Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ - ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

Τμήμα Τεχνολογίας Πληροφορικής &
Τηλεπικοινωνιών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΥΓΚΡΙΣΗ ΠΕΡΙΒΑΛΛΩΝΤΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Επιβλέπων Καθηγητής: Μακροδημήτρης Γεώργιος

Φοιτητής: Διακογιαννάκης Ηλίας *ΑΜ: 2006039*

Σπάρτη, Νοέμβριος 2012

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ **ΥΠΟΓΡΑΦΕΣ**

1.

2.

3.

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας.

Ο συγγραφέας,

Διακογιαννάκης Ηλίας

Ευχαριστίες

Έχοντας φτάσει στο τέλος της πτυχιακής μου εργασίας, αισθάνομαι υποχρεωμένος να μιλήσω για κάποιους ανθρώπους, που ο καθένας με τον δικό του τρόπο σηματοδότησε την πορεία των χρόνων μου στις προπτυχιακές σπουδές μου και να τους ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα μου, κύριο Μακροδημήτρη Γιώργο, Επιστημονικό Συνεργάτη του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας, διότι η συνεργασία μαζί του ήταν ένας καταλύτης για την ολοκλήρωση των προπτυχιακών σπουδών μου. Τα αποτελέσματα της εργασίας αυτής είναι από τη συνεργασία με τον κ. Μακροδημήτρη. Η συνεργασία μας ξεκίνησε όταν ήμουν προπτυχιακός φοιτητής στο χειμερινό εξάμηνο του 2011– 2012, στο μάθημα «Διαχείριση Έργων Πληροφορικής». Από τη συνεργασία αυτή, είχα την πρώτη εμπειρία σύγκρισης περιβαλλόντων κοινωνικής δικτύωσης που χρησιμοποιώ, όχι μόνο εγώ αλλά και σχεδόν ολόκληρος ο πλανήτης. Ερεύνησα και έμαθα τι κίνδυνοι υπάρχουν και πώς μπορώ να τους αντιμετωπίσω ούτως ώστε να κάνω μία σωστή χρήση αυτών των ιστοσελίδων.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου Γιάννη και Δέσποινα για την αμέριστη υποστήριξή τους όλα αυτά τα χρόνια, των προπτυχιακών σπουδών μου. Αφιερώνω αυτή την εργασία στους γονείς μου, ως ελάχιστη ευγνωμοσύνη για την κατανόηση και την υπομονή τους όλα αυτά τα χρόνια.

Διακογιαννάκης Ηλίας

Σπάρτη, 12 Νοεμβρίου 2012

Περιεχόμενα

Κεφάλαιο 0: Εισαγωγή **11**

Ιστορική Αναδρομή *11*

Το Φαινόμενο της Κοινωνικής Δικτύωσης *14*

Σύνδρομο του Δικτυακού Εθισμού *17*

Τα δημοφιλέστερα site κοινωνικής δικτύωσης *20*

Κεφάλαιο 1: Περιβάλλοντα Κοινωνικής Δικτύωσης **23**

1.1 Facebook *23*

1.1.1 Ιστορική Αναδρομή 23

1.1.2 Παρουσίαση 25

1.1.3 Τεχνικοί Όροι 27

1.1.4 Ρυθμίσεις απορρήτου 29

1.1.5 Επιρροές 30

1.1.6 Προβλήματα Ασφαλείας 31

1.2 Twitter *32*

1.2.1 Ιστορική Αναδρομή 32

1.2.2 Παρουσίαση 33

1.2.3 Τεχνικοί Όροι 35

1.2.4 Πολιτική απορρήτου 35

1.2.5 Επιρροές 36

1.2.6 Προβλήματα Ασφαλείας 37

1.3 GooglePlus *38*

1.3.1 Ιστορική Αναδρομή 38

1.3.2 Παρουσίαση 39

1.3.3 Τεχνικοί Όροι 41

1.3.4 Πολιτική Απορρήτου 42

1.3.5 Επιρροές 43

1.3.6 Προβλήματα Ασφαλείας 44

Κεφάλαιο 2:Εξειδίκευση Προβλημάτων **47**

2.1 Facebook *48*

2.1.1 hacking 48

2.1.2 Κοινωνικά Προβλήματα 55

2.1.3 Προσβολές Προσωπικότητας 58

2.2 Twitter *61*

2.2.1 Hacking 61

2.2.2 Κοινωνικά προβλήματα 66

2.2.3 Προσβολές προσωπικότητας 67

2.3 Googleplus *70*

2.3.1 Hacking 70

2.3.2 Κοινωνικά Προβλήματα 72

2.3.3 Προσβολές Προσωπικότητας 73

2.4 Πνευματικά Δικαιώματα σε Περιβάλλοντα Κοινωνικής Δικτύωσης *74*

Κεφάλαιο 3: Νομοθεσία **77**

Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο 79
Ιοι- Προστασία των δεδομένων από ιούς 80
Προστασία δεδομένων προσωπικού χαρακτήρα 82
Απάτη μέσω του Διαδικτύου 82
Spamming 82
Προστασία της Πνευματικής Ιδιοκτησίας 83
Δικαιοδοσία στο Ιντερνετ 83

Κεφάλαιο 4: Θέσπιση κανόνων ασφαλείας **85**

4.1 Από την πλευρά του χρήστη *85*

4.2 Από την πλευρά των ιστοσελίδων *87*

Κεφάλαιο 5: Συμπεράσματα **89**

Έρευνα **90**

Σύνολο: 90
Ηλικία: Έως 20 χρόνων 97
Ηλικία:21-30 104
Ηλικία: 31-45 111
Ηλικία: 46-77 118

Βιβλιογραφία **125**

Περιεχόμενα Εικόνων

Εικόνα 1: Πόσα άτομα χρησιμοποιούν κοινωνικά δίκτυα σε μερικές από τις μεγαλύτερες χώρες του κόσμου. 16
Εικόνα 2: Πώς θα ήταν τα online δίκτυα αν μπορούσαμε να τα απεικονίσουμε 20
Εικόνα 3: Logo Facebook 23
Εικόνα 4: TheFacebook 23
Εικόνα 5: Χρήστες του Facebook βάσει την ηλικία 24
Εικόνα 6: Το Facebook στο χρηματιστήριο 25
Εικόνα 7: Πριν 26
Εικόνα 8: Μετά 27
Εικόνα 9: Αρχική σελίδα Facebook 27
Εικόνα 10: Ρυθμίσεις απορρήτου Facebook 30
Εικόνα 11: Υπάρχει ασφάλεια στο Facebook; 31
Εικόνα 12: Logo Twitter 32
Εικόνα 13: Νέο Logo 32
Εικόνα 14: Παλιό Logo 32
Εικόνα 15: Twitter – follow me 34
Εικόνα 16: Αρχική σελίδα Twitter 35
Εικόνα 17: Twitter privacy settings 36
Εικόνα 18: Διαφημιστικό logo Twitter 37
Εικόνα 19: Twitter και ασφάλεια 37
Εικόνα 20: Logo Googleplus 38
Εικόνα21: Ένα προφίλ στο Googleplus 39
Εικόνα 22: Αρχική σελίδα Googleplus 41
Εικόνα 23: Privacy settings Googleplus 43
Εικόνα 24: Το Googleplus θα κατακτήσει πολλούς χρήστες ανά τον κόσμο 44
Εικόνα 25: Ασφάλεια στο Googleplus 45
Εικόνα 26: Facebook phishing,scams,hacking 48
Εικόνα 27: Facebook phishing 50
Εικόνα 28: cookie που κρατά συνδεδεμένους χρήστες - Facebook 53
Εικόνα 29: Τι γνωρίζει το Facebook για εμάς 54
Εικόνα 30: Ασφάλεια στο Facebook 55
Εικόνα 31: Εικόνα Facebook 55
Εικόνα 32: Εικόνα Facebook 57
Εικόνα 33: Εικόνα κατά του ρατσισμού 60
Εικόνα 34: Εικόνα Twitter κατά τη διάρκεια του DoS 61
Εικόνα 35: εικόνα Twitter όταν ήταν overfload 64
Εικόνα 36: Anonymous στο twitter 64
Εικόνα 37: κίνδυνοι στο ιντερνέτ 65
Εικόνα 38: Ρατσιστική επίθεση 68
Εικόνα 39: Ρατσιστική επίθεση 2 68
Εικόνα 40: κλοπή χρημάτων μέσω διαδικτύου 70
Εικόνα 41: Logo για Ασφάλεια στο Googleplus 71
Εικόνα 42: Stop SOPA and PIPA 75

Κεφάλαιο 0: Εισαγωγή

Ιστορική Αναδρομή

Ο άνθρωπος είναι από τη φύση του κοινωνικό ον, έλεγε ο Αριστοτέλης. Η κοινωνικότητα είναι μια αξία πολύ σημαντική, ίσως η σημαντικότερη για την ανθρώπινη κοινωνία. Ο άνθρωπος έχει την ανάγκη να ζει και να συναναστρέφεται με άλλους και πάντα ψάχνει νέους δρόμους για την επαφή με περισσότερο κόσμο. Ξεκινάει με την οικογένεια, το σχολείο, τη γειτονιά. Με την εξέλιξη της τεχνολογίας μπήκαν στη ζωή του, ο ηλεκτρονικός υπολογιστής και το διαδίκτυο. Ο άνθρωπος έμαθε ότι μπορούσε μέσω του διαδικτύου να έρθει σε επαφή με άλλους από όλα τα μέρη του κόσμου. Από εκείνη τη στιγμή έψαχνε να βρει τρόπους για να επικοινωνήσει με αυτούς. Οι πρώτες σελίδες κοινωνικής δικτύωσης εμφανίζονται τη δεκαετία του 1990. Δεν είχαν τη μορφή και τις λειτουργίες που έχουμε συνηθίσει σήμερα.

Θα ξεκινήσουμε με το World Wide Web και το Mosaic. Το World Wide Web (WWW) είναι μια από τις σημαντικότερες καινοτομίες του διαδικτύου. Σε γενικές γραμμές το διαδίκτυο είναι μια πλατφόρμα που καθιστά εξαιρετικά εύκολο να διασυνδέει έγγραφα τα οποία είναι διαθέσιμα μέσω αυτού. Σήμερα, σχεδόν ο καθένας που χρησιμοποιεί το Διαδίκτυο μπορεί εύκολα να έχει πρόσβαση σε αυτό με τη χρήση ενός απλού web browser, όπως του google chrome, του safari, του opera ή του Mozilla Firefox. Το web browser Mosaic κυκλοφόρησε το 1993. Ήταν browser εύκολος στη χρήση, με γραφικά που δημιουργούνται από το πρόγραμμα περιήγησης NCSA. Έδωσε τη δυνατότητα σε χρήστες ηλεκτρονικών υπολογιστών να έχουν ευκολότερη πλοήγηση στον ιστό και προβολή εικόνων ενσωματωμένων στο κείμενο και όχι εικόνων σε ξεχωριστό παράθυρο. Θα πρέπει να σημειωθεί ότι ο Marc Andreessen που ήταν ο ηγέτης του Mosaic, προχώρησε στην ανάπτυξη του Netscape browser, το οποίο για το μεγαλύτερο μέρος της δεκαετίας του 1990 ήταν το πιο ευρέως χρησιμοποιούμενο πρόγραμμα περιήγησης.

Ακολούθησε ο πόλεμος των browser. Το Netscape ήταν η υπερδύναμη. Ήταν μια δύναμη όχι μόνο σε τιμή μετοχών αλλά και σε μερίδιο αγοράς. Σε ένα σημείο στα μέσα της δεκαετίας του 1990, το ποσοστό που χρησιμοποιούσε το Netscape ήταν σχεδόν 85% του συνόλου των υπολογιστών για την περιήγηση στο διαδίκτυο. Τότε η Microsoft συνειδητοποίησε ότι το διαδίκτυο και συγκεκριμένα το web ήταν μια σημαντική πτυχή της τεχνολογίας για να επενδύσει σε αυτό. Με την κυκλοφορία των Windows 98, η Microsoft συμπεριέλαβε ένα δωρεάν πρόγραμμα περιήγησης που έχει ήδη εγκατασταθεί στο ολοκληρωμένο λειτουργικό σύστημα των Windows που ονομάζεται Internet Explorer. Σε

λίγα χρόνια, το μερίδιο αγοράς του Netscape περιορίστηκε από το 85% που κατείχε σε ποσοστό μικρότερο από 1%. Από το 2003, το Netscape έπαψε να υπάρχει. Η Microsoft υποχρεώθηκε από την κυβέρνηση των ΗΠΑ αλλά και από άλλες κυβερνήσεις παγκοσμίως να σταματήσει την κατάχρηση μονοπωλιακής ισχύος όσον αφορά τους web browser. Παρόλα αυτά η χρήση του Microsoft Internet Explorer αυξήθηκε, από το ελάχιστο ποσοστό που χρησιμοποιείτο στα μέσα της δεκαετίας του 1990 σε πάνω από 90% λόγω της ενσωμάτωσής του στα windows 98.

Όσον αφορά το Firefox ήταν αρχικά ένας γραφικός web browser που αναπτύχθηκε στις αρχές της δεκαετίας του 1990 από το Mozilla Corporation, ωστόσο σήμερα, είναι ένας από τους ταχύτερα αναπτυσσόμενους browser ανοικτού κώδικα στο διαδίκτυο. Ο Mozilla Firefox κυκλοφόρησε αρχικά με τη νέα μορφή του στις 9 Νοεμβρίου 2004. Σήμερα, το μερίδιο αγοράς του αντιστοιχεί περίπου στο 15% του συνόλου, που είναι ένα απίστευτο κατόρθωμα για ένα πρόγραμμα περιήγησης ανοιχτού κώδικα, να το επιτύχει μέσα σε λίγα χρόνια.

Οι ηλεκτρονικοί υπολογιστές που είχαν πρόσβαση στο διαδίκτυο όμως στην αρχή ήταν μόνο μερικές εκατοντάδες ή και μερικές χιλιάδες. Γρήγορα όμως ο αριθμός αυτός έφτασε τις εκατοντάδες χιλιάδες στις αρχές του 1990. Με τόσες πολλές πληροφορίες στο διαδίκτυο, έπρεπε να βρεθεί ένας γρήγορος και αποτελεσματικός τρόπος για την αναζήτηση και ανάκτηση πληροφοριών. Έτσι έκαναν την εμφάνιση τους οι μηχανές αναζήτησης για να εκπληρώσουν αυτή την ανάγκη. Την εξεύρεση δηλαδή όλων των τύπων των πληροφοριών μέσω του Διαδικτύου (ειδικότερα το World Wide Web). Δύο μηχανές αναζήτησης που έφεραν την επανάσταση του Διαδικτύου κατά τη διάρκεια της δεκαετίας του 1990 και στις αρχές του 2000 ήταν η yahoo και η Google.

Ο άνθρωπος όμως παράλληλα με την εξέλιξη της τεχνολογίας είχε βρει νέους δρόμους επικοινωνίας. Ήταν τα γνωστά σε όλους μας forum, τα e-mail και τα chat room. Με την πρόσβαση στο διαδίκτυο και μέσω ενός browser ο χρήστης μπορούσε να έχει προσωπική επικοινωνία με έναν άλλο χρήστη. Ξεκίνησε με τη μορφή ενός απλού κειμένου. Σήμερα όμως μπορεί μέσω e-mail να γίνει η αποστολή συνημμένων αρχείων, εικόνων ακόμα και streaming video. Το forum ξεκίνησε ως ψηφιακός πίνακας συστήματος. Σήμερα, το φόρουμ επιτρέπει στα μέλη να δημιουργήσουν νήματα (θέματα), να συζητήσουν τα θέματα αυτά, έχουν μια συζήτηση με τα άλλα μέλη, κλπ. Υπάρχουν φόρουμ για σχεδόν κάθε κατηγορία, (π.χ. αυτοκίνητα, αθλητικά, τεχνολογίας υπολογιστών, pop κουλτούρα, μουσική, κτλ). Στα

chat room ο χρήστης μπορούσε να έρθει σε επαφή με κάποιον άλλο χρήστη σε πραγματικό χρόνο για πρώτη φορά. Ακλούθησαν το mIRC, MSN, skype και πολλά ακόμα.

Ενώ chat rooms, forums και online dating sites και τα υπόλοιπα προγράμματα επικοινωνίας εξακολουθούν να είναι εξαιρετικά δημοφιλή, κατά τα πρώτα μέχρι τα μέσα του 2000 ένα άλλο κοινωνικό φαινόμενο εμφανίστηκε στο Διαδίκτυο, οι ιστότοποι κοινωνικής δικτύωσης. Σήμερα, site κοινωνικής δικτύωσης όπως twitter και Facebook είναι δυο από τα πιο δημοφιλή και επιτυχημένα site. Οι χώροι αυτοί φροντίζουν για τους νέους, τους έφηβους και τους ενήλικες που επιθυμούν να έχουν τη δική τους ατομική παρουσία σε απευθείας σύνδεση με τη μορφή της δικής τους σελίδας και να δημιουργούν σχέσεις με τους άλλους. Οι ιστότοποι κοινωνικής δικτύωσης δεν είναι μόνο για διασκέδαση, στην πραγματικότητα, αλλά είναι χρήσιμοι και για τα άτομα που επιθυμούν να δικτυώσουν τις επιχειρήσεις τους. [1]

Το Φαινόμενο της Κοινωνικής Δικτύωσης

Η κοινωνική δικτύωση αποτελεί κατά πολλούς ένα εκπληκτικό τεχνολογικό φαινόμενο του 21ου αιώνα. Τι συμβαίνει όμως σε αυτές τις σελίδες; Τα άτομα δημιουργούν προφίλ δικού τους περιεχομένου, το οποίο μπορούν να μοιραστούν με ένα ευρύ δίκτυο ατόμων, ακόμα και σε παγκόσμιο επίπεδο. Μπορούν να σχολιάζουν το περιεχόμενο άλλων προφίλ και έχουν τη δυνατότητα για μεταφόρτωση φωτογραφιών, καταχώριση εγγράφων ημερολογίου, δημιουργία κειμένων με εικόνες, μουσική και βίντεο κ.α. Οι δυνατότητες των ιστοσελίδων πολλαπλές. Οι χρήστες μπορούν να δημιουργήσουν μία εικονική πραγματικότητα, όπου μπορούν να φτιάξουν ψηφιακά πρόσωπα και να συνομιλήσουν με «φίλους» τους, σε πραγματικό χρόνο ανταλλάσοντας ηλεκτρονικά ψηφιακό υλικό. Πρόκειται για δραστηριότητα ιδιαίτερα προσφιλή στους νέους και δεν απαιτεί εξειδικευμένες τεχνικές γνώσεις. Σήμερα το διαδίκτυο έχει κατακλυσθεί με περίπου 350 ιστότοπους του είδους, οι οποίοι διαχωρίζονται με βάση τον τρόπο εγγραφής των χρηστών, το είδος του περιεχομένου, και έχουν εκατομμύρια μέλη.

Πιο συγκεκριμένα τα site κοινωνικής δικτύωσης προσφέρουν στους χρήστες τους πολλά οφέλη και πλεονεκτήματα. Τα κοινωνικά δίκτυα έχουν παγκόσμια έκταση και πολυφωνία. Ο χρήστης έχει τη δυνατότητα δημιουργίας δεσμών με μεγάλο πλήθος ατόμων τα οποία μπορεί να βρίσκονται και σε μεγάλη γεωγραφική απόσταση αφού τα site συγκεντρώνουν πλήθη ανά τον κόσμο. Έτσι καταργείται κατά κάποιο τρόπο η απόσταση. Αποτέλεσμα, ο χρήστης να είναι σε θέση να δημιουργήσει μεγάλης ποικιλίας κοινωνικούς δεσμούς, γνωρίζοντας έτσι κουλτούρες άλλων λαών με διαφορετικές συνήθειες και χαρακτηριστικά, να ανταλλάξει ιδέες και απόψεις. Ο άνθρωπος με αυτόν τον τρόπο διευρύνει τις γνώσεις και τους ορίζοντες του. Ακόμα υπάρχει η δυνατότητα δραστηριοποίησης ατόμων απ' όλο τον κόσμο με τον ίδιο σκοπό. Για παράδειγμα μία παγκόσμια ομάδα φιλόζωων, οπαδοί ομάδας ποδοσφαίρου, και πολλές άλλες. Πολλά σημαντικά οφέλη είναι επίσης η ανεύρεση και ανταλλαγή video και φωτογραφιών στις οποίες ο χρήστης δεν θα μπορούσε να έχει πρόσβαση αλλιώς, η δυνατότητα άμεσης ενημέρωσης αφού οι ειδήσεις στο διαδίκτυο μεταδίδονται με ταχύτατους ρυθμούς και τέλος άφθονη ψυχαγωγία με online παιχνίδια, μουσική, ακόμα και με παρακολούθηση video.

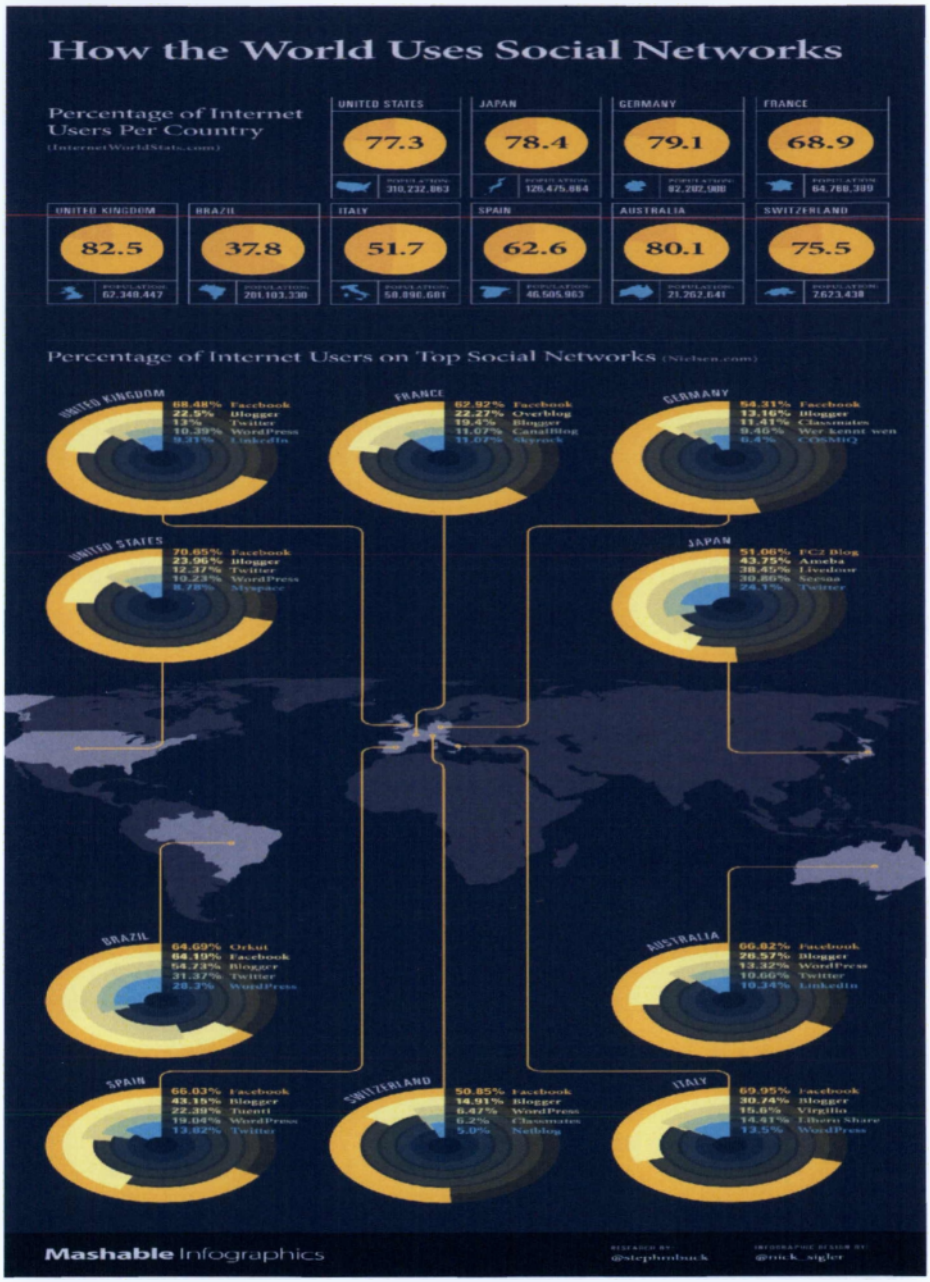
Με την είσοδο όμως στον δικτυακό κόσμο και συγκεκριμένα στα site κοινωνικής δικτύωσης ερχόμαστε αντιμέτωποι με την αντιμετώπιση προβλημάτων που απορρέουν από τη δημιουργία και τη χρήση τους. Υπάρχουν θέματα ασφαλείας των προσωπικών δεδομένων των χρηστών με τη διαρροή για παράδειγμα προσωπικών φωτογραφιών, και άλλων προσωπικών στοιχείων με ανεξέλεγκτες συχνά συνέπειες, ο κίνδυνος της εξαπάτησης

δηλαδή σύνδεση με άτομα που ισχυρίζονται ότι είναι κάποιοι που δεν είναι, καταπάτηση πνευματικών δικαιωμάτων, προσβολές προσωπικότητας, θέματα hacking καθώς και εμφάνιση παιδόφιλων, βιαστών που εκμεταλλεύονται τα site αυτά για τους απώτερους σκοπούς τους και τέλος ο βομβαρδισμός του χρήστη με διαφημιστικά μηνύματα τα οποία βέβαια αποτελούν το κύριο έσοδο των site κοινωνικής δικτύωσης.

Σύμφωνα με έρευνα της Εθνικής Στατιστικής Αρχής, οι λόγοι χρήσης του διαδικτύου είναι ποικίλοι και ολοένα αυξανόμενοι. Η αναζήτηση πληροφοριών και on-line υπηρεσιών παραμένει στην κορυφή της λίστας των δραστηριοτήτων μέσω διαδικτύου (ποσοστό 93,4%). Επίσης, οκτώ στους δέκα χρήστες χρησιμοποίησαν το 2010 το διαδίκτυο για επικοινωνία. Αύξηση παρουσιάζουν χρήσεις του διαδικτύου που αφορούν στην αποστολή μηνυμάτων σε chat sites, blogs και ομάδες συζήτησης (My Space, Facebook κλπ), η συμμετοχή και η ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο (αύξηση 11% περίπου).

Επίσης, σύμφωνα με μια νέα έκθεση του Ινστιτούτου Μελλοντικών Τεχνολογικών Μελετών του Κοινού Κέντρου Ερευνών (JRC) της Ευρωπαϊκής Επιτροπής, το ποσοστό των κοινωνικά δικτυωμένων ευρωπαίων χρηστών αυξάνεται στο 64% (δηλαδή πάνω από δύο στους τρεις) για τα άτομα ηλικίας κάτω των 24 ετών. Παγκοσμίως 165 εκατ. χρήστες συνδέονται κάθε μήνα στις διάφορες υπηρεσίες κοινωνικής δικτύωσης (Facebook, MySpace, Twitter κ.α.). Περίπου μια στις τρεις ευρωπαϊκές επιχειρήσεις (25 – 35%) εκτιμάται ότι πειραματίζεται με κάποια μορφή κοινωνικής δικτύωσης. Η χρήση τους είναι ευρέως διαδεδομένη και στη χώρα μας. Σύμφωνα με δημοσίευση του Συνδέσμου Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας (ΣΕΠΕ), ένας στους τρεις Έλληνες (36%) χρησιμοποιεί σήμερα τα κοινωνικά δίκτυα με σκοπό να έρθει σε επικοινωνία με τους φίλους του, να εκφραστεί, να ψυχαγωγηθεί, να αποδράσει, να φλερτάρει και να εκτονωθεί. Η ενασχόληση εμφανίζει πολύ σημαντικά ποσοστά στους νέους: το 79% μεταξύ των ηλικιών από 13 έως 17 ετών και το 72% μεταξύ των ηλικιών από 18 έως 24 ετών ασχολούνται με τα κοινωνικά δίκτυα. Η άνοδος χρήσης των κοινωνικών δικτύων έφτασε στο 36% από το Σεπτέμβριο ως το Δεκέμβριο του 2010. Μεταξύ των δημοφιλέστερων προορισμών κοινωνικών δικτύων περιλαμβάνονται τα: Facebook, Youtube, Twitter, myspace.com, hi5 και flickr. Ειδικότερα το Facebook αποτελεί τον δημοφιλέστερο κόμβο, αφού συγκεντρώνει επισκεψιμότητα της τάξεως του 21% των Ελλήνων σε επίπεδο ημέρας, του 31% σε επίπεδο εβδομάδας και του 33% σε επίπεδο μήνα, ενώ ραγδαία αποτυπώνεται η εξέλιξη του, καθώς έχει πενταπλασιαστεί ο αριθμός των ημερήσιων επισκεπτών του μέσα στα τελευταία 2 χρόνια.

Παρακάτω βλέπουμε ένα ινφόγραμμα για την χρήση των κοινωνικών δικτύων σε μερικές από τις μεγαλύτερες και πιο γνωστές χώρες του κόσμου. Όπως φαίνεται η χρήση τους βρίσκεται σε πολύ υψηλά επίπεδα, και το πιο διαδεδομένο site κοινωνικής δικτύωσης είναι το Facebook.



Εικόνα 1: Πόσα άτομα χρησιμοποιούν κοινωνικά δίκτυα σε μερικές από τις μεγαλύτερες χώρες του κόσμου.

Σύνδρομο του Δικτυακού Εθισμού

Έχει παρατηρηθεί όμως ότι οι χρήστες που απλά δικτυώνονται κοινωνικά μέσω των site αυτών είναι ελάχιστοι, αφού στην πραγματικότητα το μεγαλύτερο πλήθος αναλώνει ένα τεράστιο κομμάτι της ημέρας του σε αυτά. Στο σπίτι, στην καφετέρια, στο δρόμο, ακόμα και στη δουλειά πολλοί χρήστες θα μπουν στο λογαριασμό τους έστω και για λίγο. Γιατί συμβαίνει όμως αυτό; Σύμφωνα με το ψυχολογικό άρθρο [«Ο εθισμός του Facebook. Γιατί κολλάμε εύκολα σε αυτό;» του Ψυχολόγου Μερσινία Θωμά] ο άνθρωπος αρχικά βιώνει κοινωνικά μια προσωπική ανασφάλεια. Στις μέρες μας η κοινωνία έχει αλλάξει, ο άνθρωπος φοβάται με την κατάσταση που επικρατεί με αποτέλεσμα να οδηγείται στην απομόνωση. Το Facebook λοιπόν για παράδειγμα ήρθε να δώσει τη λύση. Εκεί δημιουργούνται νέες φιλίες από άτομα με κοινά ενδιαφέροντα, που τους επιλέγουμε εμείς. Ο άνθρωπος όσο περισσότερους φίλους έχει τόσο πιο πετυχημένος αισθάνεται. Όμως είναι καλός φίλος αυτός που θα ανταλλάξετε ένα ηλεκτρονικό δώρο σε κάποιο ηλεκτρονικό παιχνίδι;

Τα site κοινωνικής δικτύωσης λοιπόν έχουν αποσπάσει μεγάλο μέρος της ζωής μας και πολλές φορές οδηγούν σε εθισμό. Το γνωστό σύνδρομο του δικτυακού εθισμού. Τα συμπτώματα είναι ποικιλότροπα και διαφορετικά. Για παράδειγμα όταν «σερφάρουμε» σε σελίδες κοινωνικής δικτύωσης έχουμε την αίσθηση της ευφορίας και είναι σχεδόν αδύνατο να σταματήσουμε την δραστηριότητά μας και να ασχοληθούμε με κάτι άλλο, ξοδεύοντας όλο και περισσότερο χρόνο. Παραμελούμε έτσι πολλές φορές την οικογένειά μας αλλά και φίλους που δεν έχουν λογαριασμό σε αυτά. Αποτέλεσμα; Προβλήματα στη δουλειά, στο σχολείο και στο σπίτι. Η ανάλωση πολλών ωρών στον υπολογιστή προκαλεί και σοβαρά σωματικά προβλήματα όπως είναι η σκολίωση, οι ημικρανίες, η ξηρότητα στα μάτια, η μυωπία, ακόμα και προβλήματα προσωπικής υγιεινής. Ειδικά οι νέοι πολλές φορές όταν έχουν εθιστεί πλήρως δεν είναι καν σε θέση να αναγνωρίσουν το πρόβλημά τους. Εκεί χρειάζεται πολλές φορές η παρέμβαση ειδικού.

Το φαινόμενο ξεκινάει από τη μικρή κιόλας ηλικία. Εμφανίζεται κυρίως σε παιδία 10-14 ετών κατά την πρώιμη εφηβεία αλλά αρκετές φορές και σε ακόμα μικρότερη ηλικία. Όμως το φαινόμενο είναι πολύ πιο συχνό κατά την ηλικία των 15-17. Σε αυτό στο στάδιο της ζωής τους οι έφηβοι είναι ευάλωτοι αφού είναι η περίοδος όπου πειραματίζονται και σταδιακά αυτονομούνται.

Πλέον ο διαδικτυακός εθισμός αναγνωρίζεται από την ψυχιατρική κοινότητα ως ξεχωριστή ψυχοσωματική διαταραχή και γι' αυτό το λόγο ακολουθείται ειδική θεραπεία. Στη χώρα μας υπάρχουν πολλά κέντρα που βοηθούν στην αποτοξίνωση των εφήβων. Κάθε

περίπτωση παρακολουθείται από μια ομάδα αποτελούμενη από παιδίατρο, παιδοψυχίατρο, παιδοψυχολόγο και έναν οικογενειακό σύμβουλο. Κατά τη διάρκεια της θεραπείας δεν διακόπτεται η χρήση του διαδικτύου αλλά ο έφηβος ενασχολείται και με άλλες δραστηριότητες μαθαίνοντας έτσι να θέτει όρια. Τα αποτελέσματα δείχνουν ότι ένα στα τρία παιδία ανταποκρίνονται πολύ θετικά στη θεραπεία ειδικά όταν η εξάρτηση βρίσκεται σε πρώιμο στάδιο.

Ωστόσο και ο ρόλος των γονέων είναι εξίσου σημαντικός τόσο στην πρόληψη, όσο και στην αντιμετώπιση τυχόν εθισμού του παιδιού. Η γνώση είναι δύναμη, οπότε ο γονιός θα πρέπει να έρχεται ο ίδιος σε επαφή με το διαδίκτυο για να ξέρει πώς θα το αντιμετωπίσει αν και οι περισσότεροι γονείς δεν το γνωρίζουν και δεν δείχνουν και διατεθειμένοι να έρθουν σε επαφή με αυτό. Ταυτόχρονα, καλό θα ήταν οι γονείς να χρησιμοποιούν κάποιες φορές το διαδίκτυο μαζί με το παιδί ούτως ώστε κατά την εφηβεία ο νέος να έχει ήδη βάλει κάποια όρια στη χρήση του. Καλό λοιπόν θα είναι ο υπολογιστής να βρίσκεται σε κάποιο κοινόχρηστο χώρο και όχι στο δωμάτιο του παιδιού. Ενώ, τέλος, οι γονείς θα πρέπει να συζητούν για τις διαδικτυακές διαδρομές του παιδιού τους, ώστε να έχουν πάντοτε ενημέρωση για τις ιστοσελίδες που επισκέπτεται, τα άτομα με τα οποία συνομιλεί και τις πληροφορίες που ανταλλάσει με άλλα άτομα.[2][πηγή: wikipedia]

Το σύνδρομο του δικτυακού εθισμού εμφανίζεται κυρίως στη νεαρή ηλικία δεν παύει όμως να υπάρχει και σε μεγαλύτερες ηλικίες. Ειδικά η χρήση των site κοινωνικής δικτύωσης έχουν οδηγήσει αρκετούς ανθρώπους στον εθισμό. Οι ενήλικες χρησιμοποιούν σε μεγάλο βαθμό τους ιστότοπους, μιλώντας με φίλους, σχολιάζουν αναρτήσεις, ανεβάζουν φωτογραφίες καθ' όλη τη διάρκεια της ημέρας μη έχοντας άλλες ενασχολήσεις. Δημιουργούνται έτσι προβλήματα στο σπίτι, παρασέρνουν κατά κάποιο τρόπο τα παιδιά, παραμελούν τις δουλειές του σπιτιού, πολλές φορές τα παιδιά και τους συζύγους τους. Ακόμα και στη δουλειά η χρήση είναι εκτεταμένη. Πολλές εργατοώρες χάνονται, μη δίνοντας την πλήρη προσοχή που απαιτείται. Σε τέτοιες περιπτώσεις και οι ενήλικες θα πρέπει να ζητάνε τη βοήθεια ειδικού. Θα πρέπει να οριοθετούν το χρόνο απασχόλησης τους στο διαδίκτυο και να βρουν διαφορετικές ασχολίες. Αφιερώνοντας περισσότερο χρόνο στην οικογένεια, στους φίλους και στη δουλειά τους.

Πώς όμως θα γνωρίζει κάποιος ότι είναι εξαρτημένος; Η εξάρτηση διαπιστώνεται όταν ο χρήστης απαντήσει θετικά σε πέντε από τις οχτώ διαγνωστικές ερωτήσεις της Dr. Kimberly Young, υπεύθυνη ψυχολόγου σε ένα από τα μεγαλύτερα διαγνωστικά κέντρα διαδικτυακής εξάρτησης.

Τα διαγνωστικά κριτήρια της Young για την εξάρτηση από το Διαδίκτυο είναι τα εξής:

1. Αισθάνεσαι απορροφημένος στο διαδίκτυο (σκέψου μια προηγουμένη ή μια μελλοντική περίοδο σύνδεσης στο διαδίκτυο);

2. Αισθάνεσαι την ανάγκη να χρησιμοποιείς το διαδίκτυο για, διαρκώς αυξανόμενα, χρονικά διαστήματα για να επιτύχεις την ικανοποίησή σου;

3. Έκανες, επανειλημμένα, προσπάθειες, που δεν ήταν επιτυχημένες, για να ελέγξεις ή να περιορίσεις ή να σταματήσεις ολοκληρωτικά τη χρήση του διαδικτύου;

4. Αισθάνεσαι ανήσυχος, βαρύθυμος, μελαγχολικός και ευέξαπτος όταν προσπαθείς να περιορίσεις ή να σταματήσεις ολοκληρωτικά το διαδίκτυο;

5. Όταν είσαι συνδεδεμένος με το διαδίκτυο, παραμένεις συνδεδεμένος για περισσότερο χρόνο από όσο σκόπευες αρχικά;

6. Έχεις χάσει ή κινδύνευσες να χάσες μια σημαντική σχέση, μια σημαντική εργασία, μια εκπαιδευτική ευκαιρία ή μια ευκαιρία καριέρας, επειδή είσαι χρήστης του διαδικτύου;

7. Είπες ποτέ ψέματα σε μέλη της οικογένειας σου, στο γιατρό σου ή στον ψυχολόγο σου, για να κρύψεις την έκταση της χρήσης, από σένα, των εφαρμογών του διαδικτύου;

8. Χρησιμοποιείς το διαδίκτυο, σαν ένα τρόπο απόδρασης από τα προβλήματα ή ανακούφισης της πολύ κακής σου διάθεσης; (π.χ. αισθήματα έλλειψης βοήθειας, ενοχής, ανυπομονησίας, μελαγχολίας) ;

Τα δημοφιλέστερα site κοινωνικής δικτύωσης

Οι δημοφιλέστερες ιστοσελίδες κοινωνικής δικτύωσης σε Αμερική και Ευρώπη είναι το Facebook, Twitter, Flickr, Beboo και Myspace. Στην κορυφή ως προς την προτίμηση των χρηστών βρίσκεται το γνωστό Facebook, απαριθμώντας περίπου 200 εκατομμύρια χρήστες. Θραύση ανά τον κόσμο με 117 εκατομμύρια μέλη κάνει το Haboo, ενώ σε Ινδία και Βραζιλία χρησιμοποιείται από 65 εκατομμύρια χρήστες το Orcut. Αμιγώς ελληνική ιστοσελίδα social network είναι το zoo.gr, το οποίο ονομάζεται meeting point και αριθμεί περισσότερους από 890.000 χρήστες.[3]

Εικόνα 2: Πώς θα ήταν τα online δίκτυα αν μπορούσαμε να τα απεικονίσουμε

Επιλέξαμε να ασχοληθούμε με τα Facebook, twitter και Googleplus καθώς είναι ευρέως διαδεδομένα, με εκατομμύρια χρήστες ανά τον κόσμο και ταυτόχρονα τα πιο διαδεδομένα στην Ελλάδα. Η χρήση τους έχει γίνει κομμάτι της καθημερινότητας μας. Οι ιστότοποι αυτοί εκτός από τα θετικά έχουν και πολλά προβλήματα όπως αναφέραμε παραπάνω τα οποία θα αναδείξουμε με παραδείγματα.

Πρώτο την εμφάνισή του έκανε το Facebook, έπειτα το Twitter και πιο πρόσφατα το Googleplus. Οι συγκεκριμένες ιστοσελίδες έγιναν ευρέως γνωστές λόγω της μοναδικότητας τους σε κάποιες λειτουργίες καθώς και της προώθησης τους. Το Facebook για παράδειγμα ξεκίνησε από το πανεπιστήμιο Harvard της Αμερικής και ήταν το πρώτο site που προσέφερε στο χρήστη ότι χρειαζόταν. Προσφέρει τα πάντα, από το ανέβασμα φωτογραφιών, βίντεο και links μέχρι την ενημέρωση φίλων και γνωστών για τον προορισμό των διακοπών σας! Ακόμα περιλαμβάνει τα διάφορα παιχνίδια και τις απίστευτα εθιστικές εφαρμογές που κρατάνε τους χρήστες απασχολημένους για κάμποσες ώρες τη μέρα . Ήταν το πρώτο site που παρείχε όλο το πακέτο. Βοήθησε πολύ στην προώθηση του ο ιδρυτής του γνωστού site

μουσικής Napster, SeanParker. Το Twitter έγινε ευρέως γνωστό από τα γνωστά σε όλους μας tweets, τα οποία είναι κειμενάκια μέχρι 140 χαρακτήρες που οι χρήστες αναρτούν στο προσωπικό τους προφίλ και μπορούν να τα δουν άτομα που δεν είναι απαραίτητο να βρίσκονται στη λίστα φίλων τους. Αυτό γίνεται γιατί η πολιτική του ιστότοπου διαφέρει στο θέμα αυτό. Ο εκάστοτε χρήστης μπορεί να κάνει «follow» κάποιον άλλο. Τα tweets μπορούν να τα δουν όλοι οι followers του χρήστη. Τέλος το Googleplus είναι δημιούργημα της google. Το Googleplus έκανε την εμφάνιση του αργότερα από τα προηγούμενα, αλλά μέσα σε λίγους μόνο μήνες κατάφερε να συγκεντρώσει εκατομμύρια χρήστες. Η διαφορά του βρισκόταν στην καινοτομία. Προσέφερε στο χρήστη ατομική videoκλήση, ομαδική videoκλήση καθώς και διαφορετική, πιο αυστηρή πολιτική απορρήτου.

