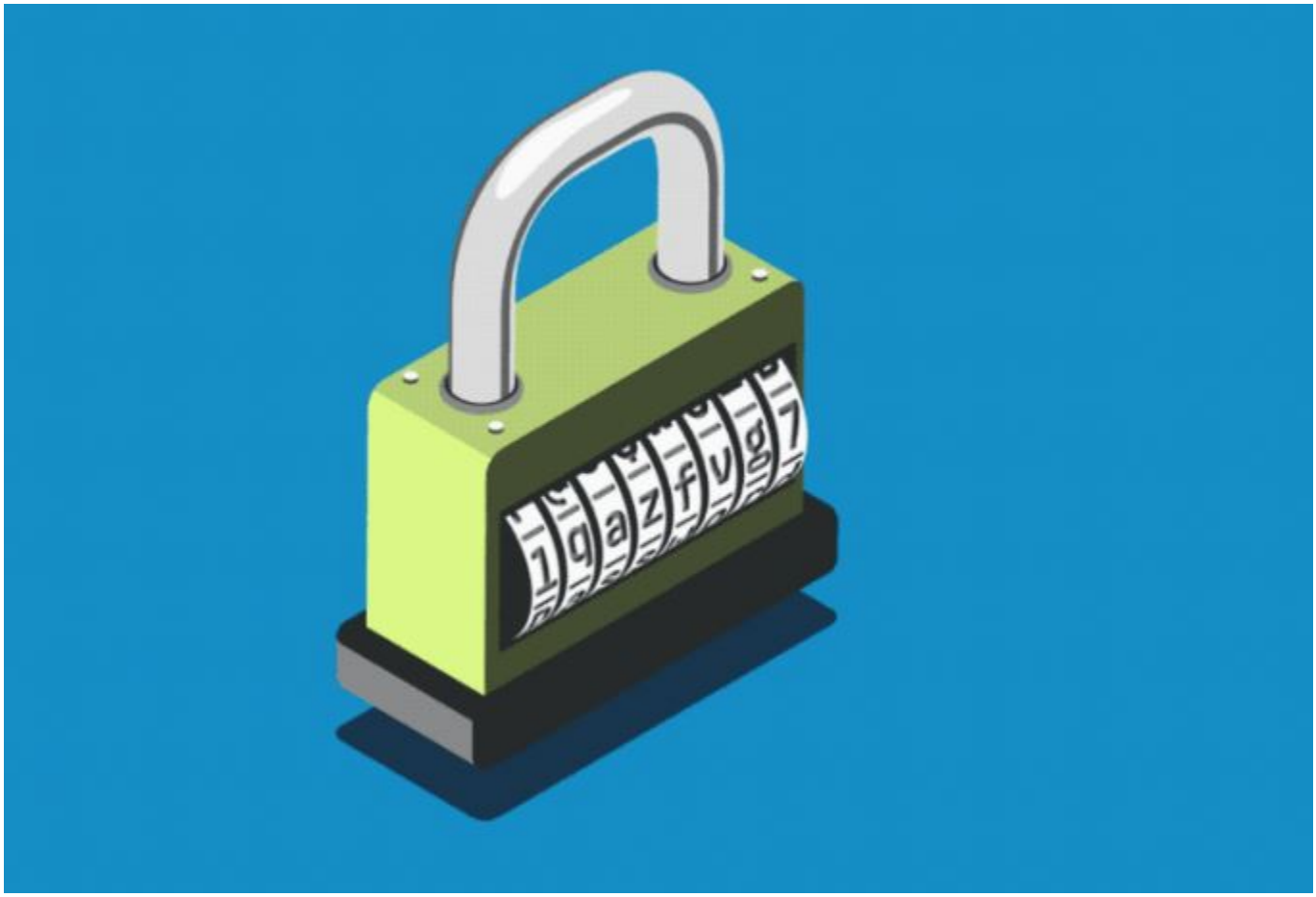
