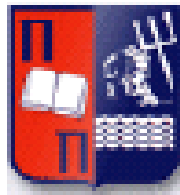


ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

Τμήμα: Ψηφιακών Συστημάτων

Μάρτιος 2015



Πτυχιακή Εργασία

*Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το
Facebook κ.λπ.*

Φοιτητής

Ρίκας Ιωάννης

Επιβλέπων Καθηγητής

Λαμπρινουδάκης Κωνσταντίνος

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον Αναπληρωτή Καθηγητή του τμήματος των Ψηφιακών Συστημάτων, κύριο Κωνσταντίνο Λαμπρινουδάκη, ο οποίος ήταν ο επιβλέπων της πτυχιακής μου εργασίας, για τη βοήθεια και την εξαιρετική καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια της εκπόνησής της. Τον ευχαριστώ πολύ ακόμα για την άριστη συνεργασία που υπήρχε μεταξύ μας.

Τέλος, θα ήθελα να ευχαριστήσω από τα βάθη της καρδιάς μου, τον πατέρα μου Κωνσταντίνο και τη μητέρα μου Αντωνία που είναι πάντα δίπλα μου και για την υποστήριξη και την εμπιστοσύνη που μου παρέχουν σε καθετί που κάνω

Εισαγωγή

Στη σημερινή εποχή όπου το διαδίκτυο αποτελεί το βασικότερο μέσο πληροφόρησης, ενημέρωσης και επικοινωνίας των σύγχρονων κοινωνιών, η χρήση των κοινωνικών δικτύων έχει επικρατήσει για την δικτύωση και την επικοινωνία μεταξύ των ανθρώπων αλλά και για άλλες σημαντικές για την κοινωνία λειτουργίες. Τα οφέλη των κοινωνικών δικτύων είναι αναρίθμητα, όμως και οι κίνδυνοι εξαιτίας της χρήσης τους είναι αντίστοιχα μεγάλοι. Ένας απ' αυτούς, κι ίσως και ο πιο σημαντικός, είναι η παραβίαση της ιδιωτικότητας των ατόμων. Στην παρούσα πτυχιακή εργασία θα μελετήσουμε το ρόλο των κοινωνικών δικτύων στη σημερινή κοινωνία και θα αναλύσουμε τη σχετική νομοθεσία που τα διέπει αλλά και το πώς, κατά τη χρήση τους, μπορεί να προστατευτεί η ιδιωτικότητα.

Στο πρώτο κεφάλαιο της εργασίας, γίνεται μια γενική αναφορά στα κοινωνικά δίκτυα, παρουσιάζεται η ιστορική τους αναδρομή και η εξέλιξη τους κι επίσης αναλύονται τα πιο δημοφιλή κοινωνικά δίκτυα της εποχής.

Στο δεύτερο κεφάλαιο καταγράφεται η έννοια της ιδιωτικότητας και γίνεται μια εμβάθυνση στα είδη και στα μοντέλα προστασίας της ιδιωτικότητας ενώ τονίζεται και η ανάγκη της προστασίας των προσωπικών δεδομένων.

Το τρίτο κεφάλαιο περιλαμβάνει θέματα σχετικά με τις απαιτήσεις της ιδιωτικότητας στα κοινωνικά δίκτυα καθώς αναλύονται οι κίνδυνοι που ελλοχεύουν και παρατηρούνται σχετικά με αυτήν.

Το τέταρτο κεφάλαιο αφορά τους τρόπους προστασίας της ιδιωτικότητας στα κοινωνικά δίκτυα με βάση τους κινδύνους που προαναφέρθηκαν.

Τέλος, στο πέμπτο κεφάλαιο γίνεται μια συμπερασματική αναφορά σχετικά με τα θέματα που καταγράφηκαν στα προηγούμενα κεφάλαια και προτείνονται περαιτέρω θέματα για ανάλυση για μελλοντικές εργασίες.

Πανεπιστήμιο Πειραιώς

Περιεχόμενα

Πίνακας Περιεχομένων

Ευχαριστίες.....	2
Εισαγωγή.....	3
Περιεχόμενα.....	5

Κεφάλαιο 1: Κοινωνικά Δίκτυα

1.1 Εισαγωγή στα κοινωνικά δίκτυα.....	9
1.2 Ιστορική αναδρομή και εξέλιξη.....	13
1.3 Τύποι κοινωνικών δικτύων.....	18
1.3.1 Ιστοσελίδες κοινωνικής δικτύωσης.....	19
1.3.2 Blogs.....	19
1.3.3 Forums.....	20
1.3.4 Multimedia sharing.....	22
1.3.5 Microblogs.....	22
1.4 Οφέλη και κίνδυνοι.....	23
1.5 Δημοφιλή κοινωνικά δίκτυα.....	27
1.5.1 Facebook.....	27
1.5.2 LinkedIn.....	31
1.5.3 Twitter.....	33
1.5.4 Google Plus.....	35
1.5.5 Pinterest.....	37
1.5.6 YouTube.....	38

Κεφάλαιο 2: Η Έννοια της Ιδιωτικότητας

2.1	Εισαγωγή	41
2.2	Ορισμός της ιδιωτικότητας	42
2.3	Ιστορικά στοιχεία	43
2.4	Είδη Ιδιωτικότητας	46
2.5	Η ανάγκη προστασίας προσωπικών δεδομένων	46
2.6	Μοντέλα προστασίας της ιδιωτικότητας	49

Κεφάλαιο 3: Κίνδυνοι Ιδιωτικότητας στα Κοινωνικά Δίκτυα

3.1	Απαιτήσεις ιδιωτικότητας στα κοινωνικά δίκτυα	53
3.1.1	Ανωνυμία	54
3.1.2	Μη παρατηρησιμότητα	56
3.1.3	Προστασία δεδομένων	57
3.1.4	Ψευδωνυμία	58
3.2	Κίνδυνοι ιδιωτικότητας στα κοινωνικά δίκτυα	59
3.2.1	Πλαστοπροσωπία	60
3.2.2	Κλοπή ταυτότητας	61
3.2.3	Κακόβουλο λογισμικό	62
3.2.4	Phishing	63
3.2.5	Data Mining	65

Κεφάλαιο 4: Προστασία της Ιδιωτικότητας στα Κοινωνικά Δίκτυα

4.1	Παραδείγματα παραβίασης της ιδιωτικότητας σε κοινωνικά δίκτυα	68
-----	---	----

*Προστασία της ιδιωτικότητας σε Social Networks και
πλατφόρμες όπως το Facebook κ.λπ.*

4.2 <u>Τρόποι προστασίας της ιδιωτικότητας στα κοινωνικά δίκτυα.....</u>	<u>72</u>
4.2.1 <u>Αντίμετρα χρηστών.....</u>	<u>73</u>
4.2.2 <u>Αντίμετρα κοινωνικών δικτύων.....</u>	<u>76</u>
<u>Κεφάλαιο 5: Συμπεράσματα.....</u>	<u>81</u>
<u>Βιβλιογραφία.....</u>	<u>84</u>

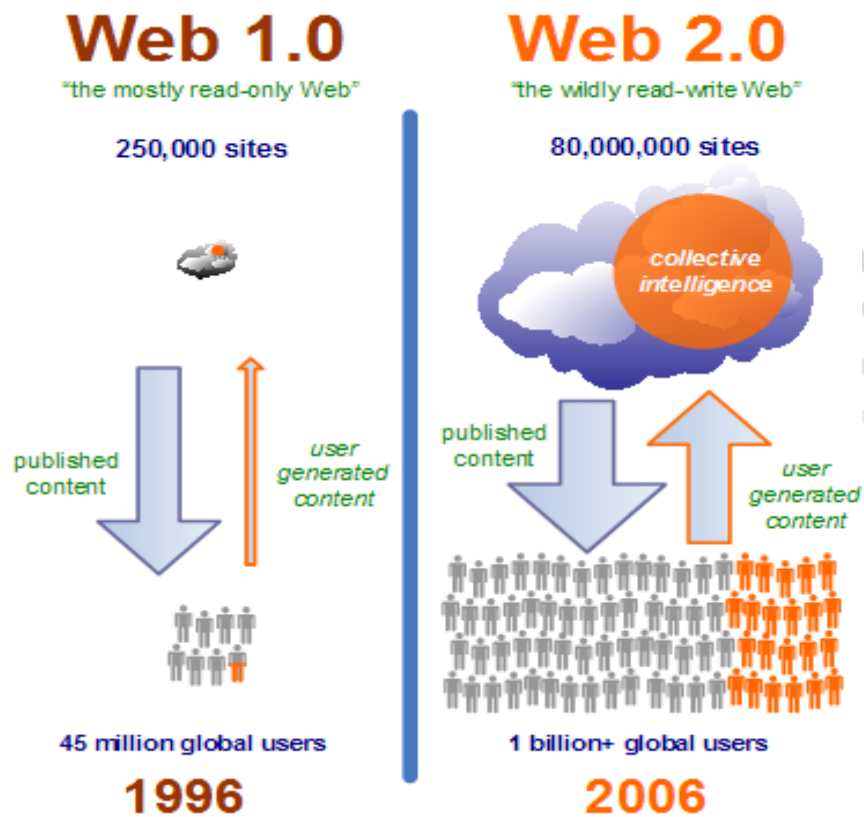
Πανεπιστήμιο Πειραιώς

Κεφάλαιο 1: Κοινωνικά Δίκτυα

1.1 Εισαγωγή στα κοινωνικά δίκτυα

Η εξέλιξη του διαδικτύου έχει επηρεάσει διάφορες πτυχές και κομμάτια της καθημερινότητας όλων των ανθρώπων. Το διαδίκτυο το οποίο αρχικά ξεκίνησε ως ένα εργαλείο συλλογής και αποθήκευσης πληροφοριών, εξελίχτηκε σε ένα πολύ σημαντικό μέσο για την ανθρώπινη επικοινωνία.

Πιο βασικό συστατικό αυτής της εξέλιξης ήταν η μετάβαση από το Web 1.0 στο Web 2.0. Ενώ πρωταρχικός στόχος του Web 1.0 ήταν η εύκολη πρόσβαση των χρηστών σε πληροφορίες και δεδομένα, ο κυριότερος στόχος του Web 2.0 ήταν η βέλτιστη επικοινωνία μεταξύ των χρηστών. Με την χρήση του Web 2.0 αναπτύχθηκαν μια σειρά από εργαλεία και πλατφόρμες όπου οι άνθρωποι μοιράζονται απόψεις, γνώμες και εμπειρίες. Το διαδίκτυο έπαψε πλέον να είναι ένα μέσο όπου ο χρήστης αλληλοεπιδρά με μια εφαρμογή αλλά έγινε το μέσο όπου οι χρήστες μπορούν να αλληλοεπιδράσουν μεταξύ τους με δεκάδες τρόπους. Η υπηρεσία που έχει επικρατήσει ως δημοφιλέστερη, και είναι πλέον γνωστή στο σύνολο των χρηστών είναι τα κοινωνικά δίκτυα, τα οποία αποτελούν ένα παγκόσμιο κοινωνικό φαινόμενο της σύγχρονης εποχής.



Εικόνα 1: Από το Web 1.0 στο Web 2.0

Τα κοινωνικά δίκτυα είναι μια κοινωνική δομή αποτελούμενη από κόμβους και συνδέσεις κόμβων οι οποίοι αντιπροσωπεύουν φυσικά πρόσωπα ή οργανισμούς. Οι συνδέσεις μεταξύ αυτών των κόμβων φανερώνουν έναν ή περισσότερους τύπους αλληλεξάρτησης ανάμεσά τους. Τέτοιοι τύποι αλληλεξάρτησης μπορεί να είναι φιλία, συγγένεια, ενδιαφέρον γνωριμίας, κοινά ενδιαφέροντα, εμπορικές συναλλαγές και γενικότερα οτιδήποτε μπορεί να συνδέσει ή να δημιουργήσει ένα είδος σχέσης ανάμεσα σε δύο ή περισσότερους ανθρώπους. Ένα άτομο συνδέεται με ορισμένους κόμβους, οι οποίοι αποτελούν τις επαφές του. Κάθε άτομο έχει μια αποκλειστική σχέση επικοινωνίας και αλληλεπίδρασης με τις επαφές του που διαφοροποιείται ανάλογα με τα πρότυπα και τους κανόνες του εκάστοτε κοινωνικού δικτύου. [1]

Σε κάθε κοινωνικό δίκτυο οι κόμβοι παραμένουν συνδεδεμένοι μεταξύ ανταλλάσσοντας πόρους, όπως δεδομένα και πληροφορίες. Οι ανταλλασσόμενοι αυτοί πόροι θεωρούνται ότι αποτελούν σχέσεις στα κοινωνικά δίκτυα, και τα άτομα που σχετίζονται με αυτές τις σχέσεις, διατηρούν έναν δεσμό. Ανάλογα με τον αριθμό και τον τύπο των ανταλλασσόμενων πόρων αντιστοιχεί και η ισχύς του κάθε δεσμού, αφού ο κάθε ένας μπορεί να είναι από αδύνατος έως δυνατός.

Πιο συγκεκριμένα στα δίκτυα αυτά οι χρήστες έχουν τη δυνατότητα να δημιουργήσουν και να αναρτήσουν στο διαδίκτυο ένα προφίλ είτε δημόσιο (δηλαδή ορατό σε όλους τους επισκέπτες του προφίλ), είτε ιδιωτικό (δηλαδή ορατό μόνο στους χρήστες που ο ιδιοκτήτης του προφίλ το επιτρέπει και σε κανέναν άλλο). Στα προφίλ αυτά οι χρήστες μπορούν να αναρτήσουν τα προσωπικά τους στοιχεία, τα προσωπικά τους ενδιαφέροντα, απόψεις, φωτογραφίες, βίντεο κ.α. Σκοπός της ανάρτησης αυτών των στοιχείων είναι η προβολή τους σε άλλους χρήστες και η αλληλεπίδραση μαζί τους. Οι χρήστες επιλέγουν με ποιους θα μοιράζονται τα προσωπικά τους στοιχεία δημιουργώντας λίστες με άλλους χρήστες, οι οποίοι αποκαλούνται «διαδικτυακοί φίλοι».

Η δημιουργία αυτών των λιστών και η σύναψη εν προκειμένω σχέσεων μεταξύ των χρηστών των κοινωνικών δικτύων διαφέρει από το ένα κοινωνικό δίκτυο στο άλλο. Οι συνηθέστερες μορφές σύναψης σχέσεων μεταξύ δύο χρηστών στα κοινωνικά δίκτυα είναι πρώτον με την συναίνεση του ενός από τους δύο και δεύτερον με την συναίνεση και των δύο χρηστών. Στην πρώτη περίπτωση αυτός που συναινεί στην σύναψη σχέσης αποκαλείται “follower” ή “fan” και στην δεύτερη αποκαλείται “friend”. Η σύναψη τέτοιων σχέσεων είναι από τα πιο σημαντικά

ζητήματα σ' ένα κοινωνικό δίκτυο και αποτελεί και τον πιο βασικό λόγο χρήσης τους.

Από τη στιγμή που δύο χρήστες επιλέγουν να είναι “friends” μπορούν να δουν την δραστηριότητα του άλλου καθώς επίσης και να δημοσιεύουν και οι ίδιοι περιεχόμενο στο προφίλ του «διαδικτυακού τους φίλου». Ακόμα δίνεται η δυνατότητα της μεταξύ τους ιδιωτικής συνομιλίας συνήθως μέσω μηνυμάτων αλλά και μέσω βιντεοκλήσης σε ορισμένες περιπτώσεις.



Εικόνα 2: Τα παγκόσμια Social Media

Ο κάθε χρήστης που δημιουργεί ένα προφίλ σ' ένα κοινωνικό δίκτυο στις περισσότερες περιπτώσεις μπορεί να χρησιμοποιήσει ένα προγενέστερο δίκτυο φιλίας. Μπορεί να αναζητήσει έναν συγκεκριμένο χρήστη με διάφορους τρόπους. Οι πιο συνηθισμένοι είναι μέσω της διεύθυνσης ηλεκτρονικού ταχυδρομείου του άλλου χρήστη και μέσω της αναζήτησης του ονόματός του. Επίσης οι περισσότερες σελίδες κοινωνικής δικτύωσης προτείνουν νέους «διαδικτυακούς φίλους» στους χρήστες τους με κριτήρια τα κοινά ενδιαφέροντα ή τους τρίτους «διαδικτυακούς φίλους» που έχουν μεταξύ τους. [2]

Χρόνο με το χρόνο οι σελίδες κοινωνικής δικτύωσης έχουν όλο και μεγαλύτερη απήχηση παγκοσμίως και ο αριθμός των ανθρώπων που τα χρησιμοποιούν ολοένα και αυξάνεται. Πολλοί χρήστες χρησιμοποιούν τα κοινωνικά δίκτυα για να κάνουν νέους φίλους, για να επικοινωνήσουν με άτομα που βρίσκονται σε μακρινή απόσταση από αυτούς, για να έρθουν σε επαφή με άτομα που έχουν κοινά ενδιαφέροντα ή κοινές πεποιθήσεις, για να προωθήσουν τα προϊόντα ή και τις υπηρεσίες της επιχείρησής τους και για πολλούς άλλους λόγους. Για τους λόγους αυτούς, όπως ακόμα και το γεγονός πως είναι ιδιαίτερα χρηστικά και προσαρμόσιμα στις ανάγκες όλων, εξηγούν τη διάδοσή τους. Εξάλλου και σύμφωνα με τους **(Ajjan & Hartshorne, 2008)** τα κοινωνικά δίκτυα «είναι διαδικτυακές υπηρεσίες που στην ουσία αποτελούν «προσωπικούς χώρους» για επικοινωνία και διαμοιρασμό περιεχομένου. Χαρακτηρίζονται από ευκολία στη χρήση, από γρήγορη προσαρμογή στις αλλαγές της καθημερινής ζωής, διευκολύνουν τη δημιουργία αυθόρμητων σχέσεων, και διευρύνουν την αλληλεπίδραση και την επικοινωνία.»

1.2 Ιστορική αναδρομή και εξέλιξη

Παρόλο που τα κοινωνικά δίκτυα έχουν ακμάσει με έναν απίστευτο ρυθμό τα τελευταία χρόνια, αυτά έκαναν τα πρώτα τους βήματα και εμφανίστηκαν σε πολύ πρώιμο στάδιο πριν από τρεις δεκαετίες.

Από το 1985 και μετά έχουμε την εμφάνιση των πρώτων γενικών online κοινοτήτων οι οποίες εισήγαγαν τα chat rooms (δωμάτια συζητήσεων) και ορισμένα βοηθητικά εργαλεία διαχείρισης με στόχο την

αλληλεπίδραση των χρηστών και την διακίνηση ιδεών σχετικά με διάφορα θέματα. Έτσι εμφανίστηκαν κατά σειρά τα “The WELL” (1985), “Theglobe.com” (1994), “GeoCities” (1994) και το “Tripod.com” (1995). Αυτές οι κοινότητες υπήρξαν οι πρώτοι πρόγονοι των σημερινών κοινωνικών δικτύων και ειδικότερα υπήρξαν η αφετηρία για τον όρο που σήμερα αποκαλούμε blogging. [3]

Ωστόσο η πρώτη ολοκληρωμένη σελίδα κοινωνικής δικτύωσης που εμφανίστηκε ήταν το SixDegrees.com (1997). Το εν λόγω site ήταν το πρώτο που συνδύαζε τα κυριότερα από τα χαρακτηριστικά που διακρίνουμε στα σημερινά κοινωνικά δίκτυα. Η δυνατότητα δημιουργίας profile, η αποστολή μηνυμάτων σε φίλους και η πλοήγηση σε λίστα φίλων ήταν μερικά από αυτά τα χαρακτηριστικά τα οποία προσέλκυσαν εκατομμύρια χρήστες στην συγκεκριμένη υπηρεσία. Παρά την υψηλή του δημοτικότητα όμως το πρώτο ολοκληρωμένο κοινωνικό δίκτυο έκλεισε το 2000.