Κεφάλαιο 1: Περιβάλλοντα Κοινωνικής Δικτύωσης

1.1 Facebook

1.1.1 Ιστορική Αναδρομή

Το facebook είναι ένας ιστότοπος κοινωνικής δικτύωσης με ιδρυτή τον Mark Zuckerberg φοιτητής του πανεπιστημίου του Harvard, με τη βοήθεια των συγκατοίκων του και συμφοιτητών του στο κολέγιο, Eduardo Saverin, Dustin Mosqovitz και Crhis Hughes . Αρχικά ήταν προσβάσιμο μόνο στους φοιτητές του πανεπιστημίου ενώ σύντομα επεκτάθηκε και σε άλλα κολέγια στη Βοστόνη όπως το Ivy league και το Stanford University με αρχικό σκοπό να μπορούν οι νεοεισερχόμενοι φοιτητές να γνωριστούν μεταξύ τους. Το 2005 το δικαίωμα για την πρόσβαση στον ιστότοπο επεκτάθηκε και σε μαθητές συγκεκριμένων λυκείων μέχρι που το 2006 το Facebook έγινε προσβάσιμο σε κάθε άνθρωπο στον πλανήτη εφόσον η ηλικία του ξεπερνούσε τα 13 χρόνια.

Εικόνα 3: Logo Facebook

Αναλυτικότερα όλα ξεκίνησαν στις 28 Οκτωβρίου 2003. Ο Mark Zuckerberg και οι τρεις συμφοιτητές του όντας στο δεύτερο έτος του πανεπιστημίου δημιούργησαν έναν ιστότοπο τον οποίο ονόμασαν αρχικά Facemash. Το site ήταν χιουμοριστικό καθώς ήταν ένα παιχνίδι στην ουσία του τύπου «hot or not». Ανέβασε φωτογραφίες φοιτητριών του Harvard τις οποίες οι επισκέπτες θα μπορούσαν να σχολιάσουν αν είναι hot ή όχι. Πώς όμως κατάφερε να βρει και να ανεβάσει τόσες φωτογραφίες; Σύμφωνα με την εφημερίδα του Harvard, «The Harvard Crimson» ο Mark Zuckerberg παραβίασε το δίκτυο υπολογιστών εννέα σπιτιών[1] και αντέγραψε τα ID των φοιτητών τα οποία περιείχαν φωτογραφίες και κάποιες βασικές πληροφορίες για τον κάθε φοιτητή. Το site είχε τεράστια ανταπόκριση αφού για τις 4 πρώτες ώρες που έμεινε ανοιχτό δέχτηκε 450 επισκέπτες οι οποίοι είδαν 22,000 εικόνες. Το site όμως λίγες μέρες αργότερα έκλεισε μετά από εντολή του πανεπιστημίου και ο Mark Zuckerberg βρέθηκε κατηγορούμενος για καταπάτηση δικαιωμάτων, παραβίαση ασφαλείας και καταπάτηση απορρήτου κλέβοντας φωτογραφίες φοιτητών και ανεβάζοντάς τες στο διαδίκτυο. Στο τέλος όμως όλες οι κατηγορίες αποσύρθηκαν.

Μετά από 6 μήνες ο Mark Zuckerberg άρχισε να γράφει κώδικα για ένα καινούριο site. Στις 4 Φεβρουαρίου του 2004 ήταν έτοιμο το

Εικόνα 4: TheFacebook

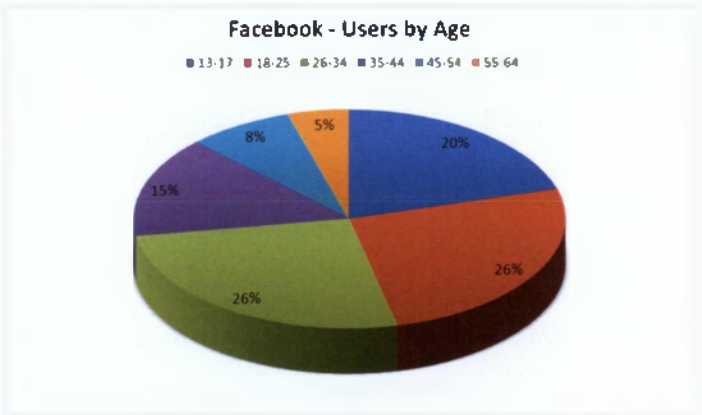
«Thefacebook». Το πρώτο 24ωρο είχε 1200-1500 εγγραφές, μεγάλη επιτυχία για τον ιστότοπο. 6 μέρες αργότερα 3 φοιτητές του Harvard, ο Cameron Winklevoss, ο Tyler Winklevoss και ο Divya Naredra ισχυρίστηκαν ότι ο Mark Zuckerberg, τους είχε εξαπατήσει λέγοντας ότι θα τους βοηθήσει να φτιάξουν το κοινωνικό δίκτυο Harvardconnection.com αφού εκείνοι δεν είχαν τις γνώσεις ενώ στην πραγματικότητα χρησιμοποίησε την ιδέα τους για να φτιάξει το Thefacebook.

Στα μέσα του 2004 και με τη βοήθεια του Sean Parker ο οποίος συμβούλευε τον Mark Zuckerberg στα βήματά του, η βάση του Facebook μεταφέρθηκε στην Καλιφόρνια και κατοχύρωσε το domain name Facebook.com.

Το Σεπτέμβρη του 2005 έγινε το επόμενο βήμα. Το Facebook εξαπλώθηκε και σε πολλά άλλα πανεπιστήμια καθώς και σε υπαλλήλους εταιριών συμπεριλαμβανομένων των Apple και Microsoft. Το Σεπτέμβρη του επόμενου έτους το Facebook θα ήταν πλέον ανοιχτό για όλο τον κόσμο ηλικίας άνω των 13.

Το 2010 σκηνοθετήθηκε και μία αμερικάνικης παραγωγής δραματική βιογραφική ταινία με θέμα την Ιστορία δημιουργίας της κοινωνικής σελίδας και τις μηνύσεις που ακολούθησαν. Η ταινία είχε τεράστια επιτυχία αφού είχε παγκόσμιες εισπράξεις 224,900,000 δολάρια.

Σήμερα το Facebook απαριθμεί 845 εκατομμύρια ενεργούς χρήστες όλων των ηλικιών που συνδέονται από τον υπολογιστή τους, από το κινητό και από το tablet. Παρακάτω βλέπουμε τα ποσοστά χρήσης της σελίδας με βάση την ηλικία των χρηστών. [4]



Εικόνα 5: Χρήστες του Facebook βάσει την ηλικία

Σύμφωνα με πληροφορίες η αναμενόμενη είσοδος της Facebook στο χρηματιστήριο είναι προγραμματισμένη για τις 17 Μαΐου και εξαρτάται κυρίως από τον χρόνο που θα

χρειαστούν οι ρυθμιστικές αρχές για να εγκρίνουν την πρόσφατη εξαγορά ύψους ενός δισεκατομμυρίου της Instagram.

Αποκαλύπτεται, μάλιστα, ότι η εξαγορά της Instagram στο 1 δις έγινε επειδή ο Zuckerberg πίστευε ότι μετά την είσοδο της εταιρείας του στο χρηματιστήριο η αξία των μετοχών θα ήταν μεγαλύτερη από πριν. Με βάση αυτή τη θεωρία η Facebook συμφώνησε να πληρώσει το 30 τοις εκατό σε μετρητά και το υπόλοιπο 70 τοις εκατό σε μετοχές. Διάφορες πηγές αναφέρουν ότι στόχος της εταιρείας είναι να συγκεντρώσει περίπου 10 δις δολάρια από την πώληση των μετοχών με την εκτιμώμενη αξία να ανέρχεται στα 104 δις δολάρια.

Σε κάθε περίπτωση θα ξέρουμε περισσότερα για το θέμα καθώς πλησιάζουμε στην ημερομηνία της 17ης Μαΐου ενώ θα έχει ενδιαφέρον να παρατηρήσουμε την πορεία της εταιρείας από 'κει και πέρα[5]

Εικόνα 6: Το Facebook στο χρηματιστήριο

1.1.2 Παρουσίαση

Ο ιστότοπος είναι μία δωρεάν σελίδα κοινωνικής δικτύωσης για όλες τις ηλικίες. Ο χρήστης μπορεί να φτιάξει το δικό του προφίλ με φωτογραφίες, προσωπικά ενδιαφέροντα, πληροφορίες για το πώς μπορεί κάποιος να έρθει σε επαφή μαζί του, καθώς και πολλές

άλλες πληροφορίες. Υπάρχει επικοινωνία μεταξύ φίλων καθώς και άλλων χρηστών με προσωπικά μηνύματα, δημόσια μηνύματα καθώς και συνομιλία σε πραγματικό χρόνο μέσω chat. Τελευταία έχει προστεθεί φωνητική κλήση καθώς και βίντεο κλήση. Ακόμα υπάρχει η δυνατότητα δημιουργίας ή συμμετοχής σε κάποια ομάδα με κοινά ενδιαφέροντα όπως είναι τα group καλλιτεχνών, αθλητών, πολιτικών και άλλων οργανώσεων, και ομάδες ενημέρωσης με ειδήσεις από όλο τον κόσμο. Το Facebook όμως δεν σταμάτησε εκεί. Ο χρήστης μπορεί να ψυχαγωγηθεί μέσα από τη σελίδα με εκατοντάδες εφαρμογές και παιχνίδια της αρεσκείας του. Πολλά δημοφιλή παιχνίδια είναι το poker, το mafiawars, το castleville και το cityville.

Εκτός από τα προσωπικά προφίλ στο Facebook συναντά κανείς και προφίλ εταιριών και μαγαζιών τα οποία προωθούν τα προϊόντα τους και ανεβάζουν συνδέσμους με εικόνες και προσφορές. Οργανώνονται και διαφημίζονται και συναυλίες καλλιτεχνών, ή συγκεντρώσεις για κάποιο σκοπό. Ακόμα πολλές προεκλογικές εκστρατείες ξεκινούν από το Facebook. Τέλος έχει ξεκινήσει ένα πρόγραμμα για την online προβολή ταινιών μέσω της σελίδας.

Πρόσφατα άλλαξε και η εμφάνιση του προφίλ των χρηστών, από απλή μορφή σε μορφή timeline. Το timeline ξεκινάει από την δημιουργία του προφίλ του χρήστη, μέχρι το σήμερα δείχνοντας τη ζωή του σε βήματα. Φωτογραφίες που έχει ανεβάσει, συνδέσμους και καταστάσεις. Έχει δηλαδή πλέον την παρακάτω μορφή.

Εικόνα 7: Πριν

Εικόνα 8: Μετά

Πώς γίνεται κανείς μέλος; Το Facebook είναι ελεύθερο για όλους. Απαραίτητα για την εγγραφή είναι το ονοματεπώνυμο χρήστη, ένα e-mail, το φύλλο, καθώς και η ημερομηνία γέννησης όπως φαίνεται παρακάτω. [6]

Εικόνα 9: Αρχική σελίδα Facebook

1.1.3 Τεχνικοί Όροι

Το Facebook κατασκευάστηκε από το μηδέν χρησιμοποιώντας λογισμικό ανοιχτού κώδικα. Οι προγραμματιστές έχτισαν την πλατφόρμα με δικές τους εφαρμογές.

Η ομάδα προγραμματιστών της πλατφόρμας του Facebook έχει υλοποιήσει και συντηρεί ανοιχτού κώδικα SDK (Software Development Kit,μια ομάδα εργαλείων που επιτρέπουν τη δημιουργία εφαρμογών) για Android, iOS, Javascript και PHP.Κάποια από τα εργαλεία είναι:

Codemod: Βοηθάει σε μεγάλου μεγέθους μετατροπές κώδικα οι οποίες μπορούν να γίνουν μερικώς αυτόματα αλλά απαιτούν ανθρώπινη επίβλεψη και περιστασιακή μεσολάβηση.

Facebook Animation: Είναι μια συλλογή διάφορων JavaScript η οποία χρησιμοποιείται για την δημιουργία προσαρμοσμένων animation με την διαχείριση των τεχνολογιών DOM και CSS.

Phabricator: Είναι μια συλλογή διαδικτυακών εφαρμογών των οποίων η χρήση διευκολύνει την σύνθεση, αναθεώρηση και συνεισφορά κώδικα. Είναι επί του παρόντος διαθέσιμο ως πρόωρη έκδοση και χρησιμοποιείται από εκατοντάδες προγραμματιστές του Facebook καθημερινά .

PHPEmbed: Κάνει την σύνθεση PHP πραγματικά απλή για όλους τους προγραμματιστές. Η συλλογή αυτή δημιουργήθηκε με βάση το PHPSAPI ως ένα πιο προσιτό και απλοποιημένο API.

Phpsh: Παρέχει ένα αλληλεπιδρών περιβάλλον για την PHP το οποίο έχει ως χαρακτηριστικά, ιστορικό εντολών, ολοκληρώσεις tab και γρήγορη πρόσβαση στα έγγραφα του κώδικα. Είναι κυρίως γραμμένο στην Python.

Three20: Είναι μία συλλογή Objective-C για προγραμματιστές iPhone που παρέχει πολλαπλά στοιχεία και βοηθούς διαχείρισης δεδομένων για την επιφάνεια χρήστη, η οποία χρησιμοποιήθηκε σε παλαιότερες εκδόσεις εφαρμογών iPhone.

XHP: Είναι μια προέκταση της PHP η οποία ενισχύει την σύνταξη της γλώσσας έτσι ώστε να μπορούν να μεταφραστούν τεμάχια έγγραφων XML σε έγκυρες εντολές.

XHProf: Είναι ένας λειτουργικού επιπέδου ιεραρχικός δημιουργός προφίλ PHP που είναι εξοπλισμένος με μια απλή επιφάνεια πλοήγησης γραμμένη σε HTML.

Για την υποδομή χρησιμοποιούνται:

Apache Cassandra: Είναι ένα κατανεμημένο σύστημα αποθήκευσης για την διαχείριση δομημένων δεδομένων που σχεδιάστηκε με την δυνατότητα κλιμάκωσης σε μεγάλα μεγέθη επί πολλών server με καμία περίπτωση αποτυχίας.

Apache Hive: Είναι ένας πυλώνας αποθήκης δεδομένων χτισμένος από Hadoop, που παρέχει εργαλεία που καθιστούν ικανή την περίληψη δεδομένων, άντληση πληροφοριών adhoc και ανάλυση μεγάλου μεγέθους δεδομένων.

FlashCache: είναι μιας γενικού σκοπού write back blockcache για Linux. Γράφτηκε ως μέθοδος Linux Kernel με δυνατότητα φόρτισης, χρησιμοποιώντας το Device Mapper και βρίσκεται κάτω από το σύστημα αρχείων.

HipHop for PHP: Μεταμορφώνει κώδικα PHP σε υψηλά βελτιστοποιημένο κώδικα C++. Προσφέρει υψηλές επιδόσεις και γράφτηκε κατά την περίοδο των δύο τελευταίων χρόνων.

Open Compute Project: Είναι ένα ανοιχτό σχέδιο hardware που σκοπό έχει την επιτάχυνση των κέντρων δεδομένων και καινοτομιών server και παράλληλα αυξάνει την αποδοτικότητα των υπολογιστών μέσω συνεργασίας σχετικών πρακτικών και τεχνικών προδιαγραφών.

Scribe: Είναι μια κλιμακωτή υπηρεσία αθροίσματος ημερολογίων δεδομένων που διαπερνούνται σε πραγματικό χρόνο από μεγάλο αριθμό server.

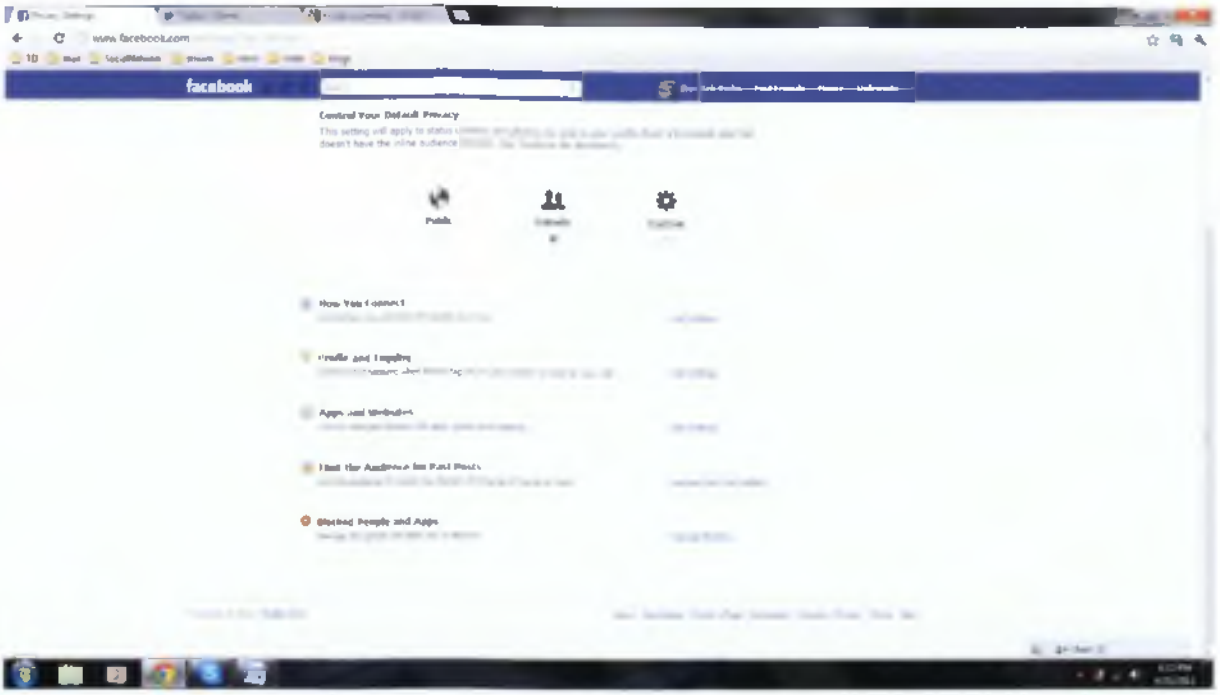
Thrift: Παρέχει ένα πλαίσιο εργασίας για σύνθεση κλιμακωτών υπηρεσιών διασταύρωσης γλωσσών στην C++,Java, Python, PHP και Ruby.

Tornado: Είναι ένα σχετικά απλό, πλην μπλοκαρίσματος πλαίσιο εργασίας server διαδικτύου γραμμένο σε Python. Είναι σχεδιασμένο για να μπορεί να αντέχει χιλιάδες παράλληλες συνδέσεις, κάνοντας το έτσι ιδανικό για υπηρεσίες διαδικτύου σε πραγματικό χρόνο. [7]

1.1.4 Ρυθμίσεις απορρήτου

Το Facebook δεν επικεντρώθηκε μόνο στη δημιουργία υπηρεσιών για τη διασκέδαση των χρηστών αλλά και λειτουργιών για την προστασία των προσωπικών τους δεδομένων.

Συγκεκριμένα υπάρχει ξεχωριστή σελίδα στον ιστότοπο που ονομάζεται privacy settings. Εκεί ο χρήστης μπορεί να ελέγξει και να τροποποιήσει το πώς θα διασφαλίζονται τα προσωπικά του δεδομένα. Από τα πιο απλά, όπως η αλλαγή κατάστασής του μέχρι τις εφαρμογές που χρησιμοποιεί. Κάθε φορά για παράδειγμα που ανανεώνει την κατάστασή του μπορεί να επιλέξει αν θα είναι ορατή σε όλους ή μόνο στους φίλους ή μόνο σε κάποιους από αυτούς. Επίσης μπορεί να ελέγξει ποιοι θα του στέλνουν μηνύματα και αιτήματα φιλίας, καθώς και ποιος μπορεί να γράψει στον τοίχο του, ή να δει τι είναι γραμμένο ακόμα και αν βρίσκεται στη λίστα φίλων του. Επιπλέον μπορεί να ελέγξει τις εφαρμογές που χρησιμοποιεί και τέλος να αναφέρει κάποια άσχημη συμπεριφορά ή spam. Έχει τέλος τη δυνατότητα να μπλοκάρει ανεπιθύμητα άτομα. Πρόσφατα προστέθηκε η επιλογή να μπορεί ο χρήστης να λαμβάνει όλο το υλικό και τις πληροφορίες που τον αφορούν και κατέχει στις βάσεις δεδομένων της η εταιρία.[8]



Εικόνα 10: Ρυθμίσεις απορρήτου Facebook

1.1.5 Επιρροές

- Η δημιουργία του Facebook έχει επηρεάσει την κοινωνική ζωή των ανθρώπων με ποικίλους τρόπους. Ο χρήστης μπορεί να είναι συνδεδεμένος με πολλά μέσα στη σελίδα, όπως το κινητό και ο υπολογιστής. Με αυτόν τον τρόπο μπορεί να είναι συνέχεια σε επαφή με συγγενείς και φίλους απ' όλο τον κόσμο με την προϋπόθεση να είναι συνδεδεμένος στο διαδίκτυο. Έτσι μπορούν να έρθουν και πάλι σε επαφή φίλοι από το σχολείο, μακρινοί συγγενείς και άτομα που είχαν χαθεί. Παράδειγμα ο John Watson ξαναβρήκε τη χαμένη κόρη του από το facebook μετά από 20 χρόνια. Βέβαια η σελίδα έχει κατηγορηθεί από πολλούς ότι προκαλεί αντικοινωνικότητα αφού πλέον ο κόσμος δεν έχει άμεση επαφή παρά μόνο μέσω διαδικτύου.
- Μεγάλη επιρροή έχει ασκήσει και στα media, αφού πλέον πολλές καμπάνιες ξεκινάνε από αυτό όπως για το top gear και το American idol. Ακόμα εφημερίδες και κανάλια το χρησιμοποιούν για να ενημερώσουν τον κόσμο με άρθρα και ειδήσεις.
- Ακόμα πολλές φιλανθρωπίες γίνονται πράξη αφού υπάρχει η δυνατότητα βοήθειας μεγάλου αριθμού ανθρώπων παγκοσμίως μιας και το Facebook είναι ευρέως

γνωστό. Ο κάθε χρήστης μπορεί να δίνει ένα μικρό ποσό για να βοηθήσει σε κάποιο φιλανθρωπικό έργο σε όποιο μέρος του κόσμου και να λαμβάνει χώρα.

- Τέλος δεν μπορούσε να μην επηρεάσει την πολιτική ζωή. Όλα ξεκίνησαν το Ιανουάριο του 2008 όταν η σελίδα σε συνεργασία με το ABC και το κολέγιο Saint Anslem έδωσε στους χρήστες τη δυνατότητα να δούνε σε ζωντανή μετάδοση το debate ρεπουμπλικάνων και δημοκρατικών. Οι χρήστες μπορούσαν να ψηφίσουν ή να στείλουν ερωτήσεις προς τους πολιτικούς. Πλέον πολλές εκστρατείες οργανώνονται μέσω της σελίδας και πολλοί πολιτικοί έχουν group όπου οι ψηφοφόροι μπορούν να μπουν και να μαθαίνουν νέα, ομιλίες που θα γίνουν, να ακούσουν κάποιο πολιτικό λόγο και πολλά άλλα.

Για όλους αυτούς τους λόγους και τις δυνατότητες που προσφέρει ο ιστότοπος στο χρήστη, το Facebook έχει γίνει η πιο διαδεδομένη σελίδα κοινωνικής δικτύωσης στον κόσμο με τους περισσότερους χρήστες.

1.1.6 Προβλήματα Ασφαλείας

Τα facebook παρά τα όσα προσφέρει, τη φήμη του και τους εκατομμύρια χρήστες σε όλο τον κόσμο δεν παύει να έχει προβλήματα. Ένα μείζον πρόβλημα είναι το hacking ή αλλιώς security attacks. Τέτοια είναι: Like jacking, one of phishing attack, phishing page with exploits, worm based virus, bredolab attack, τα οποία θα αναλυθούν σε επόμενο κεφάλαιο.[9]

Ακόμα προσβολές προσωπικότητας, για παράδειγμα ένας χρήστης αναρτά υβριστικά σχόλια για έναν άλλο. Θέματα παιδοφιλίας και βιαστών καθώς δεν είναι λίγες οι περιπτώσεις όπου κάποιος προσπάθησε να εκμεταλλευτεί το Facebook για να προβεί σε παράνομες πράξεις.

Εικόνα 11: Υπάρχει ασφάλεια στο Facebook;

1.2 Twitter

1.2.1 Ιστορική Αναδρομή

Εικόνα 12: Logo Twitter

Το Twitter είναι και αυτό ένα online κοινωνικό δίκτυο. Επίσης χαρακτηρίζεται ως microblogging service. Το microblog διαφέρει από το τυπικό blog αφού στην πράξη είναι μικρότερο επιτρέποντας όμως στους χρήστες την ανταλλαγή μικρών κειμένων, εικόνες και βίντεο. Δημιουργήθηκε το Μάρτιο του 2006 από τους JackDorsey, Noah Glass, Evan Williams και Biz Stone. Ο Dorsey πρότεινε την ιδέα για τη χρησιμοποίηση μιας υπηρεσίας SMS για να επικοινωνεί μια μικρή ομάδα ανθρώπων. Το αρχικό κωδικό όνομα για το project ήταν twttr. Όσον αφορά την τελική ονομασία ο Dorsey συγκεκριμένα δήλωσε: «...we cam eacross the word 'Twitter', and it was just perfect. The definition was 'a short burst of inconsequential information,' and 'chirps from birds'. And that's exactly what the product was.» Το οποίο σημαίνει: σκεφτήκαμε τη λέξη Twitter η οποία είναι τέλεια. Ο ορισμός ήταν μια μικρή έκρηξη ασήμαντων πληροφοριών και τιτίβισμα πουλιών.

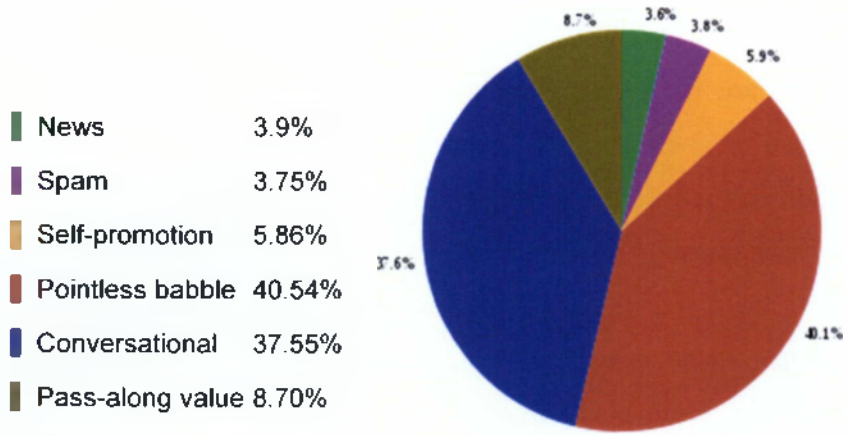
Το πρωτότυπο χρησιμοποιήθηκε αρχικά σαν υπηρεσία για τους υπαλλήλους της Odeo ενώ η ολοκληρωμένη έκδοση παρουσιάστηκε στο κοινό στις 15 Ιουλίου του 2006. Το σημείο καμπής για τη δημοτικότητα του twitter ήταν το 2007 στη διάσκεψη του Southwest Interactive. Κατά τη διάρκεια του τα tweets τριπλασιάστηκαν και από τα 20,000 έφτασαν τα 60,000 τη μέρα. Οι εντυπώσεις στη διάσκεψη ήταν ιδιαίτερα θετικές. Συγκεκριμένα ο blogger ScottBeale είπε ότι το Twitter κυριαρχεί απόλυτα. Το ίδιο δήλωσε και ο Social software researcher Danah Boyd. Το προσωπικό του Twitter κέρδισε το πρώτο βραβείο στο φεστβάλ, Web Award Prize. Στις 22 Ιανουαρίου του 2010 άρχισε να χρησιμοποιεί τη σελίδα και η NASA και συγκεκριμένα ο αστροναύτης T.J. Creamer από τον Internation Space Station.Τον Αύγουστο του ίδιου έτους η εταιρία όρισε διευθυντή τον Adam Brain ενώ το Σεπτέμβρη επανασχεδίασε το site με νέο λογότυπο. Παράλληλα τα γραφεία της εταιρίας μεταφέρθηκαν στο San Francisco.

Εικόνα 14: Παλιό Logo

Εικόνα 13: Νέο Logo

Η εξέλιξη του Twitter ήταν ραγδαία. Είχε 400,000 tweets ανά τρίμηνο το 2007. Το 2008 έφτασαν τα 100 εκατομμύρια, ενώ τα tweets εκτοξεύτηκαν το Φεβρουάριο του 2010 καθώς οι χρήστες ξεπέρασαν τα 50 εκατομμύρια tweet τη μέρα. Τέλος το Μάρτιο του 2011 έφτασαν τα 140 εκατομμύρια τη μέρα. Αποτέλεσμα το Twitter από την 22η θέση στα κοινωνικά δίκτυα κατέλαβε την Τρίτη. Στα μεγάλα γεγονότα τα tweets ανά δευτερόλεπτο έσπαγαν κάθε ρεκόρ. Για παράδειγμα στη νίκη των Los Angeles Lakers στους τελικούς του NBA το 2010 στέλνονταν 3,085 tweets το δευτερόλεπτο. [10]

Παρακάτω βλέπουμε ένα διάγραμμα με το είδος των tweet που δημοσιεύονται.



1.2.2 Παρουσίαση

Το Twitter έφερε το κάτι διαφορετικό στο κόσμο της online κοινωνικής δικτύωσης. Ο βασικός μηχανισμός της σελίδας είναι η αποστολή και προβολή μηνυμάτων που στέλνονται από διαφορετικούς χρήστες. Αυτά τα μηνύματα κειμένου ονομάζονται tweets. Το μέγεθος του κειμένου δεν ξεπερνά τους 140 χαρακτήρες και προβάλλεται στο προφίλ του χρήστη.

Η δημιουργία φιλίας με άλλα άτομα διαφέρει σε σχέση με τις υπόλοιπες σελίδες κοινωνικής δικτύωσης. Στο Twitter δεν στέλνεται αίτημα φιλίας. Ο χρήστης για να βλέπει τα μηνύματα κειμένου κάποιου φίλου, γνωστού ή κάπου διάσημου αρκεί να τον κάνει follow. Ο άλλος χρήστης δεν είναι υποχρεωμένος να σε κάνει follow και αυτός για να είναι δυνατή η προβολή των tweet του. Ταυτόχρονα όμως δεν μπορεί να έχει τη δυνατότητα να επιλέξει ποιος θα τον κάνει follow και ποιός όχι. Για παράδειγμα ένας τραγουδιστής μπορεί να έχει 1000 followers οι οποίοι βλέπουν τις αναρτήσεις του και ο ίδιος να έχει follow50 άτομα.

Μέσα από το Twitter ο χρήστης μπορεί να ενημερώσει τους followers του για κάποια είδηση, για έναν σύνδεσμο, για τον προορισμό των διακοπών του και πολλά άλλα. Και ένας καλλιτέχνης να ενημερώσει τους θαυμαστές του για την έκδοση κάποιου καινούριου τραγουδιού ή την οργάνωση κάποιας συναυλίας. Επίσης υπάρχει η επιλογή retweet η οποία δημοσιοποιεί ξανά το ίδιο tweet στο προφίλ του χρήστη που το πάτησε και το βλέπουν και οι δικοί του followers.

Επιπλέον υπάρχουν keyboard shortcuts για να κάνουν ακόμα πιο εύκολη τη περιήγηση και τη χρήση του twitter από το χρήστη. Για παράδειγμα με το γράμμα N δημιουργείται νέο tweet.

Εκτός από αυτές τις καινοτομίες η σελίδα δίνει και κάποιες επιλογές οι οποίες υπάρχουν και σε άλλους ιστότοπους κοινωνικής δικτύωσης όπως είναι η ανάρτηση φωτογραφιών και συνδέσμων μουσικής.

Πρόσφατα προστέθηκε και η επιλογή όπου Facebook και Twitter συνδέονται και τα tweets εμφανίζονται και στην προσωπική κατάσταση του χρήστη στο λογαριασμό του στο Facebook εάν αυτός το επιθυμεί.

Εικόνα 15: Twitter – follow me

Τέλος ο χρήστης μπορεί να συνδεθεί στο λογαριασμό του όπως και στις υπόλοιπες σελίδες κοινωνικής δικτύωσης. Έχοντας δηλαδή πρόσβαση σε internet μέσα από το κινητό του τηλέφωνο, από τον ηλεκτρονικό υπολογιστή και από το tablet του.

Το Twitter είναι δωρεάν και για την εγγραφή του χρήστη χρειάζεται μόνο Ονοματεπώνυμο, e-mailκαι κωδικός πρόσβασης όπως φαίνεται παρακάτω. [11]

Εικόνα 16: Αρχική σελίδα Twitter

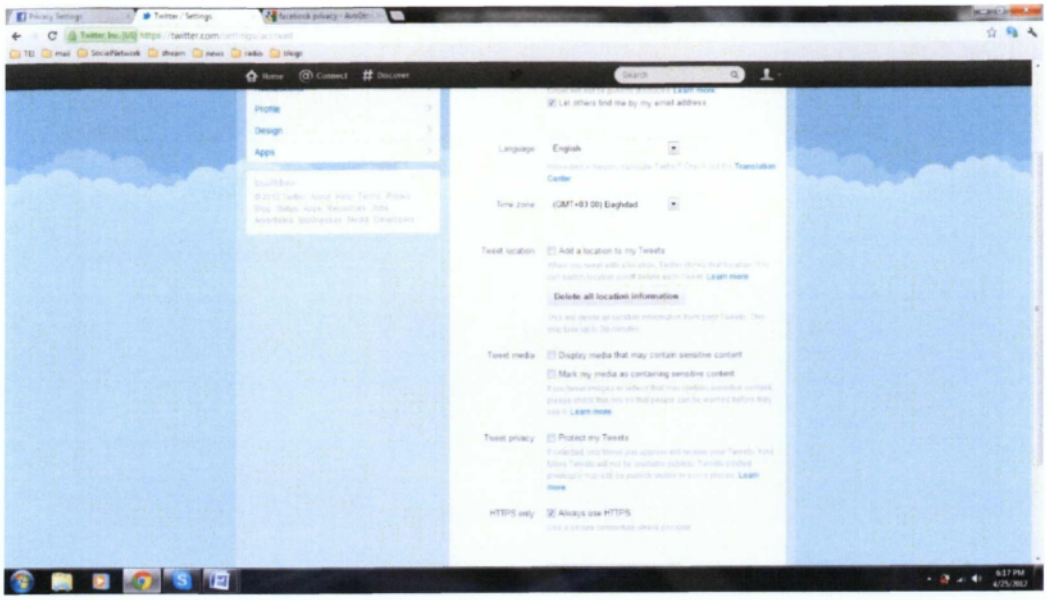
1.2.3 Τεχνικοί Όροι

Το Twitterείναι και αυτό χτισμένο σε λογισμικό ανοιχτού κώδικα από την αρχή μέχρι το τέλος. Οι μηχανικοί έχουν συμβάλλει στην απελευθέρωση πολλών εφαρμογών ανοιχτού κώδικα. Επίσης δηλώνουν ότι είναι ευγνώμονες προς την κοινότητα ανοιχτού κώδικα για τη συνεισφορά τους και οι ίδιοι θέλουν να κρατήσουν υγιή και αμοιβαία τη σχέση τους. Κάποια από τα προγράμματα και τις γλώσσες που έχουν χρησιμοποιηθεί είναι τα εξής:

Apache Cassandra, Apache Hadoop, Apache Pig, Apache Subversion, Apache Thrift, Closure, Drupal, Eclipse, Ender, Gerrit, Git, Jenkins, Python, linux, Openjdk, Ruby και άλλα. [12]

1.2.4 Πολιτική απορρήτου

Η πολιτική Απορρήτου στο Twitter είναι διαφορετική από τη στιγμή που ο χρήστης είναι περιορισμένος στη χρήση tweet και δεν μοιράζεται μεγάλο όγκο πληροφοριών. Παρόλα αυτά υπάρχει η δυνατότητα να ελέγξει ο χρήστης ορισμένες εφαρμογές. Μπορεί δηλαδή να επιλέξει αν θα είναι ορατή ή όχι η τοποθεσία από όπου αναρτήθηκε το κάθε tweet. Κάποιος χρήστης μπορεί να ανεβάσει ένα σχόλιο για έναν αγώνα ποδοσφαίρου που παρακολουθεί και να επιθυμεί και να αναρτήσει την τοποθεσία του, δηλαδή το γήπεδο. Σε κάποιο άλλο tweet δεν επιθυμεί. Ακόμα υπάρχει η επιλογή μαρκαρίσματος ενός tweet ως «ευαίσθητου» και τέλος υπάρχει η επιλογή tweet privacy όπου ο χρήστης μπορεί να επιλέξει ποιά άτομα θα είναι σε θέση να δουν την ανάρτηση των tweet.



Εικόνα 17: Twitter privacy settings

1.2.5 Επιρροές

- Η εμφάνιση του Twitter έχει επηρεάσει την ζωή μας. Αυτό συμβαίνει γιατί έχει χρησιμοποιηθεί για να ικανοποιήσει μια πληθώρα σκοπών. Για παράδειγμα έχει χρησιμοποιηθεί για την οργάνωση διαμαρτυρίας. Αυτές οι οργανώσεις διαμαρτυρίας είναι πολλές φορές γνωστές και ως «Twitter revolutions», όπως είναι για παράδειγμα η εξέγερση στην Αίγυπτο το 2011 και οι διαμαρτυρίες στην Τυνησία επίσης το 2011.
- Ακόμα έχει βοηθήσει ώστε η τηλεόραση να γίνει πιο «κοινωνική» . Το Twitter έχει χρησιμοποιηθεί επιτυχώς στο να ενθαρρύνει ανθρώπους να βλέπουν ζωντανά γεγονότα, ιδιαίτερα στην Αμερική. Τέτοια γεγονότα είναι τα Oscar, ο τελικός κυπέλου κλπ.
- Επιπλέον το Twitter είναι ένα εύκολο μέσο να κρατήσουν επαφή άτομα πολυάσχολα, που δεν προλαβαίνουν να ενημερώσουν τον κύκλο τους για το αν είναι καλά, για τυχόν προβλήματα ή κάποιο χαρμόσυνο νέο. Ένα γρήγορο tweet δίνει τη λύση.
- Ακόμη και στην πολιτική ζωή έχει επιφέρει αλλαγές αφού μέσω Twitter μπορεί να διαδοθεί ένα προεκλογικό μήνυμα, μία εκλογική καμπάνια, πολλές φορές ασκείται και αντιπολίτευση μέσω Twitter.

Γενικότερα όποιο γεγονός συμβαίνει στη ζωή κάποιου πλέον το Twitter είναι από τα πρώτα μέσα για να διαδοθεί. Είτε αυτό το γεγονός είναι το πιο ασήμαντο είτε το πιο σημαντικό. Έχει πλέον γίνει και αυτό ένα μέρος της καθημερινότητας του ανθρώπου και αυτό φαίνεται από τα 750 tweet που στέλνονται ανά δευτερόλεπτο σε όλο τον κόσμο.

Εικόνα 18: Διαφημιστικό logo Twitter

1.2.6 Προβλήματα Ασφαλείας

Όπως και στο facebook έτσι και στο twitter υπάρχουν θέματα ασφαλείας αλλά όχι σε τόσο μεγάλο βαθμό. Έχουν γίνει επιθέσεις όπως denial of service attack, worm infect και τέλος Phishing attacks. Επιπλέον μπορεί να υπάρξουν και εδώ προσβολές προσωπικότητας μέσω ανάρτησης ενός tweet, εξαπάτηση, πλαστοπροσωπία, για παράδειγμα μπορεί κάποιος να παριστάνει ότι είναι κάποιος διάσημος. Τέλος εδώ δεν συναντάμε περιπτώσεις βιασμών και παιδεραστίας.

Σε γενικές γραμμές το Twitter δεν εμφανίζει μεγάλο εύρος προβλημάτων hacking από τη στιγμή που η δράση του χρήστη στη σελίδα είναι κατά κάποιο τρόπο περιορισμένη στην αποστολή κειμένων. [13]

Εικόνα 19: Twitter και ασφάλεια

1.3 GooglePlus

1.3.1 Ιστορική Αναδρομή

Από τον κόσμο της online κοινωνικής δικτύωσης δεν μπορούσε να λείπει ο κολοσσός του ιντερνέτ, η google. Η σελίδα κοινωνικής δικτύωσης της Google ονομάζεται Googleplus και πολλές φορές εμφανίζεται και ως G+.

Εικόνα 20: Logo Googleplus

Η εταιρία βλέποντας ότι ο κόσμος στρέφεται όλο και περισσότερο στα περιβάλλοντα κοινωνικής δικτύωσης αποφάσισε να επενδύσει και εκείνη σε αυτά προσπαθώντας τα προσφέρει στο χρήστη κάτι διαφορετικό. Με λίγα λόγια η εταιρία θα έφτιαχνε μία σελίδα ακριβώς στα μέτρα του χρήστη. Η υπηρεσία έγινε προσβάσιμη σαν πρώτη φάση μόνο με πρόσκληση στις 28 Ιουνίου του 2011. Οι ήδη υπάρχοντες χρήστες μπορούσαν να στείλουν πρόσκληση μόνο σε άτομα άνω των 18. Μέσα σε δύο εβδομάδες η Google δήλωσε ότι οι χρήστες έφτασαν τους 10 εκατομμύρια και 2 εβδομάδες αργότερα τους 25 εκατομμύρια. Μέχρι το τέλος του χρόνου το Googleplus καταμετρούσε 90 εκατομμύρια χρήστες.

