

# Κωδικοί πρόσβασης

---

## Εισαγωγή



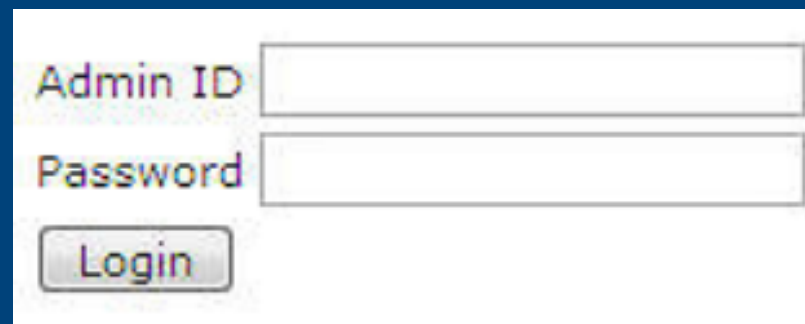
Πηγή: FlickrR

Ένα βασικό εργαλείο αναγνώρισης στις διάφορες ηλεκτρονικές υπηρεσίες, ο κωδικός πρόσβασης, είναι συχνά η μόνη προστασία έναντι ανεπιθύμητων εισβολών με δυνητικά καταστροφικές συνέπειες.

Ωστόσο, συχνά είναι ένα κακώς διαχειριζόμενο εργαλείο, καθώς πολλοί χρήστες δεν διστάζουν, για παράδειγμα, να χρησιμοποιήσουν πολύ απλούς κωδικούς πρόσβασης. Τέτοιοι κωδικοί είναι πιο εύκολο κάποιος να τους μαντέψει και να τους παραβιάσει. Είναι σημαντικό να γνωρίζετε τι διακυβεύετε με τους κωδικούς πρόσβασης και να γνωρίζετε πώς μπορείτε εύκολα να τους προστατεύσετε και να τους θυμάστε.

## ■ Αναγνώριση του χρήστη

Η χρήση ηλεκτρονικών υπολογιστών περιλαμβάνει συχνά την αναγνώριση χρηστών του διαδικτύου. Η πιο κοινή τεχνική βασίζεται στο ζεύγος «εγγραφή (login) / κωδικός (password)». Ανάλογα με την κατάσταση, το αναγνωριστικό μπορεί να είναι δημόσιο ή ιδιωτικό, αλλά συχνά δεν προστατεύεται επαρκώς. Ο κωδικός πρόσβασης είναι το εργαλείο που εξασφαλίζει την απαραίτητη ασφάλεια.

A screenshot of a web login form. It features two input fields: the top one is labeled "Admin ID" and the bottom one is labeled "Password". Below these fields is a button labeled "Login". The labels and the button text are in a blue, sans-serif font.

Πηγή: Flickr

# ■ Κύριος κίνδυνος: κλοπή ταυτότητας

*Ορισμός της Wikipedia:*

Κλοπή ταυτότητας είναι η σκόπιμη χρήση της ταυτότητας κάποιου άλλου, συνήθως ως μέθοδος για οικονομικό όφελος ή για να λάβει πίστωση και άλλα οφέλη στο όνομα ενός άλλου προσώπου και ίσως σε βάρος ενός άλλου προσώπου.

*Πρόβλημα:*

Ο προσδιορισμός της σχέσης μεταξύ παραβιάσεων δεδομένων και κλοπής ταυτότητας είναι πρόκληση, κυρίως επειδή τα θύματα κλοπής ταυτότητας συχνά δεν γνωρίζουν πώς έχουν αποκτηθεί τα προσωπικά τους στοιχεία και η κλοπή ταυτότητας δεν είναι πάντα ανιχνεύσιμη από τα θύματα.

## Συνεπώς....

Οι λειτουργοί εξυπηρέτησης που ζητούν αναγνώριση πρέπει να εφαρμόζουν πολυάριθμα μέτρα ασφαλείας για τη διαχείριση κωδικών πρόσβασης. Πρόκειται για ένα πολύ σημαντικό ζήτημα, για το οποίο όμως έχουμε λίγο έλεγχο.

→ Χρησιμοποιήστε κωδικό που δεν θα μπορεί να τον μαντέψει εύκολα ένας hacker

- Αποφύγετε απλούς κωδικούς όπως 12345, ημερομηνία γέννησης, ίδιο κωδικό πρόσβασης και εγγραφής κ.λ.π.
- Ο κωδικός πρέπει να είναι μεγάλος (τουλάχιστον 14 γράμματα/ψηφία)
- Πρέπει να είναι διαφοροποιημένος (κεφαλαία γράμματα, μικρά γράμματα, αριθμοί, ειδικοί χαρακτήρες κ.λ.π.)
- Ένας σοβαρός χειριστής θα εφαρμόσει κάποια μέτρα ασφαλείας όπως περιορισμένο αριθμό προσπαθειών, *captcha*



Πηγή: FlickR

## ■ Αλλά...

Οι περισσότεροι έχουν πολλούς λογαριασμούς και είναι πολύ σημαντικό να διαφοροποιήσετε τους κωδικούς πρόσβασής σας. Ως αποτέλεσμα, είναι περίπλοκο να τους απομνημονεύσετε όλους. Η διατήρηση κωδικών πρόσβασης σε μια θέση είναι επίσης επικίνδυνη.

