4.

ΠΡΟΣΤΑΤΕΨΤΕ ΤΑ ΨΗΦΙΑΚΑ ΣΑΣ ΤΙΜΑΛΦΗ

Όπως φροντίζετε τα πολύτιμα αντικείμενα στο σπίτι σας, το ίδιο θα πρέπει να κάνετε για τις πληροφορίες που αποθηκεύετε στο διαδίκτυο - είτε είναι τα οικονομικά σας αρχεία, σαρώσεις του διαβατηρίου σας, είτε η διεύθυνση ή ο αριθμός του τηλεφώνου σας, αξίζει να σκεφτείτε σχετικά με το **πού** αποθηκεύετε τα πολύτιμα προσωπικά σας δεδομένα και πώς μπορείτε να τα προστατεύσετε.

Ένας **επιφανειακός καθαρισμός** είναι πολύ καλός εάν θέλετε να κάνετε μερικές γρήγορες βελτιώσεις όσο πίνετε έναν καφέ. Αναζητήστε συγκεκριμένες πληροφορίες που βρίσκονται στο email σας ή σε άλλους λογαριασμούς και διαγράψτε τις: σαρώσεις της ταυτότητάς σας, τα τραπεζικά σας στοιχεία ή πληροφορίες για την ασφάλεια υγείας σας, για να αναφέρουμε μερικές. Εάν είναι κάτι που θα σας χρειαστεί μετέπειτα, μπορείτε πάντα να το κατεβάσετε ή να το τυπώσετε πριν το διαγράψετε από το email σας.

Ένας **βαθύς καθαρισμός** είναι πιο σχολαστικός και είναι καλό να γίνεται μια φορά τον χρόνο. Αρχειοθετήστε τα πάντα στο email ή τον λογαριασμό σας σε κοινωνικά δίκτυα, κατεβάστε τα στον υπολογιστή σας και διαγράψτε τα περιεχόμενα των λογαριασμών σας κάνοντας μια καινούργια αρχή.

Συμβουλή Μην διαγράφετε απλώς – αδειάστε επίσης τον κάδο απορριμμάτων σας και τα προσωρινά αρχεία!

Είναι στο χέρι σας αν θα φτιάξετε αντίγραφα ασφαλείας για τα αρχεία και τα έγγραφά σας σε μια υπηρεσία σύννεφου (cloud) ή θα τα σώσετε σε έναν εξωτερικό δίσκο ή κάποιο USB.

Ανεξάρτητα από τον τρόπο που θα τα αποθηκεύσετε, βεβαιωθείτε ότι δεν θα τα χάσετε, ότι έχουν δυνατό password και έχει νόημα για εσάς.

5.

ΔΙΑΔΩΣΤΕ ΤΟ

Μπορεί να είναι εύκολο να το ξεχάσουμε, αλλά το διαδίκτυο λέγεται «ιστός» για ένα λόγο. **Είμαστε όλοι συνδεδεμένοι online** μέσα από διαφορετικά δίκτυα, όχι μόνο ως «φίλοι» στα social media, αλλά επίσης μέσω των επαφών στους λογαριασμούς των email και τις φωτογραφίες που μοιραζόμαστε διαδικτυακά. Όταν ασφαλίζετε τους λογαριασμούς σας, ενδυναμώνετε τα passwords και καθαρίζετε τα δεδομένα σας, δεν επωφελείστε μόνο εσείς -**όλοι όσοι με τους οποίους είστε συνδεδεμένοι γίνονται λίγο πιο ασφαλείς από αυτή σας την προσπάθειά.**

Όταν καθαρίζετε το email και τους λογαριασμούς σας στα κοινωνικά δίκτυα, σκεφτείτε τι ακόμη θα μπορούσατε να κατεβάσετε που θα βοηθούσε τους φίλους ή τους συνεργάτες σας: οι λεπτομέρειες του τραπεζικού λογαριασμού της αδερφή σας, κωδικούς κλειδιά για το γραφείο σας ή μια σάρωση του διαβατηρίου του γιού σας είναι κάποια από τα αρχεία που μπορεί να προκαλέσουν πονοκέφαλο αν πέσουν σε λάθος χέρια.

Διαδώστε το! Η αύξηση της ψηφιακής ασφάλειας μπορεί να είναι τόσο απλή όσο το να ακολουθήσετε μερικά βασικά βήματα. Μοιραστείτε αυτό το Data Detox με τους φίλους, την οικογένεια ή τους συνεργάτες σας, για να τους βοηθήσετε να αλλάξουν τις συνήθειες τους με τρόπους που έχουν νόημα για αυτούς.

