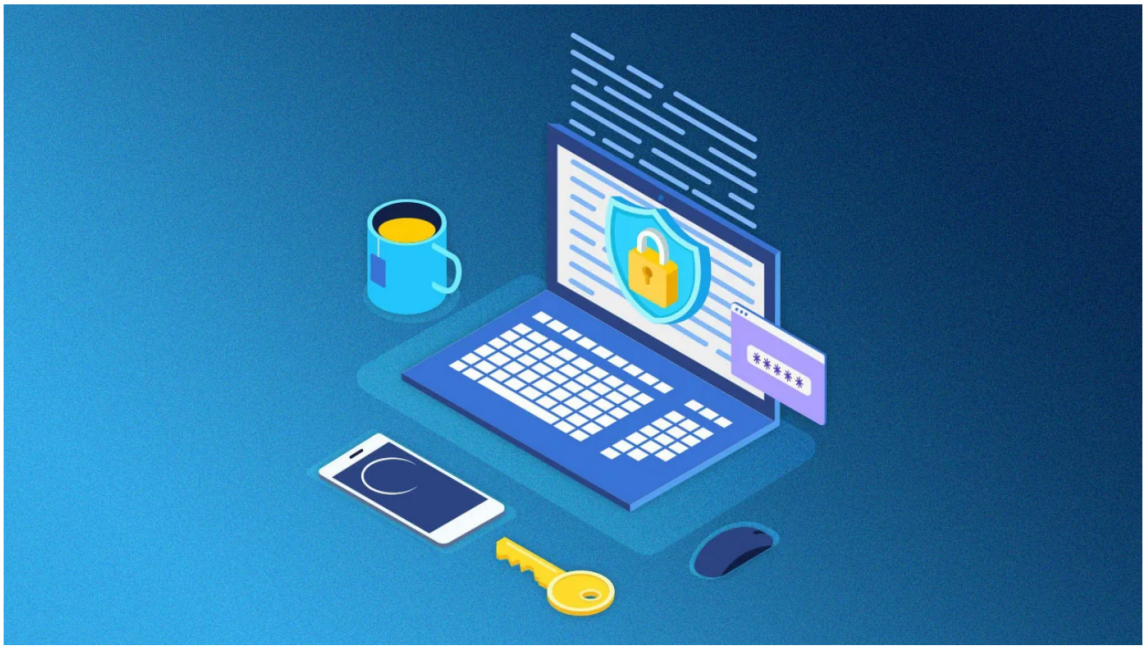
12 απλά πράγματα που μπορείτε να κάνετε για να είστε πιο ασφαλείς στο διαδίκτυο

κολουθήστε αυτές τις απλές συμβουλές για να προστατεύσετε τις συσκευές, τα δεδομένα και την ταυτότητά σας στο διαδίκτυο.

από Βαγγέλης Κομνής Ιούλ 30, 2022



8. Χρησιμοποιήστε διαφορετικές διευθύνσεις email για διαφορετικούς τύπους λογαριασμών

(Image: Getty Images/Nadezhda Buravleva)

Δεν περνάει μια μέρα χωρίς να ακούσουμε για άλλη μια παραβίαση δεδομένων. Όταν μια μεγάλη εταιρεία με χαλαρή ασφάλεια εκθέτει τα προσωπικά σας δεδομένα, πληροφορίες κωδικών πρόσβασης ή φωτογραφίες, δεν μπορείτε να κάνετε τίποτα γι 'αυτό. Αντίθετα, εστιάστε στον εαυτό σας και στην προστασία της ασφάλειας και της ιδιωτικής σας ζωής στο σπίτι. Δεν θέλετε να χάσετε όλες τις φωτογραφίες σας από ένα ransomware ή να χάσετε όλα τα χρήματα σας από ένα Trojan, σωστά;

Το να κάνετε τις συσκευές σας, την ταυτότητά σας στο διαδίκτυο και τις δραστηριότητές σας πιο ασφαλείς, πραγματικά δεν απαιτεί μεγάλη προσπάθεια. Στην πραγματικότητα, πολλές από τις συμβουλές μας σχετικά με το τι μπορείτε να κάνετε για να είστε πιο ασφαλείς στο διαδίκτυο συνοψίζονται σε κάτι περισσότερο από την κοινή λογική. Τα παρακάτω tips θα σας βοηθήσουν να παραμείνετε ασφαλείς.

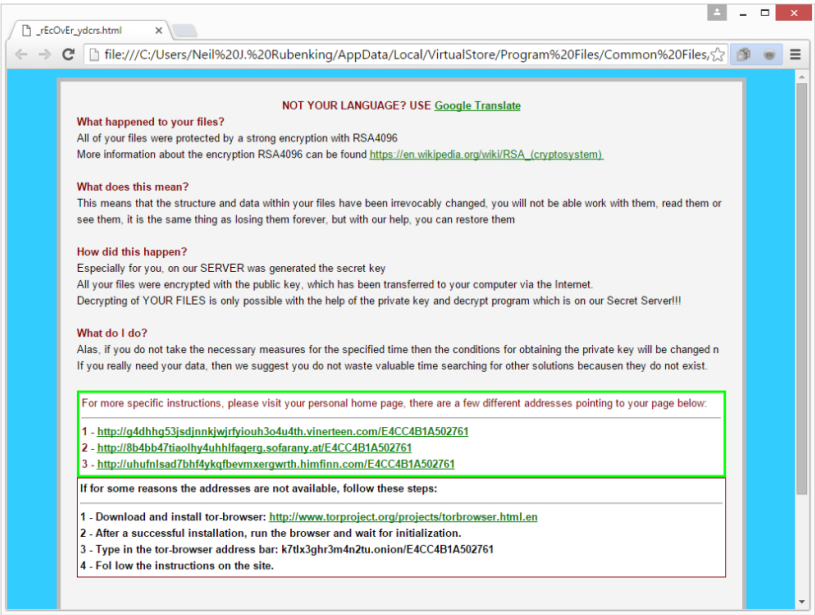
1. Εγκαταστήστε ένα Antivirus και διατηρήστε το ενημερωμένο

