Οι πέντε παγίδες του Facebook

Δεν είναι λίγοι οι χρήστες του Facebook που κινδύνεψαν να χάσουν την ηρεμία τους, τη δουλειά τους, το σπίτι τους, ακόμα και την ίδια τους τη ζωή, από δεδομένα που δημοσιεύτηκαν στο συγκεκριμένο κοινωνικό δίκτυο.

Αρκετές φορές, όμως, τα δεδομένα αυτά δεν διέρρευσαν από κάποιο κενό ασφαλείας, ούτε από κάποιον hacker. Όσο περίεργο κι αν ακούγεται, τα δημοσίευσαν οι ίδιοι οι χρήστες, πιστεύοντας λανθασμένα ότι θα τα έβλεπαν μόνο οι φίλοι τους.

Διαβάστε παρακάτω ποια είναι τα στοιχεία που δεν θα πρέπει ποτέ να δημοσιεύετε στα κοινωνικά δίκτυα, ανεξάρτητα από τις ρυθμίσεις ασφαλείας σας:

1) **Την ημερομηνία γενεθλίων σας:** πράγματι, είναι πολύ ωραίο το να διαβάζουμε δεκάδες ή εκατοντάδες ευχετήρια μηνύματα την ημέρα των γενεθλίων μας στο Facebook, έστω και μέσα από μια «ψυχρή» οθόνη. Το πρόβλημα, όμως, είναι πως η ημερομηνία γενεθλίων είναι ένα από τα λίγα στοιχεία που χρειάζεται κάποιος προκειμένου να υποκλέψει τον κωδικό σας ή την ταυτότητά σας. Αν είναι εφικτό, μην καταχωρήσετε καθόλου την ημερομηνία ή τουλάχιστον παραλείψτε το έτος γέννησης. Άλλωστε, οι πραγματικοί σας φίλοι ήδη θα το γνωρίζουν.

2) **Την τοποθεσία σας:** πολλοί χρήστες του Facebook χρησιμοποιούν αρκετά συχνά την υπηρεσία geotagging του κοινωνικού δικτύου, προκειμένου να δημοσιεύσουν την τοποθεσία τους στα status και τα μηνύματά τους, τις φωτογραφίες τους και, βέβαια, μέσω των check-in. Κάποιοι μάλιστα το κάνουν συνέχεια. Το πρόβλημα εδώ είναι πως αποδέκτης των πληροφοριών αυτών δεν είναι μόνο οι φίλοι σας, αλλά ενδεχομένως και επιτήδειοι... Γνωρίζοντας την τοποθεσία σας και πιθανώς το διάστημα που θα βρίσκεστε εκεί και πόσο χρόνο θα σας πάρει να επιστρέψετε, υπάρχει πιθανότητα κάποιοι να εκμεταλλευτούν την κατάσταση. Αρκετές φορές στο παρελθόν χρήστες οι οποίοι δημοσίευαν συνέχεια φωτογραφίες ή γενικά πληροφορίες σχετικά με τις διακοπές τους έπεσαν θύματα διαρρήξεων.

Αντί να «ανεβάζετε» φωτογραφίες από το κινητό σας και να λέτε σε όλο το Facebook πόσο ωραία περνάτε στις διακοπές σας, το ασφαλέστερο θα ήταν να χρησιμοποιήσετε γραπτά μηνύματα για το δεύτερο και να δημοσιεύσετε τις φωτογραφίες σας αφού γυρίσετε σπίτι.

3) **Την κατάσταση της σχέσης σας:** είτε είστε σε σχέση είτε όχι, δεν είναι πάντα η καλύτερη ιδέα να το δημοσιεύετε. Ο λόγος δεν είναι τόσο η ίδια η κατάσταση της σχέσης σας, όσο η πιθανή αλλαγή της σε «Ελεύθερος/η». Κάτι τέτοιο μπορεί να δώσει το έναυσμα σε ενοχλητικούς χρήστες, ακόμα και επιτήδειους να σας «βομβαρδίσουν» με μηνύματα. Τέτοιου είδους ενόχληση συνήθως μπορεί να

αντιμετωπιστεί με block ή αναφορά του χρήστη, στην περίπτωση όμως που αυτός γνωρίζει αρκετά για εσάς τα πράγματα περιπλέκονται.

