilation of the latest social media statistics of consumer adoption and usage, Smart Insghts.

22. **Conover Michael D.** , Bruno Goncalves, Jacob Ratkiewicz, Alessandro Flammini, Filippo Menczer**,** 2011, *Pages:192-199, Predicting the Political Alignment of Twitter Users, Third International Conference on Privacy, Security, Risk and Trust, IEEE*

23. ***COUNCIL OF EUROPE****,* 28/01/2019, https://www.coe.int/en/web/portal/28-january-data-protection-day,[30/01/2019]

24. Cutillo L ,Molva R,Strufe T., 2009, pages 94–101, *Safebook: A privacy-Preserving Online Social Network Leveraging on Real-lLfe Trust,* IEEE.

25. **DailyMail** , 2011 , *Bank worker fired for Facebook post comparing her 7-an-hour wage to Lloyds boss's 4000-an-hour salary*, http://dailym.ai/fjRTlC [27/09/2018]

26.Dam Wis,5/02/2009 *School teacher suspended for Facebook gun photo*, https://www.foxnews.com/story/schoolteacher-suspended-for-facebook-gun-photo[27/09/2018]

27.**De Salve A., P. Mori, L. Ricci,**2018, Volume 27 pages 154 – 176, *A survey on privacy in decentralized online social networks,* ELSEVIER.

28.Dwyer Catherine, 2011, Volume: 3, Issue 3 pages 58-63, *Privacy in the age of Google and Facebook,* IEEE

29.**Elishar Aviad, M. Fire, D. Kagan, Y. Elovici,** 2012, pages 7 – 12, International Conference on Social Informatics ,*Organizational Intrusion: Organization Mining Using Socialbots.* Lausanne, Switzerland : IEEE.

30.**Epstein Robert, Ronald E. Robertson,** 2015, pages 4512 – 4521,*The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections,* Research Gate.

31.**Epstein Robert,** 2015, How Google Could Rig the 2016, https://www.politico.com/ Election./magazine/story/2015/08/how-google-could-rig-the-2016-election-121548, [12/11/2018].

32.**Eytan Bakshy, Itamar Rosenn, Cameron Marlow, Lada Adamic,** 2012, Pages 519-528, *The Role of Social Networks in Information Diffusion,* ACM .

33.Felt A., D. Evans, 2008, Workshop on Web 2.0 Security and Privacy. Oakland, CA. 22 May 2008, *Privacy Protection for Social Networking Platforms,*University of Virginia .

34.**Fire Michael, Member, Roy Goldschmidt, and Yuval Elovici,** 2014, VOL. 16, NO. 4, *Online Social Networks: Threats and Solutions,* IEEE.

35.**Garside Juliette,** 2013, *Facebook loses millions of users as biggest markets peak*,, https://www.theguardian.com/technology/2013/apr/28/facebook-loses-users-biggest-markets, The Gardian, [25/102018]

36.Ghemri Lila*, 2015,* pages 187 – 199, *A User Centered Approach to Managing Privacy in Online Social Networks,* Proceedings of Informing Science & IT Education Conference (InSITE).

37.Gilad Lotan, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce, danah boyd, 2011, Volume 5 pages 1375-1405,*The arab spring — the revolutions were tweeted: Information flows during the 2011 tunisian and egyptian revolutions* **,** International Journal of Communication- University of Southern California.

38.**Ginosar A., Y. Ariel, 2017,** volume: 54 Issue :7, Pages 948-957, *An analytical framework for online privacy research:What is missing?,* ELSEVIER.

39.Golbeck Jennifer, Cristina Robles, Michon Edmondson, Karen Turner, 2011, pages 149 – 156, Third International Conference on Privacy, Security, Risk, and Trust *Predicting Personality from Twitter,* IEEE.

40.**Griffin, Andrew** *, 2018, FACEBOOK MUST FACE LAWSUIT OVER FACIAL RECOGNITION TECHNOLOGY, JUDGE RULES,*https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-facial-recognition-lawsuit-california-privacy-security-cambridge-analytica-a8308211.html, [17/04/2018].

41.Hao Wang Yi Liu, Tong Li,Ping Li,Jie Ling, 2018, Pages 873-880, *Attribute-based handshake protocol for mobile healthcare social networks,*ELSEVIER.

