4.

ΜΕΙΩΣΤΕ ΤΑ ΙΧΝΗ ΣΑΣ

Τα τηλέφωνα, οι ταμπλέτες και οι υπολογιστές τείνουν να έχουν προεγκατεστημένα προγράμματα περιήγησης που δεν δίνουν προτεραιότητα στο απόρρητό σας. Στη θέση τους μπορείτε να **κατεβάσετε και να χρησιμοποιήσετε ένα πρόγραμμα περιήγησης** που διατηρεί ήδη τη διαδικτυακή δραστηριότητά σας περισσότερο ιδιωτική ως προεπιλογή, προστατεύοντας σας από προγράμματα παρακολούθησης.

Και για επιπλέον προστασία απορρήτου, μπορείτε να εγκαταστήσετε κάποια επιπλέον προγράμματα, γνωστά και σαν "πρόσθετα και επεκτάσεις" (αυτά τα μίνι-προγράμματα είναι εύκολα στην εγκατάσταση στον περιηγητή σας **τα οποία κάνουν την διαδικτυακή σας δραστηριότητα ακόμα πιο ιδιωτική**).

5.

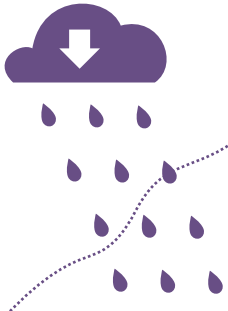
ΑΦΑΙΡΕΣΤΕ ΤΙΣ ΕΤΙΚΕΤΕΣ (TAGS) ΑΠΟ ΤΟΝ ΕΑΥΤΟ ΣΑΣ ΚΑΙ ΤΟΥΣ ΑΛΛΟΥΣ

Μήπως έχετε συμβάλει στη συγκέντρωση δεδομένων των φίλων σας επισημαίνοντάς τους (tag) σε φωτογραφίες και δημοσιεύσεις στο παρελθόν; Ελαφρύνετε τη φόρτωση των δεδομένων τους (αλλά και τη συνείδησή σας κατά τη διαδικασία αυτή) **αφαιρώντας την επισήμανση από αυτούς** σε όσες περισσότερες φωτογραφίες και δημοσιεύσεις μπορείτε.

Μεταδώστε το! Ενθαρρύνετε τους φίλους, την οικογένεια και τους συναδέλφους σας να συμμετάσχουν στον έλεγχο των δεδομένων που κοινοποιούνται. Εάν εργαστούμε όλοι μαζί για να ελέγξουμε τα ίχνη των δεδομένων μας, μπορούμε να βοηθήσουμε καλύτερα ο ένας τον άλλον στην αποτοξίνωση.

Για να αποκλείσετε κατασκοπευτικές διαφημίσεις και αόρατα προγράμματα ιχνηλάτησης, εγκαταστήστε το uBlock Origin (για Chrome, Safari και Firefox) ή το Privacy Badger (για Chrome, Firefox και Opera).

Για να βεβαιωθείτε ότι οι συνδέσεις σας σε ιστότοπους είναι ασφαλείς όπου αυτό είναι εφικτό, εγκαταστήστε το HTTPS Everywhere: αυτή είναι μια επέκταση προγράμματος περιήγησης που διασφαλίζει ότι η επικοινωνία σας με πολλούς σημαντικούς ιστότοπους είναι κρυπτογραφημένη και προστατευμένη κατά τη μεταφορά.



DATA DETOX KIT

ΕΛΕΓΞΤΕ ΤΑ ΔΕΔΟΜΕΝΑ ΤΟΥ SMARTPHONE ΣΑΣ

για να αυξήσετε την προστασία της διαδικτυακής ιδιωτικής ζωής σας

Εάν αναλογιστείτε τι φανερώνουν στους άλλους τα δεδομένα σας σχετικά με εσάς, μπορεί να μη φαίνεται τόσο σημαντικό: ποιος νοιάζεται αν είστε λάτρης της μουσικής κάντρι, αν σας αρέσει να αγοράζετε περισσότερα παπούτσια από όσα χρειάζεστε ή αν ξεκινάτε να σχεδιάζετε τις επόμενες διακοπές σας έναν χρόνο νωρίτερα;

