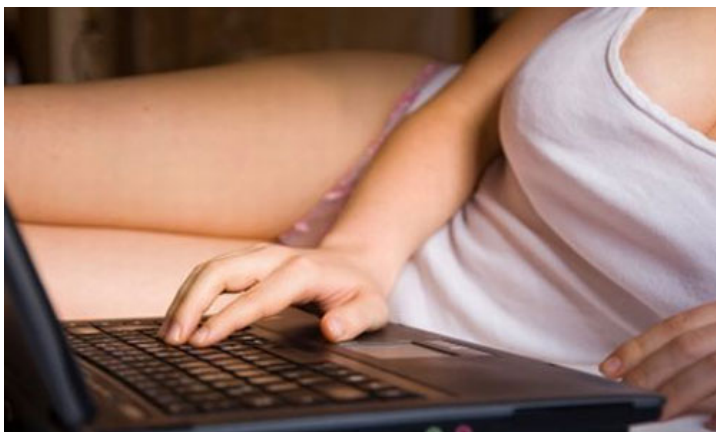




Ha csak a személyes és vállalati e-mail fiókunkat, Facebook-kontónkat, Windows felhasználói fiókunkat és a naponta használt sok más szolgáltatást összeszámoljuk, nagyon hamar összegyűl egy tucatnyi olyan, amelyet jelszóval védünk.

A mai napig a leggyakrabban használt biztonsági eszköznek, a jelszavas védelemnek rengeteg idegesítő tulajdonsága van, amit jellegéből adódóan sosem fog levetkőzni. Ezekkel még egy ideig meg kell küzdenünk, hiszen egyelőre nem létezik reális alternatíva a jelszó kiváltására, így nem árt tisztában lenni néhány alapvető biztonsági szabállyal.

1, 2, 3, 4, mondd jelszavam, hová mégy?

Valószínűleg egy rosszakaró vagy spammer jegyzetömbjébe – már ha vagyunk olyan okosak, mint az a több millió felhasználó, aki olyan jelszavakat választott, mint a **password**, **123456** vagy **12345678**.

Ez a három vezeti ugyanis a 2012-es jelszólistát

: bármilyen hihetetlen, idén ez a három volt a legnépszerűbb és ugyanakkor legrosszabb jelszó is.

A statisztikát most nem obskurus brit tudósok állították össze, hanem több millió ellopott jelszó alapján készült – ez is bizonyítja, hogy az ilyen és hasonló kombinációk használata egyáltalán nem biztonságos.

Bár abszolút értékben legtöbbször a fentieket használják, sokan születési évüket, nevüket, becenevüket vagy kutyájuk nevét írják meg jelszóként. Szóval ne csodálkozzunk, ha egy

A kukac nem véd meg

A word cloud shaped like a password field. The top part of the cloud contains the numbers '123456' in large, white, bold font. Below this, the word 'password' is written vertically in a large, blue, sans-serif font. The rest of the cloud is filled with various words and numbers in different colors (green, yellow, blue, white) and sizes, including '123456789', 'qwerty', '12345678', '1234567', '1234567890', '12345678901', '123456789012', '1234567890123', '12345678901234', '123456789012345', '1234567890123456', '12345678901234567', '123456789012345678', '1234567890123456789', '12345678901234567890', '123456789012345678901', '1234567890123456789012', '12345678901234567890123', '123456789012345678901234', '1234567890123456789012345', '12345678901234567890123456', '123456789012345678901234567', '1234567890123456789012345678', '12345678901234567890123456789', '123456789012345678901234567890', '1234567890123456789012345678901', '12345678901234567890123456789012', '123456789012345678901234567890123', '1234567890123456789012345678901234', '12345678901234567890123456789012345', '123456789012345678901234567890123456', '1234567890123456789012345678901234567', '12345678901234567890123456789012345678', '123456789012345678901234567890123456789', '1234567890123456789012345678901234567890', '12345678901234567890123456789012345678901', '123456789012345678901234567890123456789012', '1234567890123456789012345678901234567890123', '12345678901234567890123456789012345678901234', '123456789012345678901234567890123456789012345', '1234567890123456789012345678901234567890123456', '12345678901234567890123456789012345678901234567', '123456789012345678901234567890123456789012345678', '1234567890123456789012345678901234567890123456789', '12345678901234567890123456789012345678901234567890', '123456789012345678901234567890123456789012345678901', '1234567890123456789012345678901234567890123456789012', '12345678901234567890123456789012345678901234567890123', '123456789012345678901234567890123456789012345678901234', '1234567890123456789012345678901234567890123456789012345', '12345678901234567890123456789012345678901234567890123456', '123456789012345678901234567890123456789012345678901234567', '1234567890123456789012345678901234567890123456789012345678', '12345678901234567890123456789012345678901234567890123456789', '123456789012345678901234567890123456789012345678901234567890', '1234567890123456789012345678901234567890123456789012345678901', '12345678901234567890123456789012345678901234567890123456789012', '123456789012345678901234567890123456789012345678901234567890123', '1234567890123456789012345678901234567890123456789012345678901234', '12345678901234567890123456789012345678901234567890123456789012345', '123456789012345678901234567890123456789012345678901234567890123456', '1234567890123456789012345678901234567890123456789012345678901234567', '12345678901234567890123456789012345678901234567890123456789012345678', '123456789012345678901234567890123456789012345678901234567890123456789', '1234567890123456789012345678901234567890123456789012345678901234567890', '12345678901234567890123456789012345678901234567890123456789012345678901', '123456789012345678901234567890123456789012345678901234567890123456789012', '1234567890123456789012345678901234567890123456789012345678901234567890123', '12345678901234567890123456789012345678901234567890123456789012345678901234', '123456789012345678901234567890123456789012345678901234567890123456789012345', '1234567890123456789012345678901234567890123456789012345678901234567890123456', '12345678901234567890123456789012345678901234567890123456789012345678901234567', '123456789012345678901234567890123456789012345678901234567890123456789012345678', '1234567890123456789012345678901234567890123456789012345678901234567890123456789', '12345678901234567890123456789012345678901234567890123456789012345678901234567890', '123456789012345678901234567890123456789012345678901234567890123456789012345678901', '1234567890123456789012345678901234567890123456789012345678901234567890123456789012', '12345678901234567890123456789012345678901234567890123456789012345678901234567890123', '123456789012345678901234567890123456789012345678901234567890123456789012345678901234', '1234567890123456789012345678901234567890123456789012345678901234567890123456789012345', '12345678901234567890123456789012345678901234567890123456789012345678901234567890123456', '123456789012345678901234567890123456789012345678901234567890123456789012345678901234567', '123456789012345

