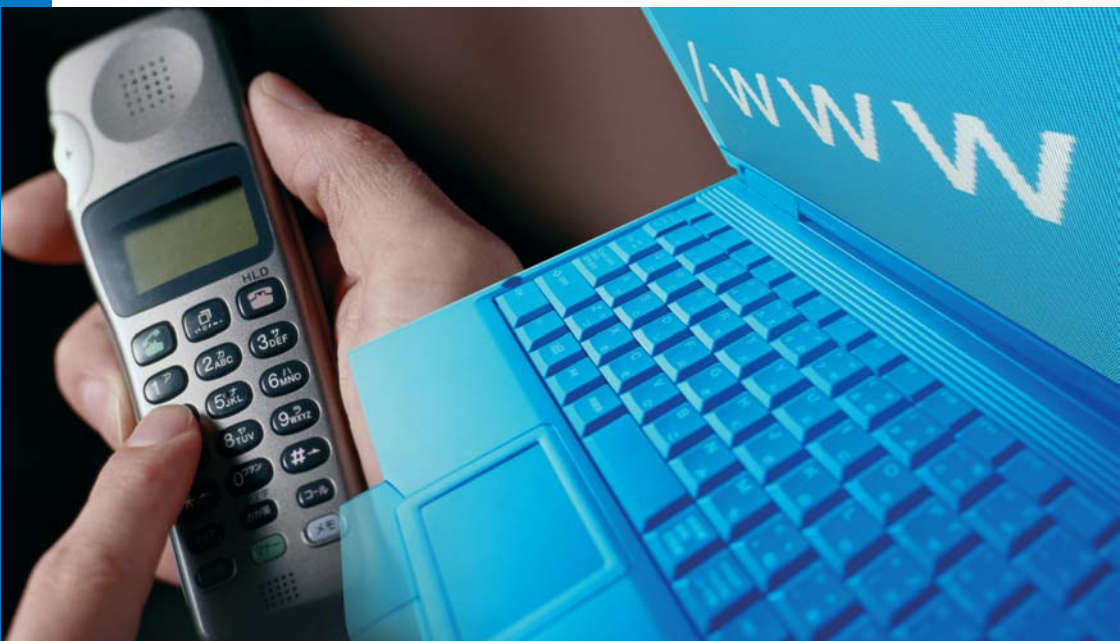




**ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ**

Χρήση του Διαδικτύου και των κινητών τηλεφώνων



**Μη δημοσιοποιείτε υπερβολικά προσωπικά
σας δεδομένα στο Διαδίκτυο.**

Δεν ξέρετε από ποιους και πώς μπορεί να χρησιμοποιηθούν

Δεν είστε ανώνυμοι στο Διαδίκτυο

Οι ενέργειές σας αφήνουν ίχνη

**Τα προσωπικά σας δεδομένα στο Διαδίκτυο μπορεί
να κλαπούν χωρίς να το γνωρίζετε**

**Τα περισσότερα κινητά τηλέφωνα διαθέτουν φωτογραφική
μηχανή και ο καθένας μπορεί να γίνει ερασιτέχνης παπαράτσι**

Περίληψη

Η χρήση του Διαδικτύου τα τελευταία χρόνια συνεχώς αυξάνεται και εμφανίζονται διαρκώς νέες τάσεις και νέοι τρόποι χρήσης του. Πολλά προσωπικά δεδομένα εκτίθενται σε εκατομμύρια σελίδες στις οποίες μπορεί να έχει πρόσβαση από οποιοδήποτε μέρος του κόσμου οποιοσδήποτε έχει σύνδεση στο Διαδίκτυο.

Πρέπει να μάθουμε να το χρησιμοποιούμε σωστά ώστε να επωφελούμαστε από τις υπηρεσίες που μπορεί να μας παρέχει χωρίς να εκθέτουμε τα προσωπικά μας δεδομένα και να θέτουμε σε κίνδυνο την ιδιωτική μας ζωή.

Προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία που αναφέρεται σε κάποιο πρόσωπο που μπορεί να αναγνωριστεί. Προσωπικά δεδομένα είναι και οι φωτογραφίες.

