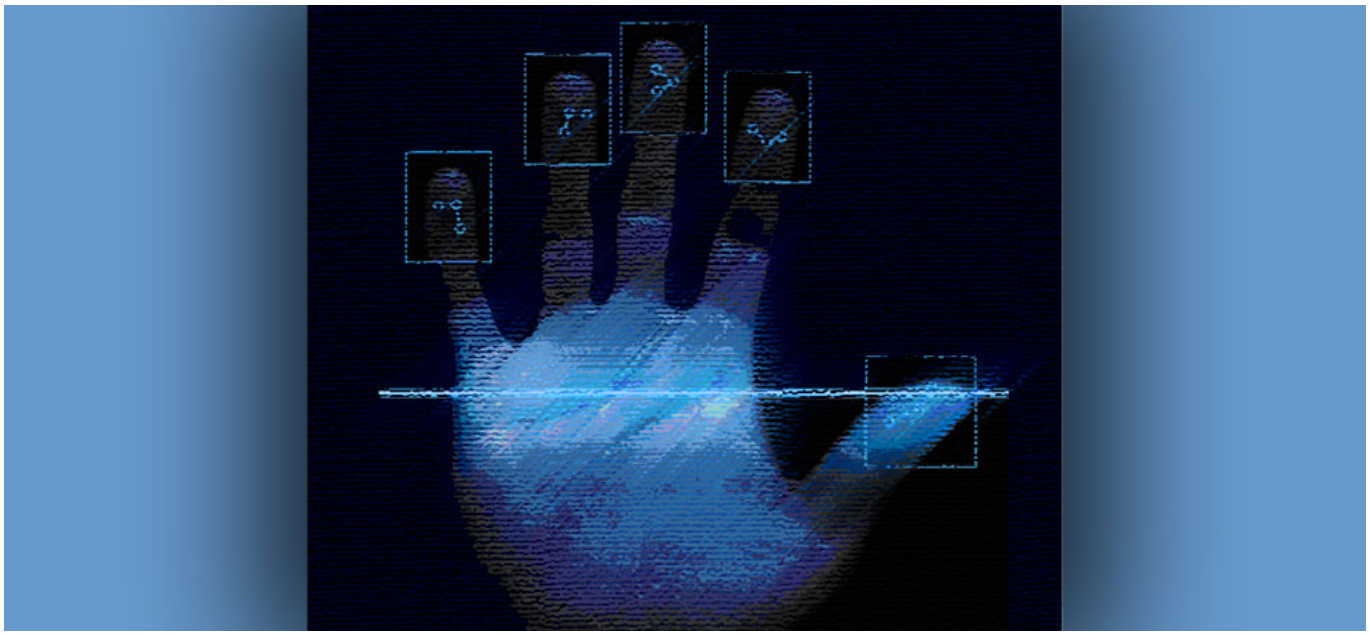
17 Ιουλίου 2014

Έξι παράγοντες για αυξημένη ασφάλεια του υπολογιστή σας

/ Πεμπτουσία

Image not found or type unknown



Τις υποσχέσεις που δίνουμε κάθε πρωτοχρονιά συνήθως δεν τις τηρούμε… Υποσχόμαστε στον εαυτό μας ότι το νέο έτος θα είναι η χρονιά που θα σταματήσουμε το κάπνισμα, θα κάνουμε δίαιτα ή ότι θα ξεκινήσουμε το πρόγραμμα που έχουμε προπληρώσει στο γυμναστήριο! Γι' αυτό θα πρέπει να είμαστε λίγο πιο ελαστικοί με τον αυτό μας και να υποσχόμαστε πράγματα που είναι πραγματικά εφικτά. Έτσι κι εμείς θα σας παραθέσουμε έξι τρόπους που πιστεύουμε ότι μπορούμε όλοι να ακολουθήσουμε προκειμένου να παρέχουμε αυξημένη ασφάλεια στον προσωπικό μας υπολογιστή.