Το πρόβλημα έγκειται στο τι συμβαίνει με τα δεδομένα σας. Όταν συλλέγονται για μεγάλο χρονικό διάστημα, **προκύπτουν προσωπικά ψηφιακά μοτίβα**: οι συνήθειες, οι κινήσεις, οι σχέσεις, οι προτιμήσεις, οι πεποιθήσεις και τα μυστικά σας αποκαλύπτονται σε όσους αναλύουν και βγάζουν κέρδος από αυτά, όπως επιχειρήσεις και μεσάζοντες εμπορίας δεδομένων.

Καθώς ακολουθείτε αυτήν την Αποτοξίνωση Δεδομένων, θα πάρετε μια ιδέα για το πώς και γιατί συμβαίνουν όλα αυτά, και θα μάθετε πρακτικά βήματα για να ελέγχετε τα ίχνη των δεδομένων σας στο διαδίκτυο.

Ας ξεκινήσουμε!

Ένα προϊόν από
TACTICAL TECH

Μετάφραση

datadetoxkit.org/gr
#datadetox

1.

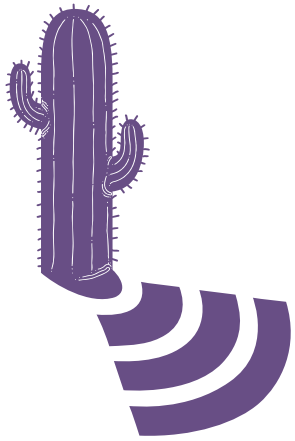
ΑΛΛΑΞΤΕ ΤΟ ΟΝΟΜΑ ΤΗΣ ΣΥΣΚΕΥΗΣ ΣΑΣ

Κάποια στιγμή μπορεί να χρειάστηκε να «ονομάσατε» το τηλέφωνό σας λόγω Wi-Fi, Bluetooth ή και τα δύο, ή ίσως το όνομα δημιουργήθηκε αυτόματα κατά την εγκατάσταση.

Αυτό σημαίνει ότι το «Τηλέφωνο του Άλεξ Τσανγκ» είναι αυτό που είναι ορατό στον κάτοχο του δικτύου Wi-Fi, και αν το Bluetooth σας είναι ενεργοποιημένο, είναι ορατό και σε οποιονδήποτε στην περιοχή που έχει επίσης ενεργοποιημένο το Bluetooth του.

Σίγουρα δεν θα ανακοινώνατε το όνομά σας κατά την είσοδό σας σε ένα καφέ, εστιατόριο ή αεροδρόμιο, επομένως ούτε το τηλέφωνό σας.

Μπορείτε να **αλλάξετε το όνομα του τηλεφώνου σας σε κάτι που να περιορίζει την ταυτοποίησή σας,** παραμένοντας ωστόσο ο εαυτός σας. Δείτε πώς:



iPhone:
Αλλαγή ονόματος τηλεφώνου:
Ρυθμίσεις → Γενικά → Σχετικά → Αλλάξτε το όνομα

Android:
Αλλαγή ονόματος Wi-Fi:
Ρυθμίσεις → Wi-Fi → μενού → Για προχωρημένους / Περισσότερες λειτουργίες → Wi-Fi Απευθείας → Μετονομασία Συσκευής

Αλλαγή ονόματος Bluetooth:
Ρυθμίσεις → Bluetooth → Ενεργοποιήστε το Bluetooth αν είναι απενεργοποιημένο → μενού → Μετονομασία Συσκευής → Απενεργοποιήστε το Bluetooth

2.

ΚΑΘΑΡΙΣΤΕ ΤΑ ΙΧΝΗ ΤΗΣ ΤΟΠΟΘΕΣΙΑΣ ΣΑΣ

Παρόλο που μπορεί να φαίνεται ότι τα δεδομένα της τοποθεσίας σας είναι απλά τυχαία κομμάτια πληροφοριών, εάν συνδυαστούν όλα μαζί, θα μπορούσαν να αποκαλύψουν **σημαντικές λεπτομέρειες για εσάς** και τις συνήθειές σας, όπως πού ζείτε, πού εργάζεστε και πού σας αρέσει να βρίσκεστε με τους φίλους σας. Αυτό είναι που το κάνει ιδιαίτερα περιζήτητο σε πολλές εταιρείες και μεσάζοντες εμπορίας δεδομένων.

