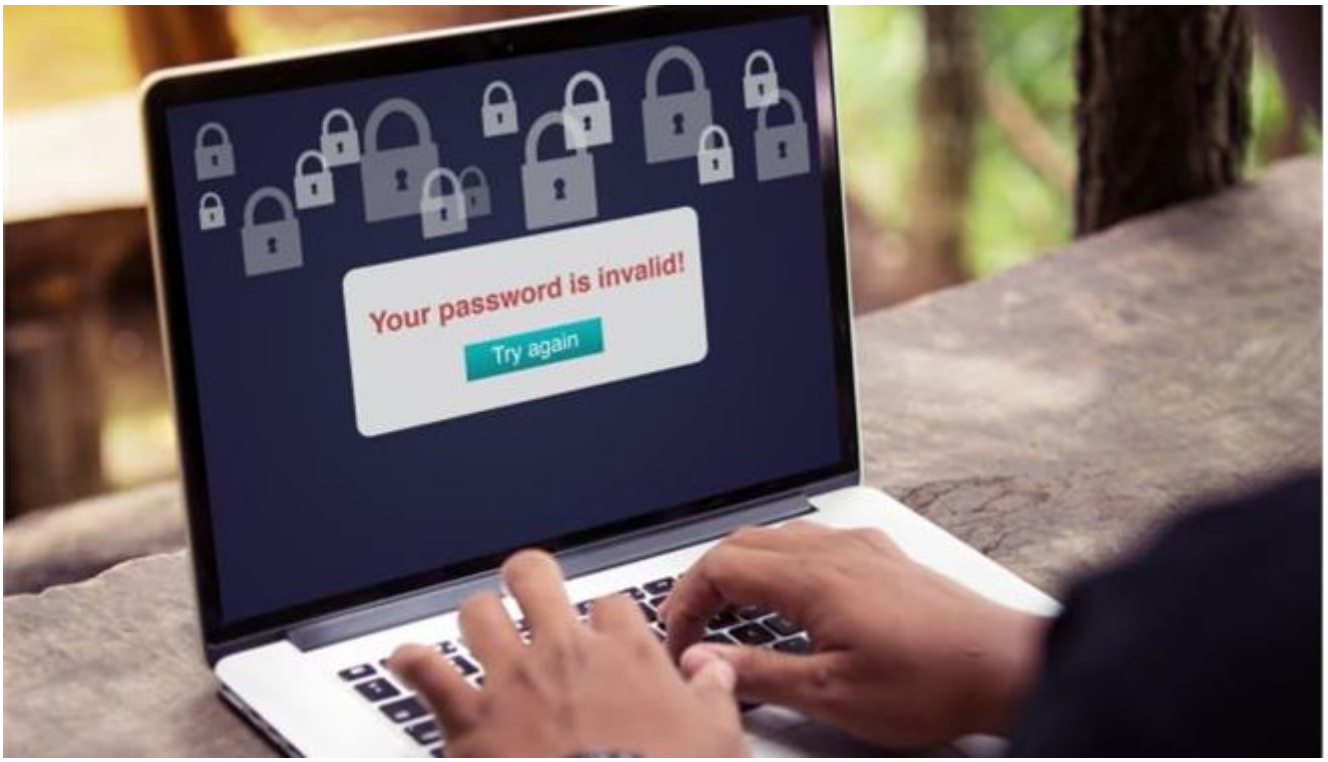
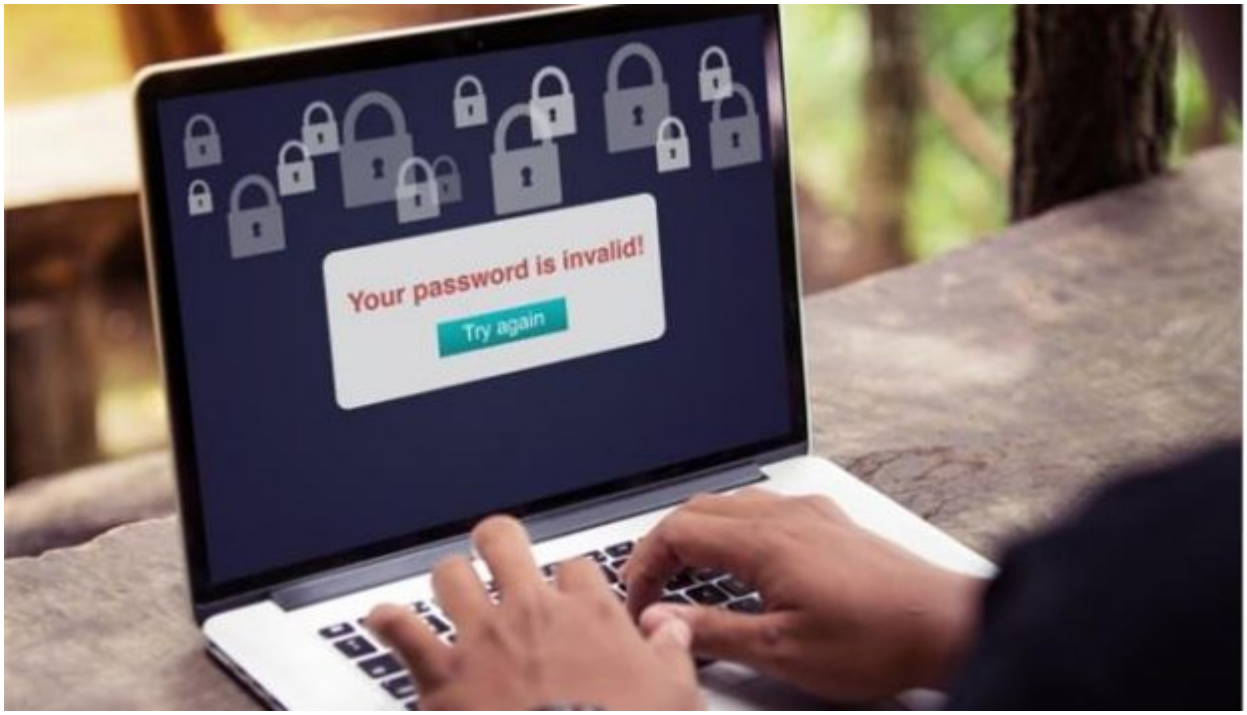
21 Ιανουαρίου 2018