Μην δημοσιοποιείτε υπερβολικά προσωπικά σας δεδομένα στο Διαδίκτυο. Δεν ξέρετε από ποιους και πώς μπορεί να χρησιμοποιηθούν

Αρκετοί χρήστες δημοσιοποιούν πολλά προσωπικά τους δεδομένα σε προσωπικές τους ιστοσελίδες στο Διαδίκτυο χωρίς να γνωρίζουν από ποιους και πώς μπορούν να χρησιμοποιηθούν. Οποιοσδήποτε μπορεί να βλέπει τα στοιχεία αυτά όπως οι γονείς τους, άτομα που τους ζηλεύουν, ή ακόμη και εγκληματίες με σκοπό κλοπής της ταυτότητας τους (identity theft).

Σε μερικές περιπτώσεις ακόμη και αν διαγράψουν κάποια στοιχεία από την ιστοσελίδα τους, τα στοιχεία αυτά μπορεί να είναι ακόμη διαθέσιμα στο Διαδίκτυο μέσω αντιγράφων που διατηρούν ορισμένες μηχανές αναζήτησης του Διαδικτύου (search engines).

Δεν είστε ανώνυμοι στο Διαδίκτυο. Οι ενέργειες σας αφήνουν ίχνη

Αρκετοί πιστεύουν ότι στο Διαδίκτυο είναι ανώνυμοι και ότι δεν αποκαλύπτονται τα προσωπικά τους δεδομένα, αλλά στην πραγματικότητα οι ενέργειες μας στο Διαδίκτυο αφήνουν ίχνη τα οποία σε ορισμένες περιπτώσεις μπορούν να χρησιμοποιηθούν για αναγνώριση μας. Σε κάθε επίσκεψη μας σε κάποια ιστοσελίδα καταγράφεται η διεύθυνση IP του υπολογιστή μας και μπορεί επίσης να τοποθετηθούν στον υπολογιστή μας μικρά αρχεία που ονομάζονται cookies από διάφορες ιστοσελίδες που έχουμε επισκεφθεί, τα οποία σε μερικές περιπτώσεις μπορεί να χρησιμοποιηθούν για παρακολούθηση των κινήσεων μας στο Διαδίκτυο.

Τα προσωπικά σας δεδομένα στο Διαδίκτυο μπορεί να κλαπούν χωρίς να το γνωρίζετε

Τον τελευταίο καιρό έχουν αυξηθεί οι κίνδυνοι κλοπής των προσωπικών δεδομένων στο Διαδίκτυο.

Τα προγράμματα spyware που μπορεί να εγκατασταθούν στον υπολογιστή κάποιου χρήστη μέσω κάποιου ιού ή μαζί με κάποιο άλλο δωρεάν πρόγραμμα μαζεύουν διάφορα προσωπικά δεδομένα του χρήστη και τα αποστέλλουν στο Διαδίκτυο. Συχνά αποστέλλονται διάφορα πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου (email) που προσπαθούν να ξεγελάσουν τους χρήστες ώστε να δώσουν τους κωδικούς πρόσβασης που διαθέτουν για διάφορες υπηρεσίες του Διαδικτύου (Phishing). Υπάρχουν και αρκετές απάτες όπως για παράδειγμα περιπτώσεις όπου οι χρήστες λαμβάνουν κάποιο email που γράφει ότι έχουν κερδίσει σε κάποιο λαχείο αλλά για να λάβουν τα κέρδη θα πρέπει να πληρώσουν κάποια έξοδα μεταφοράς των χρημάτων.

Τα περισσότερα κινητά τηλέφωνα διαθέτουν φωτογραφική μηχανή και ο καθένας μπορεί να γίνει ερασιτέχνης παπαράτσι

Απαγορεύεται να βγάλετε φωτογραφία ή βίντεο κάποιο άτομο χωρίς πρώτα να λάβετε την συγκατάθεση του. Ακόμα και αν πάρετε συγκατάθεση για τη φωτογράφιση,



απαιτείται επιπρόσθετα και η λήψη συγκατάθεσης και για κοινοποίηση ή δημοσίευση των φωτογραφιών και των βίντεο. Στην Κύπρο υπήρξαν πολλές περιπτώσεις όπου φωτογραφίες και βίντεο που είχαν ληφθεί από κινητά τηλέφωνα είχαν σταλεί από κινητό σε κινητό με αποτέλεσμα να κυκλοφορήσουν σε χρόνο ρεκόρ σε ολόκληρη την Κύπρο.

