Μερικοί χρήσιμοι κανόνες από την ESET για τη δημιουργία ισχυρών passwords

Οι κίνδυνοι που παραμονεύουν στον εικονικό κόσμο του διαδικτύου πολλές φορές δεν γίνονται αντιληπτοί σε μερικούς χρήστες, που έχουν μεγαλώσει στην εποχή που δεν υπήρχε Internet και κοινωνικά δίκτυα, σε αντίθεση με τις νέες γενιές που μεγαλώνουν στην ψηφιακή εποχή και είναι πιο υποψιασμένες. Θέλοντας να βοηθήσει τους ανυποψίαστους χρήστες, ο Ondrej Kubovic, IT Security Specialist της ESET, προσφέρει μερικούς βασικούς κανόνες για ασφαλή passwords.

1. Δημιουργήστε ένα μοναδικό κωδικό πρόσβασης για κάθε λογαριασμό και μην το μοιραστείτε με κανέναν.
2. Ο κανόνας είναι – όσο μεγαλύτερος ο κωδικός πρόσβασης, τόσο πιο ασφαλής. Ξεκινήστε με τουλάχιστον 8 χαρακτήρες, αλλά επιμηκύνετε τον κωδικό αν χρησιμεύει για να προστατεύει πολύτιμα δεδομένα ή λογαριασμούς. Αν έχετε πρόβλημα να θυμηθείτε ένα σύνθετο κωδικό πρόσβασης, μπορείτε επίσης να επιλέξετε μια συνθηματική φράση ή να χρησιμοποιήσετε έναν password manager (αναλύονται παρακάτω)
3. Αποφύγετε κοινές λέξεις, ονόματα, ημερομηνίες, αριθμούς ή προφανείς επιλογές, όπως 12345678, password ή qwerty.
4. Προσθέστε ένα ψηφιακό κομμάτι, όπως αριθμούς και

ειδικούς χαρακτήρες (@, #,!, κλπ), ή χρησιμοποιήστε τα αντικαθιστώντας κάποια από τα γράμματα στον κωδικό πρόσβασής σας.
5. Εάν επιλέξετε την αντικατάσταση, προσπαθήστε να μην χρησιμοποιήσετε τις συνήθεις «ανορθογραφίες», όπως αντικατάσταση του «α» με «@» ή «ι» με «1» ή «!».
6. Αλλάξτε τακτικά τους κωδικούς πρόσβασής. Και εδώ ισχύει ότι όσο πιο σημαντικά τα δεδομένα που προστατεύονται, τόσο πιο σύντομα πρέπει να αλλάζουν οι κωδικοί.
7. Ένας από τους σημαντικότερους κανόνες είναι να μην χρησιμοποιήσετε ξανά τον ίδιο κωδικό πρόσβασης σε άλλους λογαριασμούς. Με αυτόν τον τρόπο, αν κλαπεί, κινδυνεύει μόνο ένας λογαριασμός, και αξίζει να το επισημαίνουμε ακόμη κι αν επαναλαμβανόμαστε.

Στη θεωρία μπορεί να ακούγεται αρκετά απλό, αλλά η πραγματικότητα είναι πιο σύνθετη. Πολλαπλές μελέτες έχουν δείξει ότι ο μέσος χρήστης έχει δεκάδες κωδικούς πρόσβασης για έναν ακόμη μεγαλύτερο αριθμό λογαριασμών, γεγονός που δυσχεραίνει τη διαχείρισή τους. Ωστόσο, υπάρχουν στρατηγικές για να παραμείνετε ασφαλείς διευκολύνοντας τη διαδικασία. Το πρώτο πράγμα που μπορεί να βοηθήσει είναι οι συνθηματικές φράσεις, ή αλλιώς passphrases, που παρόλου που είναι μεγαλύτερες από τους κωδικούς πρόσβασης, είναι πιο εύκολο να απομνημονευτούν. Ένας άλλος τρόπος είναι η χρήση ενός αξιόπιστου password manager, που αποθηκεύει όλους τους κωδικούς σε ένα μέρος, και το μόνο που χρειάζεται να θυμάται ο χρήστης είναι ένα από αυτά, εκείνο δηλαδή που θα του επιτρέψει να ξεκλειδώσει την εφαρμογή.