Στις 6 Αυγούστου του 2011 το κάθε μέλος της σελίδας είχε τη δυνατότητα να προσκαλέσει μέχρι 150 άτομα, ενώ στις 20 Σεπτεμβρίου το Googleplus άνοιξε τις πόρτες του στο κοινό χωρίς να είναι απαραίτητη πρόσκληση με την προϋπόθεση ο χρήστης να είναι άνω των 18. Άτομα μικρότερης ηλικίας δεν ήταν δυνατό να εγγραφούν. Στις 27 Οκτωβρίου ανακοινώθηκε η διαθεσιμότητα σύνδεσης στη σελίδα και από άλλες εφαρμογές και μέσα σε μία μέρα το Googleplus έγινε η πιο διάσημη δωρεάν εφαρμογή για κινητό i-phone. Το Νοέμβρη του 2011 η Google ενσωμάτωσε και άλλες υπηρεσίες στη σελίδα όπως το googlemail, και το googlemaps. Μέχρι το τέλος του χρόνου το Googleplus απαριθμούσε 400 εκατομμύρια χρήστες. Τέλος στις 26 Ιανουαρίου του 2012 ο ιστότοπος άνοιξε και για έφηβους. Όπως δήλωσε ο Vice President for Product Management, Bradley Horowitz οι χρήστες μπορούν να είναι και νεότεροι των 18 και το όριο ηλικίας έπεσε στα 13 χρόνια.

Το αρνητικό όμως στην ιστορία του Googleplus μέχρι σήμερα είναι ότι σύμφωνα με δηλώσεις του Todd Wasserman στις 28 Φεβρουαρίου του 2012 οι χρήστες ξοδεύουν κατά μέσο όρο μόλις 3,3 λεπτά το μήνα στην υπηρεσία, ενώ αντίστοιχα στο Facebook για παράδειγμα οι χρήστες αναλώνονται κατά μέσο όρο 7,5 ώρες το μήνα.[πηγή: Wikipedia]

Για το λόγο αυτό η Google έχοντας πάντα ως στόχο την δημιουργία μιας ενιαίας «κοινωνικής» εμπειρίας σε ολόκληρο το δίκτυο των υπηρεσιών της, αναγκάστηκε να προβεί

σε μεγάλες αλλαγές, με πλήρως ανανεωμένο περιβάλλον χρήσης. Με λίγα λόγια πρόκειται για έναν πλήρη επανασχεδιασμό που στόχο έχει την πιο απλή χρήση αλλά και την καλύτερη αισθητική της υπηρεσίας. Ακόμα προχώρησε σε αλλαγές στην πολιτική απορρήτου και στους όρους παροχής υπηρεσιών. Ένας κύριος στόχος είναι και η ενθάρρυνση των χρηστών σε συζητήσεις αφού σε αυτόν τον τομέα όπως αναφέραμε η Google χωλαίνει. Γι αυτό το λόγο σημαντικό ρόλο παίζει η εφαρμογή Hangouts, που ήταν από την αρχή σημαντική λειτουργία της υπηρεσίας. Στη νέα έκδοση αποκτά δική του σελίδα, έτσι διευκολύνεται η διεξαγωγή κλήσεων και ενθαρρύνεται και η διεξαγωγή συνομιλιών. [14]

Παρακάτω παρουσιάζουμε τη νέα μορφή του προφίλ:

Εικόνα21: Ένα προφίλ στο Googleplus

1.3.2 Παρουσίαση

Ο ShimritBen-Yair, product manager δήλωσε: «On Facebook I overshare. On Twitter, I undershare. If Google hits that spot in the middle, we can revolutionize social interaction». Οι λειτουργίες δηλαδή του googleplus θα φέρουν την επανάσταση στον χώρο των σελίδων κοινωνικής δικτύωσης. Πώς όμως θα κατορθώσει να το επιτύχει αυτό η google;

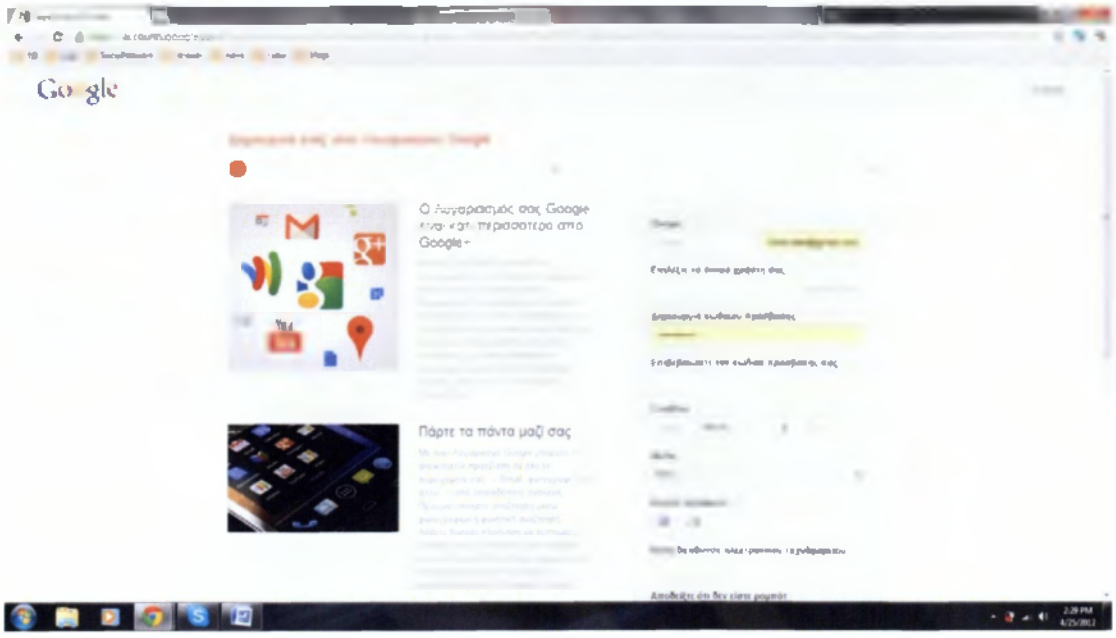
Αρχικά, προσφέρει στο χρήστη ότι και τα υπόλοιπα social networks. Τη δημιουργία δηλαδή ενός προσωπικού προφίλ όπου ο χρήστης μπορεί να ανεβάσει φωτογραφίες, video, προσωπικές πληροφορίες, να κάνει φιλίες, να έρθει σε επικοινωνία με άλλους και να διασκεδάσει.

Έδωσε όμως έμφαση στη δημιουργία κύκλων για την οργάνωση της λίστας φίλων σε ομάδες. Οι ομάδες αυτές ονομάζονται circles. Ο χρήστης χωρίζει τις επαφές του σε κύκλους ατόμων τους οποίους μπορεί να επιλέξει αν επιθυμεί να είναι ορατοί από τρίτους. Ο διαχωρισμός των επαφών γίνεται με «draganddrop» της επαφής μέσα στον κύκλο. Το όνομα και η κατηγορία του κάθε κύκλου δίνονται από τον χρήστη. Για παράδειγμα μπορεί οι κύκλοι να διαχωριστούν ως εξής. Οικογένεια, φίλοι, δικτυακοί φίλοι κλπ. Μπορεί σε έναν κύκλο να προστεθεί και άτομο το οποίο δεν διαθέτει googleplus με την προσθήκη του e-mail του, το οποίο θα λαμβάνει με e-mail τα νέα και το ανέβασμα φωτογραφιών. Επίσης ο χρήστης επιλέγει εάν οι φωτογραφίες του για παράδειγμα ή κάποια ανάρτηση του θα είναι ορατή σε όλους ή σε συγκεκριμένους κύκλους. Τέλος ο χρήστης μπορεί να κάνει follow κάποιον άλλο και να τον προσθέσει στον κύκλο following χωρίς ο άλλος χρήστης να υποχρεούται να τον κάνει φίλο. Ένας διάσημος για παράδειγμα έχει τη δυνατότητα να έχει όσους followers επιθυμεί χωρίς να υποχρεούται να τους έχει στη λίστα φίλων του.

Μία άλλη εφαρμογή της υπηρεσίας που βασίστηκε η Google είναι τα hangouts. Τα hangouts είναι μέρη όπου μπορεί να δημιουργηθεί ατομική ή ομαδική βιντεοκλήση. Πρόσφατα η εταιρία δημιούργησε ξεχωριστή σελίδα για αυτή την εφαρμογή. Επιπλέον ο χρήστης μπορεί να διασκεδάσει επιλέγοντας κάποιο από τα παιχνίδια που προσφέρει η υπηρεσία τα οποία βέβαια είναι ακόμα μικρά σε αριθμό. Ακόμα, ενσωματωμένα στο Googleplus βρίσκονται και άλλες υπηρεσίες της Google όπως το googlemail και το googlemaps.

Τέλος όπως και στα υπόλοιπα social network η σύνδεση μπορεί να γίνει και από κινητό τηλέφωνο, ηλεκτρονικό υπολογιστή και tablet με σύνδεση στο internet. [15]

Για να δημιουργήσει κάποιος λογαριασμό στην υπηρεσία τα μόνα που απαιτούνται είναι: ονοματεπώνυμο, φύλλο, ηλικία καθώς και ένα e-mail.



Εικόνα 22: Αρχική σελίδα Googleplus

1.3.3 Τεχνικοί Όροι

Για τη δημιουργία του Googleplus έχουν χρησιμοποιηθεί κυρίως Java και javascript, ενώ για τα hangouts έχει χρησιμοποιηθεί ένας client-server.

Το Google+ χρησιμοποίει Java με Guice όσον αφορά τους server και παρατεταμένη χρήση JavaScript και Closure όσον αφορά τον παραλήπτη. Το Closure είναι ένα σετ εργαλείων για προγραμματιστές JavaScript που θέλουν να γράψουν πλούσιες διαδικτυακές εφαρμογές και χρησιμοποιείται από την Google για το Gmail, τους χάρτες και έγγραφα. Είναι ενδιαφέρον ότι η Google δεν επέλεξε να χρησιμοποιήσει το GWT, που είναι σχεδιασμένο για Wave και Adwords, μια τεχνολογία που στοχεύει περισσότερο προγραμματιστές Java αντί για JavaScript. Το HTML5 HistoryAPI έχει προστεθεί για να «διατηρεί όμορφα URL παρότι είναι μια εφαρμογή AJAX (παλιότεροι περιηγητές δεν την υποστηρίζουν)», και το περίγραμμα Closure είναι συχνά μεταφρασμένο στον server έτσι ώστε "η σελίδα να μεταφράζεται πριν το οποιοδήποτε JavaScript φορτώσει. Ύστερα το JavaScript βρίσκει τα σωστά DOM nodes και προσκολλάει τους διαχειριστές συμβάντων κτλ για να το κάνει αποκριτικό."

Το φανταστικό μέρος των Closure περιγραμμάτων είναι ότι μπορούν να διαβαστούν και από Java και JavaScript. Έτσι μπορεί να χρησιμοποιηθεί Java στην μεριά των server για να γυρίσουν τα περιγράμματα σε HTML, αλλά μπορεί να γίνει το ίδιο σε JavaScript στην μεριά του παραλήπτη για δυναμική μετάφραση. Για παράδειγμα, αν γραφτεί ένα προφίλ κατευθείαν στο URL, θα μεταφραστεί στην μεριά των server, αλλά αν απλά περιηγηθεί

κάποιος σε ένα προφίλ από μια άλλη σελίδα, θα γίνει με AJAX και θα μεταφραστεί στην μεριά του παραλήπτη χρησιμοποιώντας το ίδιο περίγραμμα.

Το πίσω μέρος είναι χτισμένο σε BigTable και Colossus, της το σύστημα της Google που χρησιμοποιείται για αναζήτηση σε πραγματικό χρόνο.

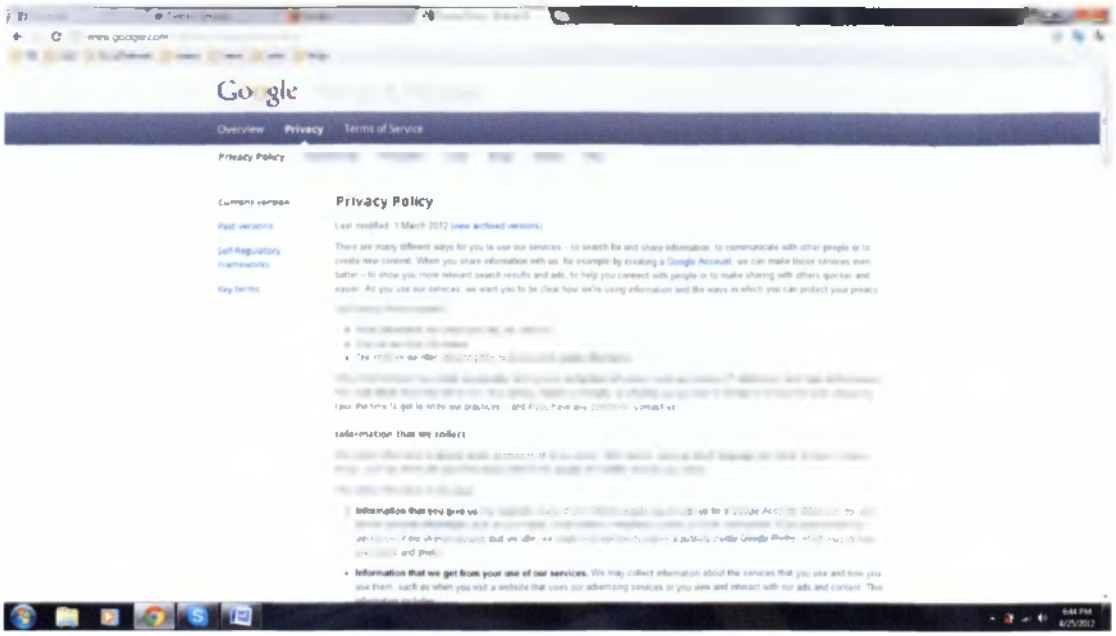
Το Google+ Hangouts είναι μια άμεσα συνδεμένη πλατφόρμα cloud βίντεο συνάντησης βασισμένη σε XMPP, Jingle. TRP, ICE, STUN, SRTP, το οποίο έχει πάρει μια τελείως διαφορετική προσέγγιση από το Skype που χρησιμοποιεί δίκτυο P2P. Το Hangouts είναι μια τεχνολογία παραλήπτη-server/cloud που βασίζεται βαριά στον πυλώνα της Google. Δεν υπάρχουν στοιχεία για το πόσους πόρους χρησιμοποιεί το Hangouts αλλά αναμένεται να είναι πολλοί. Και όλα αυτά γίνονται για να παρέχεται χαμηλό διάστημα ερεθισμού-αντίδρασης για ευχάριστη επικοινωνία μεταξύ των χρηστών.

Το Hangouts χρειάζεται το ίδιο plug-in όπως και το GoogleTalk αλλά σκοπεύουν να το μεταφέρουν σε WebRTC, ένα πλαίσιο εργασίας βασισμένο σε JavaScript για επικοινωνία με βίντεο, που είναι opensource και υποστηρίζεται από την Google, Mozilla και Opera. Όταν το WebRTC ολοκληρωθεί στο Chrome, δεν θα υπάρχει ανάγκη να ληφθεί το plug-in για Hangouts αν τρέχει από FireFox, Opera ή Chrome. Τότε, το Hangouts θα χρησιμοποιεί το VP8 codec που παρέχεται με το WebRTC αντί για το H.264 που χρησιμοποιείται τώρα. [16]

1.3.4 Πολιτική Απορρήτου

Το Googleplus για να μπορέσει και αυτό να ικανοποιήσει τις απαιτήσεις του κόσμου, δημιούργησε μία σελίδα από όπου ο χρήστης μπορεί να προβεί σε ρυθμίσεις για την ασφάλεια των προσωπικών του δεδομένων, το profile and privacy.

Από εκεί ο χρήστης ελέγχει τα πάντα. Αρχικά έχει τη δυνατότητα να κάνει το προφίλ του αόρατο στο κοινό, ή να επιλέξει ποιες πληροφορίες του θα είναι ορατές στους υπόλοιπους. Επίσης, το τι μοιράζεται με τους κύκλους του, όπως φωτογραφίες, συνδέσμους, αναρτήσεις βίντεο κλπ. Ακόμα και ποια άτομα από τους κύκλους του θα φαίνονται στους υπόλοιπους. Επιπλέον ο χρήστης μπορεί να χρησιμοποιήσει το dashboard για να δει και να τροποποιήσει πληροφορίες που έχουν αποθηκευτεί στο google λογαριασμό του. Τέλος στο privacy center υπάρχουν λεπτομέρειες για την πολιτική απορρήτου της εταιρίας.



Εικόνα 23: Privacy settings Googleplus

1.3.5 Επιρροές

- Το Googleplus δεν έχει κλείσει ακόμα ένα χρόνο από τη δημιουργία του και έχει φτάσει τους 200 εκατομμύρια χρήστες πράγμα που υποδηλώνει ότι η δημιουργία του έχει επηρεάσει τον κόσμο.
- Αρχικά οι καινοτομίες που προσφέρει όπως τα hangout, οι ατομικές και ομαδικές βιντεοκλήσεις έδωσαν άλλο στίγμα στη σελίδα και προσέφεραν στο χρήστη τη δυνατότητα για πλήρη επικοινωνία χωρίς τη χρήση κάπου προγράμματος. Αποτέλεσμα, και άλλα social networks όπως το Facebook πρόσθεσαν τη συγκεκριμένη εφαρμογή στις υπηρεσίες τους.
- Ακόμα με τις δηλώσεις της εταιρίας για την παροχή μεγαλύτερης ασφάλειας προσωπικών δεδομένων οδήγησε πολλούς χρήστες στη σκέψη ότι πολλές σελίδες δεν προσφέρουν τη μέγιστη ασφάλεια. Αποτέλεσμα, ο προβληματισμός για την έκθεση των προσωπικών τους δεδομένων.
- Όπως και οι υπόλοιποι ιστότοποι κοινωνικής δικτύωσης έτσι και το Googleplus έχει προσφέρει τη δυνατότητα στους χρήστες να έρχονται σε επαφή παρά τις μεγάλες γεωγραφικές αποστάσεις, εταιρίες μπορούν να προβάλλουν τα προϊόντα τους μέσω των προφίλ τους και συμβάλλει στην ανάπτυξη και εξέλιξη του social networking.

Ο Amit Singhal, Google search engineer δήλωσε: «*We're still just scratching the surface of marrying human relationships with information. There's a huge opportunity which someone*

else will fill — or we will fill.», δηλαδή ότι προσπαθούν να παντρέψουν τις ανθρώπινες σχέσεις με την πληροφορία. Μια ευκαιρία που τους έχει δοθεί για να το κάνουν, αλλιώς θα το κάνει κάποιος άλλος. Ενώ ο Vic Gundotra, senior vice president of social for Google ανέφερε: «*We needed a code name that captured the fact that either there was a great opportunity to sail to new horizons and new things, or that we were going to drown by this wave*». Η Google με λίγα λόγια προσπαθεί να ανοίξει νέους ορίζοντες στον κόσμο και να καταφέρει αυτά που δεν κατάφεραν άλλοι. [17]

Εικόνα 24: Το Googleplus θα κατακτήσει πολλούς χρήστες ανά τον κόσμο

1.3.6 Προβλήματα Ασφαλείας

Το Googleplus είναι ένα πρόσφατο σύστημα και έτσι είναι δύσκολο να είναι κανείς αυστηρός στο έπακρο με την κριτική του. Όμως αντιμετωπίζονται και εδώ αρκετά θέματα όσον αφορά την ασφάλεια των δεδομένων του χρήστη από την ίδια τη σελίδα αλλά και από επιθέσεις τρίτων.

Όσον αφορά τη σελίδα για παράδειγμα, έχει επιτρέψει την πρόσβαση σε φωτογραφίες που έχει ανεβάσει ο χρήστης να είναι ορατές από οποιονδήποτε ο οποίος ξέρει την ακριβή URL διεύθυνση του αρχείου και υπάρχουν μέθοδοι hacking όπου μπορούν να γνωστοποιήσουν σε τρίτους αυτά τα URL. Υπάρχουν ευάλωτα σημεία στους server της google που έχουν εντοπιστεί και από όπου γίνεται υποκλοπή των αρχείων εικόνων. Ακόμα υπάρχει αλγόριθμος ο οποίος «μαντεύει» τις διευθύνσεις, και τέλος μία επίθεση που ονομάζεται Man in the Middle με τη βοήθεια της οποίος αποσπώνται οι διευθύνσεις κατά τη διάρκεια προβολής των εικόνων από τους χρήστες.[18]

Συναντά κανείς ακόμα Internal threats, phishing attacks, worm based virus και άλλα. Δεν έχουν γίνει αναφορές ακόμα για περιπτώσεις παιδεραστίας και βιασμών και κανείς δεν το εύχεται, αλλά ο ιστότοπος είναι καινούριος και ο κόσμος δεν αναλώνεται και σε μεγάλο αριθμό ωρών.[πηγή:Thehackernews.com]

Εικόνα 25: Ασφάλεια στο Googleplus

Κεφάλαιο 2:Εξειδίκευση Προβλημάτων

Από τη στιγμή που οι σελίδες κοινωνικής δικτύωσης έγιναν κομμάτι ζωής πολλών ανθρώπων, τράβηξαν και την προσοχή πολλών κακόβουλων επιθέσεων από τρίτους με σκοπό την παραβίαση προσωπικών δεδομένων. Υπάρχει μια πληθώρα μεθόδων για την υποκλοπή δεδομένων μέσα από το προφίλ ενός χρήστη. Τέτοιες είναι τα spam. Το spam διαδίδεται μέσω e-mail και εξαπλώνεται στο κοινωνικό δίκτυο μέσα από τη λίστα φίλων του χρήστη ο οποίος το δέχεται πρώτος. Ακόμα τα thirdpartyapplications. Τα application είναι ένας μεγάλος τομέας μέσα από τον οποίο οι επιτιθέμενοι αποκτούν πρόσβαση στο κοινωνικό δίκτυο και κατ' επέκταση στα προσωπικά δεδομένα χρηστών. Επίσης τα worms, τα οποία αναπαράγουν τους εαυτούς τους και χρησιμοποιούνται στην απόσπαση προσωπικών πληροφοριών όπως κωδικοί και αριθμοί λογαριασμών τραπεζών. Επιπλέον το XXS. Ο κώδικας της σελίδας εμβάλλει στα κοινωνικά δίκτυα, κλέβει cookies και αναγκάζει το χρήστη να κατεβάσει malware. Ακόμα τα plug-ins τα οποία εγκαθίστανται μέσω εφαρμογών στα κοινωνικά δίκτυα όπως στο flash και στο Silverlight. Τα plug-in είναι απειλή για προσωπικές πληροφορίες. Τέλος τα phishing attacks. Σε αυτές τις επιθέσεις ο επιτιθέμενος παριστάνει τον απλό χρήστη και στέλνει αιτήματα σε άλλους χρήστες χρησιμοποιώντας URL το οποίο του δίνει πρόσβαση σε προσωπικές πληροφορίες μετά την αποδοχή του αιτήματος από τον άλλο χρήστη. [πηγή: SecurityAnalysisofSocialNetworks, GRADUATEPROJECTREPORT]

Ακόμα συναντάμε, όπως και στη ζωή έξω από τον κόσμο του διαδικτύου, προσβολές προσωπικότητας καθώς και περιπτώσεις βιαστών και παιδόφιλων. Στο κεφάλαιο που ακολουθεί θα αναλύσουμε και θα δώσουμε παραδείγματα από τέτοιες επιθέσεις, σε σελίδες κοινωνικής δικτύωσης.

2.1 Facebook

2.1.1 hacking

Το Facebook είναι από τα πιο δημοφιλή social networking web sites με ένα τεράστιο πλήθος χρηστών. Οι χρήστες αυτοί, στον κόσμο της σελίδας μοιράζονται πολλά από τα προσωπικά τους δεδομένα δίνοντας έτσι έναυσμα σε

Εικόνα 26: Facebook phishing,scams,hacking

hackers για κακόβουλες επιθέσεις.

Ένας τρόπος υποκλοπής προσωπικών δεδομένων είναι το: Most Hilarious Video Attack. Είναι μία από τις πρόσφατες επιθέσεις η οποία προσελκύει τους χρήστες του Facebook να δουν το πιο αστείο βίντεο. Μετά το κλικ στο συγκεκριμένο σύνδεσμο ο χρήστης οδηγείται σε μία ψεύτικη σελίδα login του Facebook μέσα από την οποία ο επιτιθέμενος μπορεί να αποσπάσει τα στοιχεία login του χρήστη. Έπειτα μπορεί να ανακατευθύνει το χρήστη σε μια άλλη σελίδα ενημερώνοντάς τον ότι είναι ο νικητής ενός κινητού και να τον παρακινήσει να δώσει προσωπικά του στοιχεία όπως διεύθυνση και τηλέφωνο. [πηγή: websense]

Μία ακόμα συνηθισμένη επίθεση στο Facebook είναι το likejacking. Το likejacking είναι μια επίθεση η οποία προσπαθεί να μπερδέψει το χρήστη παροτρύνοντάς τον να κάνει like σε ένα ενδιαφέροντα σύνδεσμο με μήνυμα όπως για παράδειγμα: «δείτε τι έκανε αυτός ο μαθητής και τον έδιωξαν από το σχολείο». Εάν ο χρήστης κλικάρει το μήνυμα, το worm τον μεταφέρει σε μια άλλη σελίδα ενώ το μήνυμα που είχε διαβάσει μεταφέρεται στη σελίδα του προφίλ του, από όπου μπορούν να το δουν και να το κλικάρουν και οι φίλοι του. [πηγή: Elinor Mills, sophos].

Στα phishing attacks ο επιτιθέμενος διαδίδει e-mail με διάφορα θέματα. Ο ανυποψίαστος χρήστης ανοίγοντάς το θα οδηγηθεί σε μια ψεύτικη σελίδα login σελίδα του Facebook. Εάν εισάγει τα στοιχεία του, αυτά αυτόματα αποστέλλονται στον επιτιθέμενο.

Οι επιθέσεις βασισμένες σε worms δρουν παρόμοια. Βασιζόμενοι στην απροσεξία του χρήστη διαδίδουν στο Facebook προσελκυστικά μηνύματα. Ο σύνδεσμος σε κατευθύνει στο Youtube και σου προτείνει να κατεβάσεις ένα flash player, προφανώς ψεύτικο. Μια

κακόβουλη εγκατάσταση ξεκινά η οποία αποσπά προσωπικά στοιχεία, όπως η φωτογραφία προφίλ του χρήστη. [πηγή:MichaelArrington]

BredolabAttack. Άλλος ένας τρόπος επίθεσης χρήστη του Facebook. Η συγκεκριμένη επίθεση ενημερώνει το χρήστη με κάποιο μήνυμα οδηγώντας τον στην εγκατάσταση κακόβουλων προγραμμάτων στη μορφή zip. Ο επιτιθέμενος αποκτά πλήρη πρόσβαση στον υπολογιστή του χρήστη.

Ο χρήστης στο Facebook χρησιμοποιεί μια πληθώρα εφαρμογών με τους φίλους του και δε διστάζει να χρησιμοποιήσει προσωπικά του δεδομένα όπως φωτογραφίες έχοντας στο μυαλό του ότι ένα antivirus ή ένα firewall τον προστατεύουν. Σε πείραμα που έγινε από καθηγητές του Πανεπιστημίου Πειραιά, Κωνσταντίνου Πατσάκη, Αλέξανδρου Ασθενίδη και Αβραάμ Χατζηδημητρίου, το οποίο δημοσιεύτηκε με τίτλο: «Social Networks as an attack platform: Facebook Case Study» δημιουργήθηκε μία κακόβουλη εφαρμογή. Στην εφαρμογή αυτή δημιουργήθηκε ένα απλό slide-show εικόνων από εικόνες αστείων σκυλιών, ένα τέλειο προφίλ επίθεσης και την συλλογή πληροφοριών υπό την άγνοια του χρήστη. Επισημάνθηκε ότι η εφαρμογή είναι για τεστ, παρόλα αυτά το Facebook δεν έλεγξε το περιεχόμενο και η εφαρμογή αναρτήθηκε στην κύρια λίστα εφαρμογών. Η συλλογή πληροφοριών στέλνονταν σε e-mail. Για τις ανάγκες τις εφαρμογής χρησιμοποιήθηκαν FBML, FBJS, PHP και javascript. Αξίζει να σημειωθεί ότι οι FBML και FBJS παρέχονται από τη σελίδα για την διευκόλυνση στη δημιουργία εφαρμογών. Παρακάτω παρουσιάζεται ένα e-mail που στάλθηκε μετά την επίσκεψη κάποιου στην εφαρμογή.

```
| Date : 2008..09..29 1 7 : 2 2 : 0 2 | IP :

? . ? . ? . ? | Browser : Mo z i l l a / 5 . 0

(Windows ; U; Windows NT 5 . 1 ; en ;

rv : 1 . 9 . 0 . 3 ) Gecko /2008092417

F i r e f o x / 3 . 0 . 3 | P o r t s : ( 1 : open ),

( 7 : open ), ( 9 : open ), ( 2 1 : open ),

( 1 1 0 : open ), ( 2 3 : open ), ( 2 : c l o s e d ),

( 3 : c l o s e d ), ( 4 : c l o s e d ), ( 5 : c l o s e d ),

( 6 : c l o s e d ), ( 8 : c l o s e d ), ( 1 0 : c l o s e d ),
```

```
( 4 4 5 : c l o s e d ), ( 1 7 2 3 : c l o s e d ), ( 3 3 8 9 : c l o
s e d ),

( 5 9 0 0 : c l o s e d ), ( 8 0 : c l o s e d ), |

Loc a l Scanning : ( 1 : open ), ( 7 : open ),

( 9 : open ), ( 2 1 : open ), ( 1 1 0 : open ), ( 2 3 : open ),

( 2 : c l o s e d ), ( 3 : c l o s e d ), ( 4 : c l o s e d ),

( 5 : c l o s e d ), ( 6 : c l o s e d ), ( 8 : c l o s e d ),

( 1 0 : c l o s e d ), ( 4 4 5 : c l o s e d ), ( 1 7 2 3 : c l o s e
d ),

( 3 3 8 9 : c l o s e d ), ( 5 9 0 0 : c l o s e d ), ( 8 0 : c l o s
e d )
```

Έτσι είναι ορατές στο hacker τα port του χρήστη τα οποία είναι ανοιχτά και στα οποία μπορεί να επιτεθεί ο hacker.

Ένας χρήστης για να αποδείξει τα κενά ασφαλείας στο Facebook βρήκε τον τρόπο και δημοσίευσε φωτογραφίες του ιδρυτή του, Mark Zuckerberg. Σύμφωνα με αναφορές σε διεθνή ΜΜΕ, στις φωτογραφίες των μελών στις οποίες θα μπορούσε κάποιος να αποκτήσει πρόσβαση, συμπεριλαμβάνονται και όσες είναι κρυμμένες ή μη δημόσιες! Αυτό μπορεί να γίνει με τη χρήση του χαρακτηριστικού «Αναφορά Περιεχομένου» του Facebook, το οποίο χρησιμοποιείται για να κρατήσει το site κοινωνικής δικτύωσης καθαρό και να αφαιρούνται τυχόν επιβλαβείς εικόνες, μηνύματα ή γενικότερα ακατάλληλο περιεχόμενο. Σε πρώτο στάδιο, χρησιμοποιείται η επιλογή «αναφορά / μπλοκ» του λογαριασμού στο Facebook. Από τις επιλογές που εμφανίζονται στη συνέχεια, επιλέγεται το «Ανάρμοστη φωτογραφία του προφίλ». Στη συνέχεια ζητείται από το Facebook ο προσδιορισμός της ακατάλληλης φωτογραφίας. Επιλέγοντας την αναφορά φωτογραφίας, το σύστημα συνεχίζει προσκαλώντας τον κακόβουλο χρήστη να προσθέσει και επιπλέον φωτογραφίες. Αν ο ίδιος επιλέξει να το κάνει, θα του επιτραπεί πρόσβαση σε όλες τις φωτογραφίες του θύματος, συμπεριλαμβανομένων και εκείνων που έχουν επισημανθεί ως ιδιωτικές. [πηγή:

Εικόνα 27: Facebook phishing

techit.gr 07/12/2011]

Σε άρθρο της η εφημερίδα Καθημερινή δημοσίευσε ότι σύμφωνα με έρευνα της εταιρίας ασφαλείας Sophos καθημερινά παραβιάζονται 600,000 λογαριασμοί χρηστών. Οι λογαριασμοί παραβιάζονται από hacker που θέλουν είτε να υποκλέψουν τα προσωπικά δεδομένα των χρηστών είτε να στείλουν αμέτρητα διαφημιστικά μηνύματα. Το γεγονός αυτό, το οποίο το επιβεβαίωσε και το ίδιο το Facebook με ανάρτηση σε επίσημο blog, ανάγκασε τους υπεύθυνους του δημοφιλούς ιστοχώρου κοινωνικής δικτύωσης να δημιουργήσουν δύο νέες υπηρεσίες προστασίας, τα Trusted Friends και το App Passwords. Έτσι, με το Trusted Friends, κάθε χρήστης μπορεί να ορίσει 3-5 έμπιστους «φίλους» του, στους οποίους θα σταλεί ένας κωδικός που θα ξεμπλοκάρει τον λογαριασμό του στην περίπτωση που έχει ξεχάσει τον κωδικό του. Επίσης, με το App Passwords, μπορεί να καθορίσει ξεχωριστούς κωδικούς για να μπαίνει σε εφαρμογές τρίτων εταιριών / προγραμματιστών.[πηγή: εφημερίδα Καθημερινή 09/11/2011)

Ένα σοβαρό ακόμα πρόβλημα που αντιμετωπίζει η σελίδα είναι τα scams τα οποία δίνουν και παίρνουν. Τα scams είναι παραπλανητικά μηνύματα που μπορούν να ξεγελάσουν και τους πιο έμπειρους χρήστες. Σύμφωνα με άρθρο της Dailymail ένα ευφυέστατο scam απειλεί να διαγράψει το λογαριασμό χρήστη στο Facebook. Η εν λόγω απάτη μιμείται τις συνήθεις διαδικασίες ασφαλείας που ακολουθεί η Facebook σε περίπτωση που υποπέσει στην αντίληψή της ανάρμοστη συμπεριφορά από μέρους κάποιου χρήστη. Υπό μορφή e-mail, κατηγορεί το χρήστη ότι έχει παραβεί τους "Όρους Χρήσης" του κοινωνικού δικτύου, προσβάλλοντας ή παρενοχλώντας άλλους χρήστες, φροντίζοντας μάλιστα να τον ενημερώσει ότι ο λογαριασμός του θα διαγραφεί μέσα στις επόμενες 24 ώρες. Σε εκείνο το σημείο, το e-mail μεταφέρει το χρήστη σε μια υποτιθέμενη σελίδα "Απενεργοποίησης Λογαριασμού", η οποία ζητά προσωπικές λεπτομέρειες για τον ίδιο, καθώς και πληροφορίες της πιστωτικής κάρτας του για να γίνει η απαραίτητη εξακρίβωση. Πέρα από την υποκλοπή προσωπικών δεδομένων, μόλις κάποιος πέσει στην παγίδα, το e-mail αποστέλλεται αυτομάτως στους φίλους του, με αποτέλεσμα να εξαπλώνεται ανεξέλεγκτα. Φροντίζετε, λοιπόν, να είστε πολύ προσεκτικοί και ειδικότερα σε τέτοιου είδους ασυνήθιστα email... [πηγή: techgear,dailymail 25/06/2011]

Ένα ακόμα scam τάραξε τον κόσμο του Facebook μετά το θάνατο του ιδρυτή της Apple, Steve Jobs. Την ώρα που ο κόσμος θρηνούσε το θάνατό του, υπήρξαν κάποιοι επιτήδειοι οι οποίοι θέλησαν να το εκμεταλλευτούν. Όπως ενημέρωσε η ιστοσελίδα Nakedsecurity κυκλοφόρησε στο Facebook ένα παραπλανητικό μήνυμα το οποίο παρότρυνε τους

ανυποψίαστους χρήστες να πατήσουν σύνδεσμο για να κερδίσουν 50 i-pads. Μια υποτιθέμενη προσφορά της Apple προς τιμή του θανάτου του ιδρυτή της. Περισσότεροι από 15000 χρήστες εξαπατήθηκαν και «πάτησαν» το συγκεκριμένο σύνδεσμο, ο οποίος οδηγούσε σε ερωτηματολόγιο για τη συλλογή προσωπικών δεδομένων των χρηστών καθώς και σε προώθηση άλλων κακόβουλων ιστοσελίδων.[πηγή: techgear 06/10/2011]

Στις 15 Νοεμβρίου 2011 ένα ασυνήθιστο φαινόμενο παρατηρήθηκε για μερικές μέρες στο Facebook με ολοένα και περισσότερους χρήστες να διαμαρτύρονται για την εμφάνιση πορνό στο προφίλ τους. Οι αντιδράσεις εξαπλώθηκαν και σε άλλες σελίδες κοινωνικής δικτύωσης όπως στο Twitter όπου χιλιάδες χρήστες έγραψαν σχόλια του τύπου: «Το Facebook έγινε και επίσημα ιστοσελίδα πορνό». Πέρα από τις πονηρές εικόνες ορισμένοι χρήστες έκαναν λόγο και για αποκρουστικές εγκληματικές εικόνες. Η όλη κατάσταση οδήγησε πολλούς χρήστες στην απενεργοποίηση των λογαριασμών τους αρνούμενοι να επιστρέψουν μέχρι τη λύση του ζητήματος. Ας μην ξεχνάμε ότι και πολλοί ανήλικοι χρησιμοποιούν τη συγκεκριμένη σελίδα. Πολλοί κατηγόρησαν για το γεγονός τη δημοφιλή ομάδα Anonymous αφού η δημοφιλής ομάδα hacker είχε δηλώσει 10 μέρες πριν το γεγονός ότι θα καταστρέψει το Facebook. Έκτοτε όμως δεν ασχολήθηκε ξανά με το κοινωνικό δίκτυο.[πηγή: techgear, neowin 15/11/2011)

Εκτός όμως από τις επιθέσεις από τρίτους κατηγορείται και το ίδιο το Facebook για παραβίαση προσωπικών δεδομένων. Όπως ισχυρίζεται ο δημοφιλής επιχειρηματίας και hacker Nick Cubrilovic, το Facebook συνεχίζει να παρακολουθεί το χρήστη ακόμα και μετά την αποσύνδεσή του από τη σελίδα. Συγκεκριμένα ανακάλυψε ότι το Facebook αντί να διαγράφει τα cookies κατά την αποσύνδεση του χρήστη, τα διατηρεί με κάποιες μετατροπές. Έτσι οι πληροφορίες του λογαριασμού συνεχίζουν να βρίσκονται στα cookies κάτι που σημαίνει ότι κάθε φορά που ο χρήστης επισκέπτεται μια σελίδα οι προσωπικές του πληροφορίες στέλνονται πίσω στο Facebook.

```
Cookie:
datr=tdnZTOt21HOTpRkRzS-6tjKP;
openid_p=101045999;
act=1311234574586%2F0;
L=2;
locale=en_US;
lu=ggIZeheqTLbjoZ5Wgg;
lsd=IkRq1;
reg_fb_gate=http%3A%2F
%2Fwww.facebook.com%2Findex.php%3Flh%3Dbf0ed2e54fb
wZ3n_VN7xw1BvUw;
reg_fb_ref=http%3A%2F
%2Fwww.facebook.com%2Findex.php%3Flh%3Dbf0ed2e54fb
_VN7xw1BvUw
```

Εικόνα 28: cookie που κρατά συνδεδεμένους χρήστες - Facebook

Αν κάτι τέτοιο αποδειχθεί σωστό, μιλάμε για σοβαρή παραβίαση της ιδιωτικής ζωής των χρηστών. Αρκετοί χρήστες έχουν ήδη ξεσηκωθεί. Το Facebook υπερασπιζόμενο δήλωσε ότι τα δεδομένα που συλλέγονται από τα cookies έχουν να κάνουν καθαρά με την προστασία από κακόβουλες ενέργειες όπως το spamming και το phishing και σε καμία περίπτωση για διαφημιστικούς σκοπούς.[πηγή: techgear 26/09/2011]

Ακόμα μια είδηση ήρθε να ταράξει τα νερά. Όλοι ξέραμε ότι το Facebook αποθηκεύει προσωπικά μας δεδομένα, κανείς δεν ήξερε όμως το πόσα. Όπως αποκάλυψε η σελίδα Europe v Facebook το δημοφιλές κοινωνικό δίκτυο αποθηκεύει μέχρι 880 σελίδες πληροφοριών για κάθε προφίλ χρήστη. Πέρα λοιπόν από τις πληροφορίες του ονόματος, ημερομηνίας γέννησης κλπ η σελίδα καταχωρεί λίγο πολύ τα πάντα. Events που έχουμε παρευρεθεί, άτομα που έχουμε διαγράψει, ακόμα και τις πολιτικές μας προτιμήσεις. [19]

Εικόνα 29: Τι γνωρίζει το Facebook για εμάς

Μετά τα συνεχή παράπονα των χρηστών του Facebook, η εταιρία αποφάσισε να μιλήσει επίσημα στη USAtoday δια στόματος του μηχανικού Arturo Bejar και να δώσει λεπτομέρειες σχετικά με το θέμα της παρακολούθησης χρηστών. Αρχικά η παρακολούθηση ξεκινά την πρώτη φορά που επισκέπτεται ο χρήστης το Facebook, με τη δημιουργία ενός browsercookie, ενώ σε περίπτωση διαγραφής δημιουργείται και ένα session cookie. Έτσι κάθε φορά που ο χρήστης επισκέπτεται μια σελίδα η οποία διαθέτει Facebook plug-in το cookie ενημερώνει το Facebook για την ονομασία της σελίδας και την ώρα της επίσκεψης. Επιπλέον αποστέλλονται η διεύθυνση IP, ο browser που χρησιμοποιείται κλπ. Τα στοιχεία κρατούνται στο αρχείο για 90 ημέρες.

Έπειτα σβήνονται. Το Facebook έχει τη δυνατότητα να παρακολουθεί τις κινήσεις του χρήστη ακόμη και όταν δεν είναι συνδεμένος στο κοινωνικό δίκτυο, κάτι για το οποίο δημιουργήθηκε μεγάλη αναστάτωση, αλλά ο Bejar δηλώνει κατηγορηματικά ότι αυτό είναι ενάντια στην πολιτική της εταιρίας και φυσικά δεν εφαρμόζεται.

Εξάλλου, όπως είχε δηλώσει πρόσφατα και ο Mark Zuckerberg, η πρακτική παρακολούθησης των χρηστών είναι τυπική για οποιοδήποτε online δίκτυο που σχετίζεται με διαφημίσεις, συμπεριλαμβανόμενων των Google, Microsoft και Yahoo.

