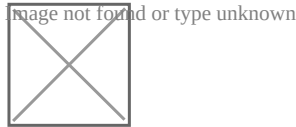


FBI: αλλάζετε συχνά κωδικούς! Ερευνητές: Μην αλλάζετε passwords...

/ [Πεμπτούσία](#)



Είναι μια ερώτηση που τη συναντάμε συνεχώς: Να αλλάζουμε συχνά τους κωδικούς πρόσβασης (passwords) που χρησιμοποιούμε;

Κανονικά θα περίμενε ότι το FBI παρέχει αποτελεσματικές συμβουλές ασφάλειας, αλλά ένα tweet που δημοσίευσε πρόσφατα έκανε πολλούς εμπειρογνώμονες ασφάλειας να αναρωτιούνται αν τελικά ισχύει κάτι τέτοιο. Συγκεκριμένα, το FBI στις 25 Νοεμβρίου έστειλε ένα tweet-συμβουλή για να βοηθήσει (υποτίθεται) τους χρήστες του διαδικτύου να παραμείνουν ασφαλείς. «Αγορές online την εορταστική περίοδο; Κρατήστε τους λογαριασμούς σας ασφαλείς, χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης και να τους αλλάζετε συχνά,» αναφέρει το FBI.

Οι ασφαλείς λογαριασμοί με την χρήση ισχυρών κωδικών πρόσβασης (passwords) είναι πράγματι μια καλή συμβουλή, όμως το τελευταίο μέρος της πρότασης προκάλεσε διαμάχες. Η συχνή αλλαγή κωδικών πρόσβασης, περιγράφεται πολύ

συχνά σαν μια κακή πρακτική, επειδή αν το κάνετε επανειλημμένα μπορεί τελικά σας οδηγήσει στην χρήση εύκολων κωδικών που μπορούν να σπάσουν γρήγορα από hackers.

Επιπλέον, είναι αποδεδειγμένο ότι οι εταιρείες που αναγκάζουν τους εργαζομένους τους να αλλάζουν συνεχώς τους κωδικούς πρόσβασής τους, εκτίθενται περισσότερο σε επιθέσεις για τους ίδιους λόγους: οι εργαζόμενοι καταλήγουν να χρησιμοποιούν απλούστερους κωδικούς πρόσβασης που είναι πιο εύκολο να θυμούνται κάτι το οποίο δεν είναι και η ασφαλέστερη πρακτική.

Έτσι οι εμπειρογνώμονες ασφάλειας αμφισβήτησαν τα tweets του FBI, και ένας από αυτούς που συνέστησε ακριβώς το αντίθετο ήταν και ο Per Thorsheim.

Σε δήλωσή του στο Motherboard, ο Thorsheim εξήγησε ότι η συχνή αλλαγή των κωδικών πρόσβασης δεν θα πρέπει να γίνεται και ότι υπάρχουν και άλλοι τρόποι για να παραμείνετε ασφαλείς στο διαδίκτυο. «Είμαι έκπληκτος και είναι λυπηρό να βλέπω ότι το FBI συνεχίζει να δίνει τέτοιες συμβουλές όταν αξιόπιστες ακαδημαϊκές έρευνες, πολυάριθμες οργανώσεις, εταιρείες και η ίδια η κυβέρνηση των ΗΠΑ αναφέρουν για τουλάχιστον μισό χρόνο τώρα ότι η συχνή αλλαγή των κωδικών πρόσβασης είναι κακή ιδέα. ... Αν και δεν ξέρω ποιος από το FBI έχει τον έλεγχο του λογαριασμού τους στο Twitter, φαίνεται όμως ότι δεν γνωρίζει τις τρέχουσες βέλτιστες πρακτικές.»

Λοιπόν, πώς μπορείτε να προστατεύσετε τον εαυτό σας online χωρίς να αλλάζετε passwords συχνά; Ο ευκολότερος τρόπος είναι να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης που μπορεί να δημιουργήσει και να «θυμάται» σύνθετους κωδικούς πρόσβασης που είναι δύσκολο να σπάσουν. Φυσικά υπάρχουν πολλοί διαχειριστές κωδικών, όπως οι LastPass, 1Password, RoboForm κλπ, αλλά αποθηκεύουν τους κωδικούς στο σύννεφο.

Συμβουλή μας: Προτιμήστε έναν offline password manager σαν τον KeePass. Ο συγκεκριμένος διαχειριστής είναι δωρεάν και αποθηκεύει τοπικά τους κωδικούς σας χρησιμοποιώντας ισχυρή κρυπτογράφηση.

Επιπλέον, φροντίστε να ενεργοποιήσετε τον έλεγχο ταυτότητας δύο παραγόντων σε όποια υπηρεσία διαθέτει το χαρακτηριστικό ασφαλείας και αποφύγετε να χρησιμοποιείτε τα ίδια passwords σε πολλές υπηρεσίες.

Πηγή: Secnews.gr