

Κωδικοί πρόσβασης: Ο λάθος τρόπος να τους χρησιμοποιείτε!

/ [Πεμπτούσία](#)



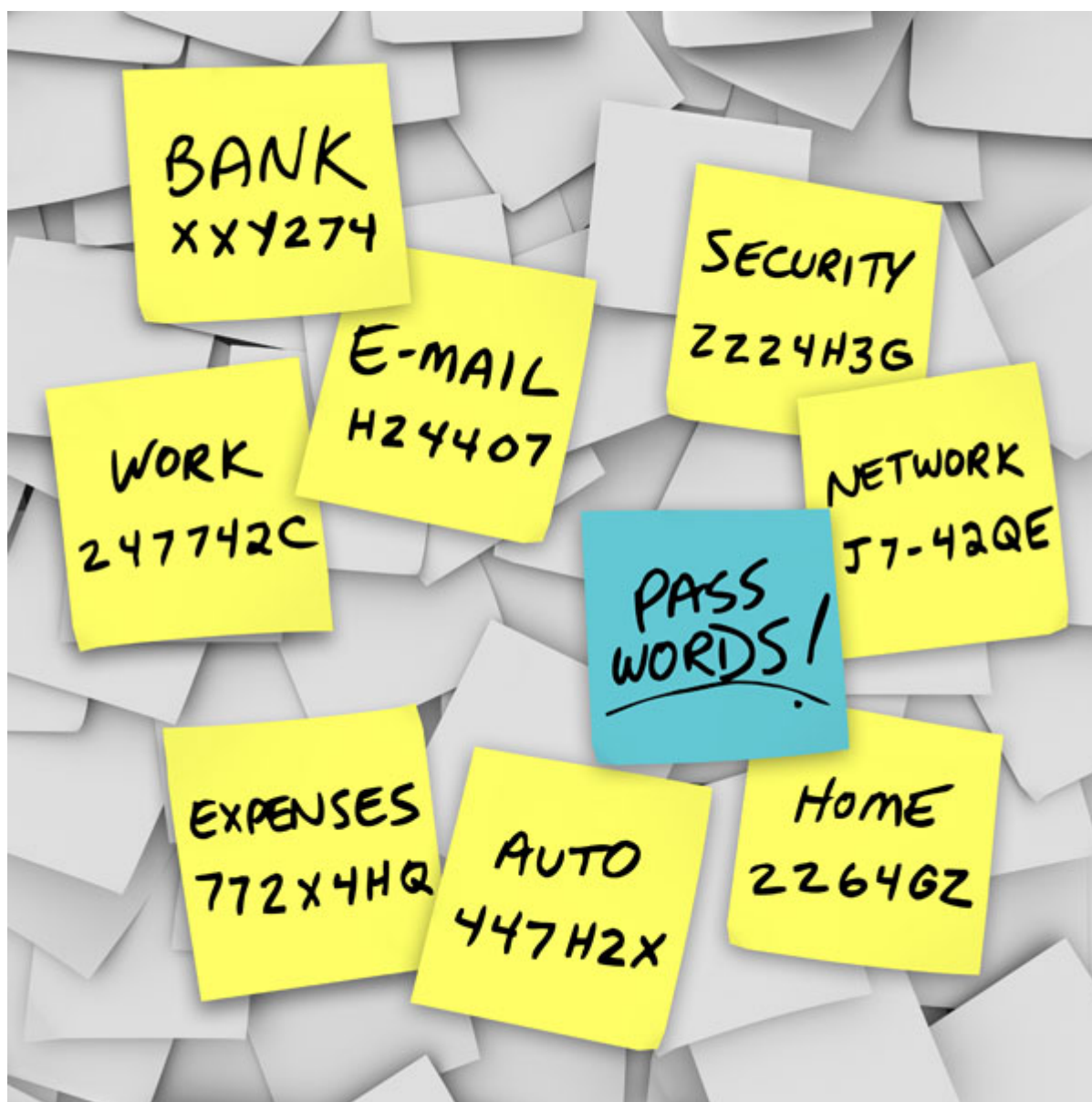
Οι κωδικοί πρόσβασης υπάρχουν από το 200 π.Χ. και με την εξέλιξη στην ψηφιακή εποχή, ο καθένας έχει έναν ή δύο κωδικούς για να προστατεύσει προσωπικά του στοιχεία. Παρόλα αυτά, αυτό το μέτρο προστασίας γίνεται πολύ αναξιόπιστο και ανασφαλές όταν οι άνθρωποι χρησιμοποιούν καταχρηστικά τους κωδικούς τους.

Η Kaspersky Lab ανέλυσε το πώς οι χρήστες προστατεύουν τους online λογαριασμούς τους σε μια πρόσφατη μελέτη. Όπως αποδείχθηκε, σχεδόν το ένα τρίτο των ερωτηθέντων έχουν δύο ή τρεις παρόμοιους [κωδικούς πρόσβασης](#) για όλους τους λογαριασμούς τους. Επιπλέον, ένας στους επτά ερωτηθέντες χρησιμοποιεί έναν κωδικό πρόσβασης για όλους τους λογαριασμούς τους.