Δεν είναι λίγες οι περιπτώσεις όπου stalker, «κυνηγοί» δηλαδή, έχουν φθάσει στα άκρα, προκειμένου να πλησιάσουν χρήστες κοινωνικών δικτύων ακόμα και πρόσωπο με πρόσωπο. Το καλύτερο που μπορείτε να κάνετε είναι να αγνοήσετε τελείως την κατάσταση σχέσης ή ακόμα και να την έχετε μονίμως «σε σχέση», προκειμένου να αποτρέψετε κάθε είδους ενόχληση.

4) **Το γεγονός ότι είστε μόνοι στο σπίτι:** ιδίως για μικρά παιδιά, τα οποία έχουν την τάση να «διαφημίζουν» τέτοιου είδους γεγονότα στους φίλους τους (και ταυτόχρονα σε όλο το Facebook), μια τέτοια τακτική μπορεί να αποβεί επικίνδυνη. Οι λόγοι είναι προφανείς και πάνω κάτω οι ίδιοι με τα δύο προηγούμενα στοιχεία.

Οι γονείς θα πρέπει να ελέγχουν προληπτικά τις αναρτήσεις των παιδιών τους στο διαδίκτυο, αλλά και να φροντίσουν να τα ενημερώσουν για τους πιθανούς κινδύνους. Το ίδιο βέβαια μπορεί να ισχύει και για εφήβους ή ακόμα και για ενήλικες. Επομένως, φροντίζετε να ειδοποιείτε τους φίλους σας μέσω τηλεφώνου ή γραπτού μηνύματος, όχι μέσω του Facebook.

5) **Φωτογραφίες και ονόματα παιδιών, συγγενών και φίλων**: οι γονείς, στη συντριπτική πλειονότητά τους, δημοσιεύουν στα κοινωνικά δίκτυα φωτογραφίες των παιδιών τους μαζί με το όνομα και την ημερομηνία γέννησης. Πολλές φορές μάλιστα αυτό γίνεται προτού καλά καλά γυρίσουν από το μαιευτήριο. Παράλληλα, δημοσιεύουν φωτογραφίες συγγενών και φίλων κάνοντας «tag» τα ονόματά τους χωρίς προηγουμένως να λάβουν τη συγκατάθεσή τους. Αυτό μπορεί να προξενήσει δύο ειδών προβλήματα. Αρχικά, χρησιμοποιώντας αυτά τα στοιχεία, ακόμα και αν πρόκειται απλώς για ένα όνομα, οι stackers μπορούν πιο εύκολα να πλησιάσουν εσάς ή ακόμα και τα παιδιά σας, προσποιούμενοι πως είναι γνωστοί κάποιων φίλων ή συγγενών.

Πέραν τούτου, τίθεται και το θέμα της χρήσης των φωτογραφιών, αφού τα άτομα που απεικονίζονται σ’ αυτές μπορεί να μη θέλουν να δημοσιευτούν στο διαδίκτυο, ειδικά αν οι φωτογραφίες περιλαμβάνουν το όνομά τους.

Για αυτόν ακριβώς τον λόγο αποφεύγετε να δημοσιεύετε. Σε περίπτωση που θέλετε, μπορείτε να πάρετε την άδεια των συγγενών ή φίλων σας για τη δημοσίευση, χωρίς βέβαια να τους κάνετε «tag» με το όνομά τους.

Σε γενικές γραμμές, οι αναβαθμισμένες υπηρεσίες ασφαλείας και απόρρητου του Facebook βέβαια μπορεί να σας δώσουν τη δυνατότητα να μοιράζεστε όλα τα παραπάνω μόνο με αυτούς που θέλετε. Το θέμα όμως είναι πως δεν υπάρχει τρόπος να γνωρίζετε ποιος πραγματικά τα διαβάζει στον λογαριασμό τους.

Πέρα από την πιθανότητα κάποιος τρίτος να τα διαβάσει ενώ ο φίλος σας έχει το Facebook ανοικτό στον υπολογιστή του, κάλλιστα θα μπορούσε το προφίλ του να έχει πέσει «θύμα» κλοπής ή hacking, με αποτέλεσμα οι πληροφορίες σας να βρεθούν σε λάθος χέρια.

Επομένως, ακόμα και με τις πιο αυστηρές ρυθμίσεις, η πιθανότητα κινδύνου από τέτοιου είδους δημοσιεύσεις είναι μεν μικρή, αλλά υπαρκτή.