Τα **antivirus** μπορεί να θεωρούνται λογισμικά προστασίας από ιούς, αλλά στην πραγματικότητα σας προστατεύουν από διάφορες κυβερνοαπειλές. Το **Ransomware** κρυπτογραφεί τα αρχεία σας και απαιτεί πληρωμή για την επαναφορά τους. Τα **Trojan** φαίνονται σαν έγκυρα προγράμματα, αλλά από πίσω, κλέβουν τις προσωπικές σας πληροφορίες. Τα **bots** μετατρέπουν τον υπολογιστή σας σε στρατιώτη σε έναν "στρατό ζόμπι", έτοιμο να εμπλακεί σε μια επίθεση **DDoS**, να στείλει ανεπιθύμητα μηνύματα ή οτιδήποτε άλλο διατάξει αυτός που έχει τον έλεγχο. Ένα αποτελεσματικό **antivirus** προστατεύει από αυτά και πολλά άλλα είδη **malware**.

Θεωρητικά, μπορείτε να ρυθμίσετε το **antivirus** σας και να το αφήσετε να κάνει τη δουλειά του στο παρασκήνιο. Στην πράξη, θα πρέπει να το κοιτάζετε συχνά. Τα περισσότερα βοηθητικά προγράμματα προστασίας από ιούς εμφανίζουν ένα **banner** ή ένα εικονίδιο για να σας δείξουν την κατάσταση του υπολογιστή. Εάν ανοίξετε το πρόγραμμα και δείτε κίτρινο ή κόκκινο χρώμα, ακολουθήστε τις οδηγίες για να επαναφέρετε τα πράγματα στη σωστή τους πορεία.

Μπορεί να σκεφτείτε ότι τα **Windows** έχουν ήδη εγκαταστημένο ένα **antivurs**. Το Microsoft Windows Defender Security Center όχι μόνο ενσωματώνεται στο λειτουργικό σύστημα, αλλά αναλαμβάνει αυτόματα την προστασία όταν δεν εντοπίζει κανένα άλλο πρόγραμμα προστασίας από ιούς και το ίδιο αυτόματα παραμερίζεται όταν εγκαθιστάτε προστασία τρίτων. Το θέμα είναι ότι αυτό το ενσωματωμένο **antivirus** δεν συγκρίνεται με τις καλύτερες λύσεις άλλων κατασκευαστών. Ακόμη και τα καλύτερα δωρεάν **AV** είναι πολύ καλύτερα από το **Windows Defender**. Μην βασίζεστε λοιπόν σε αυτό όταν υπάρχουν καλύτερες λύσεις προστασίας.

Είτε έχετε επιλέξει ένα απλό πρόγραμμα προστασίας από ιούς είτε μια πλήρη σουίτα ασφαλείας, θα πρέπει να το ανανεώνετε κάθε χρόνο. Μπορείτε πάντα να διακόψετε την συνδρομή σας, εάν έχετε την επιθυμία να μεταβείτε σε διαφορετικό προϊόν.



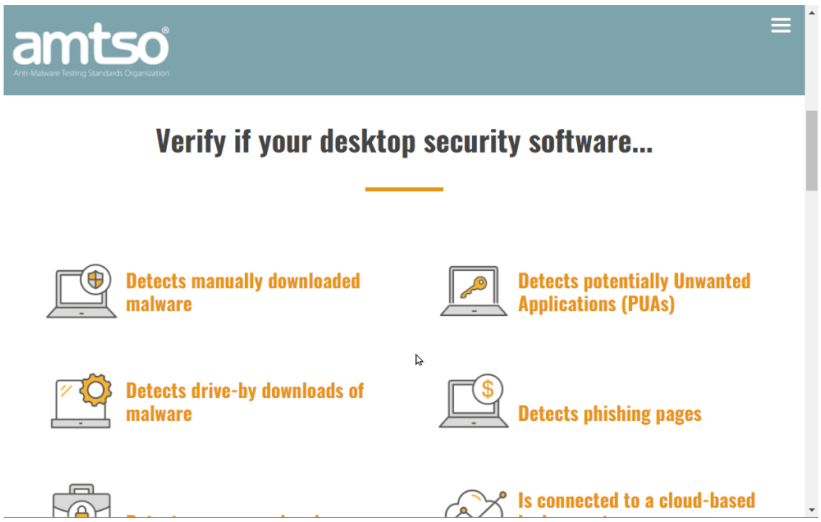
Ακόμη ένα πράγμα. Εάν η σουίτα προστασίας από ιούς ή η σουίτα ασφαλείας δεν διαθέτει προστασία για ransomware, σκεφτείτε να προσθέσετε ένα ξεχωριστό επίπεδο προστασίας. Πολλά βοηθητικά προγράμματα ειδικά για **ransomware** είναι εντελώς δωρεάν, επομένως δεν υπάρχει λόγος να μην δοκιμάσετε μερικά από αυτά και να επιλέξετε αυτό που σας ταιριάζει καλύτερα.