Μπορεί να είναι φυσιολογικό, ας πούμε, η εφαρμογή χαρτών σας να έχει πρόσβαση στο που βρίσκεστε. Αλλά ίσως εκπλαγείτε όταν δείτε σε πόσες εφαρμογές έχετε δώσει άδεια πρόσβασης στην τοποθεσία σας. Αυτό που μπορείτε να κάνετε είναι να **ανατρέξετε στις άδειες κάθε εφαρμογής και να απενεργοποιήσετε τις υπηρεσίες τοποθεσίας.** Αναζητήστε τις εφαρμογές που η τοποθεσία δεν είναι πραγματικά αναγκαία για την υπηρεσία (χρειάζεται πράγματι αυτό το παιχνίδι να γνωρίζει που βρίσκεστε;) και αυτές που δεν θέλετε εσείς να την γνωρίζουν;

Android:
Ρυθμίσεις → Εφαρμογές → Διαχειριστείτε την πρόσβαση τοποθεσίας ανά εφαρμογή

iPhone:
Ρυθμίσεις → Απόρρητο → Υπηρεσίες τοποθεσίας → Διαχειριστείτε την πρόσβαση τοποθεσίας ανά εφαρμογή

3.

ΤΑΚΤΟΠΟΙΗΣΤΕ ΤΙΣ ΕΦΑΡΜΟΓΕΣ ΣΑΣ

Οι εφαρμογές των μέσων κοινωνικών δικτύωσης, τα παιχνίδια και οι εφαρμογές για τον καιρό ενδιαφέρονται για τα δεδομένα σας … και ίσως να συλλέγουν πολλά από αυτά.

Η απαλλαγή από αυτές τις τυχαίες εφαρμογές στο τηλέφωνό σας που δεν χρησιμοποιείτε ποτέ μπορεί να είναι ένας ισχυρός τρόπος για να αποτοξινώσετε τον ψηφιακό εαυτό σας.

Επιπλέον, η τακτοποίηση μπορεί επίσης να ελευθερώσει χώρο στο τηλέφωνό σας, να μειώσει τη χρήση των δεδομένων και να αυξήσει τη διάρκεια ζωής της μπαταρίας. Αυτό μπορεί ακόμη και να αυξήσει τη συνολική απόδοση, ανάλογα με την εφαρμογή.

Android:
Ρυθμίσεις → Εφαρμογές → Επιλέξτε την εφαρμογή που θέλετε να απεγκαταστήσετε → Απεγκαταστήστε

iPhone:
Πατήστε και κρατήστε πατημένο ένα εικονίδιο εφαρμογής μέχρι να εμφανιστεί ένα μενού.

Πατήστε την επιλογή διαγραφής της εφαρμογής από τη λίστα.

Επιβεβαιώστε τη διαγραφή της εφαρμογής.

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.

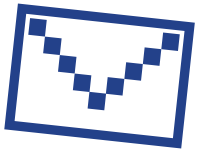
Τα δυνατότερα των passwords χρησιμοποιούν έναν συνδυασμό γραμμάτων, αριθμών και ειδικών συμβόλων. Αυτή η πολύτιμη συμβουλή εξακολουθεί να δημιουργεί έναν ισχυρότερο, πιο δύσκολο να μαντέψει κανείς κωδικό πρόσβασης. Κάποια συστήματα κωδικών πρόσβασης δυστυχώς δεν επιτρέπουν τη χρήση ειδικών συμβόλων (όπως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

4.

ΚΑΝΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ ΝΑ ΑΚΟΥΣΤΕΙ

Αν δεν είστε χαρούμενοι με τους εθιστικούς και πειστικούς σχεδιασμούς ή την παραπληροφόρηση σε ιστοσελίδες, μπορείτε να στείλετε email, να γράψετε στο Twitter και να γνωστοποιήσετε στις εταιρείες ότι δεν συμφωνείτε με τις πρακτικές τους. Όταν οι εταιρείες πιέζονται να κάνουν κάτι από τους χρήστες τους (από τα πιο πολύτιμα περιουσιακά τους στοιχεία) υπάρχει μια πιθανότητα να αλλάξουν.