1. **Εγκατάσταση ενός προγράμματος παροχής ασφάλειας (anti-virus).** Είτε έχετε κάποιο Windows PC, ή Apple Mac, ή κάποιο Android smartphone θα πρέπει να εγκαταστήσετε ένα πρόγραμμα antivirus, το οποίο θα πρέπει να είναι πάντα ενημερωμένο. Τα περισσότερα κακόβουλα λογισμικά (περίπου 200.000 νέα δείγματα που εντοπίζονται από ερευνητές ασφάλειας καθημερινά) αφορούν τα Windows, αλλά υπάρχουν πολλοί ακόμα κίνδυνοι που

αφορούν χρήστες Mac και Android. Το ευχάριστο νέο για τους χρήστες iPhone είναι ότι δεν είναι εκτεθειμένοι σε μεγάλο κίνδυνο εάν δεν έχουν πραγματοποιήσει jailbreak στη συσκευή τους. Βέβαια, ακόμα και τότε ο κίνδυνος δεν είναι τόσο μεγάλος όσο στις υπόλοιπες συσκευές.

2. **Πραγματοποιείτε τις απαραίτητες ενημερώσεις.** Νέες ευπάθειες εντοπίζονται συνεχώς και κάποιες από αυτές τις εκμεταλλεύονται οι hackers προκειμένου να κλέψουν τα προσωπικά σας δεδομένα ή να μολύνουν τον υπολογιστή σας με κακόβουλο λογισμικό. Θα πρέπει να έχετε πάντα πραγματοποιείτε τις απαραίτητες ενημερώσεις όχι μόνο στο λειτουργικό σας σύστημα αλλά και σε άλλα προγράμματα που έχετε εγκατεστημένα στον υπολογιστή σας.
3. **Κρυπτογράφηση του σκληρού δίσκου.** Σε πολλούς έχει τύχει να χάσουν ή να τους κλέψουν τον φορητό ή τον επιτραπέζιο υπολογιστή τους. Φυσικά, εκτός από το γεγονός ότι θα στεναχωρηθούμε για την συσκευή, υπάρχει κάτι πολύ χειρότερο να σκεφτούμε...ότι ο κλέφτης θα αποκτήσει όλα μας τα προσωπικά δεδομένα, όπως αρχεία, μηνύματα ηλεκτρονικούς ταχυδρομείου, φωτογραφίες κ.α. Η πλήρης κρυπτογράφηση του δίσκου σημαίνει ότι κανείς δεν θα είναι σε θέση να αποκτήσει πρόσβαση στα δεδομένα του σκληρού δίσκου.
4. **Ισχυροί κωδικοί πρόσβασης.** Σταματήστε να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε όλες τις ιστοσελίδες. Να θυμάστε ότι αν ένας hacker καταφέρει να κλέψει τον κωδικό πρόσβασής σας από μια ιστοσελίδα, θα μπορεί να αποκτήσει πρόσβαση και σε όλες τις υπόλοιπες που είστε εγγεγραμμένοι. Μπορείτε εγκαταστήσετε ένα πρόγραμμα διαχείρισης κωδικών, όπου μπορείτε να αποθηκεύσετε όλους τους κωδικούς σας καθώς και να αναπαράγετε ισχυρούς κωδικούς. Ένα από αυτά τα προγράμματα είναι και το http://keepass.info/.
5. **Ασφάλεια στα μέσα κοινωνικής δικτύωσης.** Το 2014 θα πρέπει να πάρετε λίγο πιο σοβαρά το τι κοινοποιείτε στο διαδίκτυο. Ελέγξτε τις ρυθμίσεις ασφάλειας του λογαριασμού σας σε όλες τις υπηρεσίες κοινωνικής δικτύωσης.
6. **Backup.** Αυτό είναι κάτι που το αναφέρουμε συνέχεια και θα συνεχίσουμε, καθώς είναι ο παλαιότερος και πιο σίγουρος τρόπος να διατηρήσουμε τα αρχεία μας ασφαλή.

Αυτά λοιπόν είναι τα μέτρα που σας προτείνουμε, τα οποία και πιστεύουμε ότι είναι αρκετά εύκολα για να τα υιοθετήσετε. Καλή τύχη και αν χρειάζεστε παραπάνω συμβουλές μην διστάσετε να μας ρωτήσετε!

Αναδημοσίευση: SecNews.gr