2. Εξερευνήστε τα εργαλεία ασφαλείας που έχετε εγκαταστήσει στον υπολογιστή σας

Πολλές εφαρμογές και ρυθμίσεις βοηθούν στην προστασία των συσκευών και της ταυτότητάς σας, αλλά είναι πολύτιμες μόνο εάν γνωρίζετε πώς να τις χρησιμοποιείτε σωστά. Για να έχετε τη μέγιστη χρησιμότητα από αυτά τα εργαλεία, πρέπει να κατανοήσετε τα χαρακτηριστικά και τις ρυθμίσεις τους. Για παράδειγμα, το **smartphone** σας είναι σχεδόν βέβαιο ότι περιλαμβάνει μια επιλογή για να το βρείτε αν χαθεί, και ίσως να το έχετε ενεργοποιήσει. Το έχετε δοκιμάσει όμως, ώστε να ξέρετε πώς να το χρησιμοποιήσετε εάν χρειαστεί;

Τα περισσότερα εργαλεία προστασίας από ιούς έχουν τη δύναμη να αποκρούουν τις δυνητικά

ανεπιθύμητες εφαρμογές (PUA), ενοχλητικές εφαρμογές που δεν είναι ακριβώς κακόβουλο λογισμικό, αλλά δεν κάνουν τίποτα ωφέλιμο. Η ανίχνευση PUA δεν έρχεται ενεργοποιημένη εξαρχής σε όλα τα λογισμικά. Ελέγξτε τις ρυθμίσεις ανίχνευσης και βεβαιωθείτε ότι οι δικές σας έχουν διαμορφωθεί έτσι ώστε να αποκλείουν αυτά τα παράσιτα. Ομοίως, η σουίτα ασφαλείας σας μπορεί να έχει στοιχεία που δεν είναι ενεργά μέχρι να τα ενεργοποιήσετε. Όταν εγκαθιστάτε ένα νέο προϊόν ασφαλείας, ξεφυλλίστε όλες τις σελίδες του κύριου παραθύρου και τουλάχιστον ρίξτε μια ματιά στις ρυθμίσεις. Εάν σας προσφέρει μια αρχική ξενάγηση, μην την παραλείψετε, αντίθετα περάστε την περιήγηση μεθοδικά, δίνοντας προσοχή σε όλα τα χαρακτηριστικά.



Για να βεβαιωθείτε ότι το antivirus σας έχει ρυθμιστεί και λειτουργεί σωστά, μπορείτε να μεταβείτε στη σελίδα ελέγχου λειτουργιών ασφαλείας στον ιστότοπο του AMTSO (Οργανισμός προτύπων δοκιμών κατά του κακόβουλου λογισμικού). Εάν το πρόγραμμα προστασίας από ιούς δεν περάσει την δοκιμή, ήρθε η ώρα να επικοινωνήσετε με την τεχνική υποστήριξη και να μάθετε γιατί.

3. Χρησιμοποιήστε μοναδικούς κωδικούς πρόσβασης για κάθε σύνδεση

Ένας από τους ευκολότερους τρόπους με τους οποίους οι χάκερ κλέβουν πληροφορίες είναι λαμβάνοντας συνδυασμούς ονομάτων χρήστη και κωδικών πρόσβασης από μια πηγή και δοκιμάζοντας τους ίδιους συνδυασμούς αλλού. Για παράδειγμα, ας υποθέσουμε ότι οι χάκερ πήραν το όνομα χρήστη και τον κωδικό πρόσβασής σας παραβιάζοντας έναν πάροχο email. Μπορεί να προσπαθήσουν να συνδεθούν σε τραπεζικούς λογαριασμός ή μεγάλα ηλεκτρονικά καταστήματα χρησιμοποιώντας τον ίδιο συνδυασμό ονόματος χρήστη και κωδικού πρόσβασης. Ο μοναδικός καλύτερος τρόπος για να αποτρέψετε μια παραβίαση δεδομένων από το να έχει το λεγόμενο "domino effect" είναι να χρησιμοποιήσετε έναν ισχυρό, μοναδικό κωδικό πρόσβασης για κάθε μεμονωμένο διαδικτυακό λογαριασμό που έχετε.

Η δημιουργία ενός μοναδικού και ισχυρού κωδικού πρόσβασης για κάθε λογαριασμό δεν είναι δουλειά για έναν άνθρωπο. Αυτός είναι ο λόγος για τον οποίο χρησιμοποιείτε τη δημιουργία τυχαίων κωδικών πρόσβασης που είναι ενσωματωμένη στους password managers. Αρκετοί πολύ καλοί διαχειριστές κωδικών πρόσβασης είναι δωρεάν και χρειάζεται λίγος χρόνος για να αρχίσετε να τους χρησιμοποιείτε. Ωστόσο, οι διαχειριστές κωδικών πρόσβασης επί πληρωμή προσφέρουν γενικά περισσότερες δυνατότητες. Από την άλλη, εάν έχετε γνώσεις προγραμματισμού μπορείτε να φτιάξετε έναν "σπιτικό password manager", ο οποίος ίσως να μην έχει τις ίδιες δυνατότητες αλλά σίγουρα θα καλύψει κάποιες ανάγκες σας.

Όταν χρησιμοποιείτε έναν password manager, ο μόνος κωδικός πρόσβασης που πρέπει να θυμάστε είναι ο κύριος κωδικός πρόσβασης που κλειδώνει τον ίδιο τον password manager. Όταν ξεκλειδωθεί, σάς συνδέει αυτόματα στους διαδικτυακούς λογαριασμούς σας. Αυτό όχι μόνο σας βοηθά να παραμείνετε πιο ασφαλείς, αλλά αυξάνει επίσης την αποτελεσματικότητα και την παραγωγικότητά σας. Δεν θα ξοδεύετε πλέον χρόνο πληκτρολογώντας τα στοιχεία σύνδεσής σας ή αντιμετωπίζοντας τη χρονοβόρα διαδικασία της επαναφοράς ενός ξεχασμένου κωδικού πρόσβασης.