Όπως καταλαβαίνετε, οι κινήσεις του καθένα μας στο Διαδίκτυο παίζουν το ρόλο τους στη δημιουργία τάσεων (έστω και άθελα μας) και γίνονται χρυσό εργαλείο για τις διαφημιστικές εταιρίες. [πηγή: Usa Today 18/11/2011]

Εικόνα 30: Ασφάλεια στο Facebook

2.1.2 Κοινωνικά Προβλήματα

Εκτός από τα προβλήματα που αντιμετωπίζει το Facebook με τα προσωπικά δεδομένα των χρηστών, έρχεται αντιμέτωπο και με κοινωνικά θέματα όπως, παιδόφιλους, βιαστές, δολοφόνους και ρατσιστές, οι οποίοι χρησιμοποιούν τη σελίδα για να βρουν ανυποψίαστα θύματα κυρίως μικρής ηλικίας. Συχνό φαινόμενο αποτελεί η δημιουργία λογαριασμού από βιαστές, δολοφόνους και παιδόφιλους οι οποίοι δηλώνουν διαφορετική ταυτότητα για να προσεγγίσουν τα θύματά τους.

Τρανταχτό παράδειγμα ένας 33χρονος, ο οποίος δήλωνε 17χρονος και ήταν δολοφόνος και βιαστής. Θύμα του μια 17χρονη. Η νεαρή κοπέλα βρήκε φριχτό θάνατο όταν το ραντεβού που βγήκε με τον δήθεν 17χρονο την έφερε αντιμέτωπη με τον 33χρονο βιαστή, ο οποίος τη βίασε και τη σκότωσε. Το θύμα σύμφωνα με πληροφορίες απλά αναζητούσε αγόρι στο διαδίκτυο και

Εικόνα 31: Εικόνα Facebook

την προσέλκυσε ένας όμορφος και καλογυμνασμένος νεαρός. Πίσω από αυτό το προφίλ κρυβόταν ο εν λόγω δράστης ο οποίος είχε καταδικαστεί και στο παρελθόν για βιασμό υπό την απειλή μαχαιριού. Ο ίδιος παραδέχτηκε ότι συνολικά διατηρούσε 10 λογαριασμούς ως 17-19χρονος νεαρός σε ηλεκτρονικά δίκτυα με πάνω από 6,000 φίλους. Η μητέρα της 17χρονης ζήτησε σοκαρισμένη από τους γονείς να προσέχουν με ποιους επικοινωνούν τα παιδιά τους στο διαδίκτυο καταγγέλλοντας τα κοινωνικά δίκτυα ότι κάνουν πολύ εύκολη την επαφή των παιδιών με ανώμαλους, ενώ το Facebook αναγκάστηκε να δημοσιεύσει ανακοίνωση με την οποία προειδοποιεί τους ανηλίκους να προσέχουν την επικοινωνία που έχουν με αγνώστους στο διαδίκτυο. [20]

Επίσης στη Βρετανία δεκαοκτάχρονη οργάνωσε δολοφονία δεκαπεντάχρονου μέσω Facebook. Ο άτυχος νεαρός δέχτηκε το Μάρτιο του 2010 επίθεση από συμμορία εφήβων στο σταθμό Βικτώρια του Λονδίνου σε μια πρωτοφανής βιαιότητας πράξη, αφού δέχτηκε μαχαιριές, κλωτσιές και μπουνιές μέχρι που στο τέλος ξεψύχησε. Ο φόνος του σχεδιάστηκε στο Facebook καθώς η έχθρα μεταξύ μαθητών σε δύο «αντίπαλα σχολεία» οδήγησε στη βία. Την ώρα του μεσημεριανού διαλείμματος η άριστη μαθήτρια Victoria Osoteku έφυγε από το σχολείο και αγόρασε ένα σετ μαχαιριών με τα οποία όπλισε την έφηβη συμμορία των 20 ατόμων. Μετά το σχολείο όλοι μαζί κυνήγησαν το θύμα. Την ώρα που κατέρρεε αιμορραγώντας, η κάμερα ασφαλείας συνέλαβε την Οσοτέκου να του δίνει την τελική κλωτσιά στο κεφάλι και να φεύγει τρέχοντας. [21]

Ένα like στη διάσημη σελίδα κοινωνικής δικτύωσης οδήγησε σε δολοφονία. Στις 8 Μαΐου 2010 30χρονος βρέθηκε δολοφονημένος σε πάρκινγκ νυχτερινού κέντρου στο ύψος Κορωπίου. Κατά την εξιχνίαση της υπόθεσης ως φερόμενος δράστης φάνηκε ένας 26χρονος, αλβανικής καταγωγής ο οποίος εξοργίστηκε από ένα «like» σε μια από τις φωτογραφίες μιας συναδέλφου του. Όπως κατέθεσε η κοπέλα, βουλγαρικής καταγωγής, είχε παλιότερα δεσμό με τον 26χρονο Αλβανό ο οποίος όπως δήλωσε εξακολουθούσε να της κάνει σκηνές ζηλοτυπίας μέσω Facebook. Σύμφωνα με την κατάθεση, ο 26χρονος Αλβανός έστρεψε το ενδιαφέρον του προς τον 30χρονο συνάδερφό της, όταν είδε ότι η νεαρή είχε αναρτήσει στο προφίλ της φωτογραφίες μαζί του από μια εκδήλωση της εταιρείας καλλυντικών όπου εργάζονταν. Επίσης, φέρεται να εξοργίστηκε από το γεγονός ότι ο 30χρονος είχε πατήσει στο Facebook «like», σε μια από τις φωτογραφίες της συναδέρφου του.[22]

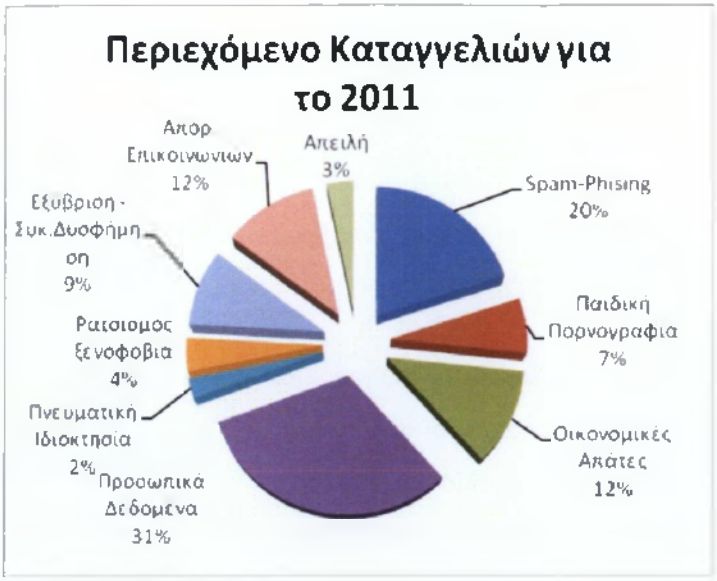
Επίσης σύμφωνα με άρθρο του newsit.gr κάποιοι έκλειναν ραντεβού με ανήλικες χρησιμοποιώντας προφίλ γνωστού ηθοποιού. "Οι κοπέλες έρχονταν στο καμαρίνι στο

θέατρο έτοιμες για όλα" είπε ο ηθοποιός αποκαλύπτοντας το περιστατικό. Όπως αποκάλυψε ο ίδιος, κάποιος είχε δημιουργήσει λογαριασμό χρησιμοποιώντας το όνομα του και έκλεινε ραντεβού με ανυποψίαστες ανήλικες. Ο ηθοποιός μάλιστα απευθύνθηκε στην δίωξη ηλεκτρονικού εγκλήματος, αλλά η απάντηση που πήρε είναι πως "είναι δημόσιο πρόσωπο και δεν μπορούν να τον βοηθήσουν, βγείτε και πείτε πως το προφίλ δεν είναι δικό σας".[πηγή: newsit.gr 06/12/2011]

Εικόνα 32: Εικόνα Facebook

Τέλος σοκ προκάλεσε στα Χανιά η είδηση ότι 22χρονη δασκάλα δημοτικού αποπλανούσε μαθητές μέσω Facebook. Μετά από καταγγελία της μητέρας 15χρονου στην Κρήτη, η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διερεύνησε την υπόθεση αποπλάνησης ανηλίκων από την δασκάλα. Σύμφωνα με ανακοίνωση της Αστυνομίας, η 22χρονη χρησιμοποιούσε την ιδιότητα της για να προσεγγίζει ανηλίκους, ηλικίας 10 έως 15 ετών μέσω facebook, προφασιζόμενη ότι θα τους βοηθούσε στα μαθήματά τους και αφού κέρδιζε την εμπιστοσύνη τους, τους αποπλανούσε, προχωρώντας σε ερωτικές πράξεις μαζί τους. Από ψηφιακή έρευνα και ανάλυση ηλεκτρονικών δεδομένων εντοπίστηκαν διάλογοι με άσεμνο και ανάρμοστο περιεχόμενο της 22χρονης με 15χρονοανήλικο, μαθητή Γυμνασίου στην Κρήτη. Οι διάλογοι ήταν καταχωρημένοι στον προσωπικό λογαριασμό του ανηλίκου. Κατά την εξέτασή του από το κλιμάκιο της Δίωξης Ηλεκτρονικού Εγκλήματος, ο 15χρονος επιβεβαίωσε τόσο τους διαλόγους, όσο και την αποπλάνησή του από την 22χρονη. Ειδικότερα, προέκυψε ότι η 22χρονη είχε ερωτική επαφή μαζί του, πριν πέντε περίπου μήνες. Για την αποπλάνηση η μητέρα του ανηλίκου ζήτησε την ποινική δίωξη της δασκάλας.[πηγή: news247 10/01/2012].

Στο παρακάτω διάγραμμα βλέπουμε το περιεχόμενο καταγγελιών για το 2011 στην Ελλάδα.



Τα συγκλονιστικά στοιχεία ανακοίνωσαν οι υπεύθυνοι του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου και της ανοιχτής γραμμής καταγγελιών SafeLine.

Τα στοιχεία δείχνουν ότι κατά τη διάρκεια του δεύτερου εξαμήνου του 2011 διπλασιάστηκε ο αριθμός των καταγγελιών που αφορούσε στην παιδική πορνογραφία σε σύγκριση με το Α΄ εξάμηνο. Συνολικά, κατατέθηκαν περισσότερες από εκατό σχετικές αναφορές και για την αποτελεσματική αντιμετώπισή τους καταχωρήθηκαν στην κοινή βάση δεδομένων της οργάνωσης Inhope (www.inhope.org). Μέλος της συγκεκριμένης οργάνωσης είναι και η SafeLine και μέσα από την κοινή βάση δεδομένων προωθήθηκαν στις άλλες ανοικτές γραμμές καταγγελιών ανάλογα με τη χώρα προέλευσης της παράνομης ιστοσελίδας![23]

2.1.3 Προσβολές Προσωπικότητας

Το Facebook προσφέρει την ελευθερία λόγου και έκφρασης. Έτσι παρατηρήθηκε το φαινόμενο δημιουργίας ομάδων ρατσιστικού περιεχομένου. Τα μέλη των ομάδων αυτών δεν έχουν σεβασμό προς τον συνάνθρωπο και τη διαφορετικότητά του. Δεν γνωρίζουν την έννοια της ισότητας και της αλληλεγγύης και έτσι στρέφονται κατά κάποιων κοινωνικών ομάδων με σκοπό να τις σχολιάσουν, να τις μειώσουν και τελικά να τις υποβαθμίσουν. Συχνό είναι ακόμα το φαινόμενο οι ομάδες αυτές να απευθύνονται σε άτομα με μειωμένες ικανότητες όπως είναι τα άτομα με ειδικές ανάγκες. Τέλος και σε μεμονωμένα άτομα για διάφορους λόγους.

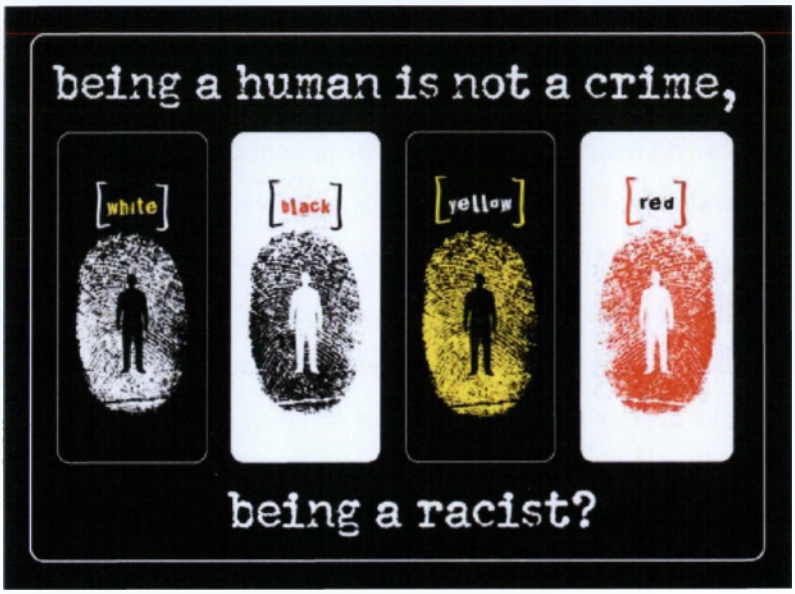
Σύμφωνα με άρθρο της εφημερίδας «Το Έθνος» μια μαθήτρια απεβλήθει οριστικά από το σχολείο της για τη δημιουργία ομάδας στο facebook κατά της διευθύντριας του σχολείου. Ο τίτλος της ομάδας στη σελίδα κοινωνικής δικτύωσης ήταν: «Κι εγώ μισώ τη διευθύντρια της Χρυσοπηγής» και προσκάλεσε και συμμαθητές της να γίνουν μέλη σε αυτή. Το γεγονός έγινε γνωστό και συγκλήθηκε συμβούλιο καθηγητών και τιμώρησε τη μαθήτρια αποβάλλοντάς τη από το σχολείο παρά τη μεταμέλεια της νεαρής, η οποία και ζήτησε συγγνώμη από την διευθύντριά της. [24]

Σε άρθρο της Ελευθεροτυπίας έγινε γνωστή η ακόλουθη ιστορία με πρωταγωνιστή έναν αλλοδαπό φοιτητή. Ο συγκεκριμένος φοιτητής δεν άντεχε να βλέπει στο Facebook τις σελίδες με τα υβριστικά σχόλια κατά των ξένων και προσπάθησε να αντιδράσει. Έγινε μέλος σε ένα από αυτά με το πραγματικό του όνομα και προσπάθησε να πείσει τα μέλη της ομάδας με τα επιχειρήματά του να αλλάξουν γνώμη. Δεν το κατάφερε όμως. Αντίθετα δέχτηκε υβριστικά σχόλια του τύπου: «Γύρνα πίσω στην πατρίδα σου κωλαλβανέ» και «Έλληνας γεννιέσαι, δεν γίνεσαι». Εκείνος χωρίς να προσβάλλει κανέναν συνέχισε μέχρι που το ίδιο το Facebook τον σκότωσε. Του απαγόρεψε την είσοδο στο συγκεκριμένο group και παράλληλα διέγραψε ότι είχε αναρτήσει όχι μόνο στη συγκεκριμένη σελίδα αλλά και σε άλλες. Δημιουργούνται όμως μέσω αυτής της ιστορίας πολλά ερωτήματα. «Είναι αδύνατον, λοιπόν, να διαφωνήσεις με ρατσιστές στο Διαδίκτυο, κύριοι διαχειριστές του Facebook; Αν εκφράσεις αντιρατσιστικές απόψεις κινδυνεύεις με διαγραφή του λογαριασμού σου! Δεν εξετάζουμε το γεγονός ότι υπάρχουν τόσα φασιστικά groups στο Facebook. Δημοκρατία έχουμε, υπάρχει χώρος για όλες τις απόψεις. Όμως, από πότε μπορούν να... καθορίζουν οι φασίστες ποιοι θα έχουν άποψη και ποιοι όχι, και μάλιστα βρίζοντας και απειλώντας; Αυτή είναι η ελευθερία της λεγόμενης κοινωνικής δικτύωσης;». [25]

Εκτός από την Ελλάδα έχουν εντοπιστεί και αλλού παρόμοια φαινόμενα. Το δικαστήριο του Πακιστάν για παράδειγμα είχε μπλοκάρει προσωρινά το Facebook επειδή φιλοξενούσε ένα «βλάσφημο» διαγωνισμό για γελοιογραφίες του Μωάμεθ. Οποιαδήποτε απεικόνιση του προφήτη Μωάμεθ θεωρείται βλάσφημη από τους μουσουλμάνους. Η δημοσίευση τέτοιων γελοιογραφιών σε εφημερίδες της Δανίας το 2005 οδήγησε σε βίαιες διαμαρτυρίες σε πολλές μουσουλμανικές χώρες. Από τα 50 άτομα που σκοτώθηκαν στις ταραχές, τα πέντε έχασαν τη ζωή τους στο Πακιστάν.[26]

Τέλος έχουν παρατηρηθεί και φαινόμενα ρατσισμού και σε άτομα με αναπηρίες. Μία από τις ομάδες οι οποίες αναγράφουν υβριστικά σχόλια κατά των Α.με.Α. έχει την επωνυμία

"Λέμε ΝΑΙ στην ευθανασία όσων πάσχουν από σωματική ή διανοητική αναπηρία" που φιλοξενείται στο Facebook. Οι εμπνευστές της ομάδας και μερικές δεκάδες ομοϊδεάτες τους συνυπογράφουν σε σχόλια τα ακόλουθα: «Στηρίζουμε την ευθανασία των ατόμων με αναπηρία καθώς επιβαρύνουν την εθνική οικονομία και τη δημόσια υγεία, παρασιτώντας στην κοινωνία χωρίς να προσφέρουν». Και επιπλέον ζητούν μέσα από το συγκεκριμένο groupτην μεγαλύτερη δυνατή ... συστράτευση των χρηστών του Facebook, κατά των ατόμων με αναπηρίες.[27]



Εικόνα 33: Εικόνα κατά του ρατσισμού

2.2 Twitter

2.2.1 Hacking

Το Twitter όπως έχουμε αναφέρει είναι μια σελίδα κοινωνικής δικτύωσης λίγο διαφορετική από τις υπόλοιπες, δεν παύει όμως να συναντάμε και εδώ προβλήματα ασφαλείας.

Στις 6 Αυγούστου του 2009 το Twitterπαρέμεινε κλειστό για τέσσερις ώρες. Ο λόγος μια επίθεση που ονομάζεται Denial of Service (DoS). Με αυτήν την επίθεση ο hackerδημιούργησε ένα wormτο οποίο στάλθηκε στο δίκτυο. Αυτό towormκατανάλωσε όλο το εύρος ζώνης το οποίο ήταν διατεθειμένο για το Twitterκαθώς και για μερικές άλλες σελίδες κοινωνικής δικτύωσης. Έτσι στάλθηκαν στο δίκτυο «άχρηστες» πληροφορίες σε μεγάλο μέγεθος. Το δίκτυο υπερφορτώθηκε και δημιούργησε DoS. «Cyxymu» ήταν το όνομα του λογαριασμό από τον οποίο στάλθηκε η συγκεκριμένη επίθεση. Η επίθεση στάλθηκε σε μορφή tweetκαι γρήγορα διαδόθηκε σε όλο το δίκτυο προκαλώντας τεράστια «κίνηση». Η εταιρία anti-virus McAfee βρήκε ότι οι hackerχρησιμοποίησαν τη συγκεκριμένη μέθοδο για να προσεγγίσουν τους χρήστες στην ώστε να εισέλθουν σε κακόβουλα site.Επίσης την ίδια χρονιά, τέσσερις ακόμα επιθέσεις πραγματοποιήθηκαν. Ένα wormαυτή τη φορά διαδόθηκε και επιτέθηκε στο twitterμε τέσσερις επαναλαμβανόμενες επιθέσεις. Κάθε φορά αυξανόταν η ένταση του wormδιαδίδοντάς το και με αυτόν τον τρόπο υπέκλεπταν προσωπικές πληροφορίες από τους λογαριασμούς των χρηστών. Ακόμα έκανε ενημερώσεις στις πληροφορίες και στις καταστάσεις τους.

Εικόνα 34: Εικόνα Twitter κατά τη διάρκεια του DoS

Όπως και στο Facebookέτσι και στο Twitterσυναντάμε phishing attacks. Σε μια πρόσφατη phishing attack χρησιμοποιήθηκαν torrentως μέσο για να επιτύχουν πρόσβαση στα προφίλ των χρηστών. Οι ανυποψίαστοι χρήστες οι οποίοι αναζητούσαν πληροφορίες σε forum ήταν τα κύρια θύματα από αυτή την επίθεση. Οι επιτιθέμενοι δημιούργησαν ένα σύνδεσμο torrent ο οποίος ανακατεύθυνε το χρήστη σε μια σελίδα όπου έπρεπε να δώσει τα στοιχεία σύνδεσης του λογαριασμού του. Έτσι μπορούσε ο hackerνα πάρει πληροφορίες για τους λογαριασμούς των χρηστών. [28]

Στις 6 Ιανουαρίου του 2009 hackerκατάφεραν να αποκτήσουν πρόσβαση σε περισσότερους από 30 λογαριασμούς Twitter διασήμων εκ των οποίων του Barack Obama, της Britney Spears και του FOXNews. Το Twitterκλείδωσε γρήγορα τους λογαριασμούς και τους επέστρεψε στους πραγματικούς ιδιοκτήτες τους αφού πρώτα όμως σταλθεί αρκετά

μηνύματα μέσω αυτών. Από το λογαριασμό του ανταποκριτή του CNN Rick Sanchez, στάλθηκε ένα tweet λέγοντας ότι είναι υπό την επήρεια ναρκωτικών και δεν θα ήταν σε θέση να εργαστεί εκείνη τη μέρα. Μέσα από το λογαριασμό του FOXNews ανακοινώθηκε ότι ο Bill O Riley (παρουσιαστής talk show) είναι ομοφυλόφιλος. Το Twitterισχυρίστηκε ότι οι επίθεση έγινε μέσα από τα support tools της εταιρίας τα οποία και έκλεισαν μέχρι να ασφαλιστούν.

Στις 11 Απριλίου του 2009 το Twitter «υποφέρει» από μια σειρά επιθέσεων worm. Οι επιθέσεις wormκράτησαν την ομάδα ασφαλείας του Twitteraπασχολημένη για μερικές μέρες καθώς προσπαθούσαν να εντοπίσουν «μολυσμένους» λογαριασμούς και να σβήσουν κάποια tweet που είχαν αναρτηθεί από αυτούς. Αναλυτικότερα, στις 11 Απριλίου άρχισε να διαδίδεται το worm Mikeyy ενθαρρύνοντας τους χρήστες να επιλέξουν ένα σύνδεσμο, τον StalkDaily.com. Με την είσοδο του χρήστη στη σελίδα αυτή, ο λογαριασμός του «μολυνόταν» και διέδιδε και αυτός με τη σειρά του το συγκεκριμένο μήνυμα και ούτω καθεξής. Η επίθεση κράτησε μέχρι τις 13 Απριλίου, αλλά δεν κλάπηκε καμία πληροφορία από τους χρήστες.

Την ίδια χρονιά, στελέχη του Twitterπέσανε θύματα, όταν ένας hackerπήρε στην κατοχή του και μοίρασε 300 έγγραφα τα οποία αφορούσαν επιχειρησιακές υποθέσεις του Twitterκαι τα οποία αποθηκεύτηκαν σε εφαρμογές της υπηρεσίας Google. Η αιτία ήταν ο εύκολος κωδικός και ο συνιδρυτής του Twitter, Biz Stone δήλωσε ότι η Googleδεν έχει καμία σχέση με την επίθεση. Ο hackerισχυρίστηκε ότι είχε υπό την κατοχή του, τους λογαριασμούς του άλλου συνιδρυτή Evan Williams, της γυναίκας του, καθώς και αρκετών υπαλλήλων. Ο Williamsαρνήθηκε ότι ο hackereίχε στην κατοχή του το λογαριασμό του, αλλά το επιβεβαίωσε για τη γυναίκα του.

Στις 14 Αυγούστου 2009 το Twitterχρησιμοποιήθηκε για να διαχειριστεί το botnet. Ένας ελεγκτής ασφαλείας του ArborNetworks ανακάλυψε ότι hackersχρησιμοποιούσαν το Twitterγια να οργανώσουν ένα botnet, ένα δίκτυο δηλαδή από μολυσμένους υπολογιστές. Οι ιδιοκτήτες του botnet συνεχώς δουλεύουν για να βρουν νέους τρόπους ώστε τα δίκτυά τους να δουλεύουν συνεχώς, και το πιο πρόσφατο μέσο ήταν το Twitter.Το IDGNews Service ανέφερε ότι λογαριασμοί Twitterπου έχουν ανασταλεί χρησιμοποιούνταν για να στέλνουν tweet με συνδέσμους εκτελέσιμων αρχείων, οι οποίοι χρησιμοποιούνταν από το botnet.

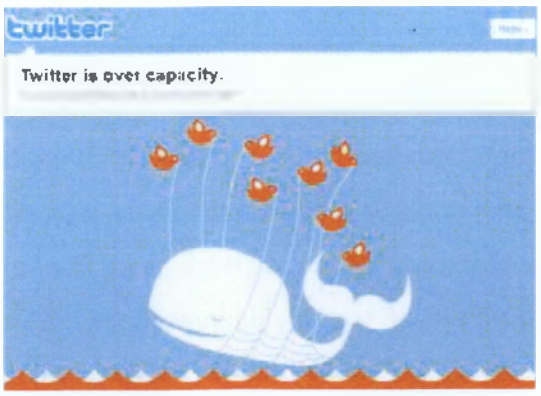
Ακόμα είναι γνωστό ότι το Twitter έχει προσελκύσει πολλούς διάσημους οι οποίοι έχουν βρει ένα νέο μέσο για να επικοινωνούν με τους θαυμαστές τους. Ο αριθμός των θαυμαστών όμως εκτοξεύτηκε στα ύψη και αυτό τράβηξε την προσοχή πολλών hacker. Παρά την προσπάθεια του Twitter να απαγορεύσει τους πολύ προφανείς κωδικούς πρόσβασης, δεν σταμάτησε το hacking, με τους γνωστότερους χρήστες να έχουν υποστεί τις συνέπειες. Από τη Lady Gaga μέχρι τον Ashton Kutcher, αλλά και πολύ περισσότερο στον Justin Bieber, του οποίου κυκλοφόρησε το τηλέφωνό του, αλλά στη συνέχεια και αυτός με τη σειρά του ανακάλυψε τον hacker και μοίρασε το δικό του τηλέφωνο. [29]

Στις 9 Σεπτεμβρίου 2011 ένας λογαριασμός twitter που ανήκε στο κανάλι NBCNews πέρασε στα χέρια hacker, ο οποίος έκανε μια φάρσα. Διέδωσε ότι ένα αεροπλάνο συνετρίβη στην περιοχή της Νέας Υόρκης. Ο λογαριασμός αμέσως τέθηκε σε λειτουργία offline ενώ το κανάλι διέψευσε την είδηση και απολογήθηκε. Συγκεκριμένα ο διευθυντής του καναλιού Brian Williams δήλωσε: «Ο λογαριασμός Twitter του NBC News πέρασε σε χέρια hacker. Ως αποτέλεσμα οι ψεύτικοι ισχυρισμοί για την συντριβή του αεροσκάφους στο σημείο μηδέν στη Νέα Υόρκη. Δουλεύουμε στο Twitter για να διορθώσουμε την κατάσταση και απολογούμαστε για τον τρόμο τον οποίο προκάλεσε η είδηση από αυτήν την ανεύθυνη πράξη. Ο λογαριασμός είχε περίπου 130.000 followers πολλοί από τους οποίους είδαν την είδηση πριν κλείσει ο λογαριασμός, οι οποίοι διέδωσαν το νέο και αλλού μιλώντας για μια νέα τρομοκρατική επίθεση λόγω της επετείου για την επίθεση στους δίδυμους πύργους την εντεκάτη Σεπτεμβρίου. Ο σύμβουλος του καναλιού Ryan Osborn δήλωσε ότι είδε το μήνυμα να εμφανίζεται 40 δευτερόλεπτα αφού το δημοσίευσαν οι hacker ενώ βρισκόταν ο ίδιος στο λογαριασμό και σύντομα συνειδητοποίησε ότι ο κωδικός είχε αλλάξει. Στα επόμενα λεπτά ο λογαριασμός έκλεισε. [30]

Τα spamδεν θα έλειπαν και από το Twitter. Σύμφωνα με το McAfee spammers παρότρυναν χρήστες να ανεβάσουν οι ίδιοι spam στους λογαριασμούς τους έναντι κάποιας αμοιβής. Πολλοί θέλησαν να βάλουν λίγα ακόμα χρήματα στις τσέπες τους και έτσι ανέβασαν κακόβουλους συνδέσμους στα προφίλ τους. Ποτέ όμως δεν εισέπραξαν χρήματα από αυτή τους την κίνηση. [31]

Ακόμα μέσα από παιχνίδια προσέλκυαν τους χρήστες. Αλλά πολλές φορές η διασκέδαση έχει κόστος. Με αυτό το spammes sage για παιχνίδια, οι spammer προσέφεραν δωρεάν παιχνίδια αλλά υπήρχε μεγάλη πιθανότητα μαζί με το παιχνίδι να κατεβάσουν και malwareήspyware στο σύστημά τους. [32]

Σύμφωνα με το Sophos, κυκλοφόρησε μια phishing attack σε μορφή tweet. Οι hackerενθάρρυναν τους χρήστες να πατήσουν ένα σύνδεσμο ο οποίος έλεγε: «Σε είδα γυμνό» ή «σε είδα σε ένα βίντεο». Πολλοί χρήστες εξαπατήθηκαν και θέλοντας να το εξακριβώσουν έπεσαν θύματα των hacker καθώς δεν υπήρχαν φωτογραφίες ή βίντεο με τους ίδιους.. απλά malware. [33]



Εικόνα 35: εικόνα Twitter όταν ήταν overfload

Ένα άλλο φαινόμενο όχι και τόσο γνωστό, η οποίο ήρθε στην επιφάνεια από ερευνητές της Symantec, είναι το Web Rubber necking. Τι είναι όμως το Rubber necking; Για παράδειγμα σε ένα ατύχημα πριν καθαριστεί ο χώρος περνάνε μηχανές και κόβουν ταχύτητα θέλοντας να δουν τι έχει συμβεί. Όμως πολλές φορές λόγω απροσεξίας καταλήγουν να είναι θύματα. Το ίδιο συμβαίνει και στο διαδίκτυο. Χρήστες ακούν για μια επίθεση στο Twitterγια παράδειγμα και σπεύδουν στις σελίδες να δουν τι έχει συμβεί και καταλήγουν και αυτοί θύματα της επίθεσης. Γι αυτό το λόγο όταν υπάρχει σελίδα υπό επίθεση, πιστέψτε το και αφήστε το. [34]

Ένα νέο Twitter spam οδηγεί σε ψεύτικη επίθεση anti-virus. Όπως δήλωσε εκπρόσωπος της GFIδίνεται από τους spammersύνδεσμος για ελεύθερο anti-virus καθώς το σύστημά τους βρίσκεται σε κίνδυνο. Όταν ο χρήστης κατεβάσει το δήθεν anti-virus το μόνο που καταφέρνει είναι να περάσει στον υπολογιστή του το Winwebsec (malware). Η GFIυποστηρίζει ότι τα προϊόντα τους αναγνωρίζουν το malware ως Trojan.Win32.Fakeav.tri. Το συγκεκριμένο malware ανήκει στην «οικογένεια» fake vimes και επανατοποθετείται κάθε 3 με 6 ώρες. [35]

Επιπλέον, με τέτοιου είδους κόλπα οι γνωστοί πλέον σε όλο τον κόσμο Anonymous προσπαθούν να ξεγελάσουν χρήστες και να τους εντάξουν στις επιθέσεις τους. Συγκεκριμένα το hacker group Anonymous έχει στο Twitter 250.000 followers αλλά οι ειδικοί στην ασφάλεια της Sophos προειδοποιούν τους θαυμαστές ότι μπορεί

Εικόνα 36: Anonymous στο twitter

άθελά τους να πάρουν μέρος σε επιθέσεις της ομάδας. Σύνδεσμοι των Anonymous που προωθούνται μέσω Twitter από τους χρήστες μπορεί να κάνουν τον υπολογιστή του χρήστη μέσο κάποιας επίθεσης. Οι επιθέσεις αυτές ονομάζονται: «a denial of service attacks». Η Αμερικάνικη κυβέρνηση ανακοίνωσε ότι οποιαδήποτε ανάμειξη χρηστών, είτε αυτή γίνεται άθελα τους θα έχει διώξεις. [36]

Σύμφωνα με ανακοίνωση της Kaspersky το Νοέμβρη του 2011 τοTwitterδέχτηκε πολλές επιθέσεις από spams. Μέλη της σελίδας είδαν να δέχονται γάλο αριθμό spamπου τους παρότρυνε να στείλουν πρόσκληση σε φίλους για να δημιουργήσουν και αυτοί λογαριασμό στον ιστότοπο. Οι σύνδεσμοι των προσκλήσεων όμως οδηγούσαν σε σελίδες πορνογραφίας. Επιπλέον στην ίδια αναφορά η kasperksy αναφέρει ότι διαπιστώθηκε η ύπαρξη πολλών μνημάτων ηλεκτρονικού ταχυδρομείου κοινοποιώντας προσκλήσεις από «ηλεκτρονικά καταστήματα». Οι προσκλήσεις αυτές ζητούσαν από το χρήστη να ακολουθήσει ένα σύνδεσμο για αγορές προϊόντων. Φυσικά οι σύνδεσμοι αυτοί οδηγούσαν σε malware. Τέλος σύμφωνα με την έκθεση υπάρχει μια αύξηση του ποσοστού των phishing attacks στην Υπηρεσία Εσωτερικών Εσόδων, στο τέλος του 2011, με το θέμα να περιστρέφεται γύρω από τις ετήσιες αποδόσεις καταθέσεων στις ηνωμένες Πολιτείες. [37]

Για όλους αυτούς του λόγους το σώμα ναυτικού των Ηνωμένων Πολιτειών απαγόρεψε τη χρήση σελίδων κοινωνικής δικτύωσης όπως αυτή του Twitter, δηλώνοντας ότι τέτοιες σελίδες γενικότερα έχουν προβλήματα από κακόβουλους χρήστες και περιεχόμενα και είναι μεγάλο ρίσκο η έκθεση πληροφοριών σε αυτά. Δεν απαγορεύτηκε όμως στους πεζοναύτες η προσωπική χρήση του Twitter. Δεν ήταν όμως μόνο το πολεμικό ναυτικό που προέβη σε μια τέτοια κίνηση, καθώς και άλλοι οργανισμοί απαγόρεψαν σελίδες κοινωνικής δικτύωσης κατά τη διάρκεια της εργασίας τους. Σύμφωνα με μία έρευνα του Rober half Technology περισσότεροι από 14.000 οργανισμοί έχουν πάρει μια τέτοια απόφαση.

Εικόνα 37: κίνδυνοι στο ιντερνέτ

2.2.2 Κοινωνικά προβλήματα

Το Twitterόπως έχουμε αναφέρει είναι ένα social networkδιαφορετικό από τα υπόλοιπα. Το γεγονός ότι βασίζεται σε μικρά κείμενα 140 γραμμάτων και δεν έχει πληθώρα εφαρμογών, καθώς και ότι οι αναρτήσεις είναι ανοιχτές στο κοινό, έχει περιορίσει εγκλήματα, όπως βιασμοί, παιδοφιλία και δολοφονίες. Το twittereίναι επίσης ένα sitekοινωνικής δικτύωσης που απευθύνεται κυρίως σε άτομα μεγαλύτερης ηλικίας οπότε δεν έχουμε την εμφάνιση παιδόφιλων, χωρίς όμως όλα αυτά να σημαίνουν ότι οι περιπτώσεις αυτές είναι ανύπαρκτες. Και εδώ κάποιος μπορεί να κάνει followέναν άλλο χρήστη από τη στιγμή που γίνεται χωρίς τη συγκατάθεση του δεύτερου, και μέσω κάποιου tweetπου αναφέρει την πιθανή του τοποθεσία να τον εντοπίσει και να προβεί σε κάποιο έγκλημα. Ακόμα ο ίδιος ο δράστης μπορεί σε προσωπικό του tweetνα παραπλανήσει άλλο χρήστη λέγοντας ότι νιώθει μοναξιά και ψάχνει παρέα, ή ότι ψάχνει σύντροφο.

Το γεγονός ότι στο Twitterδεν έχουμε επιθέσεις από παιδόφιλους δεν σημαίνει ότι οι παιδόφιλοι δεν χρησιμοποιούν τη σελίδα για να επικοινωνούν μεταξύ τους. Κρυμμένοι πίσω από ψεύτικα ονόματα ανταλλάζουν tweetκαι μπορούν να διανέμουν πορνογραφικό υλικό εύκολα και γρήγορα όπως δήλωσε ο Dennis Grabowski, πρόεδρος της μη κυβερνητικής ομάδας «no abuse in internet». Απλά με μερικά κλικ μπορούν και διανέμουν στο Twitterβίντεο και εικόνες. «Όλο και περισσότερα tweetκαι σύνδεσμοι με πορνογραφικό υλικό στέλνονται μέσω του δικτύου» συμπλήρωσε ο πρόεδρος, αναφερόμενος στα αυξημένα νούμερα λογαριασμών Twitterπου έχουν αναφερθεί από χρήστες στην οργάνωσή τους. Συχνά οι παιδόφιλοι χρησιμοποιούν το Twitteryια να ενημερωθούν ακόμα και για το κλείσιμο ιστοσελίδων με παιδική πορνογραφία καθώς και για τη δημιουργία νέων. Τέλος ο Denniw Grabowskiυπογραμμίζει ότι το Twittereίναι ένα μεγάλο δίκτυο και είναι δύσκολος ο εντοπισμός των παιδόφιλων. Όμως θα έπρεπε όλοι οι χρήστες να ενδιαφερθούν και να αναφέρουν μόλις δουν κάποιο tweetμε πορνογραφικό υλικό. [38]

Η Kate Gosselin είχε ενοχληθεί από παιδόφιλο στο Twitter. Ο συγκεκριμένος χρήστης είχε φωτογραφία ενός ηθοποιού και είχε follow την διάσημη παρουσιάστρια δημοσιεύοντας ακατάλληλα tweet με περιεχόμενο παιδικής πορνογραφίας. Το περιστατικό αναφέρθηκε και ο λογαριασμός του χρήστη μπλοκαρίστηκε.

Εκτός από τους παιδόφιλους, συμμορίες χρησιμοποιούν τη σελίδα για να οργανώσουν επιθέσεις είτε μεταξύ τους είτε σε τρίτους. Ένας δεκαπεντάχρονος, μέλος της συμμορίας TheNewDons ισχυρίζεται ότι το twittereίναι χρήσιμο για τον εντοπισμό βίαιων πράξεων. Το αστυνομικό τμήμα της Νέα Υόρκης χρησιμοποιεί το Twitteraπό τη μεριά του για να

αποτρέψει τις συγκεκριμένες επιθέσεις, εντοπίζοντας τις online κινήσεις των μελών των συμμοριών. [39]

Το Twitterχρησιμοποιείται ακόμα, από εγκληματίες, για την οργάνωση μορφής διαδηλώσεων που φέρνουν το χάος. Στο Λονδίνο για παράδειγμα πρόσφατα έγινε εξέγερση με πολλές καταστροφές. Ομάδα νέων κατηγορήθηκε ότι μέσω της σελίδας κοινωνικής δικτύωσης ώθησε τον κόσμο και τον οργάνωσε. Συνεννοούνταν και ήταν ένα βήμα μπροστά και από την αστυνομία για να μπορούν να ξεφεύγουν. Στη Φιλαδέλφεια ένας άντρας δέχθηκε επίθεση από 30 άτομα, τα οποία σύμφωνα με πληροφορίες οργανώθηκαν μέσω Twitter. [40]

Ακόμα πολλοί διαρρήκτες επωφελούνται από αφελείς δημοσιεύσεις στο Twitter. Οι κλέφτες γνωρίζουν πότε οι ιδιοκτήτες βρίσκονται εκτός πόλης και έτσι χτυπούν ανενόχλητοι τα σπίτια. Σύμφωνα με τελευταία στοιχεία το 80% των διαρρηκτών χρησιμοποιούν τέτοιου είδους πληροφορίες.

2.2.3 Προσβολές προσωπικότητας

Οι χρήστες στο Twitterόπως και στις υπόλοιπες σελίδες κοινωνικής δικτύωσης έχουν ελευθερία λόγου. Πολλές φορές όμως η ελευθερία λόγου που δίνεται σε κάποιους χρησιμοποιείται για να εκφράσει ρατσιστικά σχόλια για μια μειονότητα, ή απλά για να προσβάλλει ένα πρόσωπο. Τέτοιες περιπτώσεις κατάχρησης της ελευθερίας λόγου έχουμε και εδώ.