Ένα προϊόν από TACTICAL TECH

Μετάφραση

datadetoxkit.org/gr
#datadetox

DATA DETOX KIT

ΑΛΛΑΞΤΕ ΤΙΣ ΡΥΘΜΙΣΕΙΣ ΣΑΣ

για να κρατήσετε τα δεδομένα σας ασφαλή

Αν το ίντερνετ ήταν απλά ένα μέρος για να μοιράζεστε φωτογραφίες σκύλων που φοράνε κουστούμια δεινοσαύρων, δεν θα υπήρχε μεγάλη ανάγκη για κωδικούς πρόσβασης (passwords). Αλλά το διαδίκτυο είναι ένα μέρος όπου πληρώνετε τους λογαριασμούς σας, συνταγογραφείτε τα φάρμακά σας και το χρησιμοποιείτε για να εισέλθετε στις δημόσιες υπηρεσίες. Όταν σκέφτεστε όλα τα «ψηφιακά τιμαλφή» σας, τα οποία μοιράζεστε μέσω του ίντερνετ -και αποθηκεύετε στις συσκευές σας- **δεν θα θέλατε να τα κρατήσετε τόσο ασφαλή όσο το πορτοφόλι ή τα κλειδιά σας;**

Υπάρχει ένας απλός τρόπος να δυσκολέψετε τους άλλους από το να έχουν πρόσβαση στα ψηφιακά τιμαλφή σας: **μη τους διευκολύνετε να μαντέψουν τους κωδικούς πρόσβασής σας**. Οι περισσότεροι άνθρωποι δεν χρειάζονται ειδικές τεχνικές δεξιότητες για να μπουν στους λογαριασμούς σας -μπορούν να το καταφέρουν κάνοντας μερικές υποθέσεις για τους κωδικούς σας ή τρέχοντας ένα αυτοματοποιημένο πρόγραμμα.

Και μόλις καταφέρουν να αποκτήσουν πρόσβαση σε έναν λογαριασμό, μπορούν να δοκιμάσουν τον παραβιασμένο κωδικό σε άλλους λογαριασμούς σας, να συλλέξουν πληροφορίες για εσάς και τις συνήθειες σας, να πάρουν το έλεγχο άλλων λογαριασμών που σας ανήκουν, είτε ακόμη να χρησιμοποιήσουν την ψηφιακή σας ταυτότητα.

Ακολουθώντας αυτό το Data Detox, θα μάθετε πρακτικούς τρόπους για να αυξήσετε τη διαδικτυακή σας ασφάλεια.

Ας ξεκινήσουμε!

1.

ΚΛΕΙΔΩΣΤΕ ΤΗΝ ΨΗΦΙΑΚΗ ΣΑΣ ΠΟΡΤΑ

Κλείδωμα οθόνης: οι κωδικοί, τα μοτίβα, τα δακτυλικά αποτυπώματα ή η αναγνώριση προσώπου που χρησιμοποιείτε για να έχετε πρόσβαση στη συσκευή σας είναι κάποιες από τις **καλύτερες άμυνες σας** απέναντι σε κάποιον που μπορεί να θέλει να μπει στη συσκευή σας. Αλλά υπάρχουν πολλά είδη εκεί έξω και μπορεί να είναι δύσκολο να γνωρίζετε ποιο είναι το σωστότερο για εσάς.

Το να έχετε ένα οποιοδήποτε κλείδωμα στο τηλέφωνο, το tablet ή τον υπολογιστή σας, σας παρέχει περισσότερη προστασία από το να μην έχετε καθόλου. Όπως οι διαφορετικοί τύποι κλειδαριών που βάζετε στις πόρτες σας έτσι **κάποια κλειδώματα οθόνης είναι δυνατότερα από άλλα.**

Από όλες τα κλειδώματα που υπάρχουν εκεί έξω, οι μεγάλοι, μοναδικοί κωδικοί πρόσβασης είναι τα δυνατότερα. Αυτό σημαίνει ότι αν ξεκλειδώνετε τη συσκευή σας με έναν κωδικό πρόσβασης, αυτός θα πρέπει να περιλαμβάνει γράμματα, νούμερα και ειδικούς χαρακτήρες.

Ας υποθέσουμε ότι χρησιμοποιείτε ένα βασικό swipe για να ανοίξετε το τηλέφωνό σας. Μπορείτε να αυξήσετε την ασφάλειά σας ρυθμίζοντας έναν μακρύ κωδικό πρόσβασης. Μήπως τώρα χρησιμοποιείτε ένα μοτίβο κλειδώματος; Μήπως να κάνατε αυτό το μοτίβο μεγαλύτερο; Χρησιμοποιείτε το 1234 σαν το PIN σας; Μήπως να ρίχνατε τα ζάρια εφτά φορές και να απομνημονεύατε αυτό το PIN καλύτερα; **Μια μικρή αλλαγή μπορεί να συμβάλει σημαντικά στη διατήρηση του ελέγχου των συσκευών σας.**

2.

