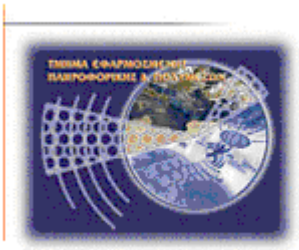
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

Τμήμα Μηχανικών Πληροφορικής



Πτυχιακή Εργασία

Τίτλος: Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Αντώνης Θεοδώρου (ΑΜ: 2934)

Ηράκλειο – 08/12/2016

Επόπτης Καθηγητής: Δρ. Παπαδάκης Νίκος

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

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

Ευχαριστίες

Με την ολοκλήρωση της πτυχιακής μου εργασίας νιώθω την ανάγκη να ευχαριστήσω τον Δρ. Παπαδάκη Νίκο και το Δρ. Μανιφάβα Χαράλαμπο για την πολύτιμη και σημαντική βοήθεια τους καθ' όλη τη διάρκεια της εκπόνησης της πτυχιακής εργασίας γιατί χωρίς την καθοδήγηση τους και την παροχή των κατάλληλων εφοδίων τίποτα δεν θα ήταν κατορθωτό σήμερα. Επίσης θα ήθελα να ευχαριστήσω όσους ανθρώπους ήταν κοντά μου τον τελευταίο καιρό αλλά και κατά την διάρκεια των σπουδών μου αφού με την στήριξη και την υπομονή τους με ενθάρρυναν μέχρι το τέλος και είμαι εδώ σήμερα.

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Λεπτομέρειες
08/12/2016	Τελική	Προσομοίωση της τελικής έκδοσης με το πρότυπο του επιβλέπων καθηγητή
30/06/2016	1.5	**Μέρος Β** Ανάλυση και Σχολιασμός Ερωτηματολογίου
10/05/2016	1.4	**Μέρος Β** Διανομή Ερωτηματολογίου στους ερωτηθέντες
07/04/2016	1.3	**Μέρος Β** Προγραμματισμός και Δημιουργία Ερωτηματολογίου
12/12/2015	1.2	**Μέρος Α** Κεφάλαιο 3 και Κεφάλαιο 4
11/11/2015	1.1	**Μέρος Α** Κεφάλαιο 2
10/09/2015	1.0	**Μέρος Α** Κεφάλαιο 1

Περίληψη

Η παρούσα πτυχιακή εργασία χωρίζεται σε δυο κύριες ενότητες και σχετίζεται με τα προσωπικά δεδομένα και το πως οι διαρροές προσωπικών δεδομένων εν αγνοία μας μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες αλλά και συμβουλές με τρόπους που θα διασφαλίζουν τα προσωπικά δεδομένα με την εφαρμογή μηχανισμών ενίσχυσης.

Το πρώτο μέρος χωρίζεται σε τέσσερα κεφάλαια. Αρχικά στο 1ο κεφάλαιο θα γίνει ανάλυση της νομοθετικής έννοιας στο πέρασμα των χρόνων των προσωπικών δεδομένων σε Διεθνές αλλά και σε Ευρωπαϊκό επίπεδο όπου είναι πλήρως εναρμονισμένη η Κύπρος.

Ακολουθεί το 2ο κεφάλαιο που θα γίνει περιγραφή και ανάλυση του προβλήματος της έκθεσης των προσωπικών δεδομένων στο διαδίκτυο με έμφαση στην ιδιωτικότητα στον κυβερνοχώρο και τι ορίζεται προσωπικό δεδομένο στο κόσμο του διαδικτύου. Θα αναφερθούν και θα σχολιαστούν τα κοινωνικά μέσα δικτύωσης που κυριαρχούν στην αγορά εν έτη 2016 και πως η λανθασμένη χρήση τους από ανυποψίαστους χρήστες τους μπορεί να τους αφήσει απροστάτευτους και έρμαιο στους κακόβουλους χρήστες/hackers αλλά και το πως παρακολουθούνται τα ψηφιακά μας βήματα από διεθνείς οργανισμούς.

Στο 3ο κεφάλαιο θα γίνει αναφορά σε μεθόδους ανίχνευσης παραβίασης των προσωπικών δεδομένων αλλά και σε τεχνολογίες ενίσχυσης και επιτήρησης της ιδιωτικότητας του χρήστη.

Στο 4ο κεφάλαιο θα γίνει αναφορά στις πολλές τεχνικές που υπάρχουν για την προστασία των προσωπικών δεδομένων των χρηστών του διαδικτύου και με ποίο τρόπο μπορεί ο κάθε χρήστης να νιώθει ασφαλής για τα προσωπικά του δεδομένα.

Το δεύτερο μέρος αφορά το πρακτικό κομμάτι της πτυχιακής όπου θα γίνει λεπτομερής παρουσίαση των αποτελεσμάτων ποιοτικής και πρωτοποριακής έρευνας για την Κύπρο με θέμα τα προσωπικά δεδομένα στην σύγχρονη εποχή και το πόσο επηρεάζουν την ηλεκτρονική ζωή του ανθρώπου και ανάλυση τους με βάση το ευρύτερο κοινωνικό και πολιτισμικό πλαίσιο που αναφερόμαστε.

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Οι δυο βασικοί πυλώνες που θα αναφερθούν στην έρευνα είναι τα δημογραφικά χαρακτηριστικά του Κύπριου χρήστη του διαδικτύου και η διερεύνηση ασφαλούς χρήσης των προσωπικών δεδομένων. Θα σκιαγραφηθεί ο Κύπριος πολίτης σαν χρήστης του διαδικτύου, θα γίνει συζήτηση των αποτελεσμάτων και θα γίνει σύγκριση με άλλες παρόμοιες έρευνες που έχουν γίνει στον τομέα αύτο.

Abstract

This dissertation is divided in two main chapters. It looks at how personal information can be leaked and stolen without our knowledge and consent, so they could be used from malicious users and it will give suggestions on ways to detect and insure the safety of these information through the establish of enhancement mechanisms.

First Chapter

First chapter is divided in four sections. Section 1 looks at how the law has been modified through time on protecting personal data in Europe and international level which Cyprus is fully harmonized.

Section 2 will describe and analyze the problem that exists with online personal data and what defines data as personal information. Also it will look at social media and how one can be vulnerable to hackers or even international organizations especially when they are not cautious and use the social media in a wrong way.

Section 3 will look at different detection methods for cyber user's privacy and how technological enforcements can help keep this information private.

At Section 4 will mention several techniques that we can use to keep secret our privacy in internet world and in which way any user will feel safe about his/her privacy.

Second Chapter

Here it will present in detail the results from the qualitative research that took place in Cyprus which looked at how personal information in the modern era can affect ones online profile. Also it will look at detection methods and techniques to ensure the users's personal information from malicious users and hackers.

The two main pillars which will mention in the research are the demographic characteristics of the Cypriot cyber users and the amplification of the safe use of their privacy. We will outlined the Cypriot citizen such a cyber user, we will discuss about the results and last but not least we will compare these results with others researches that took place in the same sector.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

ΚΕΦΑΛΑΙΟ 1ο – ΕΙΣΑΓΩΓΗ

1.1 Ορισμός των προσωπικών δεδομένων

Τα προσωπικά δεδομένα ορίζονται ως «η κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, απ' τα οποία δεν μπορούν πλέον να προσδιορισθούν τα δεδομένα που αναφέρονται στο φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.»

Συνεπώς τα προσωπικά δεδομένα συνιστούν κάθε πληροφορία που αναφέρεται και προσδιορίζει ένα άτομο, όπως δεδομένα αναγνώρισης που είναι το όνομα, το επώνυμο, η ηλικία, η οικογενειακή κατάσταση, η διεύθυνση κατοικίας και εργασίας, το επάγγελμα, η εκπαίδευση, η οικονομική κατάσταση, τα ηλεκτρονικά ίχνη, τα ενδιαφέροντα, οι δραστηριότητες και οι συνήθειες ενός ατόμου κ.α.

Ορισμένες μάλιστα κατηγορίες προσωπικών δεδομένων, που αναφέρονται στην βάση της ιδιωτικής μας ζωής χαρακτηρίζονται ευαίσθητα δεδομένα και τυγχάνουν μεγαλύτερης προστασίας. Τα ευαίσθητα δεδομένα αφορούν κυρίως τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, την υγεία και κοινωνική πρόνοια, την ερωτική ζωή και τον σύντροφο του καθενός, τις ποινικές διώξεις και καταδίκες. Δηλαδή αφορούν περισσότερο τον άνθρωπο σε σχέση με τον κοινωνικό και πολιτισμικό πόλο της κοινωνίας και είναι από τα προσωπικά δεδομένα και δικαιώματα του ανθρώπου που καταπατώνται πιο εύκολα.

1.1.2 Νομοθετική Έννοια σε Διεθνές επίπεδο

Τέλος της δεκαετίας του 1940 κατοχυρώθηκε για πρώτη φορά το δικαίωμα της προστασίας των προσωπικών δεδομένων, μέσω του άρθρο 12 της Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα το οποίο αναφέρει ότι «κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Ο καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.»

Έτσι ακολούθησε η απόφαση 2450/19-12-1968 η οποία απώτερο σκοπό είχε την προστασία των δικαιωμάτων του ατόμου για τα οποία αναφέρονται σε ζητήματα καταπάτησης ανθρωπίνων δικαιωμάτων. Αυτά προκύπτουν από τη χρήση των σύγχρονων ηλεκτρονικών μέσων, την ραγδαία εξέλιξη της τεχνολογίας έτσι γεννήθηκε η επιτακτική ανάγκη οριοθέτησής της και θέσπισης ενός νόμου ο οποίος θα περιείχε τα πιο πάνω χαρακτηριστικά

Τότε ένας Διεθνής Οργανισμός ο Ο.Ο.Σ.Α το 1980 προχώρησε στην έκδοση των ονομαζόμενων «Κατευθυντήριων Αρχών που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων» με σκοπό την προστασία των προσωπικών δεδομένων . Ωστόσο δεν είχαν δεσμευτικό χαρακτήρα δηλ. δεν ήταν απαραίτητο να τον εφαρμόσουν όλα τα κράτη, όμως θεσπίστηκε σε μεγάλο αριθμό χωρών όπου αρκετά νομοθετικά πλαίσια που εφαρμόστηκαν αργότερα είχαν σαν εφαλτήριο τις συγκεκριμένες κατευθυντήριες αρχές και κοινά χαρακτηριστικά που διέπουν τις διασυνοριακές αυτές ροές.

Λόγω της καθοριστικής συμμετοχής των πιο πάνω κατευθυντήριων αρχών θα ήταν παράλειψη να μην αναφερθούμε σ’ αυτές, οι οποίες είχαν καθοριστικό ρόλο στην μετέπειτα θέσπιση νομότυπων ροών. Με την αρχή περιορισμένης συλλογής τίθεται το ζήτημα της συλλογής προσωπικών δεδομένων όμως βάζοντας όρια στη συλλογή τους όπου με την ενημέρωση και την άδεια του εκάστοτε χρήστη αυτό να γίνεται με νόμιμα μέσα σε αντίθεση με αυτό που γινόταν στο παρελθόν.

Η αρχή Ποιότητας των δεδομένων και η αρχή Προσδιορισμού Σκοπού στις οποίες αναφέρεται ότι τα προσωπικά δεδομένα πρέπει να είναι σχετικά και να συμπίπτουν με

το σκοπό για το οποίο θα χρησιμοποιηθούν και να είναι πλήρη, ακριβή και διαρκώς ενημερωμένα, ώστε να μην υπάρξει παρερμηνεία τους.

Η αρχή Περιορισμένης Χρήσης στην οποία αναφέρεται ότι τα προσωπικά δεδομένα δε θα πρέπει να γίνονται γνωστά σε τρίτους ή να χρησιμοποιούνται για σκοπούς άλλους πέραν από αυτούς που έχει συμφωνηθεί, εκτός εάν υπάρχει σχετική συναίνεση του χρήστη ή επιβάλλεται από το νόμο (π.χ εγκληματικές υποθέσεις). Η αρχή Προστασίας Ασφάλειας αναφέρει ότι τα προσωπικά δεδομένα θα πρέπει να τυγχάνουν προστασίας ούτως ώστε να αποφεύγονται κίνδυνοι όπως η απώλεια, η πρόσβαση σε μη εξουσιοδοτημένα άτομα, καταστροφή ή αποκάλυψη σε τρίτες οντότητες.

Η αρχή Διαφάνειας στην οποία αναφέρεται ότι θα πρέπει να υπάρχει γενική αρχή διαφάνειας όσον αφορά στις πολιτικές και πρακτικές που ακολουθούνται για τη συλλογή και επεξεργασία των προσωπικών δεδομένων.

Η αρχή Συμμετοχής του Ατόμου στην οποία αναφέρεται ότι ο άνθρωπος έχει το κάθε δικαίωμα να αποκτά επιβεβαίωση σχετικά με το αν ο υπεύθυνος των δεδομένων έχει στοιχεία που αφορούν το εν λόγω άτομο και να του κοινοποιούνται δεδομένα που σχετίζονται με αυτό: σε εύλογο χρονικό διάστημα, με λογικό αντίτιμο, με εύλογο τρόπο και με εύκολο τρόπο λήψης. Επίσης πρέπει να γίνεται κοινοποίηση των λόγων απόρριψης των αιτημάτων του ώστε να διατηρεί τη δυνατότητα της αντίδρασης επί αυτών. Όμως μπορεί να αμφισβητήσει στοιχεία που σχετίζονται με αυτό και εάν έχει δίκιο, να μπορεί να προχωρεί σε διόρθωση, τροποποίηση, συμπλήρωση ή διαγραφή των δεδομένων αυτών.

Τέλος με την αρχή Ευθύνης αναφέρεται ότι ο υπεύθυνος διαχείρισης των προσωπικών δεδομένων θα πρέπει να είναι υπόλογος σχετικά με την τήρηση των παραπάνω αρχών.

Το νομοθετικό πλαίσιο που θεσπίστηκε είχε ως στόχο την ταυτόχρονη συνύπαρξη του δικαιώματος του απόρρητου και της προστασίας των προσωπικών δεδομένων των ανθρώπων, αλλά παράλληλα και το δικαίωμα της συλλογής πληροφοριών, το οποίο πηγάζει από το δικαίωμα της ελεύθερης έκφρασης δημοκρατικής προσωπικής άποψης.

1.1.3 Νομοθετική Έννοια στην Ε.Ε

Μετά την εμφάνιση της πληροφορικής έγινε πλέων αναγκαία η θέσπιση κανόνων με περισσότερη λεπτομέρεια για την προάσπιση των δικαιωμάτων του ατόμου μέσα από την προστασία των προσωπικών δεδομένων. Μέχρι τα μέσα της δεκαετίας του 1970, η Επ. Υπουργών του Συμβουλίου της Ευρώπης είχε εκδώσει διάφορα ψηφίσματα όσον αφορά στην προστασία των προσωπικών δεδομένων.

Έτσι την δεκαετία του 1980 οδηγήθηκε προς υπογραφή η Σύμβαση "για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων" πιο γνωστή και ως Σύμβαση 108. Η συγκεκριμένη σύμβαση προστατεύει το άτομο από ενδεχόμενες καταχρηστικές ενέργειες και αποβλέπει στη ρύθμιση της διασυνοριακής ροής προσωπικών δεδομένων κάτι εφάμιλλο με τις κατευθυντήριες αρχές οι οποίες θεσπίστηκαν σε διεθνές επίπεδο λίγο καιρό πριν. Αυτή συνιστά σημείο αναφοράς σχετικά με τη θέσπιση νόμων περί προστασίας των προσωπικών δεδομένων. Έτσι εφαρμόζεται σε οποιαδήποτε επεξεργασία προσωπικών δεδομένων η οποία λαμβάνει χώρα οπουδήποτε όπως την επεξεργασία προσωπικών δεδομένων από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου. Στόχος της είναι η προστασία του ατόμου από ενδεχόμενες καταχρηστικές ενέργειες που αποβλέπουν στη ρύθμιση της διασυνοριακής ροής προσωπικών δεδομένων.

Λίγο πριν την καινούρια χιλιετία λόγω και της ραγδαίας εξέλιξης των ψηφιακών τεχνολογιών στα τηλ/κά δίκτυα προστέθηκε και η Κοινοτική Οδηγία 97/66/ΕΚ150 «περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα». Έτσι είχε ως αποτέλεσμα την δημιουργία νέων προκλήσεων σχετικά με την προστασία της ιδιωτικότητας των χρηστών. Η Κοινοτική Οδηγία 97/66/ΕΚ150 αφορά κυρίως ζητήματα ασφάλειας των υπηρεσιών και των δικτύων, των δεδομένων σχετικά με την κίνηση και τη χρέωση του απόρρητου των επικοινωνιών, το δικαίωμα της μη αναλυτικής χρέωσης, της αναγραφής της ταυτότητας του καλούντος, της αυτόματης προώθησης κλήσεων, την αναγραφή των στοιχείων στους τηλεφωνικούς καταλόγους των χρηστών καθώς και τις μη ζητηθείσες κλήσεις για εμπορικούς σκοπούς.

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Το 2002 η Ε.Ε αντικατέστησε την τελευταία προαναφερθείσα Οδηγία η οποία αφορούσε την «επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών». Η ύπαρξη της οδηγίας αυτής για την προστασία της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα και η δέσμευση των κοινοτικών υπηρεσιών αντανακλούν στην προάσπιση της ιδιωτικότητας από την Ευρωπαϊκή Ένωση και στην παρουσία ενός δείγματος ρυθμίσεων που εξειδικεύουν τους κανόνες της Οδηγίας.

Αρχικά εναρμονίζονται οι διατάξεις των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, Επίσης διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ε.Ε.

Κατοχυρώνεται το απόρρητο των επικοινωνιών που διενεργούνται μέσω δημόσιου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των δεδομένων κίνησης τα οποία πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας. Όσα δεδομένα αφορούν συνδρομητές και χρήστες, υποβάλλονται σε επεξεργασία και αποθηκεύονται.

Τέλος τονίζεται ότι για την χρησιμοποίηση αυτόματων συστημάτων κλήσης και επικοινωνίας για εμπορικούς σκοπούς, απαιτείται προηγουμένως η συγκατάθεση του συνδρομητή και εφόσον δεν αποκρύπτονται η ταυτότητα του αποστολέα και η διεύθυνση για αποστολή αιτήματος τερματισμού. Κάτι παρόμοιο που το συναντούμε καθημερινά στην ζωή μας είναι η αποστολή διαφημιστικών ή ενημερωτικών emails στο προσωπικό μας λογαριασμό τα οποία ενδείκνυται να περιέχουν την επιλογή unsubscribe ώστε να αφαιρεθεί ο προσωπικός μας λογαριασμός από την βάση δεδομένων τους και να γίνει τερματισμός της επικοινωνίας.

Πιο πρόσφατα και λίγο πριν την σημερινή δεκαετία θεσπίστηκε μια καινούρια οδηγία η οποία περιέχει διατάξεις που ρυθμίζουν τη δημοσιοποίηση των παραβάσεων προσωπικών δεδομένων, παρέχει συστάσεις προς τα θιγόμενα πρόσωπα και υποχρεώνει τον πάροχο να ενημερώνει για τα μέτρα που έχουν ληφθεί για την αντιμετώπιση της παραβίασης. Ακόμα παροτρύνει τους χρήστες των υπηρεσιών

ηλεκτρονικών επικοινωνιών να προβαίνουν σε αναγκαία μέτρα προφύλαξης του τεχνικού εξοπλισμού τους από κακόβουλο λογισμικό και κακόβουλους χρήστες.

Η πρόταση που κατέθεσε η Ε.Ε πριν 4 χρόνια αφορούσε στη ριζική αλλαγή των ρυθμιστικών κανόνων προστασίας των προσωπικών δεδομένων στα κράτη μέλη της ευρωπαϊκής ένωσης. Κύριος στόχος της διαδικασίας αυτής είναι μία ενιαία πολιτική που θα εφαρμόζεται από όλα τα ευρωπαϊκά κράτη μέλη, στη οποία ο ευρωπαίος πολίτης θα είναι βασικός επόπτης της προστασίας των πληροφοριών. Μακροπρόθεσμοι στόχοι αυτής της πρότασης ήταν η απλούστευση της νομικής έννοιας με μία σειρά καθοριστικών ρυθμίσεων έτσι ώστε να καταστεί η ψηφιακή αγορά, ενιαία σε όλο τον επιχειρηματικό τομέα. Να ενδυναμώσει την πληροφορική διάθεση και να γίνει έγκυρη και έγκαιρη συγκατάθεση ενημέρωση του χρήστη για τον οποίο αναφέρεται. Να αναπτυχθούν τεχνολογικές μέθοδοι για την άμεση λήψη αποφάσεων από το χρήστη και να θεσπιστεί η ανάγκη για την συστηματική προστασία των ανηλίκων πολιτών του διαδικτύου.

Σήμερα με την συνεχιζόμενη και ραγδαία αύξηση της πληροφορίας η Ε.Ε αναγκάζεται να εναρμονιστεί πλήρως στις ανάγκες της εποχής που ζούμε όπου τα έξυπνα τηλέφωνα και τα μέσα κοινωνικής δικτύωσης είναι αναπόσπαστο κομμάτι της καθημερινότητας μας. Τελευταία με ακόμα τρεις καινούριες τροποποιήσεις οδηγίες ήρθε να εξαλείψει ακόμα περισσότερο την ανασφάλεια που επικρατεί στους χρήστες/πολίτες της Ε.Ε έτσι ώστε να διασφαλίζεται η προστασία της ιδιωτικής ζωής στις ηλεκτρονικές πληροφορίες.

Οι οδηγίες αυτές έχουν δεσμευτικό χαρακτήρα έτσι ώστε όλα τα κράτη μέλη να είναι πλήρως εναρμονισμένα στις οδηγίες της κομίσιον. Αυτά θα πρέπει να προχωρήσουν στην ίδρυση και στον ορισμό μιας αρμόδιας αρχής με σκοπό την πρόληψη, ανίχνευση, διερεύνηση και δίωξη πιο σοβαρών εγκλημάτων όπως η τρομοκρατία. Αυτή η αρχή θα είναι αρμόδια για τη συλλογή και διαχείριση των δεδομένων PNR από τους αερομεταφορείς και ακολούθως θα γίνεται η μεταβίβασή τους στις αρχές.

1.2 Προσωπικά Δεδομένα στην Κύπρο του 2016

Η Κύπρος ως κράτος-μέλος της Ευρωπαϊκής Ένωσης, όφειλε και οφείλει να εναρμονιστεί με βάση τις κοινοτικές Οδηγίες επομένως ότι ισχύει σε Διεθνές και σε Ευρωπαϊκό επίπεδο ισχύει και για την Κύπρο.
Μέσω του Επίτροπου προστασίας προσωπικών δεδομένων προσωπικού χαρακτήρα γίνεται μια προσπάθεια ευαισθητοποίησης γύρω από την έννοια των προσωπικών δεδομένων και πόσο σημαντικά είναι αυτά τα δεδομένα να είναι επαρκώς ασφαλισμένα.

Η κρατική μηχανή της χώρας με την βοήθεια μεγάλων ιδιωτικών εταιριών της χώρας, προσπαθούν να επιστήσουν την προσοχή στο πόσο σημαντική είναι η προστασία των Κυπρίων πολιτών και των οργανισμών της χώρας για να αυξηθεί η προσδιοριστική τάση για αυτοπροστασία.

Εκτίμηση κινδύνου

Επανεξέταση των υφιστάμενων συστημάτων για τον προσδιορισμό του κινδύνου της ιδιωτικής ζωής σε όλο τον οργανισμό. Αυτό περιλαμβάνει την εξέταση σε ροές δεδομένων και στις διαδικασίες συλλογής δεδομένων, καθώς και τεχνικούς ελέγχους και επιχειρησιακές διαδικασίες για την εφαρμογή της τήρησης της προστασίας των δεδομένων σε όλο τον οργανισμό.

Πολιτική Προστασίας Προσωπικών Δεδομένων

On-line, Off-line ανάπτυξη ή αναθεώρηση των πολιτικών απορρήτου για την υποστήριξη και τη συμμόρφωση με όλους τους σχετικούς νόμους και τη νομοθεσία, τους κανονισμούς και τις προσδοκίες των χρηστών.

Πρόγραμμα συμμόρφωσης

Βοηθώντας τους οργανισμούς να αναπτύξουν ένα εσωτερικό πρόγραμμα για τη διαχείριση της διαρκούς συμμόρφωσης με τις πολιτικές προστασίας της ιδιωτικής ζωής και των δεδομένων τους.

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Επιχειρησιακές διαδικασίες και Εφαρμογή

Προσδοκία ανάπτυξης και αναθεώρησης των επιχειρησιακών διαδικασιών περιλαμβανομένης της διακυβέρνησης που θα βοηθήσει στην απόδειξη ότι η προστασία της ιδιωτικής ζωής είναι σημαντικό ζήτημα και υλοποιείται σε καθημερινές δραστηριότητες.

Λύσεις Προστασίας Προσωπικών Δεδομένων

Αντιμετώπιση των ειδικών προκλήσεων της ιδιωτικής ζωής που συνδέονται με την παρουσία στο Διαδίκτυο ενός οργανισμού μέσω της αξιολόγησης των κινδύνων, την ανάπτυξη και την εφαρμογή των πολιτικών και των προτύπων και τη χρήση αποκλειστικών τεχνολογιών ενίσχυσης της προστασίας της ιδιωτικής ζωής.

Έλεγχος Προστασίας Προσωπικών Δεδομένων

Ολοκληρώνοντας ένα προσαρμοσμένο πλήρες πρόγραμμα ελέγχου της ιδιωτικής ζωής, προκειμένου να προσδιοριστούν τα αποθέματα των προσωπικών δεδομένων και των μοντέλων αξιοποίησης και να παρέχουν εκτίμηση της επάρκειας του προγράμματος συμμόρφωσης της ιδιωτικής ζωής.

Εκπαίδευση και Ευαισθητοποίηση

Παροχή προσαρμοσμένης εκπαίδευσης των χρηστών για την προστασία προσωπικών δεδομένων στους οργανισμούς όσον αφορά τις ευαίσθητες δραστηριότητες της ιδιωτικής ζωής και την εφαρμογή των κωδίκων πρακτικής προστασίας της νομοθεσίας.