Εισηγήσεις

Μην αποκαλύπτετε στις προσωπικές σας ιστοσελίδες υπερβολικά προσωπικά σας δεδομένα. Να είστε ιδιαίτερα προσεκτικοί σε ποιους κοινοποιείτε τα προσωπικά σας δεδομένα στο Διαδίκτυο. Εγκαταστήστε στον υπολογιστή σας κάποιο Firewall και κάποιο πρόγραμμα που να εντοπίζει τα προγράμματα Spyware.

Μη βγάζετε φωτογραφίες (ή βίντεο) με το κινητό σας τηλέφωνο χωρίς συγκατάθεση και μην τις κοινοποιείτε στο Διαδίκτυο ή σε φίλους σας χωρίς συγκατάθεση των ατόμων που παρουσιάζονται σ' αυτές.

Για περισσότερες πληροφορίες και μέτρα προστασίας σχετικά από τους πιο πάνω κινδύνους διαβάστε τις οδηγίες που ακολουθούν.

1. Κίνδυνοι από δημοσίευση των προσωπικών μας δεδομένων

Η χρήση του Διαδικτύου τα τελευταία χρόνια συνεχώς αυξάνεται και εμφανίζονται διαρκώς νέες τάσεις και νέοι τρόποι χρήσης του. Πολλά προσωπικά δεδομένα εκτίθενται σε εκατομμύρια σελίδες στις οποίες μπορεί να έχει πρόσβαση από οποιοδήποτε μέρος του κόσμου οποιοσδήποτε έχει σύνδεση στο Διαδίκτυο.

Πρέπει να μάθουμε να το χρησιμοποιούμε σωστά ώστε να επωφελούμαστε από τις υπηρεσίες που μπορεί να μας παρέχει χωρίς να δημοσιοποιούμε χωρίς λόγο τα προσωπικά μας δεδομένα και να θέτουμε σε κίνδυνο την ιδιωτική μας ζωή.

1.1. Blogging

Πρόσφατα παρατηρούνται αρκετές νέες τάσεις στο Διαδίκτυο όπου οι χρήστες δημοσιοποιούν πολλά προσωπικά τους δεδομένα χωρίς να γνωρίζουν τους κινδύνους που πιθανόν να προκαλέσει αυτή η ενέργεια τους.

Μια από αυτές τις τάσεις είναι το *blogging* όπου οι χρήστες του Διαδικτύου διατηρούν ημερολόγιο στο Διαδίκτυο (blog) όπου γράφουν διάφορες σκέψεις τους, διάφορα θέματα που τους απασχολούν, ή απλά τι κάνουν στην καθημερινή τους ζωή. Αυτή η ενέργεια τους όμως έχει συνήθως ως αποτέλεσμα να εκθέτουν πολλά προσωπικά τους δεδομένα χωρίς να γνωρίζουν από ποιους και πώς μπορούν να χρησιμοποιηθούν.

Αρκετοί έχουν την εντύπωση ότι το blog τους το διαβάζουν μόνο οι φίλοι τους, αλλά πολλές φορές το κοινό στο οποίο απευθύνονται είναι πολύ πιο μεγάλο από ότι υπολογίζουν. Οποιοσδήποτε μπορεί να το διαβάζει χωρίς αυτοί να το γνωρίζουν, όπως οι γονείς τους, άτομα που τους ζηλεύουν και θέλουν να τους κάνουν κακό ή ακόμη και εγκληματίες.

Αρκετές φορές αυτά που γράφει κάποιος στο Διαδίκτυο μπορεί να παρερμηνευτούν. Αν για παράδειγμα κάποιος γράψει ότι του άρεσε μια ταινία στην οποία γίνεται αναφορά στη χρήση ναρκωτικών μπορεί κάποιος να τον θεωρήσουν ως χρήστη ή πιθανόν μελλοντικό χρήστη ναρκωτικών.