Το μεγάλο δίλημμα των κωδικών

/ Επιστήμες, Τέχνες & Πολιτισμός



Οι ισχυροί είναι δύσκολο να απομνημονευθούν, ενώ οι αδύναμοι μπορούν εύκολα να «σπάσουν» από επίδοξους χάκερ – Ποια είναι τα απαραίτητα βήματα για ασφαλή password



Αντιμέτωποι με το δίλημμα ισχυροί κωδικοί, που όμως είναι δύσκολο να απομνημονευθούν ή αδύναμοι κωδικοί, τους οποίους είναι εύκολο να θυμάται κανείς, έρχονται όλο και πιο συχνά οι χρήστες του Ιντερνετ παγκοσμίως.

Με την εξάρτησή τους από τους λογαριασμούς τους στο Διαδίκτυο να βαίνει συνεχώς αυξανόμενη, οι άνθρωποι καλούνται να αποφασίσουν πώς να επιλέγουν τους κωδικούς πρόσβασης. Μερικοί καταλήγουν να χρησιμοποιούν ισχυρούς και διαφορετικούς κωδικούς πρόσβασης για κάθε λογαριασμό, ώστε να μην μπορούν να παραβιαστούν ή να τους εκμεταλλευτούν εγκληματίες. Ομως διατρέχουν τον κίνδυνο να τους ξεχνούν με το πέρασμα του χρόνου. Αλλοι επιλέγουν κωδικούς που μπορούν να τους απομνημονεύσουν εύκολα διευκολύνοντας τη ζωή τους. Ωστόσο, διατρέχουν τον κίνδυνο οι κωδικοί αυτοί να βρεθούν το ίδιο εύκολα στα χέρια ψηφιακών εγκληματιών.