ΚΕΦΑΛΑΙΟ 2ο – ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

2.1 Η έννοια της ιδιωτικότητας

Η προστασία της ιδιωτικής ζωής είναι μια ιδέα που υπήρχε πριν από τα σημερινά τηλ/κά δίκτυα και τεχνολογίες και είναι μια φυσική δράση του ατόμου ως ένα από τα δημόσια και βασικά δικαιώματα του.

Η εξελισσόμενη και ταχεία εξέλιξη των νέων τεχνολογιών, όπως τα δίκτυα τηλεπικοινωνιών και ειδικότερα το Διαδίκτυο, ιδιαίτερα με την παρουσίαση του κ. Berners-Lee το 1991 ο οποίος παρουσίασε το World Wide Web. Το www παρουσιάστηκε σαν ένα Internet που δεν ήταν απλώς ένας τρόπος για να στείλει κάποιος αρχεία από το ένα μέρος στο άλλο, αλλά ήταν το ίδιο ένα "web" από πληροφορίες που ο καθένας θα μπορούσε να ανακτήσει στο Διαδίκτυο δηλαδή σαν μια πολύ μεγάλη βάση δεδομένων γεμάτη από πληροφορίες.

Στην Κύπρο το διαδίκτυο παρουσιάστηκε 4 χρόνια μετά και ονομαζόταν λογοδίκτυο. Η σύνδεση γινόταν μέσω τηλεφωνικής γραμμής, με ταχύτητα μόλις 64 Kbps ενώ δεν επιτρεπόταν να γίνει ταυτόχρονη χρησιμοποίηση του τηλεφώνου και του διαδικτύου.

Η χρήση του Διαδικτύου έχει αυξηθεί με ταχείς ρυθμούς και πλέων θεωρείται μέρος της καθημερινής μας ζωής αφού μεγάλος όγκος εργασιών που διεκπεραιώνουμε γίνεται μέσω του διαδικτύου. Σήμερα μια επιχείρηση δεν έχει να κερδίσει κάτι αν όλα της τα αρχεία είναι σε μορφή μη διαχειρήσημη και ακατάλληλη για επεξεργασία γιατί θα απαιτείτε πολύς χρόνος μέχρι να ολοκληρωθεί η οποιαδήποτε ενέργεια. Τελευταία η δημόσια υπηρεσία και διάφοροι κρατικοί οργανισμοί είναι οι τελευταίοι που μηχανογραφήθηκαν έτσι ώστε ο πολίτης να εξυπηρετείτε πιο αποτελεσματικά, γρήγορα και μεθοδικά.

Η ιδιωτικότητα παρουσιάζεται ως «η μη εισβολή, ο έλεγχος των πληροφοριών και η περιορισμένη πρόσβαση στα προσωπικά δεδομένα, όπου η έννοια αυτή συνδέεται με διάφορες έννοιες όπως τα προσωπικά χαρακτηριστικά του ατόμου, τις προσωπικές επικοινωνίες και τα προσωπικά δεδομένα.»

2.2 Η διαδικτυακή ιδιωτικότητα και τα προσωπικά δεδομένα

Η ιδιωτικότητα στο διαδίκτυο αποτελεί αναπόσπαστο κομμάτι της ιδιωτικότητας της πληροφορίας η οποία αφορά την απαίτηση του ατόμου να μην είναι διαθέσιμα τα προσωπικά του δεδομένα σε άλλα άτομα και οργανισμούς. Η ιδιωτικότητα αναφέρεται στη δυνατότητα του ατόμου να ασκεί ένα σημαντικό βαθμό ελέγχου σχετικά τη χρήση των προσωπικών του δεδομένων. Η διαδικτυακή ιδιωτικότητα ορίζεται με το δικαίωμα της διατήρησης της προσωπικής ιδιωτικότητας σχετικά με την αποθήκευση, τη μετατροπή, τη διάθεση σε άλλους και την επίδειξη πληροφοριών μέσω του διαδικτύου, οι οποίες αφορούν κάποιο χρήστη.

Μέσα στα πλαίσια της οριοθέτησης των προσωπικών δεδομένων ο διεθνής οργανισμός O.E.C.D αναφέρθηκε σε αυτά ως η οποιαδήποτε πληροφορία που σχετίζεται με την ταυτοποίηση ενός ατόμου.
Σύμφωνα λοιπόν με τον οργανισμό είναι προσωπικά δεδομένα τα οποία έχουν δημιουργηθεί από τον ίδιο το χρήση ή δραστηριότητες στο διαδίκτυο όπως πληρωμές κάποιου λογαριασμού για παράδειγμα. Ο προσδιορισμός της θέσης του ατόμου μέσω του κινητού τηλεφώνου ή μέσω της διεύθυνσης IP συνιστούν προσωπικό δεδομένο. Επίσης όλα τα δημογραφικά στοιχεία και οτιδήποτε άλλο μπορεί να περιέχεται στην κατηγορία των προσωπικών δεδομένων. Αυτό θεωρείται δημοσιοποίηση των προσωπικών δεδομένων και αυτές οι προσωπικές συναλλαγές έχουν προκαλέσει αύξηση της ανησυχίας μεταξύ των χρηστών του Διαδικτύου για την ιδιωτική ζωή.

Γνωστό είναι και το θέμα που προέκυψε με το σκάνδαλο σχετικά με την δράση της NSA από το 2013 όταν αυτό αποκαλύφθηκε από τον Edward Snowden πρώην πράκτορα της CIA, πως αυτή κατασκοπεύει τους Αμερικάνους χρήστες και όχι μόνο και γίνεται επεξεργασία των προσωπικών δεδομένων τους. Τότε μετά τις αποκαλύψεις ξεκίνησε ένα κύμα διαδηλώσεων εναντίον της εκάστοτε κυβέρνησης και της μυστικής υπηρεσίας πληροφοριών που οι οποίες είχαν σαν αποτέλεσμα την δημιουργία του USA Freedom Act μια πράξη ελευθερίας που επέβαλλε περιορισμούς στην δράση της NSA. Το εφαλτήριο και η αφορμή να περαστεί το μήνυμα πως η Αμερική έχει ανάγκη μια τέτοια υπηρεσία ήταν μετά την τρομοκρατική επίθεση στις 11 Σεμπτεβρίου 2001 στους δίδυμους πύργους κάτι που έπληξε την ασφάλεια της Η.Π.Α. Αυτή η μυστική υπηρεσία λειτουργά με κρυπτογραφημένους κώδικες,

κώδικες που δύσκολα θα καταλάβει ο μέσος Αμερικάνος και δημιουργεί συστήματα κωδικοποίησης συνομιλιών για ολόκληρη την τηλεπικοινωνία είτε τηλεφωνική είτε διαδικτυακή και περιφέρεται γύρω από την πολιτική, στρατιωτική και τρομοκρατική μάζα της χώρας.

Οι ανησυχίες προστασίας της ιδιωτικής ζωής δε είναι πρωτοφανές θέμα, αλλά παρουσιάστηκε από την αρχή της εντατικής χρήσης του διαδικτύου, μετά την είσοδο της τελευταίας δεκαετίας όπου τα κοινωνικά δίκτυα και το διαδίκτυο έγινε καθημερινό κομμάτι της καθημερινής μας ζωής. Έτσι, οι χρήστες είχαν αρχίσει να συνειδητοποιούν την σημασία των προσωπικών τους δεδομένων και πόσο ευαίσθητα είναι.

Ο λόγος που οι χρήστες άργησαν να συνειδητοποιήσουν τη σημασία της προστασίας της ιδιωτικής ζωής στο Διαδίκτυο, είναι ότι η πλειοψηφία των χρηστών του Διαδικτύου δεν νοιάζονται για την ιδιωτική τους ζωή αφού δεν πίστευαν πως μπορεί να τύχει κάτι αρνητικό σε αυτούς αφού η ελλιπής ενημέρωση που είχαν σε σύγκριση με την υποβαθμισμένη ανάγκη για παρουσία στο διαδύκτιο είχε σαν κύριο γνώμονα την απομάκρυνση οποιωνδήποτε προκαταλήψεων ή ανησυχιών είχαν οι χρήστες για αυτά.

2.3 Μέσα Κοινωνικής Δικτύωσης και ιδιωτικότητα στο διαδίκτυο

Η έμφυτη τάση του ανθρώπου να επικοινωνεί με τους άλλους καθώς και η ανάγκη του να αλληλεπιδρά με αυτούς καλύφθηκε δια μέσω των μέσων κοινωνικής δικτύωσης. Η κοινωνική δικτύωση λοιπόν ορίζεται ως η επέλαση της γνώσης με τη δημιουργία ζεύξεων με άλλα άτομα που έχουν παρόμοιες ανάγκες, ενδιαφέροντα και ασχολίες. Μέσω της κοινωνικής δικτύωσης κάποιος χρήστης επικοινωνεί με άλλους χρήστες και μπορεί να αλλάξει και να ανταλλάξει ιδέες, απόψεις, εμπειρίες, σκέψεις, συναισθήματα,, καταστάσεις και να εμπλουτίσει τις γνώσεις και τα ενδιαφέροντα που έχει από αυτού του είδους επικοινωνία.

Πρόκειται για μια βασική ανθρώπινη δραστηριότητα, η οποία ακολουθείται σε όλο το φάσμα της ζωής και της ύπαρξης του ανθρώπινου οργανισμού κατά την επέλαση του χρόνου η οποία γινόταν είτε με τη χρήση του τηλεφώνου, ή του ραδιοφώνου, ή των ταχυδρομικών υπηρεσιών και τώρα πλέων με το διαδικτύου το οποίο είναι κάτι που διευρύνει τα όρια της επικοινωνιακής διαδικασίας και βοηθάει να προετοιμάσουμε και να αφομοιώσουμε τις νέες συνιστώσες και συντεταγμένες προϋποθέτει η τεχνολογική εποχή που διανύουμε.

Στη σύγχρονη εποχή η κοινωνική δικτύωση έχει μετατραπεί σε μια δραστηριότητα που γίνεται μόνο διαδικτυακά και η σύνδεσή της με τεχνολογικές υπηρεσίες και λογισμικό δίνει τη δυνατότητα στους ανθρώπους να επικοινωνούν με άλλα άτομα, οπουδήποτε κι αν βρίσκονται ανά το παγκόσμιο σε οποιαδήποτε ώρα της ημέρας και οποιαδήποτε στιγμή. Οι πληροφορίες αυτές μπορούν να ανταλλάσσονται με τη μορφή ηλεκτρονικών μηνυμάτων, φωτογραφιών, βίντεο μέχρι και ηχογραφήσεων.

Τα κοινωνικά δίκτυα ορίστηκαν ως το αποτέλεσμα της άθροισης των προσωπικών επαφών του ατόμου οι οποίες συντελούν στη διατήρηση της κοινωνικής ταυτότητας του χρήστη, συμμετέχουν στις υπηρεσίες που τους παρέχονται, έχουν πρόσβαση στις πληροφορίες και δημιουργούν νέες κοινωνικές επαφές.

Απλοποιούν, βελτιώνουν την ταχύτητα και το εύρος της διάδοσης των πληροφοριών. Προσφέρουν πολλούς και διάφορους τρόπους επικοινωνίας ένας προς έναν, ένας προς πολλούς πολλοί προς πολλούς επιτρέποντας την επικοινωνία να πραγματοποιείται είτε σε πραγματικό χρόνο είτε αναδρομικά με την πάροδο μιας συγκεκριμένης και

καθορισμένης χρονικής περιόδου στο πέρασμα του χρόνου. Ένας χρήστης μπορεί να χρησιμοποιήσει για τη σύνδεση σε Μέσα Κοινωνικής Δικτύωσης έναν υπολογιστή, μια ηλεκτρονική ταμπλέτα, σε μια κινητή συσκευή ακόμα και σε μια έξυπνη τηλεόραση.

Τα μέσα κοινωνικής δικτύωσης λοιπόν ορίζονται ως « μέσο όπου τα άτομα είναι σε θέση να επικοινωνούν με οποιονδήποτε τρόπο θεωρούν κατάλληλο διαδικτυακά σε μία κοινότητα ή μια ομάδα». Αυτό, όμως εξαρτάται από το επίπεδο στο οποίο, οι πληροφορίες είναι δεδομένες και πόσο εκτεθειμένες είναι στην κοινότητα ή ομάδα.

Τα επίπεδα των διαδεδομένων πληροφοριών είναι τρία. Η 1^{η} κατηγορία είναι τα κατασκευάσματα, δηλαδή με ποια εργαλεία μπορούν να γίνουν ορατές οι πληροφορίες και πως μπορούν να ανιχνευθούν. Ποιες πληροφορίες θα γίνουν ορατές στους υπόλοιπους χρήστες και θα είναι προσβάσιμες προς αυτούς επιλέγεται από τον ίδιο τον χρήστη αλλά εξαρτάται και από την μεταξύ τους σύνδεση. Η επόμενη κατηγορία είναι οι φραγμοί οι οποίοι συμβάλλουν στον αποτελεσματικό και ευρύτερο έλεγχο και στην μέγιστη και ποιοτική διαχείριση των πληροφοριών των χρηστών που είναι συνδεδεμένοι με τον χρήστη. Η 3^{η} και τελευταία κατηγορία περιλαμβάνει τα μέσα και τις συνθήκες όπου διατίθενται για να εκφράσει ο χρήστης τα αισθήματα και τις ανάγκες του χωρίς να υπολογίζεται και να είναι απαραίτητη να γίνει αντιληπτή η αξία και το αποτέλεσμα του αισθήματος ή της ανάγκης και η κατανόηση αυτών.

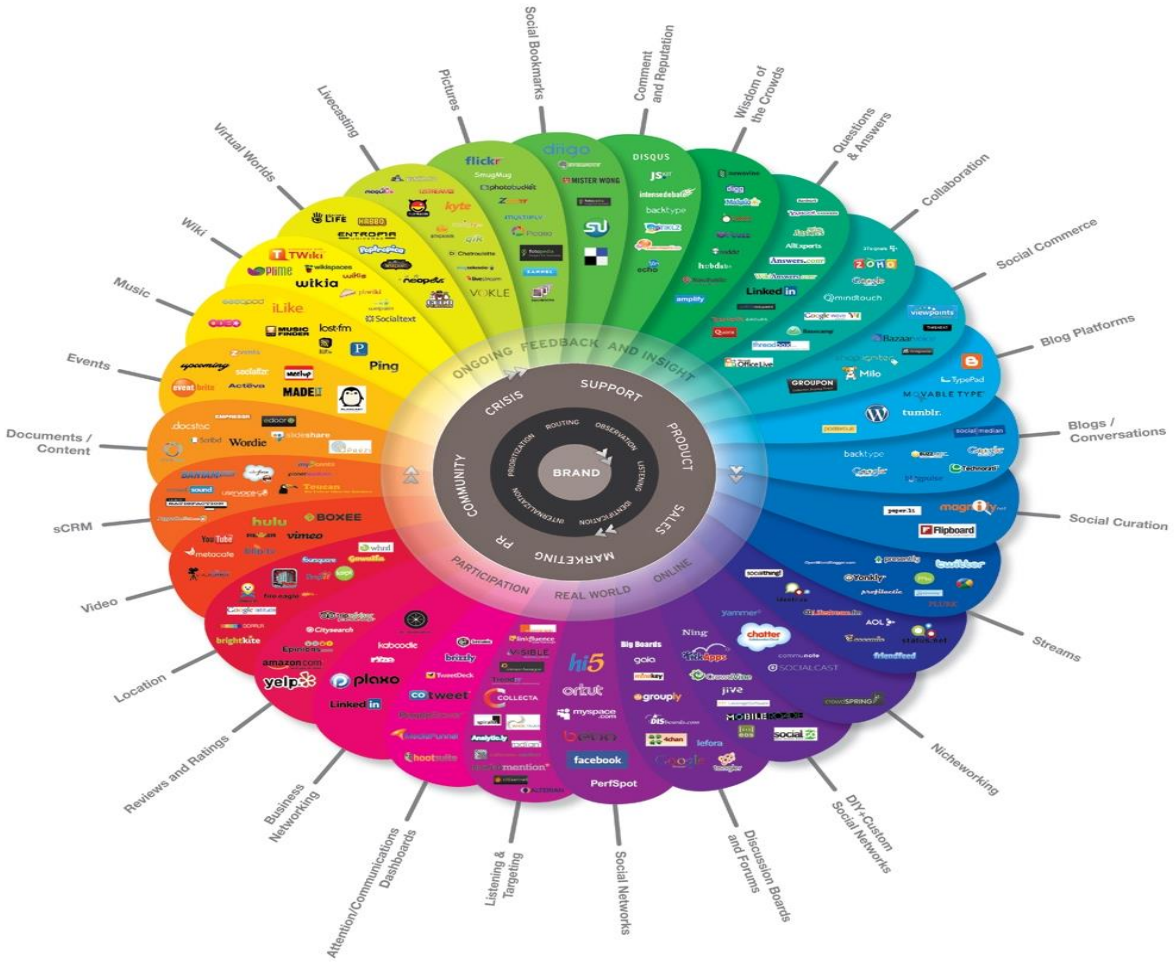
Τα μέσα κοινωνικής δικτύωσης υποστηρίζουν ποικίλες μορφές περιεχομένου, όπως κείμενο, βίντεο, φωτογραφίες, ήχο. Πολλά από αυτά κάνουν χρήση περισσοτέρων του ενός από αυτές τις επιλογές ως προς το περιεχόμενο. Επίσης, επιτρέπουν αλληλεπιδράσεις που από άλλες διαδικτυακές πλατφόρμες μέσω e-mail ή μηνυμάτων στο προσωπικό ταχυδρομείο και άλλων μορφών εισαγωγής ροών και πληροφοριών. «Χαρακτηρίζονται από διαφορετικά επίπεδα συμβολής των χρηστών οι οποίοι μπορούν να δημιουργήσουν, να σχολιάσουν ή να παρακολουθήσουν τα κοινωνικά Δίκτυα.» Οι υπηρεσίες και τα μέσα κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες να διαμορφώσουν ένα προσωπικό προφίλ ανάλογα με τις ανάγκες και τα θέλω τους.

Μία σελίδα κοινωνικής δικτύωσης είναι ελεύθερη και προσβάσιμη από όλους τους χρήστες του Internet και στόχο έχει να προσελκύσει άτομα ή εταιρίες που ενδιαφέρονται να διαφημίσουν είτε προϊόντα, είτε κάποια υπηρεσία τους. Ο όρος

κοινωνικά δίκτυα αυτή την εποχή έχει ταυτιστεί με το Facebook (σύμφωνα με μια πρόσφατη έρευνα που έγινε επί κυπριακού εδάφους το 95% απάντησε ότι έχει δημιουργήσει λογαριασμό και τον χρησιμοποιεί στο εν λόγω μέσο κοινωνικής δικτύωσης).

Τα Μ.Κ.Δ παρέχουν στον χρήστη πολλές επιλογές, ως προς την ασφάλεια και την ιδιωτικότητα του και την επιλογή των χρηστών που θα μπορούν να επικοινωνήσουν μαζί του, τι πληροφορίες θέλουν να μοιραστούν αλλά και τι περιεχόμενο θέλουν να βλέπουν στα δίκτυα αυτά.

Σκοπό έχουν να « δημιουργήσουν κοινότητες ανθρώπων στο διαδίκτυο που έχουν κοινά ενδιαφέροντα και δραστηριότητες. Το διαδίκτυο είναι ένας κοινός τόπος όπου λειτουργούν οι κοινωνικές δικτυώσεις και τα άτομα που είναι εγγεγραμμένα στις κοινότητες μπορούν να επικοινωνούν με πολλούς τρόπους και να ανταλλάσσουν απόψεις.»

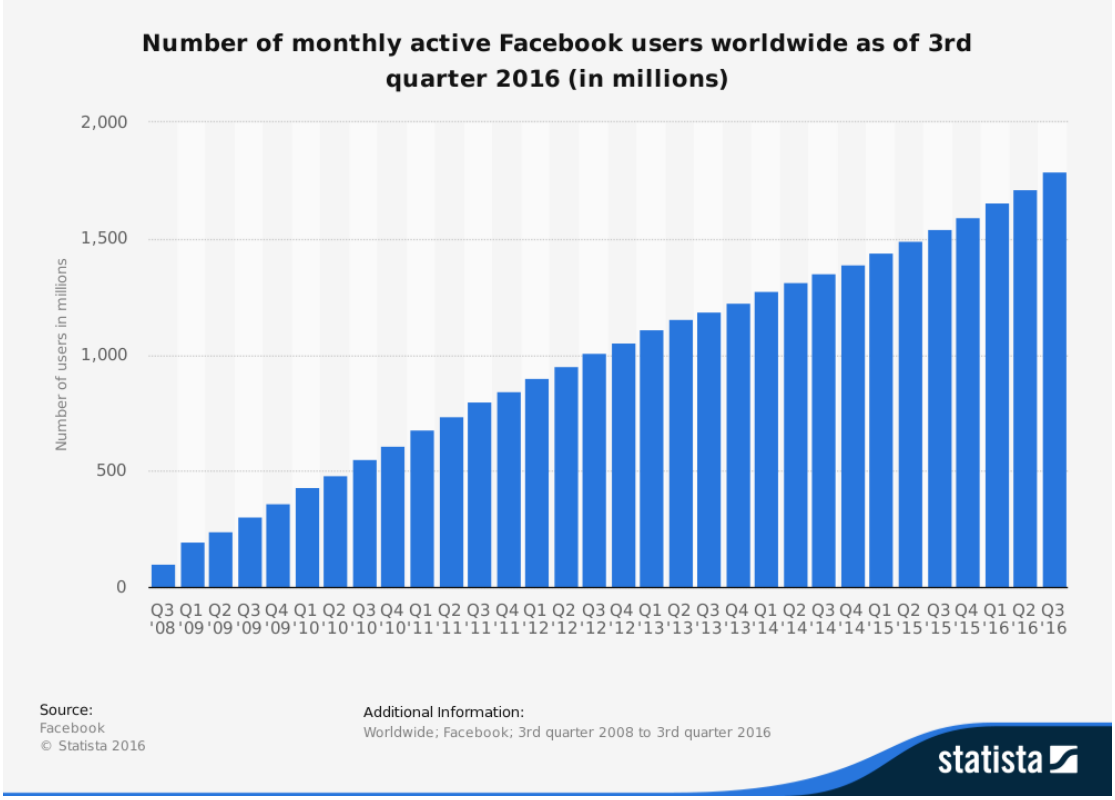


Εικόνα 1: Διάγραμμα Μέσων Κοινωνικής Δικτύωσης

2.3.1 Facebook

Το Facebook αποτελεί σήμερα το πιο φημισμένο, διαδεδομένο και επιτυχημένο μέσο κοινωνικής δικτύωσης που έχει υπάρξει ποτέ. Δημιουργήθηκε για πρώτη φορά στις 04 Φεβρουαρίου 2004 και ο ιδρυτής του είναι ο Μαρκ Ζάκερμπεργκ από τις Η.Π.Α.

Στην αρχή ήταν ένα τοπικό μέσο κοινωνικής δικτύωσης και συγκεκριμένα λειτούργησε αρχικά στο Πανεπιστήμιο Χάρβαρντ όπου οι φοιτητές μπορούσαν να δουν και να γνωρίσουν άλλους συμφοιτητές τους από το ίδιο το πανεπιστήμιο. Σήμερα υπολογίζεται ότι υπάρχουν πάνω από 1,7 δις εγγεγραμμένοι χρήστες σ' αυτό και τα κέρδη του είναι περισσότερα από 4 δις.



Εικόνα 2: Καταμέτρηση ανά μήνα των χρηστών του FB

Ο χρήστης μπορεί να δημιουργήσει ένα δικό του προσωπικό προφίλ στο οποίο μπορεί να ανεβάζει και να το ενημερώνει με τις δικές του πληροφορίες, τις φωτογραφίες και βίντεο και ακόμα να ενημερώνει για το που βρίσκετε την συγκεκριμένη χρονική στιγμή. Το digital marketing και η αυξημένη επιθυμία του ανθρώπου να προβαίνουν σε αγορές διαδικτυακά έχουν αναγάγει το Facebook στην μεγαλύτερη πλατφόρμα διαφημιστικών και ενημερωτικών ενημερώσεων αφού ο οποιοσδήποτε μπορεί να διαφημίσει την επιχείρηση του χωρίς καθόλου έξοδα και να πουλήσει έξυπνα το αντικείμενο στο οποίο ειδικεύεται. Πολλές μικρές επιχειρήσεις επιβίωσαν μέσα από την οικονομική κρίση με την βοήθεια του FB. Το μόνο που έκαναν ήταν η δημιουργία ηλεκτρονικού καταστήματος μέσω του FB όπου ο υποψήφιος καταναλωτής βλέπει τα προϊόντα του εκάστοτε καταστήματος. Αν του αρέσει κάτι, το παραγγέλει και μετά ο καταστηματάρχης το αποστέλει σπίτι του εύκολα και γρήγορα χωρίς την παραμικρή ταλαιπωρία. Πολλοί χρήστες έχουν δικές τους προσωπικές σελίδες που ενημερώνουν καθημερινά και αυτές έχουν ενημερωτικό είτε διαφημιστικό είτε ψυχαγωγικό σκοπό.

Ένας χρήστης του facebook έχει τη δυνατότητα αποστολής αιτημάτων φιλίας σε άλλους χρήστες και αυτοί με τη σειρά μπορούν να επιλέξουν αν θα τον δεχτούν ή όχι. Επίσης, μπορεί να δέχεται εισερχόμενα μηνύματα μέσω του ηλεκτρονικού του ταχυδρομείου ή να δέχεται άμεσα μηνύματα μέσω της συνομιλίας όπως επίσης και να πραγματοποιεί κλήσεις και βιντεοκλήσεις.

Τελευταία μας δίνεται ακόμα και η δυνατότητα ομαδικής κλήσης μέσω της εφαρμογής του FB το messenger με την οποία μπορούμε να μιλήσουμε σε όλους τους φίλους μας που έχουμε στη συγκεκριμένη ομάδα. Πριν λίγες μέρες λάνσαραν μια ιδέα με την οποία ο χρήστης θα μπορεί να αγοράζει απευθείας από την σελίδα προϊόντα κάτι που θα μοιάζει με το Ebay και το Amazon. Οι λειτουργίες τις οποίες χρησιμοποιούν περισσότερο οι χρήστες του Facebook και είναι οι πιο διαδεδομένες είναι το like, το share και το comment.