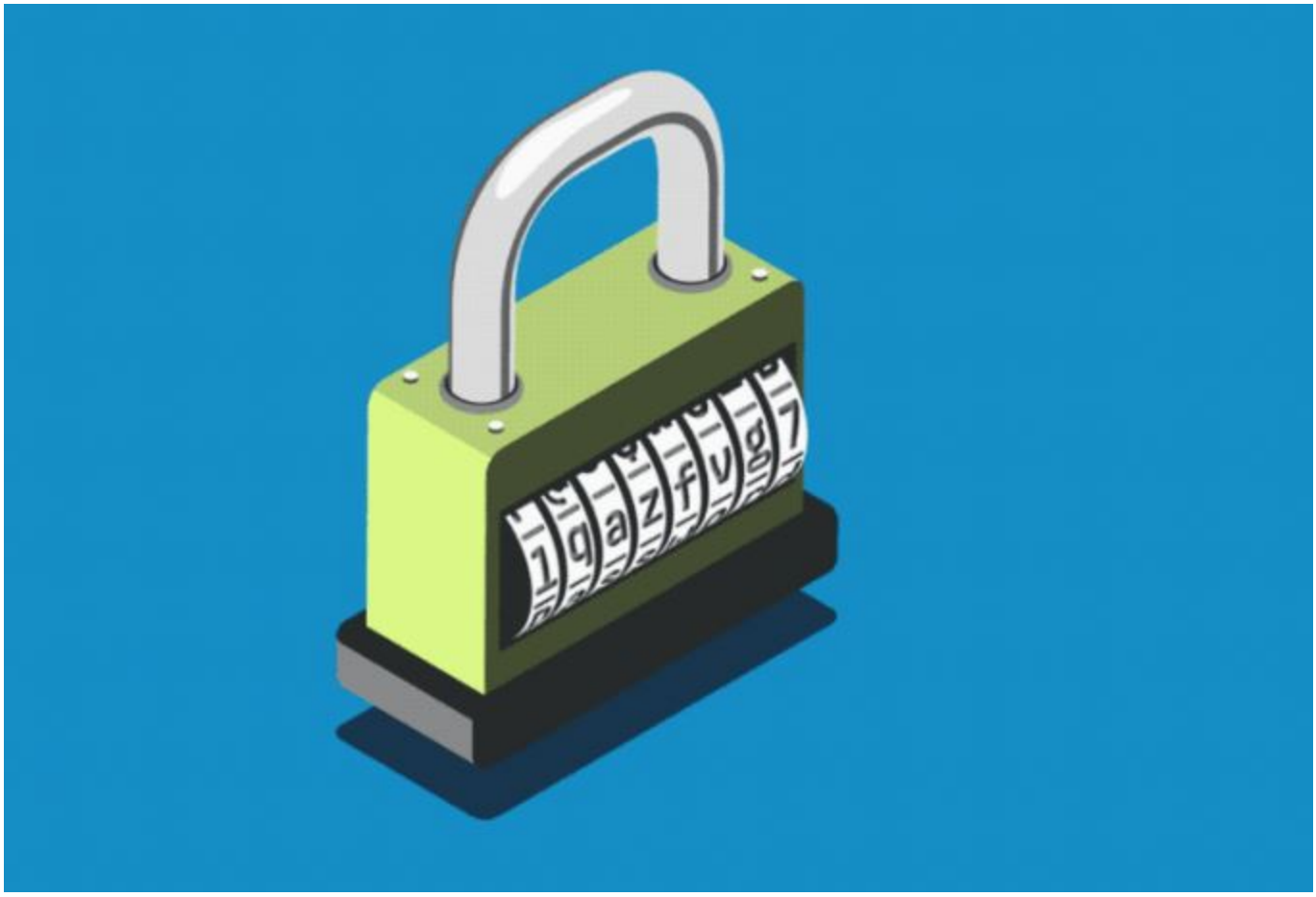
13 Μαρτίου 2021