Ερευνα της Kaspersky Lab αποκάλυψε το δίλημμα που αντιμετωπίζουν οι χρήστες όταν προστατεύουν τους λογαριασμούς τους στο Διαδίκτυο. Οταν πρόκειται για την αποθήκευση κωδικού πρόσβασης, σύμφωνα με την έρευνα, οι μισοί (51%) αποθηκεύουν τους κωδικούς επισφαλώς, με έναν στους τέσσερις (23%) να τους γράφει σε σημειωματάριο ώστε να μη χρειάζεται να τους θυμάται. Οπως τονίζει η εταιρεία ψηφιακής ασφάλειας, πολλοί χρήστες κατανοούν την ανάγκη ισχυρών κωδικών πρόσβασης στους λογαριασμούς τους. Οταν ρωτήθηκαν ποιοι τρεις λογαριασμοί τους στο Διαδίκτυο απαιτούν τους ισχυρότερους κωδικούς πρόσβασης, το 63% των καταναλωτών επέλεξε λογαριασμούς online banking, το 42% εφαρμογές πληρωμής, συμπεριλαμβανομένων των ηλεκτρονικών

πορτοφολιών και το 41% λογαριασμούς για ηλεκτρονικές αγορές.

Το βέβαιο είναι ότι πολλοί χρήστες εξακολουθούν ακόμη και σήμερα να χρησιμοποιούν ακατάλληλα password για την πρόσβαση στους λογαριασμούς τους στο Διαδίκτυο. Αυτό αποδεικνύει λίστα που δόθηκε πρόσφατα στη δημοσιότητα από τη SplashData και περιλαμβάνει τους χειρότερους από πλευράς ασφάλειας κωδικούς πρόσβασης που χρησιμοποιήθηκαν το 2017.

Εύκολα θύματα. Τα στοιχεία της λίστας, σύμφωνα με την ESET, βασίστηκαν σε έρευνα περισσότερων από πέντε εκατομμυρίων κωδικών πρόσβασης από λογαριασμούς χρηστών που έπεσαν θύματα κυβερνοεγκληματιών.

Στις πρώτες 30 θέσεις της λίστας συγκαταλέγονται κωδικοί όπως 123456, password, 12345678, qwerty, football, iloveyou, admin, welcome, login, abc123, starwars, master, hello, 654321, harley κ.ά. Οι συγκεκριμένοι κωδικοί πρόσβασης είναι πολύ απλοί και εύκολα μπορεί να τους μαντέψει ένας επίδοξος χάκερ. Για τον λόγο αυτό περιλαμβάνονται μαζί με άλλα δημοφιλή password στις βάσεις δεδομένων που διατηρούν οι κυβερνοεγκληματίες για password-cracking.

«Τα καλά νέα», σύμφωνα με την ESET, είναι ότι «οι κωδικοί πρόσβασης μπορούν να είναι ασφαλείς και με τα σωστά βήματα μπορούν εύκολα να δημιουργηθούν ισχυρά password». Καταρχάς με μία αξιόπιστη εφαρμογή password manager κάθε χρήστης μπορεί να έχει στη διάθεσή του ένα πρόγραμμα που όχι μόνο αποθηκεύει τους κωδικούς πρόσβασης αλλά μπορεί ταυτόχρονα να δημιουργεί πολύπλοκα password.

Μέτρα από τους ιστότοπους. Από την πλευρά τους, οι ιστότοποι επίσης θα πρέπει να θωρακιστούν καλύτερα ώστε να εξασφαλίζουν την προστασία των ευαίσθητων πληροφοριών. Παράλληλα, θα πρέπει να είναι πιο αυστηροί στην επιλογή των κωδικών που εισάγουν οι χρήστες απορρίπτοντας password που χρησιμοποιούνται συχνά ή έχουν εκτεθεί σε παραβιάσεις δεδομένων.

Τέλος, η πιστοποίηση διπλού παράγοντα (2FA) μπορεί να αποδειχθεί σωτήρια, καθώς είναι πολύ ασφαλέστερη από τους κωδικούς πρόσβασης. Κατά την πιστοποίηση διπλού παράγοντα απαιτείται ένας επιπλέον τυχαίος κωδικός ή ένα μήνυμα SMS παράλληλα με τον κωδικό πρόσβασης, οπότε ακόμη και αν ένα password πέσει σε λάθος χέρια, δεν μπορεί εύκολα να παραβιαστεί ένας λογαριασμός. Ηδη, twitter, Google, LinkedIn και Dropbox και πολλές άλλες ηλεκτρονικές υπηρεσίες προσφέρουν πλέον την πιστοποίηση διπλού παράγοντα ως προαιρετικό, πρόσθετο μέτρο ασφαλείας.

Πηγή: tanea.gr