Για τη σωστή και ομαλή χρήση του facebook, υπάρχει ένα σύνολο όρων και υποχρεώσεων χρήσης της ιστοσελίδας το οποίο είναι προσαρμοσμένο ανάλογα με το νομικό πλαίσιο της κάθε χώρας με την εξαίρεση, όμως ότι σε όποια διαφωνία των όρων με αυτούς της χώρας επικρατεί αυτό της χώρας της έδρας του Facebook. Το Facebook θεωρείται ως ένα ευνοϊκό εκπαιδευτικό εργαλείο, λόγω της δομής και

των διαφόρων υπηρεσιών κοινής ωφελείας. Μπορεί να χρησιμοποιηθεί για ανταλλαγή σημειώσεων μεταξύ των μαθητών/φοιτητών ή ακόμα και άμεση επικοινωνία με τον εκπαιδευτικό για επίλυση απορίων.

Η χρήση του Facebook για επικοινωνία συνίστανται σε δραστηριότητες, όπως η δυνατότητα επικοινωνίας μεταξύ των χρηστών από οποιοδήποτε μέρος κι αν βρίσκονται, διευκολύνοντας την συζήτηση, χωρίς το παραμικρό κόστος. Οι άνθρωποι μπορούν να ανταλλάξουν ιδέες, να ανταλλάσσουν πληροφορίες και να συνεργάζονται με όποιους έχουν κοινά συμφέροντα, τις ιδέες και τις ανάγκες.

2.3.2 Instagram

Το Instagram είναι μία υπηρεσία κοινωνικής δικτύωσης, η οποία δημιουργήθηκε το 2010 από τους Κέβιν Σίστρομ και Μάικ Κρίγκερ. Το όνομα της προέρχεται από τον συνδυασμό της λέξης Instant και telegram.

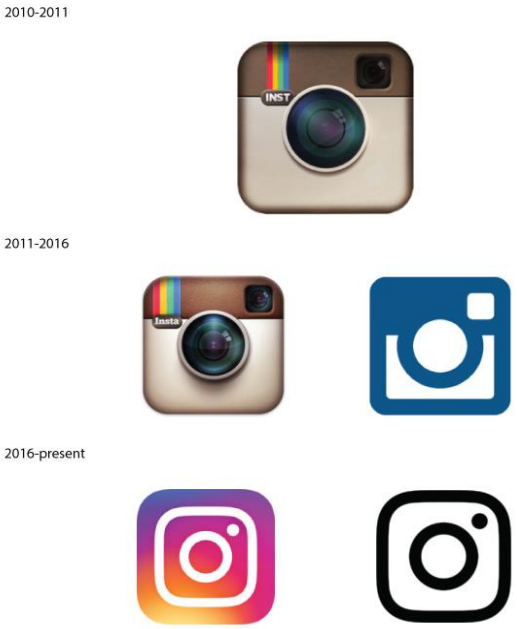
Ασχολείται αποκλειστικά με τη λήψη, επεξεργασία και τη δημοσίευση φωτογραφιών και βίντεο ενώ περιέχει και προσωπικό χώρο για ανταλλαγή μηνυμάτων μεταξύ των χρηστών. Φημίζεται για την ειδικότητα που έχει στις φωτογραφίες μέσω των πολλών φίλτρων που διατίθενται για την επεξεργασία της φωτογραφίας,. Από το 2012 το Instagram πουλήθηκε στο facebook έναντι 1 δισεκατομμυρίου δολαρίων.

Στο Instagram μπορεί ο κάθε χρήστης να δημιουργήσει το δικό του προφίλ στο οποίο μπορεί να ανεβάσει εικόνα για το προφίλ του. Κάθε νέο προφίλ, αρχικά, είναι δημόσιο και κάθε χρήστης μπορεί να έχει πρόσβαση στις εικόνες και τα βίντεο, αυτό όμως μπορεί να αλλάξει από τις ρυθμίσεις. Πιο συγκεκριμένα, ο χρήστης επιλέγει ποιοι θα μπορούν να βλέπουν τις πληροφορίες που αυτός ανεβάζει.

Στο Instagram υπάρχουν οι followers κάτι αντίστοιχο με τους friends στο facebook, δηλαδή κάθε χρήστης ακολουθεί τους χρήστες του οποίους επιθυμεί να βλέπει το υλικό που ανεβάζουν. Ακολουθώντας χρήστες, οι φωτογραφίες και τα βίντεο τους προβάλλονται μέσω της αρχικής σελίδας του χρήστη. Κάθε χρήστης έχει τη δυνατότητα να χρησιμοποιήσει τη λειτουργία της κάμερας της εφαρμογής, για να τραβήξει μια φωτογραφία ή ένα βίντεο και στη συνέχεια τα επεξεργαστεί μέσω των

διαφόρων φίλτρων και εργαλείων της εφαρμογής. Το ανέβασμα φωτογραφιών και βίντεο είναι εφικτό μονάχα μέσω των κινητών συσκευών και όχι μέσω υπολογιστή. Από τον υπολογιστή μπορεί κανείς να αποκτήσει πρόσβαση μόνο σε ορισμένες λειτουργίες της εφαρμογής όπως την προβολή φωτογραφιών, να ακολουθήσει φίλους του και να δηλώσει ποιες φωτογραφίες του αρέσουν.

Πρόσφατα το Instagram έδωσε την δυνατότητα στους χρήστες που το χρησιμοποιούν να μπορούν να ανεβάσουν την ιστορία τους είτε αυτό είναι φωτογραφία είτε βίντεο άλλα προβάλλεται μέσα σε εννέα δευτερόλεπτα και είναι διαθέσιμη μόνο για μια ήμερα κάτι παρόμοιο με το σκεπτικό του Snapchat. Σήμερα υπολογίζεται πως την εφαρμογή χρησιμοποιούν πέραν των 200 εκ. χρηστών ανά τον κόσμο.



Εικόνα 3: Τα logo του Instagram μέχρι και σήμερα

2.3.3 YouTube

Το YouTube είναι το πιο δημοφιλή κοινωνικό μέσο αναπαραγωγής και διάδοσης βίντεο, αφού, κάθε μήνα το επισκέπτονται πάνω από 1 δισεκατομμύριο ενεργοί χρήστες και ανήκει στη Google. Ιδρύθηκε από τους Τσαντ Χάρλεϊ, Στιβ Τσεν, Τζαουέντ Καρίμ στην Καλιφόρνια των Η.Π.Α.

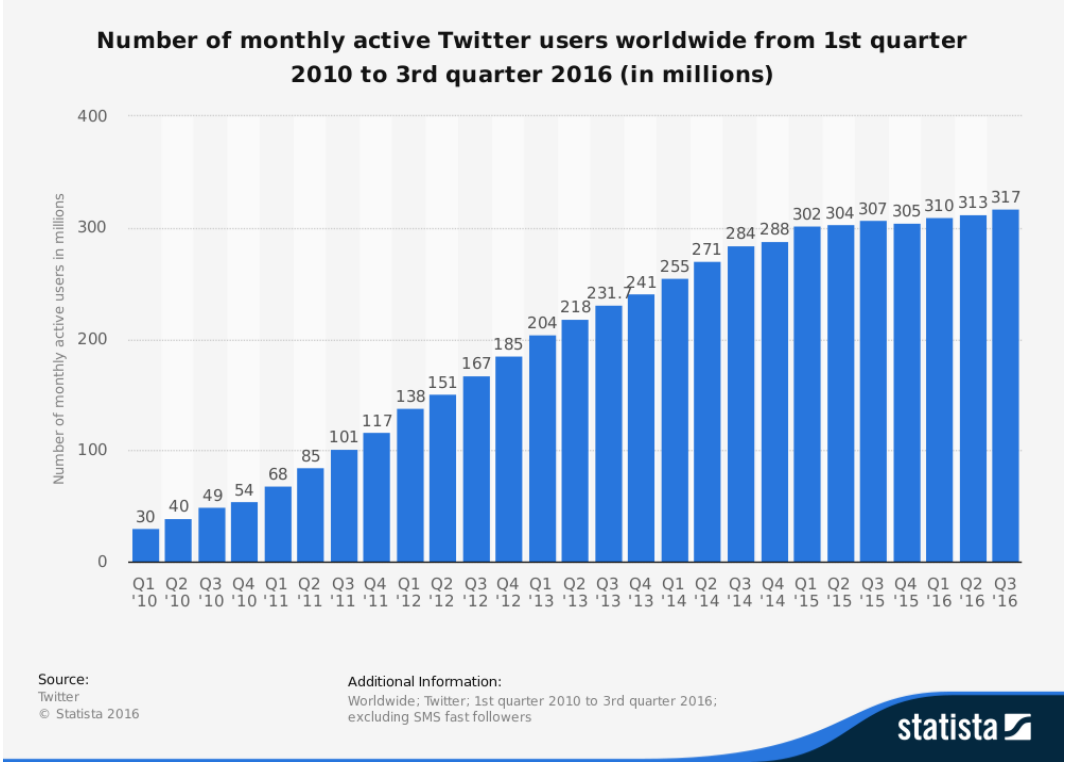
Για πολλούς το Youtube θεωρείται κοινωνικό δίκτυο, αφού μπορούν να έχουν προφίλ, χωρίς αυτό να είναι απαραίτητο και να αλληλεπιδρούν μεταξύ τους κάνοντας σχόλια ή να κάνουν εγγραφές σε κανάλια άλλων χρηστών ώστε να ενημερώνονται για τα καινούρια βίντεο που ανεβαίνουν από το κανάλι αυτού που τους ενδιαφέρει. Επομένως, οι χρήστες του Youtube εκτός από δικό τους προφίλ μπορούν να δημιουργήσουν και δικό τους κανάλι στο οποίο μπορούν να ανεβάσουν δικά τους βίντεο. Κάθε βίντεο περιέχει λειτουργίες όπως «Μου αρέσει» και «Δε μου αρέσει» ο σύνδεσμος του βίντεο αν ο χρήστης θέλει να το μοιραστεί με άλλους.

Εικόνα 4 : Ο "2J" είναι ο No1 «Youtuber» σε Κύπρο και Ελλάδα με περισσότερους από 700.000 χρήστες να ακολουθούν το κανάλι του και με 170 εκ προβολές στα βίντεο του

2.3.4 Twitter

Το Twitter δημιουργήθηκε από τους Jack Dorsey, Evan Williams, Biz Stone, και Noah Glass το Μάρτιο του 2006. Αυτό που χαρακτηρίζει το Twitter είναι ότι ο χρήστης έχει την δυνατότητα να ανανεώσει το στάτους του μέχρι συγκεκριμένο αριθμό χαρακτήρων. Κυριότερες λειτουργίες αυτού του μέσου δικτύωσης είναι το retweet, να δηλώσει ο χρήστης αν του αρέσει κάποιο tweet και να απαντά στα διάφορα tweets που τον ενδιαφέρουν. Από το Μάιο του 2015, το Twitter έχει περισσότερους από 500 εκατομμύρια χρήστες, από τους οποίους πάνω από 332 εκατομμύρια είναι ενεργοί.

Όσον αφορά το πώς πήρε το όνομα του το εν λόγω σαιτ, αρχικά το ονόμασαν Twitch το οποίο σημαίνει συσπώμαι, το οποίο προήλθε από την δόνηση του κινητού τηλεφώνου. Αναζητώντας όμως περισσότερες επιλογές για την ονομασία του σαιτ κατέληξαν στην λέξη Twitter, η οποία έχει ως ορισμό της, μια μικρή έκρηξη επουσιωδών πληροφοριών.



Εικόνα 5: Η μηνιαία καταμέτρηση των ενεργών χρηστών του Twitter

Το Twitter λοιπόν είναι ένα κοινωνικό μέσο δικτύωσης το οποίο δίνει τη δυνατότητα στους χρήστες του να γράφουν σύντομα μηνύματα και να διαβάζουν τα μηνύματα άλλων χρηστών της υπηρεσίας, τα λεγόμενα tweets.

2.3.5 LinkedIn

Για το LinkedIn οι περισσότεροι πιστεύουν πως είναι σχετικά πρόσφατο αλλά δημιουργήθηκε το 2002 από τον Ρέιντ Χόφμαν στις Η.Π.Α. Σήμερα αποτελεί το νούμερο ένα επαγγελματικής κοινωνικής δικτύωσης και δίνει την δυνατότητα στα μέλη του να δημιουργήσουν το επαγγελματικό τους προφίλ, να αναζητήσουν εργασία και να δικτυωθούν περισσότερο με άτομα του ιδίου τομέα που δραστηριοποιούνται. Ο χρήστης έχει τη δυνατότητα λεπτομερούς παρουσίασης της εργασιακής εμπειρίας του και ανάλυση του εκπαιδευτικού υπόβαθρου. Επίσης παρέχεται η δυνατότητα παροχής συστάσεων από συναδέλφους και συνεργάτες και άλλες δυνατότητες όπως η δημοσίευση και ο διαμοιρασμός αναρτήσεων, παρουσιάσεων κ.α.

Μια πολύ καλή επιλογή για δημιουργία βιογραφικού είναι η εξαγωγή σε PDF μορφή των στοιχείων των οποίων έχει εισάγει ο χρήστης στο LinkedIn. Έχει πάρα πολλές επιλογές που βοηθούν και καθοδηγούν τον χρήστη να έχει μια σωστή δομή και εμφάνιση στο προφίλ του. Κατά την προσωπική μου άποψη αποτελεί το πιο χρήσιμο μέσο κοινωνικής δικτύωσης που υπάρχει σήμερα αφού η προσφορά του είναι παράπλευρη. Αρχές Δεκεμβρίου του 2016 ανακοινώθηκε η εξαγορά του LinkedIn από την Microsoft έναντι του ποσού των 26,2 δις δολαρίων με διάφορους προγραμματισμούς και ενέργειες που έχουν κατά νου να είναι προ των πυλών.

2.3.6 Snapchat

Το Snapchat από όταν δημιουργήθηκε το Απρίλιο του 2011 από τους Evan Spiegel, Bobby Murphy, Reggie Brown, εξαπλώθηκε σε όλα τα μήκη και τα πλάτη της γης έγινε γρήγορα το μέσο κοινωνικής δικτύωσης της νεολαίας. Το χρησιμοποιούν επί το πλείστον νεαρά άτομα τα οποία ανταλλάζουν φωτογραφίες και βίντεο συνοδευόμενα με διάφορα φίλτρα και άλλα αντικείμενα. Θυμίζει λίγο το Instagram αφού σαν βάση του έχει τις φωτογραφίες και τα βίντεο αλλά είναι πρωτότυπο για αυτό και γρήγορα

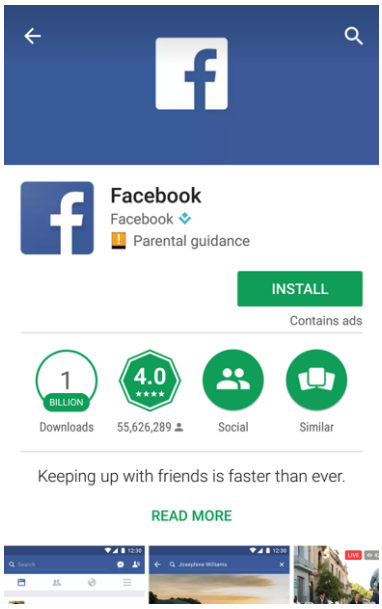
αγαπήθηκε από τους νέους.

Σήμερα υπολογίζεται ότι στο Snapchat γίνονται 7 δις προβολές βίντεο ανά μέρα και μόνο από το Google Store έχουν εγκαταστήσει την εφαρμογή 10 εκ χρήστες.

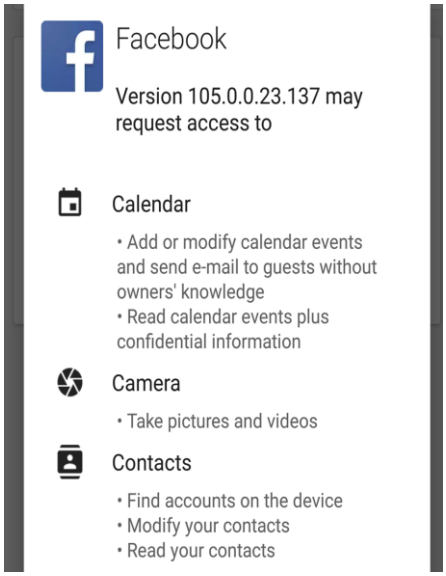
2.4 Κοινωνικά Δίκτυα και Διαρροές Προσωπικών Δεδομένων

Η αποκάλυψη προσωπικών πληροφοριών σε online υπηρεσίες κοινωνικής δικτύωσης είναι ένα δίκοπο μαχαίρι. Ωστόσο, η διαρροή των προσωπικών δεδομένων, ειδικά η ταυτότητα του ατόμου, μπορεί να προκαλέσει κακόβουλες επιθέσεις τόσο στον πραγματικό κόσμο στον και στο διαδίκτυο όπως η ανεπιθύμητη παρακολούθηση, συκοφαντική δυσφήμηση, και εξατομικευμένες αυτόκλητες επικοινωνίες. Ο σημερινός χρήστης εν αγνοία του εκθέτει πάρα πολλά προσωπικά του δεδομένα που αν πέσουν στην αντίληψη κακόβουλων χρηστών θα χρησιμοποιηθούν για τους λάθους σκοπούς.

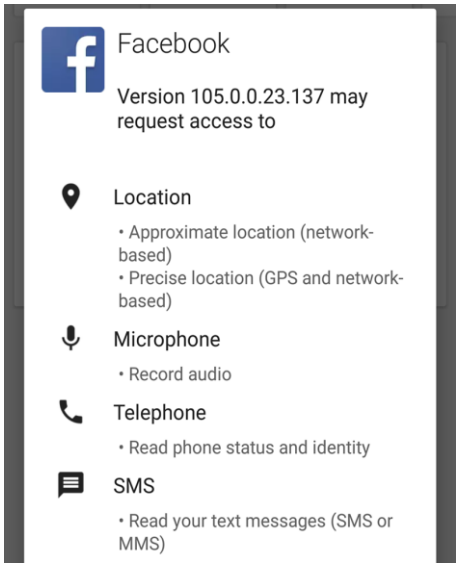
Ποίος από εμάς δεν έχει κατεβάσει εφαρμογή στο smartphone από το Play Store σε λειτουργικό Android. Υπάρχουν πολλές χρήσιμες εφαρμογές ή παιχνίδια που μπορούμε να περάσουμε τον χρόνο μας. Αυτή είναι η θετική πλευρά. Η αρνητική είναι όταν ο χρήστης αρχίζει να κατεβάζει την εφαρμογή αυτή τον ρωτάει αν θέλει να έχει πρόσβαση σε συγκεκριμένες λειτουργίες του τηλεφώνου του. Μια εφαρμογή με πάρα πολλές αιτήσεις για πρόσβαση σε αυτές τις λειτουργίες του smartphone, είναι η εφαρμογή του FB και στις πιο κάτω φωτογραφίες θα αναφέρουμε περιληπτικά τι μπορεί να κάνει.



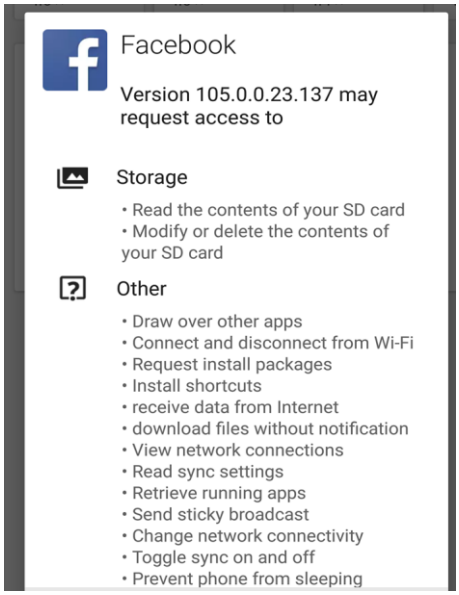
Εικόνα 6: Μέχρι και αυτή την στιγμή περισσότεροι από 55 εκ χρήστες έχουν κατεβάσει την εφαρμογή του FB στο smartphone ή table τους



Εικόνα 7: Το FB ζητά να έχει πρόσβαση στο ημερολόγιο, στην φωτογραφική του smartphone και στις επαφές του τηλεφώνου



Εικόνα 8: Το FB ζητά πρόσβαση στη τοποθεσία, στο μικρόφωνο του smartphone, στην λειτουργία τηλεφώνου της συσκευής του smartphone και στα προσωπικά μηνύματα



Εικόνα 9: Το FB ζητά πρόσβαση στην μνήμη του τηλεφώνου μας αλλά και σε άλλες λειτουργίες όπως φαίνεται δίπλα

Όπως βλέπουμε και πιο πάνω φτάνουμε στο συμπέρασμα ότι το FB έχει πρόσβαση σχεδόν σε ολόκληρα τα προσωπικά μας δεδομένα. Ευτυχώς για εμάς μας δίνεται η δυνατότητα να αφαιρέσουμε μετά τις άδειες για τις οποίες πήρε το FB κατά την διάρκεια της λήψης του. Όμως οι περισσότεροι αγνοούν την ύπαρξη αυτής της δυνατότητας και έτσι επιτρέπουν στο FB να διαχειρίζεται τα προσωπικά τους δεδομένα εν αγνοία τους.

2.4.1 Spamming

Τα spam mail αποτελούν πολύ σημαντικό πρόβλημα στην εποχή αυτή. Είναι πραγματικά μια επιχειρηματική δραστηριότητα με την οποία οι spammers στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου με πληροφορίες για τα προϊόντα βασιζόμενοι σε μαζικές λίστες διευθύνσεων ηλεκτρονικού ταχυδρομείου. Για την προστασία των χρηστών από το spamming, η ακαδημαϊκής κοινότητα και η βιομηχανία έχουν αναπτύξει μια σειρά από anti-spam μηχανισμούς και μεθόδους.

Μπορεί να παραβιαστεί ακόμα και μια καλά διαμορφωμένη διεύθυνση ηλεκτρονικού ταχυδρομείου όπου μπορούν να χρησιμοποιήσουν για την αποστολή spam mail και αν έχει σταλεί από έναν από τους φίλους του χρήστη. Με αυτόν τον τρόπο, το mail μπορεί να παρακάμψει το φίλτρο και να παραδοθεί στο ανυποψίαστο θύμα..

Οι spammers μπορούν να κάνουν χρήση των πραγματικών ονομάτων με δύο τρόπους. Μπορούν να χρησιμοποιήσουν το πραγματικό όνομα του παραλήπτη στο περιεχόμενο της αλληλογραφίας του και επίσης να δημιουργήσουν μηνύματα spam που να μοιάζουν σαν να έχουν σταλεί από ένα φίλο του χρήστη, χρησιμοποιώντας το πραγματικό όνομα του χρήστη. Ο χρήστης δύσκολα μπορεί να επαληθεύσει την αυθεντικότητα του μηνύματος ηλεκτρονικού ταχυδρομείου και αν πατήσει τον σύνδεσμο θα πέσει θύμα απάτης αφού το μήνυμα δεν θα είναι από τον πραγματικό του φίλο αλλά από ένα κακόβουλο χρήστη.

2.4.2 Phishing

Παρόμοιες δυσκολίες υπάρχουν και σε σχέση με την ανίχνευση του phishing. Στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου, τα οποία περιέχουν μια σύνδεση με μία ψεύτικη σελίδα, με σκοπό την απόκτηση ευαίσθητων πληροφοριών των ανθρώπων όπως ένας τραπεζικός λογαριασμός, ένα όνομα χρήστη ή έστω και μια διεύθυνση email. Εταιρείες που αποσκοπούν στην ανίχνευση του phishing, είναι το eBay, η Amazon και η PayPal που σε συνεργασία με το δικό τους τμήμα IT προσπαθούν να καταπολεμήσουν το phishing. Κοινοί κανόνες περιλαμβάνουν "τον έλεγχο για το αν το e-mail περιλαμβάνει το πραγματικό σας όνομα, γιατί οι phishers δεν έχουν διαθέσιμα προσωπικά δεδομένα. Ωστόσο, η υπόθεση ότι οι phishers δεν έχουν προσωπικές πληροφορίες ενδέχεται να είναι λανθασμένο δεδομένου ότι η αυτό-αποκάλυψη γίνεται όλο και πιο συχνή στα μέσα κοινωνικής δικτύωσης. Το ακούσιο πρόβλημα διαρροής του ονόματος θα επιδεινώσει περαιτέρω το πρόβλημα, καθώς θα είναι πιο δύσκολο για τους χρήστες και τους μηχανισμούς ανίχνευσης phishing να επαληθεύσουν την αυθεντικότητα μιας ιστοσελίδας.

2.4.3 Spoofing

Ένα σημαντικό πρόβλημα στις μέρες μας είναι το spoofing η λεγόμενη πλαστογράφηση. Είναι ένας τύπος απάτης όπου ο εισβολέας προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα ή στις πληροφορίες του χρήστη προσποιούμενος ότι είναι ο χρήστης. Ο κύριος σκοπός είναι να προσπαθήσουν να ξεγελάσουν τον χρήστη έτσι ώστε να εκμυστηρευτεί ευαίσθητες πληροφορίες, προκειμένου να αποκτήσουν πρόσβαση σε τραπεζικούς λογαριασμούς, ή το σύστημα του υπολογιστή του ή ακόμα και να κλέψουν προσωπικές πληροφορίες όπως κωδικούς πρόσβασης ή διευθύνσεις email. Υπάρχουν διάφορα είδη πλαστογράφησης συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου, αναγνώριση κλήσης, και κακόβουλες επιθέσεις στο προσωπικό URL.

Ένα συχνό φαινόμενο είναι όταν βρίσκουμε στο προσωπικό μας mail διάφορα παραπλανητικά μηνύματα τα οποία στάλθηκαν από κακόβουλους χρήστες και μας παρουσιάζονται σαν να είναι από τράπεζες, εταιρίες πωλήσεις αγαθών ή και από κοινωνικά δίκτυα. Σκοπό έχουν να πείσουν τον χρήστη ότι είναι αληθινά και αυτός να

προχωρήσει στον σύνδεσμο που του αναφέρεται. Αν ο χρήστης προχωρήσει ζητάει στοιχεία πιστωτικής κάρτας και σε περίπτωση που ο χρήστης τα εισάγει θα έχει πέσει θύμα απάτης.