Εικόνα 3: Η αρχική σελίδα του SixDegrees.com

Παρόμοιες προσπάθειες ανάμεσα σ’ αυτά τα χρόνια υπήρξαν από πολλές άλλες κοινότητες όπως το “blackplanet.com”, το “MiGente.com” και το “LiveJournal.com” στα οποία ένας χρήστης μπορούσε να δημιουργήσει profile και να προσθέσει φίλους χωρίς την έγκριση του

άλλου μέρους. Επίσης στις αρχές του 21^{ου} αιώνα είχαμε την εμφάνιση των πρώτων κοινωνικών δικτύων που έδιναν έμφαση στις επιχειρήσεις. Αρχικά το “Ryze.com” και λίγο αργότερα το “LinkedIn” θέλησαν να βοηθήσουν τα άτομα να έρθουν σε επαφή με τα επιχειρηματικά τους δίκτυα και να βελτιώσουν το επιχειρηματικό τους προφίλ. Το LinkedIn θεωρείται μέχρι σήμερα το κορυφαίο κοινωνικό δίκτυο για επαγγελματίες. [4]

Το 2002 εμφανίστηκε το “Friendster” το οποίο έμελλε να γίνει γρήγορα πολύ δημοφιλές αλλά και εξίσου απότομα να φθαρεί και να πέσει η δημοτικότητά του. Αιτίες για την υποβάθμιση του “Friendster” ήταν η υπερφόρτωση των servers της σελίδας λόγω του μεγάλου πλήθους των χρηστών που οδήγησε σε τεχνικά προβλήματα αλλά και η απογοήτευση των χρηστών για την διαχείριση του “Friendster” από τους υπεύθυνους της σελίδας. Οι δύο αυτοί λόγοι οδήγησαν σε μαζική αποχώρηση της πλειοψηφίας των χρηστών από το συγκεκριμένο κοινωνικό δίκτυο άρα και στην παρακμή του. Αυτό το γεγονός κατάφερε να το εκμεταλλευτεί ένα άλλο κοινωνικό δίκτυο το οποίο είχε κάνει την εμφάνιση του λίγους μήνες πριν. Το “MySpace” ιδρύθηκε το 2003 και ένα χρόνο αργότερα είχε γίνει το κορυφαίο κοινωνικό δίκτυο της εποχής. Αρχικά προσέλκυσε τους δυσαρεστημένους χρήστες του “Friendster” φτιάχνοντας μια ισχυρή βάση εγγεγραμμένων χρηστών και στη συνέχεια κατάφερε να αναπτυχθεί σε βαθμό ώστε τα επόμενα χρόνια να έχουν profile στο “MySpace” δεκάδες εκατομμύρια άτομα. Αυτή του η επιτυχία οφείλεται κυρίως στον πολύ καλό του σχεδιασμό και στο ότι ήταν το πρώτο κοινωνικό δίκτυο που επέτρεπε στους χρήστες να προσαρμόσουν όπως ήθελαν το profile τους με την χρήση html κώδικα. Ακόμα ένα άλλο στοιχείο που βοήθησε στην επιτυχία του “MySpace” ήταν η εκθετική αύξηση των γρήγορων

συνδέσεων internet παγκοσμίως, που οδήγησε όλο και πιο μεγάλο μέρος του πληθυσμού στην επιθυμία χρήσης σελίδων κοινωνικής δικτύωσης.

Μια ακόμα σελίδα κοινωνικής δικτύωσης που ιδρύθηκε το 2004 και που είχε πολύ μεγάλη επιτυχία και απότομη έκρηξη του αριθμού των χρηστών της ήταν το “Hi5”. Ενδεικτικά αναφέρεται ότι μεταξύ άλλων, βρέθηκε ανάμεσα στις 20 πρώτες ιστοσελίδες σε επισκεψιμότητα παγκοσμίως και επιπρόσθετα ήταν το κορυφαίο κοινωνικό δίκτυο σε πολλές χώρες στην Ευρώπη και στη Λατινική Αμερική. Επίσης από το 2004 και μετά άρχισαν να δημιουργούνται ιστοσελίδες με κάποια χαρακτηριστικά κοινωνικών δικτύων που παρείχαν υπηρεσίες σε κάποιο συγκεκριμένο τομέα όπως σε φωτογραφίες ή σε βίντεο ή σε μουσική ή σε μηνύματα ή και σε άλλους τομείς. Έτσι έχουμε την εμφάνιση σελίδων όπως του “YouTube”, του “Flickr”, του “Last.FM” οι οποίες γνώρισαν πολύ μεγάλη επιτυχία και είναι μέχρι σήμερα ανάμεσα στις κορυφαίες στον τομέα τους. [4]



Εικόνα 4: Το λογότυπο του “Hi5”

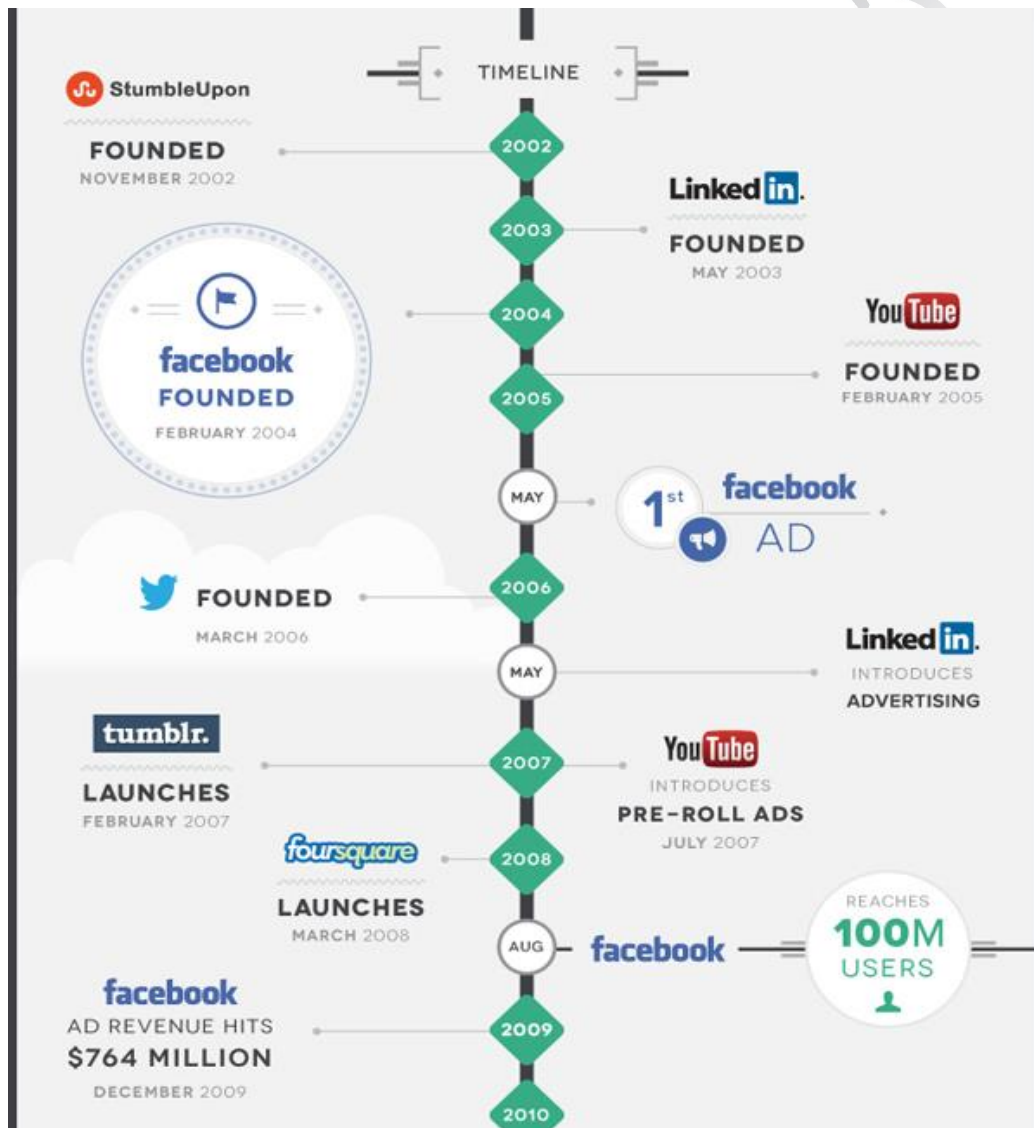
Όπως είδαμε το 2004 ιδρύθηκαν αρκετές σελίδες κοινωνικής δικτύωσης που είναι επιτυχημένες μέχρι και σήμερα, όμως η συγκεκριμένη χρονιά

μπορεί να χαρακτηριστεί ως χρονιά «ορόσημο» για τα κοινωνικά δίκτυα για έναν ακόμη λόγο. Τον Φεβρουάριο του έτους αυτού ξεκίνησε τη λειτουργία του η ιστοσελίδα που έμελλε να κυριαρχήσει στα κοινωνικά δίκτυα τα επόμενα χρόνια και εν τέλει να χαρακτηριστεί ως ένα από τα μεγαλύτερα κοινωνικά φαινόμενα της εποχής μας. Το «Facebook» ιδρύθηκε από τον Mark Zuckerberg και αρχικά ήταν διαθέσιμο μόνο για τους φοιτητές του αμερικάνικου πανεπιστημίου “Harvard”. Μετά την επιτυχία που είχε στο “Harvard” το «Facebook» σιγά σιγά επεκτάθηκε και έγινε διαθέσιμο και για άτομα που φοιτούσαν σε άλλες σχολές. Τελικά έγινε διαθέσιμο για όλους τους χρήστες παγκοσμίως στα τέλη του 2006 και έκτοτε παρουσίασε φοβερή άνοδο και δημοτικότητα. Σήμερα θεωρείται αδιαμφισβήτητο το κορυφαίο κοινωνικό δίκτυο παγκοσμίως και το χρησιμοποιούν εκατοντάδες εκατομμύρια άνθρωποι ανά τον κόσμο ενώ έχουν γίνει άπειρες συζητήσεις για το κοινωνικό αυτό «φαινόμενο». Εκτός της πολύ ευπαρουσίαστης και απλής πλατφόρμας του “Facebook” που κέρδισε τις εντυπώσεις των χρηστών, ένα άλλο σημαντικό στοιχείο που βοήθησε στη μεγάλη δημοτικότητά του ήταν η δυνατότητα ανάπτυξης εφαρμογών από τρίτους προγραμματιστές οι οποίες χρησιμοποιούνται μέσω του “Facebook”. [5]

Την τελευταία δεκαετία ξεκίνησαν την λειτουργία τους κι άλλες ιστοσελίδες κοινωνικής δικτύωσης που άφησαν το στίγμα τους τα τελευταία χρόνια. Κυριότερη εξ’ αυτών είναι το “Twitter”, η πλατφόρμα του οποίου ξεκίνησε τη λειτουργία της το 2006 και επέτρεπε την ανάρτηση σύντομων μηνυμάτων έως 140 χαρακτήρων στη σελίδα του κάθε χρήστη. Είναι ένα κοινωνικό δίκτυο που απέκτησε μεγάλη δημοτικότητα και θεωρείται μέχρι και σήμερα το «αντίπαλο δέος» του “Facebook”. Αντίθετα το “Google Plus” που δημιουργήθηκε από την

Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το Facebook κ.λπ.

κολοσσό εταιρία “Google” το 2011, με πολλά κοινά στοιχεία με το δημιούργημα του Zuckerberg και με σκοπό να ξεπεράσει το “Facebook”, απέτυχε να κερδίσει την προσδοκώμενη μάζα των χρηστών με αποτέλεσμα την όλο και πιο φθίνουσα δραστηριότητα σε αυτό.



Εικόνα 5: Η πρόσφατη ιστορία των κοινωνικών δικτύων

1.3 Τύποι κοινωνικών δικτύων

Τα κοινωνικά δίκτυα μπορούν να κατηγοριοποιηθούν σε ορισμένες υποκατηγορίες. Οι κυριότερες από αυτές αναλύονται στη συνέχεια.

1.3.1 Ιστοσελίδες κοινωνικής δικτύωσης

Οι ιστοσελίδες κοινωνικής δικτύωσης αποτελούν εικονικές online κοινότητες στις οποίες ένας χρήστης δημιουργεί ένα προφίλ με προσωπικές πληροφορίες και μπορεί να διαμοιραστεί περιεχόμενο μέσα σε αυτό με τους φίλους του ή με τις ομάδες χρηστών που έχει επιλέξει να αλληλεπιδρά. Αποτελούν την πιο διαδεδομένη μορφή των κοινωνικών δικτύων και αποτέλεσαν το πρώτο μέσο για τη διάδοση της κοινωνικής δικτύωσης. Στόχος των ιστοσελίδων αυτών είναι η κοινωνικοποίηση των χρηστών με φίλους, συγγενείς, συνάδερφους, γνωστούς κλπ. Οι πιο γνωστές ιστοσελίδες κοινωνικής δικτύωσης διαχρονικά είναι το “Facebook”, το “Myspace” και το “Google Plus”. Το πρώτο αποτελεί το πιο γνωστό και δημοφιλές κοινωνικό δίκτυο παγκοσμίως και είναι από τα βασικότερα σημεία αναφοράς και συζήτησης για τον 21^ο αιώνα.

1.3.2 Blogs

Τα blogs ή ιστολόγια αποτελούν συνήθως διαδικτυακά προσωπικά ημερολόγια ενός χρήστη. Οι δημιουργοί των ιστολογίων μπορούν να










αναρτήσουν στους διαδικτυακούς αυτούς τόπους καταχωρήσεις κειμένων όπως απόψεις, πληροφορίες, γνώμες, σημειώσεις και γενικά οτιδήποτε μπορεί να χαρακτηριστεί σαν καταχώρηση προσωπικού ημερολογίου. Τις περισσότερες φορές σε αυτά οι δημοσιεύσεις εμφανίζονται σε αντίστροφη χρονολογική σειρά, δηλαδή η πιο πρόσφατη δημοσίευση εμφανίζεται πρώτη, όμως έχουν πολύ μεγαλύτερες δυνατότητες παραμετροποίησης της προσωπικής σελίδας του κάθε χρήστη σε σχέση με τις ιστοσελίδες κοινωνικής δικτύωσης. Τα blogs διαχειρίζονται από ένα άτομο, αλλά είναι δυνατή η αλληλεπίδραση με άλλους χρήστες οι οποίοι μπορούν να διαβάσουν και να σχολιάσουν μια δημοσίευση. Οι πιο γνωστές πλατφόρμες δημιουργίας ενός blog είναι το “Blogger” και το “WordPress”. [6]

1.3.3 Forums

Ένα forum του διαδικτύου είναι μια online ιστοσελίδα συζητήσεων όπου οι χρήστες μπορούν να αναρτήσουν τα μηνύματα τους σχετικά με κάποιο θέμα ανταλλάσσοντας απόψεις με άλλους χρήστες. Μια τέτοια ιστοσελίδα αναφέρεται αποκλειστικά σε ένα ή περισσότερα θέματα συζητήσεων όπως για παράδειγμα μια ποδοσφαιρική ομάδα ή θέματα σχετικά με την τεχνολογία ή σχετικά με την ροκ μουσική κ.λπ. Ένα forum λοιπόν με πολλούς ενεργούς χρήστες μπορεί να περιέχει μεγάλο αριθμό πληροφοριών γύρω από ένα θέμα και είναι ένα εξαιρετικό μέσο ανταλλαγής απόψεων, ιδεών και γνώσεων. Σε ένα forum ανάλογα με τα δικαιώματα του κάθε χρήστη μπορεί τα μηνύματα του να χρειάζονται έγκριση από τον διαχειριστή του εκάστοτε forum ώστε να προβληθούν σε

**Προστασία της ιδιωτικότητας σε Social Networks και
πλατφόρμες όπως το Facebook κ.λπ.**

αυτό. Επίσης ένα forum συζητήσεων είναι ιεραρχικό και έχει τη μορφή «δέντρου» στη δομή του. Έτσι τα forum μπορούν να συμπεριλαμβάνουν έναν αριθμό από άλλα υπό-forums, κάθε ένα από τα οποία μπορεί να έχει πάνω από ένα “topic”(θέμα). Σ’ ένα “topic” καθενός forum, κάθε νέα συζήτηση που ξεκινάει ονομάζεται “thread”(νήμα), και στο καθένα από τα “threads” μπορούν όσοι χρήστες επιθυμούν να αναρτήσουν τα μηνύματά τους. [7]

Forum		Last Post	Threads	Posts
Practically Networked				
	General Discussions (4 Viewing)	VPN vs Telnet by cszeto Today 07:07 AM	1,543	5,199
	Sharing (10 Viewing) Discuss problems or contribute tips about how you shared an Internet connection, data, printers and more with multiple users.	2 x DSL lines & 1 GB Hub by nward4 Today 10:15 AM	2,346	7,996
	Wireless Networks (5 Viewing) Tips, tricks and advice for setting up an 802.11-based network in your home or office.	Health issue concern by cszeto Today 07:02 AM	2,206	7,779
	Alternative Networks Networks aren't just Ethernet and radio waves. Ask questions here about HomePlug (powerline), HomePNA (phoneline), and any other unique network types.	Remote Gaming by cszeto 02-05-2008 05:17 AM	79	298
	Routers/Hardware (10 Viewing) Discussions and troubleshooting the latest routers, switches, hubs, NICs and other products for SOHO networking.	Linksys WRT54G Boot up Problem by cszeto Today 06:59 AM	1,776	5,748
	Applications/Software (3 Viewing) Share with others the software you use to keep a network running smoothly.	Access Server online by cszeto 02-19-2008 01:29 PM	94	315
	Security Discuss the security issues any small network faces and get some solutions to your problems.	The freeware latest version... by cszeto 10-24-2007 06:18 PM	56	186
	Networking Lounge A place for casual chat with fellow networkers	employers laptop on my home... by cszeto 04-12-2008 10:06 AM	29	59
	Feedback Have comments/suggestions about the forum? Post them here!	Forum trouble by JPhyc 07-27-2007 11:50 AM	1	4

Εικόνα 6: Η εμφάνιση ενός “forum”

1.3.4 Multimedia sharing

Όλες οι υπόλοιπες ιστοσελίδες κοινωνικής δικτύωσης που αναφέρθηκαν και θα αναφερθούν έχουν σαν κοινή συνισταμένη την δυνατότητα ανταλλαγής πληροφοριών-δεδομένων. Σε αντίθεση με αυτές, οι ιστοσελίδες multimedia sharing, ή αλλιώς ιστοσελίδες κοινής χρήσης πολυμέσων δίνουν τη δυνατότητα κοινής χρήσης φωτογραφιών, ήχου ή βίντεο μεταξύ των χρηστών. Στις σελίδες multimedia sharing οι χρήστες δεν είναι απαραίτητο να δημιουργήσουν το δικό τους προφίλ ενώ μπορούν να σχολιάσουν τις αναρτήσεις περιεχομένου των άλλων χρηστών. Η πιο γνωστή ιστοσελίδα multimedia sharing είναι το “YouTube” που επιτρέπει τον διαμοιρασμό οποιουδήποτε είδους βίντεο και έχει τεράστια απήχηση στο κοινό. Το “YouTube” ακόμα αποτελεί και ένα εξαιρετικό μέσον προώθησης υπηρεσιών από επιχειρήσεις προς καταναλωτές. Στον τομέα της φωτογραφίας κυριαρχούν το “Flickr” και το “Pinterest” το οποίο είναι το νεότερο από τα πολύ επιτυχημένα social network σε όλο τον πλανήτη. Τέλος η γνωστότερη υπηρεσία multimedia sharing για ηχητικά αρχεία είναι το “Soundcloud” που ξεκίνησε τη λειτουργία του το 2008. [8]

1.3.5 Microblogs

Τα microblogs στην ουσία αποτελούν μια υποκατηγορία των Blogs που αναλύθηκαν προηγουμένως. Ουσιαστικά τον όρο των microblogs τον εισήγαγε το “Twitter” με την ίδρυσή του το 2006. Το “Twitter” θεωρείται

το 2^ο πιο δημοφιλές κοινωνικό δίκτυο σήμερα, μετά το “Facebook”, καθώς έχει πάνω από 250 εκατομμύρια χρήστες και έτσι θεωρείται αδιαπραγμάτευτα το κορυφαίο microblog. Όπως και στα blogs, έτσι και εδώ ένας χρήστης μπορεί με τις αναρτήσεις του να εκφράσει τις ιδέες του, τις απόψεις του, τα συναισθήματά του, τις πληροφορίες του αλλά και να σχολιάσει τις αναρτήσεις των άλλων χρηστών. Η βασική διαφορά με τα blogs είναι το γεγονός πως σ’ ένα microblog, η κάθε ανάρτηση ή καταχώρηση είναι πολύ σύντομη, όπως στο “Twitter” για παράδειγμα που είναι 140 χαρακτήρες το πολύ η κάθε καταχώρηση. Μια ακόμα διαφορά με τα blogs, είναι πως στα microblogs είναι πολύ λιγότερες οι δυνατότητες παραμετροποίησης της προσωπικής σελίδας του κάθε χρήστη σε σχέση με αυτά. Τα microblogs επίσης χρησιμοποιούνται πλέον ευρύτατα από ειδησεογραφικά δίκτυα σε όλο τον κόσμο για την αναφορά και την κάλυψη ζωντανών γεγονότων και έκτακτων ειδήσεων. [9]

1.4 Οφέλη και κίνδυνοι

Με την χρήση των μέσων κοινωνικής δικτύωσης μπορούν να προκύψουν πολλά και ποικίλα οφέλη για τους χρήστες τους τα οποία μπορούν να εξηγήσουν σε μεγάλο βαθμό την όλο και μεγαλύτερη τους εξάπλωση παγκοσμίως. Ένα από τα πιο σημαντικά πλεονεκτήματα των κοινωνικών δικτύων λοιπόν, είναι το γεγονός πως επιτρέπουν την άμεση αλληλεπίδραση μεταξύ των χρηστών κάτι που διάφορα μέσα του διαδικτύου προσπάθησαν να επιτύχουν, χωρίς όμως να τα καταφέρουν όπως τα κοινωνικά δίκτυα. Επίσης ένα παρεμφερές πλεονέκτημα είναι το

ότι τα μέσα κοινωνικής δικτύωσης παρέχουν στους χρήστες τους τη δυνατότητα δημιουργίας σχέσεων με πολλούς άλλους χρήστες παγκοσμίως που βρίσκονται πολύ μακριά ο ένας από τον άλλο, με διαφορετικά χαρακτηριστικά, συνήθειες και από διαφορετικές κουλτούρες και πολιτισμούς. Έτσι με λίγα λόγια τα κοινωνικά δίκτυα μηδενίζουν τις αποστάσεις ανάμεσα στους χρήστες για την μεταξύ τους επικοινωνία.