**Πώς να αντιμετωπίσετε αυτό το ζήτημα;**

**Για να περιορίσετε αυτό το πρόβλημα απομνημόνευσης, υπάρχουν τρεις συμπληρωματικές μέθοδοι:**

- Χρησιμοποιείτε “προτάσεις για κωδικούς” εύκολες να τις θυμάστε αλλά δύσκολες στο να τις μαντέψει κάποιος
- Χρησιμοποιείτε μικτές μεθόδους ταυτοποίησης
- Χρησιμοποιείτε έναν διαχειριστή κωδικών

# « Προτάσεις για κωδικούς »

Αντί να χρειάζεται να θυμάστε πολύπλοκους κωδικούς όπως "Mζ9@X##Kl", σας συμβουλεύουμε να υιοθετήσετε «προτάσεις για κωδικούς», πιο εύκολο να τους θυμάστε, αλλά πιο πολύπλοκοι στο να αποκωδικοποιηθούν και να κλαπούν.

Πρόκειται για τη διατήρηση πολλών όρων εμπνευσμένων από στοιχεία γνωστά μόνο από τον χρήστη. Αντί της ημερομηνίας και του τόπου γέννησης, θα μπορούσαμε να βάλουμε ένα "γεννημένος στις έντεκα Η27 μια Πέμπτη". Αυτή η πρόταση μπορεί να είναι ή να μην είναι σχετική με την υπηρεσία για την οποία χρησιμοποιείται (με έναν μη προφανή τρόπο) και να μπορεί κάποιος να τη θυ-

Αυτό καθιστά δυνατή τη συμφιλίωση των πλεονεκτημάτων ενός σύνθετου κωδικού πρόσβασης και της εύκολης απομνημόνευσης!

# Μικτές μέθοδοι ταυτοποίησης

Οι διαχειριστές παρέχουν μικτές μεθόδους ταυτοποίησης όπου θα ζητηθεί από το χρήστη επιπρόσθετο στοιχείο εκτός από τον κωδικό πρόσβασης. Για μεγάλες επιχειρήσεις, η ταυτοποίηση γίνεται συχνά με πρόσθετο έλεγχο. Τις περισσότερες φορές, πρόκειται για την αναφορά ενός εφήμερου κώδικα που μεταδίδεται με SMS.

Το μειονέκτημα σε αυτή τη βελτίωση της προστασίας λογαριασμού είναι η μετάδοση πρόσθετων δεδομένων (αριθμός τηλεφώνου στο παράδειγμα που δόθηκε, επικύρωση μέσω ηλεκτρονικού ταχυδρομείου, επικύρωση έξυπνης κάρτας, βιομετρικά δεδομένα μπορούν επίσης να χρησιμοποιηθούν σε παρόμοιες περιπτώσεις).

Προσέξτε!

Το να δώσετε τον αριθμό τηλεφώνου σας στην τράπεζά σας είναι δικαιολογημένο, αλλά το να δώσετε βιομετρικά στοιχεία για μια ηλεκτρονική αγορά δεν είναι!

# Διαχειριστές κωδικών



Πηγή: Flickr

Ανεξάρτητα από το πώς δημιουργείτε τους κωδικούς σας, το να τους θυμάστε είναι πάντα η μεγαλύτερη πρόκληση! Μια καλή λύση είναι να χρησιμοποιήσετε έναν διαχειριστή κωδικών.

Σχεδόν όλα τα προγράμματα περιήγησης προσφέρουν την επιλογή να θυμούνται τους κωδικούς σας. Αυτή η δυνατότητα, ακόμα και αν απλοποιεί τη ζωή σας, μπορεί να είναι επικίνδυνη. Μερικοί περιηγητές, όπως το Firefox, αποθηκεύουν τους κωδικούς από προεπιλογή και σε απλό κείμενο!

Αν πραγματικά θέλετε να χρησιμοποιήσετε αυτή την επιλογή, το καλύτερο είναι να δημιουργήσετε έναν κύριο κωδικό. Έτσι θα προστατεύσετε την πρόσβαση σε καταχωρημένους κωδικούς.

## ■ Διαχειριστές κωδικών (2)

Η καλύτερη λύση είναι να χρησιμοποιήσετε έναν εξωτερικό διαχειριστή κωδικών πρόσβασης. Αυτό το λογισμικό πρέπει να εγκατασταθεί στον υπολογιστή σας. Θα διαχειρίζεται την απομνημόνευση των κωδικών πρόσβασης για εσάς. Τα πιο σοβαρά λογισμικά κρυπτογραφούν τους κωδικούς πρόσβασης που γίνονται προσβάσιμοι μόνο με τον κύριο κωδικό πρόσβασης που είναι επομένως ο μόνος που ο χρήστης πρέπει να θυμάται.

Παραδείγματα λογισμικών: Lastpass, Onepassword, Dashlane

Σημαντικό σημείο που πρέπει να αναφερθεί, τα λογισμικά Αυτά είναι δωρεάν!



# Ευχαριστούμε!

Ερωτήσεις;

---