Εικόνα 10: Παράδειγμα απάτης με την χρήση spoofing

2.4.4 Sniffing

Το sniffing λόγω της ραγδαίας αύξησης των δημόσιων Wi-Fi spots που υπάρχουν είναι ο ανερχόμενος τρόπος υποκλοπής μη αποκρυπτογραφημένων δεδομένων όπως κωδικούς πρόσβασης του ανυποψίαστου θύματος από τον κακόβουλο χρήστη. Οι τελευταίοι εκμεταλλεύονται το γεγονός ότι χρησιμοποιείται νόμιμα από τους διαχειριστές συστημάτων για να ελέγξουν την ποιότητα και να διορθώσουν την κίνηση του δικτύου, ελέγχουν και παρακολουθούν τα πακέτα που διακινούνται μέσα στο δίκτυο. Ο χρήστης μπορεί να προστατευθεί με το κατάλληλο λογισμικό αφού έτσι θα έχει ανιχνεύσει αν η κίνηση του δικτύου έχει υποκλαπεί από κάποιον κακόβουλο χρήστη. Τα δεδομένα πρέπει να είναι κρυπτογραφημένα με SSL έτσι ώστε να μην μπορείς κανείς να σας υποκλέψει στοιχεία αφού με αυτού του είδους κρυπτογράφηση θα είστε ασφαλισμένοι. Οποιαδήποτε προσπάθεια να τροποποιήσουν ή να λάβουν δεδομένα θα είναι αποτυχημένη επειδή λόγω των κρυπτογραφημένων δεδομένων θα αντιμετωπίσουν σφάλμα με κάτι που θα ήταν εμφανής αν οι πληροφορίες αποκρυπτογραφούνταν από την άλλη πλευρά.

ΚΕΦΑΛΑΙΟ 3ο – ΜΕΘΟΔΟΙ ΑΝΙΧΝΕΥΣΗΣ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

3.1 Ορισμός παραβίασης προσωπικών δεδομένων

Ως ασφάλεια πληροφοριών ορίζεται μια σειρά «από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας των πληροφοριών τα οποία μπορούν να δημιουργήσουν πρόβλημα στην επιχειρησιακή λειτουργία ενός οργανισμού και να απειλήσουν την ασφάλεια των πληροφοριών, δηλαδή την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών που ο οργανισμός επεξεργάζεται».

Ως παραβίαση προσωπικών δεδομένων ορίζεται η «παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλο τρόπο σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.»

Η υποκλοπή στοιχείων ταυτότητας είναι η κατάχρηση προσωπικών δεδομένων και η κατακρεούργηση της προσωπικής διαδικτυακής ελευθερίας του ατόμου με σκοπό την υποβάθμιση και εκμετάλλευση κάποιου προσώπου χωρίς τη συγκατάθεσή του. Εκτός από τις βασικές πληροφορίες όπως το όνομα και τη διεύθυνση, ο υποκλοπέας τρίτων στοιχείων αναζητά αριθμούς πιστωτικών καρτών ή και αριθμούς τραπεζικών λογαριασμών, πιστοποιητικά γέννησης ή διαβατήρια.

Έτσι η πληροφορία αυτή επιτρέπει στους υποκλοπείς στοιχείων ταυτότητας να διαπράξουν πολλές μορφές απάτης όπως να υιοθετήσουν τρίτους χρηματοοικονομικούς λογαριασμούς, να ανοίξουν νέους λογαριασμούς στο όνομα του θύματος εν αγνοία του, να εκτρέπουν μηνύματα ηλεκτρονικού ταχυδρομείου στη διεύθυνση του ανυποψίαστου θύματος αλλά και σημαντικά μηνύματα στην διεύθυνση τους, να υποβάλλουν αιτήσεις για λήψη δανείων, πιστωτικών καρτών κ.ά.

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η ανάγκη για εκχώρηση των αξιών και των αναγκών της πληροφορικής στην καθημερινή μας ζωή, η εμβάθυνση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας άλλαξαν εκ βάθος το περιβάλλον χρήσης της προσωπικής πληροφορίας, αλλά και θέματα που είχαν να κάνουν με την προστασία και ανάγονταν σε θέματα πρώτου βαθμού με κύριο γνώμονα την προστασία της.

Σε αυτό το θεσμικό αντίβαρο διαμορφώνεται η ανάγκη για προστασία προσωπικών δεδομένων. Σε αντίθεση με την ιδιωτικότητα όπου αναλύσαμε πριν, η προστασία προσωπικών δεδομένων είναι θέμα άκρως σημαντικό αφού είναι στενά συνδεδεμένο με την τεχνολογική εξέλιξη το τεχνολογικό βήμα του ανθρώπου, καθώς κρίνεται πως οι προϋπάρχουσες επιλογές δεν προσφέρουν και δεν εμπνέουν αρκετή προστασία προς τους κινδύνους και τις επιθέσεις στις οποίες ο χρήστης είναι ευάλωτος.

Λαμβάνοντας ιδιαίτερα σοβαρά τις δυσλειτουργίες και τις επιπτώσεις της ηλεκτρονικής κατεργασίας της online πληροφορίας, η προστασία προσωπικών δεδομένων δεν αφορά μόνο στη ρύθμιση και προστασία της πληροφορίας που θεωρείται από τον χρήστη ως ιδιωτική και άκρως εμπιστευτική αλλά κυρίως γιατί ο χρήστης επιθυμεί διακαώς τον τερματισμό και τον περιορισμό της χρήσης των προσωπικών του δεδομένων.

Κατά τον τρόπο αυτό ή έκταση και η μέθοδος διαμόρφωσης των στελεχών μας επιβάλλει να αναλύσουμε πολύ προσεκτικά και συνειδητά τις καλύτερες δυνατές συνθήκες για επιτάχυνση των διαδικασιών έτσι ώστε η προστασία των προσωπικών δεδομένων να καταστεί το ο κύριος πυλώνας της υγιείς πληροφορικής.

Η αυτούσια διαδικτυακή πληροφορία χαρακτηρίζει κάθε πληροφορία και κάθε δεδομένο που πρόσκειται σε κάποιον ανθρώπινο οργανισμό και το γεγονός ότι η ιδιωτικότητα και η προστασία των προσωπικών δεδομένων μπάζει από παντού, μας δίνει την τροφή για σκέψη για να δημιουργήσουμε τεχνολογίες και τεχνικές ενίσχυσης της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων των χρηστών.

3.2 Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Η αρχική προσπάθεια ενίσχυσης της ιδιωτικότητας στο διαδίκτυο αφορά στην εμφάνιση Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας οι οποίες στηρίζονται την ιδέα ότι η τεχνολογία δύναται να ενισχύσει την ιδιωτικότητα και όχι να την καταπατήσει. Η διεθνής κοινότητα με μια σειρά τεχνολογιών ενίσχυσης προσπάθησε να ενισχύσει την ιδιωτικότητα. Με την πάροδο του χρόνου αυτές οι τεχνολογίες σημειώνουν σημαντική πρόοδο και αναλυτές και ερευνητές ψάχνουν τρόπου μες τους οποίους θα προστατευθεί περισσότερο η ιδιωτικότητα του χρήστη. Κάποιες από αυτές τις τεχνολογίες θα τις αναφέρουμε πιο κάτω.

3.2.1 Enhanced privacy ID (EPID)

Η τεχνολογία ενισχυμένης προστασίας προσωπικών δεδομένων της Intel (EPID) παρέχει μια διαδικτυακή γέφυρα η οποία σχεδιάστηκε για να βοηθήσει τις συσκευές να συνδέονται με ασφάλεια και σύμφωνα με την πλατφόρμα IoT της intel όπου αποτελεί ένα σημαντικό μέρος του αλγορίθμου Direct Anonymous Attestation (DAA).

Παρέχει σταθερή ταυτότητα στη συσκευή με τέτοιο τρόπο ώστε να είναι συμβατό με τα πρότυπα ISO και TEE. Βοηθά στην προστασία της ιδιωτικής ζωής με την προηγμένη τεχνολογία της ανωνυμίας αφού η επέκταση της χρήσης της EPID σε όλο το φάσμα του τομέα θα βοηθήσει να παραχθούν λύσεις πιο ασφαλείς ανεξάρτητα από την επιλογή συσκευής και εταιρίας προμηθευτή.

Σε αντίθεση με τους παραδοσιακούς αλγόριθμους ψηφιακών υπογραφών κάθε εταιρεία έχει ένα μοναδικό δημόσιο κλειδί επαλήθευσης και ένα μοναδικό ιδιωτικό κλειδί υπογραφής, Επίσης παρέχει ένα δημόσιο κλειδί επαλήθευσης που συνδέεται με άλλα πολλά κλειδιά των μοναδικών ιδιωτικών κλειδιών υπογραφής και δημιουργήθηκε να μπορεί να παρέχονται στοιχεία αναγνώρισης για μια συσκευή. Παρέχει μια πρόσθετη χρησιμότητα με την οποία μπορεί να ανακαλέσει ένα ιδιωτικό κλειδί για να γίνει μια υπογραφή ακόμη και αν το ίδιο το κλειδί είναι άγνωστο.

Η έκδοση ενός κλειδιού EPID μπορεί να γίνει απευθείας από τον εκδότη δημιουργώντας ένα κλειδί EPID και να το παραδώσει με ασφάλεια στον χρήστη.

3.2.2 TPM 2

Η πλατφόρμα Trusted Platform Module (TPM2) προσφέρει διευκολύνσεις για την ασφαλή παραγωγή των κρυπτογραφικών κλειδιών, και τον περιορισμό της χρήσης τους, εκτός από μια γεννήτρια τυχαίων αριθμών. Είναι συμβατή πλατφόρμα με την τελευταία έκδοση των Windows 10 και Windows 10 Mobile. Σχετίζεται με την ασφάλεια του κρυπτό-επεξεργαστή που έχει σχεδιαστεί για να πραγματοποιεί λειτουργίες κρυπτογράφησης σε ποικιλία συσκευών Με την ύπαρξη της μπορούμε να λύσουμε μια σειρά προβλημάτων που είτε προϋπήρχαν είτε δεν είχαν λυθεί από την προηγούμενη έκδοση

Περιλαμβάνει πολλαπλούς μηχανισμούς φυσικής ασφάλειας έτσι ώστε να μπορεί να βοηθήσει στην πρόληψη του κακόβουλου λογισμικού από τυχόν παραποιήσεις με τις λειτουργίες ασφαλείας της προηγούμενης έκδοσης TPM.

Μερικά από τα βασικά πλεονεκτήματα της χρήσης της τεχνολογίας TPM είναι ότι μπορεί να παράγει, αποθηκεύσει, να χρησιμοποιήσει και να προστατεύσει κρυπτογραφικά κλειδιά. Χρησιμοποίηση της τεχνολογίας TPM για τον έλεγχο ταυτότητας στην πλατφόρμα χρησιμοποιώντας ένα μοναδικό κλειδί έγκρισης. Τέλος συμβάλει στην ενίσχυση της ακεραιότητας της πλατφόρμας με τη λήψη και αποθήκευση των μετρήσεων της ασφάλειας.

3.2.3 PETs

Οι τεχνολογίες PETs ενισχύουν την προστασία της ιδιωτικότητας στα πληροφοριακά συστήματα αποτρέποντας την παράνομη συλλογή, χρήση και αποκάλυψη προσωπικών δεδομένων. Επιπλέον παρέχουν τη δυνατότητα σε κάθε άτομο μέσω διαφόρων εργαλείων, να ελέγχουν τα προσωπικά τους δεδομένα. Οι τεχνολογίες κρυπτογράφησης δημιουργήθηκαν για να μπορούν να βοηθήσουν τα άτομα και τους οργανισμούς στην προστασία των προσωπικών δεδομένων εξαιτίας της ευρείας διάδοσης των ηλεκτρονικών υπολογιστών και την έλευση του διαδικτύου ως νέο μέσο επικοινωνίας.

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Η έννοια των τεχνολογιών PETs εμφανίστηκε για πρώτη φορά το 1995. Από την αρχή, οι τεχνολογίες PETs έδωσαν έμφαση στην ανάγκη να ενσωματώσουν τις καθολικές αρχές των Θεμιτών πρακτικών σχετικά με τις πληροφορίες (FIPS) – καθολικές αρχές προστασίας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα - στο πραγματικό κώδικα και λειτουργία των τεχνολογιών και των συστημάτων επεξεργασίας πληροφοριών. Όλες οι τεχνολογίες PETs κινούνται γύρω από τρεις σταθερούς πυλώνες, την αρχή του επιδιωκόμενου σκοπού και στους περιορισμούς χρήσης, στην συμμετοχή του ατόμου και στην υψηλή προστασία. Σημαντικές λειτουργίες τους είναι να αποτρέπουν μη εξουσιοδοτημένη πρόσβαση σε προσωπικές επικοινωνίες και αποθηκευμένα αρχεία, να αυτοματοποιούν την ανάκτηση πληροφοριών, να διευκολύνουν τις συναλλαγές και να φιλτράρουν τυχών ανεπιθύμητα μηνύματα

ΚΕΦΑΛΑΙΟ 4º – ΤΕΧΝΙΚΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Υπάρχουν πολλές διαφορετικές τεχνικές προστασίας και μέθοδοι όπου μπορεί να προστατευθεί η ιδιωτικότητα και των προσωπικών δεδομένων των χρηστών του διαδικτύου. Ορισμένες τεχνικές επιτρέπουν στους χρήστες να διαχειρίζονται τα cookies που αποθηκεύουν οι διάφορες σελίδες που επισκέπτεται ο χρήστης για μελλοντική χρήση. Σε κάποιους άλλους παρέχετε η δυνατότητα να σερφάρουν στο διαδίκτυο ανώνυμα είτε από ανώνυμη περιήγηση είτε από κάποιο πρόγραμμα περιήγησης που σβήνει τα ίχνη τους και δύσκολα μπορούν να ανιχνευθούν. Μέσω του δικτύου του οποίου είμαστε συνδεδεμένοι μας παρέχεται κάποια ασφάλεια η οποία είναι πιο δύσκολο να παρακαμφθεί από ότι ένας κανονικός υπολογιστής χρήστη. Οι διάφορες τεχνικές παρέχουν ορισμένη προστασία της ιδιωτικότητας των χρηστών του διαδικτύου, έτσι ώστε να μπορούν να επωφεληθούν πλήρως από την τεχνολογία.

4.1 Ισχυροί Κωδικοί Πρόσβασης

Για να αποτρέψουμε τέτοιων ειδών επιθέσεις θα πρέπει να εφαρμόσουμε κάποιες μεθόδους οι οποίες θα ασφαλίσουν την λειτουργία του υπολογιστή μας και θα αποτρέψουν τις επιθέσεις από κακόβουλους χρήστες. Θα πρέπει λοιπόν να έχουμε ένα ισχυρό κωδικό πρόσβασης ο οποίο πρέπει να περιέχει κεφαλαία και πεζά γράμματα, αριθμούς και σύμβολα. Ο πιο δυνατός συνδυασμός είναι αυτός που περιέχει έστω και ένα χαρακτήρα από τις τέσσερις κατηγορίες και συνήθως οι σελίδες που δημιουργούμε τους κωδικούς μας δείχνουν πόσο δυνατός είναι ο κωδικός που δημιουργήσαμε. Δεν πρέπει ποτέ να σημειώνουμε κάπου τους κωδικούς που χρησιμοποιούμε και επίσης σημαντικό είναι να γίνεται τακτική αλλαγή τους. Μόλις τελειώσουμε την εργασία που έχουμε σε μια ιστοσελίδα πρέπει πάντα να αποσυνδέουμε τον λογαριασμό μας και ειδικά αν είμαστε σε εξωτερικούς χώρους όπως είναι μια βιβλιοθήκη ή ένα internet café.

4.2 Antivirus

Πρέπει να έχουμε εγκατεστημένα προγράμματα Antivirus τα οποία αποτρέπουν ιούς και άλλα είδη malware να μολύνουν τον υπολογιστή μας. Μια καλή λύση για να αποτρέψουμε τέτοια προβλήματα από τον υπολογιστή μας είναι να εγκαταστήσουμε virtual machines όπως είναι το Ubuntu το οποίο είναι λειτουργικό σύστημα ανοιχτού κώδικα και έχει σαν βάση του το Linux. Το θετικό αυτό του λειτουργικού συστήματος είναι ότι παρέχει μεγαλύτερη ασφάλεια αφού έχει κλειστές όλες τις θύρες επικοινωνίας και τα περισσότερα προγράμματα είναι δωρεάν έτσι μειώνονται οι πιθανότητες να πέσετε θύμα απάτης αν προσπαθήσετε να κάνετε κάτι crack ή να βρείτε patches κάτι που σας ενδιαφέρει. Είναι πολύ σημαντικό και ειδικά στις επιχειρήσεις που υπάρχουν ευαίσθητα αρχεία να παρακολουθούμε αρκετά συχνά την ασφάλεια του δικτύου μας και να ελέγχουμε ότι κάθε συσκευή που ελέγχεται πάνω στο δίκτυο δεν είναι μολυσμένη.

4.3 Plug-ins

Ακόμη και αν το πρόγραμμα περιήγησης μας έχει ρυθμιστεί ορθά για να κρύψει πληροφορίες για την αναγνώριση μας, τα plug-ins που χρησιμοποιούμε μπορούν να θέσουν σε κίνδυνο την ανωνυμία μας, έτσι θα πρέπει να αποφεύγουμε τη λειτουργία plug-ins εκεί που δεν είναι απαραίτητο. Πρώτα απ 'όλα, να ρυθμίσουμε τον browser να ζητά την έγκριση μας για να τρέξει οποιοδήποτε plug-in. Στη συνέχεια πρέπει να βεβαιωθούμε ότι τρέχουμε sandboxed plug-ins. Στην πιο ακραία περίπτωση ένα plug-in θα μπορούσε να χρησιμοποιηθεί για να συλλέξει τα προσωπικά μας στοιχεία από έναν οργανισμό όπως η NSA. Δεν είναι και λίγες οι φορές που ακούσαμε στα M.M.E για την δράση της και τι φημολογείται ότι κάνει. Οι χρήστες των Windows μόνο μπορούν να τρέξουν τα προγράμματα περιήγησης μια εφαρμογή που ονομάζεται sandboxed, που ακόμα και λιγότερο εξελιγμένα προγράμματα περιήγησης μπορούν να έχουν τα ίδια οφέλη. Κάτι παρόμοιο με το sandboxed χρησιμοποιούν και τα προγράμματα antivirus (π.χ Avast), το οποίο μας επιτρέπει να τρέξουμε προγράμματα, να επισκεφθούμε σελίδες και να κατεβάσουμε αρχεία σε ένα ασφαλές περιβάλλον εκτός του υπολογιστής μας έτσι δεν μπορούμε να επηρεαστούμε αν κάποιο από αυτά είναι μολυσμένο.

4.4 Δημιουργία Ψευδωνύμων

Υπάρχουν εργαλεία που λαμβάνουν υπόψη τα προσωπικά δεδομένα με σκοπό την προστασία της ιδιωτικότητας. Οι υπηρεσίες ανωνυμίας επιτρέπουν στο χρήστη να περιηγηθεί στο Internet χωρίς φόβο και ασφάλεια. Ο χρήστης μπορεί να καταχωρήσει τα στοιχεία του με σιγουριά αφού αυτά δεν πρόκειται να περάσουν στα χέρια τρίτων και δεν θα χρησιμοποιηθούν για εμπορικούς σκοπούς ή για άλλους αθέμιτους λόγους. Εκεί λοιπόν δημιουργείται ένας αριθμός ψευδωνύμων, τα οποία ο χρήστης μπορεί να χρησιμοποιεί ταυτόχρονα στο Διαδίκτυο. Η αρχή των πληρεξούσιων είναι απλή, δηλαδή αρχικά δημιουργείται ένας λογαριασμός σε ένα αξιόπιστο και ασφαλές πάροχο Υπηρεσιών Διαδικτύου. Έτσι ένας χρήστης μπορεί να καταχωρήσει τα προσωπικά στοιχεία του με τη διαβεβαίωση ότι δεν θα περάσουν σε άλλα μέρη ή να χρησιμοποιηθούν για σκοπούς μάρκετινγκ. Ένα συχνό φαινόμενο είναι να πωλούνται πολύ μεγάλες βάσεις δεδομένων που περιέχουν τα στοιχεία μας σε διαφημιστικές εταιρίες ή για εταιρίες που δημιουργούν έρευνες. Αυτό είναι ένα πολύ ανησυχητικό θέμα για την Κύπρο γιατί πάρα πολλά τέτοια στοιχεία καταλήγουν σε αυτές τις εταιρίες. Πολλοί χρήστες ενώ δεν έχουν δώσει κάπου τα στοιχεία τους έρχονται αντιμέτωποι καθημερινά με δεκάδες spam μηνύματα σταλμένα από υπηρεσίες μέχρι και πολιτικούς. Δημιουργείται λοιπόν ένας αριθμός ψευδωνύμων τα οποία ο χρήστης μπορεί να χρησιμοποιεί ταυτόχρονα στο Διαδίκτυο. Υπάρχουν παραδείγματα όπου ο χρήστης μπορεί να πραγματοποιεί τις πληρωμές του έμμεσα μέσω μιας έμπιστης τρίτης οντότητας ώστε οι online συναλλαγές μπορεί να χρεωθούν έμμεσα στον πελάτη μέσω της άλλης οντότητας.

4.5 Τυφλή ψηφιακή υπογραφή

Μια τυφλή ψηφιακή υπογραφή εγγυάται την ανωνυμία του χρήστη. Η διαφορά μεταξύ των δύο τύπων υπογραφής (ψηφιακή και μη ψηφιακή) είναι ότι δεν δίνει ενδείξεις ως προς την ταυτότητα του προσώπου που χρησιμοποιεί το αντικείμενο. Ότι το αντικείμενο είναι γνήσιο επιβεβαιώνεται από ανεξάρτητο τρίτο δίνοντας την ψηφιακή του υπογραφή αφού ούτε ο χρήστης ούτε η ταυτότητα του χρήστη εμφανίζεται. Αυτό το είδος της ψηφιακής υπογραφής χρησιμοποιείται για σύστημα πληρωμών. πχ bitcoins.

4.6 Δημιουργία διαφορετικών e-mails

Οι ανώνυμοι εξυπηρετητές ή εξυπηρετητές με ψευδώνυμα επιτρέπουν στο χρήστη να δημιουργεί ανώνυμους λογαριασμούς email. Κάθε ανώνυμος λογαριασμός έχει ένα μοναδικό ID, ώστε οι παραλήπτες να μπορούν να αποκριθούν σε ένα ανώνυμο μήνυμα. Οι εξυπηρετητές αυτοί παρέχουν λογαριασμούς και για απλό σερφάρισμα στο Διαδίκτυο. Ανώνυμοι servers επιτρέπουν στους χρήστες να δημιουργήσουν ανώνυμους λογαριασμούς e-mail. Κάθε ανώνυμο λογαριασμό εκχωρείται ένα μοναδικό αναγνωριστικό, έτσι ώστε οι παραλήπτες μπορούν να ανταποκριθούν σε ένα ανώνυμο μήνυμα ηλεκτρονικού ταχυδρομείου. Οι διακομιστές παρέχουν λογαριασμούς για τα δύο e-mail και δραστηριότητες για περιήγηση στο web. Με αυτό τον τρόπο αποτρέπουμε τους κακόβουλους χρήστες από το να μας μολύνουν.

Είναι λανθασμένο να χρησιμοποιούμε εταιρικά mails για την πρόσβαση μας σε προσωπικές μας σελίδες όπως είναι λάθος και να έχουμε στα mail μας εκατοντάδες μηνύματα από διάφορα μέσα κοινωνικής δικτύωσης που αφορούν τα notifications, αφού θα είναι πολύ πιθανόν κάποιο σημαντικό email να το αγνοήσουμε λόγων των πολλών μηνυμάτων. Επίσης παρόμοια μέθοδος που έχει να κάνει επίσης με mail είναι το re-mailer στο διαδίκτυο. Οι υπηρεσίες αυτές δέχονται μηνύματα ηλεκτρονικού ταχυδρομείου και αφαιρούν τις πληροφορίες που προσδιορίζουν την προέλευση του μηνύματος και έτσι διαβιβάζουν το μήνυμα στον προκαθορισμένο χρήστη. Έτσι και με τις δυο αυτές μεθόδους μειώνεται στο ελάχιστο η εκροή προσωπικών δεδομένων.

