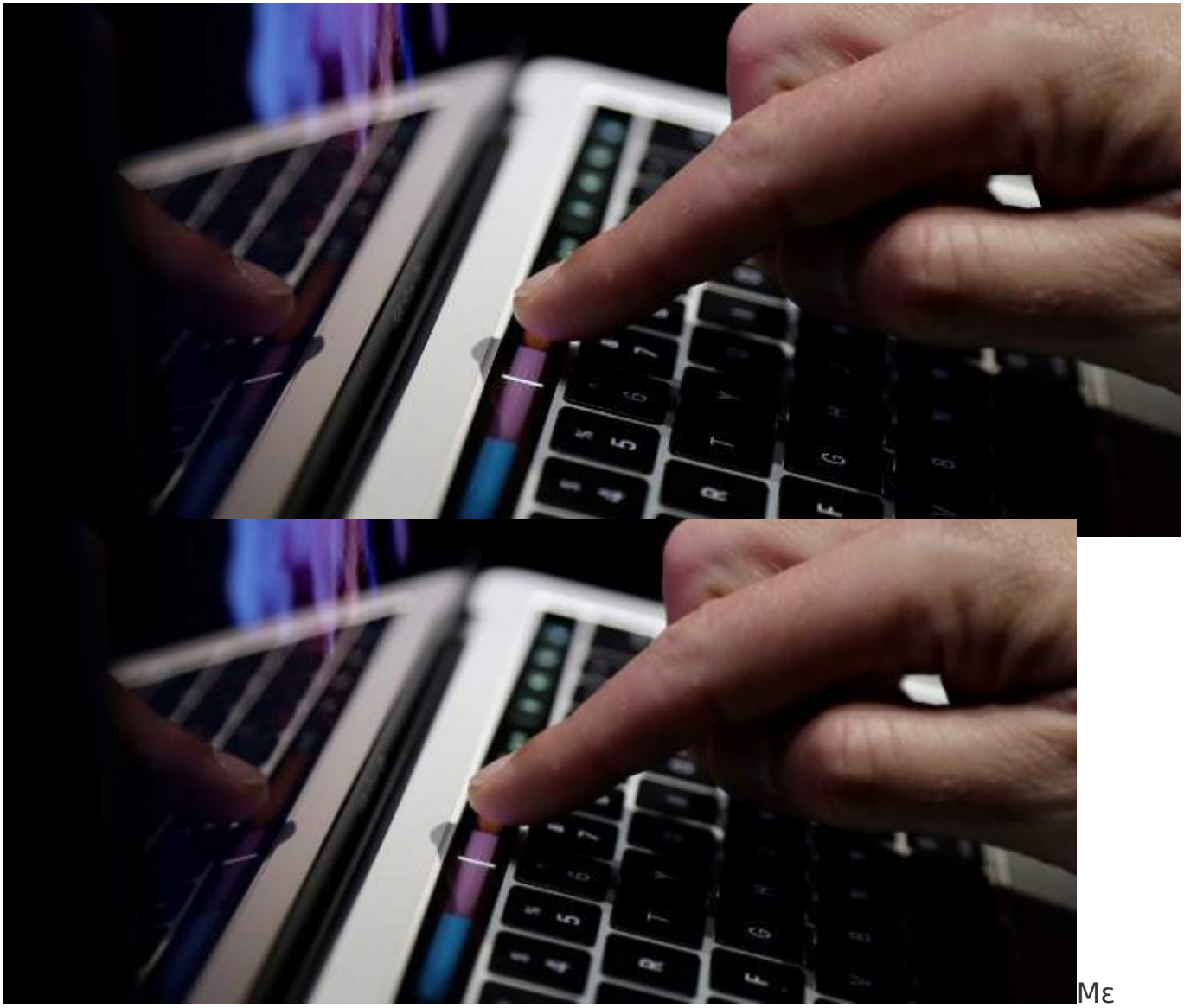
10 Φεβρουαρίου 2017

Οι συμβουλές των ειδικών ασφαλείας της Google για να προστατεύσεις τον υπολογιστή σου

/ Επιστήμες, Τέχνες & Πολιτισμός



Με αφορμή την ημέρα ασφαλούς διαδικτύου, οι ειδικοί ασφάλειας της Google δίνουν συμβουλές για να κρατήσετε τα δεδομένα σας ασφαλή στο διαδίκτυο.

Μέχρι πρόσφατα, ζητήματα όπως «κωδικός πρόσβασης», «ηλεκτρονικό ψάρεμα», «κρυπτογράφηση» και «εισβολή στο λογαριασμό» δεν αποτελούσαν ενδιαφέρον θέμα συζήτησης. Όμως σήμερα, περισσότερο από ποτέ, είναι σημαντικό για τον καθένα να καταλάβει τα βασικά της διαδικτυακής ασφάλειας.