Σε μια περίπτωση στο εξωτερικό μια κοπέλα που έγραφε σε blog τις πολιτικές τις απόψεις, έτυχε να αναφέρει στο blog της σε ποιο εστιατόριο θα πήγαινε το βράδυ και όταν έφτασε στο εστιατόριο συνάντησε εξαγριωμένους αναγνώστες του blog της οι οποίοι δεν συμφωνούσαν με τις πολιτικές τις απόψεις.

Είναι καλό να έχετε υπόψη ότι ακόμη και αν κάποιος διαγράψει κάποια στοιχεία από το blog που διατηρεί, δεν είναι σε θέση να γνωρίζει αν έχουν διαγραφεί εντελώς από το Διαδίκτυο, καθώς ορισμένες φορές πιθανόν να υπάρχουν αποθηκευμένα αντίγραφα σε μηχανές αναζήτησης (search engines) του Διαδικτύου που δεν γνωρίζουμε για πόσο καιρό ακριβώς διατηρούνται.

Προτού αρχίσετε να γράφετε σε blog θα πρέπει να σκεφτείτε τι είδους προσωπικά δεδομένα θα αποκαλύπτετε και πόσο κίνδυνο πιστεύετε ότι διατρέχετε από την αποκάλυψη των προσωπικών σας δεδομένων (π.χ. μια νεαρή κοπέλα διατρέπει περισσότερους κινδύνους παρενόχλησης από ότι ένας άντρας).

Εάν έχετε την τάση να αποκαλύπτετε πολλά προσωπικά δεδομένα θα ήταν καλό να χρησιμοποιήσετε κάποια υπηρεσία με την οποία να μπορείτε να προστατεύετε το blog σας με κωδικούς πρόσβασης, όπου πρόσβαση θα μπορούν να έχουν μόνο έμπιστοι φίλοι σας.

1.2. Social networking

Μια άλλη πολύ δημοφιλής τάση είναι η χρήση των ιστοσελίδων *social networking* όπως το MySpace και το Facebook όπου οι χρήστες δημιουργούν προσωπικές τους ιστοσελίδες όπου δημοσιεύουν τα ενδιαφέροντα τους και φωτογραφίες τους και μπορούν να συνδεθούν με άλλους χρήστες σε «δίκτυα» ή ομάδες κοινών ενδιαφερόντων.

Οι νεαροί κυρίως χρήστες του Διαδικτύου είναι ενθουσιασμένοι με αυτού του είδους τις ιστοσελίδες γιατί με αυτόν τον τρόπο μπορούν να παρουσιάσουν την προσωπικότητά τους και να γνωρίσουν άτομα με παρόμοια ενδιαφέροντα ή να έρθουν σε επαφή με παλιούς συμμαθητές από προηγούμενα σχολεία τους.

Ορισμένες από αυτές τις ιστοσελίδες επιτρέπουν την ανάγνωση των προσωπικών ιστοσελίδων των χρηστών μόνο σε μαθητές/φοιτητές του σχολείου τους (που έχουν διεύθυνση ηλεκτρονικού ταχυδρομείου με το ίδιο όνομα (domain) όπως για παράδειγμα ...@uccollege.com). Αυτό όμως δίνει την αίσθηση περισσότερης ασφάλειας και έχει ως αποτέλεσμα την αποκάλυψη περισσότερων προσωπικών δεδομένων αφού οι περισσότεροι χρήστες είναι με την εντύπωση πως ότι γράφουν στην ιστοσελίδα τους τα διαβιβάζουν μόνο οι συμμαθητές τους. Δεν υπολογίζουν όμως ότι μπορούν να έχουν πρόσβαση και καθηγητές τους, η διεύθυνση του σχολείου και απόφοιτοι του σχολείου οι οποίοι διαθέτουν ηλεκτρονική διεύθυνση με το ίδιο domain.

Και σε αυτού του είδους τις σελίδες υπάρχουν παρόμοιοι κίνδυνοι από την έκθεση υπερβολικών προσωπικών δεδομένων όπως και στο blogging.

Υπάρχουν αρκετές περιπτώσεις σε κολέγια στο εξωτερικό όπου φοιτητές δημοσίευσαν για πλάκα στις προσωπικές τους σελίδες φωτογραφίες από πάρτι όπου ήταν μεθυσμένοι ή έκαναν βανδαλισμούς και όταν ανακάλυψε τις φωτογραφίες η διεύθυνση του κολεγίου τους απέβαλε.