ΚΑΝΕ ΤΟ ΣΩΣΤΟ

Η δημιουργία κορυφαίων κωδικών πρόσβασης (passwords) είναι εύκολη. Το μόνο που χρειάζεται να κάνετε είναι να ακολουθήσετε κάποιες βασικές αρχές. Τα passwords πρέπει να είναι:

Μεγάλα: τα passwords πρέπει να έχουν το λιγότερο 8 χαρακτήρες. Ακόμη καλύτερα; 16-20 χαρακτήρες

Μοναδικά: κάθε password που χρησιμοποιείτε -για κάθε site- πρέπει να είναι διαφορετικό

Τυχαίο: το password δεν πρέπει να ακολουθεί ένα λογικό μοτίβο ή να είναι εύκολο να το φανταστεί κανείς. Εδώ τα προγράμματα διαχείρισης κωδικών πρόσβασης (passwords managers) είναι πολύ βοηθητικά.

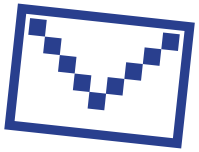
Τα δυνατότερα των passwords χρησιμοποιούν έναν συνδυασμό γραμμάτων, αριθμών και ειδικών συμβόλων. Αυτή η πολύτιμη συμβουλή εξακολουθεί να δημιουργεί έναν ισχυρότερο, πιο δύσκολο να μαντέψει κανείς κωδικό πρόσβασης. Κάποια συστήματα κωδικών πρόσβασης δυστυχώς δεν επιτρέπουν τη χρήση ειδικών συμβόλων (όπως @#$%-=+), αλλά ένα αρκετά μεγάλος συνδυασμός γραμμάτων και αριθμών είναι πολύ καλύτερος από έναν μικρότερο.

Ιδανικά, θα πρέπει να χρησιμοποιείτε έναν **ειδικό διαχειριστή κωδικών πρόσβασης** για να δημιουργείτε και να αποθηκεύετε όλους τα passwords σας. Ένας password manager – όπως το 1Password, το Firefox Lockwise, και το KeePassXC, τα οποία συνίστανται από τους ειδικούς στην ασφάλεια – είναι βασικά μια εφαρμογή της οποίας ο μοναδικός σκοπός είναι να προστατέψει τα διαπιστευτήρια των συνδέσεων σας και άλλα προσωπικά δεδομένα.

3.

ΠΡΟΣΘΕΣΤΕ ΕΝΑ ΔΕΥΤΕΡΟ ΚΛΕΙΔΙ

Η ρύθμιση του ελέγχου ταυτότητας δύο παραγόντων (2FA) ή του ελέγχου ταυτότητας πολλών παραγόντων (MFA) σημαίνει ότι ακόμη και αν κάποιος εντοπίσει τον κωδικό πρόσβασής σας, **πιθανότατα δεν θα έχουν τον πρόσθετο παράγοντα που χρειάζεται για να μπουν.**



Ρίξτε μια ματιά στις ρυθμίσεις ασφαλείας των ιστότοπων και των εφαρμογών που χρησιμοποιείτε περισσότερο για να δείτε εάν μπορείτε να ρυθμίσετε αυτό το επιπλέον κλειδί. Ξεκινήστε με τις πιο σημαντικές - τυχόν εφαρμογές οικονομικών ζητημάτων ή υπηρεσίες όπως το email, τις οποίες χρησιμοποιείτε για την ανάκτηση των άλλων λογαριασμών σας.

Google:
Συνδεθείτε στο myaccount.google.com → Ασφάλεια → Επαλήθευση σε 2 βήματα → Έναρξη

Facebook:
μενού → Ρυθμίσεις → *Ασφάλεια και Σύνδεση* → Έλεγχος Ταυτότητας Δύο Παραγόντων

Συμβουλή: Κατά τη δημιουργία ενός επιπλέον επιπέδου επαλήθευσης, θα πρέπει να επιλέξετε έναν δεύτερο τρόπο επιβεβαίωσης ότι είστε εσείς. Προσπαθήστε να αποφύγετε τη χρήση SMS (μηνύματα κειμένου που αποστέλλονται στον αριθμό του τηλεφώνου σας) ως δεύτερο παράγοντα, σε περίπτωση που χάσετε το τηλέφωνό σας. Το email είναι συνήθως μια πιο αξιόπιστη επιλογή.