Ακόμα ένα όφελος που παρατηρείται εξαιτίας της χρήσης των κοινωνικών δικτύων είναι το γεγονός πως καλύπτουν την ανάγκη σε έναν άνθρωπο να μοιραστεί με άλλους ανθρώπους κάποιες σκέψεις, απόψεις, ή ιδέες του, όπως επίσης και η δυνατότητα που έχει ένας χρήστης να αναζητήσει και να διαβάσει σκέψεις άλλων ανθρώπων που τον ενδιαφέρουν ή ακόμα και να βρει φωτογραφίες ή βίντεο προερχόμενα από τους “διαδικτυακούς του φίλους”.

Επιπρόσθετα ένα άλλο σημαντικό μέρος των πλεονεκτημάτων που έχουν να κάνουν με τα κοινωνικά δίκτυα είναι το κομμάτι της γνώσης και των πληροφοριών. Με τη χρήση των μέσων κοινωνικής δικτύωσης έχουμε τη δυνατότητα της αστραπιαίας μετάδοσης των γεγονότων και την άμεση ενημέρωση για οτιδήποτε συμβαίνει στον κόσμο, τη στιγμή που συμβαίνει. Επίσης μέσω της ανοικτής επικοινωνίας που επιτυγχάνεται, ένας χρήστης μπορεί να ανακαλύψει περισσότερες πληροφορίες από άλλους χρήστες ή οργανισμούς κάτι που οδηγεί στη γενικότερη διάδοση της γνώσης. Δεν μπορεί να παραληφθεί επίσης και η ευκολότερη πρόσβαση σε ψυχαγωγικά μέσα εξαιτίας της χρήσης των κοινωνικών δικτύων.

Οι επιχειρήσεις είναι ένας ακόμα τομέας που τα μέσα κοινωνικής δικτύωσης ωφελούν. Έτσι μπορούμε να αναφέρουμε πως τα κοινωνικά δίκτυα δίνουν τη δυνατότητα της αύξησης των επιχειρηματικών επαφών και μπορούν να βελτιώσουν την επιχειρηματική φήμη της επιχείρησης με μηδαμινό ουσιαστικά κόστος, καθώς η εφαρμογή των τεχνικών του μάρκετινγκ και της έρευνας αγοράς θεωρείται πολύ αποδοτική μέσα από αυτά. Τέλος τα κοινωνικά δίκτυα παρουσιάζουν οφέλη και για τους εργαζομένους καθώς τους δίνουν μεγαλύτερες προοπτικές και ευκαιρίες στην εύρεση εργασίας, καθώς επίσης τους δίνουν και τη δυνατότητα της συζήτησης των ιδεών τους, να κάνουν ερωτήσεις στην εργοδοσία τους αλλά και να διεκδικήσουν τα εργασιακά τους δικαιώματα.



Εικόνα 7: Social Networking

Από την άλλη πλευρά του νομίσματος υπάρχουν και κάποιοι κίνδυνοι αλλά και κάποια μειονεκτήματα που προκύπτουν από την χρήση των μέσων κοινωνικής δικτύωσης. Ένα από αυτά τα μειονεκτήματα και ίσως το πιο σημαντικό είναι η επιβλαβής έκθεση της προσωπικής ζωής των χρηστών. Μέσω της χρήσης των κοινωνικών δικτύων οι προσωπικές πληροφορίες ενός χρήστη εκτίθενται με αποτέλεσμα να ελλοχεύουν πολλοί κίνδυνοι. Ένα συχνό φαινόμενο όπως και ένας κίνδυνος της χρήσης των κοινωνικών δικτύων είναι η κλοπή των προσωπικών

δεδομένων τα οποία μπορούν να χρησιμοποιηθούν για παράνομους σκοπούς. Επίσης είναι πολλές οι περιπτώσεις όπου οι χρήστες, ιδιαίτερα οι χρήστες νεαρής ηλικίας, βιώνουν τραυματικές εμπειρίες μέσα από την διαδικτυακή τους επαφή με πλήθος άγνωστων ατόμων. Η συναισθηματική κακοποίηση και ο διαδικτυακός εκφοβισμός των χρηστών μέσα από τα κοινωνικά δίκτυα είναι δύο φαινόμενα που παρουσιάζουν ιδιαίτερα ανησυχητική αύξηση τα τελευταία χρόνια.

Πέρα από τους κινδύνους που προκύπτουν για ένα άτομο εξαιτίας άλλων κακόβουλων χρηστών υπάρχουν και οι κίνδυνοι που ελλοχεύουν εξαιτίας του ίδιου του χρήστη για τον εαυτό του. Πολλές έρευνες έχουν δείξει ότι τα κοινωνικά δίκτυα λόγω της υπερβολικής χρήσης προκαλούν εθισμό σ' ένα μεγάλο ποσοστό των χρηστών τους με αποτέλεσμα την εξάρτηση σ' αυτά. Ο εθισμός αυτός φυσικά οδηγεί και σε μεγάλη σπατάλη χρόνου τον οποίο ένα άτομο, και κατ' επέκταση ολόκληρη η κοινωνία, θα μπορούσε να τον αξιοποιήσει πιο δημιουργικά. Κάτι ακόμα που δεν μπορεί να παραλειφθεί είναι η απαλοιφή των δια ζώσης διαπροσωπικών σχέσεων που προκύπτουν από την υπερβολική διαδικτυακή επικοινωνία.

Επιπρόσθετα η χρήση των κοινωνικών δικτύων αυξάνει τον κίνδυνο επίθεσης ιών από επίδοξους hackers καθώς είναι ένα πεδίο με τεράστιο αριθμό χρηστών που μεγάλο του μέρος είναι απαίδευτο στην προστασία από τέτοιες επιθέσεις. Ένα ακόμα θέμα που ταλαιπωρεί τους χρήστες στα κοινωνικά δίκτυα είναι η πληθώρα των διαφημιστικών μηνυμάτων που προβάλλονται από τα κοινωνικά δίκτυα προς αυτούς. Τέλος σε επίπεδο επιχειρήσεων η χρήση των κοινωνικών δικτύων μπορεί να οδηγήσει σε αρνητικά σχόλια από τους υπαλλήλους και στην δημιουργία

παρεξηγήσεων ή αντιδικιών είτε με την εργοδοσία είτε μεταξύ των χρηστών αυτών. [10]

1.5 Δημοφιλή κοινωνικά δίκτυα

1.5.1 Facebook

Ο ιστότοπος που μπορεί να χαρακτηριστεί ως συνώνυμο των κοινωνικών δικτύων στην εποχή μας και αντικειμενικά ο πιο επιτυχημένος και κερδοφόρος τέτοιου είδους ιστότοπος είναι αναμφίβολα το “Facebook”. Ιδρύθηκε το 2004 από τον Mark Zuckerberg και αρχικά προοριζόταν μόνο για τους φοιτητές του πανεπιστημίου του Harvard καθώς ήταν διαθέσιμο μόνο για εκείνους. Οι χρήστες μπορούσαν να εγγραφούν δωρεάν στην υπηρεσία και να δημιουργήσουν το προσωπικό τους προφίλ. Διαδόθηκε άμεσα εντός της κοινότητας του πανεπιστημίου καθώς έδινε τη δυνατότητα στους χρήστες να επικοινωνήσουν μεταξύ τους μέσω μηνυμάτων, να καταχωρούν τις προσωπικές τους πληροφορίες και να δημιουργούν ομάδες σχετικά με κάποιο θέμα. Η προέλευση του ονόματος του κοινωνικού αυτού δικτύου προέρχεται από τα έγγραφα παρουσίασης των μελών των πανεπιστημιακών κοινοτήτων που χρησιμοποιούσαν οι νέοι σπουδαστές για να γνωριστούν μεταξύ τους.



Εικόνα 8: Το λογότυπο του “Facebook”

Το “Facebook” γρήγορα ξέφυγε από τα όρια του Harvard και έγινε προσβάσιμο σταδιακά για όλους τους σπουδαστές πανεπιστημίων ενώ στη συνέχεια τέθηκε στη διάθεση και των μαθητών σχολείων. Το 2006 τελικά η υπηρεσία έγινε προσβάσιμη για όλους τους ανθρώπους του κόσμου που η ηλικία τους ήταν μεγαλύτερη από τα 13 έτη. Έπειτα η αύξηση των χρηστών του ήταν ραγδαία έτσι ώστε σήμερα να είναι το κορυφαίο μέσο κοινωνικής δικτύωσης. Σύμφωνα με μετρήσεις που πραγματοποιήθηκαν το 2013 το “Facebook” διαθέτει 1.2 δισεκατομμύρια μοναδικούς χρήστες εκ των οποίων τα 700 εκατομμύρια είναι άμεσα ενεργοί. Εξίσου εντυπωσιακοί αριθμοί μπορούν να θεωρηθούν τα 350 εκατομμύρια φωτογραφίες που “ανεβάζουν” καθημερινά οι χρήστες όπως επίσης και τα ετήσια κέρδη της υπηρεσίας που το 2012 ξεπέρασαν τα 5 δισεκατομμύρια δολάρια.

Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το Facebook κ.λπ.



Εικόνα 9: Η σελίδα εισόδου και εγγραφής του “Facebook”

Ένας χρήστης που εγγράφεται στην υπηρεσία του “Facebook” δημιουργεί το προσωπικό του προφίλ το οποίο, ανάλογα με τις ρυθμίσεις απορρήτου που θα επιλέξει ο χρήστης, μπορεί να είναι ορατό είτε μόνο στους “φίλους” του, είτε σε χρήστες που βρίσκονται σε κοινά με αυτόν δίκτυα, είτε σε όλους τους χρήστες του “Facebook”. Ο χρήστης αφού δημιουργήσει το προφίλ, μπορεί να το ενημερώσει με τις προσωπικές του πληροφορίες και έπειτα μπορεί να αναζητήσουν φίλους στο “Facebook” οι οποίοι μπορεί να είναι είτε πραγματικοί του φίλοι είτε άγνωστοι. Μετά από αυτή την αναζήτηση έχει τη δυνατότητα να στείλει “αίτημα φιλίας” στους χρήστες που επιθυμεί και στην περίπτωση που αυτοί οι χρήστες αποδεχτούν το “αίτημα φιλίας” τότε προστίθενται και οι δύο αντίστοιχα στη “λίστα φίλων” του καθενός. Ο κάθε χρήστης έχει τη δυνατότητα να “ανεβάσει” τις φωτογραφίες ή τα βίντεο που επιθυμεί στο προσωπικό του προφίλ έτσι ώστε να είναι ορατά στους “φίλους” του και ακόμα κατά τον ίδιο τρόπο μπορεί να γράψει ένα προσωπικό μήνυμα, ή “κατάσταση” όπως αποκαλείται αλλιώς, ώστε να εκφράσει τα συναισθήματά του, ή να εκφράσει την προσωπική του γνώμη ή άποψη σχετικά με οποιοδήποτε ζήτημα. Σε όλες αυτές τις δημοσιεύσεις οι υπόλοιποι χρήστες που έχουν

τα απαραίτητα δικαιώματα πρόσβασης μπορούν να σχολιάσουν τις δημοσιεύσεις αυτές ή μπορούν να δηλώσουν ότι τους αρέσει χρησιμοποιώντας το γνωστό button του “like”.



Εικόνα 10: Το σύμβολο του “like”

Οι χρήστες μπορούν να αλληλεπιδράσουν μεταξύ τους είτε δημόσια είτε ιδιωτικά. Στην πρώτη περίπτωση ένας χρήστης μπορεί να γράψει ότι θέλει στον “τοίχο” ενός άλλου χρήστη ώστε το μήνυμά του να είναι ορατό σε όλους τους φίλους του δεύτερου, ενώ στην άλλη περίπτωση μπορεί να γίνει χρήση του “inbox” ώστε δύο χρήστες να ανταλλάξουν μηνύματα μεταξύ τους τα οποία θα είναι ορατά μόνο σε εκείνους.

Επίσης πρέπει να αναφερθεί πως το “Facebook” υποστηρίζει την δυνατότητα της δημιουργίας ομάδων ή σελίδων (“Pages”) σχετικά με κάποιο θέμα αλλά και την δημιουργία εκδηλώσεων όπου ένας χρήστης μπορεί να προσκαλέσει τους “φίλους” του σε αυτές. Τέλος το “Facebook” υποστηρίζει και εφαρμογές, όπως παιχνίδια, από τρίτους προγραμματιστές οι οποίες μπορούν να εκτελεστούν μέσω της ιστοσελίδας του.

Το “Facebook” είναι ένα εξαιρετικό εργαλείο για την επικοινωνία των ανθρώπων κι ο μινιμαλιστικός σχεδιασμός του αλλά και η απλότητα της χρήσης του το βοήθησαν να είναι το πιο δημοφιλές μέσο κοινωνικής δικτύωσης. Όμως από άποψη ασφάλειας υπάρχουν αρκετοί

προβληματισμοί σχετικά με τον τόσο μεγάλο αριθμό των χρηστών που το χρησιμοποιούν αλλά και σχετικά με το πλήθος των πληροφοριών των χρηστών που υπάρχουν σ' αυτό. Οι προβληματισμοί αυτοί αφορούν κυρίως πιθανές απειλές για την προσωπική ασφάλεια των χρηστών εξαιτίας της διαθεσιμότητας των προσωπικών στοιχείων ενός χρήστη σε πολλούς άλλου ανθρώπους. Λόγω των πληροφοριών αυτών είναι ανησυχητικό το ενδεχόμενο κλοπής ταυτότητας από κάποιους χρήστες όπως επίσης και η προσωπική ασφάλεια του καθενός ειδικά σε περιπτώσεις όπου το εν δυνάμει θύμα μπορεί να ανήκει ή να υποστηρίζει ευάλωτες και στιγματιζόμενες κοινωνικές ομάδες όπως μειονότητες κτλ.

[11]

1.5.2 LinkedIn

Το “LinkedIn” αποτελεί το κορυφαίο κοινωνικό δίκτυο που απευθύνεται ειδικά σε επαγγελματίες, μπορεί να χαρακτηριστεί και σαν το “Facebook” των επαγγελματιών. Αυτό το μέσο κοινωνικής δικτύωσης ξεκίνησε τη λειτουργία του το 2003 και άμεσα ξεχώρισε λόγω του ειδικού προσανατολισμού του. Πλέον απαριθμεί πάνω από 300 εκατομμύρια χρήστες σε όλο τον κόσμο και υπερτερεί σημαντικά έναντι των ανταγωνιστών του.



Εικόνα 12: “LinkedIn”

Οι επαγγελματίες που χρησιμοποιούν το “LinkedIn”, αφού δημιουργήσουν το προσωπικό τους προφίλ, έπειτα έχουν τη δυνατότητα να δημιουργήσουν ένα δίκτυο από τις επαγγελματικές τους επαφές. Αρχικά δημιουργώντας μια “σύνδεση” (“connection”) με τους ανθρώπους με τους οποίους επιθυμούν. Αυτές οι απευθείας συνδέσεις μεταξύ των χρηστών αποκαλούνται άμεσες και μαζί με τις συνδέσεις δεύτερου βαθμού (τις άμεσες συνδέσεις του κάθε χρήστη με τον οποίο δημιουργήθηκε η αρχική άμεση σύνδεση) αποτελούν το δίκτυο του κάθε χρήστη.

Αυτή η δυνατότητα, της επαφής δηλαδή ενός επαγγελματία με άλλους επαγγελματίες που δεν τους γνωρίζει σε προσωπικό επίπεδο, προσφέρει σε αυτόν ένα εξαιρετικά μεγάλο εύρος επαγγελματικών επαφών και του εξασφαλίζει μια ιδιαίτερη διευκόλυνση στην αναζήτηση δουλειάς, άλλων ανθρώπων και επαγγελματικών ευκαιριών. Έτσι δίνεται η δυνατότητα σε εργοδότες να αναζητήσουν νέους καταρτισμένους εργαζομένους, και σε χρήστες που αναζητούν εργασία την ευκαιρία να βρουν νέες θέσεις εργασίας μέσα από τα προφίλ εταιριών ή διευθυντικών στελεχών αλλά και να εξασφαλίσουν κάποια σύσταση από κάποια κοινή επαφή με την δυνητική τους εργοδοσία. [12]

1.5.3 Twitter

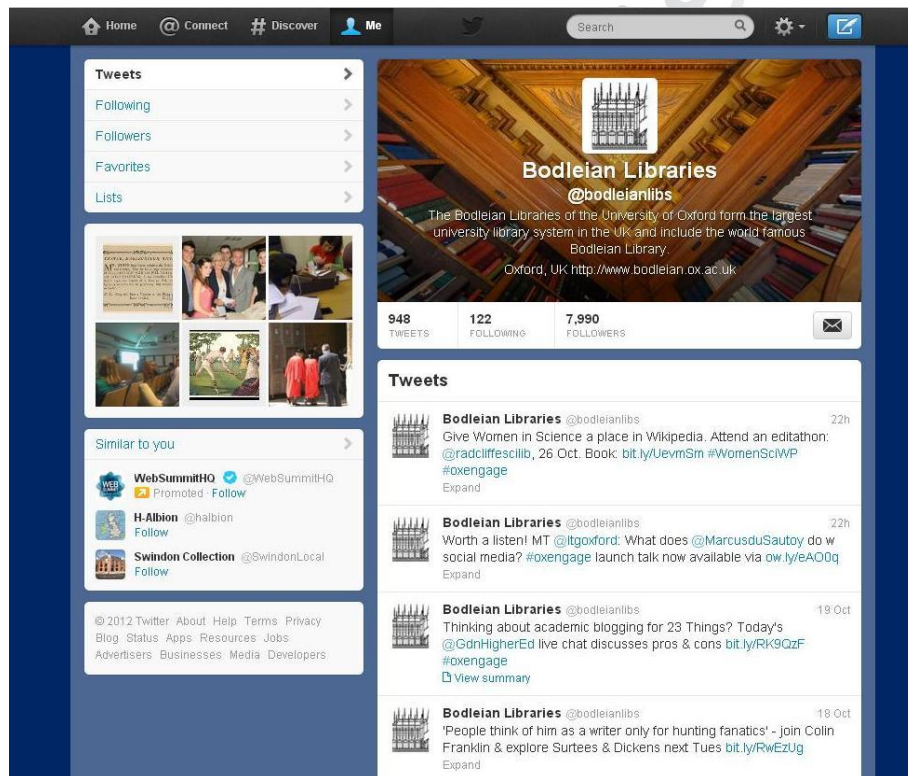
Μια από τις πιο δημοφιλείς σελίδες κοινωνικής δικτύωσης των τελευταίων ετών και ο κυριότερος ανταγωνιστής του “Facebook” είναι το “Twitter”. Το κοινωνικό δίκτυο που έχει για λογότυπο ένα καναρίνι ξεκίνησε τη λειτουργία του το 2006 και το 2014 έφτασε να έχει πάνω από 250 εκατομμύρια ενεργούς χρήστες.