4. Αποκτήστε ένα VPN και χρησιμοποιήστε το

Κάθε φορά που συνδέεστε στο Διαδίκτυο χρησιμοποιώντας ένα δίκτυο Wi-Fi που δεν σας ανήκει, θα πρέπει να χρησιμοποιείτε ένα VPN. Ας πούμε ότι πηγαίνετε σε μια καφετέρια και συνδέεστε σε ένα δωρεάν δίκτυο Wi-Fi. Δεν ξέρετε τίποτα για την ασφάλεια αυτής της σύνδεσης. Είναι πιθανό κάποιος άλλος σε αυτό το δίκτυο, χωρίς να το γνωρίζετε, να αρχίσει να ψάχνει ή να κλέβει τα αρχεία και τα δεδομένα που αποστέλλονται από τον φορητό υπολογιστή ή την κινητή συσκευή σας. Ο ιδιοκτήτης του hotspot μπορεί επίσης να είναι απατεώνας, που παρακολουθεί μυστικά από όλες τις συνδέσεις. Ένα VPN κρυπτογραφεί την κυκλοφορία σας στο Διαδίκτυο, δρομολογώντας τη μέσω ενός διακομιστή που ανήκει στην εταιρεία VPN. Αυτό σημαίνει ότι κανείς, ούτε καν ο κάτοχος του δωρεάν δικτύου Wi-Fi, δεν μπορεί να κατασκοπεύει τα δεδομένα σας.

Η χρήση ενός VPN αποκρύπτει επίσης τη διεύθυνση IP σας. Οι διαφημίσεις και οι trackers που θέλουν να σας αναγνωρίσουν ή να σας εντοπίσουν γεωγραφικά μέσω αυτής της διεύθυνσης IP, θα βλέπουν τη διεύθυνση της εταιρείας VPN. Η πλαστογράφηση της τοποθεσίας σας χρησιμοποιώντας έναν διακομιστή VPN σε άλλη χώρα μπορεί επίσης να χρησιμεύσει για το ξεκλείδωμα περιεχομένου που δεν είναι διαθέσιμο στην περιοχή σας. Σε μια πιο σοβαρή σημείωση, δημοσιογράφοι και ακτιβιστές σε καταπιεστικές χώρες χρησιμοποιούν εδώ και καιρό την τεχνολογία VPN για να επικοινωνούν με ασφάλεια.

Το αποτέλεσμα είναι ότι εάν συνδέεστε μέσω Wi-Fi (είτε είναι σε φορητό υπολογιστή, τηλέφωνο ή tablet) χρειάζεστε πραγματικά ένα VPN. Εάν δεν έχετε χρησιμοποιήσει ποτέ ξανά ή η τεχνολογία ακούγεται λίγο πιο πέρα από τις γνώσεις σας στο Διαδίκτυο, μην ανησυχείτε, έχουμε ετοιμάσει ένα κείμενο μας σχετικά με τον τρόπο ρύθμισης και χρήσης ενός VPN.

5. Χρησιμοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων μπορεί να χρειάζεται μια διαδικασία, αλλά κάνει τους λογαριασμούς σας πιο ασφαλείς. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων σημαίνει ότι πρέπει να περάσετε ένα άλλο επίπεδο ελέγχου ταυτότητας, όχι μόνο ένα όνομα χρήστη και έναν κωδικό πρόσβασης, για να εισέλθετε στους λογαριασμούς σας. Εάν τα δεδομένα σε έναν λογαριασμό είναι ευαίσθητα ή πολύτιμα και η πλατφόρμα σας προσφέρει έλεγχο ταυτότητας πολλαπλών παραγόντων, θα πρέπει να τον ενεργοποιήσετε. Το Gmail, το Evernote και το Dropbox είναι μερικά παραδείγματα διαδικτυακών υπηρεσιών που προσφέρουν έλεγχο ταυτότητας πολλαπλών παραγόντων.

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων επαληθεύει την ταυτότητά σας χρησιμοποιώντας τουλάχιστον δύο διαφορετικές μορφές ελέγχου ταυτότητας: κάτι που είστε, κάτι που έχετε ή κάτι που γνωρίζετε. Κάτι που γνωρίζετε είναι ο κωδικός πρόσβασης, φυσικά. Κάτι που είστε μπορεί να σημαίνει έλεγχο ταυτότητας με χρήση δακτυλικού αποτυπώματος ή αναγνώρισης προσώπου. Κάτι που έχετε θα μπορούσε να είναι το κινητό σας. Μπορεί να σας ζητηθεί να εισαγάγετε έναν κωδικό που αποστέλλεται μέσω κειμένου ή να πατήσετε ένα κουμπί επιβεβαίωσης σε μια εφαρμογή για κινητά. Κάτι που έχετε θα μπορούσε επίσης να είναι ένα φυσικό κλειδί ασφαλείας. Η Google και η Microsoft έχουν ανακοινώσει την στροφή τους προς αυτό το είδος ελέγχου ταυτότητας.

