10 Ιουνίου 2017

Δέκα απαραίτητα βήματα για να θωρακίσετε τον υπολογιστή σας

/ Επιστήμες, Τέχνες & Πολιτισμός

Η ESET προτείνει σε κάθε χρήστη, από τον πιο αρχάριο μέχρι τον πιο έμπειρο, 10 βήματα για να αποκρούει τις επιθέσεις κάνοντας το έργο των εγκληματιών του κυβερνοχώρου πραγματικά δύσκολο.

1. Ενημερώνετε διαρκώς το λειτουργικό σύστημα, τις εφαρμογές και τη λύση

ασφάλειας που χρησιμοποιείτε. Οι ενημερώσεις συχνά περιλαμβάνουν λύσεις για ελαττώματα ασφαλείας που έχουν βρεθεί, οπότε, ένας εισβολέας δεν θα είναι σε θέση να εκμεταλλευτεί κάθε είδους γνωστή ευπάθεια στο σύστημά σας.

2. Χρησιμοποιήστε λύσεις ασφάλειας σε υπολογιστές, smartphone και tablet. Ταυτόχρονα, αποφύγετε τη χρήση «πειρατικού» λογισμικού – εκτός του ότι είναι παράνομο, είναι απίθανο να προσφέρει την κατάλληλη προστασία. Firewalls και antivirus θα σας προστατεύσουν από Trojans και άλλους τύπους κακόβουλου λογισμικού, καθώς και από διάφορες τεχνολογίες ανίχνευσης, που οδηγούν σε διαρροή ή κλοπή πληροφοριών.

3. Κάντε αντίγραφα ασφαλείας σε τακτική βάση – ένας εξωτερικός σκληρός δίσκος είναι μία καλή λύση – και φυλάξτε τα σε ασφαλές μέρος. Φροντίστε να μην έχετε το backup σας συνεχώς συνδεδεμένο, γιατί αν ο υπολογιστής μολυνθεί με κάθε είδους ransomware, τα αρχεία, ακόμη κι αν είναι αποθηκευμένα στο cloud, μπορούν να επηρεαστούν. Χρήσιμες πληροφορίες για τη δημιουργία αντιγράφων ασφαλείας μπορείτε να βρείτε στον σχετικό οδηγό στη διεύθυνση http://www.welivesecurity.com/2015/03/31/6-ways-to-back-up-your-data/

4. Αναφέρετε phishing emails και ιστοσελίδες που τυχόν συναντάτε από οποιοδήποτε πρόγραμμα περιήγησης χρησιμοποιείτε. Αντίστοιχη αναφορά θα πρέπει να γίνει και στον κατασκευαστή του antivirus που χρησιμοποιείτε, αν δεν αναγνωρίζει ήδη το site ως μία κακόβουλη πύλη. Με αυτόν τον τρόπο, βοηθάτε στην προστασία όλων των χρηστών προειδοποιώντας για τους κινδύνους που έχετε συναντήσει.

5. Βεβαιωθείτε ότι έχετε ισχυρούς κωδικούς πρόσβασης, αλλάζετε τους τακτικά, και μην χρησιμοποιείτε το ίδιο password για πολλούς λογαριασμούς: πρόκειται για το τρίπτυχο που θα κρατήσει την ψηφιακή σας ταυτότητα ασφαλή.

6. Ενεργοποιήστε την πιστοποίηση διπλού παράγοντα, που αυξάνει σημαντικά τα επίπεδα ασφάλειας. Αν ένας κυβερνοεγκληματίας καταφέρει να κλέψει τον κωδικό πρόσβασης, δεν θα μπορέσει να προκαλέσει σημαντική ζημιά, αφού θα πρέπει να εισάγει ακόμα έναν ακόμα τυχαίο κωδικό που παράγεται από αυτό το πρόσθετο επίπεδο της ασφάλειας.

7. Εξετάστε το απόρρητο στα κοινωνικά σας δίκτυα, ελέγχοντας αν μοιράζεστε υπερβολικά πολλές ευαίσθητες πληροφορίες, σε ποιους επιτρέπετε την πρόσβαση και τι δικαιώματα έχετε παραχωρήσει σχετικά με τα προσωπικά σας στοιχεία.

8. Ελέγχοντας τακτικά την κατάσταση των τραπεζικών λογαριασμών σας μπορείτε να ανιχνεύσετε τυχόν παρατυπίες ή περίεργες συναλλαγές, όπως το να

έχει κλωνοποιηθεί η κάρτα σας ή να έχετε πέσει θύμα τραπεζικού malware.

9. Βεβαιωθείτε ότι δεν έχετε εγγραφεί σε premium υπηρεσίες SMS. Να θυμάστε ότι τα hoax, όπως συνέβη και με πρόσφατη περίπτωση στο WhatsApp που μετρά περισσότερα από 10 εκατομμύρια θύματα, έχουν τη δυνατότητα να εξαπατούν τους χρήστες, ωθώντας τους να γίνουν συνδρομητές σε υπηρεσίες λήψης SMS, για τα οποία φυσικά χρεώνονται.

10. Προσπαθήστε να ενημερώνεστε για τις εξελίξεις στο χώρο της ασφάλειας. Αν γνωρίζετε τον τρόπο που λειτουργούν τα hoax, μπορείτε να προφυλαχθείτε καλύτερα, και συζητώντας για αυτό με άλλους χρήστες τους βοηθάτε να παραμείνουν κι αυτοί προστατευμένοι.

Πηγή: tech.in.gr