Το “Twitter” εντάσσεται στην κατηγορία του microblogging καθώς η φιλοσοφία του στηρίζεται στα μικρά μηνύματα, 140 χαρακτήρων ή λιγότερων, που μπορούν να δημοσιεύσουν οι χρήστες. Λόγω αυτού του χαρακτηριστικού το “Twitter” θεωρείται το πιο γρήγορο και άμεσο μέσο κοινωνικής δικτύωσης αφού δεν υποστηρίζει οτιδήποτε περιττό παρά μόνο την άμεση δημοσίευση των μηνυμάτων που επιθυμεί να εκφράσει ο κάθε χρήστης.

Κατά την αρχική του περιήγηση στο “Twitter” ο κάθε χρήστης φτιάχνει, όπως και στα περισσότερα κοινωνικά δίκτυα, ένα προσωπικό προφίλ, όμως σε αντίθεση με το “Facebook” τα προσωπικά στοιχεία που καταχωρεί είναι πολύ λιγότερα ενώ και το σύστημα φιλίας είναι διαφορετικό. Εδώ ένας χρήστης μπορεί να κάνει “follow” έναν άλλον χρήστη χωρίς να χρειάζεται την αποδοχή του δεύτερου. Έτσι ένας χρήστης στην ουσία μπορεί να παρακολουθεί τα μηνύματα όποιου άλλου χρήστη επιθυμεί χωρίς όμως να συμβαίνει απαραίτητα και το αντίστροφο.

Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το Facebook κ.λπ.

Η προσωπική σελίδα (ή προφίλ) του κάθε χρήστη εμφανίζει τα μηνύματα που ο κάθε χρήστης καταχωρεί. Αυτά τα μηνύματα είναι γνωστά ως “τιτίβισματα” (“tweets”). Το ανώτερο όριο χαρακτήρων του κάθε “tweet” είναι 140 χαρακτήρες. Όταν ένας χρήστης καταχωρεί ένα “τιτίβισμα” αυτό γίνεται ορατό σε όλους τους χρήστες που τον “ακολουθούν” (“followers”). Σ’ ένα “tweet” μπορεί να γίνει χρήση ετικετών (“hashtags”). Όταν μια ετικέτα χρησιμοποιείται σε πολλά “tweets” τότε δημιουργείται μια “τάση” (“trend”) και οι τάσεις αυτές εμφανίζονται στην αρχική σελίδα του “Twitter”.



Εικόνα 13: Ενδεικτικό profile στο “Twitter”

Ο κάθε χρήστης μπορεί να σχολιάσει το “tweet” ενός άλλου χρήστη που ακολουθεί με ένα νέο “tweet” το οποίο επίσης δεν μπορεί να ξεπερνάει τους 140 χαρακτήρες. Επίσης υπάρχει και η δυνατότητα της αποστολής

και λήψης προσωπικών μηνυμάτων μεταξύ δύο χρηστών τα οποία είναι ορατά μόνο σε εκείνους.

Το “Twitter” χρησιμοποιείται ευρέως για άμεση μετάδοση πληροφοριών μεταξύ φίλων αλλά χρησιμοποιείται ακόμα περισσότερο από επιχειρήσεις και οργανισμούς για τη μετάδοση των τελευταίων νέων της εταιρίας, ενώ ειδικότερα παρατηρείται πολύ εκτεταμένη χρήση από ειδησεογραφικά και τηλεοπτικά δίκτυα για την άμεση μετάδοση ειδήσεων. [13]

1.5.4 Google Plus

Μια από τις πρόσφατες σε λανσάρισμα ιστοσελίδες κοινωνικής δικτύωσης είναι το “Google Plus” (“Google +”). Το 2011 η κολοσσός εταιρία “Google” παρουσίασε τη δοκιμαστική έκδοση του νέου δικού της κοινωνικού δικτύου με στόχο να ξεπεράσει τις προηγούμενες αντίστοιχες και αποτυχημένες προσπάθειές της (“Buzz”, “Wave”) αλλά και να κυριαρχήσει σε ένα κλάδο όπου η απόκτηση μεγάλου μεριδίου της αγοράς θα εγγυόταν εξωφρενικά κέρδη.

Η μεγαλύτερη εταιρία διαδικτυακών υπηρεσιών κατάφερε να εκμεταλλευτεί το όνομα της και αφότου έγινε διαθέσιμο σε όλους τους χρήστες, σήμερα το “Google Plus” έχει πάνω από 300 εκατομμύρια ενεργούς χρήστες τη στιγμή που ο αριθμός των εγγεγραμμένων χρηστών ξεπερνάει το 1 δισεκατομμύριο. Είναι το πιο άμεσα ανεπτυγμένο μέσο κοινωνικής δικτύωσης καθώς έφτασε τους 50 εκατομμύρια χρήστες σε μόλις 90 μέρες λειτουργίας, τη στιγμή που κοινωνικά δίκτυα σαν το

“Twitter” και το “Facebook” χρειάστηκαν πάνω από 1000 ημέρες για το ίδιο επίτευγμα.

Όπως και στο “Facebook”, έτσι και στο “Google Plus” η βασική δραστηριότητα είναι η επικοινωνία των χρηστών και η ανταλλαγή πληροφοριών. Ο χρήστης με την εγγραφή του δημιουργεί ένα προσωπικό προφίλ στο οποίο συμπληρώνει διάφορα στοιχεία και πληροφορίες για τον εαυτό του. Ακόμα μπορεί να αναρτήσει προσωπικές του φωτογραφίες, βίντεο και άρθρα ή συνδέσμους από το διαδίκτυο.

Η λειτουργία για την διαχείριση των φίλων ενός χρήστη στο “Google Plus” δανείζεται στοιχεία και από το “Facebook” και από το “Twitter”. Συγκεκριμένα ένας χρήστης μπορεί να προσθέσει έναν άλλο χρήστη στους “κύκλους” του μονομερώς, όπως και στο “Twitter” με την χρήση του “follow”. Όμως σε αντίθεση με το “Twitter” όπου οι χρήστες που “ακολουθεί” κάποιος βρίσκονται σε μία μοναδική λίστα, στο “Google Plus” ο χρήστης έχει τη δυνατότητα να δημιουργήσει πολλές λίστες (“κύκλους”) και να προσθέσει άτομα στον κύκλο που επιθυμεί. Ο κάθε κύκλος μπορεί να έχει διαφορετικές ιδιότητες και χαρακτηριστικά, κυρίως ιδιωτικότητας, ώστε να διαφοροποιείται το είδος της αλληλεπίδρασης που θα έχει ο χρήστης με κάθε διαφορετική ομάδα “φίλων” του.



Εικόνα 14: “Google+”

Επίσης όπως και στην πλειονότητα των υπόλοιπων κοινωνικών δικτύων έτσι και στο “Google Plus” υποστηρίζεται η υπηρεσία των προσωπικών μηνυμάτων μεταξύ δύο ή παραπάνω χρηστών. Ακόμα υποστηρίζεται και το αντίστοιχο “like” του “Facebook”, που στην προκειμένη περίπτωση ονομάζεται υπηρεσία “+1” και επιτρέπει στους χρήστες να δηλώσουν ότι τους αρέσει μια δημοσίευση από κάποιον άλλο χρήστη. Τέλος σημαντική θεωρείται και η υπηρεσία “Hangouts” η οποία επιτρέπει στους χρήστες να έρθουν σε επαφή μεταξύ τους είτε μέσω chat, είτε με ηχητικό τρόπο, είτε με την χρήση καμερών.[14]

1.5.5 Pinterest

Όπως και το “Google Plus”, έτσι και το “Pinterest” είναι ένα αρκετά νέο μέσο κοινωνικής δικτύωσης αφού η λειτουργία του ξεκίνησε το 2010. Το “Pinterest” στηρίζεται σε εντελώς διαφορετικό τρόπο

λειτουργίας από τα άλλα κοινωνικά δίκτυα που αναφέρθηκαν έως τώρα. Η λειτουργία του στηρίζεται στη λογική των κατηγοριών ή των θεμάτων που μπορεί να ενδιαφέρουν έναν χρήστη.

Πιο συγκεκριμένα επιτρέπει στους χρήστες του να δημιουργήσουν ένα “σελιδοδείκτη” (“bookmark”) από ιστοσελίδες που βρίσκουν ενδιαφέρουσες. Η διαφορά του σε σχέση με άλλες αντίστοιχες υπηρεσίες είναι ότι στο “Pinterest” δίνεται μεγάλη σημασία στην εικόνα και το βίντεο. Ο χρήστης μπορεί να “καρφίτσώσει” στο προσωπικό του πίνακα μια εικόνα και να την τοποθετήσει σε συγκεκριμένη θεματική κατηγορία της επιλογής του. Μ’ αυτόν τον τρόπο διαμοιράζεται τους “σελιδοδείκτες” που επιθυμεί με τις επαφές του.

Μπορούν να δημιουργηθούν πολλαπλοί πίνακες με διαφορετικά θέματα από κάθε χρήστη ενώ ακόμα ο κάθε χρήστης μπορεί να “ακολουθήσει” (“follow”) άλλους χρήστες ή συγκεκριμένους πίνακες, ενώ ακόμα έχει τη δυνατότητα να κάνει like, σχόλια ή να αναδημοσιεύσει τις δημοσιεύσεις που επιθυμεί.

Το “Pinterest” έχει μεγάλο ρυθμό ανάπτυξης ενώ σύμφωνα με έρευνες οι χρήστες περνούν πολύ χρόνο στο site. Άξιο αναφοράς είναι ακόμα το γεγονός πως η μεγάλη πλειοψηφία των χρηστών του είναι γυναίκες, κυρίως 25-54 ετών. Υπολογίζεται πως σήμερα το “Pinterest” χρησιμοποιούν συνολικά γύρω στα 70 εκατομμύρια χρήστες. [15]

1.5.6 YouTube

Η διαδικτυακή υπηρεσία του “YouTube” που ξεκίνησε τη λειτουργία της το 2005 αποτελεί τη μεγαλύτερη σε χρήστες και όγκο περιεχομένου μηχανή αναζήτησης και υπηρεσία παροχής βίντεο. Είναι ένα μέσο κοινωνικής δικτύωσης που το περιεχόμενο του αποτελείται αποκλειστικά από βίντεο τα οποία είτε δημιουργούν είτε αναδημοσιεύουν οι χρήστες του. Ένας τεράστιος αριθμός επιχειρήσεων επίσης το χρησιμοποιούν για να δημοσιεύουν τα βίντεο τους.

Το 2006 η κολοσσός εταιρία “Google” εξαγόρασε το “YouTube” και η επιτυχία του αποτυπώνεται στα πιο πρόσφατα στατιστικά στοιχεία της ίδιας της ιστοσελίδας. Είναι αξιοσημείωτο πως το “YouTube” χρησιμοποιούν πάνω από 1 δισεκατομμύριο χρήστες το μήνα αλλά και το γεγονός πως κάθε λεπτό ανεβαίνουν 100 ώρες βίντεο. Πάνω από 6 δισεκατομμύρια ώρες βίντεο προβάλλονται κάθε μήνα, αριθμός που αντιστοιχεί σχεδόν σε μια ώρα για κάθε κάτοικο της γης.

Ένας χρήστης μπορεί να δημιουργήσει το προσωπικό του προφίλ στο “YouTube”, το οποίο αποκαλείται “κανάλι” (“channel”). Σ’ αυτό το “κανάλι” οι χρήστες μπορούν να δημοσιεύσουν τα βίντεο που θέλουν αλλά και να δημιουργήσουν λίστες αναπαραγωγής των βίντεο που επιθυμούν. Ακόμα μπορούν να προσθέσουν τα αγαπημένα τους βίντεο. Οι χρήστες επίσης που παρακολουθούν ένα βίντεο μπορούν να δηλώσουν αν τους αρέσει ή όχι αλλά και να το σχολιάσουν. Μια άλλη δυνατότητα που παρέχει το κοινωνικό αυτό μέσο είναι το γεγονός πως ένας χρήστης μπορεί να γίνει “συνδρομητής” στα “κανάλια” των υπόλοιπων χρηστών και να λαμβάνει ειδοποιήσεις για νέα βίντεο ή για τον σχολιασμό κάποιων. Μόνο οι χρήστες που εγγράφονται στην υπηρεσία μπορούν να δημοσιεύσουν και να σχολιάσουν ένα βίντεο, ενώ οι μη εγγεγραμμένοι χρήστες μόνο να τα παρακολουθήσουν.

Η υπηρεσία του “YouTube” χρησιμοποιείται από την πλειονότητα των ιστοσελίδων για την προβολή ενός βίντεο με την ενσωμάτωση αυτών των βίντεο στα άρθρα ή τις δημοσιεύσεις των ιστοσελίδων αυτών. Επίσης επικρατεί η ενσωμάτωση των βίντεο του “YouTube” και σε άλλα κοινωνικά δίκτυα όπως το “Facebook” και το “Myspace”. [16]



Εικόνα 15: Η αρχική σελίδα του “YouTube”

Κεφάλαιο 2: Η Έννοια της Ιδιωτικότητας

2.1 Εισαγωγή

Στο παρόν κεφάλαιο εξετάζεται η έννοια της ιδιωτικότητας, καθώς επίσης και η ανάγκη γι' αυτήν αλλά και τα μοντέλα προστασία της. Ο όρος της ιδιωτικότητας αποτελεί ένα θεμελιώδες ανθρώπινο δικαίωμα. Αναγνωρίζεται από το 1890, οπότε και τον ανέφεραν οι δικαστές Warren και Brandeis στην πραγματεία τους. Όμως η προέλευση του προέρχεται από τα αρχαία χρόνια όπου ήδη διαχωριζόταν ο όρος του δημόσιου από τον ιδιωτικό βίο. [17]

Η ιδιωτικότητα, η οποία αποτελεί ένα από τα πιο σημαντικά ανθρώπινα δικαιώματα της σύγχρονης εποχής, ενισχύει και άλλες αξίες όπως η ελευθερία του λόγου και η ελευθερία της επικοινωνίας. Συνδέεται με το “δικαίωμα να μείνει κανείς μόνος του” και αναγνωρίζεται ως αναγκαία από τις περισσότερες κουλτούρες ανά τον πλανήτη. Σχεδόν κάθε χώρα περιλαμβάνει τον όρο της ιδιωτικότητας στο Σύνταγμά της και ακόμα κι αυτές που δεν το κάνουν, εδραιώνουν το δικαίωμα αυτό σε άλλες διατάξεις. Η έννοια της ιδιωτικότητας προστατεύεται επίσης από την Παγκόσμια Διακήρυξη των ανθρωπίνων δικαιωμάτων, την Ευρωπαϊκή Σύμβαση των ανθρωπίνων δικαιωμάτων αλλά και από το Διεθνές Συμβούλιο ατομικών και πολιτικών δικαιωμάτων.

Σύμφωνα με την ανθρωπολογική προσέγγιση ο κάθε άνθρωπος έχει ένα κρίσιμο επίπεδο ιδιωτικότητας, όπου αν αυτό το επίπεδο καταβαραθρωθεί υπάρχουν αρνητικές επιπτώσεις. Αυτές οι συνέπειες

είναι κυρίως σε ψυχολογικό επίπεδο καθώς είναι αποδεδειγμένο πως το κάθε άτομο είναι περισσότερο ευτυχισμένο όταν διατηρεί τον προσωπικό του χώρο τις στιγμές που το επιθυμεί. Επίσης είναι γενικά αποδεκτό πως ο συνωστισμός, όταν δηλαδή εξαλείφεται εντελώς ο προσωπικός χώρος του καθενός, μπορεί να προκαλέσει προβλήματα ιατρικής φύσεως στον άνθρωπο όπως υψηλή πίεση του αίματος και καρδιακές παθήσεις.

Από την βιολογική ανάγκη του ανθρώπου να φοράει ρούχα, να προστατεύει δηλαδή το γυμνό του σώμα, έως την σύγχρονη ανάγκη για προστασία των προσωπικών δεδομένων από την εισβολή της τεχνολογίας σε όλους του τομείς της καθημερινής ζωής του ατόμου είναι, ξεκάθαρη η απαραίτητη ύπαρξη κανόνων προστασίας της ιδιωτικής ζωής σε όλες τις κοινωνίες, είτε είναι νομικής είτε μη νομικής φύσης. [18]

2.2 Ορισμός της ιδιωτικότητας

Ως ανθρώπινο δικαίωμα είναι γενικά αποδεκτό πως η ιδιωτικότητα δεν μπορεί να οριστεί εύκολα. Για να συμβεί αυτό πρέπει να ορίζεται το περιβάλλον και το πλαίσιο για τα οποία αναφέρεται σε κάθε περίπτωση ξεχωριστά. Η ποικιλία των ορισμών μπορεί να κατηγοριοποιηθεί σε δύο ευρύτερες κατηγορίες. Από τη μία πλευρά οι ορισμοί που η ιδιωτικότητα ταυτίζεται με την προστασία των προσωπικών δεδομένων και από την άλλη πλευρά οι ορισμοί που εντάσσουν την ιδιωτικότητα σε ένα πιο γενικό πλαίσιο και εξετάζουν το κατά πόσο η κοινωνία μπορεί να εισχωρήσει και να εισβάλει στα προσωπικά ζητήματα και δεδομένα ενός ατόμου.

Για την ιδιωτικότητα έχουν κατατεθεί πολλές και διαφορετικές απόψεις από επιστήμονες και ειδικούς, από τις οποίες η πρώτη χρονολογικά προέρχεται από τους Brandeis και Warren το 1890 και ανέφερε ως ιδιωτικότητα “το δικαίωμα να βρίσκεται κανείς μόνος του”. Ο γενικότερα πιο αποδεκτός και δημοφιλής ορισμός όμως, προέρχεται από τον Alan F. Westin, ο οποίος τονίζει πως: “Η ιδιωτικότητα είναι η αξίωση των ατόμων και των ομάδων να αποφασίζουν για τον εαυτό τους πότε, πως και σε ποιο ακριβώς βαθμό οι πληροφορίες για τα άτομά τους γνωστοποιούνται στους υπόλοιπους με τους οποίους επικοινωνούν”.



Εικόνα 16: Ιδιωτικότητα

Μια πιο πρόσφατη και προσαρμοσμένη στα σημερινά δεδομένα αναφορά προέρχεται από τον Robert Ellis Smith ο οποίος επισημαίνει ότι: “Ιδιωτικότητα είναι η επιθυμία του κάθε ατόμου για ζωτικό φυσικό χώρο, όπου μπορεί να αισθάνεται απαλλαγμένος από διαφόρων τύπων παρενοχλήσεις, προσβολές ή ευθύνες και η προσπάθεια του καθενός να ελέγξει τον χρόνο και τον τρόπο αποκάλυψης των προσωπικών του πληροφοριών”. [19]

2.3 Ιστορικά στοιχεία

Το δικαίωμα στην προστασία της ιδιωτικότητας του κάθε ατόμου συναντάται εδώ και χιλιάδες χρόνια σε πολλές αναφορές. Σε κορυφαίους αρχαίους πολιτισμούς αλλά και στις γραφές των κυρίαρχων θρησκειών αναφέρεται η έννοια και η αξία της ιδιωτικότητας. Στην αρχαία Ελλάδα ο ιδιωτικός χώρος και η ιδιωτική ζωή του κάθε ατόμου αντιμετωπιζόταν με τον δέοντα σεβασμό ενώ και στην αρχαία Κίνα ήταν η ιδιωτικότητα αποδεκτή ως αξία και ως κάτι που πρέπει να τηρείται. Επίσης η έννοια αυτή εμφανίζεται σε μεγάλο αριθμό αναφορών στη Βίβλο ενώ σημαντική σημασία σ' αυτήν έδιναν και οι Εβραίοι οι οποίοι υποστήριζαν πως ένας άνθρωπος πρέπει να προστατεύεται από την παρακολούθηση άλλων ανθρώπων.