Έρευνα που διεξήγαγε η YouGov για λογαριασμό της Google καταδεικνύει ότι

περισσότεροι από τους μισούς (54%) Έλληνες millennials (θεωρούνται όσοι γεννήθηκαν μετά το ’80) που ερωτήθηκαν χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για κάποιους ή για τους περισσότερους από τους λογαριασμούς τους, κυρίως (72%) επειδή είναι δύσκολο να θυμούνται τόσους κωδικούς πρόσβασης.

Σχετικά με τους ίδιους τους κωδικούς πρόσβασης, το 12% των ερωτηθέντων έχουν χρησιμοποιήσει στο παρελθόν την λέξη ‘password’, το 14% έναν συνδυασμό από συνεχόμενα νούμερα στο πληκτρολόγιο (για παράδειγμα 1, 2, 3, 4, 5), ενώ 20% χρησιμοποιούσαν τη στιγμή της έρευνας έναν κωδικό πρόσβασης που περιλάμβανε το όνομά τους ή τα αρχικά τους. Συνολικά, το 52% δήλωσαν ότι οι γονείς τους δεν τούς έχουν μιλήσει ποτέ για την διαδικτυακή ασφάλεια και την σημασία της χρήσης ισχυρών κωδικών πρόσβασης.
Από την άλλη πλευρά, το 76% των ερωτηθέντων δήλωσαν ότι χρησιμοποιούν την υπηρεσία προστασίας της Google, “Επαλήθευση σε 2 βήματα”.
Κρατώντας τα αυτά υπόψη, παρακάτω θα βρείτε νέα στοιχεία για το πώς η Google προάγει την ασφάλεια με έξυπνο τρόπο.
Στην φετινή Ημέρα Ασφαλούς Διαδικτύου, θέλουμε να αποκαλύψουμε μερικές πληροφορίες για τα συστήματα Google που σας κρατούν ασφαλείς, αυτόματα – χωρίς διακόπτες ή κουμπιά– στο Google και πέρα από αυτό.

Ας ξεκινήσουμε με τα βασικά
Οι κωδικοί πρόσβασης είναι η πρώτη γραμμή άμυνας απέναντι στους εγκληματίες του διαδικτύου. Να χρησιμοποιείτε έναν ξεχωριστό κωδικό πρόσβασης για καθέναν από τους σημαντικούς λογαριασμούς σας, όπως το e-mail και το e-banking. Όσο μεγαλύτερος είναι ο κωδικός, τόσο πιο δύσκολο είναι να τον μαντέψει κάποιος. Μια καλή ιδέα είναι να σκεφτείτε μια φράση που μονάχα εσείς γνωρίζετε και να την συσχετίσετε με μια συγκεκριμένη ιστοσελίδα ώστε να σας βοηθήσει να την θυμόσαστε. Ή αφήστε τον Chrome να διαχειρίζεται τους κωδικούς σας. Τέλος, προσθέστε ένα επιπλέον επίπεδο ασφάλειας με την Επιβεβαίωση 2-Βημάτων.

Ξεγελώντας το «ηλεκτρονικό ψάρεμα» (phishing) για να προστατεύσετε τον λογαριασμό Google σας
Μπορεί να είναι ένα e-mail που μοιάζει σαν να προήλθε από ένα άτομο που εμπιστεύεστε, αλλά είναι ουσιαστικά η κορυφή του παγόβουνου μιας επίθεσης «ηλεκτρονικού ψαρέματος» (phishing). Ο στόχος ενός απατεώνα «ηλεκτρονικού ψαρέματος» (phisher) είναι απλός: να σας εξαπατήσει, να κλέψει προσωπικές πληροφορίες και τελικά να εισβάλει στον λογαριασμό σας.
Έχουμε θωρακίσει το Gmail έτσι ώστε να καταστρέφονται αυτόματα τα επικίνδυνα μηνύματα, πριν ακόμα τα δείτε στα εισερχόμενά σας. Εξετάζουμε ανώνυμα χιλιάδες σήματα σε όλο το Gmail -από πού προήλθε το μήνυμα, σε ποιόν