42.Heather Kelly, 30/08/2012,*Police embrace social media as crime-fighting tool*, CNN BUSINES, http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media [28/09/2018]

43. Hill, Kashmir, 2018, Facebook Was Fully Aware That Tracking Who People Call and Text Is Creepy But Did It Anyway,*https://gizmodo.com/facebook-was-fully-aware-that-tracking-who-people-call-1830884585* , [12/05/2018].

44.Jackson Brian, 2018, *Royal Bank of Canada named in New York Times' Facebook investigation,* www.itworldcanada.com,[19/12/2018].

45. James T., M. Warkentin, S. Collignon, 2015**,** Volume 52 Issue 8 pages 893-908**,** *A dual privacy decision model for online social metworks,* ELSEVIER.

46. **Jansen Bernard , Mimi Zhang, Kate Sobel, Abdur Chowdury,** 2009, Pages: 2169-2385, *Twitter power: Tweets as electronic word of mouth,* Wiley Online Library.

47. Johnson Bobbie, 2010, Privacy no longer a social norm, says Facebook founder, The Gardian, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy, [25/01/2019]

48. **Johnson M., S. Bellovin.** 2012**,** Soups' 12 Proceeding of the Eighth Symposium on Usable Privacy and Security, Article No. 9**,** *Facebook and privacy: it's complicated,* ACM.

49. **Jordaan Y., G. Van Heerden,** 2017, Volume 70 pages 90 – 96, *Online privacy-related predictors of Facebook usage intensity,* Elsevie

50. **Kader Hatem Abdul, Emad ElAbd, Waleed Ead,** 2016, Pages 20-27, *Protecting Online Social Networks Profiles by Hiding Sensitive Data Attributes,* ELSEVIER.

51.Kayes I., A. Iamnitchi. 2015, Cornell University, *A Survay on Privacy and Security in Online Social Networks,* ACM.

51.Kayes Imrul, A. L., 2017, volume 3-4 pages1-21, *Privacy and security in online social networks:A survay,* Elsevier

52.Kayes Imrul, Adriana Iamnitchi, 2015, *A Survay on Privacy and Security In Online Social Networks, Cornell University,* ACM.

53a. **Khan, Hamza,**2012, Social Networking Vs. Social Media – Understand The Difference. [Online], http://www.instantshift.com/2012/06/28/social-networking-vs-social-media-understand-the-difference,[28/06/2012] .

53b.**Khan Mehreen ,** 2018**,** *EU accuses Facebook and Twitter of delaying user protections***,** https://www.ft.com/content/c5ada116-1242-11e8-8cb6-b9ccc4c4dbbb15/02/2018, [18/2/2019]

54.Knibbs Kate, 28/5/2014, 1.8 billion images are uploaded every day: https://www.dailydot.com/debug/mary-meeker-photo-report , [15/10/2018]

55.**M. Kosinski, D. Stillwell, T. Graepel,** 2013, *Private traits and attributes are pr5dictable from digital records of human behavior,* PNAS.

56. **Kumar Mukesh A., B. Nupur Sharma, Shreesh Kumar Shrivastava,** 2014, pages 129 – 133, *Online Social Networks: Privacy Challenges and Proposed Security Framework for Facebook,* International Journal of Soft Computing and Engineering (IJSCE).

57. Kwak Haewoon, Changhyun Lee, Hosung Park, Sue Moon, 2010, Pages 591-600, *What is Twitter, a social network or a news media?,* ACM.

58. S. Labitzke, F. Werling, J. Mittag, H. Hartenstein,2013**,** Pages 13-24, *Do Online Social Metwork Friends Still Threaten My Privacy?,* ACM.

59. Lankton Nancy, D. Harrison McKnight, and Jason Bennett Thatcher, 2012, VOL. 59, NO. 4, *The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue Using a Social Networking Website,* IEEE.

60. Li N., G. Chen, 2010, pages 20 – 25, *Sharing location in online social networks,* IEEE.

61. Li Y., Y. Li, Q. Yan, R. Deng, 2014, Volume:49 pages:239 – 254, *Privacy leakage analysis in online social networks,* ELSEVIER.

