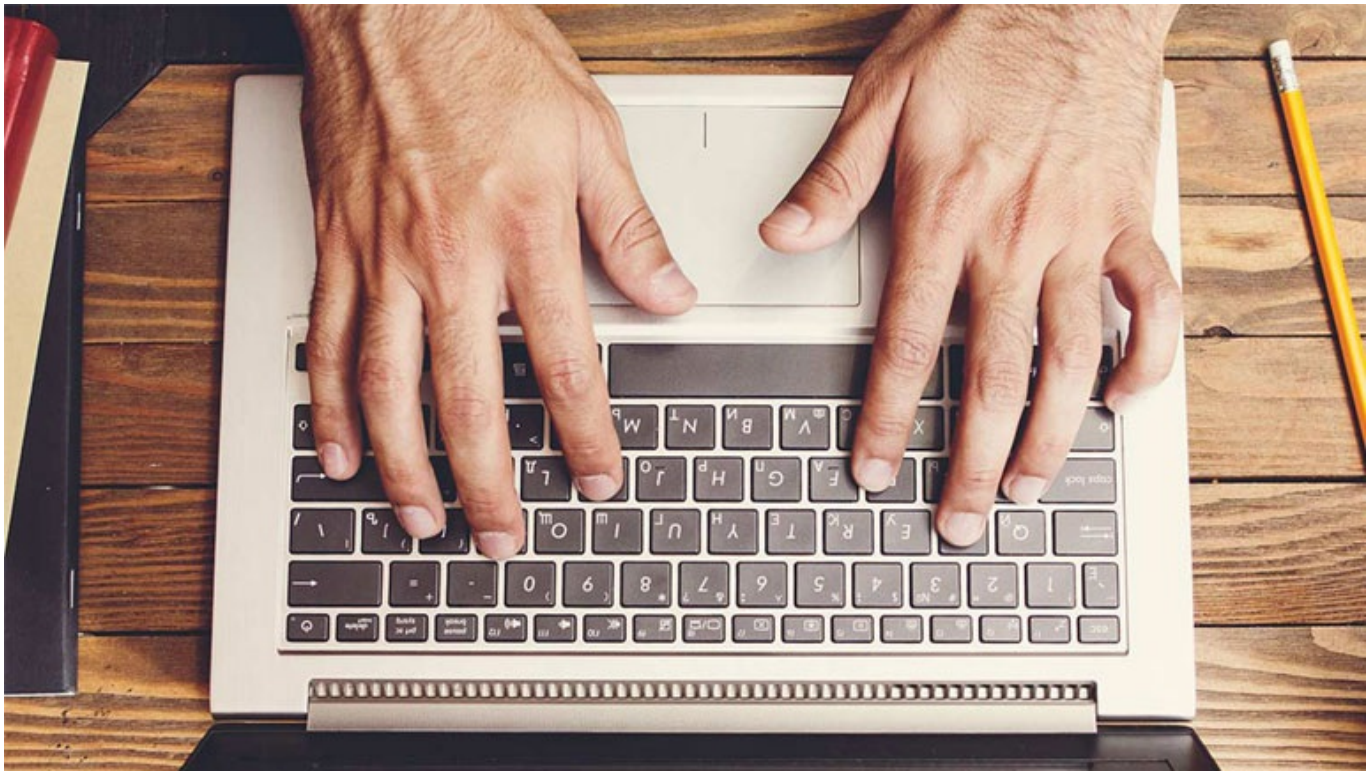
22 Φεβρουαρίου 2019

Οι μοναδικοί κωδικοί πρόσβασης είναι πιο ασφαλείς από τη συχνή αλλαγή τους

/ Επιστήμες, Τέχνες & Πολιτισμός



Στο πλαίσιο της Ημέρας Αλλαγής Κωδικού Πρόσβασης, οι ερευνητές ασφάλειας

της Kaspersky Lab συμβουλεύουν τους χρήστες ότι οι μοναδικοί και ευκολομνημόνευτοι κωδικοί πρόσβασης είναι ισχυρότεροι και αποτελεσματικότεροι από τις τακτικές αλλαγές τους όταν πρόκειται για την ασφαλή διατήρηση των δεδομένων. Οι ερευνητές μοιράζονται μερικά απλά βήματα που μπορούν να ακολουθήσουν οι χρήστες για να δημιουργήσουν τη δική τους σειρά μοναδικών κωδικών πρόσβασης. Επίσης, συνιστούν την εγκατάσταση εργαλείου διαχείρισης κωδικών πρόσβασης που θα αναλάβει να κάνει τη «βρώμικη» δουλειά της απομνημόνευσης των κωδικών πρόσβασης για λογαριασμό των χρηστών.

Οι κωδικοί πρόσβασης είναι μια καθιερωμένη μέθοδος ελέγχου ταυτότητας για τους online λογαριασμούς, αλλά η δημιουργία κωδικών που θα είναι ασφαλείς και ευκολομνημόνευτοι δεν είναι πάντα εύκολη υπόθεση και γίνεται όλο και πιο δύσκολη, καθώς οι άνθρωποι έχουν περισσότερους από έναν λογαριασμούς στο διαδίκτυο. Εάν δημιουργείτε απλούς κωδικούς πρόσβασης που είναι απίθανο να ξεχάσετε, ο κίνδυνος παραβίασης από έναν hacker είναι μεγαλύτερος. Ωστόσο, αν δημιουργήσετε έναν πιο περίπλοκο κωδικό πρόσβασης, είναι πιο πιθανό να τον ξεχάσετε, έτσι οι πιθανότητες είναι υψηλές ότι θα «κολλήσετε» σε έναν ή δύο και θα τους επαναχρησιμοποιείτε σε πολλαπλούς ιστότοπους.