απευθύνεται, τι περιέχει και πόσο συχνά ο αποστολέας έχει επικοινωνήσει μαζί σας στο παρελθόν- για να καθορίσουμε ποια μηνύματα είναι ασφαλή και ποια δεν είναι. Στην συνέχεια, φιλτράρουμε την πλειοψηφία αυτού του κακόβουλου περιεχομένου. Ο μέσος φάκελος εισερχόμενων στο Gmail περιέχει λιγότερο από 0,1% spam.
Όμως, υποθέστε ότι ένας απατεώνας κάπως καταφέρνει να βρει τα στοιχεία του λογαριασμού σας. Ίσως μία από τις επαφές σας ήταν ο φορέας μίας εκλεπτυσμένης επίθεσης, ή μπορεί να δώσατε εσείς τα στοιχεία σας κατά λάθος.
Μην ανησυχείτε, ο λογαριασμός σας είναι ακόμα προστατευμένος. Όταν συνδέεστε στον λογαριασμό σας Google, δεν σιγουρευόμαστε μόνο ότι έχετε πληκτρολογήσει τον σωστό κωδικό πρόσβασης. Ψάχνουμε επίσης για πιο διακριτικά σημάδια για να σιγουρευτούμε ότι η σύνδεση δεν είναι ύποπτη: Χρησιμοποιείτε το ίδιο τηλέφωνο που χρησιμοποιείτε συνήθως; Βρίσκεστε σε μια συνηθισμένη γνώριμη τοποθεσία ή κάπου μακριά όπου δεν έχετε ξαναβρεθεί; Έχει αυτή η απόπειρα σύνδεσης τα χαρακτηριστικά επικίνδυνων επιθέσεων που παρακολουθούμε ανά τον κόσμο;
Το μυστικό μας: η ικανότητα να αναγνωρίσουμε πιο διακριτικά σήματα-ενδείξεις δισεκατομμύρια φορές καθημερινά. Οι ενδείξεις αποκαλύπτουν πρότυπα επικίνδυνων συμπεριφορών που μας επιτρέπουν να κατανοήσουμε ακριβώς τους κινδύνους που μπορεί να απειλούν τον λογαριασμό σας. Αυτά τα συστήματα ανίχνευσης είναι κάπως σαν τον φακό του Sherlock Holmes... με την υποστήριξη μερικών data centers. Ενώνοντας αυτές τις ενδείξεις, μπορούμε να αναπτύξουμε ένα συνεχώς βελτιούμενο μοντέλο μιας ασφαλούς και υγειούς σύνδεσης. Θα συγκρίνουμε κάθε προσπάθεια σύνδεσης με αυτό το μοντέλο και σε περίπτωση που κάτι μοιάζει ύποπτο, θα ζητάμε περισσότερες ερωτήσεις σχεδιασμένες για να αποτρέπουν «διαρρήξεις», θα στέλνουμε ειδοποιήσεις στο κινητό σας, και θα σας στέλνουμε e-mail ώστε να μπορέσετε να αντιδράσετε σύντομα σε οτιδήποτε σας φαίνεται ασυνήθιστο.

Ασφάλεια στην Google… και ακόμα παραπέρα!
Χρησιμοποιούμε αυτά τα εργαλεία ασφάλειας για να διατηρήσουμε το Διαδίκτυο και τις εφαρμογές και συσκευές Android ασφαλέστερα. Παραδείγματος χάρη, έχετε ποτέ πατήσει έναν σύνδεσμο και σας έχει εμφανιστεί μια κόκκινη προειδοποίηση, σαν αυτή; Αυτή είναι η Ασφαλής Πλοήγηση (Safe Browsing) σε δράση, που σας υπενθυμίζει να μην επισκέπτεστε μια ιστοσελίδα επειδή κρύβει πιθανούς κινδύνους, όπως κακόβουλο λογισμικό ή απάτες «ηλεκτρονικού ψαρέματος» (phishing). Κάπως, σαν τον τρόπο που σαρώνουμε το διαδίκτυο για να εμφανίσουμε αποτελέσματα αναζητήσεων, το Safe Browsing σαρώνει για κακόβουλο περιεχόμενο, το οποίο αποτελεί απειλή για εσάς ή στην συσκευή σας. Είναι πάντοτε σκληρή δουλειά: δείχνουμε δεκάδες εκατομμύρια προειδοποιήσεις Ασφαλούς Πλοήγησης κάθε εβδομάδα σε πάνω από 2 δισεκατομμύρια συσκευές, σε μια ποικιλία προγραμμάτων πλοήγησης.