# Σκέψου το πριν χρησιμοποιήσεις τον Apple, Google ή Facebook λογαριασμό σου για να συνδεθείς παντού!

/ Επιστήμες, Τέχνες & Πολιτισμός



Αν έχεις πνιγεί στα ατέλειωτα website logins και συνεχώς κάνεις υπενθυμίσεις κωδικών, ένα Log in with Google ή Log in with Facebook button φαντάζει σωσίβιο. Οι υπηρεσίες προσφέρουν έναν γρήγορο τρόπο να συνεχίσεις ό,τι κάνεις χωρίς να έχεις να ρυθμίσεις έναν ολόκληρο λογαριασμό και να επιλέξεις ένα password για την ασφάλειά του. Αλλά, ενώ αυτά τα “single sign-on” tools είναι ιδιαίτερα βολικά και προσφέρουν κάποια ασφάλεια, δεν είναι πανάκεια.



Ο εύκολος τρόπος αυτός σύνδεσης που προσφέρουν οι μεγάλες εταιρείες έχουν ορισμένα πλεονεκτήματα. Για παράδειγμα αναπτύσσονται από εταιρείες που έχουν τους πόρους να τα υποστηρίξουν και να ενσωματώσουν ισχυρά security features. Ωστόσο όμως έχουν και ορισμένα μειονεκτήματα. Αν το password του λογαριασμού που χρησιμοποίησες για να συνδεθείς στις άλλες υπηρεσίες υποκλαπεί, τότε βρίσκονται σε κίνδυνο όλοι οι άλλοι λογαριασμοί σου. Και όχι μόνο έχεις να εμπιστευτείς τις εταιρείες που προσφέρουν SSO να προστατεύουν την ιδιωτικότητα και την ασφάλειά σου, αλλά πρέπει να εμπιστευτείς και όλα τα τρίτα websites που προσφέρουν αυτές τις επιλογές, να έχουν σωστή υλοποίηση του χαρακτηριστικού.

Οι κίνδυνοι δεν είναι υποθετικοί!

Αν ένα από τα passwords υποκλαπεί, τότε όλοι οι λογαριασμοί που ασφάλισες με το συγκεκριμένο password είναι στην ουσία παραβιασμένοι. Ο καλύτερος τρόπος είναι η χρήση ενός password manager που δημιουργεί ισχυρά και ασφαλή passwords όταν τα χρειάζεσαι. Όπως και με τα SSO, οι passwords managers μπορούν να αποτελέσουν ένα σημείο αδυναμίας αν κάποιος υποκλέψει το master password. Αλλά σε αντίθεση με τα single sign on setups, ένας password manager δεν απαιτεί να βασίζεσαι σε διαφορετικές και τυχαίες οντότητες του διαδικτύου

να σε προστατέψουν.

Οι κίνδυνοι δεν είναι καθόλου υποθετικοί. Τον Σεπτέμβριο του 2018, το Facebook δημοσίευσε τα αποτελέσματα μιας τεράστιας παραβίασης δεδομένων που επηρέαζε τουλάχιστον 50 εκατομμύρια χρήστες και επιπλέον μεταξύ άλλων, η παραβίαση είχε εκθέσει και οποιονδήποτε άλλο λογαριασμό οι άνθρωποι αυτοί είχαν συνδεθεί χρησιμοποιώντας το Facebook SSO.

Μια έρευνα επίσης του 2018, είχε βρει σημαντικά προβλήματα στο πως 95 ιστοσελίδες και υπηρεσίες ενσωμάτωναν λειτουργίες SSO. Σε περισσότερα από μια ντουζίνα ιστοσελίδες, ένας συνδεδεμένος χρήστης μπορούσε να αλλάξει το email του λογαριασμού χωρίς να χρειαστεί να πληκτρολογήσει ξανά το password. Παράλληλα, τέτοιες single sign in υλοποιήσεις έχουν και σημαντικά προβλήματα πρακτικά.

Αν χρησιμοποιήσεις το λογαριασμό σου στο Facebook για να συνδεθείς σε μια υπηρεσία που σου δίνει χώρο για τις φωτογραφίες σου και στη συνέχεια χάσεις ή ξεχάσεις τα στοιχεία του Facebook δύσκολα γνωρίζεις αν το Facebook ή το site που σου παρέχει χώρο για τις φωτογραφίες είναι υπεύθυνο να σου λύσει το πρόβλημα. Με λίγα λόγια ίσως δεν υπάρξει τρόπος να επαναφέρεις την πρόσβαση στις φωτογραφίες σου.

Με λίγα λόγια, όσο βολικό και αν φαίνεται δεν πρέπει να γίνεται κατάχρησή του σε καμιά περίπτωση, για τους λόγους που προαναφέρθηκαν.

**Πηγή**: techmaniacs.gr