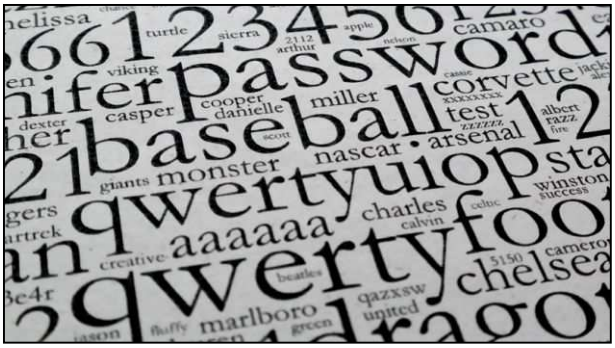
SZILÁGYI SZABOLCS

Az ön jelszavát ismerik a hekkerek?

Egy új Chrome-kiegészítővel egyszerűen és gyorsan kideríthető, hogy a felhasználó hitelesítését szolgáló karaktersorozattal visszaéltek-e már a hekkerek.



Nagyjából azóta küzd az emberiség a jelszavak problémájával, amióta kitalálta a karakteres felhasználóazonosítás módszerét. Kiváltására mindmáig nem került sor tömeges méretekben, pedig jelenleg is számos próbálkozás fut, hogy egyszerűbbé és biztonságosabbá válhasson a hitelesítési eljárás.

A Microsoft például a Windows 10 S operációs rendszerbe való beléptetésnél száműzi a hagyományos jelszavak használatát − már ami a bejelentkezést illeti. Több lehetőség is rendelkezésére áll: mobil autentikációt, biometrikus megoldásokat és USB-alapú FIDO kulcsokat egyaránt alkalmazhatnak a Microsoft Insider programjában részt vevők.

Utóbbi alkalmazását célozta meg a World Wide Web Konzorcium (W3C) is. Kezdeményezése a FIDO (Fast IDentity Online, FIDO Alliance) által fejlesztett webes API használatán alapul, ami erős kriptografikus műveletek használatára támaszkodik a jelszavak cserélgetése helyett. A szabványosítási törekvések mögé a legnépszerűbb webes böngészőket fejlesztő szervezetek, így a Google, a Mozilla, a Microsoft és az Apple is beálltak.

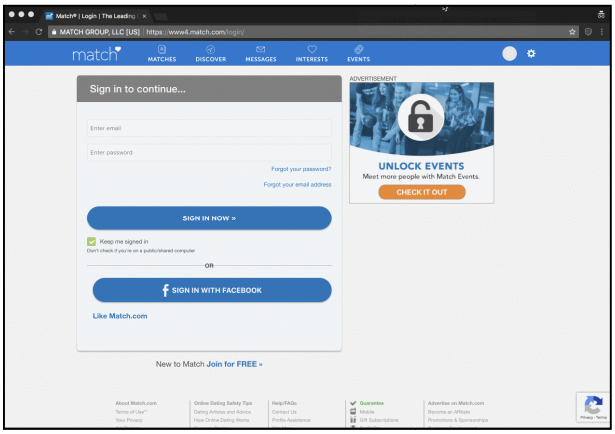
Könnyen kideríthető, biztonságos-e a jelszó

Addig azonban, amíg a fentiek közül bármelyik módszer általánosan elterjed, továbbra is kénytelenek vagyunk jelszavakat használni. Sokunk ráadásul nem fordít kellő figyelmet arra, milyen karaktersorozatot választ magának, így viszonylag egyszerű szótáralapú próbálgatással feltörni hitelesítő kódját.

Ám még akkor sem lehetünk nyugodtak, ha legalább 10 karakteres, kis- és nagybetűből, számból és minimum egy speciális karakterből álló jelszót választottunk, hiszen az elmúlt néhány évből jó néhány olyan eset ismert, amikor ezek a hitelesítő adatok a szolgáltatóktól szivárogtak ki. Az eBay-től 150 millió, a Yahoo-tól pedig félmilliárd felhasználó adatai kerültek illetéktelenek kezébe.

Jó lenne tehát felhasználói szinten tudni, hogy az adott jelszó vajon kompromittálódott már, kell-e cserélni. Ezt a funkciót nyújtja az Okta által fejlesztett PassProtect, ami a hackerek által bevett gyakorlatot használja saját javára. A támadók ugyanis többnyire – de például célzott jelszóhalászat esetében nem – értékesíteni akarják a birtokukba jutott jelszavak tömegét. Ez az információhalmaz így előbb-utóbb elérhetővé, és egyben kereshetővé válik.

Itt jön a képbe a bejelentkezés-menedzsmenttel foglalkozó Okta böngészőkiegészítője. A PassProtect a fenti adatok révén megállapítja, hogy a felhasználó jelszava bekerült-e már a hekkerek adatbázisába, pontosabban azt, hogy hányszor próbálták felhasználni a (közel)múltban lezajlott online behatolási kísérletek során. Minden egyes alkalommal, amikor használója begépel egy azonosítókódot, a kiegészítő összeveti azt adatbázisával, és ha egyezést talál, akkor nem csupán értesíti erről a tényről a monitor előtt ülőt, hanem egyben felhívja a figyelmet a jelszóváltoztatás szükségességére.



Emellett a kiegészítővel át lehet nézetni a Have I Been Pwned adatbázisát. Ennek köszönhetően nyomon követhetjük jelszavaink kiszolgáltatottságát akkor is, ha éppen nem használjuk az adott szolgáltatást.

Rábízhatjuk titkainkat az Oktára?

Egyre paranoidabbá váló világunkban gyakran akkor járunk a legjobban, ha nem bízunk meg senkiben és semmiben. Miért engedjünk tehát hozzáférést az Oktának jelszavainkhoz? A fejlesztők szerint a PassProtect vigyáz a felhasználó hitelesítő kódjaira, azokat kizárólag az adott számítógépen elemzi ki, és sosem küld róla másolatot a böngészőn keresztül. Tulajdonképpen a weboldalakon használt jelszókezelési eljárásoknál bevett gyakorlatot alkalmazza.

Ennek során először egy hash algoritmussal a jelszóból előállít egy sztringet, majd ennek első öt karakterét továbbítja az internetes adatbázisba. A Have I Been Pwned információs bázisa mintegy félmilliárd, ismerten kiszolgáltatottá vált jelszót tartalmaz. Ezekkel veti össze a karaktereket, és azokat a bejegyzéseket küldi vissza a felhasználó eszközére, melyek ugyanazzal az öt karakterrel kezdődnek. A PassProtect a letöltött, teljes jelszavakat hasonlítja az internetező komplett azonosítókódjával, és egyezés esetén értesíti erről.

Jelenleg csupán Google Chrome-ra készült el a böngészőkiegészítő, de az Okta reményei szerint hamarosan Mozilla Firefoxhoz és a mobilokon használt browserekhez is elérhető lesz. Szintén csőben van egy website-fejlesztők által használható eszköz, amivel közvetlenül be lehet ágyazni a PassProtectet a weboldalakba. Ezzel már a szolgáltatásba történő regisztrációkor meg lehet határozni, hogy a felhasználni kívánt jelszót érdemes-e inkább elkerülni.

Forrás: **https://bitport.hu/az-on-jelszavat-ismerik-a-hackerek**

Válogatta: Fonyó Istvánné