Οι συσκευές και οι εφαρμογές Android είναι ουσιαστικά ένα δίκτυο από μόνες τους, και για αυτό το λόγο έχουμε αναπτύξει το “app analyzer”, μια τροποποιημένη έκδοση του Safe Browsing που αναζητά ειδικά επικίνδυνες εφαρμογές στο Google Play, σε άλλα app stores, και στο Διαδίκτυο, και προειδοποιεί χρήστες πριν τις εγκαταστήσουν. Σε περίπτωση που κάποιες εφαρμογές αποτύχουν σε αυτό το τεστ, δεν γίνονται επιτρεπτές στο Google Play. Μια ξεχωριστή προστασία, το Verify Apps, λειτουργεί άμεσα στις συσκευές Android, ελέγχοντας προληπτικά πάνω από 6 δισεκατομμύρια εφαρμογές και 400 εκατομμύρια συσκευές, κάθε μέρα. Ελέγχει κάθε φορά που εγκαθιστάτε μια εφαρμογή, επιστρέφει τακτικά για να σιγουρευτεί ότι όλα δείχνουν ασφαλή, και αν βρεθεί κάτι ασυνήθιστο, διαγράφει την εφαρμογή.
Ανιχνεύοντας με αυτά τα εργαλεία τους προφανείς κινδύνους – γνωστές ιστοσελίδες για απάτες «ηλεκτρονικού ψαρέματος» (phishing), εφαρμογές διεφθαρμένες με ransomware που προσπαθούν να κλειδώσουν το κινητό σας μέχρι να αναγκαστείτε να πληρώσετε – μοιάζει να είναι εύκολο. Αλλά όμως, πολλοί από αυτούς τους κινδύνους μπορούν να είναι μη ανιχνεύσιμοι αν δεν ελέγχουμε καθημερινά τα δισεκατομμύρια σήματα ανά τις ιστοσελίδες και τις εφαρμογές. Όλα αυτά φαίνονται και είναι παρόμοια με τον τρόπο που αντιμετωπίζουμε την ηλεκτρονική αλληλογραφία spam στην Google! Η ικανότητα να ανιχνεύουμε τον κίνδυνο σε πολύ μεγάλη κλίμακα μας επιτρέπει να βρούμε ίχνη που οι απατεώνες ούτε καν γνώριζαν ότι άφηναν.
Έχουμε ευθύνη να σας κρατήσουμε ασφαλείς στο Google, και να κάνουμε το δίκτυο των ιστοσελίδων και των εφαρμογών πιο ασφαλή. Βελτιώνουμε διαρκώς την αυτόματη προστασία, αλλά επιθυμούμε να ενθαρρύνουμε τους χρήστες με τον έλεγχο να προσαρμόσουν τις ρυθμίσεις ασφάλειάς τους. Έχοντας αυτό υπόψιν, γιορτάστε την Ημέρα Ασφαλέστερου Διαδικτύου φέτος με ένα Security Checkup στο SecurityCheckup. Η αυτόματη προστασία, οι εύκολες ρυθμίσεις που προσαρμόζονται στις ανάγκες σας και η αφοσίωση στην καταπολέμηση των διαδικτυακών κινδύνων, είναι οι μέθοδοι που χρησιμοποιούμε για να καλύπτουμε τα νώτα σας, όταν πρόκειται για την ασφάλειά σας.
Θα κάνουμε ό,τι χρειαστεί για να παραμείνετε εσείς και ο λογαριασμός σας ασφαλείς στο διαδίκτυο. Και ναι! Συζητήστε τώρα αυτά τα θέματα με τους ανθρώπους που είναι δίπλα σας!

Ψηφιακή ασφάλεια και millenials

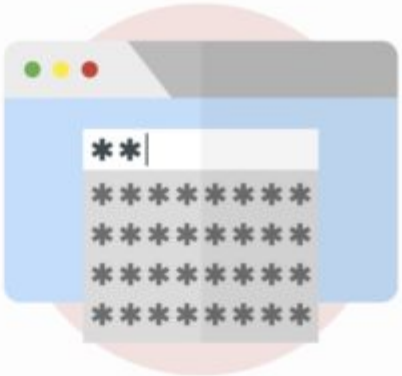
Χρησιμοποιείτε μοναδικούς κωδικούς πρόσβασης για τους λογαριασμούς σας, όπως αυτούς του ηλεκτρονικού ταχυδρομείου και των τραπεζικών συναλλαγών

54%

των millenials χρησιμοποιούν τον ίδιο κωδικό για μερικούς ή για τους περισσότερους λογαριασμούς

72%

αυτών που χρησιμοποιούν τον ίδιο κωδικό σε μερικούς ή περισσότερους λογαριασμούς είπαν ότι δεν μπορούν να θυμηθούν πολλούς κωδικούς



Αφήστε τον Chrome να σας προστατεύσει: χρησιμοποιήστε τη λειτουργία διαχείρισης κωδικών που βρίσκεται στις ρυθμίσεις του Chrome

Πηγή: iefimerida.gr