OUCH! 2023. december

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A Jelmondatok Ereje

Önnek is kimerítő és idegőrlő folyton összetett jelszavakat kitalálni? Majd ezekre emlékezni és begépelni egyesével az összes karaktert, különleges szimbólumot és számot? Nos, szerencsére van egy megoldásunk erre: az örökké erős jelmondat!

Jelmondatok

Talán nem is annyira köztudott, de jelszavaink a kibertámadók egyik elsődleges támadási vektorai. A rossz fiúk legelőször mindig a jelszavainkat veszik célba, és ha azt sikerül kitalálniuk vagy feltörniük, akkor könnyen hozzáférhetnek az e-mailjeinkhez, bankszámláinkhoz, vagy akár még a személyazonosságunkat is ellophatják. Minél gyengébbek a jelszavaink, a támadók annál könnyebben juthatnak be rendszereinkbe. Éppen ezért, egy erős jelszó az egyik leghatékonyabb módja annak, hogy megvédjük fiókjainkat és az online életünket. Eredetileg arra tanítottak minket, hogy nagyon összetett és bonyolult jelszavakat használjunk. Az alapötlet az volt, hogy minél komplexebb egy jelszó, annál nehezebb dolguk van a támadóknak és az automatizált programoknak feltörni azt. Ezzel az a probléma, hogy az összetett jelszavakat nehéz megjegyezni és helyesen begépelni. Az erős, biztonságos jelszó létrehozásának azonban van egy jobb módja is, az úgynevezett jelmondatok (passphrase) létrehozása, amelyek a bonyolultságuk helyett, inkább a hosszúságuk miatt számítanak erősnek. Nézzünk néhány példát:

Igyunk egy eros kavet!
eltunt-csiga-csavar-part

A jelmondatok tulajdonképpen szavak sorozatai, amelyek akár több mint húsz karaktert is tartalmazhatnak, ha az adott webhely ezt lehetővé teszi. Ez talán soknak tűnhet, de mindkét fenti példa több, mint húsz karaktert tartalmaz, és a jelszavakkal ellentétben a jelmondatokat sokkal könnyebb megjegyezni, és egyszerűbb is begépelni. Minél hosszabb egy jelmondat, annál biztonságosabb. Előfordulhat, hogy a jelszó megadásakor arra kér minket az oldal, hogy tegyük még bonyolultabbá azt – például szimbólumok, nagybetűk vagy számok hozzáadásával. Ennek a legegyszerűbb módja az, ha a jelmondatban szereplő betűket szimbólumokkal vagy számokkal helyettesítjük. Például, ha az e betűt 3-asra cseréljük, a fenti példák bonyolultabbá válnak, mégis elég könnyen megjegyezhetők és beírhatók maradnak:

Igyunk 3gy 3ros kav3t!
3ltunt-csiga-csavar-part

Legyen Egyedi

Annak érdekében, hogy jelszavunk valóban biztonságos legyen, minden fiókhoz egyedi jelszót kell választanunk. Ha ugyanazt a jelszót használjuk mindenhol, vagy egy könnyen azonosítható jelszómintát követünk több fióknál is, azzal veszélyeztetjük adatainkat.

Ebben az esetben a támadónak mindössze egyetlen általunk gyakran látogatott weboldalt kell feltörnie, és ha az összes többi fióknál ugyanez a jelszavunk, akkor az ellopott jelszóval a többi fiókunkhoz is hozzáférhet. Túl nehéz megjegyezni az egyedi jelmondatokat? Erre is van egy megoldásunk: a jelszókezelők.

A jelszókezelők olyan speciális számítógépes programok, amelyek biztonságosan tárolják a jelszavainkat egy titkosított, úgynevezett elsődleges jelszóval védett tárolóban. A jelszószéf eléréséhez csak az elsődleges jelszót kell megjegyeznünk, a jelszókezelő pedig automatikusan lekéri a többi jelszavunkat, és bejelentkezik a weboldalakra. A jelszókezelők egyéb funkciókkal is rendelkezhetnek, többek között például tárolhatják a biztonsági kérdésekre adott válaszainkat; jelezhetnek, ha ugyanazt a jelszót akarnánk felhasználni több fióknál; figyelmeztethetnek a hamis weboldalakra; továbbá erős jelszavakat is generálhatnak nekünk. A legtöbb jelszókezelő biztonságosan szinkronizál szinte minden számítógéppel vagy más eszközzel, így attól függetlenül, hogy milyen rendszert használunk, könnyen és biztonságosan hozzáférhetünk jelszavainkhoz.

Az Utolsó Lépés – Többfaktoros hitelesítés

Az utolsó lépés annak érdekében, hogy jelszavainkat valóban bolondbiztossá tegyük, egy második védelmi réteg hozzáadása – ez pedig a többfaktoros hitelesítés, az úgynevezett Multi-Factor Authentication (MFA). Az MFA megköveteli tőlünk, hogy legalább két azonosítóval rendelkezzünk a fiókunkba való belépéshez. Ez lehet a jelszavunk és egy biometrikus adat, például az ujjlenyomatunk; vagy lehet a jelszavunk és egy automatikusan generált számkód, amelyet egy másik eszközre vagy e-mail fiókra küldenek a bejelentkezéskor. A kód természetesen minden alkalommal egyedi, és mobiltelefonról vagy más megbízható eszközről is előállítható. Ez a folyamat nagy biztonsággal garantálja, hogy ha egy támadó meg is szerzi egyik jelszavunkat, akkor sem tud bejutni az adott fiókba, mivel nem rendelkezik a második faktorral. Az MFA-t lehetőség szerint mindig engedélyezni kell, különösen a kulcsfontosságú fiókok, például banki, nyugdíj- vagy személyes e-mail fiókok esetében. Természetesen a jelszókezelőket is ajánlott erős jelmondattal ÉS többfaktoros hitelesítéssel védeni.

A jelmondatokkal tehát egyszerűbbé tehetjük a biztonságot, ezáltal sokat segítenek fiókjaink védelmében. Annak érdekében, hogy a digitális életünk még egyszerűbb és biztonságosabb legyen, azt javasoljuk, hogy jelszavaink kezelésekor kombináljuk a jelszószéfeket és a többfaktoros hitelesítést.

A szerzőről

Quintana Patterson a Coloradói Egyetem Anschutz Medical Campusának klinikai és megfelelőségi informatikai menedzsere és a WiCyS (Women in CyberSecurity) érdekérvényesítési bizottságának elnöke. Quintana elkötelezett amellett, hogy a nők ebben az iparágban is megfelelő támogatást kapjanak és érezzék, hogy megbecsülik a munkájukat.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
Biometria: https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Többfaktoros autentikáció: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)