Αν δεν νιώθετε ότι η γνώμη σας δεν ακούγεται, υπάρχει κάτι πραγματικά δυνατό που μπορείτε να κάνετε: χρησιμοποιήστε ένα διαφορετικό site ή εφαρμογή. Αν τους έχετε δείξει ότι είστε δυσαρεστημένοι με κάτι που κάνει μια ιστοσελίδα ή εφαρμογή και τους ενημερώσετε ότι σταματήσατε να τη χρησιμοποιείτε ή την απεγκαταστήσετε(και το τολμήσουν και άλλοι άνθρωποι) **θα το παρατηρήσουν**.

5.

ΔΙΑΔΩΣΤΕ ΤΟ

Διαδώστε το! Αυτή είναι μια συμβουλή που ξεχνιέται εύκολα, αλλά μπορεί να έχει μεγάλη επίδραση. Πείτε στον περίγυρό σας, την οικογένεια και τους συνεργάτες σας για τα πράγματα που παρατηρείτε και ζητήστε τους ακόμη να έρθουν μαζί σας σε αυτό το detox!

Όλοι παλεύουν να διαχειριστούν τις τηλεφωνικές τους συνήθειες. Το σημαντικό είναι να βρείτε έναν τρόπο που να είναι σωστός για εσάς και να ταιριάζει στον τρόπο ζωής σας. Πειραματιστείτε μέχρι να βρείτε τι σας ταιριάζει πραγματικά και κάντε update στις συνήθειες σας καθώς αλλάζουν οι ανάγκες σας. Δεν υπάρχει μια λύση που να τα κάνει όλα.

Και τέλος, ενημερώστε για τις επιλογές που κάνετε σχετικά με την τεχνολογία με τους γύρω σας. Ας πούμε, αποφασίστε ότι δεν θα είστε προσβάσιμοι στο messenger κάθε μέρα μετά τις 8μμ επειδή τότε ξεκινάτε τη ρουτίνα σας μακριά απ' την οθόνη: πείτε το στην οικογένεια και τον περίγυρό σας σας έτσι ώστε αντ' αυτού να σας πάρουν τηλέφωνο ή να έρθουν στο σπίτι σας.

Κρατήστε ανοιχτό τον διάλογο, κάντε ερωτήσεις, λάβετε απαντήσειςκαι θα μπορείτε να ζήσετε μια ισορροπημένη διαδικτυακή ζωή που θα σας ταιριάζει.

DATA DETOX KIT

ΑΠΟΦΥΓΕΤΕ ΤΙΣ ΠΡΟΕΠΙΛΟΓΕΣ

Για να ενδυναμώσετε την ψηφιακή σας ευημερία

Πότε ήταν η τελευταία φορά που «βγήκατε απ' την πρίζα» και δεν αγγίξατε κάτι τεχνολογικό για μια μέρα ή τουλάχιστον για μια ώρα; Αν είστε συνεχώς online, δεν είστε μόνοι. Ένας μέσος άνθρωπος αγγίζει, κάνει κλικ και swipe στο τηλέφωνό του πάνω από 2,600 φορές την ημέρα (source). Αν κάνετε κάτι τέτοιο τόσο συχνά, θα θέλετε αυτό να αξίζει. Πώς μπορείτε να είστε σίγουροι ότι ο χρόνος που περνάτε στη συσκευή σας είναι ποιοτικός;

Ξεκινήστε γνωρίζοντας ότι η ακαταμάχητη έλξη προς την τεχνολογία δεν είναι δικό σας λάθος! Είτε το πιστεύετε είτε όχι, οι αγαπημένες εφαρμογές και ιστοσελίδες είναι σχεδιασμένες με τέτοιο τρόπο ώστε η κάθε λειτουργία, το κάθε χρώμα και ο κάθε ήχος να έχει 'τελειοποιηθεί' για να σας κρατάει αγκιστρωμένους, πεπεισμένους να επιστρέφετε για περισσότερο.