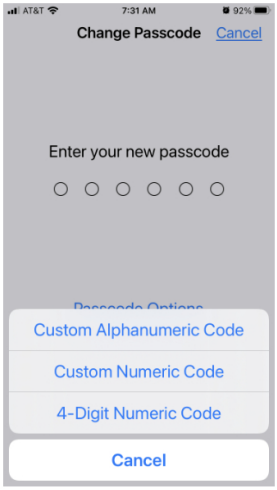
Εάν χρησιμοποιείτε απλώς έναν κωδικό πρόσβασης, οποιοσδήποτε μαθαίνει αυτόν τον κωδικό έχει πρόσβαση στον λογαριασμό σας. Με τον έλεγχο ταυτότητας πολλαπλών παραγόντων ενεργοποιημένο, ο κωδικός πρόσβασης από μόνος του είναι άχρηστος. Οι περισσότεροι password managers υποστηρίζουν πολλαπλούς παράγοντες, αν και ορισμένοι το απαιτούν μόνο όταν εντοπίζουν μια σύνδεση από μια νέα συσκευή. Η ενεργοποίηση του ελέγχου ταυτότητας πολλαπλών παραγόντων στον password manager είναι απαραίτητη.

Το άρθρο του PCMag σχετικά με το ποιος διαθέτει έλεγχο ταυτότητας πολλαπλών παραγόντων και πώς να τον ρυθμίσετε μπορεί να σας βοηθήσει να ξεκινήσετε.

6. Χρησιμοποιήστε κωδικούς πρόσβασης ακόμα και όταν είναι προαιρετικοί

Κλειδώστε με κωδικό πρόσβασης όπου μπορείτε, ακόμα κι αν είναι προαιρετικό. Σκεφτείτε όλα τα προσωπικά δεδομένα στο tablet ή το smartphone σας. Είναι σχεδιασμένα για να

προσωπικά δεδομένα και τις συνδέσεις στο smartphone σας. Είναι αδιανόητο να μην έχετε κλειδωμένες όλες αυτές τις πληροφορίες.



Πολλά smartphone προσφέρουν ένα τετραψήφιο PIN. Μην συμβιβάζεστε με αυτό. Χρησιμοποιήστε βιομετρικό έλεγχο ταυτότητας όπου είναι διαθέσιμος και ορίστε έναν ισχυρό κωδικό πρόσβασης, όχι ένα απλό τετραψήφιο PIN. Θυμηθείτε, ακόμη και όταν χρησιμοποιείτε το Touch ID ή κάτι αντίστοιχο, μπορείτε ακόμα να κάνετε έλεγχο ταυτότητας με τον κωδικό πρόσβασης, επομένως πρέπει να είναι ισχυρός.

Οι σύγχρονες συσκευές iOS προσφέρουν μια εξαψήφια επιλογή, αγνόηστή την. Μεταβείτε στις **Ρυθμίσεις > Face ID και κωδικός** και επιλέξτε **Αλλαγή κωδικού**. Εισαγάγετε τον παλιό σας κωδικό πρόσβασης, εάν χρειάζεται. Στην οθόνη για να εισαγάγετε τον νέο κωδικό, επιλέξτε **Προσαρμοσμένος αλφαριθμητικός κωδικός**. Εισαγάγετε έναν ισχυρό κωδικό πρόσβασης και, στη συνέχεια, καταγράψτε τον ως ασφαλή σημείωση στο password manager.

Οι συσκευές Android προσφέρουν διαφορετικές διαδρομές για τον ορισμό ενός ισχυρού κωδικού πρόσβασης. Βρείτε τις ρυθμίσεις, πηγαίνετέ στην επιλογή Κλείδωμα οθόνης (Screen Lock) στη συσκευή σας, πληκτρολογήστε το παλιό σας PIN και επιλέξτε Κωδικός πρόσβασης (Password) (εάν υπάρχει). Όπως και με τη συσκευή iOS, προσθέστε έναν ισχυρό κωδικό πρόσβασης και καταγράψτε τον ως ασφαλή σημείωση.

7. Πληρώστε με το Smartphone σας

Το σύστημα χρήσης πιστωτικών καρτών είναι ξεπερασμένο και καθόλου ασφαλές. Δεν φταίτε εσείς, αλλά υπάρχει κάτι που μπορείτε να κάνετε για αυτό. Αντί να χρησιμοποιήσετε την παλιά πιστωτική σας κάρτα, χρησιμοποιήστε το Apple Pay ή κάτι αντίστοιχο στο Android όπου μπορείτε. Υπάρχουν πολλές επιλογές όσον αφορά τις εφαρμογές. Στην πραγματικότητα, έχουμε μια ολόκληρη συλλογή εφαρμογών πληρωμής για κινητά.

Η ρύθμιση του smartphone σας ως συσκευής πληρωμής είναι συνήθως μια απλή διαδικασία. Συνήθως ξεκινά με τη λήψη μιας φωτογραφίας της πιστωτικής κάρτας που θα χρησιμοποιήσετε για να δημιουργήσετε αντίγραφα ασφαλείας των πληρωμών σας. Και η εγκατάσταση σχεδόν τελειώνει εκεί.

Τα POS που υποστηρίζουν πληρωμή μέσω smartphone συνήθως υποδεικνύουν το γεγονός με ένα εικονίδιο, από μια εικόνα ενός χεριού που κρατά ένα smartphone. Αν και τα περισσότερα υποστηρίζουν ανέπαφες πληρωμές, το κινητό σας πρέπει να διαθέτει NFC (υπάρχον και άλλοι τρόποι σύνδεσης και πληρωμής σε ένα POS, όπως μέσω Bluetooth ή barcode, αλλά αυτό εξαρτάται από την τράπεζα σας). Απλώς τοποθετήστε τη συσκευή σας στο τερματικό, επιβεβαιώστε με το δακτυλικό αποτύπωμα και πληρώστε.

σαχτολικό αποτύπωμα και πληρώστε.