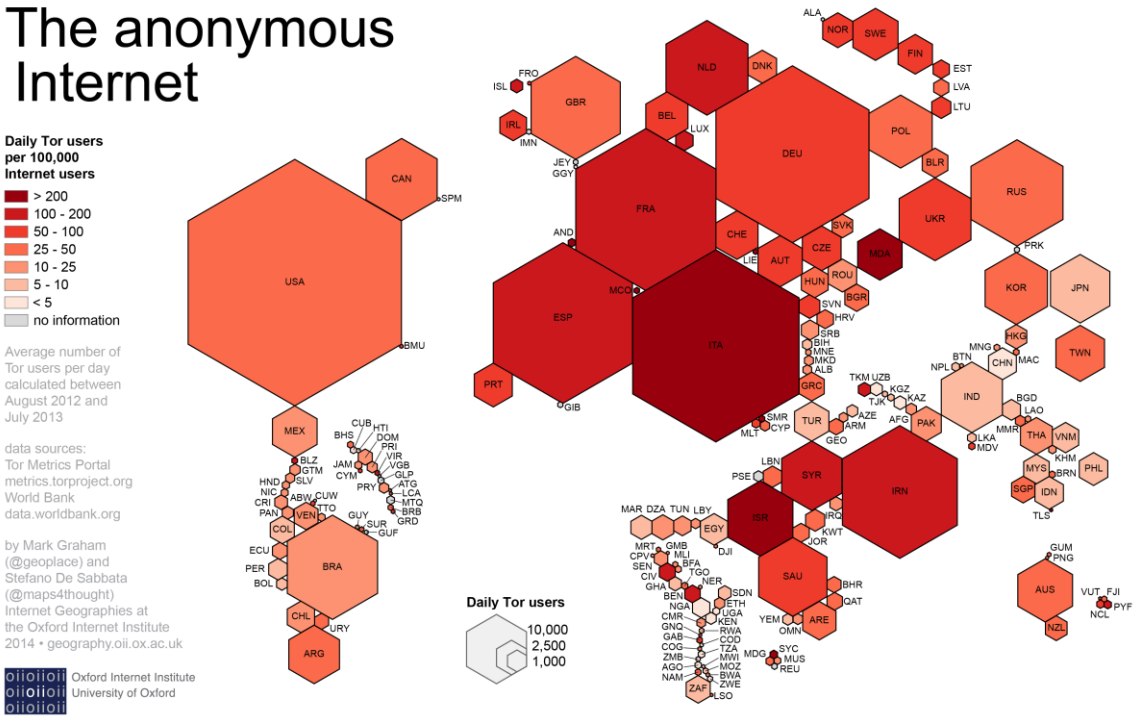
4.7 Firewalls

Τα πληρεξούσια και τα firewalls συνιστούν τα εμπόδια μεταξύ ενός υπολογιστή και του Διαδικτύου. Οι επικοινωνίες επιτρέπεται μόνο υπό ορισμένες συνθήκες και ορισμένοι τύποι επικοινωνίας μπορεί να αποκλειστούν εντελώς. Ο πληρεξούσιος υπολογιστής μπορεί να ρυθμιστεί ώστε να μπλοκάρει τις επικοινωνίες, όπως cookies, ανεπιθύμητη αλληλογραφία. Το Firewall είναι ένα εργαλείο προστασίας για την προστασία ενός δικτύου από μη εξουσιοδοτημένη πρόσβαση. Τα Firewalls επιβάλλουν μια πολιτική πρόσβασης λειτουργώντας ως πύλη μεταξύ δύο δικτύων. Ένα firewalls μπορεί να είναι είτε hardware είτε software είτε και τα δυο μαζί. Συνήθως μέσω του firewall και τους σέρβερς πολλές εταιρίες αποτρέπουν τους

εργαζόμενους τους να εγκαθιστούν προγράμματα στους Η/Υ χωρίς την άδεια του IT τμήματος ή να έχουν την δυνατότατα να χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης εν ώρα εργασίας. Πολλά προϊόντα λογισμικού επιτρέπουν στο χρήστη να δημιουργήσει προσωπικά Firewalls που εξαρτώνται από τις προτιμήσεις του και τις ρυθμίσεις του δικτύου.

4.8 Ανώνυμοι ασφαλείς περιηγητές

Υπάρχουν πολλοί ανώνυμοι περιηγητές εκεί έξω οι οποίοι ο καθένας έχει τις δίκες του ρυθμίσεις και τις δικές του λειτουργίες. Ένας πολύ γνωστός ανώνυμος περιηγητής είναι ο TOR. Ο ανώνυμος αυτός περιηγητής χρησιμοποιεί μεγάλο αριθμό δικτυού υπολογιστών ο οποίος δίνει την δυνατότητα στον χρήστη να σερφάρει διαδικτυακά μέσα από μια σειρά κρυπτογραφημένων στρωμάτων τα οποία μπορούν να κρύψουν την ταυτότητα του. Οι ανώνυμοι αυτοί περιηγητές ήρθαν να αντικαταστήσουν τους παραδοσιακούς VPN. Ο περιηγητής Tor αποτελεί σημαντικό εργαλείο ανωνυμίας και χρησιμοποιείτε συνήθως από χάκερς, κακόβουλους χρήστες, δημοσιογράφους και εγκληματικές οργανώσεις οι οποίοι μοιράζονται ανώνυμα πληροφορίες και η κάθε μια το χρησιμοποιεί για το δικό της σκοπό. Κάποιες ομάδες που το χρησιμοποιούν είναι το γνωστό Indymedia για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των μελών του. Ο καθημερινός χρήστης μπορεί εύκολα να το χρησιμοποιήσει για την προστασία της ιδιωτικής του ζωής. Ένα από τα πιο σημαντικά οφέλη του είναι ότι κρύβει την τοποθεσία που βρίσκεται ο χρήστης μέσω της IP του και το τι σελίδες επισκέπτεται. Άλλοι παρόμοιοι περιηγητές είναι οι Dooble και Avira Scout



Εικόνα 11: Καθημερινοί Χρήστες περιηγητή TOR

4.9 VPN

Οι υπηρεσίες αυτές ουσιαστικά επιτρέπουν στους χρήστες να κρύβουν τα διαδικτυακά τους ίχνη όπου η πραγματική διεύθυνση IP του χρήστη είναι κρυμμένη από τρίτους και η διαδικτυακή κυκλοφορία παραμείνει μυστική από τους διάφορους ISPs. Αν οι αρχές της χώρας είναι ενήμερες για την χρήση και την δράση των VPN μπορεί να γίνει χρήση των stealth VPNs οι οποίες αποτρέπουν εντελώς την οποιαδήποτε παρέμβαση και ανίχνευση. Αυτές προσφέρουν κατάργηση αποκλεισμού κάθε ιστοσελίδας, ανεξάρτητα από τη γεωγραφική θέση ή το τείχος προστασίας που έχουν, παρέχουν κρυπτογράφηση και μπορούν να παρακάμψουν ακόμα και τα πιο αυστηρά firewall μεγάλων χωρών. Συνήθως η χρήση τέτοιων VPN γίνεται σε χώρες όπου υπάρχει πολλή λογοκρισία όπως την Τουρκία ή Β.Κορέα και έτσι με αυτό τον τρόπο παρακάμπτονται οι οποιοιδήποτε περιορισμοί που έχει επιβάλει η χώρα Η χρήση των VPN είναι μια από τις καλύτερες επιλογές για την παράκαμψη της λογοκρισίας και της κατασκοπείας. Τα συστήματα VPN χωρίζονται σε διάφορες κατηγορίες ανάλογα με το τι προσφέρουν και τι είδους τεχνολογία χρησιμοποιούν. Κατηγοριοποιούνται σύμφωνα με τα επίπεδα ασφαλείας που παρέχουν, τα πρωτόκολλα που χρησιμοποιούν, τα στρώματα που χρησιμοποιούν για την σύνδεση

του δικτύου και άν προσφέρουν από σελίδα-σε-σελίδα ή απομακρυσμένη σύνδεση πρόσβασης.

4.10 Πρωτόκολλο HTTPS

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο αλλά συνδυάζει το απλό HTTP πρωτόκολλο και τις δυνατότητες κρυπτογράφησης που μπορεί να προσφέρει το πρωτόκολλο SSL. Σκοπός της δημιουργίας του είναι να δηλώνει ποιά διεύθυνση http είναι ασφαλή και ποία όχι. Πολλές φορές βρεθήκαμε αντιμέτωποι στο περιηγητή μας με μια σελίδα που μας έλεγε προχωρήστε με δική σας ασφάλεια. Ο λόγος ήταν γιατί το πιστοποιητικό SSL δεν μας επέτρεπε να προχωρήσουμε γιατί θα ήμασταν εκτεθειμένοι σε κακόβουλους χρήστες. Η κρυπτογράφηση που χρησιμοποιείται μας εξασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν μπορούν να κλαπούν από άλλους κακόβουλους χρήστες/τρίτους.

Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του δικτύου να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης, η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νόμιμος και ότι το πιστοποιητικό είναι έγκυρο. Έτσι οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει. Σήμερα οι πλείστες ιστοσελίδες του διαδικτύου το χρησιμοποιούνε για την ασφάλεια των πελατών τους λόγω των ευαίσθητων πληροφοριών που διακινούνται (π.χ Facebook, Bet365,τράπεζες,ταξιδιωτικές σελίδες,YouTube κ.α).

4.11 Cookies

Στα cookies συχνά αποθηκεύονται ευαίσθητες πληροφορίες οι οποίες κυκλοφορούν ανοιχτά μέσα στο Διαδίκτυο. Τα περιεχόμενα των cookies είναι θεωρητικά προσβάσιμα σε οποιονδήποτε μπορεί να τα αναλύσει ή σε οποιονδήποτε αποκτήσει πρόσβαση στον υπολογιστή του χρήστη. Τοποθετούνται στον υπολογιστή του χρήστη από έναν απομακρυσμένο web server τον οποίο έχει ήδη επισκεφτεί ο χρήστης μέσω ενός web browser. Ενώ τα cookies συνιστούν μια πολύ ισχυρή τεχνολογία για την ενίσχυση της λειτουργίας και αλληλεπίδρασης της ιστοσελίδας, αποτελούν παράλληλα και μια τεχνολογία που μπορεί να χρησιμοποιηθεί με καταχρηστικούς τρόπους παραβιάζοντας την ιδιωτικότητα του χρήστη. Μια τέτοια λειτουργία που μεγάλες αεροπορικές εταιρίες με αθέμιτα μέσα μέσω των cookies διαβάζουν τις προτιμήσεις του χρήστη για μια συγκεκριμένη πτήση μια συγκεκριμένη ημέρα. Αν πολλοί χρήστες μέσα στην μέρα επέλεξαν να δουν την ίδια πτήση και την ίδια ημέρα η εταιρία καταλαβαίνει μέσω των cookies πως υπάρχει ζήτηση και αυξάνει την τιμή με κυριότερο σκοπό το κέρδος.

Τα αρχεία των cookies πρέπει να είναι κρυπτογραφημένα όταν περιέχουν προσωπικά δεδομένα, αλλά ο χρήστης δεν έχει κανένα έλεγχο πάνω σε αυτά. Στα αρχεία cookies αποθηκεύονται ευαίσθητες πληροφορίες όπως κωδικοί πρόσβασης, στοιχεία πιστωτικής κάρτας, τα οποία κατά τη διάρκεια μιας επίθεσης δύναται να κυκλοφορήσουν ελεύθερα μέσω του διαδικτύου. Πρόσφατα ψηφίστηκε νόμος σχετικά με τα cookies για αυτό σε ότι σελίδα επισκεφθούμε μας ζητά να διαβάσουμε τους κανονισμούς γύρω από αυτό και να πατήσουμε το κατάλαβα αν συμφωνούμε. Το θετικό για τους χρήστες είναι ότι μας παρέχετε η δυνατότητα να επιτρέψουμε ή να αποτρέψουμε τις διάφορες σελίδες να αλιεύσουν πληροφορίες από εμάς μέσω των cookies. Από τις ρυθμίσεις του περιηγητή μας μπορούμε να επιλέξουμε στις πιο κάτω επιλογές: αν επιτρέπουμε να διαβάζουν τις πληροφορίες μας το οποίο τονίζεται ότι προτείνεται, να διαβάζουν τις πληροφορίες μας μέχρι να κλείσουμε τον περιηγητή, να αποτρέψουμε τις σελίδες να διαβάζουν τις πληροφορίες και να αποτρέψουμε cookies να αποθηκεύονται μέσω άλλων τρίτων ιστοσελίδων κατά την διάρκεια περιήγησης μας. Οι αλγόριθμοι του Facebook λειτουργούν τα πάντα μέσω των cookies αφού αν ψάξουμε κάτι συγκεκριμένο σε μηχανή αναζήτησης είναι πολύ πιθανόν μετά από λίγο να το δούμε στην κεντρική μας σελίδα στο Facebook ως διαφήμιση.

4.12 Ρυθμίσεις περιηγητή πλοήγησης

Κάτι πολύ σημαντικό που οι περισσότεροι δυστυχώς αγνοούν λόγω στοιχειώδης γνώσεις στους υπολογιστές και γενικά στο διαδύκτιο είναι ότι μας δίνεται η δυνατότητα μέσω των ρυθμίσεων του περιηγητή μας να επιλέξουμε για διαφορετικές ρυθμίσεις που αφορούν την ασφάλεια και την ιδιωτικότητα μας. Τέτοιες ρυθμίσεις είναι να αποτρέψουμε στον περιηγητή να κάνει χρήση της κάμερας του φορητού μας υπολογιστή και να χρησιμοποιήσει το μικρόφωνο μας. Αν χρησιμοποιούμε προγράμματα επικοινωνίας μέσω video όπως ooVoo και Skype θα μπορούσαμε να το ρυθμίσουμε να διαλέγουμε εμείς πότε θέλουμε να τα χρησιμοποιήσουμε. Επίσης πρέπει να αποτρέπουμε τον περιηγητή να διαβάζει την τοποθεσία μας. Από την μια είναι θετικό για κάποιες σελίδες να διαβάζουν την τοποθεσία μας για να μας μεταφέρουν στην ιστοσελίδα που πρέπει να βλέπουμε, αλλά από την άλλη μπορεί να χρησιμοποιηθεί για διαφημιστικούς λόγους δηλαδή μέσω του Google Ads, για παράδειγμα κάποιου χρήστη στην Κύπρο είναι πολύ πιο πιθανό να του διαφημιστεί ένα προϊόν που βρίσκεται μόνο στην Κύπρο.

4.13 JavaScript

Η javascript είναι ένα πολύ σημαντικό εργαλείο αλλά μέσω αυτής και τρόπου που είναι κατασκευασμένη μπορεί να διαρρεύσει πολλές και σημαντικές συνήθειες του χρήστη που έχει διαδικτυακά. Το αρνητικό για τους χρήστες αλλά το πλεονέκτημα της JavaScript είναι ότι χωρίς αυτήν σχεδόν όλες οι ιστοσελίδες δεν θα τρέχουν κανονικά αφού σημαντικό μέρος τους περιέχει Javascript. Το θετικό για τους χρήστες είναι ότι μπορούν να απενεργοποιήσουν την javascript ή να της επιτρέψουν να τρέχει μόνο σε σελίδες οι οποίες εμπιστεύονται. Προσωπική μου άποψη είναι ότι ο κάθε ένας ανάλογα με τις απαιτήσεις και τις συνήθειες που έχει διαδικτυακά μπορεί να κρίνει αν η JavaScript είναι πλεονέκτημα ή μειονέκτημα για εμάς. Για κάποιους με περιορισμένες λειτουργίες ίσως να είναι καλύτερο να την απενεργοποιήσουν αλλά για άλλους χρήστες που χρησιμοποιούν το gmail για παράδειγμα θα είναι πολύ χρονοβόρο και δεν θα τρέχει η σελίδα σωστά.

4.14 Κρυπτογράφηση

Ένας από τους αρχαιότερους μηχανισμούς ασφαλείας που μπορούν να χρησιμοποιηθούν για στην παροχή του απορρήτου των δεδομένων είναι η κρυπτογράφηση. Σκοπός της είναι η εξασφάλιση προστασίας της ιδιωτικότητας, κρατώντας την πληροφορία κρυφή. Η αντίστροφη διαδικασία της κρυπτογράφησης είναι η αποκρυπτογράφηση δηλαδή η μετατροπή των κρυπτογραφημένων πληροφοριών σε κάποια κατανοητή μορφή. Αυτό μπορεί να γίνει με τη στενογραφία, την τέχνη της απόκρυψης δεδομένων μέσα σε άλλα δεδομένα. Η πληροφορία είναι κρυμμένη μέσα στο μέσο, έτσι ώστε να μην γίνει αντιληπτή από ανεπιθύμητα άτομα, άλλα μόνο από τον παραλήπτη που για τον οποίο προορίζεται. Αυτό ουσιαστικά καταλήγει στη χρήση απαραίτητων δυαδικών ψηφίων σε ένα αθώο αρχείο για την αποθήκευση των ευαίσθητων δεδομένων.

Σε ένα ευρύτερο δίκτυο τα κλειδιά που πρέπει να διαχειρίζονται οι χρήστες είναι πάρα πολλά. Καθίσταται αναγκαία λοιπόν η ύπαρξη μιας οντότητας την οποία θα πρέπει όλοι να την εμπιστεύονται δηλαδή η TTP. Η οντότητα αυτή έχει πλήρη πρόσβαση στα μυστικά κλειδιά των χρηστών και θα καθιστά δυνατή την ασφαλή επικοινωνία τους. Ένα Trusted Third Party είναι μία οντότητα την οποία οι χρήστες ενός μεγάλου δικτύου εμπιστεύονται σε αυτή την διαχείρηση των κλειδιών τους, ώστε να καθίσταται δυνατή η ασφαλής επικοινωνία μεταξύ τους. Οι ευθύνες και οι υποχρεώσεις που έχει αυτή είναι αυστηρά καθορισμένες σε ένα σύστημα. Βέβαια, η μορφή ενός Trusted Third Party σε ένα συμμετρικό σύστημα κρυπτογραφίας παρουσιάζει μεγάλες διαφορές σε σχέση με αυτό ενός ασύμμετρου συστήματος. Οι κύριοι τομείς αυτής της οντότητας είναι η διαχείριση κλειδιών, υπηρεσίες ταυτοποίησης, λειτουργίες διακομιστή και λειτουργίες θεματοφύλακα.

ΚΕΦΑΛΑΙΟ 5ο – ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ

Η εργασία αυτή περιλαμβάνει πέραν του θεωρητικού μέρους και ερευνητικό μέρος όπου στην παρούσα έρευνα η συλλογή των στοιχείων έγινε με την χρήση ερωτηματολογίου, που είναι η πιο συχνά χρησιμοποιούμενη τεχνική σε δειγματοληπτικές έρευνες και η πιο ακριβής για καταγραφή των ερωτημάτων/αναγκών του εκάστοτε φορέα.

5.1 Ερωτηματολόγιο

Στο κεφάλαιο αυτό παρουσιάζονται οι στόχοι και η μεθοδολογία της έρευνας, η δομή του ερωτηματολογίου (τα δημογραφικά στοιχεία & η διερεύνηση ασφαλούς χρήσης προσωπικών δεδομένων στο διαδίκτυο) και τέλος, η περιγραφή των ευρημάτων της έρευνας.

5.1.1 Σκοπός και Στόχος του ερωτηματολογίου

Ο σκοπός της έρευνας είναι η διερεύνηση της ασφαλούς ή μη χρήσης των προσωπικών δεδομένων στο διαδίκτυο από τους κατοίκους της Κύπρου. Μέσα από το ερωτηματολόγιο επιδιώκεται να διερευνηθεί ο βαθμός και ο τρόπος με τον οποίο η προστασία των προσωπικών δεδομένων επηρεάζει τον τρόπο με τον οποίο οι Κύπριοι πολίτες χρησιμοποιούν το διαδίκτυο και κατά πόσο γίνετε εν αγνοία τους ή μη διαρροή των προσωπικών τους δεδομένων. Ταυτόχρονα απώτερος στόχος της έρευνας είναι η σκιαγράφηση του μέσου προφίλ των Κύπριων χρηστών του διαδικτύου και κατά πόσο ο Κύπριος πολίτης αντιλαμβάνεται την γενική έννοια του Διαδικτύου στην εποχή που ζούμε.

5.1.2 Μεθοδολογία έρευνας

Η μέθοδος έρευνας που χρησιμοποιήθηκε ήταν η ποσοτική – περιγραφική μέσα από τη συμπλήρωση ερωτηματολογίου. Για τη δημιουργία του δείγματος των ερωτώμενων ακολουθήθηκε η μεθοδολογία της δειγματοληψίας ευκολίας, χρησιμοποιώντας ένα όσο το δυνατόν πιο αντιπροσωπευτικό δείγμα παρατηρήσεων μέσω του οποίου επιδιώκεται η γενίκευση στον ευρύτερο πληθυσμό.

Το ερωτηματολόγιο δημιουργήθηκε σε αρχείο Word και ακολούθως κοινοποιήθηκε μέσω συγκεκριμένης ιστοσελίδας κοινωνικής δικτύωσης όπως και κατ' ιδίαν σε άτομα διαφορών ηλικιών για την σωστή εξαγωγή των επιθυμητών αποτελεσμάτων. Ακολούθως έγινε ανάλυση και συγκέντρωση των απαντήσεων στην Excel όπου δημιουργήθηκαν και οι γραφικές παραστάσεις. Στόχος της επιλογής του δείγματος ήταν και να παρθεί τυχαίο δείγμα αλλά και ο πληθυσμός του δείγματος να είναι χρήστες του διαδικτύου για μπορούν να απαντήσουν σε όλες τις ερωτήσεις με απώτερο σκοπό την διασφάλιση του αποτελέσματος. Ευτυχώς με την βοήθεια και την άψογη συνεργασία που έδειξαν οι ερωτηθείς επιτεύχθηκε η καταγραφή και συλλογή όλων των ερωτηματολογίων σε πολύ μικρό χρονικό διάστημα.

Οι τύποι των ερωτήσεων που χρησιμοποιήθηκαν ήταν κλειστού και ανοικτού τύπου όπου στις μεν κλειστές οι κατηγορίες των απαντήσεων παρέχονται στους ερωτώντες οι οποίοι απλά πρέπει να διαλέξουν την επιλογή και οι δε ανοικτές όπου οι ερωτώμενοι ήταν ελεύθεροι να απαντήσουν στις ερωτήσεις.

5.1.3 Περιγραφή ερωτηματολογίου

Το ερωτηματολόγιο αποτελείται από τις 2 κύριες ενότητες και 21 ερωτήσεις (συμπεριλαμβανομένων όλων των υποερωτημάτων). Στην πρώτη ενότητα διερευνήθηκε το προφίλ των ερωτηθέντων με την καταγραφή των δημογραφικών στοιχείων και στη δεύτερη ενότητα διερευνήθηκε η ασφαλής χρήση ή μη των προσωπικών δεδομένων στο διαδίκτυο.

Τα ζητούμενα που τέθηκαν στους ερωτώμενους στην πρώτη ενότητα περιλάμβαναν τα εξής:

1. Φύλο
2. Ηλικία
3. Οικογενειακή Κατάσταση
4. Μορφωτικό Επίπεδο
5. Επάγγελμα
6. Μηνιαίο Εισόδημα
7. Τόπος Διαμονής

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Τα ζητούμενα που τέθηκαν στους ερωτώμενους στη δεύτερη ενότητα περιλάμβαναν τα εξής:

1. Χρησιμοποιείτε ισχυρό κωδικό πρόσβασης (δηλ. περιλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και άλλα σύμβολα) ;

2. Τι κωδικό πρόσβασης χρησιμοποιείται συνήθως στο διαδίκτυο;

3. Αλλάζετε τακτικά τον κωδικό πρόσβασης;

4. Χρησιμοποιείται για κάθε λογαριασμό ξεχωριστό κωδικό πρόσβασης;

5. Κρατάτε τον κωδικό πρόσβασης μυστικό;

6. Χρησιμοποιείτε προσεκτικά τους δικτυακούς τόπους κοινωνικής δικτύωσης (αποδέχεστε μόνο άτομα που γνωρίζεται, δεν επιτρέπετε στις εφαρμογές που χρησιμοποιείται να έχουν χρήση των προσωπικών σας δεδομένων κ.α) ;

7. Προσπάθησε ποτέ κάποιος τρίτος να χρησιμοποιήσει προσωπικά σας δεδομένα χωρίς την άδεια σας; (φωτογραφίες, βίντεο, κωδικούς πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών-e banking κ.α),;

   7α.) Αν ναι, το αναφέρατε ποτέ στην Δίωξη Ηλεκτρονικού Εγκλήματος ή στην Αστυνομία;

   7β.) Πού χρησιμοποιήθηκαν τα προσωπικά σας δεδομένα (αγορά υπηρεσιών, αγορά προϊόντος, εξαπάτηση τρίτων με τα στοιχεία μου, κ.α);

8. Πραγματοποιείς αγορές μέσω διαδικτύου; Εάν όχι, γιατί;

   8α.) Αν ναι, πόσο συχνά αγοράζετε προϊόντα και υπηρεσίες μέσω διαδικτύου;

9. Σε πόσα μέσα κοινωνικής δικτύωσης διατηρείται λογαριασμό;

   9α.) Αν διατηρείται λογαριασμό πόσο χρόνο αφιερώνεται σε αυτό;

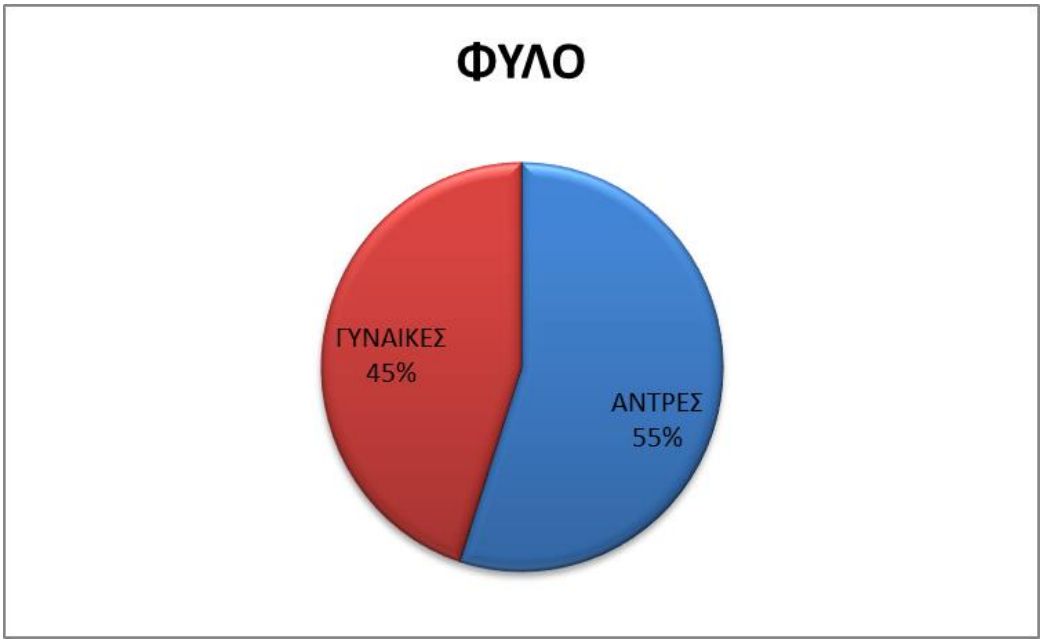
   9β.) Αν δεν διατηρείται λογαριασμό προσδιορίστε τον λόγο:

5.2 Παρουσίαση ευρημάτων

Η έρευνα πραγματοποιήθηκε το χρονικό διάστημα από τις 10/5/2016 έως 10/6/2016. Στην ενότητα αυτή παρουσιάζονται τα αποτελέσματα των δημογραφικών χαρακτηριστικών του δείγματος.