Θέλετε να βρείτε μια πιο υγιή ισορροπία ανάμεσα στην online και offline ζωή σας; Σε αυτή την ενότητα του Data Detox θα μάθετε περισσότερα.

Ας ξεκινήσουμε!

Ένα προϊόν από
TACTICAL TECH

Μετάφραση

datadetoxkit.org/gr
#datadetox

1.

ΝΑ ΕΧΕΤΕ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ ΣΤΗΝ ΠΑΡΟΥΣΑ ΣΤΙΓΜΗ

Αυτή η συμβουλή είναι πιο δύσκολη απ' ό,τι ακούγεται. Το να παραμένεις στην στιγμή απαιτεί καθημερινή εξάσκηση. Είναι σαν ένας μυς στον εγκέφαλό σας τον οποίο πρέπει να εξασκείτε τακτικά για να χτίσετε τη δύναμή του. Ξεκινήστε με το να παρατηρήσετε τη σχέσης σας με την τεχνολογία που χρησιμοποιείτε.

Πόση ώρα περνάτε στο τηλέφωνό σας;

Αν η απάντηση δεν σας προκαλεί χαρά υπάρχουν ρυθμίσεις και τεχνικές που μπορείτε να ακολουθήσετε για να ανακτήσετε τον έλεγχο πάνω στη χρήση της τεχνολογίας.

Αν στόχος σας είναι να περνάτε λιγότερο χρόνο στο Facebook, το Instagram ή το Snapchat, αλλάξτε τις ρυθμίσεις και τα δικαιώματα αυτών των εφαρμογών έτσι ώστε να δουλεύουν καλύτερα για εσάς. Κάποιες εφαρμογές όπως το Instagram έχουν μια επιλογή με την οποία η εφαρμογή ευγενικά σας υπενθυμίζει πώς φτάσατε το ημερήσιο χρονικό σας όριο.

Instagram:
Προφίλ → μενού → Ρυθμίσεις → Λογαριασμός → Η Δραστηριότητά σας → Ορισμός Καθημερινής Υπενθύμισης

Επίσης, υπάρχουν εφαρμογές οι οποίες σας βοηθούν να μετρήσετε την χρήση σας. Τα Android και τα iPhone παρέχουν πλέον τρόπους ελέγχου των συνήθειων σας. Για παράδειγμα: η εφαρμογή Ψηφιακή Ευημερία της Google αλλά και η Ενημέρωση iOS. Αυτές οι υπηρεσίες θα σας πουν πόσο συχνά κοιτάτε το τηλέφωνό σας και παρέχουν ρυθμίσεις που μπορούν να σας βοηθήσουν στον έλεγχο της χρήσης.

2.

ΒΡΕΙΤΕ ΤΑ ΣΧΕΔΙΑΣΤΙΚΑ ΤΡΙΚ

Ο πειστικός σχεδιασμός (persuasive design), επίσης γνωστός ως «τα μαύρα μοτίβα»(dark patterns), είναι designs βασισμένα πάνω στην ανθρώπινη ψυχολογία τα οποία χρησιμοποιούνται για να σας εξωθήσουν να γραφτείτε κάπου, να αγοράσετε κάτι ή να δώσετε περισσότερες προσωπικές πληροφορίες από όσες νομίζετε ή προτίθεστε.

Κοινές σχεδιαστικές παροτρύνσεις μπορεί να περιλαμβάνουν την χρήση συγκεκριμένων χρωμάτων, την τοποθέτηση των κουμπιών, ασαφή κείμενα ή ελλιπείς πληροφορίες. Μερικές φορές αυτά τα τρικ είναι προφανή, ωστόσο άλλες φορές είναι πιο δύσκολο να εντοπιστούν. Μπορεί ήδη να έχετε συναντήσει κάποιες από αυτές όταν εγγράφεστε για μία συνδρομή είτε όταν κάνετε ηλεκτρονικές αγορές. Ο λόγος που βλέπετε αυτά τα σχεδιαστικά τρικ παντού είναι επειδή δουλεύουν - μας καταφέρνουν να κάνουμε κλικ, εγγραφές, να αγοράζουμε πιο συχνά και συνεχώς να επανερχόμαστε.