Πώς είναι καλύτερο από τη χρήση της ίδιας της πιστωτικής κάρτας; Η εφαρμογή δημιουργεί έναν κωδικό ελέγχου ταυτότητας μίας χρήσης, κατάλληλος μόνο για την τρέχουσα συναλλαγή. Ακόμα κι αν κάποιος έβρισκε ή έσπαγε αυτόν τον κώδικο, δεν θα του χρησίμευε κάπου. Η πληρωμή με μια εφαρμογή smartphone εξαλείφει την πιθανότητα κλοπής δεδομένων.

Ορισμένες εφαρμογές πληρωμής smartphone σάς επιτρέπουν να πληρώνετε ηλεκτρονικά με έναν παρόμοιο κωδικό μιας χρήσης. Εάν το δικό σας δεν το κάνει, επικοινωνήστε με τον πάροχο της πιστωτικής σας κάρτας. Συνήθως, λαμβάνετε έναν προσωρινό αριθμό για χρήση στη θέση της πραγματικής πιστωτικής σας κάρτας και οι χρεώσεις πηγαίνουν στον κανονικό λογαριασμό σας. Ο προσωρινός αριθμός κάρτας δεν θα λειτουργήσει ξανά μετά τη λήξη του. Για κάτι τέτοιο απευθυνθείτε στην τράπεζα σας. Είναι αυτό που λέμε “κάρτες μιας χρήσης”.

Μπορείτε επίσης να λάβετε την προστασία αριθμών πιστωτικών καρτών μίας χρήσης χρησιμοποιώντας εφαρμογές τρίτων. Το Abine Blur Premium, για παράδειγμα, μπορεί να κρύψει αριθμούς πιστωτικών καρτών, διευθύνσεις email και αριθμούς τηλεφώνου. Ψωνίζετε και επικοινωνείτε όπως πάντα, αλλά ο έμπορος δεν λαμβάνει τις πραγματικές σας πληροφορίες.

8. Χρησιμοποιήστε διαφορετικές διευθύνσεις email για διαφορετικούς τύπους λογαριασμών

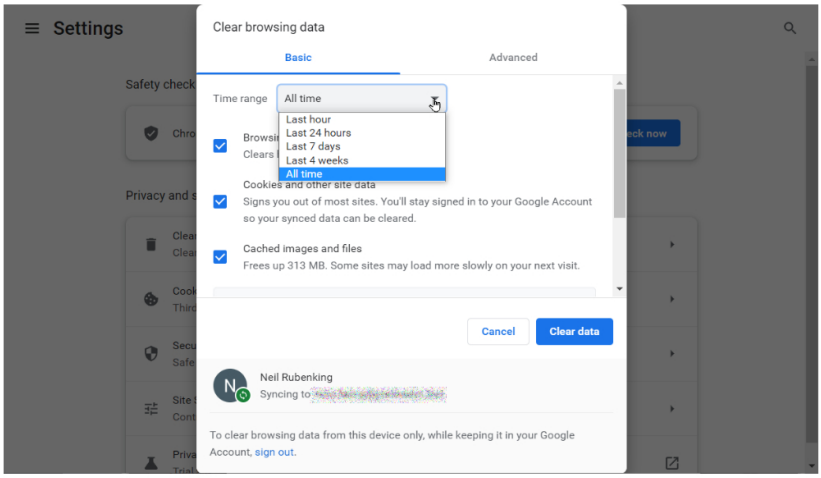
Τα άτομα που είναι τόσο οργανωμένα όσο και μεθοδικά σχετικά με την ασφάλειά τους χρησιμοποιούν συχνά διαφορετικές διευθύνσεις email για διαφορετικούς σκοπούς, για να διατηρούν ξεχωριστές τις διαδικτυακές ταυτότητες που σχετίζονται με αυτά. Εάν ένα phishing email που ισχυρίζεται ότι είναι από την τράπεζά σας έρθει στον λογαριασμό που χρησιμοποιείτε μόνο για τα μέσα κοινωνικής δικτύωσης, ξέρετε ότι είναι σίγουρα είναι απάτη.

Σκεφτείτε το ενδεχόμενο να διατηρήσετε μία διεύθυνση email αφιερωμένη στην εγγραφή σε εφαρμογές που θέλετε να δοκιμάσετε, αλλά που μπορεί να έχουν αμφισβητούμενη ασφάλεια ή που ενδέχεται να σας στέλνουν ανεπιθύμητα μηνύματα. Αφού ελέγξετε μια υπηρεσία ή μια εφαρμογή, εγγραφείτε χρησιμοποιώντας έναν από τους μόνιμους λογαριασμούς email σας. Εάν ο αποκλειστικός λογαριασμός αρχίσει να λαμβάνει ανεπιθύμητο περιεχόμενο, κλείστε τον και δημιουργήστε έναν νέο. Για να το κάνετε αυτό πιο εύκολα μπορείτε να δημιουργείτε email μιας χρήσης από το Abine Blur και άλλες τέτοιες υπηρεσίες.

Πολλοί ιστότοποι εξισώνουν τη διεύθυνση email σας με το όνομα χρήστη σας, αλλά ορισμένοι σας επιτρέπουν να επιλέξετε το δικό σας όνομα χρήστη. Εξετάστε το ενδεχόμενο να χρησιμοποιείτε διαφορετικό όνομα χρήστη κάθε φορά. Τώρα όποιος προσπαθεί να εισέλθει στον λογαριασμό σας πρέπει να μαντέψει τόσο το όνομα χρήστη όσο και τον κωδικό πρόσβασης.