Νομικά οι πρώτοι κανόνες που αφορούν την ιδιωτικότητα θεσπίστηκαν στην Ευρώπη, και στην Αγγλία πιο συγκεκριμένα, όπου στα μέσα του 18^{ου} αιώνα υπήρξαν οι πρώτοι νόμοι του εθνικού κοινοβουλίου που προστάτευαν την ιδιωτικότητα του χώρου του κάθε ατόμου. Πολλές άλλες χώρες ακολούθησαν στη συνέχεια ώστε να προστατεύσουν και με βάση το νόμο το δικαίωμα αυτό. Μέχρι και τις αρχές του 20^{ου} αιώνα χώρες όπως η Σουηδία, η Γαλλία και οι Ηνωμένες Πολιτείες της Αμερικής υπεργήφισαν και εφάρμοσαν τέτοιους νόμους.

Το πιο σημαντικό όμως βήμα για την καθολική και οικουμενική προστασία της ιδιωτικότητας έγινε το 1948 όταν και συντάχθηκε η Παγκόσμια Διακήρυξη των Ανθρωπίνων Δικαιωμάτων από τον Οργανισμό Ηνωμένων Εθνών. Η Διακήρυξη αυτή αναφέρεται γενικά στην ιδιωτικότητα και προστατεύει ιδιαίτερα την χωρική αλλά και την επικοινωνιακή ιδιωτικότητα. Μεταξύ άλλων στην Διακήρυξη δηλώνεται

πως: “Κανείς δεν πρέπει να υποβάλλεται σε αυθαίρετη ανάμειξη στην ιδιωτική του ζωή, στις οικογενειακές του υποθέσεις ή στην αλληλογραφία του καθώς και σε επιθέσεις στην τιμή και στην φήμη του. Ο καθένας έχει το δικαίωμα να ζητά την προστασία του νόμου απέναντι σε τέτοιες παρεμβάσεις”.

Μείζονος σημασίας θεωρείται επίσης και η Ευρωπαϊκή Σύμβαση για την προστασία των ανθρωπίνων δικαιωμάτων η οποία υπογράφηκε το 1950 και η οποία θεσπίζει το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών. Ανάμεσα σε άλλα αναφέρει ότι: “...πρέπει να γίνεται σεβαστή για όλους η ιδιωτική και οικογενειακή τους ζωή, ο χώρος κατοικίας τους και η αλληλογραφία τους”. Η Σύμβαση αυτή οδήγησε και την Ευρωπαϊκή Ένωση, με στόχο την υπεράσπιση αυτών των δικαιωμάτων, στη θέσπιση της Ευρωπαϊκής Επιτροπής ανθρωπίνων δικαιωμάτων και του Ευρωπαϊκού δικαστηρίου για τα ανθρώπινα δικαιώματα.

Μετά την θέσπιση τέτοιων νομικών κανόνων παγκοσμίως η ιδιωτικότητα σε πολλά κράτη ανά τον κόσμο προστατεύτηκε αλλού αρκετά επαρκώς και αλλού λιγότερο. Με την πάροδο των ετών σχεδόν σε όλα τα κράτη έγινε προσπάθεια να ισχύσουν και να δημιουργηθούν ακόμα ισχυρότεροι τέτοιοι νόμοι. Τα τελευταία έτη με την εξέλιξη της τεχνολογίας και την έκρηξη του διαδικτύου ήταν απαραίτητη η νομική κατοχύρωση για την προστασία των προσωπικών δεδομένων που αναρτούνται στο διαδίκτυο. Νέες ανάγκες και απαιτήσεις εμφανίστηκαν και όπως θα αναλυθεί σε επόμενο κεφάλαιο η κάλυψη των απαιτήσεων αυτών νομικά αλλά και είναι το κυρίαρχο θέμα σε ότι αφορά την προστασία της ιδιωτικότητας στις σύγχρονες κοινωνίες. [20]

2.4 Είδη ιδιωτικότητας

Η έννοια της ιδιωτικότητας μπορεί να χωριστεί στις παρακάτω μορφές:

- **Ιδιωτικότητα των Πληροφοριών:** αφορά τους κανόνες που καθορίζουν την συλλογή, την αποθήκευση, την επεξεργασία και την διάδοση των προσωπικών δεδομένων ενός ατόμου.
- **Ιδιωτικότητα της Σωματικής Υπόστασης:** αφορά την προστασία ενός ατόμου σε θέματα ιδιωτικότητας που έχουν να κάνουν με το σώμα του, όπως η σωματική έρευνα, η δοκιμή φαρμάκων, τα γενετικά τεστ κ.α.
- **Ιδιωτικότητα του Χώρου:** αφορά την προστασία του προσωπικού χώρου ενός ατόμου και τη θέσπιση αλλά και την τήρηση συγκεκριμένων ορίων είτε πρόκειται για το οικιακό του περιβάλλον, είτε για το εργασιακό, είτε για το δημόσιο.
- **Ιδιωτικότητα των Επικοινωνιών:** αφορά την προστασία των επικοινωνιών μεταξύ δύο ή περισσότερων ατόμων και την τήρηση του απορρήτου τους. [21]

2.5 Η ανάγκη προστασίας προσωπικών δεδομένων

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο ένα από τα είδη στα οποία χωρίζεται η έννοια της ιδιωτικότητας είναι η ιδιωτικότητα των πληροφοριών ή αλλιώς η ιδιωτικότητα των προσωπικών δεδομένων. Η

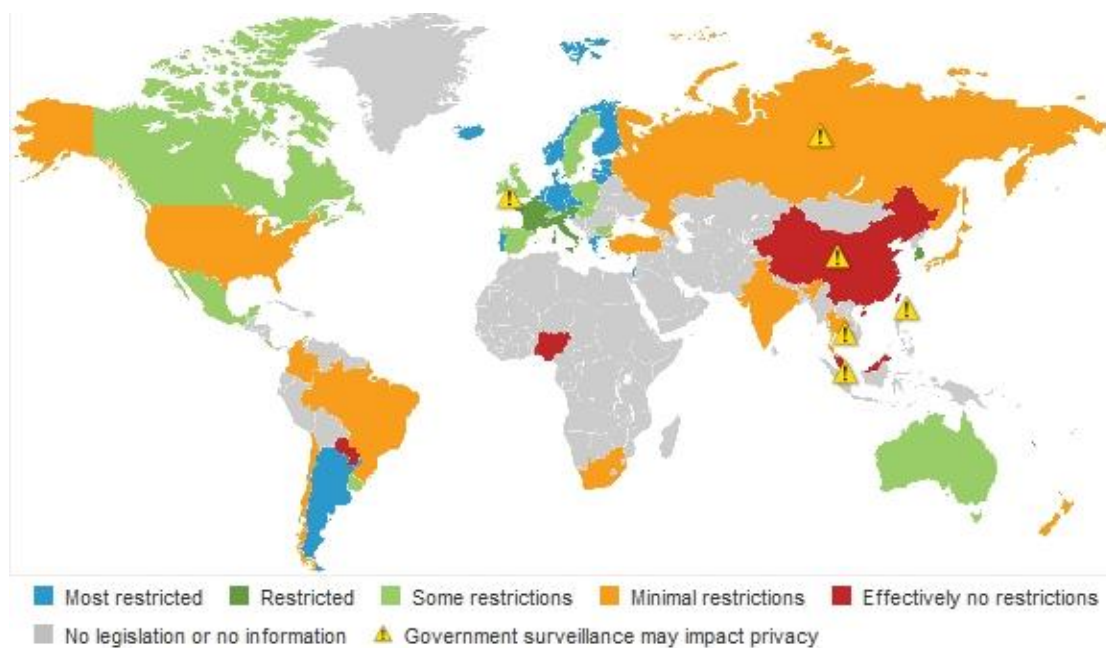
προστασία της ιδιωτικότητας των προσωπικών δεδομένων είναι κομβική στην σύγχρονη εποχή με τα τωρινά μέσα τεχνολογίας και ίσως το πιο σημαντικό μέρος της έννοιας της ιδιωτικότητας πλέον.

Μέχρι τη δεκαετία του 1960 η προστασία των προσωπικών δεδομένων ήταν ένα όχι και τόσο φλέγον και σημαντικό ζήτημα, καθώς δίχως τις νέες τεχνολογίες ήταν πρακτικά αδύνατη η ολοκληρωμένη διασύνδεση μεταξύ των προσωπικών δεδομένων και η επεξεργασία των δεδομένων αυτών για την δημιουργία στοιχείων που θα μπορούσαν να εκθέσουν ένα άτομο. Παρότι, από τα τέλη του 19^{ου} αιώνα και μετά, είχε εκφραστεί αρκετές φορές από σημαντικούς ανθρώπους ο φόβος για τους κινδύνους που θα μπορούσαν να προκύψουν από τα μέσα εισβολής στην ιδιωτική ζωή των ανθρώπων, είναι χαρακτηριστικό πως η μη προηγμένη και εξαιρετικά δαπανηρή τεχνολογία της εποχής δεν έδινε πολλά περιθώρια για την κατάλληλη αξιοποίηση των στοιχείων που συλλέγονταν. Η επιτήρηση συγκεκριμένων ατόμων ήταν υπερβολικά δαπανηρή, η επεξεργασία των δεδομένων δεν ήταν αυτόματη και ο συνδυασμός όλων αυτών έθετε ανυπέρβλητα εμπόδια στην παραβίαση της ιδιωτικής ζωής των πολιτών.

Από τα τέλη της δεκαετίας του 1960 και μετά όμως, η ηλεκτρονική επεξεργασία των δεδομένων συρρίκνωσε αυτά τα εμπόδια. Τα πανίσχυρα πληροφοριακά συστήματα που δημιουργήθηκαν έδωσαν τη δυνατότητα της επιτήρησης και της ενδελεχούς παρακολούθησης των πολιτών. Αποτέλεσμα του γεγονότος αυτού ήταν η ανάγκη για την καλύτερη προστασία των προσωπικών δεδομένων και η θέσπιση ειδικών κανόνων για τις προϋποθέσεις της συλλογής, της αποθήκευσης και της επεξεργασίας των πληροφοριών αυτών.

Τα προσωπικά δεδομένα είναι ουσιαστικά όλες οι πληροφορίες που αφορούν τις προσωπικές περιστάσεις ενός αναγνωρίσιμου προσώπου. Η προστασία αυτών των δεδομένων αφορά την Ιδιωτικότητα Πληροφοριών, ωστόσο αυτό δεν είναι ένα απόλυτο δικαίωμα καθώς μπορεί να έρθει σε σύγκρουση με άλλα δικαιώματα. Κάποια δεδομένα είναι απαραίτητο να είναι δημόσια διαθέσιμα για την συμμετοχή των ατόμων στην κοινωνία και κάποια άλλα πρέπει να μένουν ιδιωτικά και να προστατεύονται. Η κατηγοριοποίηση αυτή εξαρτάται συνήθως από το εκάστοτε νομικό πλαίσιο ενώ είναι απαραίτητο να συνυπολογίζεται και το δικαίωμα ενός ατόμου να μπορεί να επιλέξει την διάθεση ορισμένων δεδομένων που ενδέχεται να χαρακτηρίζονται ως ιδιωτικά.

Ως εκ τούτου και συνυπολογίζοντας όλα αυτά τα περίπλοκα ζητήματα θεωρήθηκε αναγκαία η νομοθετική κάλυψη αυτών των θεμάτων και έτσι οι πρώτοι νόμοι προστασίας προσωπικών δεδομένων ξεκίνησαν να θεσπίζονται στα μέσα της δεκαετίας του 1970. Χώρες όπως η Γερμανία, οι ΗΠΑ και η Σουηδία εφάρμοσαν πρώτες τέτοιους νόμους. Μεγαλύτερη επιρροή όμως άσκησε το Συμβούλιο της Ευρώπης το 1981 το οποίο με τη Σύμβαση για την προστασία των ατόμων για την αυτόματη επεξεργασία προσωπικών δεδομένων έθεσε τις βάσεις για την ενεργοποίηση νόμων σε παγκόσμιο επίπεδο. Η εξέλιξη αυτή οδήγησε σε όλο και πιο νομικά ολοκληρωμένους και εκσυγχρονισμένους νόμους και πλέον στις περισσότερες χώρες τα ηλεκτρονικά δεδομένα προστατεύονται στον βέλτιστο βαθμό σε κάθε βήμα της επεξεργασίας τους. [22]



Εικόνα 17: Ιδιωτικότητα και προστασία δεδομένων ανά τον κόσμο

2.6 Μοντέλα προστασίας της ιδιωτικότητας

Η προστασία των ιδιωτικότητας και ιδιαίτερα της ιδιωτικότητας των δεδομένων είναι εξαιρετικά σημαντικής σημασίας όπως αναφέρθηκε και σε προηγούμενα κεφάλαια. Στην πλειοψηφία των χωρών θεσπίζονται μέτρα και νόμοι για την αντιμετώπιση αυτού του ζητήματος. Για το σκοπό αυτό μπορούν να εντοπιστούν και να αναλυθούν τέσσερα διαφορετικά μοντέλα τα οποία μπορεί να είναι αλληλοσυγκρουόμενα ή συμπληρωματικά. Τα μοντέλα προστασίας της ιδιωτικότητας εφαρμόζονται παράλληλα στις περισσότερες περιπτώσεις, ενώ έχει παρατηρηθεί πως ο πιο αποτελεσματικός τρόπος διασφάλισης της ιδιωτικότητας είναι η ταυτόχρονη χρήση όλων των μοντέλων.

Το πρώτο μοντέλο προστασίας της ιδιωτικότητας που θα αναφέρουμε είναι οι ολοκληρωμένοι νόμοι (“**Comprehensive Laws**”). Αυτό το μοντέλο αναφέρεται στους νόμους ευρείας και γενικής εφαρμογής που τηρούν πολλές χώρες στον κόσμο. Οι νόμοι αυτοί προσδιορίζουν το σύνολο των κανόνων που πρέπει να εφαρμόζονται για τη συλλογή και την χρήση προσωπικών πληροφοριών και στο δημόσιο και στον ιδιωτικό τομέα. Επίσης συμπληρωματικά είναι απαραίτητη η συγκρότηση μιας δημόσιας αρχής που δρα ανεξάρτητα και επιτηρεί και διασφαλίζει την ακέραια τήρηση των κανονισμών.

Το δεύτερο μοντέλο προστασίας της ιδιωτικότητας είναι οι τομεακοί νόμοι (“**Sectoral Laws**”). Υπάρχουν ορισμένες χώρες οι οποίες δεν έχουν κάποιο γενικό νόμο για την προστασία των προσωπικών δεδομένων. Αντ’ αυτού θεσπίζουν ξεχωριστή νομοθεσία για τον κάθε τομέα που επιβάλλεται αυτό. Για παράδειγμα μπορεί να υπάρχει διαφορετική νομοθεσία για την προστασία των ιατρικών δεδομένων και διαφορετική νομοθεσία για τα δεδομένα ποινικού μητρώου. Υπάρχει ένα φάσμα μηχανισμών που προστατεύει δηλαδή τα δεδομένα αλλά απουσιάζει ένα γενικός εποπτικός μηχανισμός για το έλεγχο της ορθής προστασίας. Πρέπει να τονιστεί ότι σε κάποιες χώρες τέτοιοι νόμοι χρησιμοποιούνται συμπληρωματικά με το γενικό νόμο προσφέροντας πιο ισχυρή προστασία για κάποιους τομείς δεδομένων. Αντίθετα στις περιπτώσεις που χρησιμοποιούνται μόνο τομεακοί νόμοι παρατηρούνται διάφορα μειονεκτήματα όπως το γεγονός πως με κάθε νέα τεχνολογία απαιτείται νέος νόμος που να εξασφαλίζει τα θέματα ιδιωτικότητας και το γεγονός πως η ιδιωτικότητα σε αρκετές περιπτώσεις δεν εξασφαλίζεται επαρκώς καθώς δεν υπάρχει η απαιτούμενη ευελιξία από το νόμο.

Ένα άλλο μοντέλο προστασίας της ιδιωτικότητας είναι η αυτορρύθμιση (“**Self-Regulation**”). Πέρα από τους νόμους και τους κανονισμούς που θεσπίζει ένα κράτος για την προστασία της ιδιωτικότητας των πολιτών του, υπάρχουν και οι περιπτώσεις όπου η προστασία αυτή μπορεί να επιτευχθεί από τις ενέργειες των οργανισμών ή των επιχειρήσεων. Στο μοντέλο της αυτορρύθμισης λοιπόν, οι οργανισμοί και οι επιχειρήσεις διαμορφώνουν δικούς τους κανονισμούς, τις οδηγίες και το πλαίσιο που θα επιλέξουν για την τήρηση της ιδιωτικότητας των δεδομένων που τους αφορούν. Η έως τώρα εφαρμογή αυτού μοντέλου δεν έχει τα επιθυμητά αποτελέσματα καθώς οι κανονισμοί αυτοί συνήθως είναι είτε αναποτελεσματικοί είτε σπάνια εφαρμόζονται. Απουσιάζει η δυνατότητα επιβολής κοινής πολιτικής προστασίας αφού ο κάθε φορέας έχει τη δυνατότητα να θεσπίζει τους δικούς του κανόνες, ενώ και η επιβολή αυτών των κανόνων δεν πραγματοποιείται καθώς ο έλεγχος που πρέπει να υπάρχει από την κεντρική διοίκηση είναι στις περισσότερες περιπτώσεις προβληματικός.

Το τελευταίο μοντέλο προστασίας της ιδιωτικότητας που θα αναφερθεί είναι οι τεχνολογίες της ιδιωτικότητας (“**Technologies of Privacy**”). Το συγκεκριμένο μοντέλο βασίζεται στη δυνατότητα που έχει πλέον ο κάθε χρήστης, λόγω και της ραγδαίας τεχνολογικής προόδου, να προστατέψει τα προσωπικά του δεδομένα με τις δικές του ενέργειες. Για παράδειγμα με τη χρήση των σύγχρονων υπολογιστών ένας χρήστης που σερφάρει στο διαδίκτυο έχει τη δυνατότητα να εγκαταστήσει προγράμματα ή συστήματα που ενισχύουν την ασφάλειά του. Συστήματα όπως τα firewalls και τα ψηφιακά πιστοποιητικά είναι τέτοια παραδείγματα. Είναι δεδομένο πως δεν πρόκειται για μια απόλυτη μέθοδο προστασίας των

**Προστασία της ιδιωτικότητας σε Social Networks και
πλατφόρμες όπως το Facebook κ.λπ.**

προσωπικών δεδομένων ενός ατόμου και πως χρησιμοποιείται απολύτως ως συμπλήρωμα των προαναφερθέντων μοντέλων προστασίας. [23]

Πανεπιστήμιο Πειραιώς

Κεφάλαιο 3: Κίνδυνοι Ιδιωτικότητας στα Κοινωνικά Δίκτυα

3.1 Απαιτήσεις Ιδιωτικότητας στα Κοινωνικά Δίκτυα

Στη σημερινή παγκόσμια κοινωνία της πληροφορίας, η ιδιωτικότητα είναι ένας πολύ ευαίσθητος και αδιαπραγμάτευτος σημασίας τομέας. Ο παγκόσμιος χαρακτήρας του διαδικτύου και η μη ύπαρξη κεντρικής διαχείρισης και ελέγχου του έχουν δημιουργήσει μια σειρά από κινδύνους. Ειδικότερα στο κομμάτι των κοινωνικών δικτύων οι κίνδυνοι που σχετίζονται με την ιδιωτικότητα των δεδομένων είναι ακόμα πιο έντονοι. Προτού αναλυθούν όμως οι κίνδυνοι αυτοί, είναι απαραίτητο να επισημανθεί το “τι ζητάει” ένας χρήστη από μια υπηρεσία κοινωνικού δικτύου σε ότι αφορά την ιδιωτικότητα.

Σε ένα μέσο κοινωνικής δικτύωσης ένας χρήστης στο προσωπικό του προφίλ κοινοποιεί πολλές και ευαίσθητες σημασίας πληροφορίες, οι οποίες μπορεί να είναι από απλά στοιχεία όπως ονοματεπώνυμο και διεύθυνση κατοικίας έως πιο σύνθετες πληροφορίες όπως προσωπικά ενδιαφέροντα, προτιμήσεις ακόμα και ενδοοικογενειακά ζητήματα. Φυσικά πολλές φορές οι χρήστες κοινοποιούν τέτοιες πληροφορίες χωρίς να αντιλαμβάνονται πλήρως το μέγεθος των κινδύνων που μπορεί να προκύψουν εξαιτίας τους. Για το λόγο αυτό είναι απαραίτητο τα ίδια τα κοινωνικά δίκτυα να μεριμνούν για την προστασία των προσωπικών

δεδομένων των χρηστών τους, όπως και οι χρήστες από τη μεριά τους επιζητούν την προστασία αυτή. Έτσι είναι φρόνιμο και απαραίτητο τα μέσα κοινωνικής να τηρούν κάποιες προϋποθέσεις ασφάλειας των προσωπικών δεδομένων, δηλαδή να τηρούνται ορισμένες απαιτήσεις ιδιωτικότητας.