Όσο περισσότερο γνωρίζετε τις προτροπές και τους λεπτούς χειρισμούς που ενσωματώνονται στις ιστοσελίδες που χρησιμοποιείτε, τόσο περισσότερο εξοικειωμένοι και πληροφορημένοι θα γίνετε.

Υπάρχει μια πλειάδα πραγμάτων που μπορείτε να κάνετε για να είστε πιο έξυπνοι από τις εφαρμογές σας.

Αναγνωρίστε πότε κάποια εφαρμογή σας προτρέπει να πραγματοποιήσετε μια ενέργεια: Το πρώτο πράγμα που μπορείτε να κάνετε είναι απλά να έχετε επίγνωση της χρήσης αυτών των τεχνικών.

Μοιραστείτε τα Screenshots: Τραβήξτε ένα στιγμιότυπο απ' την οθόνη σας κάθε φορά που συναντάτε πειστικούς σχεδιασμούς στο διαδίκτυο και μοιραστείτε τα με τις φίλες σας (παραλείποντας οποιεσδήποτε προσωπικές σας λεπτομέρειες – η ιδιωτικότητα πρώτα!). Μπορείτε επίσης να ζητήσετε απ' τις εταιρείες να αλλάξουν τις πρακτικές τους.

Παραμείνετε ήρεμοι: Αν υπάρχει κάποιο ρολόι αντίστροφης μέτρησης σε μια σελίδα αγορών, αναρωτηθείτε, «Είναι πραγματικά επείγον;» Αν βρεθείτε να κάνετε κλικ σε ένα κουμπί όταν δεν θέλατε πραγματικά, σκεφτείτε τη διατύπωση που έχει χρησιμοποιηθεί πάνω στα κουμπιά ή τα χρώματα που χρησιμοποιεί η υπηρεσία. Αν αισθανθείτε σύγχυση, μην σκεφτείτε αυτόματα ότι κάνετε λάθος -σκεφτείτε τις λέξεις που χρησιμοποιεί η ιστοσελίδα ή η εφαρμογή, καθώς μπορεί να είναι ασαφείς.

3.

ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΑ MEDIA

Ακριβώς όπως μπορείτε να μάθετε να είστε πιο έξυπνοι από τις λειτουργίες και τα design τα οποία προσπαθούν συνεχώς να σας πείσουν να κάνετε scroll και click, μπορείτε επίσης να γίνετε καλοί στο να διακρίνετε νέα ή post τα οποία στοχεύουν στον να σας παραπλανήσουν.

Θα έχετε ακούσει ήδη σχετικά με το πρόβλημα της 'παραπληροφόρησης' και τα 'fake news'. Μπορείτε να ανακαλύπτετε την παραπληροφόρηση εάν συνηθίσετε να ασκείτε κριτική για όλα τα νέα τα οποία διαβάζετε, ειδικά εάν αυτά μοιάζουν να είναι αναπάντεχα, εξωφρενικά ή πολύ καλά για να είναι αληθινά.

Τελικά, θα θέλετε να επιβεβαιώνετε ποια νέα είναι αληθινά ή ψεύτικα - ειδικά αν σκοπεύετε να τα μοιραστείτε με φίλους ή την οικογένεια σας.

Από ποια ιστοσελίδα είναι αυτό;
Ποιος το έγραψε (και πότε);
Τι λέει ολόκληρο το άρθρο, πέρα από τον τίτλο;
Ποιες είναι οι πηγές στις οποίες αναφέρεται;

Εάν νομίζετε ότι είναι παραπλανητικό και θέλετε να το σταματήσετε από το να διαδοθεί, οι περισσότερες πλατφόρμες έχουν ένα σημείο στις ιστοσελίδες τους όπου μπορείτε να αναφέρετε το άρθρο. Μπορείτε επίσης να αποφασίσετε εάν θα σταματήσετε να ακολουθείτε τον λογαριασμό ο οποίος το δημοσιοποίησε.