9. Εκκαθαρίστε την προσωρινή μνήμη

Μην υποτιμάτε ποτέ πόσα γνωρίζει η κρυφή μνήμη του προγράμματος περιήγησής σας για εσάς. Τα αποθηκευμένα cookies, οι αποθηκευμένες αναζητήσεις και το ιστορικό θα μπορούσαν να παραπέμπουν σε διεύθυνση κατοικίας, οικογενειακές πληροφορίες και άλλα προσωπικά δεδομένα.



Για να προστατεύσετε καλύτερα αυτές τις πληροφορίες που ενδέχεται να κρύβονται στο ιστορικό

Για να προστατεύσετε καλύτερα αυτές τις πληροφορίες που ενδέχεται να κρύβονται στο ιστορικό σας, φροντίστε να διαγράφετε τα cookies και να διαγράφετε το ιστορικό του προγράμματος περιήγησής σας σε τακτική βάση. Είναι εύκολο. Σε Chrome, Edge, Firefox, Internet Explorer ή Opera, απλώς πατήστε Ctrl+Shift+Del για να εμφανιστεί ένα παράθυρο που σας επιτρέπει να επιλέξετε ποια στοιχεία των δεδομένων του προγράμματος περιήγησης θέλετε να διαγράψετε. Εάν χρησιμοποιείτε διαφορετικό πρόγραμμα περιήγησης, δοκιμάστε αυτόν τον συνδυασμό πλήκτρων, μπορεί να λειτουργήσει. Διαφορετικά, ψάξτε για την αντίστοιχη ρύθμιση στο μενού.

Η διαγραφή των cookies μπορεί να προκαλέσει προβλήματα σε ορισμένους ιστότοπους, μπορεί να χάσετε οποιαδήποτε ρύθμιση έχετε εφαρμόσει. Τα περισσότερα προγράμματα περιήγησης σάς επιτρέπουν να αναφέρετε τους αγαπημένους ιστότοπους των οποίων τα cookie δεν πρέπει να διαγράφονται.

Μπορείτε να διαβάσετε το άρθρο του PCMag σχετικά με τον τρόπο εκκαθάρισης της προσωρινής μνήμης σε οποιοδήποτε πρόγραμμα περιήγησης.

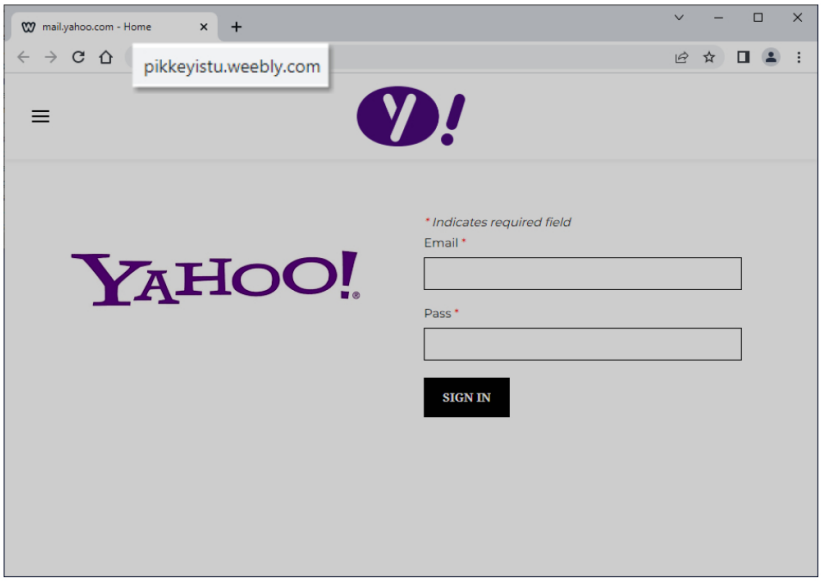
10. Απενεργοποιήστε τη λειτουργία “Αποθήκευση κωδικού πρόσβασης” στους browsers

Μιλώντας για το τι μπορεί να γνωρίζει το πρόγραμμα περιήγησής σας για εσάς, τα περισσότερα προγράμματα περιήγησης περιλαμβάνουν μια ενσωματωμένη λύση διαχείρισης κωδικών πρόσβασης. Εμείς στο PCMag δεν τα προτείνουμε, ωστόσο. Πιστεύουμε ότι είναι καλύτερο να αφήσουμε την προστασία με κωδικό πρόσβασης στους ειδικούς που δημιουργούν password managers.

Όταν εγκαθιστάτε έναν password manager τρίτου κατασκευαστή, συνήθως προσφέρει την εισαγωγή του κωδικού πρόσβασής σας από τον χώρο αποθήκευσης του προγράμματος περιήγησης. Εάν το password manager μπορεί να το κάνει αυτό, μπορείτε να είστε σίγουροι ότι κάποιο κακόβουλο λογισμικό μπορεί να κάνει το ίδιο. Επιπλέον, η διατήρηση των κωδικών πρόσβασής σας σε μια ενιαία, κεντρική διαχείριση κωδικών πρόσβασης σάς επιτρέπει να τους χρησιμοποιείτε σε όλα τα προγράμματα περιήγησης και τις συσκευές.

11. Μην πέφτετε θύματα για να κάνετε κλικ σε απάτες

Μέρος της διασφάλισης της διαδικτυακής σας ζωής είναι και το να σκέφτεστε πριν κάνετε κλικ. Το Clickbait δεν αναφέρεται μόνο σε βίντεο και σε πιασάρικους τίτλους. Μπορεί επίσης να περιλαμβάνει συνδέσμους σε email και εφαρμογές ανταλλαγής μηνυμάτων όπως το Facebook. Οι σύνδεσμοι phishing μεταμφιέζονται ως ασφαλείς ιστότοποι, ελπίζοντας να σας ξεγελάσουν για να τους δώσετε τα διαπιστευτήριά σας. Οι σελίδες Drive-by λήψεων μπορεί να προκαλέσουν αυτόματη λήψη κακόβουλου λογισμικού και να μολύνει τη συσκευή σας.