Παρατηρώντας τις απαιτήσεις ιδιωτικότητας που θα αναλυθούν στη συνέχεια είναι φανερό πως αυτές δείχνουν το τι χρειάζεται να προστατευθεί για την αποτροπή της παραβίασης της ιδιωτικότητας κατά τη χρήση ενός κοινωνικού δικτύου αλλά και κατ' επέκταση του διαδικτύου γενικότερα. Οι απαιτήσεις ιδιωτικότητας ενός κοινωνικού δικτύου λοιπόν, είναι οι εξής:

3.1.1 Ανωνυμία

Η ανωνυμία (anonymity) θεωρείται μία από τις πιο βασικές, αν όχι η σημαντικότερη, απαίτηση ιδιωτικότητας κατά τη χρήση του διαδικτύου. Στην περίπτωση των κοινωνικών δικτύων όμως είναι μια πιο σύνθετη και με πιο ιδιαίτερα χαρακτηριστικά απαίτηση.

Γενικότερα η έννοια της ανωνυμίας εξασφαλίζει πως ένας χρήστης έχει τη δυνατότητα να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει μ' έναν άλλο χρήστη ή σύστημα χωρίς να αποκαλυφθεί η ταυτότητα του. Η ανωνυμία μπορεί να χωριστεί σε τρία ξεχωριστά είδη. Την ανωνυμία του παραλήπτη, την ανωνυμία του αποστολέα και την απόλυτη ανωνυμία στην οποία και τα δύο μέρη ενός ζευγαριού επικοινωνίας παραμένει ανώνυμο. Παρότι στη χρήση του διαδικτύου είναι απόλυτα θεμιτό

κάποιος να θέλει να προστατεύσει την ταυτότητά του, εν τούτοις στα κοινωνικά δίκτυα είναι ένα αντικρουόμενο γεγονός. Αντικρουόμενο καθώς ένας από τους βασικούς λόγους χρήσης των κοινωνικών δικτύων είναι η επικοινωνία με συγγενείς, φίλους ή γνωστούς οι οποίοι φυσικά και γνωρίζουν την ταυτότητα του ατόμου με το οποίο επικοινωνούν.

Υπάρχουν όμως και οι περιπτώσεις που ένας χρήστης θα θελήσει να παραμείνει ανώνυμος, είτε για όλους τους υπόλοιπους χρήστες μιας υπηρεσίας είτε για ένα μέρος αυτών. Ορισμένα κοινωνικά δίκτυα κατέχουν εξ ορισμού τους την απαίτηση της ανωνυμίας και έτσι αυτή είναι διαθέσιμη για όλους τους χρήστες μην μπορώντας να μεταβάλλουν αυτό το γεγονός. Τέτοια κοινωνικά δίκτυα όπως το “Whisper” και το “Secret” εμφανίστηκαν στο προσκήνιο τα τελευταία χρόνια και επιτρέπουν στους χρήστες τους την απόλυτη ανωνυμία κατά την επικοινωνία τους με άλλους χρήστες. Όμως, ακόμα τουλάχιστον, υστερούν σε δημοτικότητα.

Στα πιο δημοφιλή μέσα κοινωνικής δικτύωσης το ζήτημα της ανωνυμίας είναι πιο σύνθετο. Σε κάποια κοινωνικά δίκτυα, όπως το “Facebook” η ανωνυμία πρακτικά είναι αδύνατη. Ένας χρήστης για να δημιουργήσει το προσωπικό του προφίλ οφείλει να καταχωρήσει τα αληθινά του στοιχεία αφού αν επιχειρήσει κάτι διαφορετικό θα αποκλειστεί από την χρήση της υπηρεσίας. Δίνεται όμως η δυνατότητα της μερικής ανωνυμίας. Αυτό επιτυγχάνεται με κάποιες επιλογές απορρήτου που μπορεί να επιλέξει ένας χρήστης και που με αυτές μπορεί να αποκρύψει το προφίλ του από ορισμένους χρήστες ή να το ορίσει ως ορατό μόνο στους φίλους του, τους χρήστες δηλαδή που έχει επιλέξει ο ίδιος. Έτσι ουσιαστικά είναι δυνατή η χρήση της υπηρεσίας χωρίς την αποκάλυψη της ταυτότητάς του σε όλους τους υπόλοιπους χρήστες.

Σε άλλα κοινωνικά δίκτυα όπως το “Twitter” ένας χρήστης έχει τη δυνατότητα αν θέλει να χρησιμοποιήσει την ψευδωνυμία, η οποία θα αναλυθεί στη συνέχεια. Υπάρχει και η ξεχωριστή κατηγορία των blogs όπου οι χρήστες μπορούν αν θέλουν να τα χρησιμοποιούν ανώνυμα. Δίνεται η δυνατότητα της επιλογής σε όλους, συγγραφείς και σχολιαστές των blogs, να χρησιμοποιούν το εν λόγω είδος κοινωνικού δικτύου είτε ανώνυμα είτε όχι. Τα ιστολόγια έτσι κι αλλιώς είναι περισσότερο μέσα έκφρασης προσωπικών απόψεων πολιτικού, κοινωνικού ή φιλοσοφικού χαρακτήρα αλλά και μετάδοσης πληροφοριών και ειδήσεων. Έτσι με την προστασία της ανωνυμίας των ιστολογίων επιτυγχάνεται η ελευθερία της έκφρασης η οποία είναι και συνταγματικό δικαίωμα, αφού στην αντίθετη περίπτωση θα ήταν επικίνδυνα τα φαινόμενα λογοκρισίας. [24]

3.1.2 Μη παρατηρησιμότητα

Η μη παρατηρησιμότητα (unobservability) προστατεύει την ιδιωτικότητα των χρηστών απαγορεύοντας σε κάποιον να παρατηρήσει ή να εντοπίσει τα ίχνη τους κατά την χρήση μιας υπηρεσίας.

Στην περίπτωση των κοινωνικών δικτύων η απαίτηση για μη παρατηρησιμότητα εφαρμόζεται σε κάποια εξ αυτών και για ορισμένες λειτουργίες τους. Για παράδειγμα σχεδόν σε όλα τα κοινωνικά δίκτυα ένας χρήστης μπορεί να γίνει μη ορατός και έτσι να μην είναι εμφανές στους υπόλοιπους χρήστες ότι χρησιμοποιεί εκείνη τη στιγμή την υπηρεσία. Επίσης μπορεί να παρακολουθήσει ένα βίντεο ή να δει μια φωτογραφία χωρίς να γίνει ορατό αυτό σε άλλο χρήστη. Σε άλλες

λειτουργίες όμως, όπως τα προσωπικά μηνύματα ή ο σχολιασμός φωτογραφιών δεν υπάρχει η δυνατότητα της μη παρατηρησιμότητας στα κοινωνικά δίκτυα. [25]

3.1.3 Προστασία δεδομένων

Ίσως η πιο σημαντική απαίτηση ιδιωτικότητας σε ότι αφορά τα κοινωνικά δίκτυα είναι η προστασία των δεδομένων, των προσωπικών δεδομένων δηλαδή του κάθε ατόμου.

Όπως θα αναλυθεί και σε επόμενο κεφάλαιο, οι πιο πολλοί κίνδυνοι που σχετίζονται με τα κοινωνικά δίκτυα στοχεύουν και αφορούν τα προσωπικά δεδομένα του κάθε χρήστη. Γι' αυτό το λόγο είναι απαραίτητη η προστασία αυτών των δεδομένων από την πλευρά των μέσων κοινωνικής δικτύωσης. Είναι αναγκαίο τα μέσα αυτά να δίνουν τη δυνατότητα στους χρήστες τους να επιλέγουν για τα προσωπικά τους στοιχεία το ποια και σε ποιους θα κοινοποιούνται. Ακόμα είναι απαραίτητο τα κοινωνικά δίκτυα να προστατεύουν τα προσωπικά στοιχεία των χρηστών τους από απόπειρες επιθέσεων ενώ κρίσιμης σημασίας είναι και η μη διαφημιστική εκμετάλλευση των δεδομένων αυτών από τη μεριά των κοινωνικών δικτύων ή συνεργατών τους. Καθότι ένα μεγάλο μέρος των δεδομένων αυτών είναι ευαίσθητα, είναι επίσης αναγκαίο να προστατεύεται και η ακεραιότητα άλλα και να εξασφαλίζεται η μη επεξεργασία τους. [26]

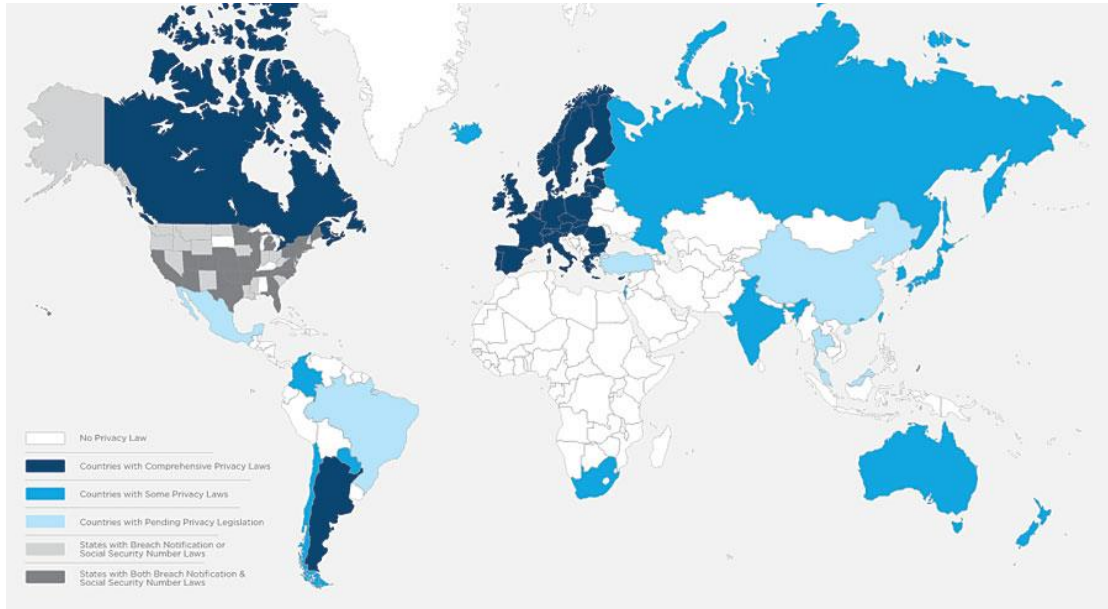
3.1.4 Ψευδωνυμία

Η έννοια της ψευδωνυμίας (pseudonymity) αναφέρεται στην προστασία ενός χρήστη από την αποκάλυψη της πραγματικής του ταυτότητας. Για να επιτευχθεί αυτό χρησιμοποιούνται ψευδώνυμα, δηλαδή αναγνωριστικά διαφορετικά και μη συσχετιζόμενα με το πραγματικό όνομα του χρήστη. Η ψευδωνυμία είναι μια λειτουργία που υλοποιείται όταν είναι αδύνατη η υλοποίηση της ανωνυμίας.

Στην περίπτωση των κοινωνικών δικτύων η ψευδωνυμία χρησιμοποιείται σε αρκετά μεγαλύτερο βαθμό από την ανωνυμία. Αυτό συμβαίνει στην πλειοψηφία των κοινωνικών δικτύων όπου οι χρήστες θέλουν να αποκρύψουν τα προσωπικά τους στοιχεία αλλά είναι απαραίτητη η εγγραφή τους σε αυτό. Έτσι χρησιμοποιούν ένα ψευδώνυμο, αντί για το πραγματικό τους όνομα, το οποίο θα είναι ορατό στους υπόλοιπους χρήστες του κοινωνικού δικτύου. Τα ψευδώνυμα αυτά στην πλειοψηφία των περιπτώσεων είναι αυτοδημιουργούμενα.

Σε μερικά μέσα κοινωνικής δικτύωσης όπως το “Facebook” η ψευδωνυμία δεν επιτρέπεται, καθώς είναι απαραίτητη η χρήση του αληθινού ονόματος του κάθε χρήστη. Στις περισσότερες των περιπτώσεων όμως, και σε κοινωνικά δίκτυα όπως το “Twitter”, μπορούν να χρησιμοποιηθούν ψευδώνυμα από τον καθένα και είναι συχνή και δημοφιλής αυτή η πρακτική. Ακόμα συχνότερα ψευδώνυμα χρησιμοποιούνται σε ειδικές κατηγορίες κοινωνικών δικτύων όπως τα “Forums”. Εκεί, όπου η ανταλλαγή απόψεων και ιδεών είναι ο κύριος λόγος χρήσης τους, τα ψευδώνυμα χρησιμοποιούνται σχεδόν σε απόλυτα

ποσοστά και οι χρήστες νιώθουν περισσότερο ελεύθεροι ώστε να εκφράσουν την προσωπική τους άποψη. [25]



Εικόνα 18: Νόμοι ιδιωτικότητας ανά τον κόσμο

3.2 Κίνδυνοι Ιδιωτικότητας στα Κοινωνικά Δίκτυα

Όλες οι απαιτήσεις που αναφέρθηκαν και που ορίζουν και επηρεάζουν σε πολλές περιπτώσεις τη λειτουργία των κοινωνικών δικτύων δεν θα υπήρχαν αν δεν εντοπιζονταν οι κίνδυνοι για την ιδιωτικότητα σε αυτά. Κίνδυνος ή αλλιώς απειλή μπορεί να χαρακτηριστεί οποιαδήποτε πιθανή ενέργεια ή γεγονός το οποίο μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων ιδιοτήτων ασφαλείας.

Οι κίνδυνοι αυτοί είναι πολλοί και σημαντικοί, καθώς και συνεχώς αυξανόμενοι με την ταυτόχρονη αύξηση χρήσης των κοινωνικών δικτύων. Τα προσωπικά προφίλ που δημιουργούν οι χρήστες στα μέσα

αυτά, πολλές φορές περιέχουν ευαίσθητες προσωπικές πληροφορίες και η προστασία τους συχνά αμφισβητείται. Υπεύθυνοι για τους κινδύνους αυτούς συνήθως είναι ενδεχόμενες κακόβουλες επιθέσεις όμως πολλές φορές οι απειλές προέρχονται είτε από σχεδιαστικά λάθη είτε από μη ηθελημένες ενέργειες.

Η χρήση και η εξάρτηση από τα κοινωνικά δίκτυα πολλών ανθρώπων τα καθιστούν ιδιαίτερα επικίνδυνα για την ιδιωτικότητα αυτών των ανθρώπων. Παρά τα οφέλη τους είναι γενικά αποδεκτό πως όσο περισσότερες προσωπικές πληροφορίες δημοσιεύει κάποιος χρήστης σε ένα ή περισσότερα κοινωνικά δίκτυα, τόσο μεγαλύτερη είναι η πιθανότητα για ενδεχόμενη ζημιά από κάποιους που έχουν κακόβουλες προθέσεις. Οι πληροφορίες αυτές είναι ικανές να προκαλέσουν κινδύνους και για τους ίδιους αλλά και για άλλους ανθρώπους. Οι κίνδυνοι που μπορούν να προκύψουν είναι οι εξής:

3.2.1 Πλαστοπροσωπία

Η πλαστοπροσωπία είναι ένα ζήτημα ασφαλείας που απασχολεί πολλούς τομείς της κοινωνικής και οικονομικής δραστηριότητας των σύγχρονων κοινωνιών. Στην περίπτωση των κοινωνικών δικτύων αφορά την κατασκευή ψεύτικων προφίλ με όνομα παρμένο από κάποιο άλλο υπαρκτό πρόσωπο και με σκοπό την προσποίηση πως δρα αυτό το άλλο υπαρκτό πρόσωπο. Είναι μια ηθελημένη κακόβουλη επίθεση και ο επιτιθέμενος δεν χρειάζεται να διαθέτει ιδιαίτερες εξειδικευμένες γνώσεις για να το πετύχει. Αρκεί η υποβολή των στοιχείων του ατόμου που θέλει

να προσποιηθεί ότι είναι. Σχεδόν σε όλα τα γνωστά κοινωνικά δίκτυα είναι εύκολο να επιτευχθεί καθώς δεν υπάρχουν επαρκείς μηχανισμοί ασφαλείας ενάντια στην εν λόγω επίθεση.

Μέσω αυτής της απειλής ο επιτιθέμενος μπορεί να πετύχει κοινωνική ζημιά ή ακόμα και οικονομική ζημιά στο θύμα του. Στην πρώτη περίπτωση, που είναι και η συνηθέστερη, είναι δυνατή η αποστολή μηνυμάτων ή η συγγραφή απόψεων οι οποίες δεν θα εκφράζουν το θύμα και παρόλα αυτά θα δημοσιεύονται εξ ονόματός του. Αυτές μπορούν να αλλοιώσουν τη γνώμη φίλων ή γνωστών του θύματος για το εν λόγω άτομο αλλά και να αμαυρώσουν τη δημόσια εικόνα του. Στην περίπτωση της οικονομικής απάτης που είναι και πιο σπάνια, ο επιτιθέμενος μπορεί να αποσπάσει μέσω της πλαστοπροσωπίας σημαντικά προσωπικά δεδομένα από κάποιον άλλο χρήστη, συνήθως στενό φίλο ή και συγγενή του θύματος. [27]

3.2.2 Κλοπή ταυτότητας

Πρόκειται για μια παραλλαγή της πλαστοπροσωπίας. Είναι μια απειλή που αποτελεί απάτη και που αφορά την συλλογή πληροφοριών που σχετίζονται με το θύμα. Τα στοιχεία αυτά χρησιμοποιούνται από τον επιτιθέμενο για την πλαστοπροσωπία του θύματος με στόχο, συνήθως, το οικονομικό όφελος. Σε αντίθεση με την απειλή της πλαστοπροσωπίας, στην κλοπή ταυτότητας δεν απαιτείται μόνο το όνομα του θύματος αλλά και διάφορες προσωπικές πληροφορίες όπως ημερομηνία γέννησης, διεύθυνση κατοικίας κ.α. Επίσης, ενώ στην πλαστοπροσωπία η απάτη

πραγματοποιείται εντός του κοινωνικού δικτύου, στην κλοπή ταυτότητας συνήθως τα προσωπικά δεδομένα κλέβονται μέσω του προσωπικού προφίλ του θύματος αλλά χρησιμοποιούνται εκτός αυτού με κάποιο άλλο τρόπο, διαδικτυακό ή μη.

Οι χρήστες των κοινωνικών δικτύων πολλές φορές αναρτούν τα προσωπικά τους δεδομένα στα προσωπικά τους προφίλ με τη θέληση τους χωρίς να σκέφτονται σχεδόν ποτέ τις συνέπειες που μπορεί να έχει αυτό. Τα ολοκληρωμένα προφίλ περιέχουν μεγάλο πλήθος ευαίσθητων πληροφοριών. Έτσι αν κάποιος αποκτήσει, μέσω επίθεσης, πρόσβαση σε αυτά μπορεί εύκολα να προβεί σε οικονομική εξαπάτηση του θύματος.
[28]



Εικόνα 19: Κλοπή ταυτότητας

3.2.3 Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό αφορά όλα τα προγράμματα τα οποία μπορεί να προκαλέσουν οποιαδήποτε βλάβη σε ένα υπολογιστικό σύστημα. Υπάρχουν χιλιάδες διαφορετικά είδη και παραλλαγές τέτοιου λογισμικού και αποτελεί ένα από τα σημαντικότερα προβλήματα της επιστήμης των

υπολογιστών γενικότερα. Πρωταρχικός στόχος είναι η μη διάδοση τέτοιου λογισμικού, όμως η χρήση των κοινωνικών δικτύων δεν βοηθάει σε αυτόν το σκοπό. Τα κοινωνικά δίκτυα είναι ιστοσελίδες με πολύ υψηλή δημοτικότητα και όπως είναι φυσικό ανάμεσα στα δισεκατομμύρια των χρηστών τους, υπάρχει ένας τεράστιος αριθμός χρηστών με ελάχιστες έως ανύπαρκτες γνώσεις για την ασφάλεια του διαδικτύου. Οι επιτιθέμενοι εκμεταλλεύονται αυτή την άγνοια, όπως και πιθανές ευπάθειες της υπηρεσίας, με στόχο τον μεγαλύτερο δυνατό διαμοιρασμό του κακόβουλου λογισμικού.