Στις 02/04/2012 και έπειτα από έρευνα της αστυνομίας ανακαλύφθηκε ότι μετά από έναν αγώνα ποδοσφαίρου του αγγλικού πρωταθλήματος ένας ποδοσφαιριστής δέχθηκε ρατσιστικά σχόλια μέσω Twitter. Όλα ξεκίνησαν όταν ο ποδοσφαιριστής της Newcastle James Perch, μετά από μια σύγκρουση με τον τερματοφύλακα της Liverpool Jose Reina δέχθηκε την κόκκινη κάρτα. Ένας χρήστης, ο οποίος πιστεύεται ότι είναι 17χρονος οπαδός της Liverpool έγραψε: «I want to punch Perch in his n***** head» και το μήνυμα τελείωσε αποκαλώντας τον αμυντικό της Newcastle«a c***». Άλλοι χρήστες έπεσαν πάνω στον δεκαεπτάχρονο λέγοντας ότι δεν είναι σωστό και ότι η αστυνομία πρέπει να ενημερώνεται. [41]

Στον Καναδά ένας παίχτης δέχτηκε ρατσιστικά σχόλια μετά από αγώνα για το NHL. Ήταν το πρώτο παιχνίδι για τα playoff. Ο Joel Ward σκόραρε 3 δευτερόλεπτα πριν λήξει το παιχνίδι

και έδωσε τη νίκη στην ομάδα του. Το πρόβλημα ήταν ότι ήταν μαύρος και ακολούθησαν ρατσιστικά σχόλια εναντίον του στο Twitteraπό την αντίπαλη ομάδα. Κάποια από τα πολλά tweet είναι τα ακόλουθα. «You guys let the _____ score? I'm done.» Και «Of all people to score it had to be the _____». Ακολούθησε πλήθος αντιδράσεων από την διοργανώτρια επιτροπή, παίχτες καθώς και άλλους οπαδούς. [42]

Εικόνα 38: Ρατσιστική επίθεση

Στις 27 Μαρτίου 2012 και ενώ η ταινία «The hunger games» είχε σπάσει τα ταμεία υπήρξαν κάποια μη ευχάριστα θέματα από κάποιους θαυμαστές του βιβλίου στο οποίο βασίστηκε η ταινία. Η συγγραφέας περιέγραφε έναν από τους ρόλους να έχει σκούρο δέρμα και στην ταινία το ρόλο πήρε μια Αφρικανο-αμερικανίδα ηθοποιός η οποία και δέχτηκε ρατσιστικά σχόλια μέσω της δημοφιλούς σελίδας Twitter. Κάποια από τα σχόλια ήταν τα εξής: «Γιατί πρέπει η Rue να είναι μαύρη;», «Γιατί η Rue είναι ένα μικρό μαύρο κορίτσι;», καθώς και πιο ρατσιστικά σχόλια, όπως «Γιατί ο παραγωγός δίνει όλους τους καλούς ρόλους σε μαύρους;» και «Είμαι ακόμα θυμωμένος που η Rue είναι μαύρη». Εκπρόσωποι της ταινίας δεν σχολίασαν καθόλου το θέμα. [43]

Εικόνα 39: Ρατσιστική επίθεση 2

Περιστατικό προσβολής προσωπικότητας με ρατσιστικά σχόλια οδήγησε την αστυνομία σε σύλληψη ενός υπόπτου. Ο ύποπτος συνελήφθη για επίθεση που έκανε μέσω Twitterστον

Σταν Κόλιμορ. Ο δημοφιλής ανταποκριτής αγώνων της PremierLeague για το «TalkSport» και πρώην ποδοσφαιριστής, έγινε το νέο «θύμα» του ρατσιστικού φαινομένου που τις τελευταίες μέρες εμφανίζεται όλο και πιο συχνά στην Αγγλία. Αναλυτικότερα, έλαβε υβριστικά και ρατσιστικά σχόλια στον προσωπικό του λογαριασμό στο Twitter. Το περιστατικό έφτασε στην αστυνομία, η οποία ξεκίνησε έρευνα και πραγματοποίησε τη σύλληψη του υπόπτου. [44]

2.3 Googleplus

2.3.1 Hacking

Το Googleplus είναι ένα πρόσφατο κοινωνικό δίκτυο, αφού λειτουργεί από τις 28 Ιουνίου 2011. Από τη στιγμή όμως που και σε αυτή τη σελίδα ο χρήστης μοιράζεται προσωπικά δεδομένα όπως φωτογραφίες, κατάσταση σχέσης, τηλέφωνο, διεύθυνση, και άλλα πολλά, δημιουργήθηκαν και εδώ θέματα με την ασφάλεια των προσωπικών δεδομένων του χρήστη. Συναντάμε μια πληθώρα διαφορετικών επιθέσεων που έχουν σκοπό την πρόσβαση σε προσωπικά δεδομένα. Για να μπορέσει ένας hackerνα εισβάλει στο λογαριασμό Googleplus ενός χρήστη αρκεί να εισβάλει στο gmail του αφού και οι δυο εφαρμογές της Googlesυνδέονται.


Εικόνα 40: κλοπή χρημάτων μέσω διαδικτύου

Τα πρώτα phishing attacks έκαναν την εμφάνισή τους από τις πρώτες μέρες λειτουργίας της σελίδας, την περίοδο που δημιουργούσε κάποιος λογαριασμό μόνο με πρόσκληση. Ήταν η ευκαιρία για κάποιους να αποδείξουν το ταλέντο τους. Πολλές ήταν οι περιπτώσεις όπου στάλθηκαν ψεύτικες προσκλήσεις σε χρήστες, οι οποίες τους οδηγούσαν σε σελίδες όπου ζητούνταν προσωπικές πληροφορίες για τη δημιουργία του λογαριασμού. Ο Fabio Assolini malware researcher της Kaspersky δήλωσε: «Το Googleplus είναι άλλη μια προσθήκη στην κόσμο της κοινωνικής δικτύωσης και τραβά το ενδιαφέρον πολλών χρηστών. Το ίδιο όμως ισχύει και για κυβερνοεγκληματίες καθώς η εταιρία Kaspersky εντόπισε κυβερνοεγκληματίες από τη Βραζιλία, οι οποίοι στέλνουν «μολυσμένες» προσκλήσεις οι οποίες οδηγούν σε κακόβουλα προγράμματα και bankingTrojans. Το συγκεκριμένο Trojan είναι .cmd και φιλοξενείται στο Dropbox.» [45]

Εκτός όμως από τα phishing attacks, την εμφάνισή τους, από τις πρώτες κιόλας μέρες λειτουργίας του, έκαναν και scams. Εκτός από τις ψεύτικες προσκλήσεις που αναφέραμε παραπάνω και είχαν ως σκοπό την απόκτηση προσωπικών πληροφοριών, πολλοί εκμεταλλεύτηκαν την μεγάλη επιθυμία των χρηστών να γίνουν μέλη στο νέο κοινωνικό δίκτυο και δημιούργησαν ψεύτικες σελίδες στις οποίες ο χρήστης είχε δυο επιλογές. Είτε να κατεβάσει ένα αρχείο το οποίο περιείχε την πρόσκληση απαντώντας σε κάποιες ερωτήσεις,

είτε να πληρώσει ένα μικρό αντίτιμο και να το αποκτήσει. Φυσικά, οι χρήστες και στις δυο περιπτώσεις εξαπατούνταν, κατεβάζοντας κακόβουλο λογισμικό ή χάνοντας χρήματα. [46]

Εικόνα 41: Logo για Ασφάλεια στο Googleplus

Ακόμα μια λειτουργία που παρέχει το Googleplus στους χρήστες μπορεί να χρησιμοποιηθεί προς όφελος κάποιων. Στους κύκλους του ο χρήστης μπορεί να προσθέσει και άτομα τα οποία δεν έχουν λογαριασμό στο κοινωνικό δίκτυο, προσθέτοντας απλά το e-mailtους. Ιδανικό για πολλούς χρήστες, αλλά και για spammer αφού στο αίτημα που στέλνεται στο e-mailτου χρήστη μπορεί να προστεθεί και σύνδεσμος που οδηγεί σε κακόβουλες εφαρμογές.

Το Googleplus φημίζεται πολύ για τα λεγόμενα Hangouts όπου ο χρήστης μπορεί να συνομιλήσει σε πραγματικό χρόνο με κάποιον άλλο. Υπάρχει και η δυνατότητα βιντεο-κλήσης. Δημιουργήθηκε λοιπόν ένα κακόβουλο Plug-in για τη συγκεκριμένη λειτουργία το οποίο υποσχόταν στους χρήστες ότι θα τους παρείχε καλύτερη ποιότητα ήχου και εικόνας. Το πάτημα όμως στο σύνδεσμο δεν θα εγκαθιστούσε το Plug-in αλλά ένα εκτελέσιμο αρχείο το οποίο εισβάλει στον υπολογιστή του χρήστη. [47]

Τον Αύγουστο του 2011 ένα νέο είδος Trojanέκανε την εμφάνισή του σε κινητά τηλέφωνα και ονομάστηκε Nickspy.C αφού είχε πολλές ομοιότητες με τους Nickspy.Aκαι Nickspy.B. Η διαφορά του με τους άλλους δύο είναι ότι «μεταμφιέζεται» σε εφαρμογή Googleplus. Αυτός ο ιός Trojan μπορεί να διακόψει μια κλήση και δίνει τη δυνατότητα στον επιτιθέμενο να ακούσει κάποια ομιλία. Η εφαρμογή χρησιμοποιήθηκε από πολλούς χρήστες λόγω της μεγάλης απήχησης του Googleplus. Μετά τον εντοπισμό της, αφαιρέθηκε από τη λίστα εφαρμογών του Androidmarket. [48]

Μια κοινή επίθεση στους χρήστες της google είναι γνωστή ως freshFishinge-mailScam. Το 2011 το συγκεκριμένο Phishingscan έκανε την εμφάνισή του. Ένα ψεύτικο e-mail της μορφής «GoogleAccountStorageQuotaExhaustedon******@gmail.com», το οποίο παραπλάνησε αρκετούς και νόμιζαν ότι προέρχεται όντως από την google, ενημέρωνε τους χρήστες ότι δεν υπάρχει αρκετός αποθηκευτικός χώρος στο mail τους. Παράλληλα προέτρεπε τους χρήστες να κάνουν μια αναβάθμιση το οποίο θα αναβάθμιζε τον αποθηκευτικό χώρο. Ο σύνδεσμος που δινόταν τους οδηγούσε στην πραγματικότητα σε μία ψεύτικη σελίδα googlemail όπου έπρεπε να δώσουν τα στοιχεία του e-mailτους για να

συνεχίσουν. Δίνοντας οι χρήστες τα στοιχεία πρόσβασής τους στο googlemail έδιναν ταυτόχρονα πρόσβαση και στο Googleplus λογαριασμό τους. [49]

2.3.2 Κοινωνικά Προβλήματα

Νέες μεθόδους έχουν σκαρφιστεί τα δίκτυα παιδόφιλων χρησιμοποιώντας τα κοινωνικά δίκτυα. Στο Googleplus για παράδειγμα, όπως και σε άλλες σελίδες κοινωνικής δικτύωσης, δημιουργούνται ομάδες με θέμα την οικογένεια και την φροντίδα των παιδιών. Μέσα από αυτές τις σελίδες παρακινούν τους γονείς να αναρτήσουν φωτογραφίες των παιδιών τους, προκειμένου να συμμετέχουν σε διαγωνισμούς ή να δημιουργήσουν ένα μεγάλο κοινωνικό δίκτυο γονέων όπου θα μπορούν να μιλάνε για τα παιδιά τους και να ανταλλάζουν απόψεις. Οι φωτογραφίες όμως αυτών των παιδιών καταλήγουν τελικά σε αρχεία με παιδιά ημίγυμνα ή εντελώς γυμνά. Φωτογραφίες δηλαδή από βαπτίσεις ή από καλοκαιρινές διακοπές στη θάλασσα. Τελικά δημοσιεύονται σε σελίδες παιδικής πορνογραφίας. Δεν είναι λίγες οι φορές όπου οι πιο θρασείς τις ανεβάζουν ακόμα και στα κοινωνικά δίκτυα. Σύμφωνα με πληροφορίες που εξέδωσε η CEO της Internet Watch Foundation, Susan Hargreaves, η συγκεκριμένη τακτική είναι ευρέως διαδεδομένη, παραθέτοντας περισσότερα από 600 παραδείγματα, ενώ οι καταγγελίες που γίνονται σε καθημερινή βάση σοκάρουν. [50]

Ακόμα, οι παιδόφιλοι έχουν αφήσει στην άκρη τις γνωστές πρακτικές προσέγγισης. Καθώς οι συνομιλίες μεταξύ αγνώστων οι οποίες διεξάγονται μέσω Διαδικτύου αποκτούν ολοένα και πιο άμεσα σεξουαλικό περιεχόμενο, οι παιδόφιλοι επιλέγουν πλέον τα θύματά τους εντός «μόλις δύο λεπτών», σύμφωνα με έρευνα που πραγματοποιήθηκε στις συνομιλίες μέσω chat καταδικασμένων παιδόφιλων και η οποία παράλληλα βασίστηκε σε συνεντεύξεις με καταδικασμένους για σεξουαλικά εγκλήματα στη Βρετανία, το Βέλγιο και τη Νορβηγία. Οι παιδόφιλοι φαίνεται ότι έχουν αρχίσει να αφήνουν στην άκρη τις γνωστές πρακτικές προσέγγισης και πλέον, εκμεταλλεύονται την ανωνυμία και την κάλυψη που τους παρέχει το ίντερνετ για να τα προσεγγίσουν άμεσα και με καθαρά σεξουαλική διάθεση, και αν αποτύχουν, απλώς να περάσουν στο επόμενο υποψήφιο θύμα. Επεκτείνονται επίσης και σε πλατφόρμες παιχνιδιών για να στοχεύσουν εφήβους, κυρίως αγόρια.

2.3.3 Προσβολές Προσωπικότητας

Όπως και τα υπόλοιπα περιβάλλοντα κοινωνικής δικτύωσης έτσι και στο Googleplus συναντάμε περιπτώσεις προσβολής της προσωπικότητας αλλά και ρατσιστικών σχολίων.

Στο Googleplus όταν κάποιος χρήστης γράψει κάτι στην κατάστασή του, μπορεί να ξεκινήσει ένα Hangoutμε φράση κλειδί, αυτό που έχει αναρτήσει. Έτσι όταν κάποιος γράψει για παράδειγμα στην κατάστασή του ένα ρατσιστικό σχόλιο για μια ομάδα, μειονότητα ή ακόμα και για μεμονωμένα άτομα, μπορεί να ξεκινήσει ένα Hangout. Στο Hangoutμπορούν να συμμετέχουν και άλλα άτομα με ρατσιστικές αντιλήψεις.

Ακόμα, όπως έχουμε αναφέρει σε προηγούμενο κεφάλαιο τα πρόσωπα που έχει κάποιος στους κύκλους του, ή ακόμα και το όνομα του κύκλου, υπάρχει επιλογή να μην είναι ορατά από άλλους χρήστες. Αυτό έχει δώσει τη δυνατότητα σε πολλούς να δημιουργήσουν κύκλους, οι οποίοι θα έχουν μέλη ρατσιστές οι οποίοι μπορούν να επικοινωνούν και να σχολιάζουν ανενόχλητοι. Ακόμα να δημιουργηθεί κύκλος εναντίον κάποιου συγκεκριμένου προσώπου. Για παράδειγμα, έχουν τη δυνατότητα οι υπάλληλοι μια εταιρίας να δημιουργήσουν έναν κύκλο μέσα στον οποίο να προσβάλλουν το διευθυντή τους, ή τα παιδιά μιας τάξης να κοροϊδεύουν τη δασκάλα τους.

Η δυνατότητα που παρέχεται από την υπηρεσία της Google για ιδιωτικότητα και ελευθερία λόγου, χρησιμοποιείται από κάποιους για να δημιουργούν ρατσιστικές ομάδες και να προσβάλλουν μειονότητες με μυστικότητα.

2.4 Πνευματικά Δικαιώματα σε Περιβάλλοντα Κοινωνικής Δικτύωσης

Σε όλα τα περιβάλλοντα κοινωνικής δικτύωσης υπάρχει η ελευθερία ο κάθε χρήστης να μπορεί να αναρτά τραγούδια, βιντεοκλίπ, traileraπό ταινίες χωρίς να είναι υποχρεωμένος να ζητήσει την άδεια του ιδιοκτήτη. Σε groupγια παράδειγμα από θαυμαστές ενός τραγουδιστή, μπορεί το κάθε μέλος να ανεβάσει κάποιο τραγούδι του καλλιτέχνη, ή κάποιο απόσπασμα από κάποια συναυλία του που θέλησε να μοιραστεί με τα υπόλοιπα μέλη της ομάδας.

Σε ότι αφορά τους χρήστες του Facebook υπάρχει στους όρους χρήσης αποποίηση των πνευματικών δικαιωμάτων των χρηστών. Το Facebook αναπτύσσεται λόγω της πληρότητας των θέσεων που καταλαμβάνουν οι χρήστες του. Αυτό που πρέπει όμως να γνωρίζουμε είναι ότι ταχυδρομώντας οποιοδήποτε περιεχόμενο δίνουμε στο Facebook την άδεια να το χρησιμοποιήσει με όποιον τρόπο θέλει. Αναλυτικά μέσα στους όρους αναγράφεται το εξής:

> *«Με την ταχυδρόμηση περιεχομένου από εγγεγραμμένους χρήστες, από οποιαδήποτε περιοχή και μέρος, οι χρήστες χορηγούν αυτόματα και επιτρέπουν στην επιχείρηση Facebook, μια αμετάκλητη, διαρκή, μη αποκλειστέα, μεταβιβάσιμη, πλήρως πληρωμένη, παγκόσμια άδεια (με το δικαίωμα στο sublicense) να χρησιμοποιήσει, αντιγράψει, αποδώσει δημόσια, επιδείξει δημόσια, να επαναφορμάρει και να μεταφράσει, απόσπασμα (γενικά ή εν μέρει) και να διανείμει το περιεχόμενο χρηστών για οποιοδήποτε σκοπό σχετικά με τον ιστοχώρο ή την προώθησή του, να προετοιμάσει σχετικές παράγωγες εργασίες με τον ιστοχώρο, ή να ενσωματώσει άλλες, και να χορηγήσει και να εγκρίνει sublicenses των ανωτέρω.»*

Σε απλή γλώσσα, αυτό σημαίνει ότι οι χρήστες δεν ελέγχουν πλέον τα πνευματικά δικαιώματα του υλικού που εναποθέτουν στον ιστοχώρο του Facebook. Για παράδειγμα, εάν φορτώσετε μια φωτογραφία σας στο Facebook, πρέπει να γνωρίζετε με βάση όσα αναγράφονται στους όρους ότι το Facebook μπορεί να δημιουργήσει αντίγραφά της και να τα πουλήσει έναντι πληρωμής ή μη, σε τρίτους χωρίς την άδειά σας ως προωθητική ενέργεια. Εάν κρατάτε κάποια προσωπικά στοιχεία στο Facebook ή προσωπικές σκέψεις, το Facebook μπορεί να τις μετατρέψει σε βιβλίο, να δημιουργήσει αντίγραφα και να τα προωθήσει στην αγορά.

Τον Ιανουάριο του 2012 ένα γεγονός συντάραξε το διαδίκτυο, επομένως και τις σελίδες κοινωνικής δικτύωσης. Δυο νομοσχέδια κατατέθηκαν στο Κογκρέσο προς ψήφιση. Το SOPA (Stop Online Piracy Act – Νομοσχέδιο για την Παύση της Διαδικτυακής Πειρατείας) στην βουλή και το PIPA (Protect Intellectual Property Act – Νομοσχέδιο για την Προστασία της Πνευματικής Ιδιοκτησίας) στη γερουσία. Το διαδίκτυο δεν θα ήταν ίδιο σε περίπτωση ψήφισης του νομοσχεδίου. Συγκεκριμένα οι σελίδες κοινωνικής δικτύωσης θα πλήττονταν ανεπανόρθωτα αφού πλέον οι χρήστες δεν θα μπορούσαν να ανεβάζουν, μουσική, βίντεο, να σχολιάσουν με ελευθερία λόγου και πολλά άλλα. Τελικά τα νομοσχέδια και μετά την αντίδραση του κόσμου καταψηφίστηκαν.

Εικόνα 42: Stop SOPA and PIPA

Κεφάλαιο 3: Νομοθεσία

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μαζί όμως με τις αλλαγές αυτές που διευκολύνουν, προάγουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής και στην τάχιστη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνίας, οι νέες τεχνολογίες και το Ιντερνετ διευκόλυναν και δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας που συνοψίζονται στον όρο Ηλεκτρονικό Έγκλημα. Μέσα στο οποίο εντάσσεται και το Διαδικτυακό Έγκλημα. Οι δύο έννοιες διαφέρουν στον τόπο που διαπράττεται το έγκλημα.

Υπάρχουν πολλές μορφές κυβερνοεγκλήματος. Σύμφωνα με τα αποτελέσματα έρευνας που διεξήγαγε η McConnell International σε 52 χώρες, με τίτλο «Cyber Crime... and Punishment» κατατάσσει τα αδικήματα που διαπράττονται στον Κυβερνοχώρο στις παρακάτω δέκα κατηγορίες: Παρεμπόδιση (κυβερνο)κυκλοφορίας, Τροποποίηση και Κλοπή δεδομένων, Εισβολή και Σαμποτάζ σε δίκτυο, Μη εξουσιοδοτημένη πρόσβαση, Διασπορά ιών, Υπόθαλψη αδικημάτων, Πλαστογραφία και Απάτη.

Οι μορφές του Ηλεκτρονικού Εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα(Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα Ηλεκτρονικά Εγκλήματα. Μέσα σε αυτές τις ρυθμίζεις περιλαμβάνονται και τα περιβάλλοντα κοινωνικής δικτύωσης από τη στιγμή που είναι αδιάσπαστο κομμάτι του διαδικτύου. Στη συνθήκη της Βουδαπέστης γίνεται αναφορά

1. Για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ. Τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών.

2. Για τα αδικήματα που σχετίζονται με τους υπολογιστές όπως η απάτη με η/υ και πλαστογραφία.

3. Για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας

4. Για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας

Επίσης η συνθήκη περιέχει ρυθμίσεις για την συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζει την αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγει το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η συνθήκη αυτή αποτελεί το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή ένωση.

Υπάρχουν φυσικά και άλλα γενικά νομοθετήματα που βοηθούν στην καταπολέμηση του Ηλεκτρονικού εγκλήματος . Στην Ευρωπαϊκή Ένωση ισχύουν :

1.Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας,

2.Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών

3.Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.

4.Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.

5.Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων

6.Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.

7.Το Σχέδιο Δράσης με αριθμό 97/C 251/01για την καταπολέμηση του οργανωμένου εγκλήματος

Οι διάφορες μορφές του ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και στην Ευρωπαϊκή Ένωση. Ειδικότερα αναλύονται οι εξής μορφές:

Παράνομη διείσδυση σε δεδομένα (hacking, cracking)- Προστασία του απορρήτου στο Διαδίκτυο

Hacking αποτελεί η μη εξουσιοδοτημένη πρόσβαση σε ξένο υπολογιστή ή συστήματα υπολογιστών η οποία καταρχήν δε γίνεται με το σκοπό της υποκλοπής, της καταστροφής ή της κατασκοπείας αλλά για την ικανοποίηση από την επιτυχία παράκαμψης των συστημάτων ασφαλείας των Η/Υ.

Cracking είναι η αλλαγή των κωδίκων πρόσβασης και η άρση της προστασίας των προγραμμάτων, η οποία καθιστά δυνατή την παράνομη αντιγραφή τους.

Η χωρίς δικαίωμα διείσδυση –πρόσβαση σε συστήματα επεξεργασίας δεδομένων έστω και όταν γίνεται χωρίς πρόθεση βλάβης τιμωρείται με το άρθρο 370Γ του Ποινικού κώδικα. Στην Ευρωπαϊκή Ένωση δεν έχουν ακόμα ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του hacking αλλά έχουν ήδη αρχίσει οι προπαρασκευαστικές εργασίες για την δημιουργία τους. Αυτά είναι:

1.Η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά για τη μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών, μνεία στις ζημιές που μπορούν να προκληθούν και παράθεση πιθανών λύσεων

2. Πρόταση Κανονισμού με αριθμό 2003.0063 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών στόχος του οποίου θα είναι να διευκολύνει την εφαρμογή των κοινοτικών μέτρων σχετικά με την ασφάλεια δικτύων και πληροφοριών και να συμβάλλει στη διασφάλιση της διαλειτουργικότητας των λειτουργιών ασφαλείας στα δίκτυα και τα συστήματα πληροφοριών.

3. Πρόταση Απόφασης Πλαισίου του Συμβουλίου με αριθμό COM/2002/0173 - CNS 2002/0086 για τις επιθέσεις κατά των συστημάτων πληροφοριών όπου στοιχειοθετείται το αδίκημα της επίθεση μέσω παράνομης πρόσβασης σε συστήματα πληροφοριών και γίνεται αναλυτική αναφορά στο τι αποτελεί παράνομη παρεμβολή σε συστήματα πληροφοριών

Ιοι- Προστασία των δεδομένων από ιούς

Μια ιδιαίτερα συχνή και επικίνδυνη μορφή εγκληματικότητας που εμφανίζεται στο διαδίκτυο είναι η αλλοίωση ή διαγραφή των δεδομένων με ιούς. Οι ιοί των υπολογιστών είναι ειδικά προγράμματα που έχουν την ικανότητα να ανατυπώνονται από μόνα τους. Διακρίνονται σε δύο μορφές: στους ιούς των προγραμμάτων και στους ιούς των συστημάτων. Η παρεμβολή ιών στο πρόγραμμα ενός υπολογιστή γεννά την αστική ευθύνη του προμηθευτή και κάθε υπαιτίου και τη συμβατική ευθύνη του προμηθευτή του προγράμματος εφόσον υπάρχει πώληση προγράμματος. Σε αυτές τις περιπτώσεις εφαρμόζονται τα άρθρα 577 και 578 του ΑΚ. Επίσης γεννά και αδικοπρακτική ευθύνη του δράστη κατά τα άρθρα 914, 919 ΑΚ. Ο υπαίτιος όμως υπέχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 ΠΚ. Στην Ευρωπαϊκή Ένωση υπάρχει η Ανακοίνωση της Επιτροπής με αριθμό COM/2001/0298 για την ασφάλεια δικτύων και πληροφοριών όπου γίνεται αναλυτική αναφορά και λεπτομερής επεξήγηση της έννοιας του ιού, του τρόπου που λειτουργεί και των τρόπων αντιμετώπισης του. Το νομοθέτημα αυτό δεν έχει ακόμα ψηφιστεί ώστε να ισχύει.

Εγκλήματα κατά της ηθικής και της αξιοπρέπειας-Προστασία ανηλίκων-Προστασία από παράνομο και βλαβερό περιεχόμενο

Παράνομο και βλαβερό περιεχόμενο που θίγει την προσωπικότητα και την ηθική των ατόμων αποτελούν η δυσφήμηση μέσω του διαδικτύου και η διάδοση πορνογραφικού υλικού. Ο προσβληθείς στην προσωπικότητα του από κάποιο μήνυμα που διακινείται στο Διαδίκτυο προστατεύεται από τις διατάξεις 361, 362, 366 και 367 του Π.Κ. Δυσχερέστερο

είναι το ζήτημα της διάδοσης πορνογραφικού υλικού στο διαδίκτυο ιδιαίτερα σε σχέση με τους ανηλίκους και την προστασία τους από την έκθεση σε αυτό.

Στην Ευρωπαϊκή Ένωση έχουν ληφθεί και ισχύουν αρκετά μέτρα για την αντιμετώπισης αυτού του είδους εγκληματικότητας.

1.Η Απόφαση του Συμβουλίου με αριθμό 2000/C 8/06 που περιέχει προτροπές του Συμβουλίου προς τα κράτη μέλη και την Επιτροπή ώστε να ληφθούν μέτρα για την προστασία των ανηλίκων στα οπτικοακουστικά μέσα και στο Ιντερνετ,

2.Η Σύσταση με αριθμό 98/560/ΕΚ όπου αναφέρονται οι συστάσεις του Συμβουλίου στα κράτη μέλη για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις οπτικοακουστικές υπηρεσίες και τις υπηρεσίες πληροφόρησης,

3.Η Απόφαση του Συμβουλίου με αριθμό 2000/375/ΔΕΥ όπου γίνεται λόγος για τα μέτρα που λαμβάνουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης ώστε οι χρήστες του διαδικτύου να βοηθήσουν στην ποινική δίωξη της παραγωγής, επεξεργασίας, διανομής και κατοχής πορνογραφικού υλικού με θέμα παιδιά,

4.Η Απόφαση του Συμβουλίου με αριθμό 2001/C 213/0301 όπου υπάρχουν οι προτροπές του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη για την προστασία των ανηλίκων σε όλα τα οπτικοακουστικά μέσα και για την προστασία των ανηλίκων στο ψηφιακό περιβάλλον και με την συμμετοχή των γονέων,

5.Η Απόφαση του Συμβουλίου με αριθμό 1999/C 362/06 όπου αναφέρεται ότι τα κράτη μεταξύ τους πρέπει να συνεργάζονται ώστε να διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη ποινικών αδικημάτων που αφορούν την παιδική πορνογραφία στο Ίντερνετ,

6.Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 65/02 για την αξιολόγηση του περιεχομένου των βιντεοπαιχνιδιών και των ηλεκτρονικών παιχνιδιών

7.Η Απόφαση 276/1999/ΕΚ για την έγκριση, την διάρκεια, τη χρηματοδότηση και τους στόχους προγράμματος για την προώθηση της ασφαλέστερης χρήσης του Ίντερνετ,

8.Η Απόφαση 1151/2003/ΕΚ που τροποποιεί την απόφαση αριθ. 276/1999/ΕΚ

9.Η Ανακοίνωση της Επιτροπής COM/2002/0152 για τα επακόλουθα μέτρα παρακολούθησης του πολυετούς κοινοτικού προγράμματος δράσης για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα

Ένα ακόμα ζήτημα που τίθεται σχετικά με την χρήση του διαδικτύου από τους ανήλικους είναι η πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα. Είναι γνωστό ότι οποιαδήποτε συναλλαγή με ανήλικο είναι άκυρη και μπορεί να επισύρει ποινή για τον αντισυμβαλλόμενο εφόσον το περιεχόμενό της δεν απευθύνεται σε παιδία και εφήβους. Στην περίπτωση όμως των ηλεκτρονικών συναλλαγών δεν είναι πάντα δυνατή η εξακρίβωση των στοιχείων του καταναλωτή. Για την προστασία των προμηθευτών που δραστηριοποιούνται μέσω κάποιας ιστοσελίδας είναι απαραίτητη η αναγραφή στους όρους χρήσης του site ότι δεν επιτρέπονται οι συναλλαγές με ανηλίκους και ότι η ιστοσελίδα δεν φέρει καμία ευθύνη.

Προστασία δεδομένων προσωπικού χαρακτήρα

Η συγκέντρωση και επεξεργασία ηλεκτρονικών δεδομένων αντιμετωπίστηκε από πολύ νωρίς ως ένας από τους μεγαλύτερους κινδύνους επέμβασης στην ιδιωτική και προσωπική σφαίρα. Τόσο στην Ελλάδα όσο και στην Ευρωπαϊκή Ένωση υπάρχει νομοθεσία που ρυθμίζει τα σχετικά με την επεξεργασίας δεδομένων όπως η Οδηγία 2002/58 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και η Οδηγία 95/46 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού.

Απάτη μέσω του Διαδικτύου

Από τη σκοπιά του ποινικού δικαίου κατά τη χρήση του Διαδικτύου είναι δυνατό να τελεστούν απάτες μέσω υπολογιστή όπου ο υπολογιστής είναι απλώς το μέσω τέλεσης της κοινής απάτης (ΠΚ 386) αλλά και απάτες με υπολογιστή όπου το οικονομικό όφελος ή ζημιά προκύπτει με απευθείας παρέμβαση στον υπολογιστή στο πρόγραμμα και στα δεδομένα του (ΠΚ 386Α). Στην Ευρωπαϊκή ένωση ισχύει η Απόφαση-πλαίσιο του Συμβουλίου με αριθμό 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών .

Spamming

Το μεγαλύτερο πρόβλημα που αφορά στις διαδικτυακές διαφημίσεις είναι το λεγόμενο spamming, δηλαδή η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο σε

χιλιάδες καταναλωτές-χρήστες του διαδικτύου . Η τακτική αυτή απαγορεύεται από την Οδηγία 2002.58 όπου στο άρθρο 13 αναφέρεται ότι « η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπικών συσκευών (φαξ) ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους» καθώς και από άλλα νομοθετήματα. Στην Ελλάδα υπάρχουν πολλά νομοθετήματα για την προστασία των καταναλωτών αλλά αναφέρονται στα μηνύματα μέσω τηλεφώνου και φαξ κυρίως και μόνο αναλογικά στο ηλεκτρονικό ταχυδρομείο.

Προστασία της Πνευματικής Ιδιοκτησίας

Η εμφάνιση των βάσεων δεδομένων σε συνδυασμό με τη διάδοση του Διαδικτύου έχει κάνει την αντιγραφή και την ηλεκτρονική διάδοση των πνευματικών δημιουργημάτων αποτελεσματική και εξαιρετικά απλή. Με τον τρόπο αυτό όμως καταστρατηγούνται τα δικαιώματα της πνευματικής ιδιοκτησίας των δημιουργών πάνω στα δημιουργήματά τους. Λεπτομερειακή ανάλυση των τρόπων προστασίας της πνευματικής ιδιοκτησίας υπάρχει στο σχετικό θέμα.

Δικαιοδοσία στο Ιντερνετ

Το πρόβλημα της δικαιοδοσίας στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες.

Α) Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης του αδικήματος θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθει η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, ο τόπος όπου ολοκληρώθηκε.

Β) Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως του αδικήματος θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

Γ) Η μικτή θεωρία, όπου ως τόπος τελέσεως του αδικήματος θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

Δ) Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της διαδικτυακής αδικοπραξίας.

Το Facebook συγκεκριμένα είναι το πρώτο socialnetwork που τέθηκε σε εποπτεία 20 χρόνων για ζητήματα ιδιωτικότητας. Η διαμάχη ξεκίνησε όταν η ΟΕΕ ανακάλυψε ότι το Facebook έχει παραβιάσει τις δεσμεύσεις του προς τους χρήστες σχετικά με ποια δεδομένα τους μοιράζονται μαζί με τρίτους. Εκτός από τη συμφωνία για την εποπτεία το Facebook δεσμεύθηκε ότι θα προσλάβει προσωπικό με ειδίκευση σε θέματα ιδιωτικότητας για τη συγκρότηση ενός ολοκληρωμένου προγράμματος προστασίας της ιδιωτικής ζωής των χρηστών του. Επίσης από εδώ και στο εξής η υπηρεσία θα πρέπει να λαμβάνει τη ρητή συγκατάθεση των χρηστών της πριν πραγματοποιήσει οποιαδήποτε αλλαγή στις ήδη υπάρχουσες ρυθμίσεις ιδιωτικότητας και τέλος όλα τα προσωπικά δεδομένα του χρήστη θα πρέπει να διαγράφονται ολοκληρωτικά με το πέρας 30 ημερών από την διαγραφή του λογαριασμού του χρήστη.

Κεφάλαιο 4: Θέσπιση κανόνων ασφαλείας

4.1 Από την πλευρά του χρήστη

Οι σελίδες κοινωνικής δικτύωσης όπως αναφέρθηκε εγκυμονούν πολλούς κινδύνους. Έτσι οι χρήστες θα πρέπει να ακολουθήσουν κάποιους κανόνες ασφαλείας για να μπορέσουν να αντιμετωπίσουν ανεπιθύμητες καταστάσεις. Έτσι από τη στιγμή που ξέρουμε πώς να προστατευτούμε δεν υπάρχει πρόβλημα να χρησιμοποιήσουμε οποιαδήποτε σελίδα κοινωνικής δικτύωσης. Όπως ισχύει σε κάθε μορφή ηλεκτρονικής επικοινωνίας, έτσι και στους ιστοχώρους κοινωνικής δικτύωσης, η γνώση θεμελιωδών κανόνων ασφάλειας και η ανάπτυξη κριτικής σκέψης είναι καθοριστικοί παράγοντες στην προστασία μας από κακόβουλους ανθρώπους, απατεώνες ή ακόμα και από ασυνείδητους επιχειρηματίες, ώστε να μπορέσουμε να απολαύσουμε τις άπειρες δυνατότητες ψυχαγωγίας, επικοινωνίας και διασκέδασης που μας παρέχονται.

Αρχικά ο κάθε χρήστης θα πρέπει να βεβαιωθεί ότι το προσωπικό του προφίλ στην εκάστοτε σελίδα είναι προσβάσιμο μόνο από φίλους του. Με αυτό τον τρόπο τα προσωπικά του δεδομένα δεν θα είναι διαθέσιμα και σε τρίτους που μπορεί να τα χρησιμοποιήσουν προς όφελός τους.

Ο κωδικός πρόσβασης είναι προσωπικός και θα πρέπει να παραμένει μυστικός. Αφού όποιος αποκτά πρόσβαση στο εικονικό προφίλ μπορεί να διαχειριστεί πλήρως όλα τα δεδομένα που εμφανίζονται σε αυτό.

Το ανέβασμα φωτογραφιών στο διαδίκτυο πρέπει να γίνεται προσεκτικά, δηλαδή επιλέγουμε ποιες φωτογραφίες θα διαθέσουμε στο ιντερνέτ. Δεν μοιραζόμαστε φωτογραφίες στις οποίες φαίνεται καθαρά η τοποθεσία η οποία βρισκόμαστε και ιδιαίτερα όταν αυτή η τοποθεσία είναι το σπίτι μας, το σχολείο μας ή μέρη που μαζευόμαστε για να διασκεδάσουμε. Έτσι μειώνονται οι πιθανότητες εντοπισμού μας στον φυσικό κόσμο.

Απαιτείται προσοχή στην επιλογή των φίλων μας. Δηλαδή η αποδοχή σε «friendrequest» δίνει την πρόσβαση στον άλλο χρήστη σε όλα τα προσωπικά δεδομένα που υπάρχουν στο προφίλ. Φωτογραφίες, στοιχεία επικοινωνίας, λίστα φίλων και πολλά άλλα.

Οι διαδικτυακοί φίλοι καλό είναι να μένουν φίλοι μόνο εκεί. Ποτέ να μην γίνεται δεκτή η συνάντηση με κάποιο άτομο που γνωρίσαμε σε κάποια σελίδα κοινωνικής δικτύωσης. Παράλληλα αν δεχτεί κάποιος οποιοδήποτε είδος εκφοβισμού ή απειλής πρέπει να

σταματήσει επιτόπου την επικοινωνία με το θύτη, ειδικά αν πρόκειται για ανήλικο, και να κάνει καταγγελία στην αστυνομία, ή σε κάποια από τις γραμμές υποστήριξης που υπάρχουν για τέτοιες περιπτώσεις.

Επιπλέον, πρέπει όλοι να θυμόμαστε ότι ακόμα και μετά τη διαγραφή του προσωπικού μας προφίλ, οι πληροφορίες δεν αφαιρούνται και ενδέχεται να τις συναντήσουμε και σε άλλες σελίδες στο διαδίκτυο.

Τέλος, μεγάλη προσοχή επιβάλλεται να δείξουν γονείς με ανήλικα παιδιά. Η απαγόρευση συνήθως οδηγεί σε άκρως αντίθετα αποτελέσματα επομένως δεν είναι λύση. Το παιδί μπορεί να χρησιμοποιεί το διαδίκτυο με την παρουσία του γονέα και έτσι να κατανοούν αμφότεροι το είδος των δραστηριοτήτων που λαμβάνουν χώρα. Σύμμαχος είναι η ενημέρωση για επιμέρους κινδύνους και απειλές και η συζήτησή τους με το παιδί.

4.2 Από την πλευρά των ιστοσελίδων

Όπως οι χρήστες πρέπει να προσέξουν κάποια πράγματα για την προσωπική τους ασφάλεια έτσι και τα κοινωνικά δίκτυα πρέπει από την πλευρά τους να υποστηρίξουν το χρήστη με κάποιες ενέργειες έτσι ώστε να του παρέχουν τη μέγιστη ασφάλεια.

Αρχικά θα μπορούσε να γίνει μια μελέτη για την καλύτερη λειτουργία των ρυθμίσεων ασφαλείας. Για παράδειγμα η δημιουργία ενός βίντεο που θα προσκαλούσε το χρήστη να δει τι κινδύνους μπορεί να συναντήσει σε ένα τέτοιο περιβάλλον, καθώς και τρόπους που θα προστατευτεί, αφού πολλές φορές κάποιος μπορεί να βαρεθεί να διαβάσει, ή ακόμα και να μην κατανοήσει τις γραπτές οδηγίες που ήδη προσφέρονται.

Ακόμα, μια επιλέον ιδέα θα ήταν η πρόσκληση σε σεμινάρια στα οποία οι χρήστες θα μπορούσαν να δουν τις δυνατότητες που παρέχονται από τις ιστοσελίδες, οδηγίες χρήσης, και οδηγίες για την αποφυγή δυσάρεστων εκπλήξεων όπως η κλοπή προσωπικών τους δεδομένων που αναφέραμε παραπάνω.

Επιπλέον, από τη στιγμή που υπάρχουν πολλοί χρήστες οι οποίοι χρησιμοποιούν ψεύτικα προφίλ με σκοπό την εξαπάτηση και την προσβολή άλλων χρηστών θα μπορούσαν τα περιβάλλοντα κοινωνικής δικτύωσης να βρουν έναν τρόπο να πιστοποιήσουν αν όντως ένα προφίλ ανήκει στο άτομο που το διαχειρίζεται. Είναι μια διαδικασία βέβαια σχεδόν αδύνατη, αφού οι χρήστες είναι εκατοντάδες εκατομμύρια ανά τον κόσμο, αλλά παραμένει εφικτή αν υπάρξει συνεργασία από όλους τους χρήστες. Μπορεί ακόμα να δημιουργηθεί ένας μηχανισμός επαλήθευσης (κάτι που ήδη έχει κάνει το Twitter και το Googleplus αλλά μόνο για επώνυμους χρήστες) σύμφωνα με τον οποίο κάθε γνήσιο προφίλ φέρει ένα ειδικό σήμα, το οποίο πιστοποιεί ότι ο συγκεκριμένος λογαριασμός ανήκει πράγματι στο πρόσωπο το οποίο εκπροσωπεί.

Ένα μείζον πρόβλημα είναι «οι τρύπες» που μπορεί να έχει ο κώδικας της σελίδας και κάνει εφικτές τις επιθέσεις από κακόβουλους χρήστες με αποτέλεσμα τη δυσαρέσκεια των υπόλοιπων. Θα πρέπει λοιπόν οι ομάδες ασφαλείας να κάνουν περισσότερους και πιο προσεκτικούς ελέγχους. Εδώ μπορούν οι εταιρίες να προσκαλέσουν και τους χρήστες, επικηρύσσοντας έναντι χρηματικής αμοιβής, την αναφορά λαθών που θα μπορούσαν να οδηγήσουν σε κάποιο κενό ασφαλείας.

Τέλος, ο σημαντικότερος κίνδυνος για την ιδιωτικότητα είναι η απειλή «εκ των έσω». Οι εταιρίες κοινωνικής δικτύωσης πουλάνε τα προσωπικά δεδομένα των χρηστών σε

διαφημιστικές εταιρίες και σε εταιρίες ανάλυσης δεδομένων. Θα έπρεπε τα κοινωνικά δίκτυα να αντλήσουν από άλλες πηγές έσοδα, όπως τα παιχνίδια, κάποια τυχόν ηλεκτρονικά δωράκια που θα μπορεί να στέλνει ο ένας χρήστης στον άλλο και σε κάποιες τυχόν επιπλέον υπηρεσίες, όπως φωτογραφίες προφίλ μεγαλύτερης ανάλυσης έναντι αμοιβής. Ωστόσο και πάλι είναι αδύνατο για τα κοινωνικά δίκτυα να χάσουν τα έσοδα από τις διαφημίσεις αφού είναι και η μεγαλύτερη πηγή εσόδων.