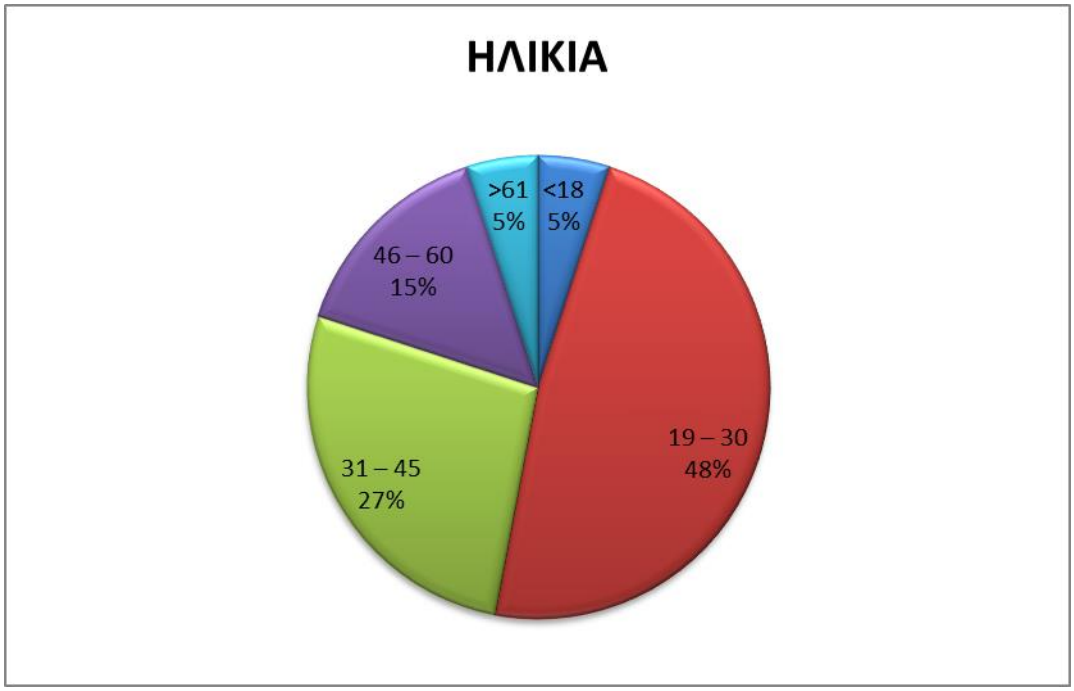
5.2.1 Δημογραφικά χαρακτηριστικά

Τα ερωτηματολόγια που συμπληρώθηκαν ήταν 104 άτομα από τα οποία έγκυρα ήταν τα 100. Από τα 100 άτομα που συμπλήρωσαν το ερωτηματολόγιο τα 55 ήταν άντρες και οι 45 γυναίκες.



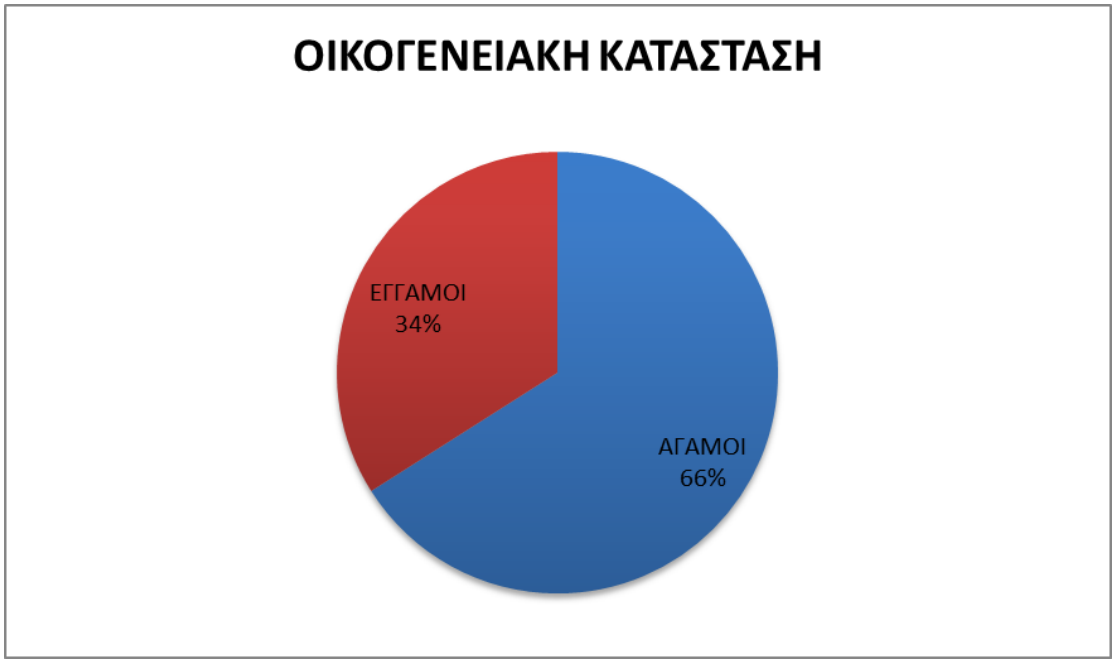
Εικόνα 12: Ερωτηματολόγιο Φύλο

Όσον αφορά την ηλικία των ερωτηθέντων αυτή διαχωρίστηκε σε ηλικιακές ομάδες όπου το μεγαλύτερο ποσοστό ανήκει στην δεύτερη και τρίτη ηλικιακή ομάδα όπως παρουσιάζονται στο ερωτηματολόγιο. Το μεγαλύτερο και αναμενόμενο ποσοστό ανήκε στην ηλικιακή ομάδα 19-30 ετών (48%), ακολούθως στην ηλικιακή ομάδα 31-45 ετών (27%) και σε μικρότερα ποσοστά στις ηλικιακές ομάδες 46-60 (15%), <18 ετών (5%) και >61 ετών (5%).



Εικόνα 13: Ερωτηματολόγιο Ηλικία

Η πλειοψηφία των ερωτηθέντων είναι άγαμοι (66%) ενώ το (34%) είναι έγγαμοι, λογικό αποτέλεσμα αν αναλογιστούμε ότι η μεγαλύτερη ηλικιακή ομάδα είναι η ομάδα από 19 ως 30 ετών.

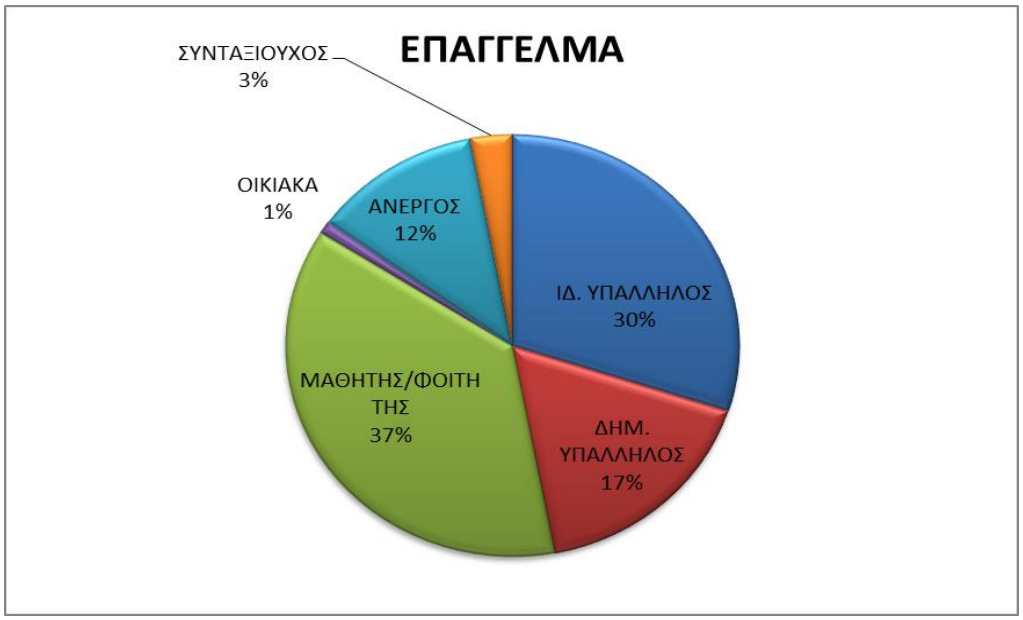


Εικόνα 14: Ερωτηματολόγιο Οικογενειακή κατάσταση

Το επίπεδο εκπαίδευσης των ερωτηθέντων είναι πολύ υψηλό καθώς το (70%) είναι πτυχιούχοι Ανώτατης /Ανώτερης Εκπαίδευσης. Ακολούθως το (22%) είναι απόφοιτοι λυκείου, το (7%) απόφοιτοι Γυμνασίου και μόλις το (1%) απόφοιτοι δημοτικού.

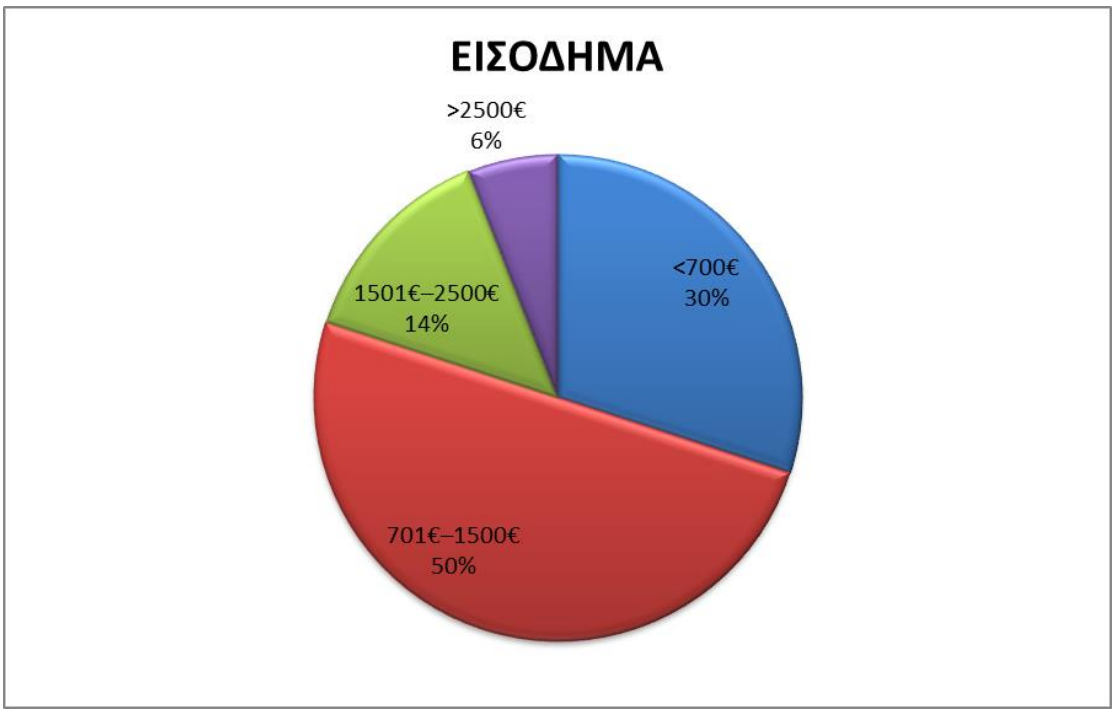
Εικόνα 15: Ερωτηματολόγιο Μορφωτικό Επίπεδο

Από τους ερωτηθέντες η πλειοψηφία είναι μαθητές/φοιτητές (37%) και ακολουθούν οι ιδιωτικοί υπάλληλοι (30%). Το (17%) είναι δημόσιοι υπάλληλοι ενώ το (12%) είναι άνεργοι. Τέλος, οι συνταξιούχοι και τα οικιακά βρίσκονται στην προτελευταία και τελευταία θέση με (3%) και (1%) αντίστοιχα.



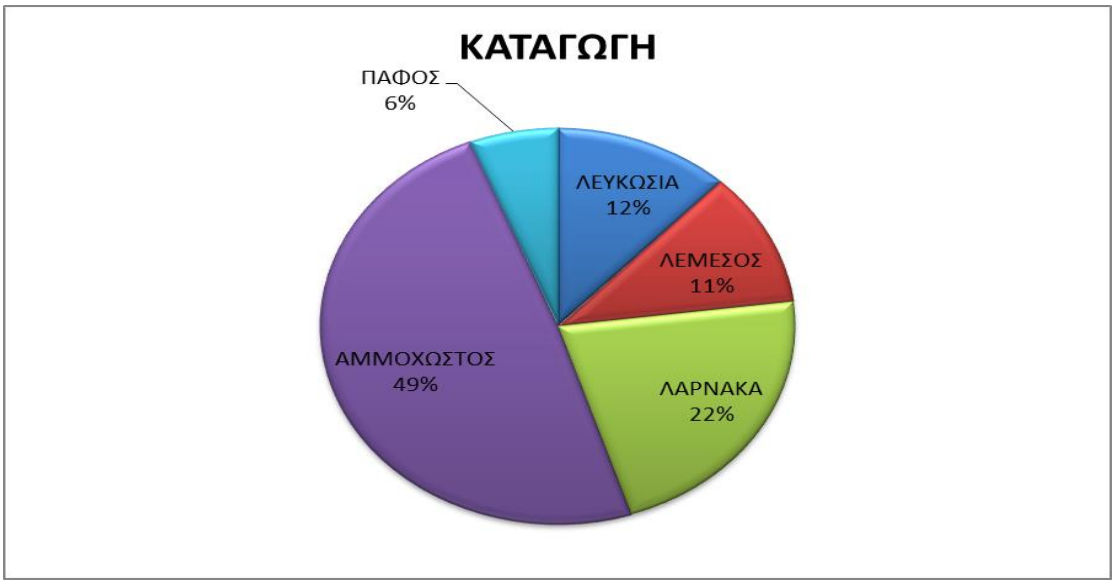
Εικόνα 16: Ερωτηματολόγιο Επάγγελμα

Η πλειοψηφία των ερωτώμενων εισοδημάτων (50%) ανήκει στην κατηγορία των μέσων εισοδημάτων (701€ - 1500€), ενώ ακολουθούν τα χαμηλά εισοδήματα μέχρι 700€ σε ποσοστό (30%). Τέλος ακολουθούν τα ποσοστά (14%) και (6%) για τα εισοδήματα 1501-2500€ και πάνω από 2500€ αντίστοιχα.



Εικόνα 17: Ερωτηματολόγιο Εισόδημα

Τέλος η πλειοψηφία των ερωτώμενων προέρχεται από την επαρχία Αμμοχώστου (49%), ενώ Λάρνακα και Λευκωσία καταλαμβάνουν την 2η και 3η θέση με ποσοστά (22%) και (12%) αντίστοιχα. Τα μικρότερα ποσοστά προέρχονται από την επαρχία Λεμεσού (11%) και (6%) από την επαρχία Πάφου.

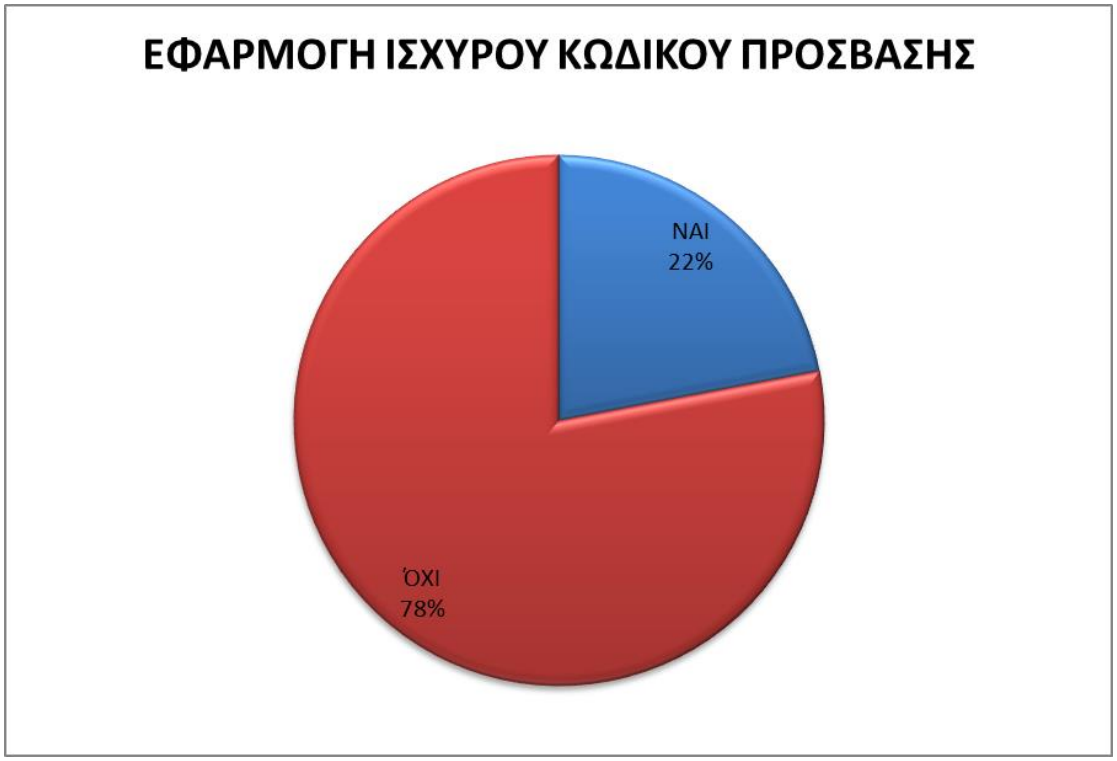


Εικόνα 18: Ερωτηματολόγιο Καταγωγή

5.2.2 Διερεύνηση ασφαλούς χρήσης των προσωπικών δεδομένων

Στο δεύτερο μέρος παρουσιάζονται τα αποτελέσματα των ερωτήσεων σχετικά με τη διερεύνηση της ασφαλούς χρήσης ή μη των προσωπικών δεδομένων στο διαδίκτυο από τους ερωτηθέντες.

Σύμφωνα με τα αποτελέσματα της ανάλυσης το μεγαλύτερο ποσοστό των ερωτηθέντων (78%) απάντησε ότι δεν χρησιμοποιεί ισχυρό κωδικό πρόσβασης, που να συμπεριλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και άλλα σύμβολα. Αντιθέτως ένα μικρό αλλά σεβαστό ποσοστό (22%) απάντησε ότι χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης στις διάφορες εφαρμογές που χρησιμοποιεί καθημερινά και εκεί που διατηρεί προσωπικούς λογαριασμούς π.χ social media.

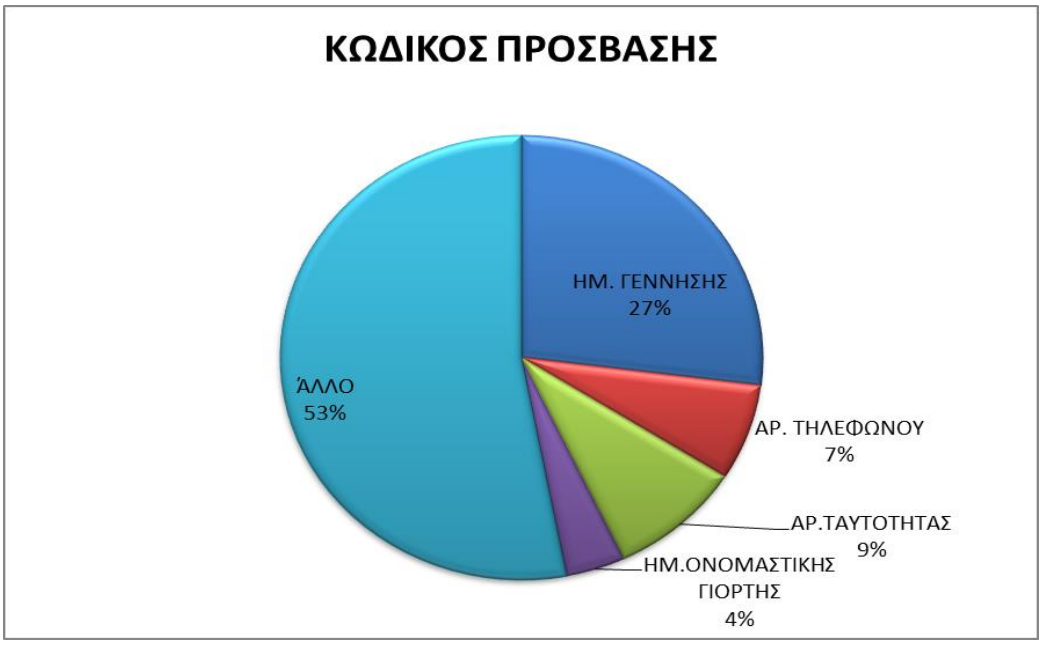


Εικόνα 19: Ερωτηματολόγιο Εφαρμογή Κωδικού Πρόσβασης

Όσον αφορά το τι κωδικό πρόσβασης χρησιμοποιούν συνήθως στο διαδίκτυο το μικρότερο ποσοστό των ερωτηθέντων (4%) απάντησε ότι χρησιμοποιεί την ημερομηνία της ονομαστικής του γιορτής. Ακολουθεί με ποσοστό (7%) ο αριθμός τηλεφώνου ενώ στην επόμενη θέση βρίσκετε με ποσοστό (9%) ο αριθμός ταυτότητας των ερωτηθέντων. Στην 2^{η} θέση βρίσκεται η ημερομηνία γέννησης με ποσοστό (27%) ενώ στην 1^{η} θέση και με ποσοστό (53%) είναι το άλλο δηλαδή κάτι που δεν αντιστοιχεί στα πιο πάνω πεδία (μερικές ενδεικτικές απαντήσεις ήταν αγαπημένη ομάδα, ημ. γάμου και ακολουθία αριθμών).

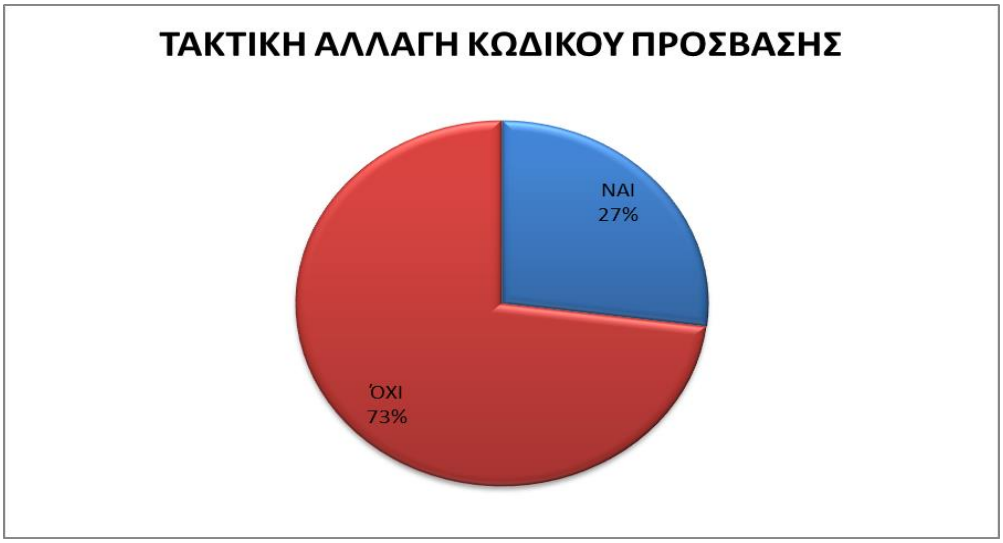
Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

Επειδή κάποιοι από τους ερωτηθείς χρησιμοποιούν κωδικούς πρόσβασης που αντιστοιχούν σε περισσότερα από ένα πεδία του ερωτηματολογίου τους ζητήθηκε όπως δηλώσουν το μεγαλύτερο σε εύρος χρήσης κωδικό πρόσβασης που χρησιμοποιούν.



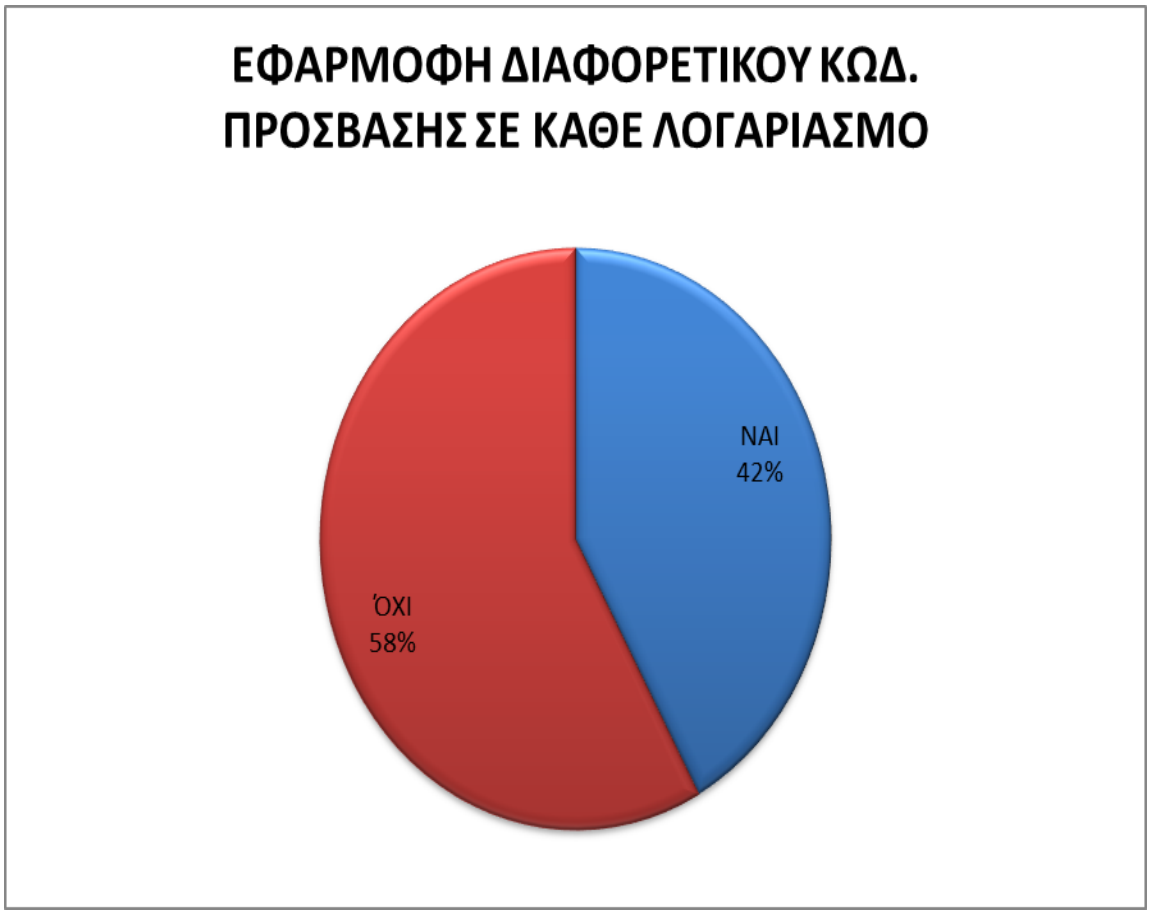
Εικόνα 20: Ερωτηματολόγιο Κωδ. Πρόσβασης

Όσον αφορά στο εάν αλλάζουν τακτικά τον κωδικό πρόσβασης το (73%) των ερωτηθέντων απάντησε ότι δεν τον αλλάζει τακτικά ενώ το (27%) ότι τον αλλάζει τακτικά. Ο κυριότερος λόγος που δεν αλλάζουν τον κωδικό τους σε σχετική μου ερώτηση είναι ότι επειδή διατηρούν αρκετούς λογαριασμούς είναι δύσκολο να απομνημονεύουν καινούριους κωδικούς.