Ορισμένες από αυτές τις υπηρεσίες δίνουν στους χρήστες διάφορα επίπεδα προστασίας, όπως για παράδειγμα να καθορίζουν οι ίδιοι από ποιους θα είναι αναγνώσιμες οι προσωπικές τους ιστοσελίδες αλλά πολύ λίγοι από τους χρήστες επωφελούνται από αυτές τις δυνατότητες.

Προτού δημιουργήσετε μια τέτοια προσωπική ιστοσελίδα είναι καλό να διαβάσετε τους όρους παροχής της υπηρεσίας (terms and conditions) και την πολιτική ασφαλείας της ιδιωτικής ζωής (privacy policy) για να γνωρίζετε τι είδους προστασία παρέχει η συγκεκριμένη υπηρεσία που έχετε επιλέξει, ποιοι μπορούν να έχουν πρόσβαση στην προσωπική σας ιστοσελίδα και κατά πόσο τα προσωπικά σας δεδομένα θα κοινοποιούνται σε τρίτους.

2. Δεν είμαστε ανώνυμοι στο Διαδίκτυο

Αρκετοί πιστεύουν ότι στο Διαδίκτυο είναι ανώνυμοι και ότι δεν αποκαλύπτονται τα προσωπικά τους δεδομένα, αλλά στην πραγματικότητα οι ενέργειες μας στο Διαδίκτυο αφήνουν ίχνη τα οποία σε ορισμένες περιπτώσεις μπορούν να χρησιμοποιηθούν για αναγνώριση μας.

Ο κάθε υπολογιστής που είναι ενωμένος στο Διαδίκτυο έχει μια μοναδική διεύθυνση (η οποία είναι διαφορετική για τον κάθε υπολογιστή) η οποία ονομάζεται *IP address* (Internet Protocol address) η οποία σε μερικές περιπτώσεις μπορεί να χρησιμοποιηθεί για αναγνώριση του χρήστη που έχει προβεί σε κάποια ενέργεια.

Σε αρκετές ιστοσελίδες που επισκεπτόμαστε ο server της ιστοσελίδας τοποθετεί στον ηλεκτρονικό υπολογιστή μας μικρά αρχεία κειμένου (text files) τα οποία ονομάζονται *cookies*. Τα cookies χρησιμοποιούνται κυρίως για αναγνώριση μας από την ιστοσελίδα την επόμενη φορά που θα την επισκεφτούμε, αλλά συχνά χρησιμοποιούνται επίσης και για να παρακολουθούνται οι κινήσεις μας στο Διαδίκτυο ώστε να διαμορφώνεται το προφίλ των προτιμήσεων μας με σκοπό να εμφανίζονται διαφημίσεις που πιθανόν να βρούμε δελεαστικές.

Μπορείτε να ρυθμίσετε τον υπολογιστή σας να μην αποδέχεται τα cookies (αλλά με αυτόν τον τρόπο πιθανόν να μην μπορείτε να έχετε πρόσβαση σε αρκετές ιστοσελίδες) ή μπορείτε να διαγράψετε κατά διαστήματα από μόνοι σας τα cookies ή σε μερικές περιπτώσεις μπορείτε να ρυθμίσετε τον υπολογιστή σας να διαγράφει όλα τα cookies όταν τελειώσετε να χρησιμοποιείτε τον παγκόσμιο ιστό (World Wide Web).

Θα πρέπει πάντα να έχετε υπόψη σας ότι στο Διαδίκτυο δεν είστε ανώνυμοι και προτού προβείτε σε οποιαδήποτε ενέργεια στο Διαδίκτυο να σκέφτεστε τις πιθανές συνέπειες της.

3. Κλοπή προσωπικών δεδομένων

Τον τελευταίο καιρό έχουν αυξηθεί οι κίνδυνοι κλοπής των προσωπικών δεδομένων στο Διαδίκτυο όπως από προγράμματα που αποστέλλουν προσωπικά δεδομένα των χρηστών στο Διαδίκτυο χωρίς αυτό να είναι σε γνώση τους (Spyware), με την παραπλάνηση των χρηστών να δώσουν τα στοιχεία τους (Phishing) και με διάφορες απάτες.