Előtérbe kerül a dilemma, hogy miért ne adhatnánk igazán bonyolult jelszavakat, ha leírjuk őket. Viszont szinte minden jelszó-tanács azzal kezdődik, hogy ezt sose tegyük, bár vannak előnyei: a mindennapokban sokkal inkább tudunk vigyázni egy fontos papírfecnire, és jobban ráérezünk, hogy pontosan ki elől kell azt eldugni. A kollégáinkat, családtagjainkat mégiscsak jobban

ismerjük, mint egy orosz hackercsapatot.

A tiéd mekkora?

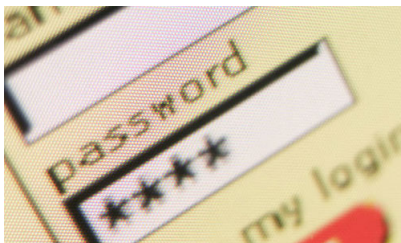
Sokaknak nem könnyű lenyelni, de igaz: a legtöbb biztonsági szakmunka évek óta arra tanít, hogy olyan jelszavakat adjunk, amit **az emberek nehezen jegyeznek meg, de a gépek könnyen feltörnek.** Gondoljunk csak bele, hány olyan szolgáltatás kéri, hogy használjunk fel mindenféle karaktertípust a jelszóban, de férjünk bele 16 karakterbe. Szinte az összes.

Pedig ha jelszavainkat hosszabb, megjegyezhető kifejezésekre cserélnénk, máris sokkal nyugodtabban alhatnánk. Vegyünk például egy támadót, aki másodpercenként 1 000 jelszóval próbálkozik. Egy öt karakteres, csupa véletlenszerű betűket tartalmazó jelszót – mondjuk azt, hogy fpqzy – mintegy három-négy óra alatt törne fel. És ezt az időt nagyon sokkal az sem tolná ki, ha néhány betű helyett számokat vagy speciális karaktereket írnánk.

De növeljük meg csak a felhasznált karakterek számát húszra, és a jelszó feltöréséhez szükséges idő is meghosszabbodik: körülbelül 6,5 billiárd évszázadra. Vagyis jóval hatékonyabb jelszó az, hogy „keresztapám egy elegáns bálnával sétált a tengerparton”, mint az, hogy „UDV@RH3LY”.

Ki jegyezze meg?

Ha már el is képzeltek, amint drága rokonunk egy cilinderes kalapot viselő bálnával andalog Konstancán, akkor már csak azt kéne kitalálni, hogy hol tudnánk felhasználni ezt a rettentően kreatív alkotást.



Gyakorlatilag az összes szolgáltatás arra kényszerít, hogy hülyébbnél hülyébb betűkombinációkat találjunk ki (aminek egyébként az lesz az eredménye, hogy mindenhol ugyanazt használjuk). Kapóra jöhetnek a password keeperek, vagyis a jelszavak biztonságos tárolására, megjegyzésére létrehozott programok, mint például a LastPass vagy a 1Password.

Ezek előnye, hogy bármilyen összetett rendszer szerint képesek jelszavakat generálni, amiket aztán különböző felhasználói fiókjainkhoz rendelhetünk, majd az egészet levédhetjük egy jól megjegyezhető, de ugyanakkor erős mesterjelszóval. Ez sem tökéletes megoldás, hiszen egyetlen, központi helyen tároljuk az összes jelszavunkat, így nem jó ötlet elfelejteni a mesterjelszót. Ajánlott valamilyen kódolt formában leírni egy darab papírra, és biztos helyen tárolni, legalább amíg megjegyezzük.

Egy biztos: olyan nem létezik, hogy tökéletes biztonság, de a mesterjelszavas módszer elviselhető kompromisszum lehet adataink biztonsága és saját kényelmünk között, miközben az agyunk sem sül ki a rengeteg kukac meg szám lehetetlen kombinációjától. Csak el ne felejtjük, hova tettük a papírt.