Κεφάλαιο 5: Συμπεράσματα

Εξετάζοντας τα κοινωνικά δίκτυα προκύπτει το ερώτημα : είναι μια τάση της εποχής και πρόσκαιρο φαινόμενο της ; « Τα μέχρι τώρα στοιχεία δείχνουν ότι δεν υπάρχει αμφιβολία πως είναι κάτι που θα συνεχίσει να αυξάνεται και να παγιώνεται, τα ποσοστά χρήσης και συμμετοχής στην Ελλάδα και σε παγκόσμιο επίπεδο είναι εντυπωσιακά».

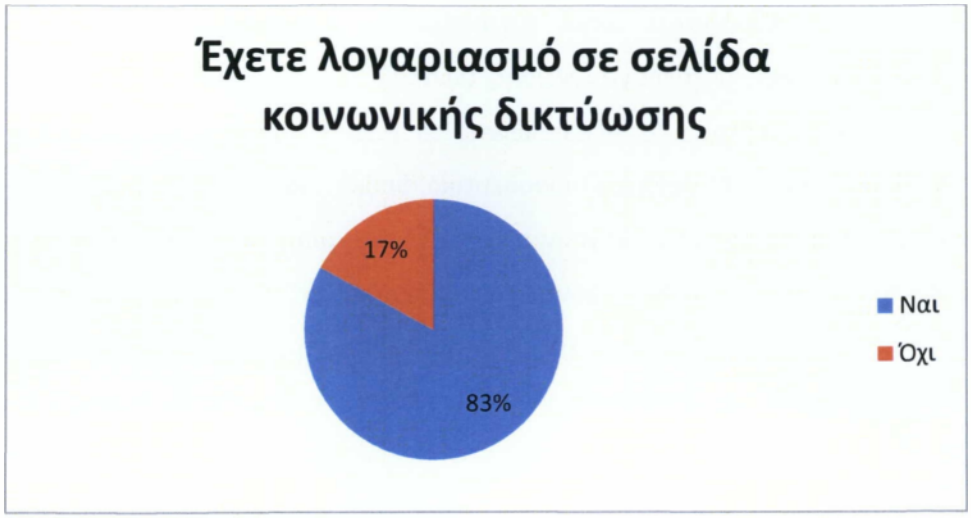
Όλοι αυτοί οι διαδικτυακοί τόποι προσφέρουν επικοινωνία, νέες φιλίες και επαγγελματικές επαφές, ανταλλαγή γνώσης, ζωντανή (online) υποστήριξη, διασκέδαση, πλασάρονται ως νεωτερισμός, αξιοποιώντας το γνωστό ιδεολόγημα ότι καθετί που εμφανίζεται ως νέο είναι εξ ορισμού προοδευτικό, θετικό, χρήσιμο, έως και απαραίτητο. Όμως, αν στην πραγματικότητα οδηγούν σε μεγαλύτερη απομόνωση ή αποξένωση στον πραγματικό κόσμο, τον πιο ενδιαφέροντα και σημαντικό απ' όλους, αν βάζουν εμπόδια στον αγώνα για την κοινωνική αλλαγή, τότε δεν θα πρέπει να χαρακτηριστούν ως κάτι νέο και προοδευτικό, αλλά ως οπισθοδρόμηση με περιβολή καινοτομίας. Οι εικονικοί κόσμοι, μεγαλύτεροι τάχα, αλλά στην πραγματικότητα μικρόκοσμοι, με ύπαρξη δανεική και ελεγχόμενη, κανείς δεν πρέπει να τους αγνοεί, επηρεάζουν ήδη εκατομμύρια ανθρώπων. Χρειάζεται ενημέρωση των παιδιών αλλά και των μεγαλύτερων, γονιών και μη. Γνώση των κινδύνων και των συνεπειών και σωστή αξιολόγηση των «ωφελημάτων». Γνώση που θα οδηγήσει στην αποδοχή ή πιθανότατα στην απόρριψη, κόντρα στο ρεύμα.

Προηγούμενες έρευνες των κοινωνικών δικτύων είχαν αγνοήσει το γεγονός ότι πρόκειται για υψηλής δυναμικής συστήματα. Για να διορθωθεί αυτό θα πρέπει οι μελλοντικές έρευνες να αντικατασταθούν από νέες μεθόδους. Για παράδειγμα ,ενώ υπήρξε μια αρχική πρόοδος χρησιμοποιώντας δειγματοληψία για να μετρήσουν την ετερογένεια και τη δυναμική των γραφημάτων, η κατά κύριο λόγο άγνωστη φύση του πραγματικού κόσμου των κοινωνικών δικτύων, παραμένει το κύριο εμπόδιο για την εξαγωγή πληροφοριών. Αν δεν ξεπεραστεί αυτό το πρόβλημα, οι μελλοντικές μετρήσεις θα συνεχίσουν να είναι χωρίς γερά θεμέλια αναγκαία για μια εις βάθος κατανόηση των κοινωνικών δικτύων.

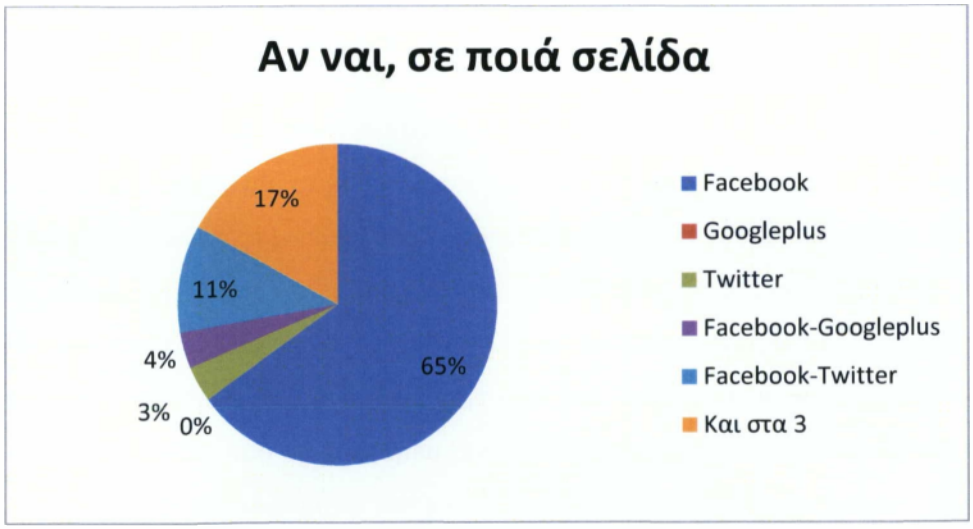
Έρευνα

Πραγματοποιήθηκε μικρή έρευνα σε 100 άτομα, ηλικίας 16 έως 77 με ερωτήσεις που αφορούν τις σελίδες κοινωνικής δικτύωσης. Η έρευνα σπάει και σε μικρότερα κομμάτια, βασισμένα στις ηλικίες των ερωτηθέντων. Αυτά είναι: έως 20 χρονών, 21-30 χρονών, 31-45 χρονών και 46-77 χρονών.

Σύνολο:



Ναι: 83 Όχι: 17

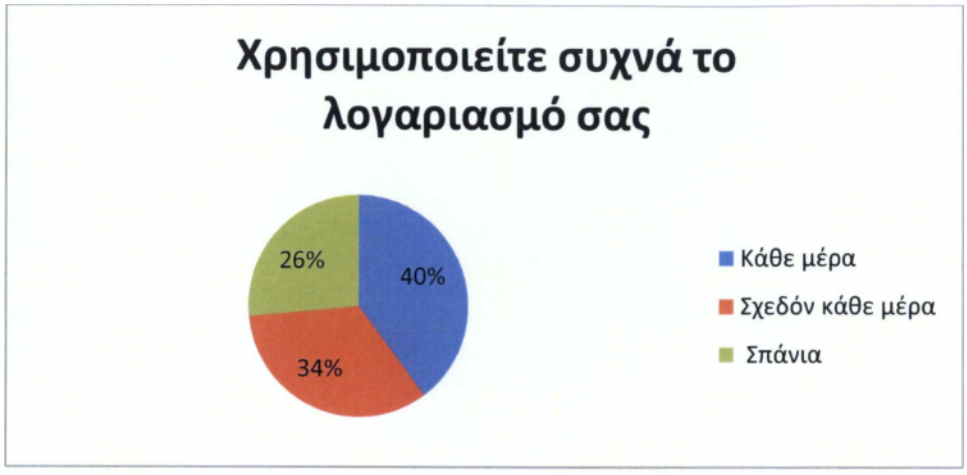


Facebook: 54 Googleplus: 0 Twitter: 3

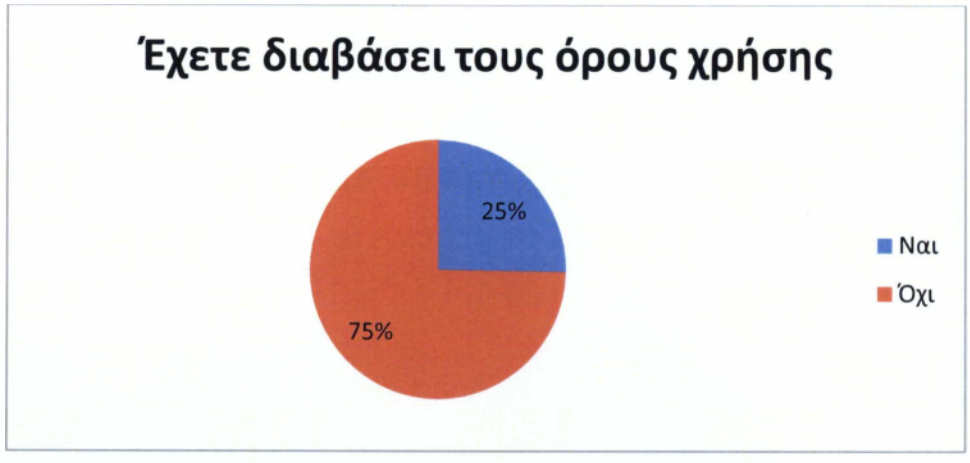
Facebook-Googleplus: 3

Facebook-Twitter: 9

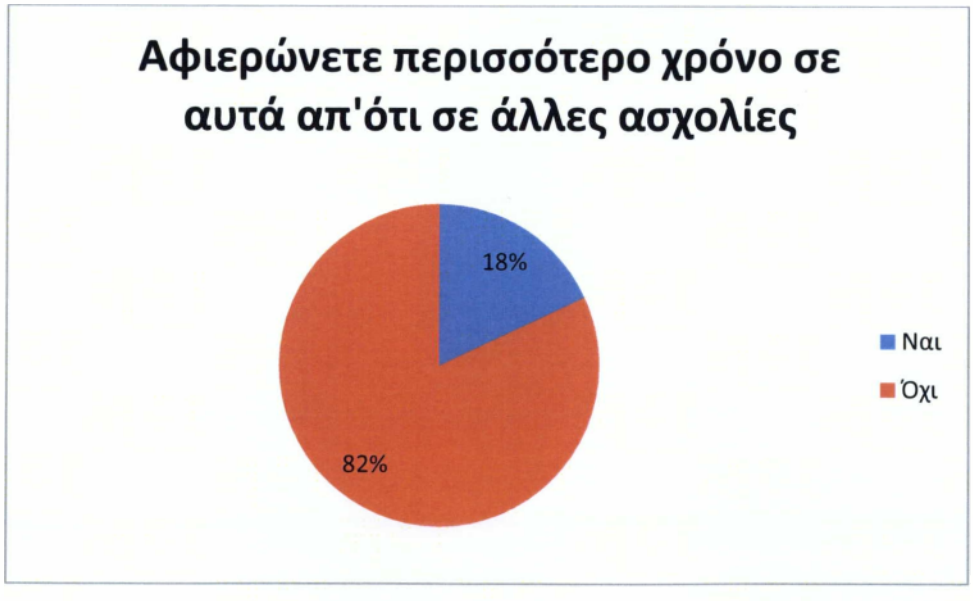
Και στα 3: 14



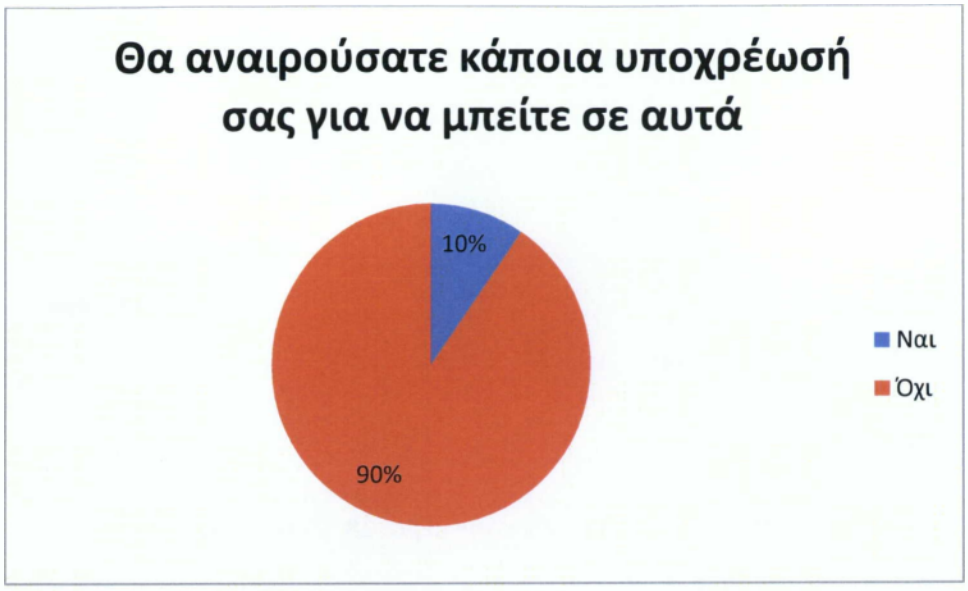
Κάθε μέρα: 33 Σχεδόν κάθε μέρα: 28 Σπάνια: 22



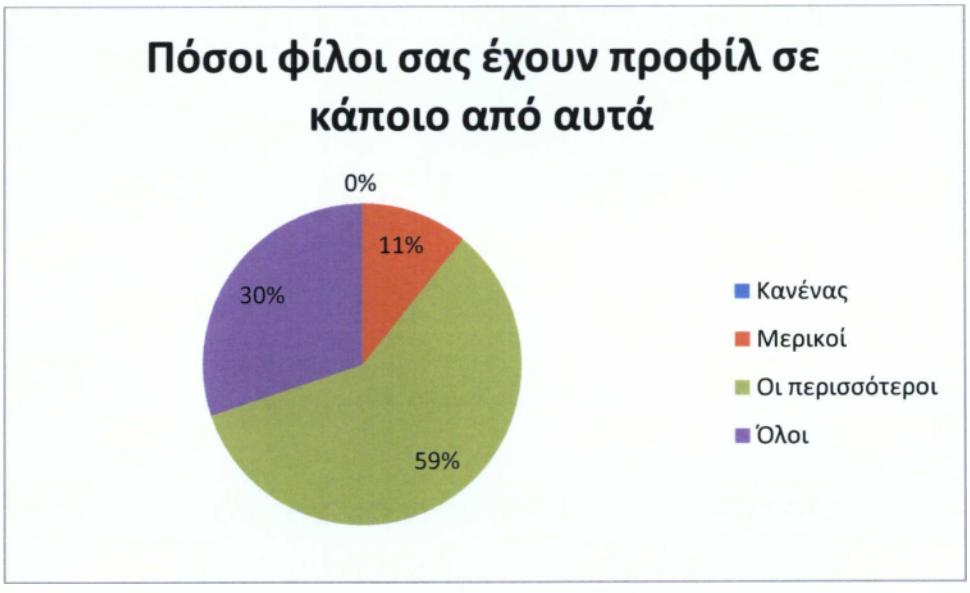
Ναι: 21 Όχι: 62



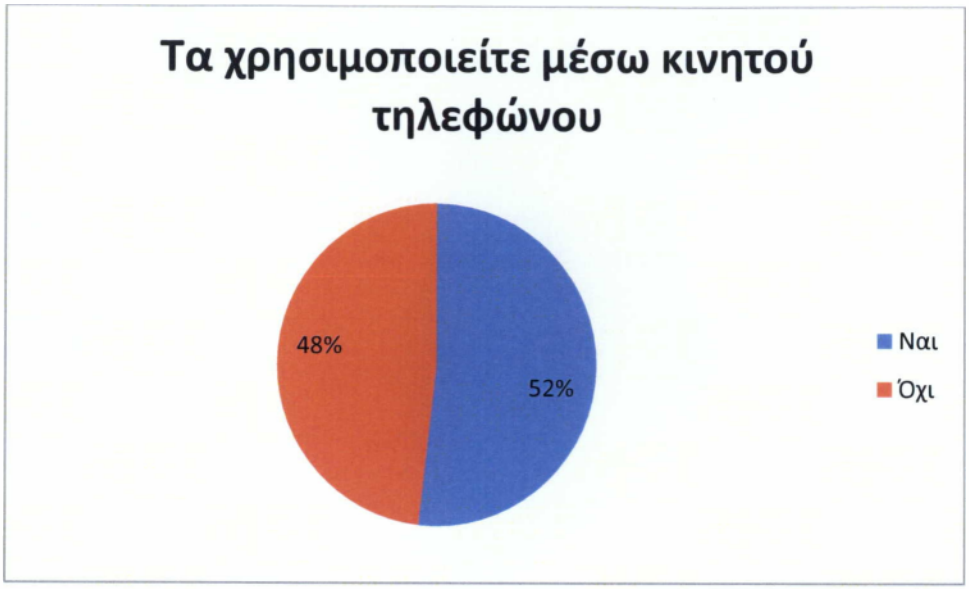
Ναι: 15 Όχι: 68



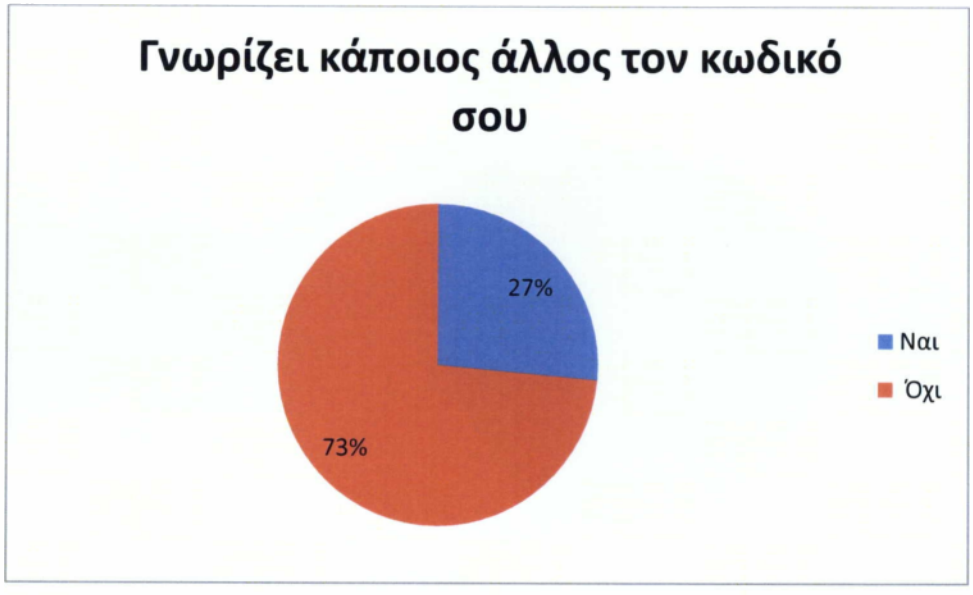
Ναι: 8 Όχι: 75



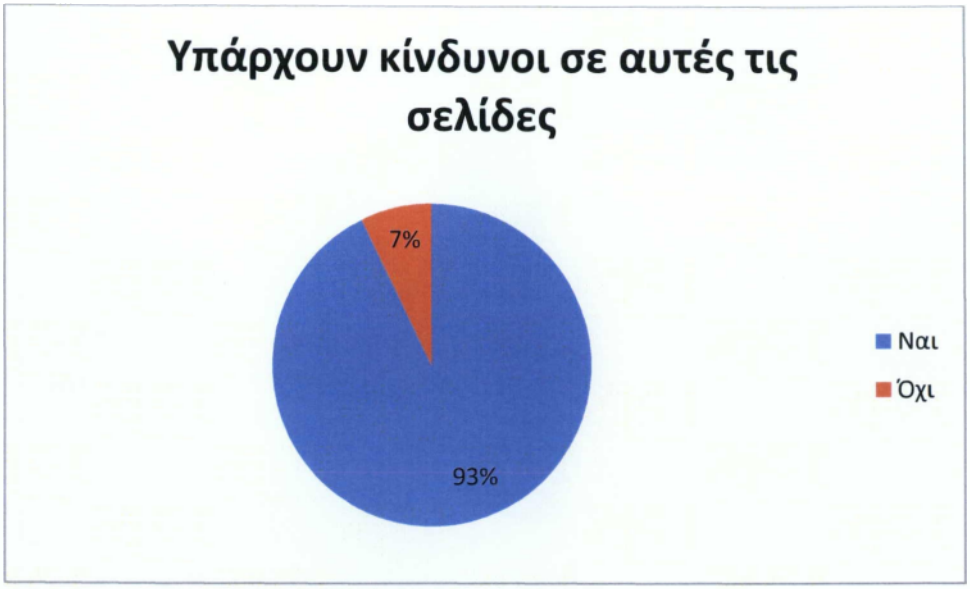
Κανένας: 0 Μερικοί: 9 Οι περισσότεροι: 49 Όλοι: 25



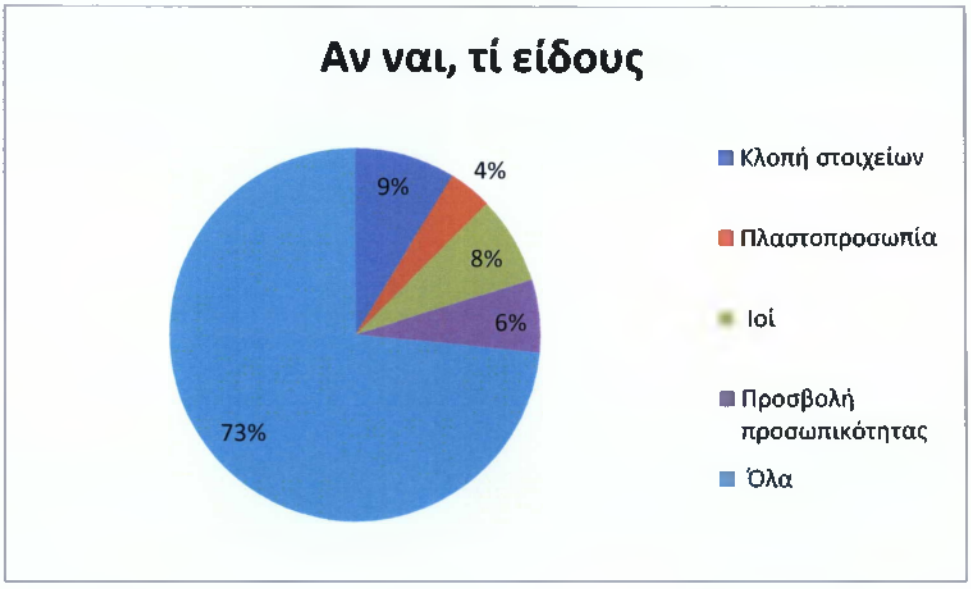
Ναι: 43 Όχι: 40



Ναι: 22 Όχι: 61

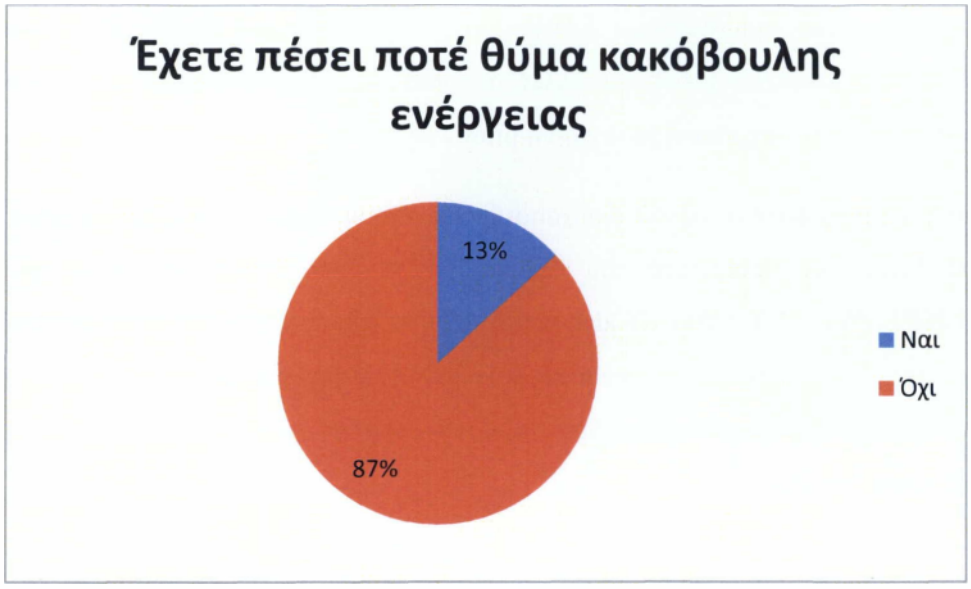


Ναι: 77 Όχι: 6

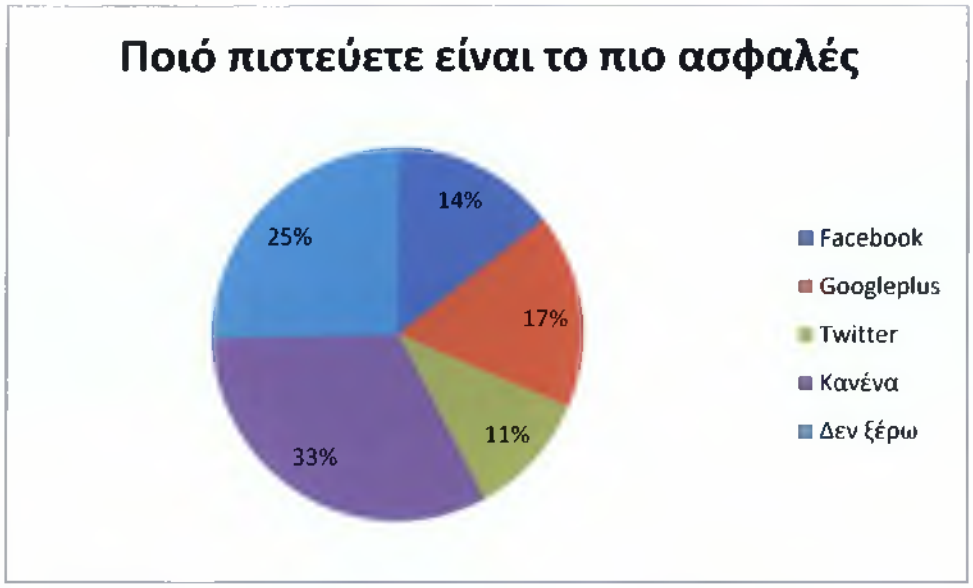


Κλοπή στοιχείων: 7 Πλαστοπροσωπία: 3 Ιοί: 6 Προσβολή προσωπικότητας: 5

Όλα: 58



Ναι: 11 Όχι: 72



Facebook: 12 Googleplus: 14 Twitter: 9

Κανένα: 27 Δενξέρω: 21

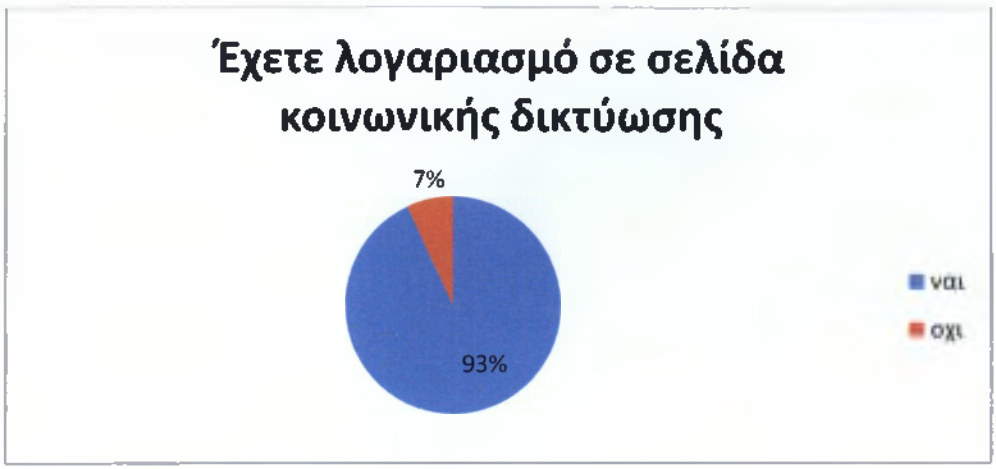
Βάση των αποτελεσμάτων της έρευνας, βλέπουμε ότι ένα πολύ μεγάλο ποσοστό διαθέτει λογαριασμό σε σελίδα κοινωνικής δικτύωσης, παρατηρούμε όμως ότι το Facebookείναι το πιο διαδεδομένο, ενώ τα Twitterκαι Googlepluseίναι λιγότερο διαδεδομένα στους Έλληνες χρήστες. Ακόμα σχεδόν ένας στους δύο χρήστες διαχειρίζεται το προφίλ του και από το κινητό.

Ενώ το πλήθος των ερωτηθέντων δηλώνει ότι μπαίνει αρκετά συχνά, βλέπουμε ότι αφιερώνουν περισσότερο χρόνο σε άλλες ασχολίες και ελάχιστοι είναι αυτοί που θα αναιρούσαν κάποια υποχρέωσή τους για να μπουν σε αυτά.

Όσον αφορά την ασφάλεια, τα 2/3 των χρηστών δεν έχουν διαβάσει τους όρους χρήσης, το 1/3 έχει δώσει τον προσωπικό του κωδικό και σε άλλα άτομα, και η συντριπτική πλειοψηφία πιστεύει ότι υπάρχουν κίνδυνοι στις συγκεκριμένες σελίδες, ενώ ένα ποσοστό της τάξης του 13% έχει πέσει θύμα κάποιας κακόβουλης ενέργειας. Τέλος ένα μεγάλο μέρος των ερωτηθέντων δεν ξέρει ποια σελίδα είναι η πιο ασφαλής ή πιστεύει ότι καμία δεν αξίζει τον συγκεκριμένο τίτλο.

Ηλικία: Έως 20 χρόνων

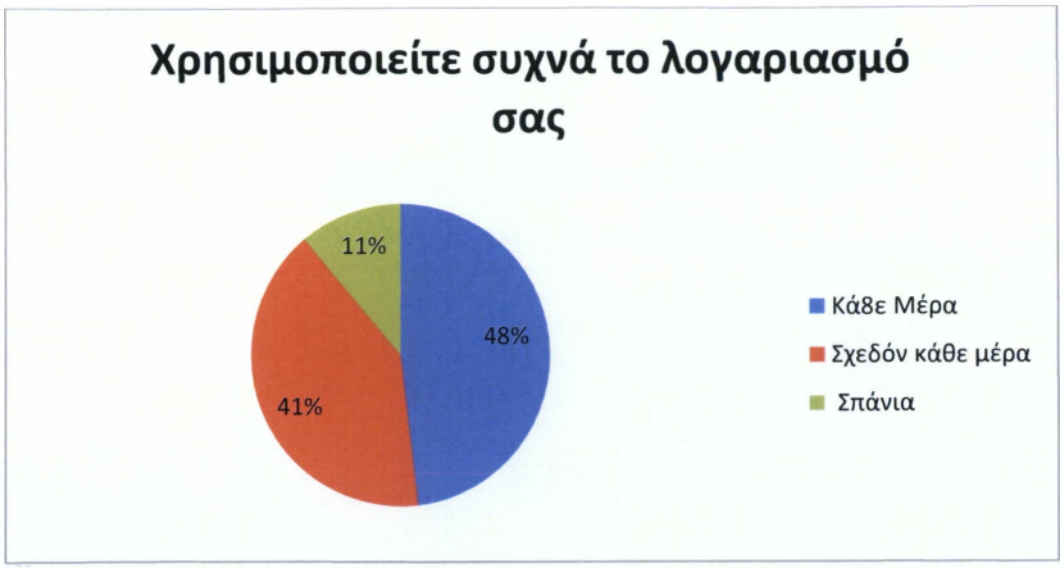
Σύνολο ατόμων: 29



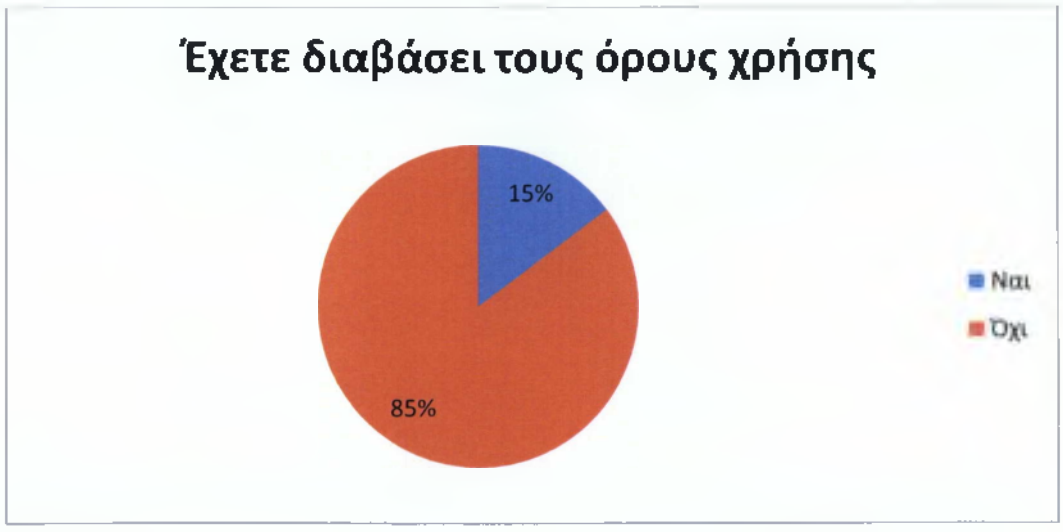
Ναι: 27 Όχι: 2

Facebook: 17 Googleplus: 0 Twitter: 1

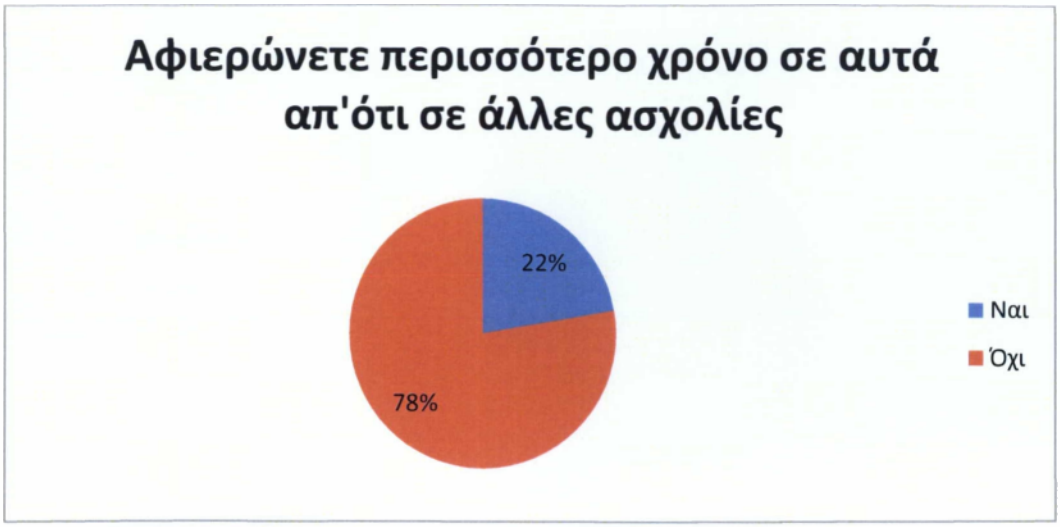
Facebook-Googleplus: 2 Facebook-twitter: 2 Καιστις 3: 5



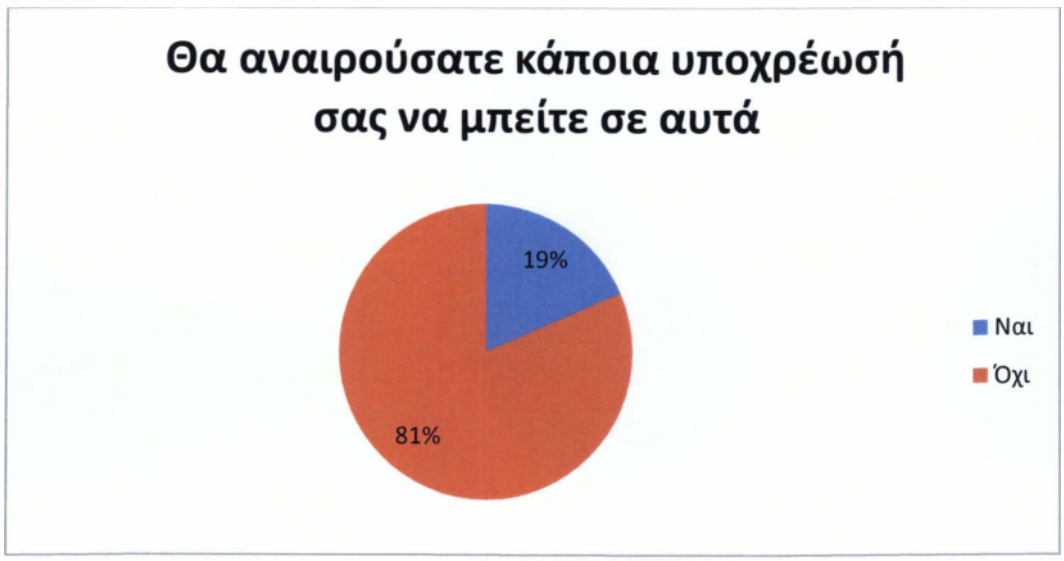
Κάθε μέρα: 13 Σχεδόν κάθε μέρα: 11 Σπάνια: 3



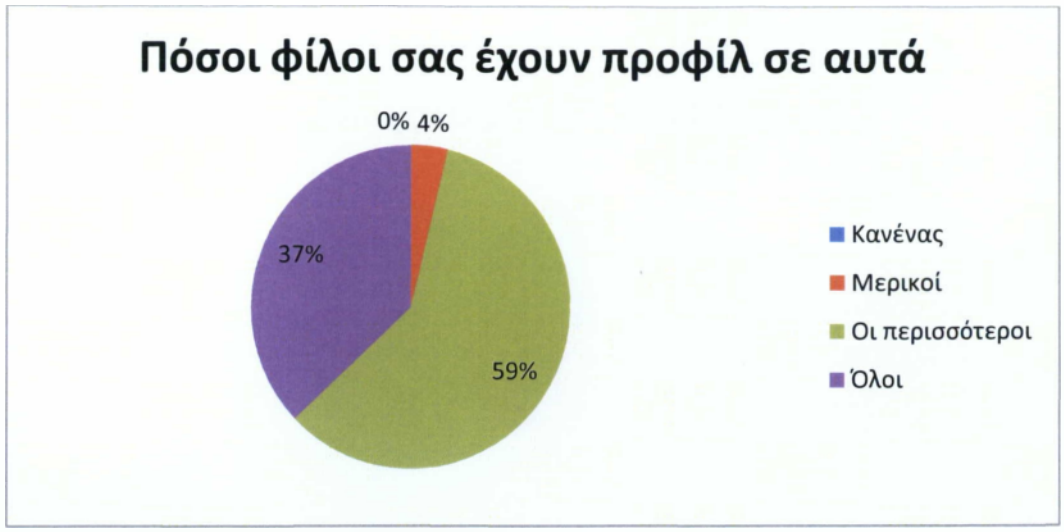
Ναι: 4 Όχι: 23



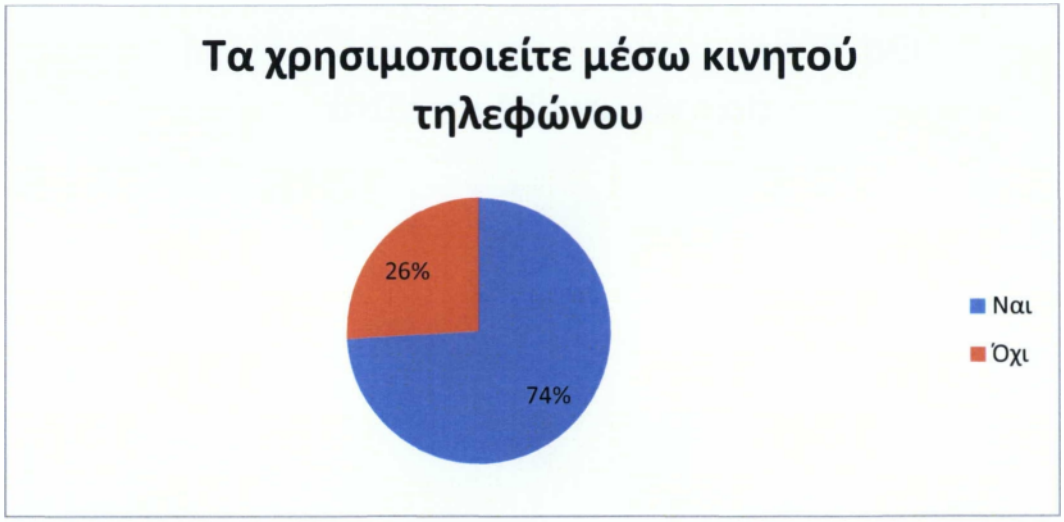
Ναι: 6 Όχι: 21



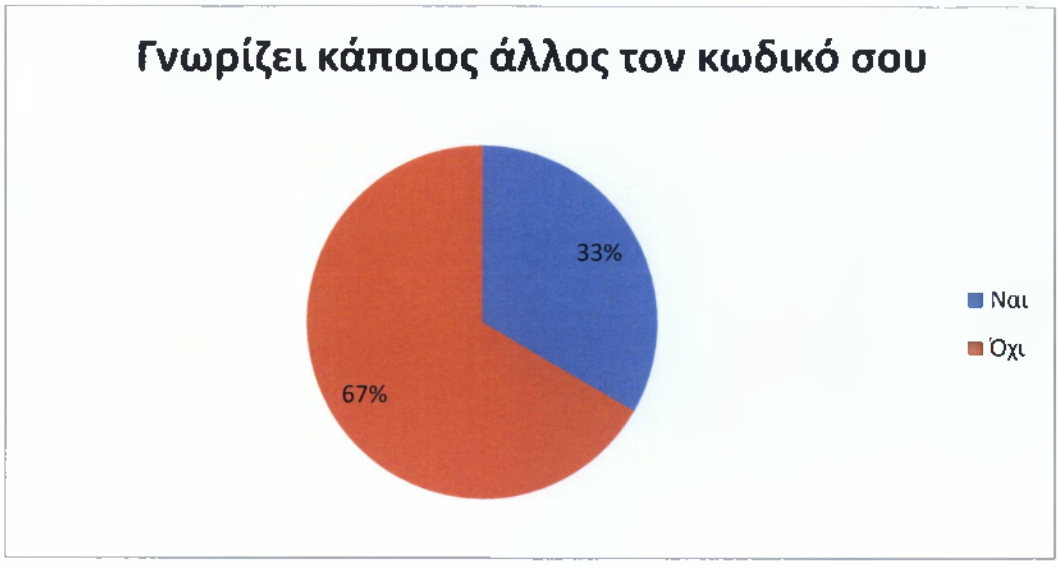
Ναι: 5 Όχι: 22



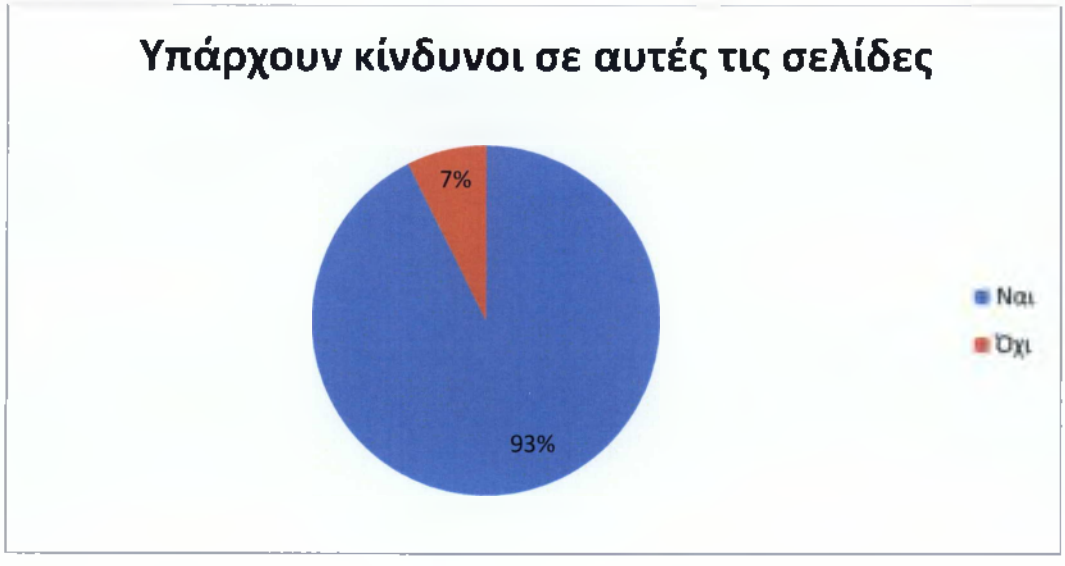
Κανένας: 0 Μερικοί: 1 Οι περισσότεροι: 16 Όλοι: 10