3.1. Spyware



Spyware ονομάζονται τα προγράμματα που εγκαθίστανται στον ηλεκτρονικό υπολογιστή του χρήστη και μαζεύουν διάφορα προσωπικά δεδομένα του και τα αποστέλλουν στο Διαδίκτυο χωρίς αυτό να είναι σε γνώση του. Αυτά τα προγράμματα μπορεί να εγκατασταθούν στον υπολογιστή είτε μέσω κάποιου ιού (virus) είτε μαζί με κάποιο άλλο δωρεάν πρόγραμμα. Υπάρχουν διαφόρων ειδών προγράμματα *Spyware*.

Τα *Key-loggers* καταγράφουν όλα τα πατήματα πλήκτρων που κάνει ο χρήστης και με αυτόν τον τρόπο μαζεύουν διάφορα προσωπικά δεδομένα συμπεριλαμβανομένων και των κωδικών πρόσβασης των χρηστών σε υπηρεσίες στο Διαδίκτυο.

Άλλου είδους προγράμματα *Spyware* χρησιμοποιούνται για πρόσβαση στον ηλεκτρονικό υπολογιστή του χρήστη που έχει μολυνθεί με το πρόγραμμα *Spyware* (Remote Access). Όταν λάβουν τον έλεγχο του υπολογιστή κάποιου χρήστη (system hijacking) μπορούν για παράδειγμα να ελέγχουν τη βιντεοκάμερα του ή μπορούν να χρησιμοποιήσουν τον υπολογιστή του για αποστολή ανεπιθύμητων διαφημιστικών μηνυμάτων spam (zombie computers ή botnets).

Τα Spyware δεν εντοπίζονται από όλα τα προγράμματα Anti-Virus γι' αυτό είναι καλό να εγκαταστήσετε κάποιο πρόγραμμα που να εντοπίζει τα Spyware, όπως το Ad-aware ή το Spybot Search & Destroy. Είναι καλό επίσης να εγκαταστήσετε κάποιο firewall που να σας ειδοποιά όταν κάποιο πρόγραμμα προσπαθεί να στείλει δεδομένα στο Διαδίκτυο.

Μπορείτε να λάβετε περισσότερες πληροφορίες σχετικά με τα Spyware από την μελέτη του Ρυθμιστή Ταχυδρομείων και Ηλεκτρονικών Επικοινωνιών της Σουηδίας η οποία είναι γραμμένη στα Αγγλικά και είναι διαθέσιμη στο Διαδίκτυο στην διεύθυνση www.pts.se/Archive/Documents/EN/Spyware_eng.pdf.

3.2. Phishing και άλλοι κίνδυνοι



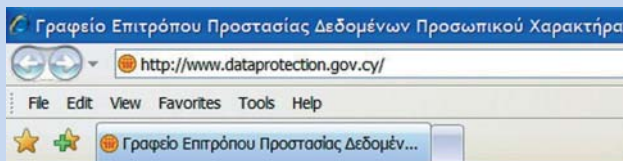
Phishing ονομάζεται η παραπλάνηση των χρηστών να δώσουν τα προσωπικά τους στοιχεία ή τους κωδικούς πρόσβασης τους, συνήθως σε κάποια πλαστή ιστοσελίδα στο Διαδίκτυο. Αρκετές φορές αποστέλλονται emails τα οποία περιέχουν σύνδεσμο (link) που παραπέμπει σε κάποια πλαστή ιστοσελίδα και καλούν τους χρήστες να πληκτρολογήσουν προσωπικά τους δεδομένα ή τους κωδικούς πρόσβασης τους.

Υπάρχουν και αρκετοί άλλοι κίνδυνοι όπως email-απάτες όπου οι χρήστες λαμβάνουν κάποιο email που γράφει ότι έχουν δέχθει κερδίσει σε κάποιο λαχείο αλλά για να λάβουν τα κέρδη θα πρέπει να αποστείλουν τα προσωπικά τους δεδομένα (συμπεριλαμβανομένων αρκετές φορές και αντίγραφο της ταυτότητας ή του διαβατηρίου τους) και να πληρώσουν κάποια έξοδα μεταφοράς των χρημάτων. Έτσι εκτός από το ότι οι απατεώνες είναι σε θέση να προβούν σε κλοπή της ταυτότητας τους, εισπράττουν επίσης και τα υποτιθέμενα έξοδα μεταφοράς των χρημάτων.