62. Liu Z., X. Wang, 2018, volume: 55 Issue :8, Pages 1005-1023, *How to regulate individuals' privacy boundaries on social network sites? A cross-cultural comparison,* ELSEVIER.

63. Madejski Michelle, Maritza Johnson, Steven M. Bellovin, 2012, *A Study of Privacy Settings Errors in an Online Social Network, IEEE International Conference on Pervasive Computing and Communications Workshops* , IEEE.

64. Madejski Michelle, Johnson, Maritza Lupe and Bellovin, Steven Michael, 2011, *The Failure of Online Social Network Privacy Settings,* Columbia University Libraries.

65. **Ma Mengyan , Saleem Alhabash and Mengyan**, 2017,*A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students?* s.l. : SAGE RESEARCH

66. Mayfield, Antony, 2008, *What is social media?* s.l. : ICrossing updated .

67. **Messing Solomon, Sean J. Westwood,** 2012, *Selective Exposure in the Age of Social Media: Endorsements Trump Partisan Source Affiliation When Selecting News Online,* SAGE PUBLICATIONS.

68. Miller, Paul, October 30, 2005, Web 2.0: Building the New Library. [Online] ARIADNE Web Magazine for Information Professional. http://www.ariadne.ac.uk/issue/45/miller/, [26/01/2019].

69. Mishra Pawan_, 2012, pages *59-65, Social Networking Websites and Image Privacy ,* Research Gate.

70. Molok N., A. Ahmad, S. Chang, 2011**,** 22nd Australasian Conference on Information Systems , *Disclosure of Organizational Information by employees on Facebook:Looking at the Potential Risk for Information Security Risks,* AIS.

71. Nagle Frank, L. S. (2009). *Can friends be trusted,* 2009, Pages:212-218 *Exploring privacy in online social networks*,International Conference on Advances in Social Network Analysis and Mining IEEE.

72.Narayanan, Arvind Elaine Shi, Benjamin I., P.Rubinstein, 2011, pages 1825-1834 *Link prediction by de-anonymization: how we won the Kaggle social network challenge Proceedings* , IEEE .

73.Nettleton David, Salas J.,2016, Volume 5 pages 87-105, *A data driven anonymization system for information rich online social network graphics. In Expert Systems with Applications,* Elsevier.

74.Newman Nic,2011, *Mainstream media and the distribution of news in the age of social discovery*, Reuters Institute for the study of Journalism

75.Nissenbaum H.,2011, Volume 140 Issue 4 Fall 2011pages 32-48 *A contextual approach to privacy online***,** The MIT Press Journal

76.Nurul Nuha, Abdul Moloka, Atif Ahmadb, Shanton Chang, 2018, Volume 43 pages 351 – 356, A case analysis of securing organisations against information leakage through online social network. In *International Journal of Information Management, ELSEVIER*.

77. **Nuha Nurul, Abdul Molok,** 2011, *Disclosure of Organizational Information byEmployees on Facebook: Looking at the Potential for Information Security Risks, 22nd Australasian Conference on Information Systems,* AIS Electronic Library (AISeL).

78. Olson Parmy*,* 2018, *Facebook's Zuckerberg Ignores 'The New Reality' By Skipping Fake News Inquiry In London,* www.forbes.com, [27/11/2018].

79. Pagliery Jose *,* 04/12/2013, *2 million Facebook, Gmail and Twitter passwords stolen in massive hack***,** https://money.cnn.com/2013/12/04/technology/security/passwords-stolen**/**, [18/11/2018].

80.**Prashant Jha**, 11/04/2013, Facebook users could swing the results in 160 Lok Sabha constituencies, 2013, http://www.thehindu.com/news/national/facebook-users-could-swing-the-results-in-160-lok-sabha-constituencies/article4607060.ece[27/09/2018]

81.Protalinski E.,16/01/2012, *56% of employers check applicants' Facebook, LinkedIn, Twitter*, http://www.zdnet.com/article/56-of-employers-check-applicants-facebook-linkedin-twitter/[28/09/2018]

82. Ragnedda Massimo,2013,pages 43 – 48,*Social Networks and the Protection of Personal Information. When Privacy Is Not Perceived As a Right, N*ovática Special English Edition

83. **Rannenberg K., D. Royer, A. Deuker,** 2009, *The Future of Identity in the Information Society: Challenges and Opportunites,* School of Law, University of Warwick, EBSCOhost.

