10 Ιουλίου 2016

# 6 πράγματα που δεν πρέπει να κάνετε ΠΟΤΕ στο Facebook (και μία συμβουλή)

/ Επιστήμες, Τέχνες & Πολιτισμός

Image not found or type unknown

Πηγή: REUTERS/Dado Ruvic/Illustration

Image not found or type unknown
*Πηγή: REUTERS/Dado Ruvic/Illustration*

Η **προστασία** των **προσωπικών δεδομένων** είναι πολύτιμη. Επιπλέον είναι και ιδιαίτερα σπάνια αυτές τις μέρες που η καθημερινότητα ορίζεται μέσα από αναρτήσεις, likes και shares.

Αυτή ακριβώς την προστασία της **ιδιωτικότητάς** μας οφείλουμε πρωτίστως να φροντίσουμε εμείς, οι ίδιοι οι χρήστες που συχνά λειτουργούμε με αφέλεια πρωτόγνωρη, πληρώνοντας το ανάλογο τίμημα.

Αναρίθμητες είναι οι περιπτώσεις που μια ανάρτηση ή ένα στοιχείο που δημοσιοποιήθηκε στην προσωπική σελίδα χρήστη του Facebook οδήγησαν σε διαρρήξεις αλλά και παρενοχλήσεις.

Με το ηλεκτρονικό έγκλημα να γιγαντώνεται και **τις αναρτήσεις προσωπικού χαρακτήρα να έχουν πλέον προτεραιότητα έναντι των ενημερωτικών μετά από την αλλαγή στον αλγόριθμο του κοινωνικού δικτύου**, παρουσιάζουμε όλα όσα εκείνα δεν πρέπει **ΠΟΤΕ** να μοιράζεστε με τους διαδικτυακούς φίλους.

## 1. Τη διεύθυνση σπιτιού και εργασίας σας -κατά λάθος.

Ναι, ίσως ακούγεται ανόητο να το κάνει κάποιος ή αυτονόητο ότι δεν θα το κάνει κάποιος. Ωστόσο ακόμη και όταν χρησιμοποιούμε την υπηρεσία geotagging, ειδικά όταν γίνεται συχνά και δείχνει πάνω κάτω την ίδια τοποθεσία θα πρέπει να γνωρίζετε ότι υποδεικνύεται στους επίδοξους stalker, ληστές και λοιπούς κακοπροαίρετους που συχνάζετε και πότε.

Επίσης, φροντίστε να έχετε έλεγχο στην κοινωνική δραστηριότητα και των φίλων σας. Εάν κάποιος σας επισκεφθεί και επιθυμεί να κάνει Check In στο διαμέρισμα

σας, οφείλει να σας ρωτήσει.

## 2. Παιδικές φωτογραφίες

Ιδιαίτερη προσοχή πρέπει να δίνουμε όταν θέλουμε να αναρτήσουμε παιδικές φωτογραφίες. Στην περίπτωση που πρόκειται για παιδιά άλλων, φροντίστε να πάρετε άδεια από τους γονείς τους. Στην περίπτωση που είναι τα δικά σας παιδιά, φροντίστε να μην προδίδετε πολλά από τα στέκια και τις σχολικές ή εξωσχολικές τους δραστηριότητες.

Με το φαινόμενο εξαφανίσεων κοριτσιών από τα σπίτια τους να οργιάζει και τις «ζυμώσεις» αυτών των παραπλανήσεων να γίνονται συνήθως στα social media, οι γονείς οφείλουν να ελέγχουν την κοινωνική δραστηριότητα των παιδιών τους αλλά και όλα όσα μοιράζονται οι ίδιοι για αυτά.

## 3. Λεπτομέρειες για τις διακοπές σας

Οι φίλοι και οι γνωστοί θα χαρούν για την απουσία σας γιατί γνωρίζουν ότι πρόκειται για μια φυγή ξεκούρασης. Ακόμη περισσότερο όμως θα χαρο΄τυν και οι επίδοξοι διαρρήκτες που έτσι γνωρίζουν πότε μπορούν να δράσουν ανενόχλητοι στα λημέρια σας. Εναλλακτική; Να κάνετε όσες λεπτομερείς αναρτήσεις θέλετε για τις διακοπές σας σε επιλεγμένο κύκλο φίλων που μπορείτε να κάνετε από τα Settings.

## 4. Προσωπικές, και δη τολμηρές, φωτογραφίες

Ναι, είστε περιορισμένοι από τους ίδιους τους κανόνες των κοινωνικών δικτύων ώστε να μην μπορείτε να κοινοποιείτε γυμνές φωτογραφίες σας. Πάντα όμως έχετε τη δυνατότητα να τις στείλετε με Snapchat ή Direct Message ή όποιο άλλο τρόπο επινοήσετε (υπάρχουν πολλοί). Κάπως έτσι, πάντα δίνετε τη δυνατότητα σε hacker να τις αλιεύσουν φέρνοντας τον γυμνό εαυτό σας στα μάτια αγνώστων και πολλών. Μην εμπιστεύεστε σε ΚΑΝΕΝΑΝ τα τολμηρά στιγμιότυπα σας.

## 5. Πιστωτική κάρτα ή άλλες πληροφορίες οικονομικής φύσης

Ναι, ακούγεται ανόητο, αλλά υπάρχουν χρήστες που έχουν δημοσιεύσει φωτογραφίες από την πιστωτική τους κάρτα στα κοινωνικά δίκτυα. Αυτονόητο ότι πρόκειται για κάτι που απαγορεύεται ρητά ωστόσο εκείνοι που γνωρίζουν από ηλεκτρονικό έγκλημα επισημαίνουν ότι και η παραμικρή λεπτομέρεια, η επωνυμία της τράπεζας με την οποία συνεργάζεστε, το μητρώνυμο, το ΑΦΜ, η ημερομηνία και ο τόπος γέννησης σας, αρκούν για να οδηγήσουν τους επίδοξους χάκερ εκεί που εκείνοι επιθυμούν.

## 6. Τοποθετήσεις, σχόλια και δημόσιες κόντρες για θέματα της επικαιρότητας

Αν δεν έχετε πειράξει τα **Privacy Settings**, τότε το πιθανότερο είναι οτιδήποτε ποστάρετε να φτάνει στο News Feed εκείνου ακριβώς που δεν θα έπρεπε. Μελέτη του Career Builder διαπίστωσε πως **4 στους 10 εργοδότες χρησιμοποιούν τα social media για να παρακολουθήσουν τη δραστηριότητα των υπαλλήλων τους**. Έρευνα του 2014 από την εταιρία ερευνών Gartner ανέφερε ότι ήδη το 60% των εταιριών «παρακολουθεί» τους εργαζομένους του στα κοινωνικά δίκτυα. Η δημιουργία μιας **Restricted List** είναι απαραίτητη.

## Μία ειλικρινής, φιλική συμβουλή

Σύμφωνα με μελέτες, το **63% των εφαρμογών που έχουμε στα κινητά και τα tablet μας αλλά και πολλές του ίδιου του Facebook, επιθυμούν κατά την εγκατάσταση τους την άδεια να ποστάρουν αντί για εμάς.** Μην το επιτρέψετε, αντιθέτως επισκεφθείτε τα settings των εφαρμογών και απενεργοποιήστε το αυτόματο posting.

Αν η εφαρμογή δεν έχει τέτοια επιλογή ή απλά επιμένει στη δική της, αυτόνομη δραστηριότητα, διαγράψτε την.

***Πηγή***: *cnn.gr*