Μην κάνετε κλικ σε συνδέσμους σε email ή μηνύματα, εκτός εάν προέρχονται από πηγή που εμπιστεύεστε. Ακόμα και τότε, να είστε προσεκτικοί. Η αξιόπιστη πηγή σας μπορεί να έχει παραβιαστεί ή το μήνυμα μπορεί να είναι ψεύτικο. Το ίδιο ισχύει και για τους συνδέσμους σε

παραβιαστεί το μήνυμα μπορεί να είναι φευτικό. Το ίδιο ισχύει και για τους συνδέσμους σε ιστότοπους κοινωνικής δικτύωσης, ακόμη και σε αναρτήσεις που φαίνεται να προέρχονται από φίλους σας. Εάν μια ανάρτηση δεν μοιάζει σαν κάτι που θα ανέβαζε ένας φίλος σας στα μέσα κοινωνικής δικτύωσης, θα μπορούσε να σημαίνει ότι ο λογαριασμός του έχει παραβιαστεί.

Για περισσότερα, διαβάστε το άρθρο μας σχετικά με το πώς να αποφύγετε το phishing.

12. Προστατέψτε το απόρρητο των μέσων κοινωνικής δικτύωσης

Υπάρχει ένα κοινό ρητό: αν δεν πληρώνεις για μια υπηρεσία, δεν είσαι πελάτης, είσαι το προϊόν. Οι ιστότοποι μέσων κοινωνικής δικτύωσης σάς διευκολύνουν να μοιράζεστε τις σκέψεις και τις φωτογραφίες σας με φίλους, αλλά είναι εύκολο να καταλήξετε να μοιράζεστε πολύ περισσότερες πληροφορίες.

Μπορείτε να κάνετε λήψη των δεδομένων σας στο Facebook για να δείτε ακριβώς τι γνωρίζει ο γίγαντας των κοινωνικών μέσων για εσάς. Μπορεί να είναι αρκετά εντυπωσιακό, ειδικά αν είστε το είδος του ατόμου που κάνει συχνά κλικ σε κουίζ που απαιτούν πρόσβαση στον λογαριασμό σας στα μέσα κοινωνικής δικτύωσης. Πραγματικά, δεν χρειάζεται να ξέρετε ποια πριγκίπισσα της Disney ή ποια ράτσα σκύλου είστε.

Μπορείτε να μειώσετε δραστικά τον όγκο των δεδομένων που πηγαίνουν στο Facebook απενεργοποιώντας εντελώς την πλατφόρμα κοινής χρήσης. Μόλις το κάνετε, οι φίλοι σας δεν μπορούν πλέον να διαρρεύσουν τα προσωπικά σας δεδομένα. Δεν μπορείτε να χάσετε δεδομένα σε εφαρμογές, επειδή δεν μπορείτε να χρησιμοποιήσετε εφαρμογές. Και δεν μπορείτε να χρησιμοποιήσετε τα διαπιστευτήριά σας στο Facebook για να συνδεθείτε σε άλλους ιστότοπους (κάτι που ήταν πάντα κακή ιδέα).

Φυσικά, και άλλοι ιστότοποι κοινωνικής δικτύωσης χρειάζονται επίσης προσοχή. Η Google πιθανότατα γνωρίζει περισσότερα για εσάς από το Facebook, οπότε λάβετε μέτρα για να διαχειριστείτε και το απόρρητό σας στη Google. Βεβαιωθείτε ότι έχετε διαμορφώσει κάθε ιστότοπο μέσων κοινωνικής δικτύωσης έτσι ώστε οι αναρτήσεις σας να μην είναι δημόσιες. Σκεφτείτε δύο φορές πριν αποκαλύψετε πάρα πολλά σε μια ανάρτηση, καθώς οι φίλοι σας μπορεί να το μοιραστούν με άλλους. Με προσοχή, μπορείτε να διατηρήσετε το απόρρητό σας χωρίς να χάσετε την ψυχαγωγία και τις συνδέσεις των μέσων κοινωνικής δικτύωσης.

ΣΧΕΤΙΚΑ ΘΕΜΑΤΑ

- Ζούμε στην Εποχή της Κυβερνοευπάθειας, εκεί όπου η εορταστική περίοδος γίνεται παιδική χαρά για τους χάκερ
- Ψεύτικα λογισμικά antivirus αποσπούν εκατομμύρια από τους χρήστες τους
- Η FTC απαγορεύει στον πάροχο antivirus Avast να πωλεί δεδομένα περιήγησης χρηστών
- Ποιο λειτουργικό σύστημα είναι ασφαλέστερο, το MacOS ή τα Windows;
- Πώς να αποφύγετε τις απάτες phishing

About Βαγγέλης Κομνής

Φοιτητής του τμήματος Μηχανικών Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών και συντάκτης της ελληνικής έκδοσης του PCMag. Όταν δεν γράφω νέα και κριτικές, παρακολουθώ σεμινάρια σε διάφορους τομείς της πληροφορικής, και όχι μόνο, σε μια προσπάθεια να γεμίσω τους τοίχους μου με χαρτιά.

More From Βαγγέλης Κομνής

- The Outlast Trials Review
- Trepang2 Review
- The Lord Of The Rings: Return To Moria Review
- SteamWorld Build Review
- Abtos Covert Review

ΣΧΟΛΙΑ