Ναι: 20 Όχι: 7



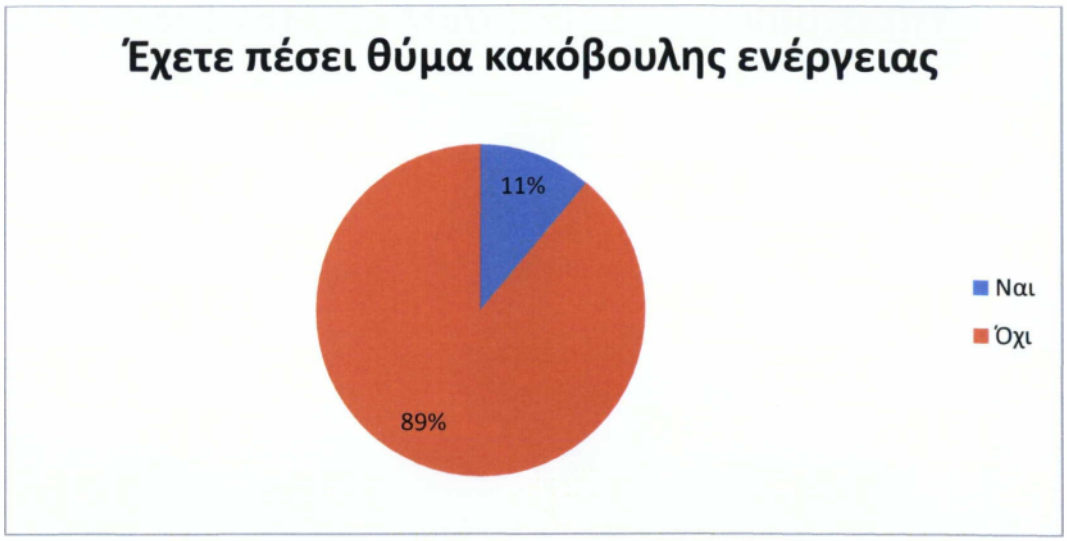
Ναι: 9 Όχι: 18



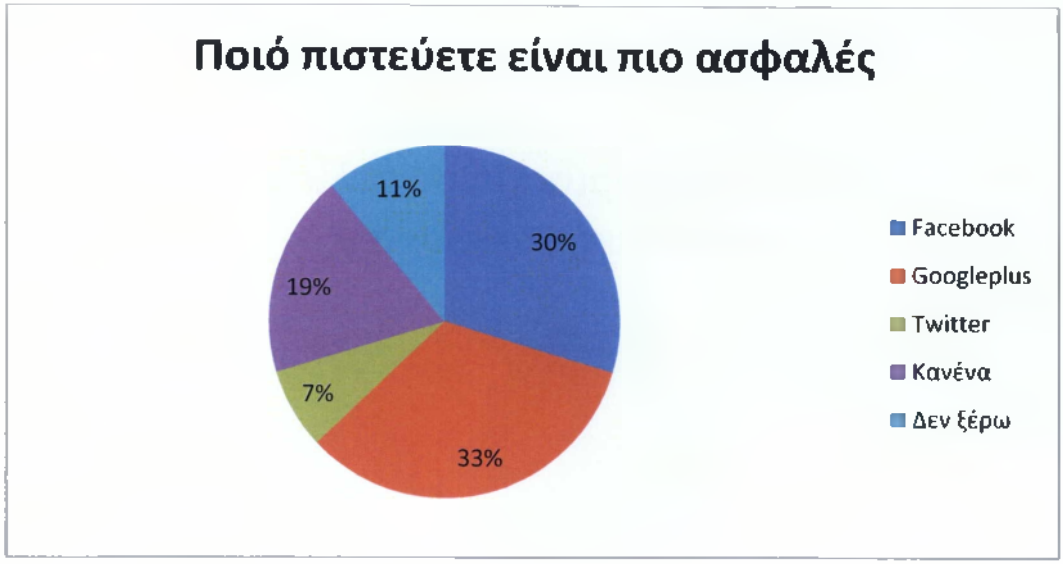
Ναι: 25 Όχι: 2

Κλοπή στοιχείων: 4 Πλαστοπροσωπία: 1 Ιοί: 1 Προσβολή Προσωπικότητας: 4

Όλα: 17



Ναι: 3 Όχι: 24



Facebook:8 Googleplus: 9 Twitter:2

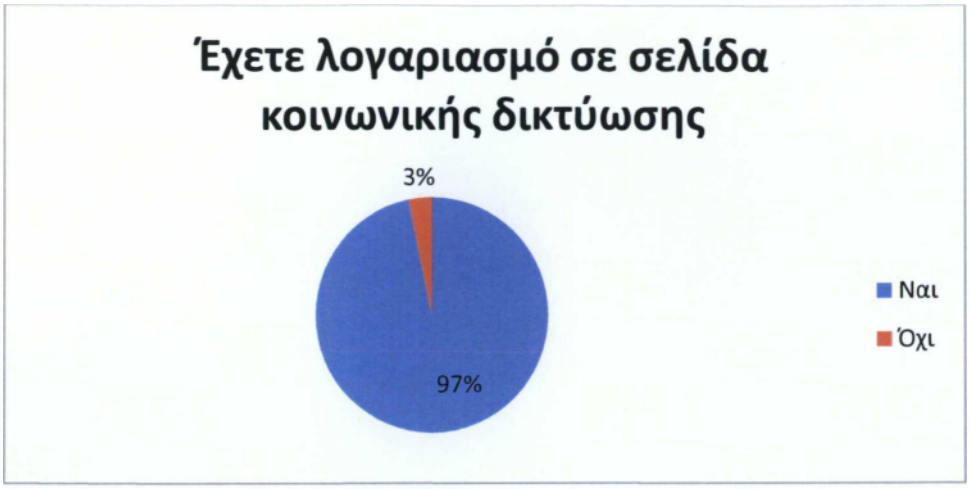
Κανένα:5 Δενξέρω:3

Πάνω από το 90% των ατόμων δηλώνει ότι έχει λογαριασμό σε περιβάλλον κοινωνικής δικτύωσης, δηλώνει αρκετά ενεργό και στην πλειοψηφία του επισκέπτεται τις σελίδες και από κινητό τηλέφωνο.

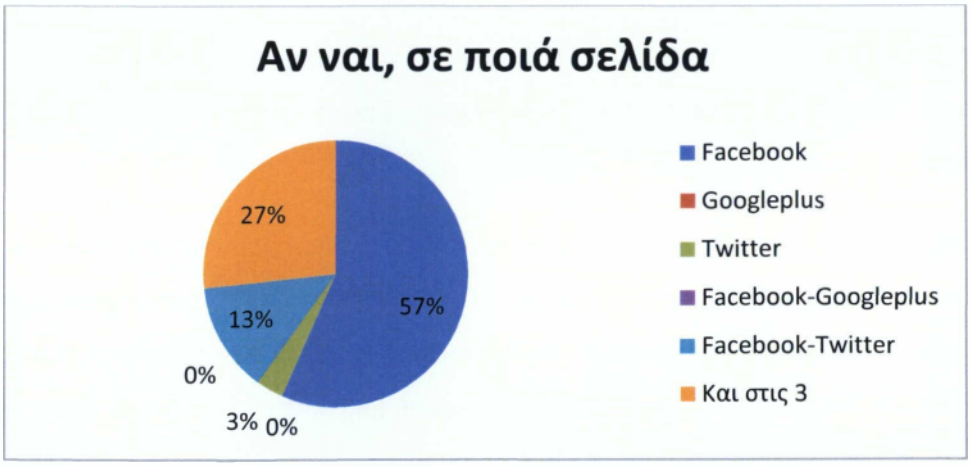
Πολύ μικρό είναι όμως το ποσοστό που έχει διαβάσει τους όρους χρήσης των σελίδων. Ακόμα δεν είναι λίγα τα άτομα που έχουν ως προτεραιότητά τους τη συγκεκριμένη ασχολία. Επιπλέον δεν διστάζουν να μοιραστούν τον προσωπικό τους κωδικό, αφού ένας στους δύο απαντά θετικά. Παρόλα αυτά πιστεύουν ότι υπάρχουν κίνδυνοι και τέλος οι απόψεις για την ασφάλεια των σελίδων δείχνουν σχεδόν μοιρασμένες.

Ηλικία:21-30

Σύνολο ατόμων:31

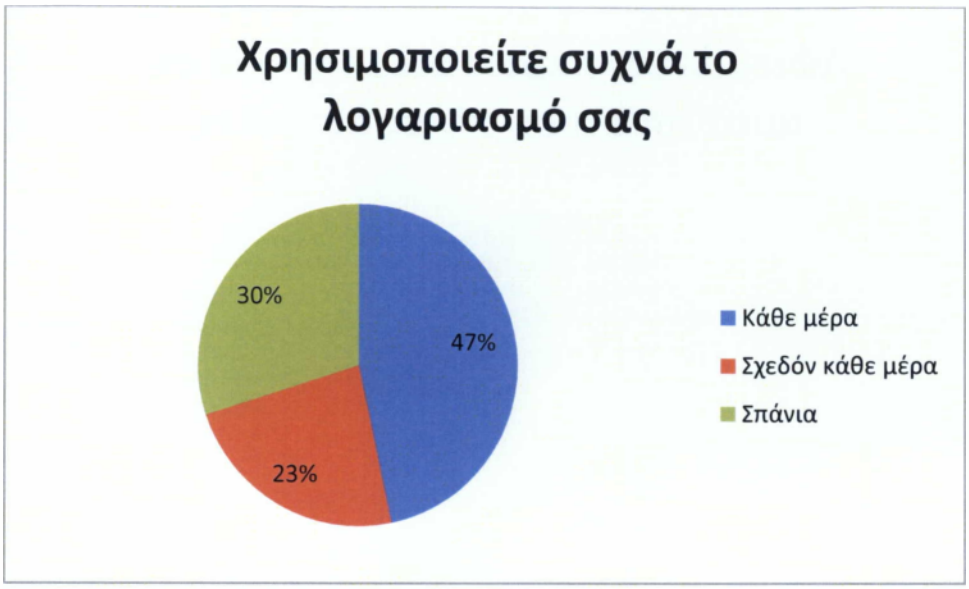


Ναι: 30 Όχι: 1

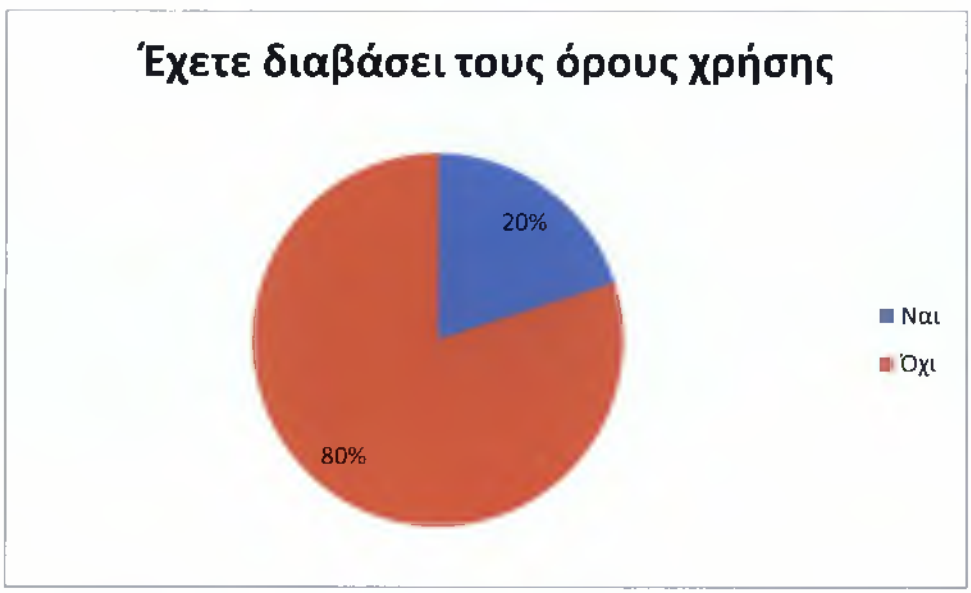


Facebook: 17 Googleplus: 0 Twitter: 1

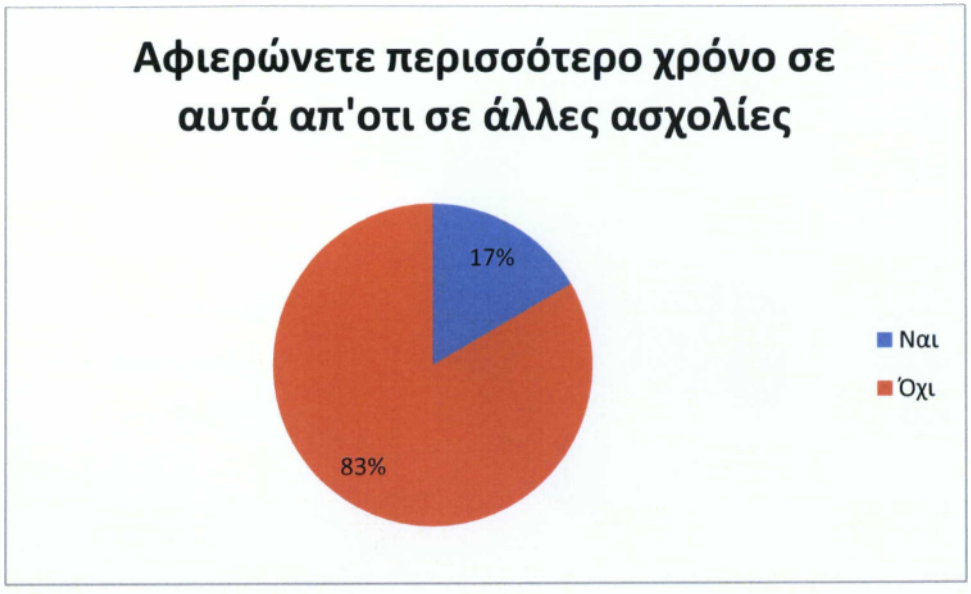
Facebook-Googleplus: 0 Facebook-twitter: 4 Καιστις 3: 8



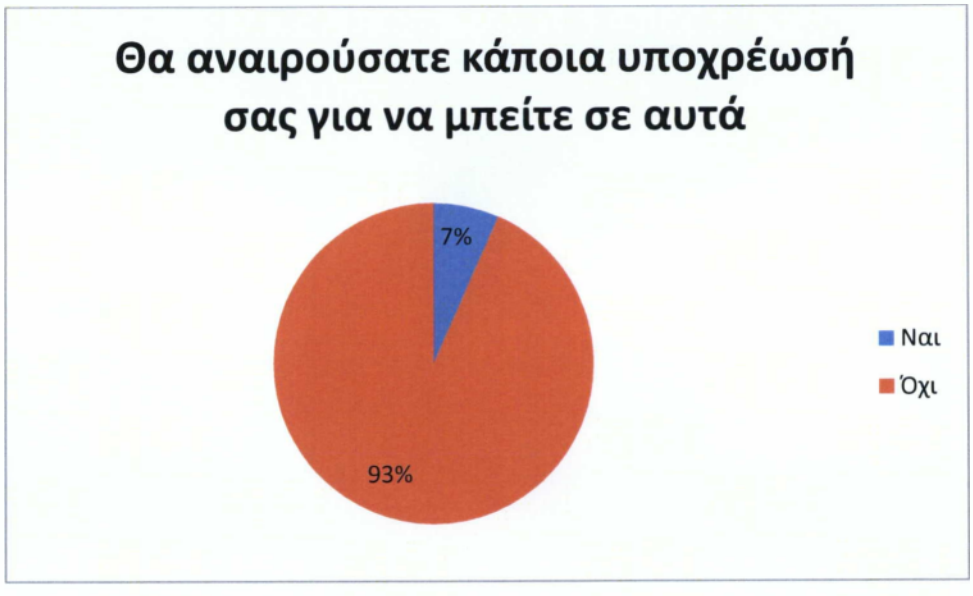
Κάθε μέρα: 14 Σχεδόν κάθε μέρα: 7 Σπάνια: 9



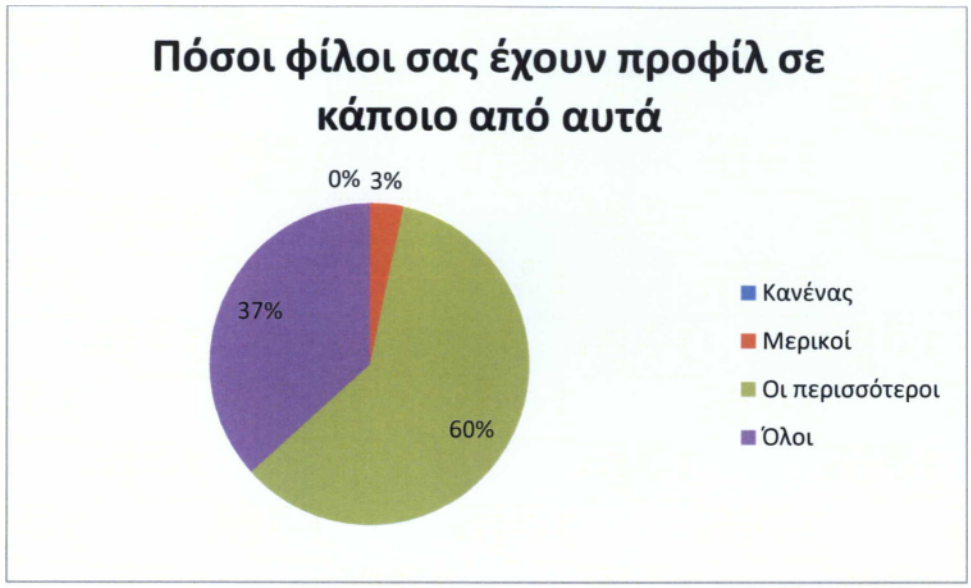
Ναι: 6 Όχι: 24



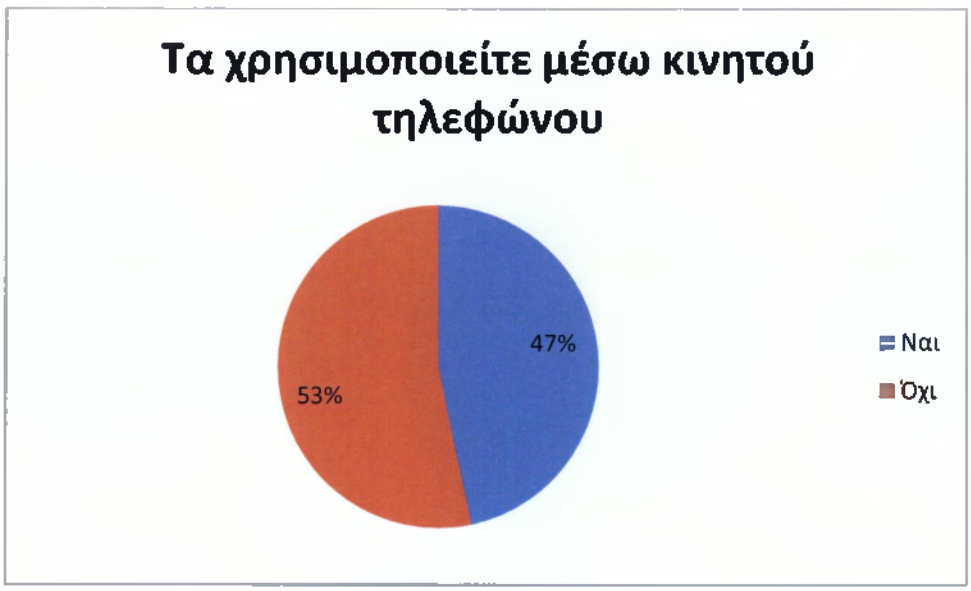
Ναι: 5 Όχι: 25



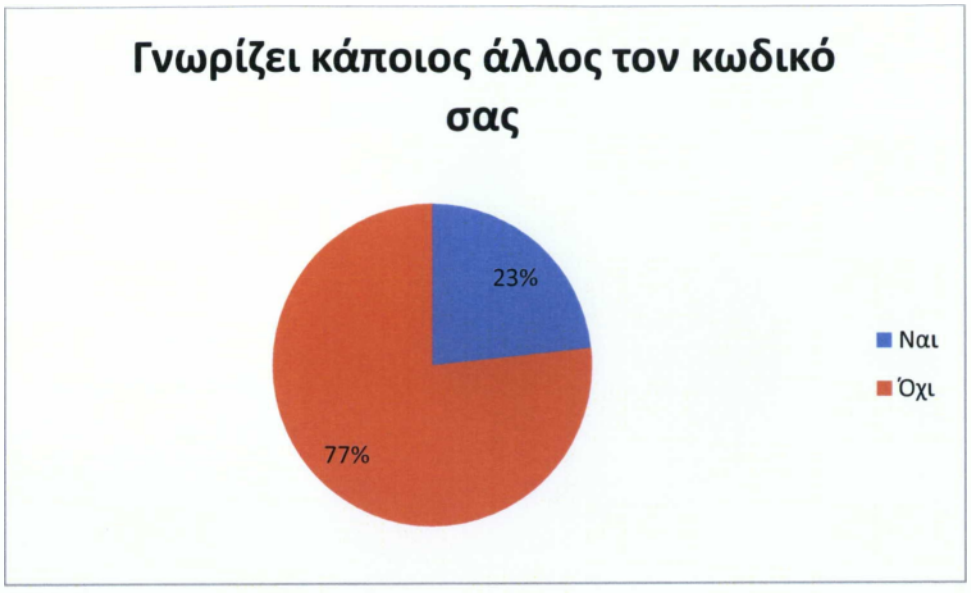
Ναι: 2 Όχι: 28



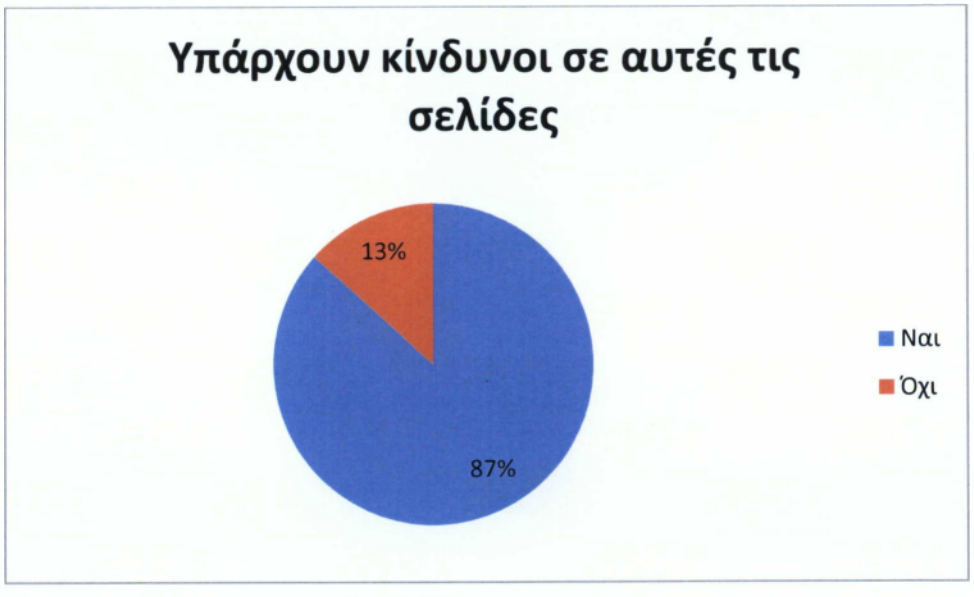
Κανένας: 0 Μερικοί: 1 Οι περισσότεροι: 18 Όλοι: 11



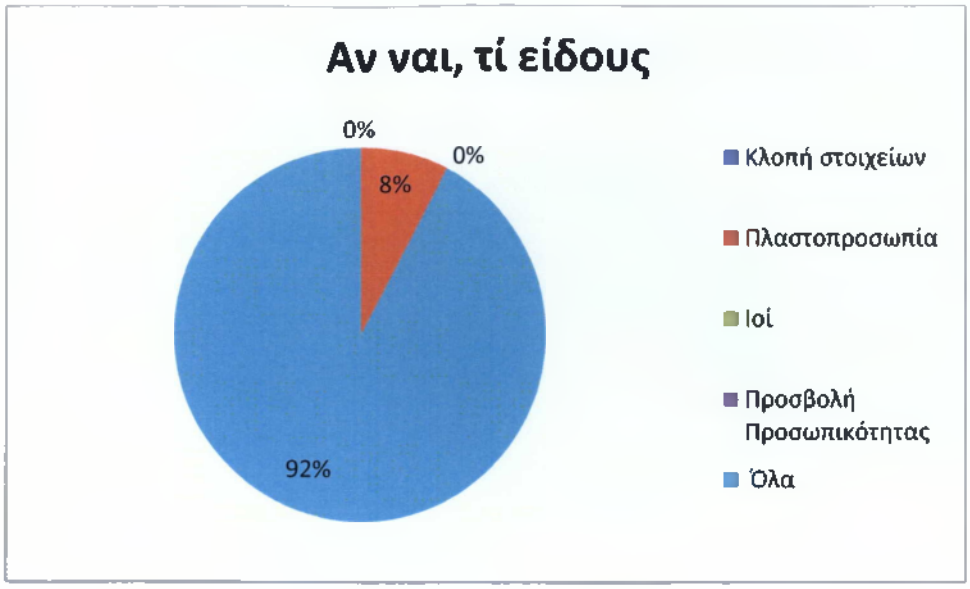
Ναι: 14 Όχι: 16



Ναι: 7 Όχι: 23

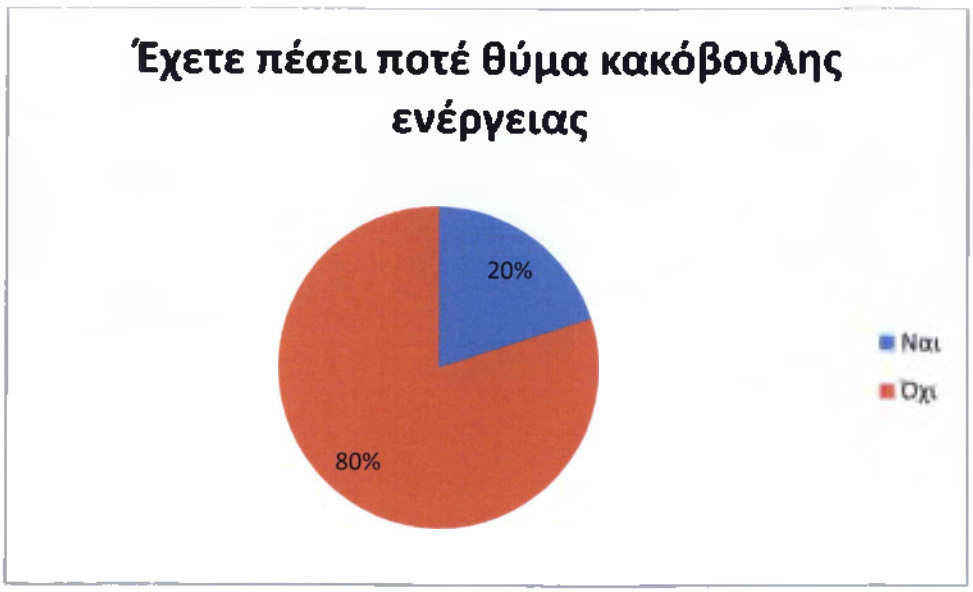


Ναι: 26 Όχι: 4

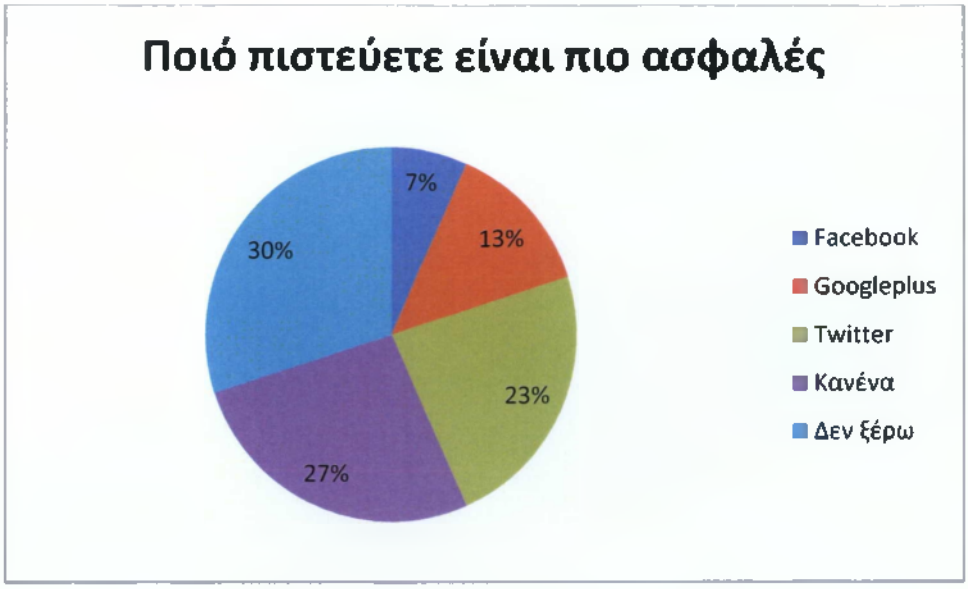


Κλοπή στοιχείων: 0 Πλαστοπροσωπία: 2 Ιοί: 0 Προσβολή Προσωπικότητας: 0

Όλα: 24



Ναι: 6 Όχι: 24



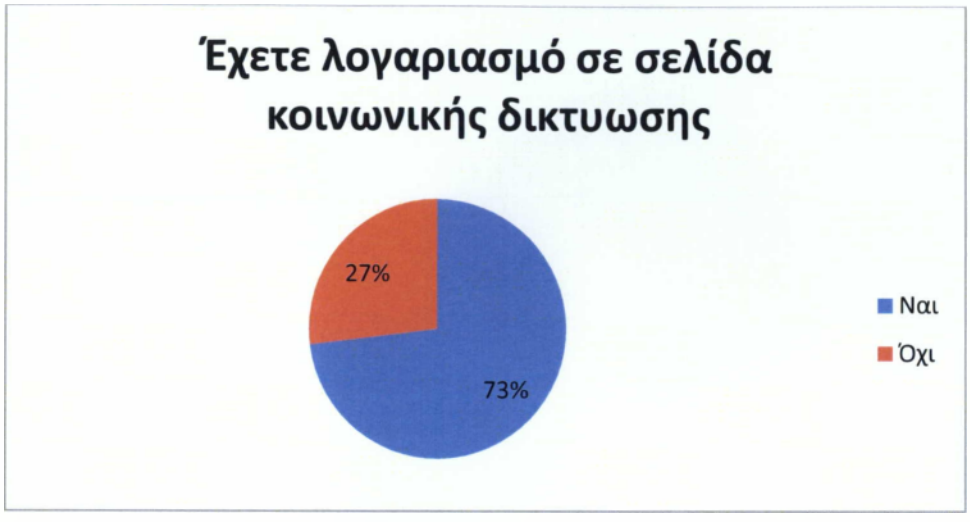
Facebook: 2 Googleplus:4 Twitter: 7

Κανένα:8 Δενξέρω: 9

Μετά την ανάλυση των δεδομένων για άτομα ηλικίας 21-30 βλέπουμε ότι τα αποτελέσματα είναι παρόμοια με το προηγούμενο εύρος ηλικίας. Παρά τα 10 χρόνια διαφοράς το σκεπτικό και οι απαντήσεις είναι παρόμοιες. Οι διαφορές τους είναι στη χρήση μέσω κινητού τηλεφώνου που εδώ δείχνει μειωμένη, και στην άνοδο ψήφων του Twitterως ασφαλέστερο περιβάλλον σε σχέση με τα υπόλοιπα.

Ηλικία: 31-45

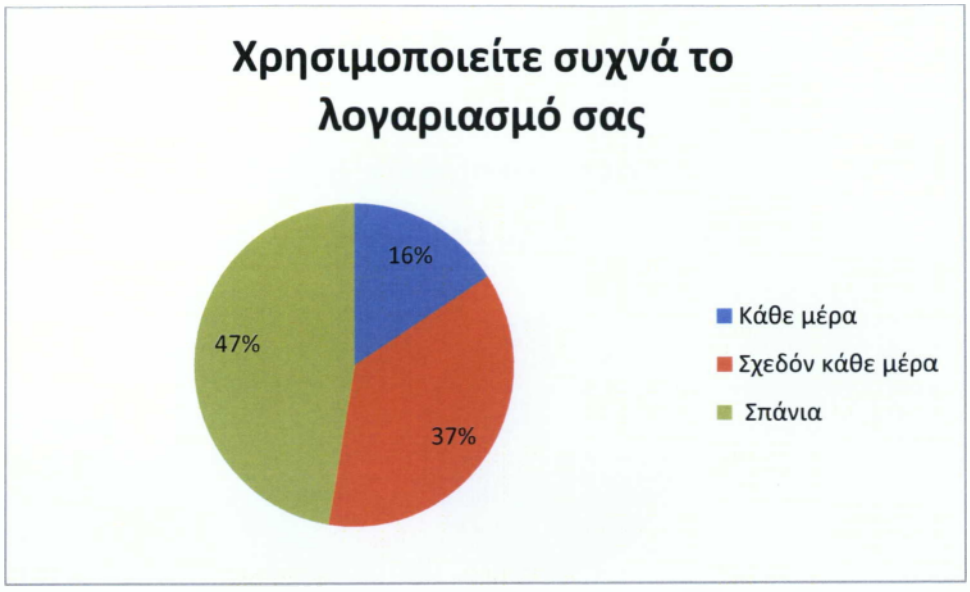
Άτομα: 26



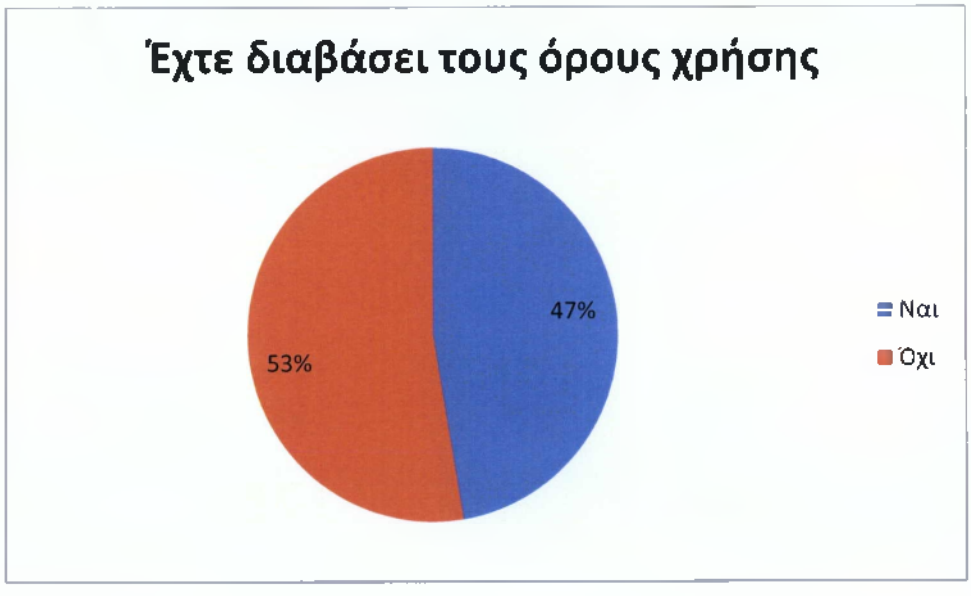
Ναι: 19 Όχι: 7

Facebook: **15** Googleplus: 0 Twitter: 1

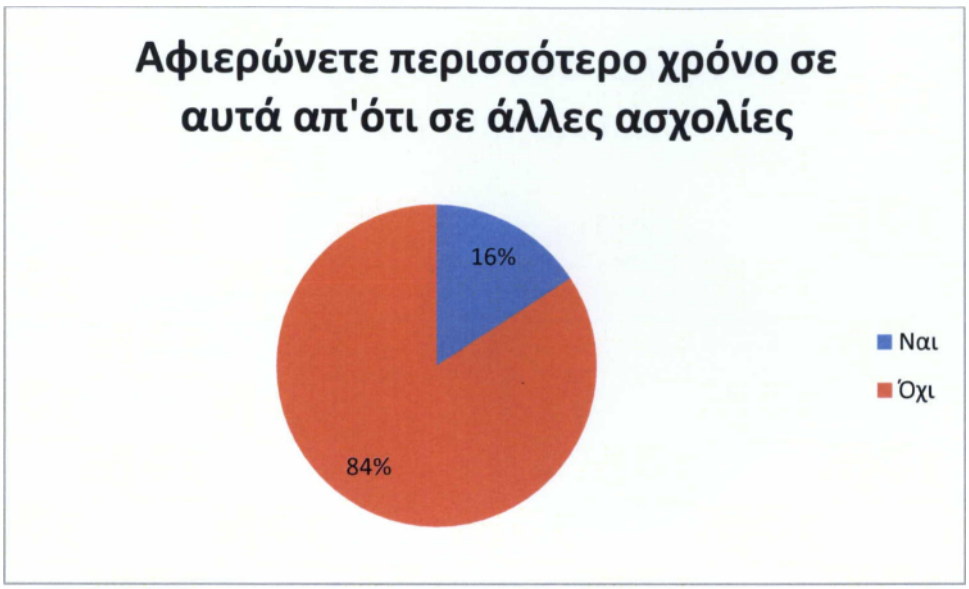
Facebook-googleplus: 1 Facebook-Twitter: 1 Καιστα 3: **1**



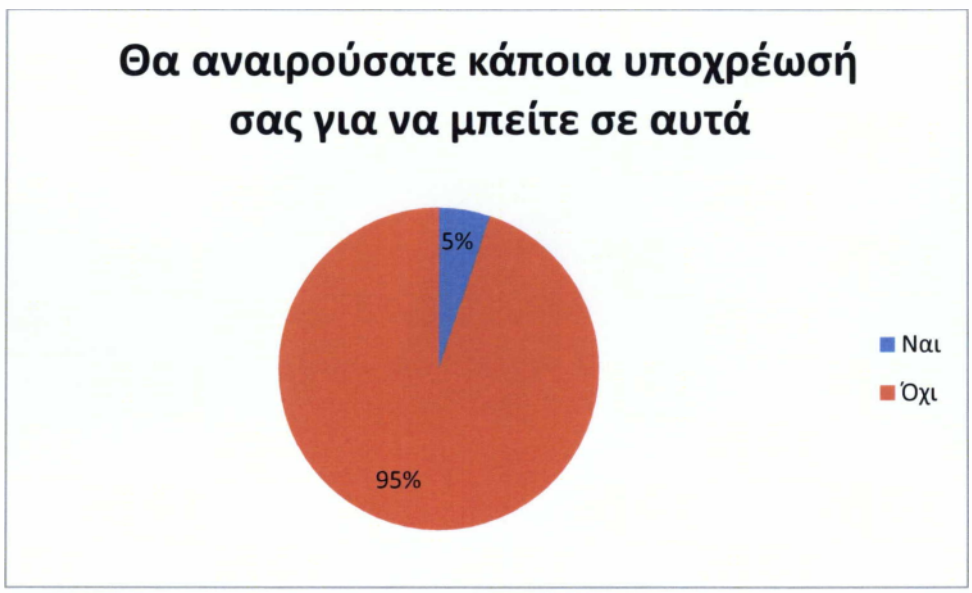
Κάθε μέρα: 3 Σχεδόν κάθε μέρα: 7 Σπάνια: 9