Γι' αυτό μην αποκαλύπτετε προσωπικές σας πληροφορίες εάν δεν είσατε σίγουροι για την ταυτότητα του αποδέκτη και τον πραγματικό σκοπό για τον

οποίο ζητούνται τα προσωπικά σας δεδομένα. Μπορείτε να πάρετε περισσότερες πληροφορίες σχετικά με το Phishing και τις διάφορες απάτες στο Διαδίκτυο από την ιστοσελίδα <http://www.fraudwatchininternational.com> ώστε να μην ξεγελαστείτε σε περίπτωση που λάβετε κάποιο από αυτά τα emails.

Μπορείτε να πάρετε περισσότερες πληροφορίες για τη χρήση Διαδικτύου και μέτρα προστασίας, από την οδηγία του Γραφείου Επιτρόπου Προστασίας Δεδομένων για το Διαδίκτυο η οποία είναι διαθέσιμη στην ιστοσελίδα του Γραφείου στη διεύθυνση <http://www.dataprotection.gov.com> στο μέρος «Νομοθεσία».



4. Κινητά τηλέφωνα

Σχεδόν όλα τα κινητά τηλέφωνα σήμερα διαθέτουν φωτογραφική μηχανή και μπορούν να λαμβάνουν εικόνες, βίντεο και ήχο. Αυτό είναι πολύ χρήσιμο ώστε να είμαστε σε θέση να καταγράφουμε ευχάριστες στιγμές διασκέδασης με φίλους ή με την οικογένεια μας, αλλά ταυτόχρονα απειλείται η ιδιωτική μας ζωή αφού ο καθένας τώρα μπορεί να γίνει ερασιτέχνης παπαράτσι.

Η εικόνα και ο ήχος αποτελούν προσωπικά δεδομένα όταν σχετίζονται με φυσικά πρόσωπα τα οποία μπορούν να αναγνωριστούν. Για να βγάλετε φωτογραφία, να βιντεογραφήσετε ή να ηχογραφήσετε κάποιο άτομο θα πρέπει πρώτα να λάβετε την συγκατάθεση του.

Στο εξωτερικό έχουν αναφερθεί περιπτώσεις όπου παιδιά χτυπούσαν συμμαθητές τους και βιντεογραφούσαν την πράξη αυτή για να τους γελοιοποιήσουν, αλλά τα βίντεο αυτά στράφηκαν εναντίον τους, αφού βοήθησαν στη σύλληψή τους.

Σε αρκετές χώρες στο εξωτερικό έχει απαγορευτεί η χρήση των κινητών τηλεφώνων που διαθέτουν φωτογραφική μηχανή σε αποδυτήρια και άλλους χώρους όπου ο καθένας αναμένει να έχει κάποιο επίπεδο προστασίας της ιδιωτικής του ζωής αλλά ακόμη και σε ανοιχτούς δημόσιους χώρους κινδυνεύει η ιδιωτική μας ζωή από κατόχους τέτοιων κινητών.

Φυσικά αρκετοί από εμάς έχουμε πολλές φορές βγάλει φωτογραφίες στην οποία φαίνονται και άλλα άτομα που έτυχε να βρίσκονται στον ίδιο χώρο. Αυτό δεν δημιουργεί πρόβλημα όταν χρησιμοποιούμε τις φωτογραφίες αποκλειστικά για προσωπική μας χρήση, αλλά δημιουργεί πρόβλημα όταν τις δημοσιεύσουμε στο Διαδίκτυο ή τις στείλουμε σε φίλους μας.

