SECURITATEA PAROLELOR

Ing. Constantin Avrămescu
C.T. ”Anghel Saligny” Bacău

Voi incerca sa sintetizez in acest articol cateva greseli de evitat in alegerea parolelor

Simplul fapt ca nu ai mai fost jefuit nu inseamna ca este sigur sa lasi usile deschise, nu-i asa? Este nevoie de **un singur incident neprevazut pentru a pierde totul** - si acelasi lucru este valabil si pentru conturile de e-mail, conturile bancare si orice alte conturi pe care le detineti online sau pe dispozitivele mobile.

Unele din cele mai proaste parole din ultimii ani ar fi urmatoarele:

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars

Dupa cum puteti vedea, acestea sunt cele mai rele dintre cele mai rele. In acest moment, oricine foloseste una dintre cele de mai sus (sau ceva apropiat unuia de mai sus) ar putea la fel de bine sa nu aiba o parola. Nu aveti idee cat de repede un hacker ar putea sparge o parola atat de simpla!

De asemenea, daca credeti ca sunteti in siguranta, deoarece parola dvs. nu este pe aceasta lista, atunci este foarte posibil sa gresiti. Aceste parole sunt proaste, deoarece toate au caracteristici de parole usor de spart.

1. Parola evidenta

Sapte dintre primele 10 cele mai proaste parole din lista sunt variatii ale aceleiasi parole, adica numere consecutive. Gasim **1234** , **12345** , **123456** , **1234567** , **12345678** , **123456789** si **12345678 90** si asta pentru ca majoritatea site-urilor cer minim 4 caractere!!!.

Este clar ca oamenii folosesc aceasta parola (si variatiile acesteia), deoarece este super usor de tastat. Doar ruleaza degetele de la stanga la dreapta peste numere! De ceea, **qwerty** si **qwertyuiop** sunt si ele in aceasta lista.

Dar parolele nu sunt *menite* sa fie usoare! Multi oameni uita acest lucru. Folosind o parola evidenta - una care nu ti-a luat nicio perioada de gandire - cere doar ca cineva sa o ghiceasca. Este ca si cum am pune un lacat ce poate fi deschis cu aproape orice cheie.

2. Parola implicita

Este uimitor faptul ca una din cele mai folosite parole este insusi cuvantul **password** / **parola**. O multime de dispozitive vin cu parola implicita, dar vin si cu asteptarea ca utilizatorul final sa schimbe acea parola cu una proprie si mult mai sigura.

Nu este surprinzator, se pare ca multi oameni sunt comozi si fie refuza, fie uita sa faca aceasta modificare. Asadar, de exemplu, **chiar daca reteaua wireless este configurata in mod corespunzator** , este nevoie de zero eforturi pentru a va sparge cineva reteaua daca utilizati in continuare parola implicita pe router.

Deci, de fiecare data cand primiti un dispozitiv sau cont nou si vi se ofera un nume de utilizator si o parola implicita - cum ar fi **admin / admin** sau **admin / parola** - faceti-va un favor si schimbati-va parolele imediat. Nu amanati pentru ca veti uita!

3. Parola scurta

Unul dintre cele **mai importante aspecte ale unei parole potrivite** este lungimea absoluta. Fiecare caracter suplimentar - fie ca este vorba de o litera, un numar sau un simbol – mareste exponential timpul in care ar putea fi ghicita.

Deci, intr-un anumit sens, nimic nu este mai rau decat o parola scurta si acest lucru este evident atunci cand te uiti la lista de parole teribile.

Va intrebati daca parola dvs. este suficient de lunga? Probabil nu este.

Concepeti parole cat mai lungi!

4. Parola „Fara numere sau simboluri”

Tinand cont de cele de mai sus, o parola mai lunga de numai litere este de obicei mai buna decat o parola mai scurta cu litere, numere si simboluri - dar o parola mai lunga care incorporeaza litere, numere si simboluri este cu siguranta cea mai puternica dintre cele trei.

Asadar, **aywiresufzklthfrs** este o parola in regula, **ayw4r2s8f8kl43f2s** este chiar mai buna, iar **a!W4_2s8#8kl43f2%** este cea mai buna. Dupa cum puteti vedea, niciuna dintre cele mai proaste parole din lista nu contine simboluri in ele. Coincidenta? Deloc!

5. Parola de tip „Informatii personale”

Chiar daca suntem tentati sa folosim numele noastre sau ale apropiatilor in parole, nu se poate spune decat un singur lucru: NU o faceti De fapt, de fiecare data cand incercati sa veniti cu o noua parola, nu includeti niciodata detalii personale. O parola buna nu ar trebui sa aiba nicio legatura cu dvs., nici macar cu sportul / hobby-ul preferat (a se vedea parolele de tip fotbal / baseball din lista)

6. Parola de tip sablon

Este foarte tentat pentru cei ce lucreaza cu foarte multe parole sa isi creeze niste sabloane mentale ce le aplica peste tastatura si astfel rezulta o cate anumita parola pentru fiecare site / aplicatie in parte. Nu e nimic in neregula daca o faceti cum trebuie. Cu toate acestea, nu recurgeti niciodata la un model excesiv de simplist, cum ar fi **1qaz2wsx** , **qwerty** sau **qwertyuiop** .

Acest sfat este cu siguranta mai important in situatiile care necesita un PIN de patru cifre - cum ar fi ATM-urile sau ecranele de blocare a smartphone-ului - deoarece PIN-urile au un numar de posibilitati mult mai mic decat parolele complete. Totusi, incercati sa va asigurati ca parolele dvs. De tip sablon nu sunt ***prea*** evidente.

Parolele bune nu sunt greu de realizat

Un alt sfat important este sa nu repetati niciodata nici o parola!

La fel de importanta ca eliminarea parolelor slabe, este, de asemenea, sa **activati verificarea** in **doi pasi** pentru fiecare cont unde aceasta optiune este disponibila. Cele mai multe conturi bancare, conturi de e-mail si conturi de cumparaturi online **accepta** astazi **verificarea in doi pasi** .

In plus, ar trebui sa aveti o parola unica pentru fiecare cont pe care il aveti. Se pare ca asta ar fi imposibil de gestionat, dar este extrem de simplu daca **incepeti sa utilizati un manager de parole**.

In sfarsit, parolele puternice sunt doar o piesa din puzzle-ul de securitate online/offline. Asigurati-va ca va invatati sa va creati **obiceiuri bune de securitate** daca doriti cu adevarat liniste sufleteasca in aceasta lume online haotica.