Parole

Introducere

Source: FlickR

Un instrument cheie pentru identificarea diverselor servicii online, parola este adesea singura barieră de protecție împotriva intruziunilor nedorite cu consecințe potențial dezastruoase.

Cu toate acestea, este adesea un instrument slab gestionat, deoarece mulți utilizatori nu ezită, de exemplu, să utilizeze parole de bază. Acestea sunt, prin urmare, mai ușor de ghicit și hack. Este important să fiți conștienți de ceea ce este în joc cu parolele și să știți cum să le asigurați cu ușurință, păstrându-le în memorie.

Identificarea utilizatorului

Utilizarea computerelor presupune adesea identificarea utilizatorilor de internet. Tehnica cea mai comună se bazează pe perechea "conectare / parolă". În funcție de situație, identificatorul poate fi public sau privat, dar este adesea slab protejat. Parola este instrumentul care asigură securitatea esențială

Source: FlickR

Risc major: furtul de identitate

Definiția Wikipedia:
Furtul de identitate este utilizarea deliberată a identității unei alte persoane, de obicei ca metodă de a obține un avantaj financiar sau de a obține alte beneficii de credit și de altă natură în numele altei persoane și, probabil, de dezavantajul sau pierderea celeilalte persoane.
Problema:
Stabilirea legăturii dintre încălcările de date și furtul de identitate este o provocare, în primul rând pentru că victimele furtului de identitate de multe ori nu știu cum s-au obținut informațiile lor personale, iar furtul de identitate nu este întotdeauna detectabil de victimele individuale

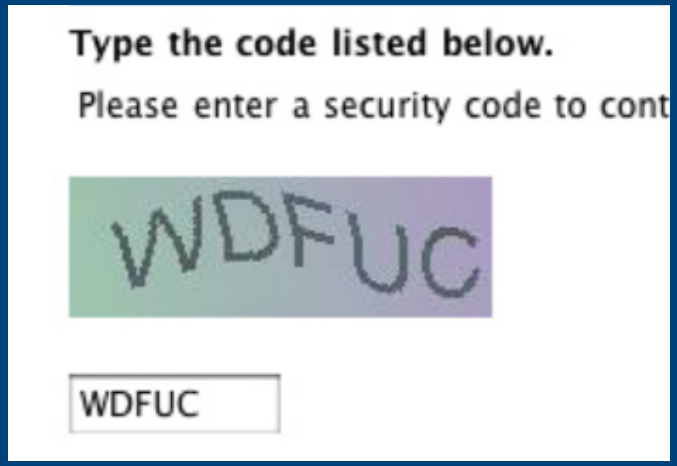
Erasmus+

Deci...

Operatorii care solicită identificarea trebuie să implementeze numeroase măsuri de securitate pentru a gestiona parolele. Aceasta este o chestiune foarte importantă, dar una asupra căreia avem puțin control.

➔ Utilizați o parolă care nu este ușor ghicită de un hacker

- *Evitați parolele de bază cum ar fi 12345, azerty, data nașterii, aceeași parolă decât datele de conectare etc.*
- *Parola trebuie să fie lungă (cel puțin 14 litere / cifre)*
- *Trebuie să fie diversificată (majuscule, cazuri inferioare, cifre, caractere speciale etc.)*
- *Un operator serios va implementa anumite măsuri de siguranță, cum ar fi numărul limitat de încercări, captcha*



Source: FlickR

Erasmus+

Dar...

Majoritatea oamenilor au multe conturi și este esențial să vă diversificați parolele. Ca urmare, este complicat memorarea tuturor. Păstrarea parolelor pe un post este de asemenea riscantă.

Deci, cum să abordăm această problemă?

Pentru a limita această problemă de memorare, sunt disponibile trei metode complementare:

- Utilizați "parole de frază" ușor de reținut, dar greu de ghicit
- Utilizați metode de identificare mixte
- Utilizați un manager de parole

« Parole de pronunție »

Mai degrabă decât să vă amintiți parolele complexe precum "Mç9 @ X ## Kl", vă sfătuim să adoptați "parole de propoziții", mai ușor de reținut, dar mai complicate pentru hacking.

Este vorba de păstrarea mai multor termeni inspirați de elemente cunoscute numai de utilizator. În loc de data și locul nașterii, am putea pune un "Născut la unsprezece H27 într-o joi". Această teză poate sau nu poate fi legată de serviciul folosit (într-o manieră nevăzută), astfel încât să poată fi amintit.

Acest lucru face posibilă reconcilierea avantajelor unei parole complexe în timp ce aceasta este memorată mai ușor!

Erasmus+

Metode de identificare mixte

Operatorii oferă metode de identificare mixte în care un utilizator suplimentar al parolei va fi solicitat de la utilizator. Pentru operațiuni mari, identificarea se face adesea cu o verificare suplimentară. De cele mai multe ori, este vorba de indicarea unui cod efemere transmis prin SMS.

Punctul nefast al acestei îmbunătățiri în protecția contului este transmiterea datelor suplimentare (numărul de telefon din exemplul dat, validarea prin e-mail, validarea unei cartele inteligente, datele biometrice pot fi de asemenea utilizate în cazuri similare).

Fiți atenți !
oferind numărul dvs. de telefon la banca dvs. poate fi justificată, dar datele biometrice pentru o achiziție de internet nu este!

Erasmus+

Managerii de parole

Source: FlickR

Indiferent de modul în care vă creați ghivecele de trecere, amintirea lor este întotdeauna cea mai mare provocare! O soluție bună poate fi utilizarea unui manager de parole.

Aproape toate browserele oferă să vă amintiți parolele. Această posibilitate, chiar dacă simplifică viața, poate fi periculoasă. Unele browsere, cum ar fi Firefox, păstrează parolele în mod implicit și în text simplu!
Dacă doriți să utilizați această opțiune, cel mai bine este să creați o parolă de bază. Acesta va proteja apoi accesul la parolele înregistrate.

Erasmus+

Administratori de parole (2)

Cea mai bună soluție este să utilizați un manager de parole externe. Acest software trebuie să fie instalat pe computer. Acesta va gestiona memorarea parolelor pentru dvs. Cele mai grave programe software criptează parolele care devin accesibile numai prin acordarea parolei principale, care este, prin urmare, singura pe care utilizatorul trebuie să o rețină.

Exemple de software: Lastpass, OnePassword, Dashlane et

Este important să remarcați faptul că acestea sunt gratuite!

1Password
Put Passwords In Their Place

Erasmus+

MULȚUMIRI!

Alte întrebări?