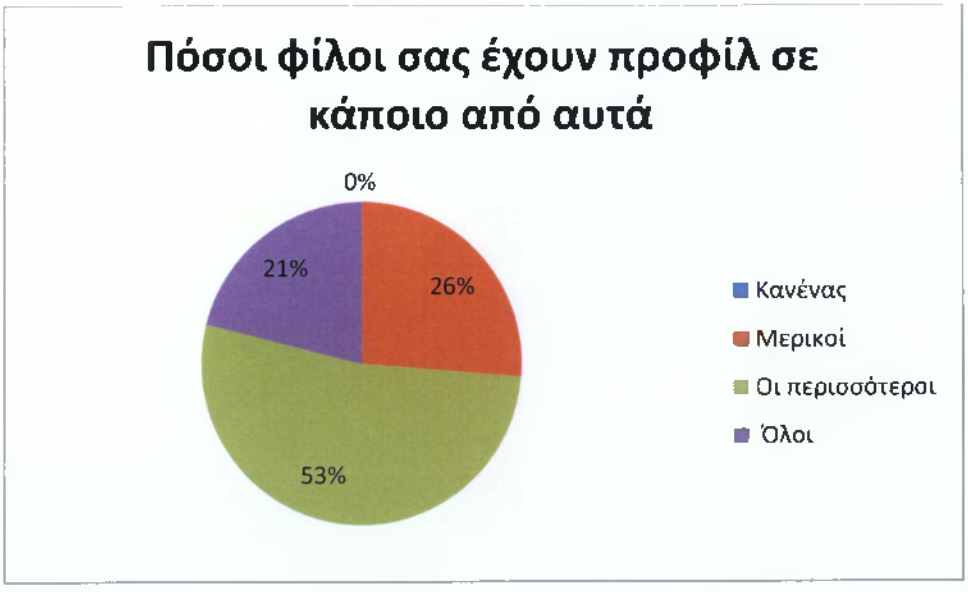
Ναι: 9 Όχι: 10



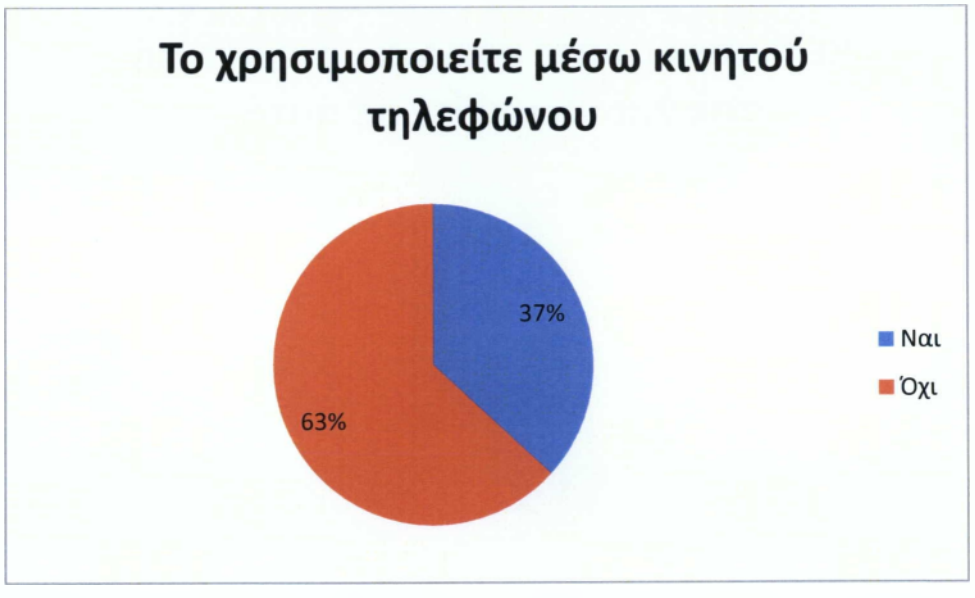
Ναι: 3 Όχι: 16



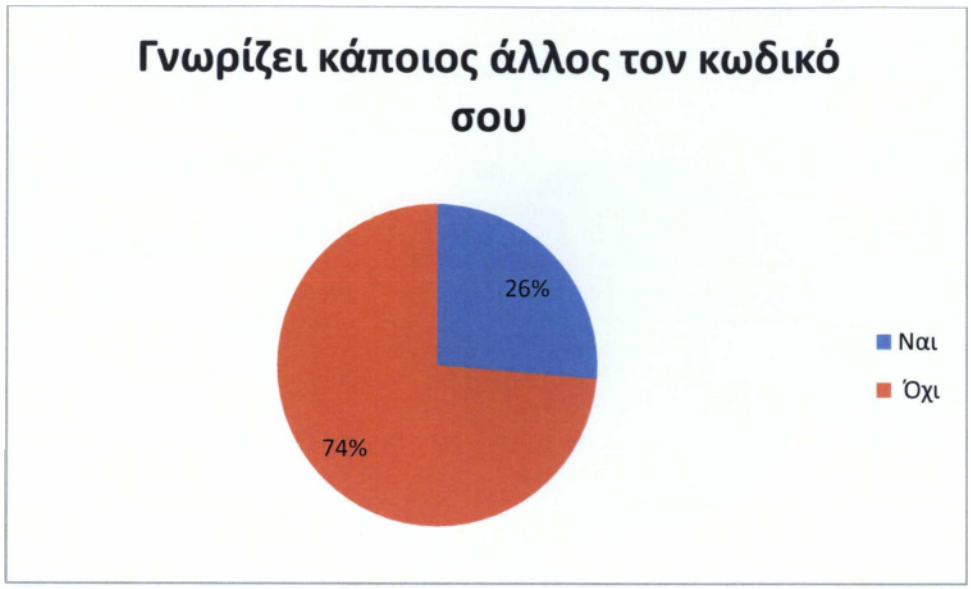
Ναι: 1 Όχι: 18



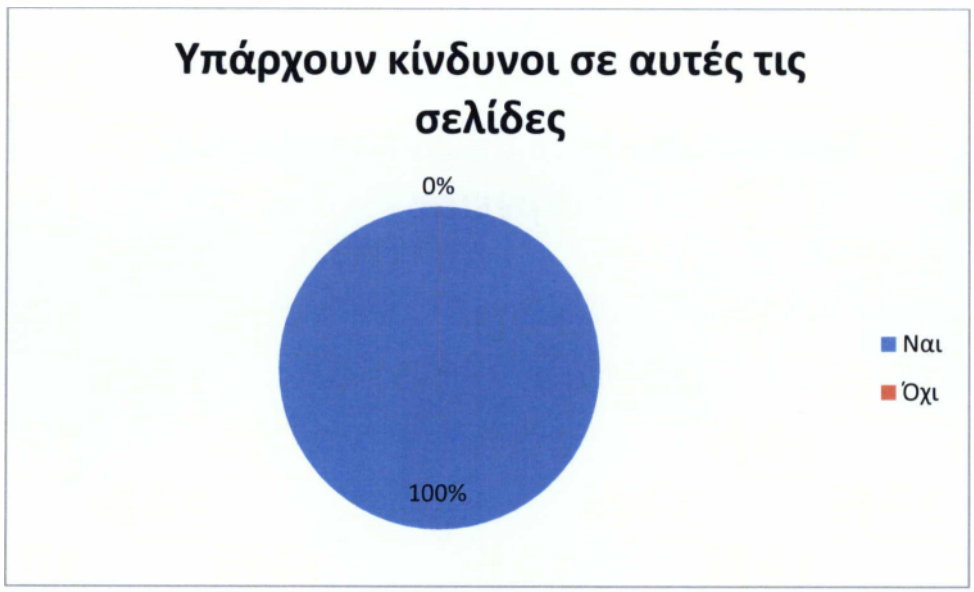
Κανένας: 0 Μερικοί: 5 Οι περισσότεροι: 10 Όλοι: 4



Ναι: 7 Όχι: 12



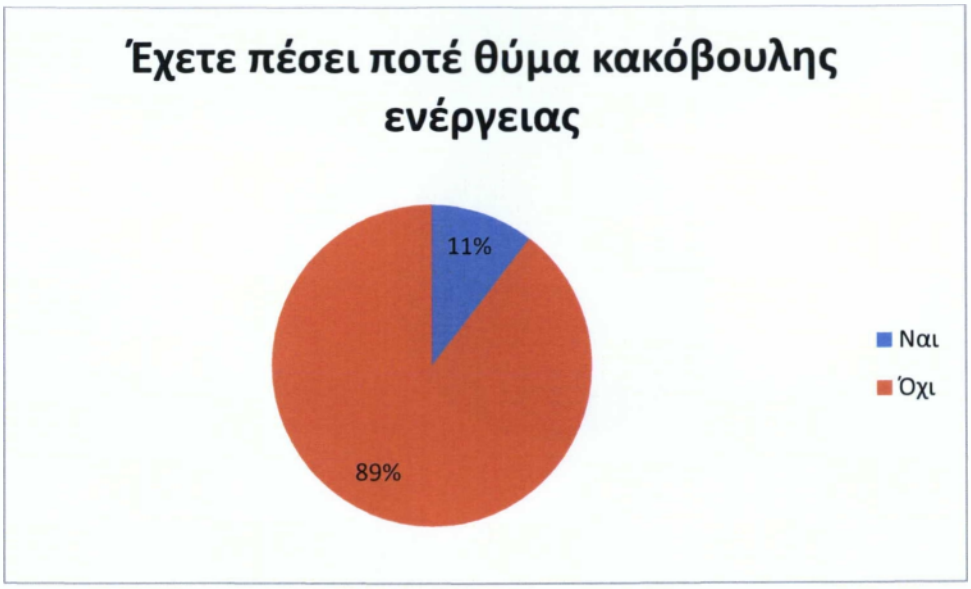
Ναι: 5 Όχι: 14



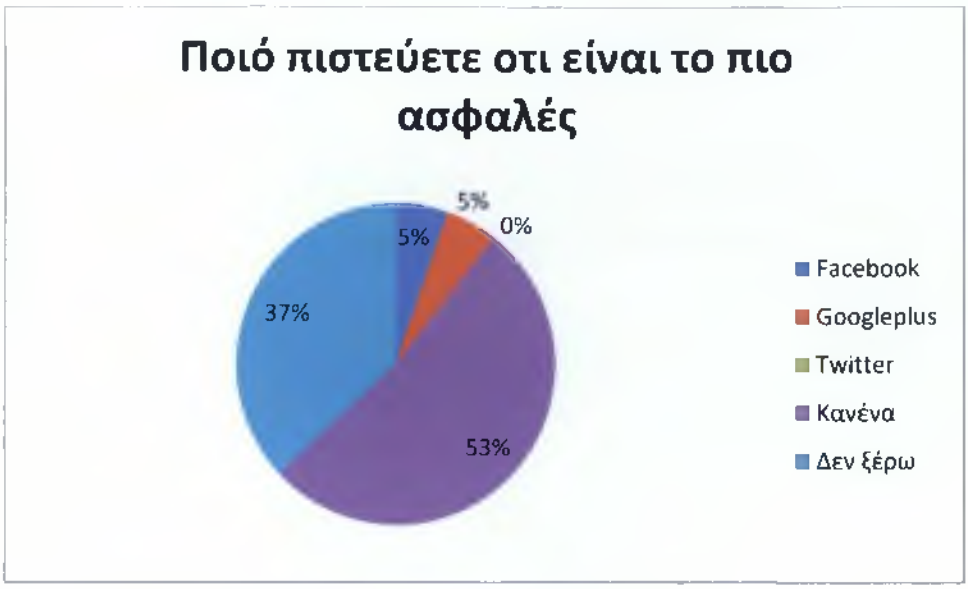
Ναι: 19 Όχι: 0

Κλοπή στοιχείων: 2 Πλαστοπροσωπία: 0 Ιοί: 3 Προσβολή προσωπικότητας: 0

Όλα: 14



Ναι: 2 Όχι: 17



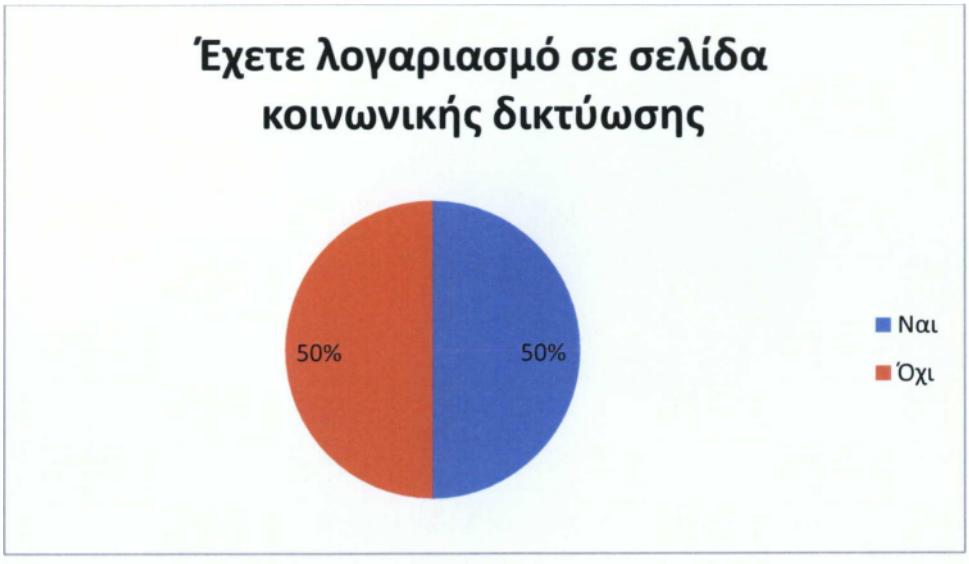
Facebook: 1 Googleplus: 1 Twitter: 0

Κανένα: 10 Δενξέρω: 7

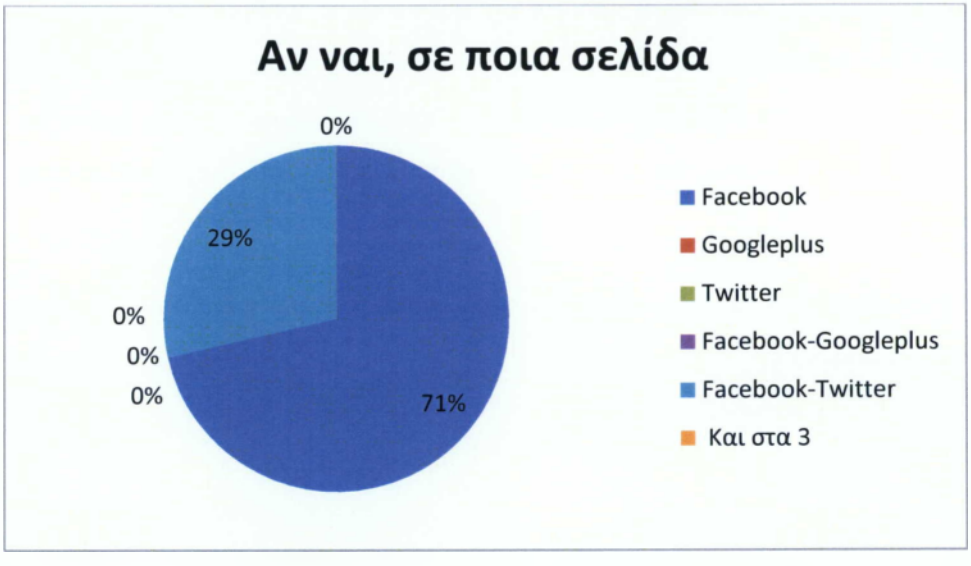
Από την ηλικία των 30 και άνω παρατηρούμε ότι αυξάνεται ο αριθμός ατόμων χωρίς λογαριασμό, ενώ και αυτοί που διατηρούν έναν προτιμούν το Facebook συντριπτικά Οι μισοί από τους οποίους χρησιμοποιούν το λογαριασμό τους σπάνια και δεν τον έχουν ως προτεραιότητα. Επιπλέον δείχνουν πιο προσεκτικοί, αφού οι μισοί σχεδόν έχουν διαβάσει τους όρους χρήσης.

Η συντριπτική πλειοψηφία δηλώνει ότι υπάρχουν κίνδυνοι και δηλώνουν ότι δεν ξέρουν και ότι κανένα δεν είναι ασφαλές.

Ηλικία: 46-77
Άτομα: 14

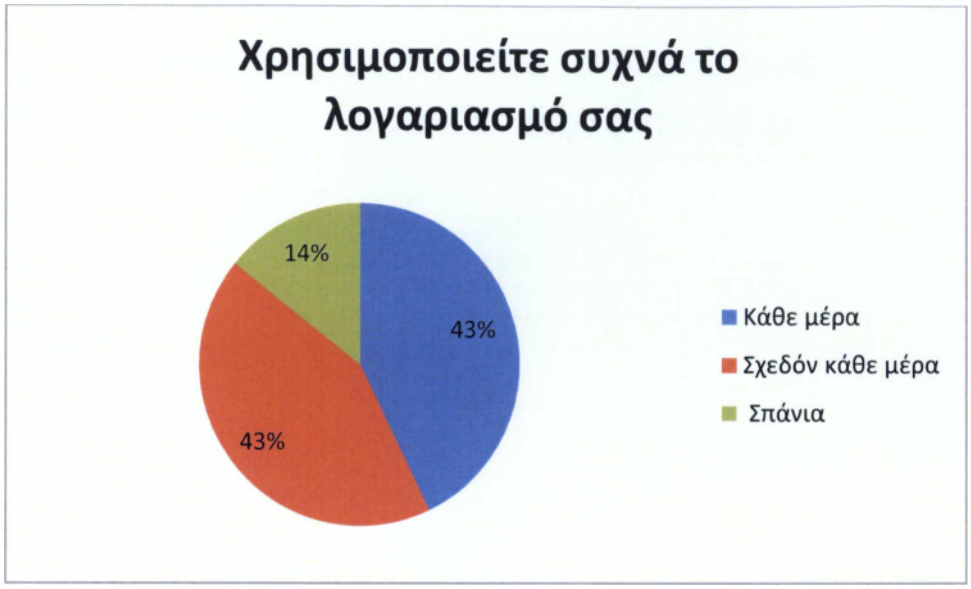


Ναι: 7 Όχι: 7

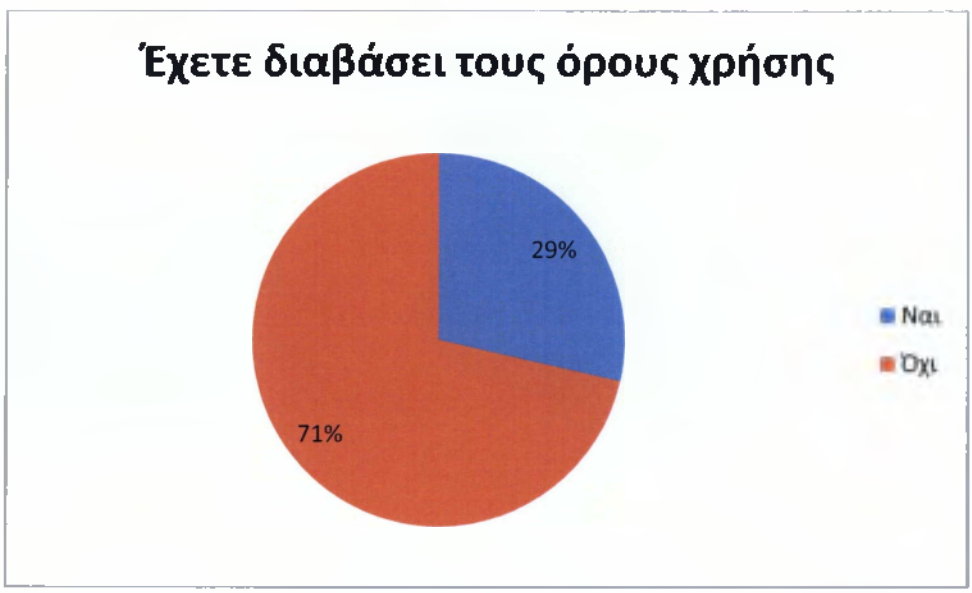


Facebook: 5 Googleplus: 0 Twitter: 0

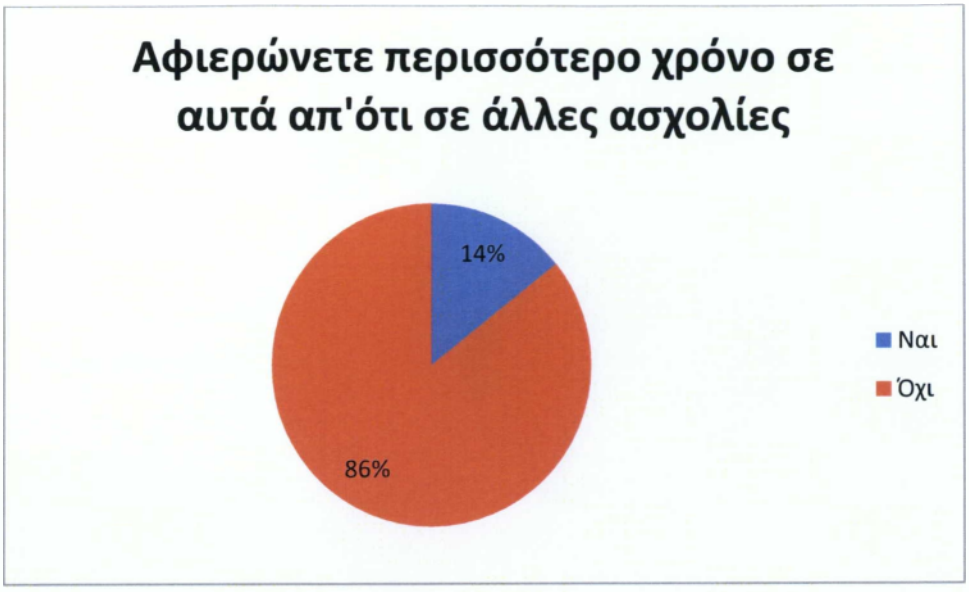
Facebook-Googleplus: 0 Facebook-Twitter: 2 Καιστα 3: 0



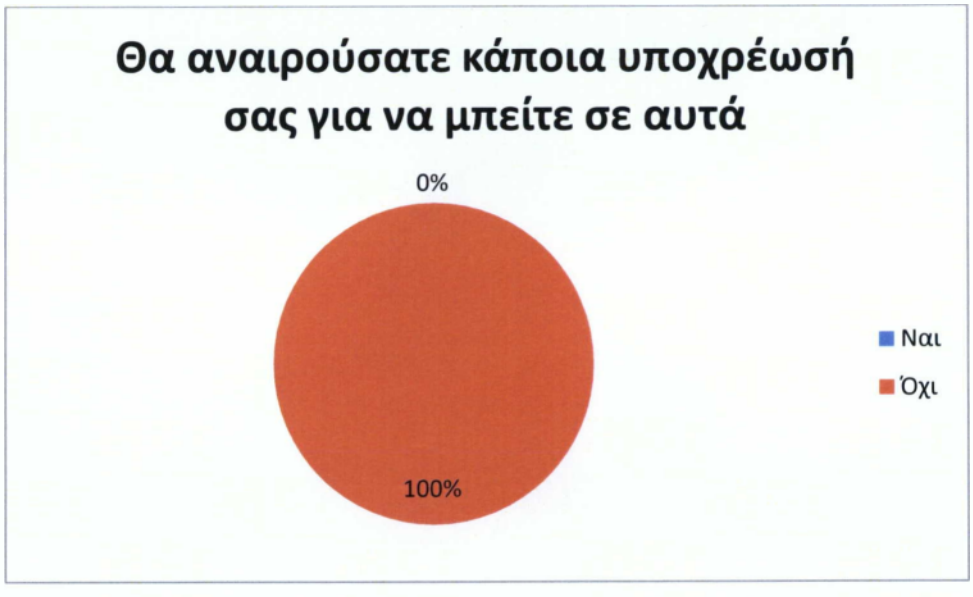
Κάθε μέρα: 3 Σχεδόν κάθε μέρα: 3 Σπάνια: 1



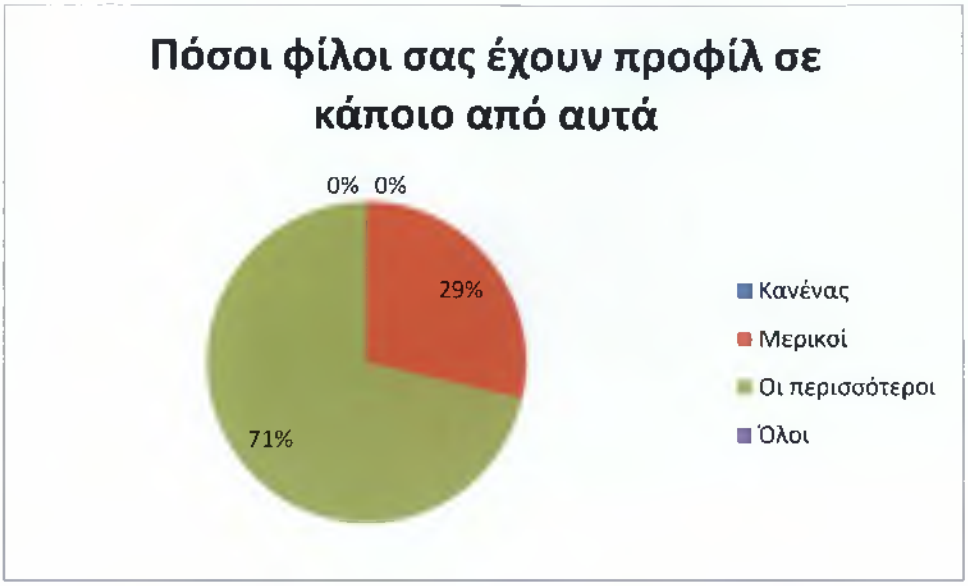
Ναι: 2 Όχι: 5



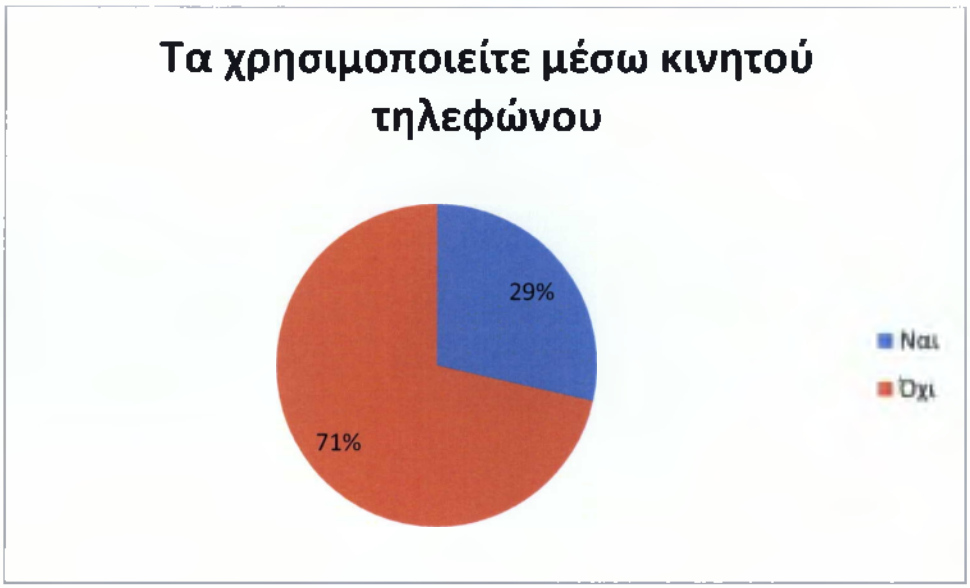
Ναι: 1 Όχι: 6



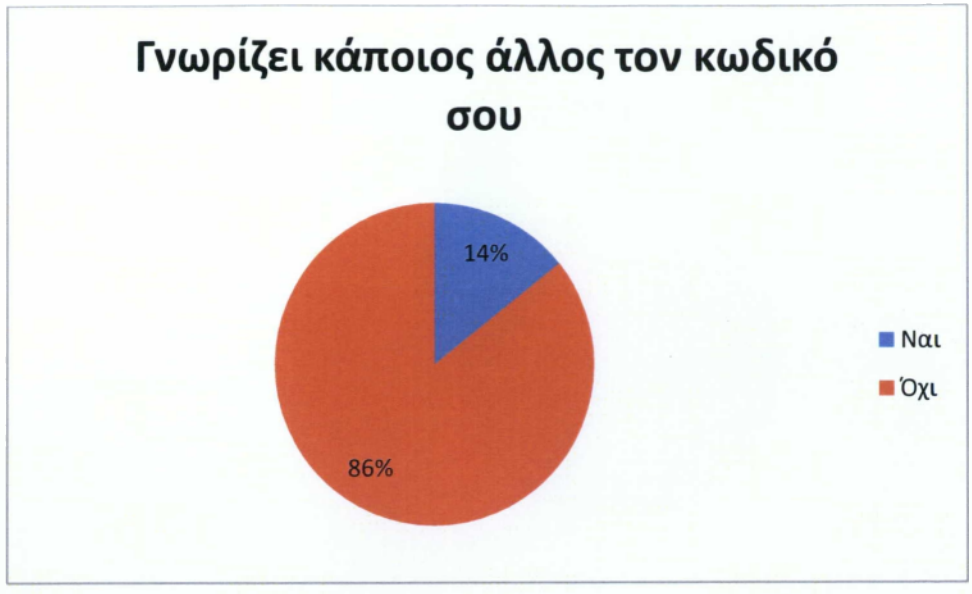
Ναι: 0 Όχι: 7



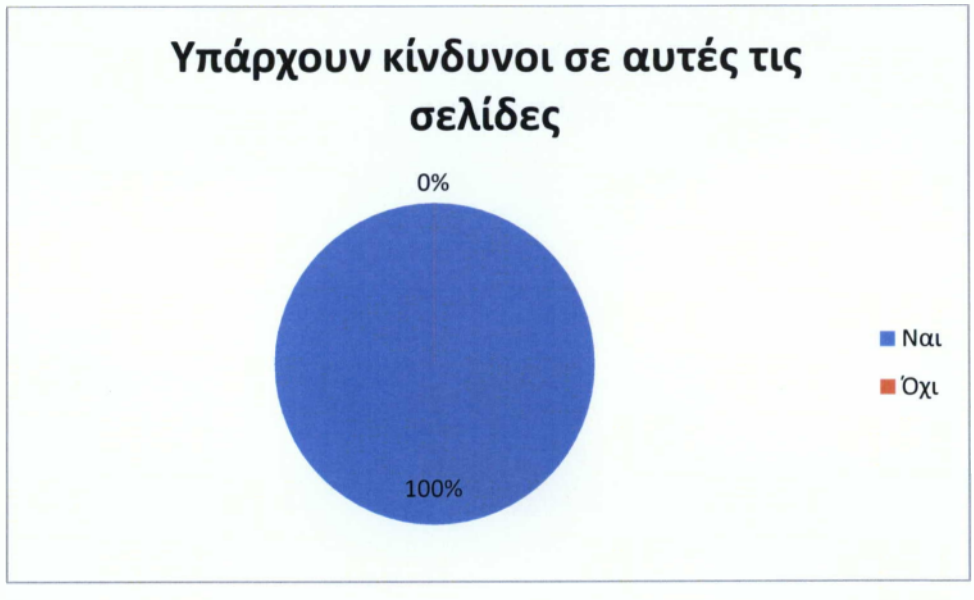
Κανένας: 0 Μερικοί: 2 Οι περισσότεροι: 5 Όλοι: 0



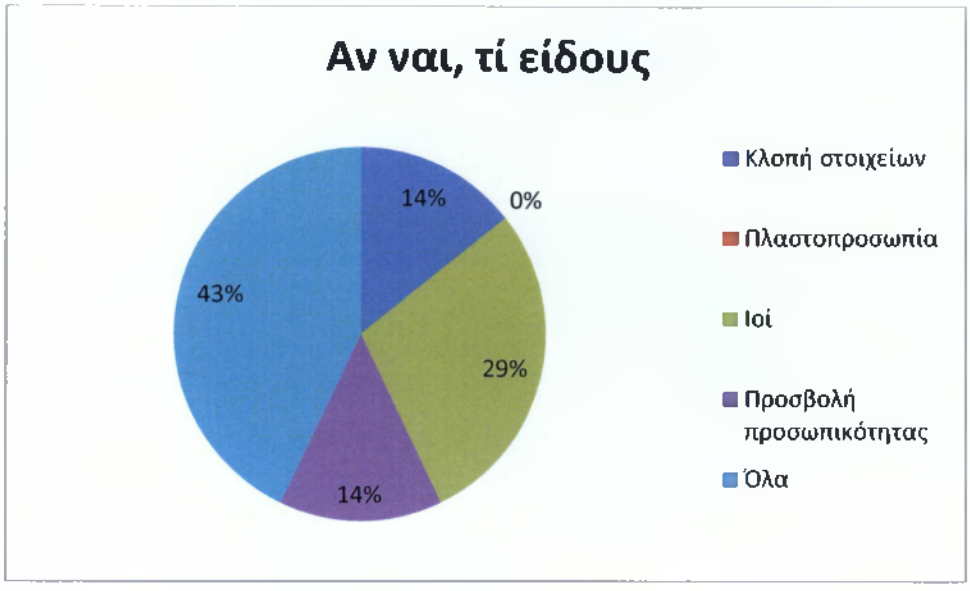
Ναι: 2 Όχι: 5



Ναι: 1 Όχι: 6

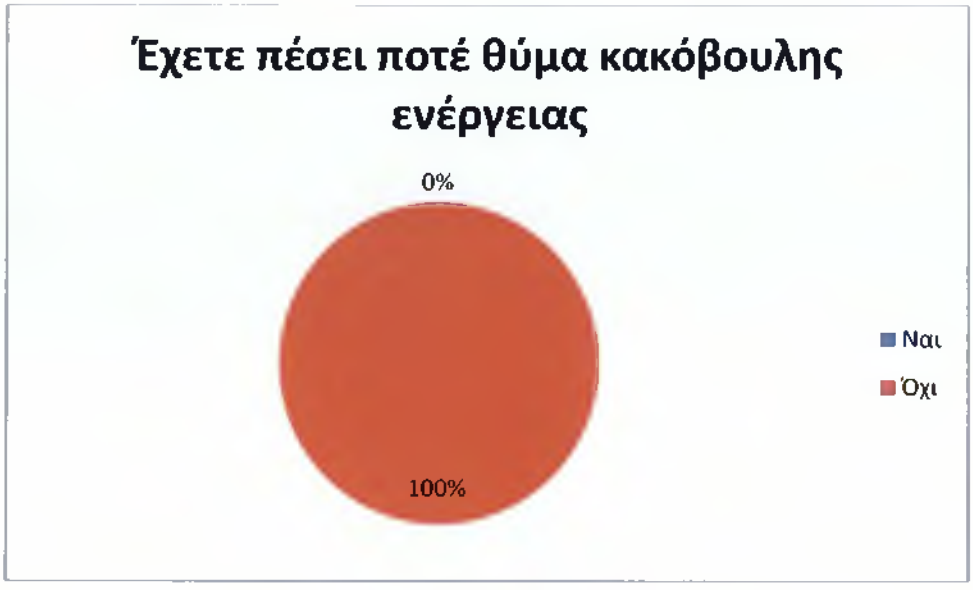


Ναι: 7 Όχι: 0

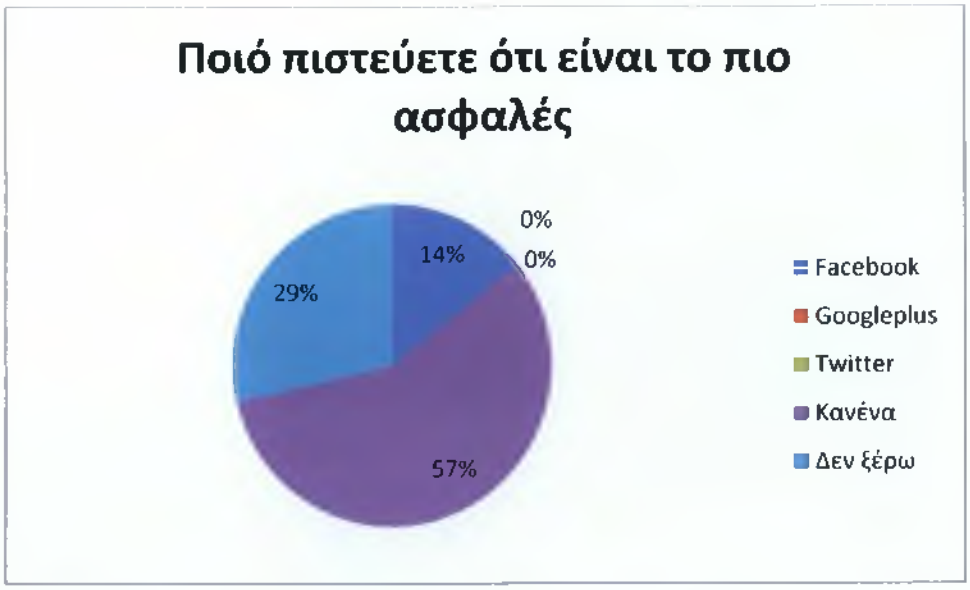


Κλοπή στοιχείων: 1 Πλαστοπροσωπία: 0 Ιοί: 2 Προσβολή προσωπικότητας: 1

Όλα: 3



Ναι: 0 Όχι: 7



Facebook: 1 Googleplus: 0 Twitter: 0

Κανένα: 4 Δενξέρω: 2

Τα άτομα μεγαλύτερης ηλικίας δείχνουν μια αποχή της τάξης του 50%. Ενώ κανείς τους δεν έχει λογαριασμό στο Googleplus. Χρησιμοποιούν συχνά το λογαριασμό τους, παρόλα αυτά δεν είναι προτεραιότητα, αφού δήλωσαν ότι δεν είναι από τις κύριες ασχολίες τους.

Όλοι πιστεύουν ότι υπάρχουν κίνδυνοι στις συγκεκριμένες σελίδες και δεν πιστεύουν ότι κάποιο από αυτά είναι ασφαλές.

Βιβλιογραφία

[1] http://www.pame.gr/diafora/kosmos/istoria-tou-diadiktuou.html#.T5QVAKt69-Y

[2] http://el.wikipedia.org/wiki/%CE%95%CE%B8%CE%B9%CF%83%CE%BC%CF%8C%CF%82_%CF%83%CF%84%CE%BF_%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

[3]http://www.foititelia.gr/home/internet/koinoniki-diktiosi-mithoi-kai-pragmatikotites.html

[4] http://en.wikipedia.org/wiki/Facebook

[5] http://www.techgear.gr/facebook-ipo-evaluation-43001/

[6] Facebook.com

[7]http://developers.facebook.com/opensource/

[8] facebook.com, Security Analysis of Social Networks, GRADUATE PROJECT REPORT

[9]Security Analysis of Social Networks, GRADUATE PROJECT REPORT

[10] http://en.wikipedia.org/wiki/Twitter

[11]http://en.wikipedia.org/wiki/Twitter, twitter.com, Security Analysis of Social Networks-GRADUATE PROJECT REPORT

http://www.onlinemagazine.gr/?p=298

[12] https://dev.twitter.com/opensource

[13]http://en.wikipedia.org/wiki/Twitter, Security Analysis of Social Networks-GRADUATE PROJECT REPORT

[14]http://www.freeweird.com/2012/04/google-plus-major-redesign.html

[15]http://www.wired.com/epicenter/2011/06/inside-google-plus-social/2/

[16]http://www.infoq.com/news/2011/07/Google-Plus

[17] http://www.wired.com/epicenter/2011/06/inside-google-plus-social/7/

[18] http://www.kirpininyeri.com/2011/07/google-plus-security-scene-1/

[19] Europevfacebook

[20] http://www.ethnos.gr/article.asp?catid=22769&subid=2&pubid=10604964

[21] http://www.mediagate.gr/Social-Media/item/17407-Dekaoktahroni-organose-ti-dolofonia-15hronoy-mathiti-sto-Facebook

[22] http://www.madata.gr/epikairotita/social/110215.html

[23] http://www.typologos.com/?p=3030

[24] http://www.ethnos.gr/article.asp?catid=22768&subid=2&pubid=10202951

[25] http://www.enet.gr/?i=news.el.article&id=141448

[26] http://www.tovima.gr/world/article/?aid=332613

[27] http://news.disabled.gr/?p=42921

[28] Security Analysis of Social Networks - GRADUATE PROJECT REPORT

[29] inews.gr 28/10/2011

[30] BRIAN STELTER and JENNIFER PRESTON, the new York times

[31] http://www.crn.com/slide-shows/security/219100457/a-look-back-at-12-twitter-attacks.htm?pgno=6

[32]http://www.crn.com/slide-shows/security/219100457/a-look-back-at-12-twitter-attacks.htm?pgno=9

[33] http://www.crn.com/slide-shows/security/219100457/a-look-back-at-12-twitter-attacks.htm?pgno=12

[34] http://www.crn.com/slide-shows/security/219100457/a-look-back-at-12-twitter-attacks.htm?pgno=13

[35] http://www.gmanetwork.com/news/story/255605/scitech/technology/new-twitter-spam-leads-to-fake-antivirus-attacks

[36] dailymail.co.uk

[37] : http://www.spamfighter.com/News-17257-Spam-Attacks-on-Twitter-Massive-during-November-2011-Kaspersky.htm

[38] Child pornography via Tweet: pedophiles abuse Twitter as a distribution channel

[39]http://gizmodo.com/5415423/ny-gangs-use-twitter-to-plan-crimes-while-the-ny-police-use-twitter-to-arrest-gangs

[40] http://www.lawofficer.com/article/news/criminals-use-flash-mob-networ

[41] http://www.mirrorfootball.co.uk

[42] http://www.care2.com/causes/nhl-player-subjected-to-racist-attacks-on-twitter.html

[43] http://www.aceshowbiz.com/news/view/00049103.html

[44] http://www.england365.com.cy

[45] Kaspersky Lab

[46] Google+: A Magnet for Scams and Malware

[47] http://threatpost.com/en_us/blogs/malware-poses-phony-google-plug-012612

[48] http://www.kompyuteran.com/2011/08/trojan-disguised-as-google-plus-app-attacks-android-phones/

[49] Fresh Phishing E-mail Scam yet again Attacks Gmail Users

[50] http://www.all4mama.gr/archives/10978