Αρκετές φορές άτομα που είχαν δει κάτι αστειό, έβγαλαν φωτογραφίες με το κινητό τηλέφωνο τους και τις δημοσίευσαν στο Διαδίκτυο ή τις έστειλαν με email σε φίλους τους, οι οποίοι με τη σειρά τους τις προώθησαν και σε άλλους φίλους τους με αποτέλεσμα να φέρνουν το άτομο της φωτογραφίας σε άσχημη θέση. Αυτή η ενέργεια εκτός από το ότι δεν είναι ηθικά σωστή είναι και παράνομη. Σε τέτοιες περιπτώσεις το άτομο που είχε βγάλει τις φωτογραφίες θα μπορούσε



τουλάχιστον να καλύψει το πρόσωπο και άλλα χαρακτηριστικά σημάδια όπως τατουάζ ή ουλές από τα οποία μπορεί να αναγνωριστεί το συγκεκριμένο άτομο της φωτογραφίας για σεβασμό προς την ιδιωτική του ζωή και τα προσωπικά του δεδομένα.

Αρκετοί θα έχουν δει τα βίντεο «Starwars kid» και «Numa Numa Dance» τα οποία έχουν δημοσιευτεί σε διάφορες ιστοσελίδες με αστεία βίντεο στο Διαδίκτυο όπως το Metacafe και το YouTube και μέσα σε μερικές εβδομάδες τα είχαν παρακολουθήσει εκατομμύρια χρήστες του Διαδικτύου σε όλο τον κόσμο. Αν και ορισμένοι πιθανόν να ήθελαν να γίνουν διασημότητες, οι περισσότεροι από εμάς δεν θα θέλαμε να καταλήξουμε θέαμα στο Διαδίκτυο.

Στην Κύπρο υπήρξαν περιπτώσεις όπου διάφορα βίντεο είχαν κοινοποιηθεί χωρίς τη συγκατάθεση των ατόμων που παρουσιάζονται σ' αυτά, αποστέλλοντας τα από κινητό σε κινητό με αποτέλεσμα να κυκλοφορήσουν σε χρόνο ρεκόρ σε ολόκληρη την Κύπρο, χωρίς να σκεφτεί κανένας τις συνέπειες που θα είχε αυτή η πράξη στα άτομα που παρουσιάζονται στα βίντεο, ή πως θα ένοιωθαν αν ήταν οι ίδιοι στη θέση τους.

Ανησυχητικό είναι επίσης και το γεγονός ότι αρκετά κινητά μπορούν να ενωθούν στο Διαδίκτυο και να αποστείλουν τις φωτογραφίες που λήφθηκαν σε κάποια ιστοσελίδα ή σε κάποιο ημερολόγιο που διατηρεί στο Διαδίκτυο ο κάτοχος του κινητού. Με αυτή τη δυνατότητα, αρκετοί δημοσιοποιούν τις φωτογραφίες τους αμέσως μετά τη λήψη τους, χωρίς να διερωτηθούν πρώτα εάν αυτή η πράξη τους θα αποκαλύψει πληροφορίες για τρίτους ή και για τους ίδιους.

Πρέπει όλοι να προσπαθήσουμε να χρησιμοποιούμε τα μέσα που μας παρέχει η σύγχρονη τεχνολογία με σύνεση και προσοχή ώστε να μη θέτουμε τον εαυτό μας ή τρίτα πρόσωπα σε κίνδυνο, να μην προσβάλλουμε ή γελοιοποιούμε τρίτα πρόσωπα και να σεβόμαστε την προσωπική ζωή τους, λαμβάνοντας υπόψη πώς θα αισθανόμασταν εμείς αν βρισκόμασταν στη θέση τους.

Οδηγία που εκδίδεται από την Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα βάσει του Άρθρου 23(ι) του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου 138(Ι)/2001

ΓΡΑΦΕΙΟ ΕΠΙΤΡΟΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Θεμιστοκλή Δέρβη 40, 3ος όροφος, 1066 ΛΕΥΚΩΣΙΑ

Τ.Θ.23378, 1682 ΛΕΥΚΩΣΙΑ, Τηλ: 22 818456, Φαξ: 22 304565

E-mail: commissioner@dataprotection.gov.cy, Website: <http://www.dataprotection.gov.cy>



Γ.Τ.Π. 377/2007- 10.000

Εκδόθηκε από το Γραφείο Τύπου και Πληροφοριών

Εκτύπωση: Χρ. Νικολάου και Υιοί Λτδ