84. Rathor A., P. Mishra, 2013, Volume 10Issue 6 pages 59 – 65**,** *Social Networking Websites and Image Privacy,*IOSR.

85.**Renner Christoph,** 2010, *Privacy in Online Social Networks,* Swiss Federal Institute of Technology (ETH Zurich).

86. Ridler Faith , 2018, *Maths teacher, 33, is suspended after secondary school pupils share five-year-old raunchy snaps and jokes about her 'big boobs' on Facebook, https://www.dailymail.co.uk/news/article-6424003/Maths-teacher-suspended-secondary-school-pupils-share-raunchy-snaps.html*, [25/11/2018].

87. **Romm *Tony , Elizabeth Dwoskin,2018,*** Facebook says it removed a flood of hate speech, terrorist propaganda and fake accounts from its site *https://www.washingtonpost.com/technology/2018/11/15/facebook-says-it-removed-flood-hate-speech-terrorist-propaganda-fake-accounts-its-site/?noredirect=on&utm_term=.43d9d94ef0de,[10/11/2018]*

88.Rosen Peter, Sherman Peter, 2014, *Hedonic Information Systems: Acceptance of Social Networking Websites,* AIS Electronic Library

89. **Sahinoglu Mehmet, Aysen DenerAkkaya, DavidAng,** 2012, Pages 163-169, *Can We Assess and Monitor Privacy and Security Risk for Social Networks?,* ELSEVIER.

90. **Şerbu Răzvan, Irina Rotariu,** 2015, Pages 73-76, *Privacy Versus Security in the Internet Era,* ELSEVIER.

91. ***S*loane Garett** , 2018, *FACEBOOK E-MAILS REVEAL ZUCKERBERG DELIBERATIONS ON USER DATA, https://adage.com/article/digital/facebook-e-mails-offer-a-unique-zuckerberg-work/315890* , [06 Δεκεμβρίου 2018].

92. **Smallwood Robert F.** , 2014, pages 119 -120, *Information Governance: Concepts, Strategies, and Best Practices,* Wiley Pablications, 2014.

93. **Spivack Nova** , Web 3.0: The Third Generation Web is Coming. *Lifeboat Foundation.* [Online] https://lifeboat.com/ex/web.3.0,[26/01/2019].

94.Staff E., 23/04/2010, Verisign,: 1.5m Facebook accounts for sale in web forum,PC Magazine, http://www.pcmag.com/article2/0,2817,2363004,00.asp[27/09/2018]

95. S. Stieger, C. Burger, M. Bohn, M. Voracek, 2013, Volume 16 No 9**,** *Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters,* Mary Ann Liebert, Inc.

96. **Stringhini G., G. Wang, M. Egele, C. Kruagel, G. Vigna, Z. Ben, Y. Zhao,** 2013 *Follow the Green:Growth and Dynamics in Twitter Followers Markets,* EBSCOhost,.

97. **Tabitha L.James, Linda Wallace, Merrill Warkentin, Byung Cho Kim, Stéphane E.Collignone,** 2017, Pages 851-865, *Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use,* ELSEVIER.31.

98.Taraszow Tatjana, Aristodemou Elena, Shitta Georgina, Laouris Yiannis, Arsoy Aysu, 2010, Volume 6 No 1 pages 81–101, Disclosure of persolan and conduct information by young people in social networking sites: An analysis using Facebook profiles as an example. Bristol UK: Intellect books, Intellect.

99. Thackeray Rosemary, Brad L. Neiger,Carl L. Hanson,James F. McKenzie, 2009, pages 338 – 343, *Enhancing Promotional Strategies Within Social Marketing Programs: Use of Web 2.0 Social Media,* SAGE PUBLICATIONS.

100. Wang H., D. He, J. Yu,2018, Volume 470 pages 15 – 27, *Privacy - preserving incentive and rewarding scheme for crowd computing in social media,* ELSEVIER

101. Wang Rui, Shuo Chen, XiaoFeng Wang*,* 2012, Symposium on Security and Privacy, *Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services,* IEEE.