Ο συνηθέστερος τρόπος επίθεσης και χρήσης αυτής της απειλής είναι μέσω ενός μηνύματος που στέλνεται σε άλλους χρήστες και παραπέμπει σε κάποια φαινομενικά “αθώα” διεύθυνση ιστοσελίδας. Αφού το θύμα ενεργοποιήσει τον συγκεκριμένο σύνδεσμο τότε το κακόβουλο λογισμικό εγκαθίσταται στον υπολογιστή του χωρίς την δική του έγκριση και σε αρκετές περιπτώσεις ένα αντίγραφο του αρχικού μηνύματος κοινοποιείται αυτόματα σε επαφές του θύματος ώστε να διαδοθεί κι άλλο το λογισμικό αυτό. Αυτό το λογισμικό σε αρκετές περιπτώσεις είναι ικανό να υποκλέψει προσωπικά δεδομένα και στοιχεία των θυμάτων με σκοπό την εξαπάτησή τους.

3.2.4 Phishing

Ένας κίνδυνος που έχει ομοιότητες με την απειλή του κακόβουλου λογισμικού είναι το phishing. Αυτό αναφέρεται σε όλους τους τρόπους με τους οποίους ο επιτιθέμενος (“phisher”) μπορεί να αποσπάσει από το

θύμα του στοιχεία όπως κωδικούς πρόσβασης λογαριασμών, αριθμούς πιστωτικών καρτών κλπ.

Όπως και στην απειλή του κακόβουλου λογισμικού, έτσι κι εδώ, ο επιτιθέμενος μπορεί να αποσπάσει αυτά τα δεδομένα μέσω ενός μηνύματος που στέλνει σε άλλους χρήστες των κοινωνικών δικτύων. Συνήθως αυτό το μήνυμα περιέχει έναν σύνδεσμο ο οποίος οδηγεί σε κάποια ιστοσελίδα που τις περισσότερες φορές μοιάζει οπτικά και έχει παρόμοιο “url” με γνωστά κοινωνικά δίκτυα όπως το “Facebook” ή με άλλες ιστοσελίδες, όπως ιστοσελίδες μεγάλων τραπεζών. Είτε από απροσεξία, είτε από ευπιστία, είτε λόγω ανεπαρκών γνώσεων αρκετά είναι τα θύματα που δεν αναγνωρίζουν τις διαφορές και εξαπατώνται. Όταν το θύμα ανοίξει αυτές τις ιστοσελίδες εμφανίζονται στην οθόνη του υπολογιστή του τα πεδία στα όποια πρέπει να καταχωρήσει το “username” και το “password” του ώστε να εισέλθει στην υποτιθέμενη υπηρεσία. Αντί για αυτό όμως τα στοιχεία αυτά στέλνονται στον “phisher” ο οποίος πλέον έχει στην κατοχή του τα στοιχεία πρόσβαση του θύματος. Από τη στιγμή που ο επιτιθέμενος αποκτά τα στοιχεία αυτά μπορεί, ανάλογα με τα στοιχεία που έχει υποκλέψει, είτε να βλάψει οικονομικά το θύμα του είτε να πραγματοποιήσει πειρατεία και να αποκτήσει τον πλήρη έλεγχο του προφίλ του. [29]

Η πειρατεία του προφίλ μπορεί να επιτευχθεί και με άλλους τρόπους εκτός του phishing, αυτοί είναι είτε με τη χρήση κακόβουλου λογισμικού είτε με άλλου είδους επιθέσεις. Στον τομέα των κοινωνικών δικτύων όμως είναι λιγότερο πιθανές.



Εικόνα 20: Phishing στ α Social Media

3.2.5 Data mining

Ο σημαντικότερος και δυσκολότερα αντιμετωπίσιμος κίνδυνος που αφορά την ιδιωτικότητα στα μέσα κοινωνικής δικτύωσης είναι αυτός της εξόρυξης δεδομένων (“data mining”). Είναι γνωστό πως τα κέρδη των μεγαλύτερων κοινωνικών δικτύων προέρχονται κατά κύριο λόγο από άλλες επιχειρήσεις μέσω της διαφήμισης. Επίσης οι χρήστες που διατηρούν προφίλ σ’ αυτά τα δίκτυα, δίνουν τα προσωπικά τους στοιχεία κατά την πλοήγηση σ’ αυτά ενώ μέσω των επιλογών τους καταχωρούνται και οι προσωπικές τους προτιμήσεις για διάφορα θέματα. Όλα αυτά τα στοιχεία συλλέγονται και επεξεργάζονται κατά τρόπο για τον οποίο η πλειονότητα των χρηστών έχει μερική ή και πλήρη άγνοια.

Τα κοινωνικά δίκτυα καταγράφουν όλες τις κινήσεις, τις ενέργειες και τις συμπεριφορές των χρηστών τους ώστε να εξάγουν τα απαραίτητα για αυτά συμπεράσματα. Όλα αυτά τα στοιχεία καταγράφονται σε βάσεις δεδομένων και μέσω του πολύ ισχυρού hardware που χρησιμοποιείται πλέον, αυτά αναλύονται. Η διαδικασία αυτή της ανάλυσης ονομάζεται

“data mining” και συνδυάζει διάφορες τεχνικές όπως στατιστική ανάλυση και δέντρα αποφάσεων. Μέσω αυτής της διαδικασίας εξερευνώνται υπερβολικά μεγάλοι όγκοι δεδομένων ώστε να εξαχθούν συμπεράσματα κυρίως για την καταναλωτική συμπεριφορά των χρηστών. Πολλά από αυτά τα συμπεράσματα οι χρήστες δεν γνωρίζουν καν ότι υπάρχουν.

Τα συμπεράσματα που εξάγονται προωθούνται σε ενδιαφερόμενες επιχειρήσεις, όπως χορηγούς ή εταιρίες ανάλυσης δεδομένων, ώστε αυτές μελετώντας τις καταναλωτικές συνήθειες των ατόμων να καθορίσουν την διαφημιστική και επικοινωνιακή τους πολιτική. Το “Facebook” έχει κατηγορηθεί πολλές φορές για παράνομη χρήση προσωπικών δεδομένων των χρηστών του. Είναι χαρακτηριστικό πως ακόμα κι αν ένας χρήστης διαγράψει κάποια στοιχεία από το προφίλ του, αυτά παραμένουν στις βάσεις δεδομένων του “Facebook” και χρησιμοποιούνται για ανάλογους σκοπούς. [30]

Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το Facebook κ.λπ.



Εικόνα 21: Εξώφυλλο του περιοδικού “Time” σχετικά με τα προσωπικά δεδομένα

Κεφάλαιο 4: Προστασία της Ιδιωτικότητας στα Κοινωνικά Δίκτυα

Όπως αναφέρθηκε και στο «Κεφάλαιο 3», οι κίνδυνοι παραβίασης της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης είναι σημαντικοί και συνεχώς αυξανόμενοι. Στο κεφάλαιο αυτό θα παρουσιαστούν ορισμένα πραγματικά παραδείγματα παραβίασης της ιδιωτικότητας που έχουν συμβεί σε δημοφιλή κοινωνικά δίκτυα και έπειτα θα προταθούν και θα αναλυθούν οι τρόποι και τα μέτρα προστασίας της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης. Τέλος θα παρουσιαστεί αναλυτικά και η περίπτωση του δημοφιλέστερου κοινωνικού δικτύου, του “Facebook”, και η ασφάλεια που αυτό παρέχει σε ότι αφορά τα προσωπικά δεδομένα.

4.1 Παραδείγματα παραβίασης της ιδιωτικότητας σε κοινωνικά δίκτυα

Η έκρηξη χρήσης των κοινωνικών δικτύων από το 2000 κι έπειτα έχει οδηγήσει και σε αντίστοιχα μεγάλο αριθμό των ζητημάτων παραβίασης της ιδιωτικότητας. Παρακάτω καταγράφονται ορισμένα από αυτά τα ζητήματα για τα περισσότερα από τα οποία έχουν υπάρξει δικαστικές διαμάχες και ατέρμονες συζητήσεις.

- **Οι διαφημίσεις του “Facebook”**

Οι παράνομες δραστηριότητες στο “Facebook” έχουν πάρει μεγάλη έκταση τα τελευταία χρόνια, ειδικά οι επιθέσεις “phishing”, η οποία είναι ο δημοφιλέστερος τρόπος για να κλέψει κάποιος τους κωδικούς πρόσβασης άλλων ατόμων και αναλύθηκε σε προηγούμενο κεφάλαιο. Σύμφωνα με δημοσίευμα ιστοσελίδας τον Απρίλιο του 2010, έγινε γνωστό πως ένας χάκερ είχε κλέψει και πουλήσει τις ταυτότητες 1,5 εκατομμυρίων χρηστών του “Facebook” σε κάποιες επιχειρήσεις οι οποίες ήθελαν να προσελκύσουν πιθανούς νέους πελάτες μέσω της χρήσης διαφημίσεων στο “Facebook”. Η παράνομη προσέγγιση έγινε με διαφημίσεις από τις επιχειρήσεις προς τους φίλους των χρηστών των οποίων κλάπηκαν τα στοιχεία τους. Όταν οι φίλοι αυτοί είδαν τις διαφημίσεις, θα τις εξέταζαν και θα είχαν γνώμη για αυτές, καθώς οι άνθρωποι ακολουθούν πολύ πιο εύκολα κάτι που τους έχει προταθεί από ένα φίλο τους σε σχέση με κάποιον άγνωστο. Σύμφωνα με έρευνα το 2.22% των χρηστών του “Facebook” πιστεύει ή ακολουθεί τις διαφημίσεις των φίλων τους. Μπορεί αυτό να φαίνεται ένα μικρό ποσοστό άλλα πρόκειται για ένα πολύ μεγάλο αριθμό χρηστών από τη στιγμή που το “Facebook” έχει πάνω από 700 εκατομμύρια ενεργούς χρήστες. Η επιρροή των διαφημίσεων στο “Facebook” είναι τεράστια και προφανής, όπως προφανές είναι και το τεράστιο κέρδος που προσελκύει τους χάκερ να κλέψουν τα στοιχεία σύνδεσης των χρηστών του πιο δημοφιλούς κοινωνικού δικτύου.

- **Spokeo**

Το “Spokeo” είναι μια μηχανή αναζήτησης ανθρώπων με αποτελέσματα που συγκεντρώνονται μετά από υπολογισμό διάφορων δεδομένων. Η ιστοσελίδα περιέχει πληροφορίες όπως την ηλικία, την κατάσταση σχέσης, την προσωπική περιουσία, τα κοντινά μέλη της οικογένειας και την διεύθυνση κατοικίας ορισμένων ανθρώπων. Οι πληροφορίες αυτές συγκεντρώνονται μέσω των στοιχείων που βρίσκονται ήδη στο διαδίκτυο ή σε άλλα δημόσια αρχεία, όμως η ιστοσελίδα δεν εγγυάται την ακρίβειά τους.

Το “Spokeo” αντιμετώπισε το ενδεχόμενο πιθανών νομικών προσφυγών από ανθρώπους που ισχυρίζονταν ότι η οργάνωση παραβιάζει τον αμερικάνικο νόμο Δίκαιης Πίστωσης Αναφοράς. Το Σεπτέμβριο του 2010 η Jennifer Purcell ισχυρίστηκε πως το “Spokeo” είχε παραβιάσει το νόμο αυτό καθώς εμπορευόταν τις προσωπικές πληροφορίες της. Η υπόθεση αυτή ακόμα εκκρεμεί. Επίσης τον Απρίλιο του 2010, ο Thomas Robins ισχυρίστηκε πως οι προσωπικές του πληροφορίες που ήταν αναρτημένες στην ιστοσελίδα ήταν ανακριβείς και δεν είχε τη δυνατότητα να επεξεργαστεί ώστε να τις μετατρέψει σε ακριβείς. Η υπόθεση αυτή απορρίφθηκε επειδή ο Robins δεν υποστήριξε πως το γεγονός αυτό και η ιστοσελίδα του προκάλεσε κάποια πραγματική ζημιά.

spokeo

Join Login

Name Email Phone Username Address

Jane Smith, Boston, MA Search

Enter a first and last name (John Doe or Jane Doe, Los Angeles, CA)

Not your grandma's phone book.

Εικόνα 22: Η ιστοσελίδα “Spokeo”

- **Το ζήτημα του “Twitter”**

Τον Ιανουάριο του 2011, η κυβέρνηση των ΗΠΑ εφάρμοσε μια δικαστική υπόθεση η οποία ανάγκαζε το κοινωνικό δίκτυο, “Twitter”, να αποκαλύψει πληροφορίες σχετικές με ορισμένους χρήστες του, οι οποίοι ήταν εμπλεκόμενοι στην υπόθεση “WikiLeaks”. Αυτή η απόφαση είναι αμφισβητήσιμη καθώς αντιβαίνει με τα δικαιώματα των χρηστών που ισχύουν σύμφωνα με το Σύνταγμα των ΗΠΑ. Το “Twitter” κινήθηκε για να αντιστραφεί αυτή η δικαστική απόφαση και υποστήριξε την ιδέα πως οι χρήστες του διαδικτύου θα πρέπει να ειδοποιούνται για τέτοια γεγονότα και να τους δίνεται η ευκαιρία να υπερασπιστούν τα συνταγματικά δικαιώματά τους στο δικαστήριο.

- **Οι εκπαιδευτικοί και το “MySpace”**

Η προστασία της ιδιωτικότητας των εκπαιδευτικών στο “MySpace” έχει δημιουργήσει διαμάχη σε όλο τον κόσμο. Διάφορα μέσα ενημέρωσης στις ΗΠΑ προειδοποιούσαν τους εκπαιδευτικούς να διαγράψουν τους λογαριασμούς τους και να προσέχουν τι δημοσιεύουν στο διαδίκτυο. Οι εκπαιδευτικοί στις ΗΠΑ μπορούν να αντιμετωπίσουν την ανάκληση των αδειών τους, αναστολές ή γραπτές επιπλήξεις ανάλογα με το παράπτωμα στο οποίο μπορεί να υπέπιπταν σε κάποιο μέσο κοινωνικής δικτύωσης. Το άρθρο ενός περιοδικού εκπαίδευσης, το

οποίο δημοσιεύτηκε τον Απρίλιο του 2007, είχε τίτλο «Μια φωτογραφία στο “MySpace” κόστισε σε μια φοιτήτρια το Πιστοποιητικό Διδασκαλίας», και αφορούσε την Stacy Snyder. Η Snyder φοιτούσε σ’ ένα πανεπιστήμιο της Πενσυλβανία, το οποίο της στέρησε το πτυχίο διδασκαλίας της, λόγω μιας φωτογραφίας που είχε κοινοποιήσει στο “MySpace” και κρίθηκε αντιεπαγγελματική. Αυτή η φωτογραφία την απεικόνιζε να πίνει κάποιο ποτό φορώντας ένα πειρατικό καπέλο και με τη λεζάντα «Μεθυσμένος Πειρατής». Τιμωρήθηκε για αυτό και σαν υποκατάστατο της δόθηκε ένα κατώτερο πτυχίο. [31]

4.2 Τρόποι προστασίας της ιδιωτικότητας στα κοινωνικά δίκτυα

Η δημιουργία ενός προφίλ σε κάποιο κοινωνικό δίκτυο άμεσα συνεπάγεται ορισμένους κινδύνους ιδιωτικότητας των προσωπικών δεδομένων. Οι κίνδυνοι αυτοί μπορούν με διάφορους τρόπους μπορούν να βλάψουν το χρήστη και κατ’ επέκταση την κοινωνία. Ο τρόπος δόμησης των κοινωνικών δικτύων καθιστά ευάλωτους τους χρήστες σε επιθέσεις που μπορεί να έχουν στόχο την ασφάλεια των προσωπικών του πληροφοριών.

Για το λόγο αυτό είναι αναγκαίο να αναλυθούν οι τρόποι με τους οποίους ένας χρήστης μπορεί να προστατευτεί με τον καλύτερο δυνατό τρόπο από τους κινδύνους αυτούς, είτε με αντίμετρα που πρέπει να εφαρμόσουν οι ίδιοι, είτε με μέτρα εφαρμοσμένα από τα ίδια τα μέσα κοινωνικής δικτύωσης.

4.2.1 Αντίμετρα χρηστών

- **Ρυθμίσεις απορρήτου**

Οι ρυθμίσεις απορρήτου είναι ένα σύνολο ρυθμίσεων που υφίστανται πλέον στην πλειοψηφία των μέσων κοινωνικής δικτύωσης και με αυτές καθορίζονται από τον κάθε χρήστη οι ρυθμίσεις που σχετίζονται με την ιδιωτικότητα και την ασφάλεια του κάθε ατομικού προφίλ και των προσωπικών δεδομένων. Μέσω των ρυθμίσεων αυτών ένας χρήστης μπορεί να επιλέξει εάν το προφίλ του θα είναι ορατό μόνο στους “φίλους” του ή και στους υπόλοιπους χρήστες, αν και το ποιος μπορεί να δημοσιεύσει το οτιδήποτε στο προφίλ του, το αν μπορεί κάποιος να σχολιάσει τις δημοσιεύσεις, το σε ποιους ακριβώς θα είναι ορατές οι φωτογραφίες του προφίλ, και άλλα πολλά.

Εάν ένας χρήστης επιθυμεί τη μέγιστη δυνατή ασφάλεια των προσωπικών του πληροφοριών τότε θα πρέπει να θέσει ενεργές αυτές τις επιλογές ώστε να επιτρέψουν την ελάχιστη δυνατή διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Συνήθως οι προεπιλεγμένες ρυθμίσεις απορρήτου προσφέρουν πολύ μικρή προστασία όποτε σχεδόν πάντα είναι απαραίτητο να τις επεξεργαστούν οι χρήστες ώστε να προστατέψουν την ιδιωτικότητά τους. Ακόμα κρίνεται απαραίτητο σημαντικά προσωπικά δεδομένα όπως ημερομηνία γέννησης, διεύθυνση κατοικίας κ.α. να ορίζονται ως ορατά μόνο σε άτομα πλήρους εμπιστοσύνης. [32]

- **Κωδικός πρόσβασης**

Ο κωδικός πρόσβασης είναι το κλειδί για να εισέρθει και κάποιος και να μπορεί να επεξεργαστεί το προσωπικό του προφίλ. Είναι απαραίτητο οι χρήστες να έχουν έναν ισχυρό κωδικό πρόσβασης ώστε να ελαχιστοποιήσουν την πιθανότητα να εισέλθει κάποιος άλλος αντί για αυτούς στο λογαριασμό τους. Ως ισχυρός κωδικός πρόσβασης ορίζεται ένας κωδικός ο οποίος αποτελείται από αρκετούς χαρακτήρες οι οποίοι θα είναι ένα σύνολο πεζών γραμμάτων, κεφαλαίων γραμμάτων, αριθμών και συμβόλων και δεν θα περιέχει λέξεις συνηθισμένες ή ευδιάκριτα σχετικές με το άτομο στο οποίο ανήκει ο λογαριασμός. Αν αυτές οι συνθήκες δεν εκπληρώνονται είναι επικίνδυνο κάποιος να μαντέψει τον κωδικό πρόσβασης του χρήστη και να αποκτήσει πρόσβαση σε πολλά ευαίσθητα προσωπικά δεδομένα του. Τέλος είναι απαραίτητο οι χρήστες να μην αποκαλύπτουν τον κωδικό πρόσβασης τους ούτε σε πολύ στενούς φίλους ή συγγενείς τους καθώς και τότε είναι προφανής ο κίνδυνος για την ιδιωτικότητά τους.



Εικόνα 23: Username και password

- **Δημοσιευμένα δεδομένα**

Τη στιγμή που ένας χρήστης δημοσιεύει το οτιδήποτε σε ένα μέσο κοινωνικής δικτύωσης τότε αυτόματα αυτό αποθηκεύεται προσωρινά σε όλο το διαδίκτυο. Επίσης τα δεδομένα από τη στιγμή που δημοσιεύονται ανήκουν στο κοινωνικό δίκτυο που συμβαίνει αυτό. Οπότε παρά τις πολιτικές προστασίας των δεδομένων που ισχύουν στα γνωστότερα κοινωνικά δίκτυα πάντα υπάρχει ο κίνδυνος αλλαγής αυτών των πολιτικών.