Οι ερευνητές της Kaspersky Lab εκτιμούν ότι η μεγαλύτερη ευπάθεια των κωδικών πρόσβασης είναι η επαναχρησιμοποίησή τους. Όπως έδειξε η πρόσφατη διαρροή περισσότερων από 700 εκατομμυρίων email και εκατομμυρίων μη κρυπτογραφημένων κωδικών πρόσβασης, τα δεδομένα από διαφορετικές παραβιάσεις μπορούν εύκολα να συνδυαστούν και να χρησιμοποιηθούν σε επιθέσεις, όπου οι χάκερ χρησιμοποιούν συνδυασμούς email/κωδικών θυμάτων για να παραβιάσουν κι άλλους λογαριασμούς που έχουν τον ίδιο κωδικό πρόσβασης.

Για να ελαχιστοποιηθεί ο κίνδυνος αυτός, δεν χρειάζεται συχνή αλλαγή των κωδικών πρόσβασης, αλλά ισχυροποίησή τους όχι μέσω πολυπλοκότητας αλλά μέσω μοναδικότητας.

Ο David Jacoby, ερευνητής στην Παγκόσμια Ομάδα Έρευνας και Ανάλυσης της Kaspersky Lab (GReAT), δήλωσε: «Υπάρχει μεγάλη σύγχυση σχετικά με το τι πράγματι σημαίνει ένας ισχυρός κωδικός πρόσβασης. Πολλοί ιστότοποι απαιτούν πλέον πολύπλοκους κωδικούς πρόσβασης που περιλαμβάνουν τουλάχιστον οκτώ ή περισσότερα κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες. Αυτή την απαίτηση είναι που πολλοί χρήστες έχουν έρθει να εξισώσουν με έναν «ισχυρό» κωδικό πρόσβασης, κάτι που μπορεί να φαίνεται αρκετά τρομακτικό».

Και πρόσθεσε: «Τα καλά νέα είναι ότι οι ισχυροί κωδικοί δεν πρέπει να είναι

απαραίτητα και τρομακτικοί! Όταν εξετάζετε το ζήτημα από την άποψη της ασφάλειας, μπορείτε να δείτε ότι οι κωδικοί πρόσβασης είναι γενικά ισχυροί αν είναι μοναδικοί για εσάς και για έναν λογαριασμό. Υπάρχουν εύκολοι τρόποι να γίνουν μοναδικοί, αλλά και ευκολομνημόνευτοι, έτσι ώστε να μην μπορούν να χρησιμοποιηθούν για την παραβίαση άλλων λογαριασμών, ακόμη και αν εκτεθούν λεπτομέρειες σε περίπτωση παραβίασης δεδομένων. Επιπλέον, υπάρχουν διαθέσιμα ασφαλή εργαλεία διαχείρισης κωδικών πρόσβασης, συμπεριλαμβανομένου του Kaspersky Password Manager, που διευκολύνουν την ασφαλή δημιουργία και χρήση δεκάδων μοναδικών κωδικών πρόσβασης».

Τα παρακάτω βήματα θα σας βοηθήσουν να δημιουργήσετε μοναδικούς, ευκολομνημόνευτους και ισχυρούς κωδικούς πρόσβασης:

Βήμα 1: Δημιουργήστε το δικό σας «σταθερό κομμάτι» (το μέρος του κωδικού πρόσβασης που δεν αλλάζει)

1. Σκεφτείτε μια φράση, στίχους τραγουδιού, αποσπάσματα από μια ταινία, ομοιοκαταληξία ή κάτι αντίστοιχο που είναι εύκολο να το θυμάστε.
2. Πάρτε το πρώτο γράμμα από τις πρώτες τρεις έως πέντε λέξεις.
3. Μεταξύ κάθε γράμματος προσθέστε έναν ειδικό χαρακτήρα: @ / # κ.λπ.

Από εδώ και στο εξής, μπορείτε να βασίσετε όλους τους μοναδικούς κωδικούς πρόσβασης σας σε αυτή τη σειρά.

Βήμα 2: Προσθέστε τη δύναμη της συσχέτισης

1. Όταν σκέφτεστε τους διαδικτυακούς λογαριασμούς για τους οποίους χρειάζεστε έναν κωδικό πρόσβασης (Facebook, Twitter, eBay, ιστοσελίδες dating, ηλεκτρονικές τραπεζικές συναλλαγές, κ.λπ.), καταγράψτε για κάθε έναν από αυτούς την πρώτη λέξη με την οποία τον συνδέεται.
2. Για παράδειγμα, εάν δημιουργείτε έναν κωδικό πρόσβασης για το Facebook, μπορεί να συσχετίσετε το Facebook με το μπλε χρώμα στο λογότυπο: οπότε μπορείτε απλά να προσθέσετε τη λέξη “μπλε” μετά το σταθερό κομμάτι.

Ο David Jacoby εξηγεί: «Για παράδειγμα, αν η φράση που σκέφτεστε είναι το «Twinkle Twinkle Little Star, How I Wonder What You Are» και ο ειδικός χαρακτήρας που θέλετε να χρησιμοποιήσετε είναι #, τότε ο κωδικός πρόσβασής σας στο Facebook θα είναι κάτι σαν: T#T#L#S#Hblue. Δεν έχει νόημα όταν το βλέπετε, ή αν κάποιος σας τον έδινε. Δεδομένου όμως ότι είναι προσωπικό για εσάς, κατανοείτε το σύστημα που έχετε χρησιμοποιήσει για τη δημιουργία του και συνδέετε τη λέξη με τον ιστότοπο, είναι εύκολο να τον θυμηθείτε!».

Πηγή: **zougla.gr**