102.Wagner C.,Mitter S., Körner C., Strohmaier M., 2012, pages 41-48, *When social bots attack: modeling susceptibility of users in online social networks,* Proceedings of the 2012 International Conference on World wide web (WWW),MSM2012.

103. **Weir George R S, Fergus Toolan, Duncan Smeed,** 2011, Technical Report, 16 (2). pp. 38-43, *The threats of social networking : old wine in new bottles?* s.l. : University of Strathclyde Glasgow,.

104.wikipedia,(2009),*FacebookBeacon,*https://en.wikipedia.org/wiki/Facebook_Beacon,https://en.wikipedia.org/wiki/Facebook_Beacon [27/09/2018]

105. Wilson, Zeynep Tufekci Christopher, 2012, Pages 363–379, *Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square,* Oxford Academic .

106. Xiaoa Xi, Chunhui Chen,Arun Kumar,Sangaiahb Guangwu, Hu,Runguo Ye,Yong Jianga, 2017, *CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks,* ELSEVIER.

107. **Yonghwan Kim, Hsuan-TingChen, Homero Gil de Zúñiga,** 2013, Pages 2607-2614**,** *Stumbling upon news on the Internet: Effects of incidental news exposure and relative entertainment use on political engagement,*ELSEVIER.Z

108.Zephoria, The Top 20 Valuable Facebook Statistics, Zephoria2017, https://zephoria.com/top-15-valuable-facebook-statistics, [10/10/2018]

109. Zhang G., Q. Jin, M. Lin, De Oracle @ UMUC, 2010, *Social media and distance education,* https://www.scribd.com/document/160525480/Social-Media-and-Distance-Education-De-Oracle, [08/11/2018]

110. **Zhang Shiwen, Qin Liu, Yaping Lin,** 2017, Pages 227-238, *Anonymizing popularity in online social networks with full utility.*

111. Zhang Shaobo, Kim-Kwang Raymond Choob, Qin Liud, GuojunWang, 2018, Pages 881-892, *Enhancing privacy through uniform grid and caching in location-based services*.

112.Zhivago Zhangab Brij B.Gupta ,2016,Volume 86 pages 914 – 925, *Social media security and trustworthiness: Overview and new direction. In Future Generation Computer System,* Elsevier.

Ελληνική Βιβλιογραφία

113. **Αγγελίνη Μίνα,** 2018, *ο «TFacebook μπορεί να οδηγήσει σε κατάθλιψη», προειδοποιούν Αμερικανοί επιστήμονες,* www.protothema.gr, [19/11/2018].

114.Κουτσογιαννοπούλου Ν., 2013, Τα νέα μέσα ηλεκτρονικής κοινωνικής δικτύωσης (Social Media) και η σχέση τους με την καταναλωτική συμπεριφορά. Πανεπιστήμιο Πατρών .

115. **Λιμνιώτης Κωνσταντίνος,** σελίδες 1 – 19, κεφάλαιο 12**,** *Διαχείριση Κινδύνων Ασφαλείας Πληροφοριακών και Επικοινωνιακών Συστημάτων*, Open University of Cyprus.

116. **Safeline** , Annual report 2017, pages 10 – 11 http://www.safeline.gr/sites/default/files/safeline_annual_report_2017gr.pdf, [15/02/2019]

117. Ευρωκυνοβούλιο , 2019, *Fighting fraud with non-cash means of payment : Council agrees its position*,https://www.consilium.europa.eu/en/press/press-releases/2018/03/09/fighting-fraud-with-non-cash-means-of-payment-council-agrees-its-position/ 09/03/2018, [18/02/2019]

118. **Ευρωπαική Ένωση, 2019, Fact Sheet** ,*Tackling online disinformation, http://europa.eu/rapid/press-release_MEMO-18-3371_en.htm*, 6/04/2018,[18/02/2019]

***119.ΣΕΠΑ**,2019, Στις 3,1 ώρες η μέση ημερήσια χρήση του Διαδικτύου στην Ελλάδα,http://*www.sepe.gr/gr/research-studies/article/10241144/stis-31-ores-i-mesi-imerisia-hrisi-tou-diadiktuou-stin-ellada/ , 08/12/2017, [19/02/2019]