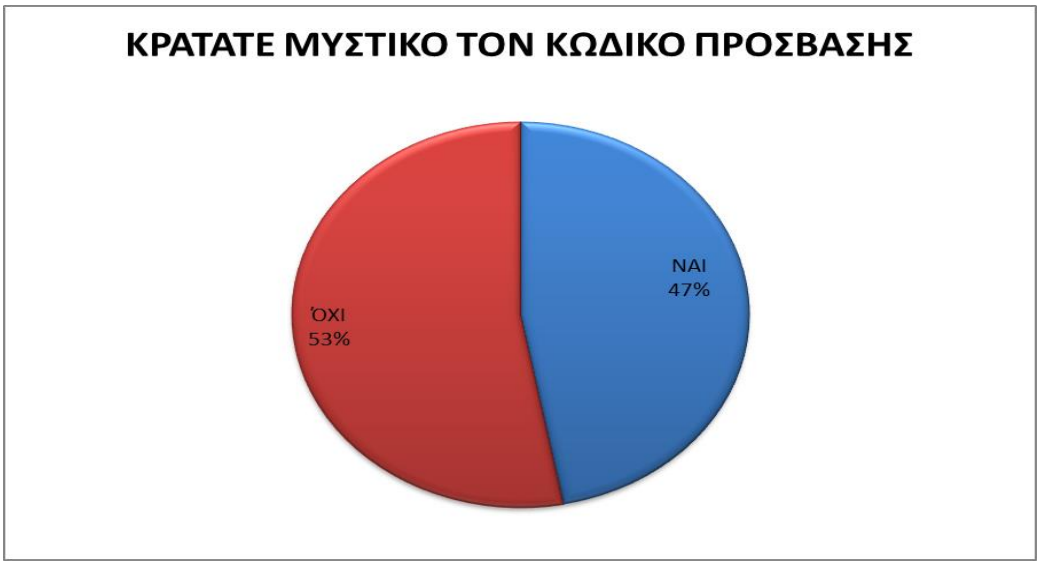
Εικόνα 21: Ερωτηματολόγιο Τακτική Αλλαγή Κωδ. Πρόσβασης

Επίσης το μεγαλύτερο ποσοστό των ερωτηθέντων (58%) απάντησε ότι δεν χρησιμοποιεί ξεχωριστό κωδικό πρόσβασης για κάθε λογαριασμό, ενώ το (42%) χρησιμοποιεί διαφορετικούς κωδικούς για κάθε λογαριασμό. Σημαντικό ρόλο παίζει και το γεγονός ότι δίνονται κάποιοι default κωδικοί πρόσβασης στους χρήστες όπου αρκετοί δεν τους αλλάζουν.



Εικόνα 22: Εφαρμογή Διαφορετικού Κωδ. Πρόσβασης

Από τα αποτελέσματα φαίνεται επίσης ότι οι ερωτηθέντες δεν κρατούν μυστικό τον κωδικό πρόσβασης σε ποσοστό (53%). Επειδή μου φάνηκε υπερβολικό το ποσοστό ζήτησα μετά από κάποιους που εμπίπτουν σε αυτή την κατηγορία να μου απαντήσουν γιατί μοιράζονται τον κωδικό τους πρόσβασης με άλλα άτομα και οι περισσότερες απαντήσεις ήταν λόγω ανασφάλειας στην σχέση τους και κοινών λογαριασμών με φίλους ή με άτομα της οικογένειας . Ένα αρκετά μεγάλο ποσοστό (47%) κρατάει μυστικό τον κωδικό πρόσβασης στους λογαριασμούς που υπό κανονικές συνθήκες θα έπρεπε να ήταν πολύ μεγαλύτερο.

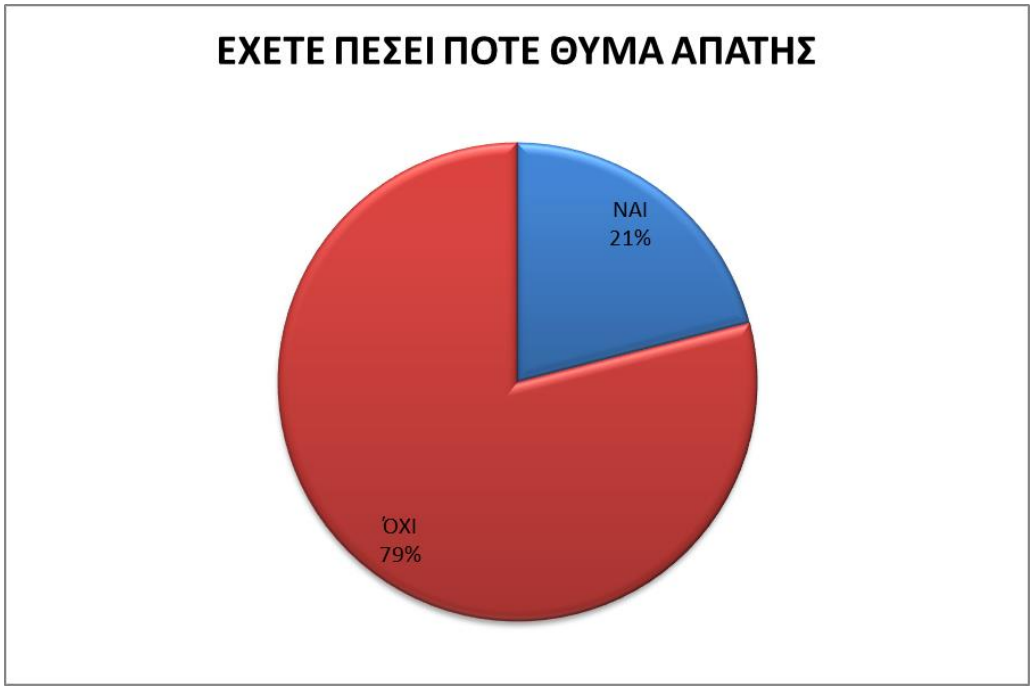


Εικόνα 23: Ερωτηματολόγιο Μυστικός Κωδ. Πρόσβασης

Η ανασφάλεια που αισθάνονται οι χρήστες αντικατοπτρίζεται και στα αποτελέσματα της ερώτησης σχετικά με το εάν χρησιμοποιούν προσεκτικά τους δικτυακούς τόπους κοινωνικής δικτύωσης, για το εάν αποδέχονται μόνο άτομα που γνωρίζουν και δεν επιτρέπουν στις εφαρμογές που χρησιμοποιούν να έχουν χρήση των προσωπικών τους δεδομένων. Το (58%) των ερωτηθέντων απάντησε ότι χρησιμοποιεί προσεκτικά τους δικτυακούς τόπους κοινωνικής δικτύωσης ενώ ένα αρκετά μεγάλο ποσοστό (42%) δεν είναι τόσο προσεκτικοί, πιθανότατα λόγω άγνοιας κινδύνων που μπορεί να προέρχονται από τη μη ορθή χρήση των προσωπικών δεδομένων στο διαδίκτυο.

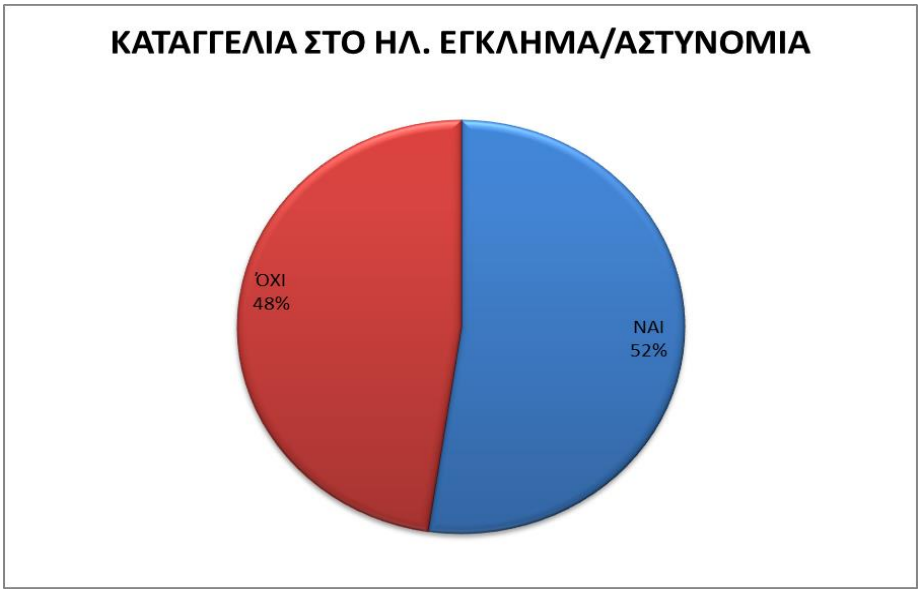
Εικόνα 24: Χρησιμοποίηση Μέσων Κοινωνικής Δικτύωσης

Όσον αφορά στην ερώτηση για το εάν προσπάθησε κάποιος τρίτος να χρησιμοποιήσει προσωπικά δεδομένα όπως φωτογραφίες, βίντεο, κωδικούς πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών e-banking κ.α., χωρίς την άδεια των ερωτηθέντων το μεγαλύτερο ποσοστό απάντησε Όχι με ποσοστό (79%), ενώ ένα αξιόλογο ποσοστό (21%) απάντησε Ναι που από μόνο του είναι ανησυχητικό



Εικόνα 25: Ερωτηματολόγιο Θύμα Απάτης

Από τα 21 άτομα που απάντησαν ότι έπεσαν θύματα υποκλοπής προσωπικών δεδομένων οι 11 δηλαδή ποσοστό (52%) το ανέφεραν στην Δίωξη Ηλεκτρονικού Εγκλήματος/Αστυνομία ενώ οι άλλοι 10 όχι που αντιστοιχεί σε (48%).



Εικόνα 26: Ερωτηματολόγιο Καταγγελία Απάτης

Επίσης από αυτούς που ήταν θύματα υποκλοπής προσωπικών δεδομένων από τρίτους εν αγνοία τους, 17 από αυτών χρησιμοποιήθηκαν για αγορά υπηρεσιών σε ποσοστό (80.9%), ενώ για 4 άτομα έγινε εξαπάτηση τρίτων με τα στοιχεία τους με ποσοστό (19.1%).

Εικόνα 27: Ερωτηματολόγιο Που έγινε χρήση τους

Το (69%) των ερωτηθέντων απάντησε ότι πραγματοποίησε έστω και μια αγορά μέσω διαδικτύου ενώ το (31%) απάντησε ότι δεν έχει πραγματοποιήσει ποτέ. Από τα 31 άτομα που απάντησαν ότι δεν πραγματοποίησαν ποτέ αγορά διαδικτυακά οι 19 απάντησαν ότι ο λόγος είναι γιατί δεν θέλουν να εκθέτουν τα προσωπικά δεδομένα , οι 8 γιατί πιστεύουν ότι τα προϊόντα που αγοράζουν μέσω διαδικτύου δεν είναι αξιόπιστα και τέλος οι 4 λόγω έλλειψης προσωπικού ελεύθερου χρόνου.

Εικόνα 28: Διαδικτυακές Αγορές

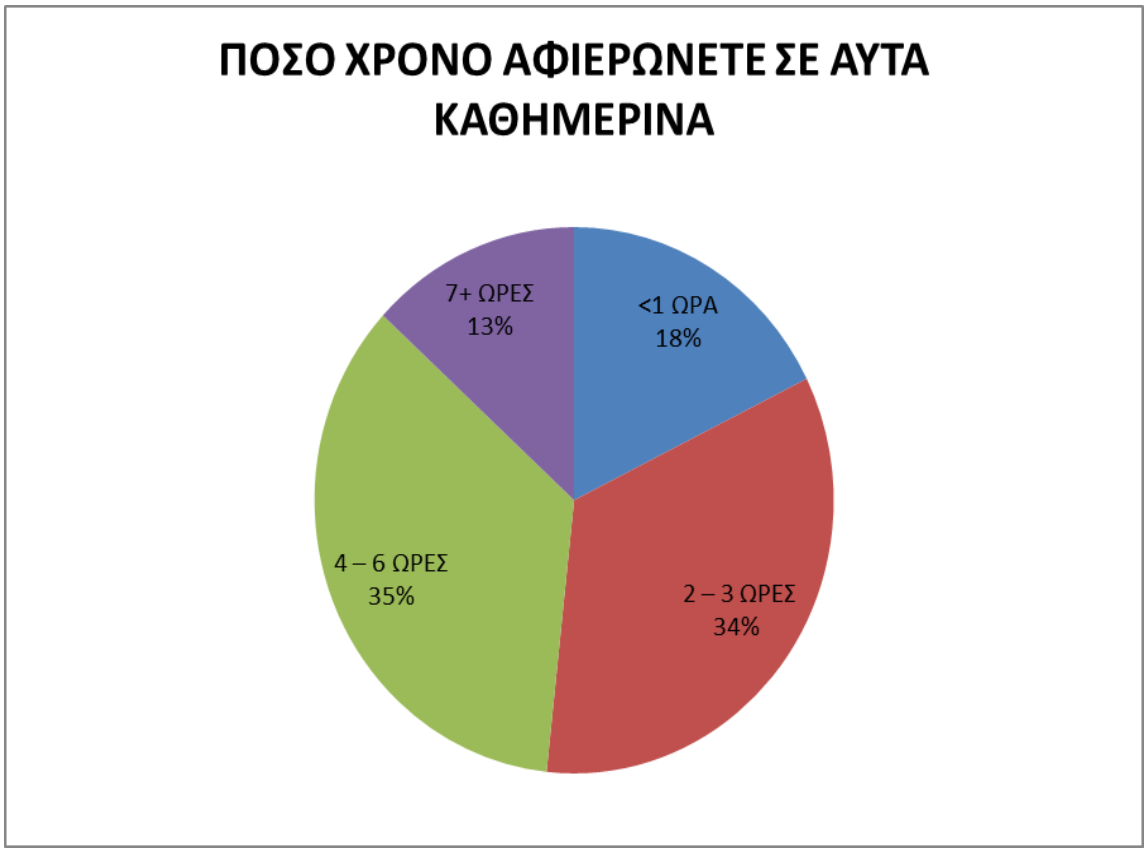
Από τους 69 που απάντησαν ότι πραγματοποιούν αγορές μέσω διαδικτύου 15 άτομα με ποσοστό (21,7%) πραγματοποιούν έστω και μια αγορά στο χρόνο. Ακολούθως 26 άτομα με ποσοστό (37,7%) πραγματοποιούν έστω και μια αγορά κάθε έξι μήνες, 21 άτομα και ποσοστό (30,5%) μια αγορά τον μήνα και τέλος 7 άτομα με ποσοστό (10,1%), μία αγορά την εβδομάδα.

Εικόνα 29: Ερωτηματολόγιο Συχνότητα Αγορών

Το (48%) των ερωτηθέντων διατηρεί λογαριασμό σε ένα μέσο κοινωνικής δικτύωσης, το (38%) σε 2 έως 3 μέσα κοινωνικής δικτύωσης, το (3%) σε 4-6 μέσα κοινωνικής δικτύωσης ενώ μόλις το (2%) σε πάνω από επτά μέσα κοινωνικής δικτύωσης. Αξιοσημείωτο είναι να αναφέρουμε ότι το (9%) δεν διατηρεί κανένα λογαριασμό σε μέσο κοινωνικής δικτύωσης.

Εικόνα 30: Ερωτηματολόγιο Αριθμός Λογαριασμών

Οι ερωτηθέντες που διατηρούν λογαριασμό σε μέσο κοινωνικής δικτύωσης αφιερώνουν αρκετό χρόνο καθημερινώς. Αυτό φαίνεται και από τα αποτελέσματα της παρακάτω ερώτησης όπου από τα 91 άτομα που διατηρούν έστω και ένα μέσο κοινωνικής δικτύωσης, τα 12 άτομα με ποσοστό (13,2%) αφιερώνουν πάνω από 7 ώρες την ημέρα, 4-6 ώρες την ημέρα αφιερώνουν 32 άτομα και ποσοστό (35,2%). Ακολούθως 31 άτομα αφιερώνουν 2-3 ώρες την ημέρα με ποσοστό (34,1%) ενώ 16 άτομα και ποσοστό (17, 6%) αφιερώνει λιγότερο από μία ώρα την ημέρα. Η συνολική διάρκεια συμπεριλαμβάνει και την παράλληλη λειτουργία των μέσων κοινωνικής δικτύωσης με άλλες εφαρμογές γι' αυτό και βλέπουμε ένα ποσοστό του (48,4%) να αφιερώνει πάνω από 4 ώρες την ημέρα.



Εικόνα 31: Ερωτηματολόγιο Καθημερινός Χρόνος Χρήσης Μ.Κ.Δ

Τέλος οι λόγοι για αυτούς που δεν διατηρούν καθόλου λογαριασμό σε μέσο κοινωνικής δικτύωσης (9 άτομα) είναι γιατί δεν βρίσκουν χρήσιμα τα μέσα κοινωνικής δικτύωσης 3 άτομα και ποσοστό (33,3%), γιατί δε θέλουν να εκθέτουν τα προσωπικά τους δεδομένα 3 άτομα και ποσοστό (33,3%) και λόγω έλλειψης προσωπικού ελεύθερου χρόνου 3 άτομα και ποσοστό (33,3%).

Εικόνα 32: Ερωτηματολόγιο Λόγοι μη χρήσης Μ.Κ.Δ

ΚΕΦΑΛΑΙΟ 6ο – ΣΥΖΗΤΗΣΗ & ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Συζήτηση

Σκοπός της παρούσας έρευνας ήταν η διερεύνηση της ασφαλούς ή μη χρήσης των προσωπικών δεδομένων στο διαδίκτυο από τους κατοίκους της Κύπρου. Επιπλέον διερευνήθηκε ο βαθμός και ο τρόπος με τον οποίο η προστασία των προσωπικών δεδομένων επηρεάζει τον τρόπο με τον οποίο οι Κύπριοι πολίτες χρησιμοποιούν το διαδίκτυο καθώς και η σκιαγράφηση του μέσου προφίλ των Κύπριων χρηστών του διαδικτύου.

6.1.1 Σκιαγράφηση μέσου προφίλ των Κύπριων χρηστών του διαδικτύου

Από τα 100 άτομα που συμπλήρωσαν το ερωτηματολόγιο οι 45 ήταν γυναίκες και οι 55 άντρες. Το μεγαλύτερο ποσοστό των συμμετεχόντων ανήκαν στις ηλικιακές ομάδες των 19-30 ετών (48%) και 31-45 ετών (27%) ενώ το (66%) των ερωτηθέντων είναι άγαμοι. Το επίπεδο εκπαίδευσης των ερωτηθέντων είναι πολύ υψηλό καθώς το (70%) είναι πτυχιούχοι Ανώτατης/Ανώτερης Εκπαίδευσης.
Η πλειοψηφία των συμμετεχόντων είναι μαθητές/φοιτητές (37%) και ακολουθούν οι ιδιωτικοί υπάλληλοι σε ποσοστό (30%). Όσον αφορά στη μηνιαία μισθολογική κλίμακα το (50%) ανήκει στην κατηγορία των μέσου εισοδήματος (701 - 1500€), ενώ ακολουθούν τα χαμηλά εισοδήματα έως 700 € σε ποσοστό (30%). Τέλος η πλειοψηφία των συμμετεχόντων προέρχεται από την Επαρχία Αμμοχώστου λόγω της καταγωγής μου με ποσοστό (49%), ενώ ακολουθεί η επαρχία Λάρνακας με ποσοστό (22%).

6.1.2 Ασφαλής ή μη η χρήση των προσωπικών δεδομένων στο διαδίκτυο

Σύμφωνα με τα αποτελέσματα της ανάλυσης το (78%) των ερωτηθέντων απάντησε ότι δεν χρησιμοποιεί ισχυρό κωδικό πρόσβασης, που να συμπεριλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και άλλα σύμβολα. Σύμφωνα με τον Bob Lord, διευθυντή ασφάλειας πληροφοριών δήλωσε ότι «Σιγουρευτείτε ότι χρησιμοποιείτε έναν ισχυρό κωδικό πρόσβασης - τουλάχιστον 10 ή και περισσότερων χαρακτήρων με ανάμειξη κεφαλαίων και πεζών γραμμάτων, αριθμό και συμβόλων». Αυτό

βλέπουμε πως σχεδόν δεν υιοθετείτε καθόλου από τους Κύπριους πολίτες αφού μόλις 2 στους 10 το εφαρμόζουν.

Σε αντίστοιχη έρευνα που έγινε και σε αντίστοιχη ερώτηση διαπιστώνεται ότι ένα μεγάλο ποσοστό χρηστών χρησιμοποιεί το ονοματεπώνυμο του για κωδικό πρόσβασης, ενώ στην δεύτερη θέση με το δεύτερο μεγαλύτερο ποσοστό ήταν η αγαπημένη τους αθλητική ομάδα. Από την παρούσα έρευνα γίνεται εμφανής η τάση των χρηστών να χρησιμοποιούν ως κωδικό πρόσβασης πράγματα της καθημερινότητάς τους και προσωπικά τους στοιχεία με πρωταρχικό σκοπό να είναι ένας κωδικός που θυμούνται εύκολα αλλά το αρνητικό είναι ότι μπορεί να γίνει και εύκολα προσβάσιμος από τρίτους.

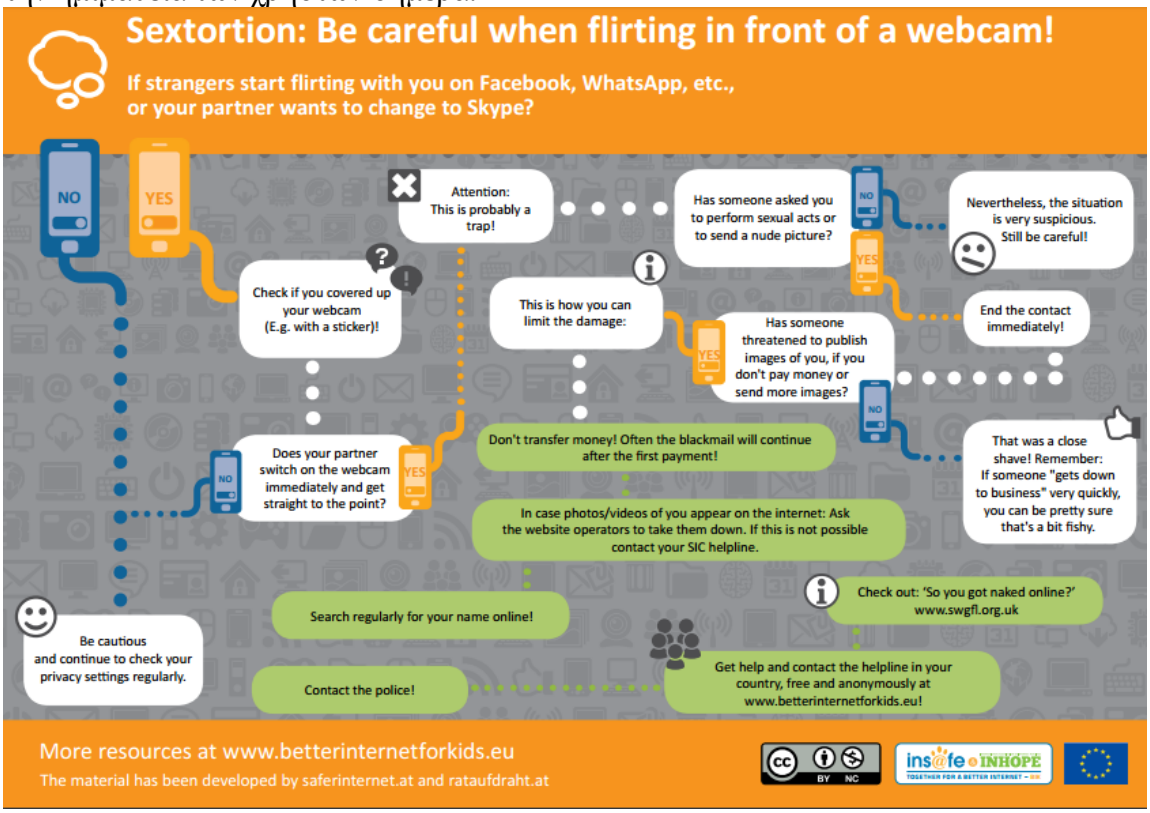
Σχετικά με το εάν αλλάζουν τακτικά τον κωδικό πρόσβασης το (73%) των ερωτηθέντων απάντησε ότι δεν τον αλλάζει τακτικά. Παρόμοια ήταν και τα αποτελέσματα μιας άλλης έρευνας με σκοπό την κατανόηση αν τα μέτρα προστασίας που παίρνουν οι χρήστες είναι επαρκή καθώς και για να διερευνηθεί κατά πόσο είναι ενήμεροι σε θέματα ασφαλείας των προσωπικών τους στοιχείων στο διαδίκτυο. Σε ερώτηση κατά πόσο αλλάζουν οι χρήστες τον κωδικό πρόσβασης βρέθηκε ότι το (50%) των ερωτηθέντων δεν αλλάζει τακτικά τον κωδικό πρόσβασης. Αυτό δείχνει ότι το κοινό δεν γνωρίζει ή δεν κατανοεί τους κινδύνους που ενέχει η αλόγιστη και λανθασμένη χρήση του διαδικτύου και των διαφόρων ιστοσελίδων με αποτέλεσμα να μην θεωρεί σκόπιμη την αλλαγή των κωδικών πρόσβασης που έχει και των άλλων προσωπικών στοιχείων. Ως εκ τούτου στην εξαγωγή των αποτελεσμάτων διαπιστώθηκε ότι το (58%) των ερωτηθέντων δε χρησιμοποιεί ξεχωριστό κωδικό πρόσβασης για κάθε λογαριασμό που διαθέτει.