Για τους λόγους αυτούς οι χρήστες χρειάζεται να έχουν μεγάλη προσοχή και να είναι απόλυτα σίγουροι στο τι πληροφορίες και δεδομένα δημοσιεύουν. Πρέπει να αποκρύπτουν οτιδήποτε μπορεί να χαρακτηριστεί ως ευαίσθητο δεδομένο και από το οποίο μπορεί να τους προκληθεί η οποιαδήποτε ζημιά. Για παράδειγμα δεν πρέπει να δημοσιεύεται κάτι που ίσως προδώσει μια προσωπική αδυναμία που θα μπορούσε να εκμεταλλευτεί ένας επιτήδειος. Επίσης θα πρέπει να αποφεύγεται η αποκάλυψη της ακριβούς τοποθεσίας που βρίσκεται την παρούσα στιγμή ένας χρήστης καθώς είναι επικίνδυνο να γνωρίζει ένας επιτήδειος την κάθε του κίνηση. [33]

- **Αναξιόπιστοι σύνδεσμοι**

Πολλές φορές οι χρήστες χρησιμοποιούν ένα κοινωνικό δίκτυο για να ανακαλύψουν νέους συνδέσμους και ενδιαφέροντα άρθρα και βίντεο. Έτσι το μεγαλύτερο ποσοστό των χρηστών είναι ιδιαίτερα δεκτικό σε συνδέσμους που μπορεί να ανακαλύψουν ή να τους αποσταλούν σ' ένα κοινωνικό δίκτυο. Τις περισσότερες φορές ένας τέτοιος σύνδεσμος είναι ασφαλής, υπάρχουν όμως και οι περιπτώσεις όπου σε κάποιους συνδέσμους μπορεί να εμπεριέχονται ιοί. Ακόμα και αυτές οι

περιπτώσεις ενδέχεται να προέρχονται από έμπιστες επαφές του χρήστη οι οποίες όμως έχουν ήδη μολυνθεί με τον ίδιο ιό. Για τους λόγους αυτούς πρέπει το κάθε μέλος ενός μέσου κοινωνικής δικτύωσης να είναι ιδιαίτερα προσεκτικό ως προς τα μηνύματα που λαμβάνει ακόμα και από τους πιο έμπιστους “φίλους” του, γιατί μπορεί να κινδυνέψει άμεσα η ιδιωτικότητά του. Μέσω των ιών μπορεί να κλαπούν ευαίσθητα προσωπικά δεδομένα, όποτε είναι η απαραίτητη η επίσκεψη μόνο αξιόπιστων τοποθεσιών. [34]

4.2.2 Αντίμετρα κοινωνικών δικτύων

- **Επαλήθευση λογαριασμών**

Το φαινόμενο και ο κίνδυνος της πλαστοπροσωπίας στα κοινωνικά δίκτυα μπορεί να αντιμετωπιστεί επιτυχώς μόνο από την σωστή εφαρμογή ενός μηχανισμού επαλήθευσης. Η πλαστοπροσωπία, μπορεί να προκαλέσει κοινωνική ή οικονομική ζημιά στα θύματά της, και αποτελεί αντικείμενο προβληματισμού σε ότι αφορά τα κοινωνικά δίκτυα. Τα ίδια τα κοινωνικά δίκτυα έχουν προσπαθήσει, σε αρχικό ακόμα στάδιο να λύσουν αυτό το ζήτημα.

Από το 2008 και μετά μεγάλα κοινωνικά δίκτυα, όπως το “Twitter” και το “Google+”, δημιούργησαν μηχανισμούς επαλήθευσης κυρίως για επώνυμους χρήστες. Αυτοί οι μηχανισμοί περιόρισαν τους ψεύτικους λογαριασμούς σε κάποιο βαθμό και σημάδευαν με ειδικό σήμα του πιστοποιημένους λογαριασμούς. Στο “Twitter” έγινε προσπάθεια

επέκτασης του μηχανισμού αυτού αλλά παρουσιάστηκαν αρκετά προβλήματα και έτσι εγκαταλείφθηκε αυτή η σκέψη. Σε αντίθεση όμως με το “Twitter” και άλλα κοινωνικά δίκτυα που εφαρμόζουν μηχανισμούς επαλήθευσης λογαριασμών για μικρό αριθμό χρηστών, στο “Facebook” έχει γίνει μια πιο σημαντική προσπάθεια και πλέον εφαρμόζεται σε μεγάλη μάζα των χρηστών η επαλήθευση των λογαριασμών μέσω ταυτοποίησης με δημόσια έγγραφα, ειδικά σε ύποπτους για πλαστοπροσωπία λογαριασμούς.



Εικόνα 24: Το σύμβολο της επαλήθευσης στο “Twitter”

Για την εξάλειψη του φαινομένου, είναι απαραίτητο και τα υπόλοιπα μέσα να υιοθετήσουν αυτή την τακτική με σκοπό την προστασία της ιδιωτικότητας των χρηστών τους και φυσικά τη μη αποκάλυψη των δεδομένων τους. [35]

- **Διαμόρφωση πολιτικής ασφάλειας**

Όπως όλα τα πληροφοριακά συστήματα που βασίζονται σε κώδικα για να λειτουργήσουν, έτσι και τα κοινωνικά δίκτυα λειτουργούν βάσει του προγραμματιστικού κώδικα στα οποία είναι γραμμένα. Το γεγονός αυτό όπως είναι προφανές τα καθιστά προσιτά σε επιθέσεις hacker. Κάθε κενό ασφαλείας που μπορεί να εμφανιστεί στον κώδικα οποιουδήποτε

κοινωνικού δικτύου είναι ευκαιρία για τον κάθε hacker ώστε να επιτεθεί. Συνήθως οι επιπτώσεις αφορούν τους χρήστες και τα δεδομένα τους αφού οι επιθέσεις συνήθως στοχεύουν σε αυτά.

Εξαιτίας των δεδομένων αυτών εξάγεται το συμπέρασμα πως πρέπει τα μέσα κοινωνικής δικτύωσης να μεριμνούν με τον καλύτερο δυνατό τρόπο ώστε να εξαλείφεται κάθε πιθανό κενό ασφαλείας. Ακόμα είναι υποχρέωση της κάθε υπηρεσίας η διαμόρφωση επαρκούς πολιτικής ασφάλειας ώστε να προστατεύονται τα δεδομένα των χρηστών τους. Χαρακτηριστικό παράδειγμα τέτοιας πολιτικής είναι το “Facebook” το οποίο από το 2011 και μετά πριμοδοτούσε με χρηματική επιβράβευση τους χρήστες που θα ανέφεραν την οποιαδήποτε ευπάθεια στο σύστημα. [36]

- **Ρυθμίσεις απορρήτου**

Όπως αναφέρθηκε και στα αντίμετρα των χρηστών είναι απαραίτητο οι χρήστες να θέτουν ενεργές όλες τις επιλογές στις ρυθμίσεις απορρήτου ώστε να επιτρέψουν την ελάχιστη δυνατή διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες και κατά συνέπεια τη μεγαλύτερη δυνατή ασφάλεια των δεδομένων τους.

Από τη μεριά τους όμως, και τα μέσα κοινωνικής δικτύωσης είναι υποχρεωμένα να προσφέρουν όσο περισσότερες επιλογές απορρήτου και ιδιωτικότητας είναι ικανά. Το “Facebook” έχει κάνει σημαντικά βήματα προόδου στον τομέα αυτό τα τελευταία χρόνια καθώς έχει προσθέσει έναν σημαντικό αριθμό ρυθμίσεων απορρήτου, ενώ άλλα κοινωνικά δίκτυα έχουν μεγάλα περιθώρια βελτιστοποίησης των ρυθμίσεων

απορρήτου τους. Υπάρχουν κοινωνικά δίκτυα όπου βασικά προσωπικά στοιχεία του χρήστη όπως το όνομα και η διεύθυνση είναι ορατά και εκτεθειμένα σε όλο τον κόσμο, χωρίς να υπάρχει η δυνατότητα απόκρυψής τους. Αυτά οφείλουν να δίνουν την δυνατότητα της επιλογής στους χρήστες τους για το πόσα και ποια δεδομένα τους θα είναι ορατά στους υπόλοιπους χρήστες. [32]

- **Κοινωνική ευθύνη**

Από οτιδήποτε αναφέρθηκε έως τώρα υπάρχει κάτι πιο σημαντικό και κρίσιμο για την προστασία των δεδομένων των χρηστών. Αυτό δεν είναι τίποτα άλλο από την εταιρική και κοινωνική ευθύνη των ίδιων των κοινωνικών δικτύων. Με βάση το είδος της υπηρεσίας που προσφέρουν τα μέσα κοινωνικής δικτύωσης κατέχουν στις βάσεις δεδομένων τους προσωπικά στοιχεία και δεδομένα εκατομμυρίων χρηστών. Αυτά τα στοιχεία είναι υπερπολύτιμα για διαφημιστικές εταιρίες και επιχειρήσεις που θέλουν να προωθήσουν τα προϊόντα τους.

Αποτελεί χρέος λοιπόν των εταιριών στις οποίες ανήκουν τα κοινωνικά δίκτυα να προστατεύουν τα προσωπικά στοιχεία και στην ουσία τους ίδιους τους χρήστες και πελάτες τους. Είναι ζήτημα ηθικό η μη πώληση στοιχείων των χρηστών τους που έχει ξεκάθαρο στόχο το κέρδος, όπως και η μη χρησιμοποίηση παραθύρων του νόμου που προστατεύει τέτοιες πρακτικές. Οποιαδήποτε παρόμοια ενέργεια οφείλουν τα κοινωνικά δίκτυα να γίνεται μόνο και αυστηρά κατόπιν σύμφωνης γνώμης και ξεκάθαρης αποδοχής του χρήστη, και φυσικά χωρίς να αντιμετωπίζει την

παραμικρή επίπτωση για κάποια πιθανή άρνησή του.



Εικόνα 25: Social Responsibility

Τέλος αποτελεί καθήκον των κοινωνικών δικτύων η χρήση των πιο εξελιγμένων και σύγχρονων μεθόδων προστασίας υλικού, λογισμικού και δεδομένων σε όλους τους τομείς και τα στάδια χρήσης όπου υπάρχει ο παραμικρός κίνδυνος υποκλοπής. Είναι απαραίτητη η χρήση μεθόδων προστασίας και στη διακίνηση των δεδομένων μέσω του διαδικτύου, αλλά και η χρήση μεθόδων αυστηρής προστασίας στους servers του εκάστοτε μέσου όπου και αποθηκεύονται όλα τα προσωπικά δεδομένα των χρηστών. [37]

Κεφάλαιο 5: Συμπεράσματα

Με βάση όλα αυτά που αναλύθηκαν στην εργασία αυτή μπορούμε να εξάγουμε μερικά συμπεράσματα και να προτείνουμε κάποια θέματα που θα μπορούσαν να αναλυθούν στο μέλλον.

Είναι γενικά αποδεκτό σε όλες τις σύγχρονες και τεχνολογικά επαρκώς ανεπτυγμένες κοινωνίες, τα κοινωνικά δίκτυα καταλαμβάνουν σημαντικότατο κομμάτι της καθημερινής επικοινωνίας των ανθρώπων. Η ανάπτυξή τους είναι συνεχής και ραγδαία. Ακόμα και σε χώρες που υπολείπονται τεχνολογικά από τον παγκόσμιο μέσο όρο, παρατηρείται μεγάλη αύξηση των μέσων κοινωνικής δικτύωσης. Τα μέσα αυτά μπορεί να είναι είτε γενικού ενδιαφέροντος, με κύριο στόχο την επικοινωνία, ή ειδικού ενδιαφέροντος όπως τα μέσα που απευθύνονται αποκλειστικά σε επαγγελματίες.

Τα πιο δημοφιλή κοινωνικά δίκτυα έχουν εκατομμύρια χρήστες και στην κορυφή όλων βρίσκεται το “Facebook” που αποτελεί από μόνο του ένα κοινωνικό φαινόμενο.

Αυτό το φαινόμενο όμως, το γενικότερο φαινόμενο των κοινωνικών δικτύων πέρα από τα οφέλη επικοινωνίας που προσφέρει μπορεί να οδηγήσει και σε σημαντικούς κινδύνους. Γενικά η τεχνολογία έχει διευκολύνει σε άπειρους τομείς τον σύγχρονο άνθρωπο όμως μία συνέπεια όλων αυτών των πλεονεκτημάτων είναι η καταπάτηση της ιδιωτικότητας του σύγχρονου ανθρώπου.

Ο άνθρωπος από τη φύση του έχει ανάγκη να προστατεύει την ιδιωτικότητά του και το δικαίωμα να μένει μόνος του. Είναι επίσης

σημαντικό τα προσωπικά δεδομένα όλων να παραμένουν προσωπικά και να μην γίνονται δημόσια, καθώς σε αντίθετη περίπτωση πολλά προβλήματα μπορούν να προκύψουν σε ατομικό και κατ' επέκταση σε κοινωνικό επίπεδο.

Τα κοινωνικά δίκτυα λόγω της φύσης τους και του τρόπου λειτουργίας τους είναι ο ιδανικός τρόπος για να διαδοθούν προσωπικά, και σε πολλές περιπτώσεις ευαίσθητα, δεδομένα. Πολλοί απατεώνες τα χρησιμοποιούν και τα εκμεταλλεύονται ώστε να εξυπηρετήσουν τους παράνομους σκοπούς τους. Οι κίνδυνοι που προκύπτουν λόγω της χρήσης των κοινωνικών δικτύων είναι πολλοί, και ξεκινούν από την πιθανή κλοπή της ταυτότητας ενός χρήστη από έναν άλλον και φτάνουν έως την επεξεργασία των προσωπικών πληροφοριών ενός χρήστη με το στόχο την εξαγωγή συμπερασμάτων συμπεριφοράς τα οποία μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς.

Εξαιτίας όλων αυτών των κινδύνων, και των πολλών παραδειγμάτων καταπάτησης της ιδιωτικότητας που έχουν συμβεί μέσω των κοινωνικών δικτύων, είναι απαραίτητο να παρθούν ορισμένα αντίμετρα προστασίας. Τέτοια αντίμετρα πρέπει να λαμβάνονται και από τη μεριά του χρήστη και από τη μεριά των κοινωνικών δικτύων. Πέρα από την προφανή ανάγκη του κάθε χρήστη να προστατεύσει την ιδιωτικότητά του και τα προσωπικά του δεδομένα, είναι απαραίτητη και η βοήθεια των ίδιων των κοινωνικών δικτύων ώστε να προστατέψουν τους χρήστες τους. Αποτελεί χρέος ως προς την κοινωνία το να μην πραγματοποιούνται παράνομες πράξεις και οι επίδοξοι απατεώνες να αποτρέπονται από αυτές.

Ως προς τις μελλοντικές μελέτες θα μπορούσε να εξεταστεί το νομικό μέρος του ζητήματος και ο τρόπος με τον οποίο θα προστατεύεται νομικά

ο κάθε πολίτης σε μια τέτοια περίπτωση, στην περίπτωση δηλαδή που δεν έχει προστατευθεί επιτυχώς η ιδιωτικότητα ενός χρήστη. Τέλος, θα μπορούσαν να εξεταστούν αναλυτικά οι κίνδυνοι και οι πιθανές επιθέσεις που μπορούν να υποστούν οι χρήστες των κοινωνικών δικτύων, όπως για παράδειγμα η περίπτωση του phishing.

Πανεπιστήμιο Πειραιώς

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Wikispaces, Κοινωνική Δικτύωση
(<http://learn20.wikispaces.com/%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE+%CE%94%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CF%83%CE%B7+%28%CE%BA%CE%B5%CE%AF%CE%BC%CE%B5%CE%BD%CE%BF%29>)
- [2] Danah M. Boyd & Nicole B. Ellison, Social Network Sites: Definition, History and Scholarship, 2007
- [3] Corey Guilbault, Second Mover Advantage: The Difference between First & Leader, 2010
(<http://cyncerely.com/tag/theglobe-com/>)
- [4] Digital Trends Staff, The History of Social Networking, 2014
(<http://www.digitaltrends.com/features/the-history-of-social-networking/>)
- [5] Sarah Phillips, A Brief History of Facebook, 2007
(<http://www.theguardian.com/technology/2007/jul/25/media.newmedia>)
- [6] Kenneth Byrd, What is a Blog?, 2011
(<http://blogbasics.com/what-is-a-blog/>)
- [7] Wikipedia, Internet Forum
(http://en.wikipedia.org/wiki/Internet_forum)
- [8] Media Sharing Sites
(<http://www.gavilan.edu/tlc/ic/media-sharing.html>)
- [9] Wikipedia, Microblog
(<http://simple.wikipedia.org/wiki/Microblog>)
- [10] Donna Cosmato, Advantages and Disadvantages of Social Networking, 2013

(http://socialnetworking.lovetoknow.com/Advantages_and_Disadvantages_of_Social_Networking)

[11] Wikipedia, Facebook

(<http://en.wikipedia.org/wiki/Facebook>)

[12] Θοδωρής Κόνσουλας, Τι είναι το LinkedIn και πώς λειτουργεί;, 2014

(<http://www.socialmedialife.gr/109338/linkedin-ti-einai-kai-pos-leitourgei/>)

[13] Wikipedia, Twitter

(<http://en.wikipedia.org/wiki/Twitter>)

[14] Wikipedia, Google+

(<http://en.wikipedia.org/wiki/Google%2B>)

[15] Wikipedia, Pinterest

(<http://en.wikipedia.org/wiki/Pinterest>)

[16] Wikipedia, YouTube

(<http://el.wikipedia.org/wiki/YouTube>)

[17] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", 1890

[18] Wikipedia, Privacy

(<http://en.wikipedia.org/wiki/Privacy>)

[19] Alan F. Westin, Social and Political Dimensions of Privacy, 2003

(<http://www.privacysummersymposium.com/reading/westin.pdf>)

[20] Global Internet Liberty Campaign, Privacy and Human Rights

(<http://gilc.org/privacy/survey/intro.html>)

[21] The Public Voice, Privacy

(http://thepublicvoice.org/issues_and_resources/privacy_01.html)

[22] Pam Dixon & Robert Gellman, Online Privacy, 2011

(https://books.google.gr/books?id=4scv_OjuUHgC&pg=PA81&lpg=PA81&dq=privacy+1970+german+sweden&source=bl&ots=knyBMk1026&sig=w6oJmW58ez8GZelPljAzp1RhEks&hl=el&sa=X&ei=jVACVYuJH4PWU6TUgKAD&ved=0CF8Q6AEwCQ#v=onepage&q=privacy%201970%20german%20sweden&f=false)

[23] EPIC, Privacy and Human Rights Report, 2006

(<http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Models.html>)

[24] Stefanos Gritzalis, Enhancing Web privacy and anonymity in the digital era, 2004

[25] Andreas Pfitzmann & Marit Hansen, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management, 2005

[26] European Commission, How will the data protection reform affect social networks?

(http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf)

[27] Leyla Bilge & Thorsten Strufe & Davide Balzarotti & Engin Kirde, All Your Contacts Are Belong to US: Automated Identity Theft Attacks on Social Networks, 2009

[28] Maksim Reznik, Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation, 2013

(<http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=1472&context=lawreview>)

[29] Tom Jagatic & Nathaniel Johnson & Markus Jakobsson & Filippo Menczer, Social Phishing, 2005

[30] Martha C. White, Big Data Knows What You're Doing Right Now, 2012

(<http://business.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/>)

[31] Wikipedia, Privacy issues of social networking sites

(http://en.wikipedia.org/wiki/Privacy_issues_of_social_networking_sites)

- [32] Ralph Gross & Alessandro Acquisti, Information Revelation and Privacy in Online Social, 2005
- [33] Inteco, Study on the Privacy of Personal Data and on the Security of Information in Social Networks, 2009
(http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/intecoaepr_privacy_and_security_social_networks_web_accessible.pdf)
- [34] Wikipedia, Criticism of Facebook
(http://en.wikipedia.org/wiki/Criticism_of_Facebook)
- [35] Gary Locke, What is a Verified Social Media Account (and Why Does it Matter?), 2014
(<http://www.commonplaces.com/blog/what-verified-social-media-account-and-why-does-it-matter/>)
- [36] Nipul Patel & Hetal Jasani, Social Media Security Policies: Guidelines for Organizations, 2010
- [37] Heidi Cohen, Facebook Needs to Be Socially Responsible and Why Marketers Must Care, 2011
(<http://heidicohen.com/facebook-needs-to-be-socially-responsible-and-why-marketers-must-care/>)