Εκτός από το θέμα της ποσότητας, υπάρχει και ένα πρόβλημα με την ποιότητα των συνδυασμών που χρησιμοποιούνται στους κωδικούς πρόσβασης. Ένας στους

10 ερωτηθέντες έχουν κωδικούς πρόσβασης που είναι μικρότεροι από οκτώ χαρακτήρες σε μήκος. Συν τοις άλλοις, πολλοί άνθρωποι (το 12%, για να είμαστε πιο ακριβείς) δεν χρησιμοποιούν κεφαλαία γράμματα, αριθμούς και / ή ειδικούς χαρακτήρες για να βελτιώσουν τους κωδικούς πρόσβασης τους. Τέτοιοι συνδυασμοί, όμως, δεν είναι καθόλου ασφαλείς.

Ωστόσο, το χειρότερο μέρος δεν είναι αυτό! Μόνο λίγοι από αυτούς απομνημονεύουν τους κωδικούς τους. Περισσότεροι από τους μισούς των ερωτηθέντων αποθηκεύουν τον κωδικό σε ένα κομμάτι χαρτί, στο τηλέφωνό τους ή σε αρχεία κειμένου στους υπολογιστές τους. Περίπου το ένα τρίτο των χρηστών που ερωτήθηκαν αποθηκεύει τους κωδικούς πρόσβασης στο πρόγραμμα περιήγησης για να επωφεληθούν από τη δυνατότητα γρήγορη σύνδεσης.



Παρακαλούμε, να θυμάστε: Εάν χρησιμοποιείτε έναν κωδικό πρόσβασης για όλους τους λογαριασμούς σας, ένας χάκερ πρέπει να παραβιάσει μόνο ΕΝΑΝ από αυτούς

για να θέσει όλους τους άλλους λογαριασμούς σας σε κίνδυνο.

Ίσως το πιο τρομακτικό κομμάτι που αποκαλύφθηκε από την έρευνα είναι η έλλειψη ευαισθητοποίησης σε ό,τι αφορά την ασφάλεια. Το ένα τέταρτο των ερωτηθέντων πιστεύουν ότι είναι ασφαλείς, καθώς δεν αποθηκεύουν τίποτα σημαντικό στις συσκευές τους. Δυστυχώς, οι δράστες δεν κυνηγούν μόνο εταιρικά δεδομένα ή κυβερνητικά μυστικά: οι [κωδικοί πρόσβασης](#) και τα logins του κάθε χρήστη είναι από μόνα τους ένας αγαπημένος στόχος των εγκληματιών του κυβερνοχώρου. Ανάλογα με τις ικανότητές τους, οι δράστες θα βρουν έναν τρόπο να χρησιμοποιήσουν τα κλεμμένα credentials σύνδεσης: για παράδειγμα, μπορούν να παραβιάσουν τον online λογαριασμό σας στην τράπεζα ή απλά να χρησιμοποιήσουν το λογαριασμό σας στο Facebook για διαδώσουν spam και ιούς.

Ακόμα κι αν εξακολουθείτε να μην ανησυχείτε, ήρθε η ώρα να καταλάβετε ότι οι αδύναμοι κωδικοί σας μπορεί να θέσουν σε κίνδυνο τους φίλους, τους συγγενείς, τους συναδέλφους, τους συνεργάτες σας και ούτω καθεξής. Άρα, σας παραθέτουμε τρεις απλούς κανόνες, που θα πρέπει να ληφθούν υπόψη.

- Ο μύθος, το ότι είναι δύσκολο να βρω και να θυμηθώ έναν αξιόπιστο κωδικό πρόσβασης είναι μόνο ένας μύθος. Υπάρχουν κάποιες μέθοδοι, οι οποίες βοηθούν να βρίσκεις και να απομνημονεύεις αρκετούς μοναδικούς [κωδικούς πρόσβασης](#) ταυτόχρονα.
- Θα πρέπει να δίνετε ιδιαίτερη προσοχή στην ασφάλεια των κύριων διευθύνσεων του ηλεκτρονικού ταχυδρομείου σας, καθώς η πρόσβαση σε άλλους λογαριασμούς μπορεί να ανακτάται με τη βοήθεια ειδοποιήσεων μέσω ηλεκτρονικού ταχυδρομείου. Μπορείτε να εξασφαλίσετε το email σας εφαρμόζοντας την ταυτοποίηση δύο παραγόντων.
- Μην αποθηκεύετε τους [κωδικούς](#) πρόσβασής σας σε ένα κομμάτι χαρτί, στο σκληρό δίσκο σας ή οποιαδήποτε άλλη συσκευή. Δεν είναι ασφαλές. Απομνημονεύστε τους.

Πηγή: secnews.gr