Από τα αποτελέσματα φαίνεται επίσης ότι οι ερωτηθέντες δεν κρατούν μυστικό τον κωδικό πρόσβασης σε ποσοστό (53%) ενώ το υπόλοιπο (47%) κρατάει μυστικό τον κωδικό πρόσβασης στους λογαριασμούς, γεγονός που δείχνει την ανασφάλεια που αισθάνεται ένα μεγάλο ποσοστό χρηστών του διαδικτύου. Είναι πολύ σημαντικό να γνωρίζουμε μόνο εμείς τον προσωπικό μας κωδικός πρόσβασής για να μειώνονται και οι πιθανότητες κακόβουλης ζημιάς από άλλους χρήστες.

Παρόμοια ήταν και τα αποτελέσματα παρόμοιας έρευνας του εξωτερικού, όπου ένας στους δύο χρήστες (46%) απάντησε ότι έχει αποκαλύψει τον κωδικό του πρόσβασης σε τρίτα άτομα. Το γεγονός αυτό υποδεικνύει ότι οι χρήστες δεν αντιλαμβάνονται

πλήρως τη σημασία της μυστικότητας του κωδικού τους αφού 5 στους 10 έχουν μοιραστεί τον προσωπικό τους κωδικό με άλλο άτομο και ο καθένας διαφορετικά.

Όσον αφορά την ερώτηση για το εάν προσπάθησε ποτέ κάποιος τρίτος να χρησιμοποιήσει προσωπικά δεδομένα όπως φωτογραφίες, βίντεο, κωδικούς πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών-e banking κ.α., χωρίς την άδεια των ερωτηθέντων το μεγαλύτερο ποσοστό απάντησε όχι (79%) ενώ ένα σημαντικό ποσοστό (21%) απάντησε θετικά. Τα αποτελέσματα έρευνας που πραγματοποιήθηκε σχετικά πρόσφατα έδειξαν ότι η συντριπτική πλειοψηφία με ποσοστό (90%) δήλωσε πως δεν έχει πέσει θύμα απάτης ποτέ, ενώ το (10%) απάντησε θετικά. Η διακύμανση του (11%) οφείλεται στο ότι λόγω της οικονομικής κρίσης η αύξηση των επιτήδειων έχει γίνει καθημερινό φαινόμενο αφού κάποιος γνωρίζοντας μόνο το ονοματεπώνυμο κάποιου και την ημερομηνία γέννησης του χωρίς ιδιαίτερες γνώσεις από υπολογιστές, μπορεί να έχει πρόσβαση στους λογαριασμούς του. Σε αντίστοιχες δραστηριότητες/ασκήσεις που είχαν στο εξωτερικό κατάφεραν να έχουν πρόσβαση σε πάρα πολλά προσωπικά δεδομένα του εκάστοτε ατόμου μόνο μέσα από ένα πολύ σύντομο διάλογο που είχαν, πράγμα που φανερώνει την ημιμάθεια των χρηστών σήμερα.



Εικόνα 33: Μεταφορά πληροφορίας και προσωπικών δεδομένων μέσω της φωτογραφικής του υπολογιστή μας

Όσον αφορά στα 21 άτομα της έρευνάς μας που απάντησαν ότι έπεσαν θύματα υποκλοπής προσωπικών δεδομένων οι 11 το ανέφεραν στην Δίωξη Ηλεκτρονικού Εγκλήματος ή στην Αστυνομία ενώ οι άλλοι 10 όχι. Επιπλέον όσοι είχαν πέσει θύματα υποκλοπής προσωπικών δεδομένων από τρίτους, χρησιμοποιήθηκαν κυρίως για ηλεκτρονική αγορά υπηρεσιών σε ποσοστό (80,9%) ενώ για εξαπάτηση τρίτων σε ποσοστό (19,1%). Το αρνητικό για την Κύπρο είναι ότι δεν δίνεται η πρέπουσα σημασία στην προστασία των προσωπικών δεδομένων από την αστυνομία και είναι και ένα παράπονο που μου εξέφρασαν κατά την διάρκεια του ερωτηματολογίου αφού η χώρα μας υστερεί αρκετά σε αυτό το κομμάτι αφού ελάχιστε υποθέσεις εξιχνιάζονται.

Όσον αφορά στις online αγορές υπηρεσιών και προϊόντων διαπιστώθηκε ότι (69%) των ερωτηθέντων πραγματοποιεί αγορές μέσω διαδικτύου ενώ το (31%) απάντησε ότι δεν πραγματοποιεί. Σε μια παρόμοια έρευνα βρέθηκαν αντίστοιχα αποτελέσματα όπου οι κυριότεροι λόγοι για τους οποίους οι χρήστες του διαδικτύου αποφεύγουν να πραγματοποιούν συναλλαγές/αγορές μέσω διαδικτύου αφορούν την έλλειψη ελέγχου σχετικά με τα προϊόντα και τις υπηρεσίες (52,3%) και η προστασία των προσωπικών τους δεδομένων (48,1%).

Το τελευταίο κομμάτι του ερωτηματολογίου αφορούσε τη χρήση των μέσων κοινωνικής δικτύωσης, το αριθμό των λογαριασμών που διατηρούν, τη συχνότητα χρήσης τους, εάν υπήρχαν κάποιοι που δεν έχουν κάπου λογαριασμό και τους λόγους για τους οποίους δεν διατηρούν λογαριασμό σε κάποιο μέσο δικτύωσης. Το (48%) των ερωτηθέντων διατηρεί λογαριασμό σε ένα μέσο κοινωνικής δικτύωσης, το (38%) σε 2 έως 3 μέσα κοινωνικής δικτύωσης, το (3%) σε 4-6 μέσα κοινωνικής δικτύωσης ενώ μόλις το (2%) σε πάνω από επτά μέσα κοινωνικής δικτύωσης. Όσον αφορά στο χρόνο που αφιερώνουν στα μέσα κοινωνικής δικτύωσης το (13,2%) και (35,2%) των ερωτηθέντων αφιερώνουν πάνω από 7 ώρες την ημέρα και 4-6 ώρες την ημέρα, αντίστοιχα. Το (34,1%) αφιερώνει 2-3 ώρες την ημέρα, ενώ το (17,7%) αφιερώνει λιγότερο από μία ώρα την ημέρα.

6.2 Συμπεράσματα

Σύμφωνα με τα πειραματικά αποτελέσματα της έρευνας διαπιστώθηκε το μεγαλύτερο ποσοστό των Κύπριων χρηστών του διαδικτύου δεν έχουν πλήρη επίγνωση της σοβαρότητας του κωδικού πρόσβασης δεδομένου ότι το μεγαλύτερο ποσοστό δεν χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης και δεν τους αλλάζει τακτικά καθώς επίσης και από το γεγονός ότι αρκετά συχνά τους αποκαλύπτουν σε τρίτους. Αποτέλεσμα της μη ορθής επιλογής του κωδικού πρόσβασης είναι το γεγονός ότι 2 στους 10 Κύπριους έπεσε θύμα υποκλοπής προσωπικών δεδομένων.

Υπάρχουν βέβαια και χρήστες οι οποίοι έχουν πλήρη επίγνωση της σοβαρότητας του κωδικού αφού δεν πραγματοποιεί ούτε αγορές μέσω διαδικτύου έστω και αν οι μεγαλύτερες σελίδες πώλησης αγαθών χρησιμοποιούν SSL κρυπτογράφηση. Κυριότερη αιτία είναι η ανασφάλεια που αισθάνονται για το γεγονός ότι εκθέτουν τα προσωπικά τους δεδομένα μέσω αυτών.

Παρόμοια εικόνα παρουσιάζεται και στις ερωτήσεις σχετικά με τα μέσα κοινωνικής δικτύωσης όπου το 91% διατηρεί από 1-7 λογαριασμούς ενώ μόλις το 9% δεν διατηρηθεί κανένα λογαριασμό γιατί δεν αισθάνονται ασφαλής σχετικά με την έκθεση των προσωπικών τους δεδομένων σε τρίτους είτε λόγω έλλειψης ελεύθερου χρόνου.

Μέσα από πολυάριθμες μελέτες γίνεται λοιπόν σαφές η ανησυχία των χρηστών του διαδικτύου αναφορικά με το ζήτημα της προστασίας των προσωπικών δεδομένων. Ως εκ τούτου τα πλεονεκτήματα του διαδικτύου υπερτερούν του φόβου αυτού με συνέπεια οι χρήστες του διαδικτύου να εξακολουθούν να το χρησιμοποιούν, καταχωρώντας έως έναν βαθμό τα προσωπικά τους δεδομένα προκειμένου να επωφεληθούν από τις υπηρεσίες του.

Είναι γεγονός όμως ότι το ζήτημα της προστασίας των προσωπικών δεδομένων αφορά ένα υπαρκτό πρόβλημα στο ευρύτερο χώρο του διαδικτύου. Η θετική μεταβολή της τεχνολογίας και των τεχνικών πρόσβασης στα δεδομένα που καταχωρούνται, αυξάνει με πολύ γοργούς ρυθμούς και τον κίνδυνο παράνομης ή καταχρηστικής επεξεργασίας τους απειλώντας όλο και περισσότερο τους χρήστες του διαδικτύου. Ως επί το πλείστον οι νόμοι και οι τεχνικές προστασίας ακολουθούν τις

τεχνολογικές αναπτύξεις που αφορούν την διαχείριση των προσωπικών δεδομένων στο διαδίκτυο, ενώ τα οικονομικά οφέλη που συνοδεύουν τις δραστηριότητες αυτές είναι τεράστια.

6.3 Προτάσεις – Βελτιώσεις

Μέσα από αυτήν την έρευνα βγήκαν αρκετά χρήσιμα συμπεράσματα που αφορούν τους Κύπριους χρήστες του διαδικτύου και το πώς αυτοί συμπεριφέρονται την σημερινή εποχή διαδικτυακά.

Στόχος λοιπόν είναι ο εκσυγχρονισμός των νόμων και των πρακτικών καθώς και η επιβολή κανόνων λειτουργίας του διαδικτύου με στόχο την προστασία των προσωπικών δεδομένων των χρηστών του καθώς και των ανεπιθύμητων παρενεργειών της κατάστασης αυτής.

Οι Κύπριοι πολίτες και γενικά όλοι οι πολίτες πρέπει να κατανοήσουν ότι με την ορθή χρήση του διαδικτύου τα πλεονεκτήματα είναι πολύ περισσότερα από τα μειονεκτήματα και είναι στο χέρι του κάθε ενός από εμάς να προστατεύσει τον εαυτό του και να μην εκθέτει τα προσωπικά του δεδομένα διαδικτυακά.

Περιττεύει να υπογραμμίσω την σημασία αυτών των στοιχείων γιατί η παρούσα δομή του συστήματος αυτού μας υποχρεώνει να προσδιορίσουμε και να καθορίσουμε τις νέες τάσεις και κατευθύνσεις απέναντι στην πρόκληση των καιρών.

Στο μέλλον οι κακόβουλοι χρήστες θα είναι ακόμη περισσότεροι και εξοπλισμένοι με ακόμα πιο σύγχρονες τεχνολογικές μεθόδους για αυτό θα ήταν σωστό να ευαισθητοποιηθεί ακόμα περισσότερο ο κόσμος γύρω από τα προσωπικά δεδομένα, να μάθει τα δικαιώματα και τις υποχρεώσεις του γιατί μπορεί όλοι κάποτε να βρεθούμε σε αυτήν την δυσάρεστη θέση.

ΒΙΒΛΙΟΓΡΑΦΙΑ (ΑΓΓΛΙΚΗ)

1. http://m.hcamag.com/hr-news/why-hr-is-critical-in-cybersecurity-228188.aspx
2. http://whatis.techtarget.com/definition/cybersecurity
3. https://en.wikipedia.org/wiki/Privacy
4. https://en.wikipedia.org/wiki/Digital_privacy
5. http://www.digitalresponsibility.org/digital-prviacy/
6. http://www.igi-global.com/dictionary/digital-privacy/46799
7. http://www.oecd.org/
8. http://www.huffingtonpost.com/news/online-privacy/
9. IPC 2012. Identity Theft: A Crime of Opportunity. Practical information about identity theft, how to avoid it, and what to do if you find you are a victim.
10. http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329
11. https://www.extremetech.com/internet/180485-the-ultimate-guide-to-staying-anonymous-and-protecting-your-privacy-online
12. PayPal: Privacy Policy https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/securitycenter/general/RecognizePhishing-outside.
13. Ebay Policies: http://pages.ebay.com/help/policies/overview.html
14. https://www.facebook.com/policies
15. http://blog.tcitechs.com/blog/how-to-secure-your-computer/
16. Zhang, Y., Egelman, S., Cranor, L., Hong, J. 2007: Phinding phish: Evaluating anti-phishing tools. In: Proceedings of the 14th Annual Network and Distributed System Security Symposium
17. http://www.allaboutcookies.org/cookies/
18. http://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp
19. https://en.wikipedia.org/wiki/Anonymous_remailer
20. https://www.lifewire.com/find-remailer-to-send-anonymous-email-1170960
21. https://www.google.com.cy/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjlsPmD8ufQAhUDwxQKHUsDAhkQFggkMAE&url=http%3A%2F%2Fwww.ipc.nsw.gov.au%2Fprivacy-protocols&usg=AFQjCNGQO-uoXv5MZElr3zgCn-Lti-mDXg&bvm=bv.141320020,d.d24

22. https://www.w3.org/Security/

23. http://www.isdecisions.com/blog/it-security/prevent-insider-threats-from-both-malicious-and-careless-activity/

24. http://www.news.com.au/technology/internet-explorer-flaw-browse-at-your-own-risk/news-story/bd7362b14dd0e3139c7d302f9575b886

25. http://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

26. http://www.echr.coe.int/Documents/Convention_ELL.pdf

27. https://www.eff.org/nsa-spying/how-it-works

ΒΙΒΛΙΟΓΡΑΦΙΑ (ΕΛΛΗΝΙΚΗ)

1. http://www.huffingtonpost.gr/2016/12/07/tech-top10-apps-2016-apple_n_13479766.html?utm_source=Contra&utm_medium=huffpost_homebig&utm_campaign=24MediaWidget
2. http://nicosiapress.com/2016/12/06/mono-toso-chrono-chriazonte-i-chaker-gia-na-spasoun-tis-pistotikes-sas/
3. http://nicosiapress.com/2016/12/06/social-media-enonoun-tis-dynamis-tous-kata-tis-tromokratias/
4. http://www.cylaw.org/nomoi/indexes/2001_1_138.html
5. http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/legislation_gr/legislation_gr?OpenDocument
6. https://el.wikipedia.org/wiki/%CE%9F%CF%81%CE%B3%CE%B1%CE%BD%CE%B9%CF%83%CE%BC%CF%8C%CF%82_%CE%9F%CE%B9%CE%BA%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%AE%CF%82_%CE%A3%CF%85%CE%BD%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%BA%CE%B1%CE%B9_%CE%91%CE%BD%CE%AC%CF%80%CF%84%CF%85%CE%BE%CE%B7%CF%82
7. http://www.sakkoulas.gr/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=1015&category_id=112&option=com_virtuemart&Itemid=118
8. http://www.techgear.gr/1-to-8-users-do-not-believe-in-cyber-threats-93821/
9. http://internet-safety.sch.gr/
10. https://gelkvproject2011.wordpress.com/2011/10/03/%CE%B4%CE%B7%CE%BC%CE%B9%CE%BF%CF%85%CF%81%CE%B3%CE%AF%CE%B1-%CE%B5%CF%81%CF%89%CF%84%CE%B7%CE%BC%CE%B1%CF%84%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%BF%CF%85/.
11. Ευρωπαϊκό Κοινοβούλιο, 2012/0010(COD), άρθρο 3(9). http://www.parliament.gr/UserFiles/e04622a9-2024-47fe-a2f4-dd557cef2882/COM%20(2012)%2010%20Final.pdf
12. http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:52011XX0721(01)
13. http://osarena.net/tutorials/packet-sniffing-klepste-dedomena-se-dimosia-wifi-spots.html

14. https://el.wikipedia.org/wiki/%CE%9C%CE%AD%CF%83%CE%B1_%CE%BA%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AE%CF%82_%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CF%83%CE%B7%CF%82

15. http://www.socialmedialife.gr/110286/social-media-sxoleio/

16. http://www.biblionet.gr/book/186197/%CE%A7%CF%81%CE%B9%CF%83%CF%84%CE%BF%CE%B4%CE%BF%CF%8D%CE%BB%CE%BF%CF%85,_%CE%9A%CF%89%CE%BD%CF%83%CF%84%CE%B1%CE%BD%CF%84%CE%AF%CE%BD%CE%BF%CF%82_%CE%9D./%CE%94%CE%AF%CE%BA%CE%B1%CE%B9%CE%BF_%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CF%8E%CE%BD_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD

17. http://gym-leptok.pie.sch.gr/efivon-apopseis/index.php/koinonika/25-pseytikoi-i-alithinoi-oi-filoi-sta-mesa-koinonikis-diktyosis-boroyme-na-stirixtoyme-s-aftoys-otan-tous-exoume-anagki

18. http://www.enastron.com.gr/%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1/

19. Μελέτη τεχνικών ανωνυμίας στο διαδίκτυο και τρόποι που αυτές εντάσσονται στην ασφάλεια πληροφοριακών συστημάτων, Κατσάνος Σ. 2015.

20. Ασύρματα οικιακά δίκτυα στην Κύπρο και ποιά η ασφάλεια τους. ΤΕ.ΠΑ.Κ Τμήμα Επικοινωνίας και Σπουδών Διαδικτύου

21. http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#1

22. https://el.wikipedia.org/wiki/%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1

23. http://www.inewsgr.com/96/poia-einai-ta-evaisthita-prosopika-dedomena-kai-poia-ta-katochyromena-dikaiomata-mas.htm

24. http://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32002L0058&from=EL

25. https://en.wikipedia.org/wiki/Computer_hardware

26. http://www.sigmalive.com/personal-data-policy

27. http://osarena.net/faqs/ti-ine-i-steganografia-pou-ke-pos-tin-chrisimopioume.html

28. http://www.bankofcyprus.com/el-GR/--/Terms-Conditions_gr/

29. http://www.police.gov.cy/police/police.nsf/All/6C0099EB04B333C2C2257E750019FB0B

30. http://www.police.gov.cy/police/police.nsf/All/42956AEC03E8025DC22578A900271F4A?OpenDocument

31. http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414

32. https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/ilektroniko-egklima

33. https://www.lawspot.gr/nomika-nea/nomimi-i-apothikeysi-prosopikon-dedomenon-ton-episkepton-se-istoselides-symfona-me

34. http://cyprustimes.com/2016/11/11/prosochi-ilektroniko-minyma-apati-sto-diadiktyo-theti-se-kindyno-prosopika-dedomena/

35. http://www.karagiannislawfirm.gr/poiniko-dikaio/613-prostasia-prosopikon-dedomenon

36. https://www.google.com/intl/el/policies/privacy/

37. https://www.google.com/intl/el/policies/privacy/#nosharing

38. https://www.torproject.org/

39. http://www.sigmalive.com/news/scitech/technology/387003/nea-allagi-sto-facebook-ala-snapchat

40. www.philenews.com%2Fel-gr%2Feidiseis-technologia%2F53%2F341508%2Fto-facebook-ypochorei-sti-logokrisia-gia-na-kataktisei-tin-kina&usg=AFQjCNFxREk5iDK4A_hWYRDAZBsS3gE46w&bvm=bv.141320020,d.d24

Παράρτημα Α Ακρωνύμια – Συντομογραφίες

0-9		
A		
B		
C		
D		
E		
F	**FB**	Facebook
G		
H		

I	**IP**	Internet Protocol
J		
K		
L		
M		
N	**NSA**	National Security Agency
O	**OECD**	Organization for Economic Co-operation and Development
P	**PNR**	Passenger Name Record
	PETs	Privacy-Enhancing Technologies

Q

R

S

T

TCP	Transmission Control Protocol
TTP	Trusted Third Party
TOR	The Onion Router

U

V

W

WWW	WORLD WIDE WEB

X

Y

Z

Παράρτημα Β Ερωτηματολόγιο

Μέρος Α. Δημογραφικά Χαρακτηριστικά

1. Φύλο:

☐ Άντρας

☐ Γυναίκα

2. Ηλικία:

☐ <18 ετών

☐ 19-30 ετών

☐ 31-45 ετών

☐ 46-60 ετών

☐ >61 ετών

3. Οικογενειακή Κατάσταση

☐ Έγγαμος/η

☐ Άγαμος /η

4. Μορφωτικό Επίπεδο

☐ Δημοτικό

☐ Γυμνάσιο

☐ Λύκειο

☐ Ανώτατη/Ανώτερη Εκπαίδευση

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

5. Επάγγελμα

- ☐ Ιδιωτικός Υπάλληλος
- ☐ Δημόσιος Υπάλληλος
- ☐ Άνεργος
- ☐ Μαθητής/φοιτητής
- ☐ Οικιακά
- ☐ Συνταξιούχος
- ☐ Άλλο

6. Μηνιαίο Εισόδημα

- ☐ Έως 700 €
- ☐ 701- 1500 €
- ☐ 1501-2500 €
- ☐ Πάνω από 2500 €

7. Τόπος Διαμονής

- ☐ Λευκωσία
- ☐ Λεμεσός
- ☐ Λάρνακα
- ☐ Πάφος
- ☐ Ελ.Αμμόχωστος

Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες

ΜΈΡΟΣ Β. Διερεύνηση ασφαλούς χρήσης προσωπικών δεδομένων στο διαδίκτυο

1. Χρησιμοποιείτε ισχυρό κωδικό πρόσβασης (δηλ. περιλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και άλλα σύμβολα) ;

☐ Ναι

☐ Όχι

2. Τι κωδικό πρόσβασης χρησιμοποιείται συνήθως στο διαδίκτυο;

☐ Ημερομηνία Γέννησης

☐ Ημερομηνία Ονομαστικής Γιορτής

☐ Αρ. Κινητού Τηλεφώνου

☐ Αρ. Δελτίου Ταυτότητας

☐ Άλλο _____

3. Αλλάζετε τακτικά τον κωδικό πρόσβασης;

☐ Ναι

☐ Όχι

4. Χρησιμοποιείται για κάθε λογαριασμό ξεχωριστό κωδικό πρόσβασης;

☐ Ναι

☐ Όχι

5. Κρατάτε τον κωδικό πρόσβασης μυστικό;

☐ Ναι

☐ Όχι

6. Χρησιμοποιείτε προσεκτικά τους δικτυακούς τόπους κοινωνικής δικτύωσης (αποδέχεστε μόνο άτομα που γνωρίζεται, δεν επιτρέπετε στις εφαρμογές που χρησιμοποιείται να έχουν χρήση των προσωπικών σας δεδομένων κ.α) ;

☐ Ναι

☐ Όχι

7. Προσπάθησε ποτέ κάποιος τρίτος να χρησιμοποιήσει προσωπικά σας δεδομένα χωρίς την άδεια σας; (φωτογραφίες, βίντεο, κωδικούς πιστωτικών καρτών, κωδικούς τραπεζικών λογαριασμών-e banking κ.α),;

☐ Ναι

☐ Όχι

7α. Αν ναι, το αναφέρατε ποτέ στην Δίωξη Ηλεκτρονικού Εγκλήματος ή στην Αστυνομία ?

☐ Ναι

☐ Όχι

7β. Πού χρησιμοποιήθηκαν τα προσωπικά σας δεδομένα (αγορά υπηρεσιών, εξαπάτηση τρίτων με τα στοιχεία μου, κ.α);

_____

_____

8. Πραγματοποιείς αγορές μέσω διαδικτύου;

☐ Ναι

☐ Όχι

Εάν όχι, γιατί;

_____

_____

8α. Αν ναι, πόσο συχνά αγοράζετε προϊόντα και υπηρεσίες μέσω διαδικτύου;

- ☐ 1 φορά την εβδομάδα
- ☐ 1 φορά τον μήνα
- ☐ 1 φορά κάθε έξι μήνες
- ☐ 1 φορά τον χρόνο
- ☐ Άλλο:

_____

9. Σε πόσα μέσα κοινωνικής δικτύωσης διατηρείται λογαριασμό;

- ☐ 0
- ☐ 1
- ☐ 2-3
- ☐ 4-6
- ☐ 7+

9α. Αν διατηρείται λογαριασμό πόσο χρόνο αφιερώνεται σε αυτό;

- ☐ >1 ώρα την ημέρα
- ☐ 2-3 ώρες την ημέρα
- ☐ 4-6 ώρες την ημέρα
- ☐ 7+ ώρες την ημέρα

9β. Αν δεν διατηρείται λογαριασμό προσδιορίστε τον λόγο:

- ☐ Δεν θέλω να εκθέτω τα προσωπικά μου δεδομένα (δεν νιώθω ασφαλής).
- ☐ Δεν βρίσκω χρήσιμα τα μέσα κοινωνικής δικτύωσης.
- ☐ Λόγω έλλειψης προσωπικού ελεύθερου χρόνου.
- ☐ Άλλο:

_____

ΤΕΛΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