
Az Ön havi biztonságtudatossági hírlevele

# Egyszerű jelszókezelés

## Áttekintés

Gyakran hallható, hogy a jelszó kulcsfontosságú a személyes fiókok megvédésében (ami igaz), azonban ritkán beszélnek azokról az egyszerű módszerekről, amelyekkel biztonságosan hozhatóak létre és kezelhetőek a jelszavak. Az alábbiakban bemutatunk három egyszerű lépést a jelszavak egyszerűsítésére, a személyes fiókok zárolására és a jövő biztosítására.

## Jelmondat

A bonyolult jelszavaknak vége. Az ilyen jelszavakat nehéz megjegyezni, nehézkes a begépelésük, és egy mai gyors számítógéppel könnyen feltörhetik a támadók. A jó jelszó megfelelően hosszú, és minél több karaktert tartalmaz annál biztonságosabb. A jelmondatok olyan megfelelően erős jelszavak, amelyek rövid mondatokból vagy véletlenszerű szavakból állnak. Például:

***Itt az idő egy erős kávéra!***
***elveszett-csiga-csúszik-a-parton***

Mindkét jelszó hosszabb, mint 20 karakter, így erősnek számítanak. Könnyű megjegyezni őket, egyszerűen begépelhetőek, azonban nehéz a feltörésük. Néha, bizonyos weboldalak vagy helyzetek megkövetelik, hogy egyéb karaktereket is használjunk (számok, nagy betűk, speciális karakterek), amivel nincs semmi baj. Azonban ne felejtsük, hogy a jelszó hossza a legfontosabb.

## Jelszó kezelők

Minden felhasználói fiókunkhoz használjunk egyedi jelszót. Ha ugyanazt a jelszót adjuk meg több fiókunkhoz is, nagy veszélynek tesszük ki magunkat. Ha egy kiberbűnöző feltöri az egyik weboldalt, amit mi is használunk és ellopja a jelszavakat, beleértve a miénket is, be tud lépni az összes felhasználói fiókunkba. Ez sokkal gyakoribb, mint gondolnánk. Hihetetlen? A www.haveibeenpwned.com weboldalon ellenőrizhetjük, melyik oldalakat törték fel, valamint, hogy jelszavunk kompromittálódott-e. Mit tehetünk ilyenkor? Használjunk jelszó kezelőt.

A jelszókezelők speciális programok, amelyek biztonságosan, egy „széfben”, kódolva tárolják jelszavainkat, csak a jelszókezelő mesterjelszavára kell emlékeznünk. Amikor egy weboldalon bejelentkezünk, a jelszókezelő automatikusan kiolvassa a jelszavunkat, és beléptet az adott weboldalra. A legtöbb jelszókezelő számos más funkcióval is rendelkezik. Eltárolja a titkos kérdésekre adott válaszainkat, figyelmeztet, ha ugyanazt a jelszót több helyen is használjuk, vagy akár megfelelően erős jelszót

generál számunkra. Ezen kívül a legtöbb jelszókezelő automatikusan szinkronizál számítógépünk és egyéb eszközeink között, így bármelyik rendszert is használjuk, könnyen és biztonságosan hozzáférhetünk jelszavainkhoz.

Végezetül egy fontos figyelmeztetés. Jegyezzük fel a mesterjelszót, és tároljuk egy biztonságos otthoni helyen. Némelyik jelszókezelőből ki tudunk nyomtatni egy visszaállító kódot is. Amennyiben elfelejtjük a jelszókezelőnk mesterjelszavát, ezzel vissza tudjuk állítani azt. Ha esetleg betegek vagyunk, vagy vészhelyzetben találjuk magunkat, házastársunk vagy családtagunk hozzá tud férni a szükséges információkhoz.

## Kétlépcsős azonosítás

A kétlépcsős azonosítás (gyakran hívják kétfaktoros vagy többfaktoros azonosításnak) egy további szinttel emeli a biztonságot. Amikor belépünk a felhasználói fiókunkba két dologra lesz szükségünk: a jelszavunkra, valamint egy számokból álló kódra, amit az okostelefonunk generál vagy üzenetként érkezik meg telefonunkra. Ez az eljárás biztosítja, hogy ha egy kiberbűnöző meg is szerzi jelszavunkat, nem férhet hozzá felhasználói fiókunkhoz. A kétlépcsős azonosítást könnyű beállítani és rendszerint csak egyszer kell használni, amikor egy új számítógépről vagy más eszközről jelentkezünk be. Használjuk, amikor csak lehetőség van rá, különösen olyan fontos fiókoknál, mint netbank, nyugdíjszámla vagy akár az e-mail fiókunk. Ha jelszókezelőt használunk, különösen ajánlott, hogy erős jelmondatot ÉS kétlépcsős azonosítást is alkalmazzunk.

Bármennyire is furcsán hangzik, ez a három egyszerű lépés vezet ahhoz, hogy megvédjük munkánkat, hírnevünket és biztosítsuk jövőbeli pénzügyi helyzetünket.

## Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

## A szerzőről

***Justin Henderson*** *(@SecurityMapper) a H & A Security Solutions társalapítója, SANS tanúsítvánnyal rendelkező oktató, valamint szerzője a "SANS Cyber Defense and SIEM" – "SANS kibervédelem és SIEM rendszerek" tanfolyamoknak. Több mint 15 éve dolgozik tanácsadóként és minden érdekli, ami a kibervédelemmel kapcsolatos.*

## Források

| | |
|---|---|
| Have I Been Pwned: | https://haveibeenpwned.com/ |
| Kétfaktoros hitelesítés: | https://twofactorauth.org/ |
| NIST SP800-63B Digitális identitás útmutató: | https://pages.nist.gov/800-63-3/sp800-63b.html |
| Poszter: Te vagy a célpont: | https://www.sans.org/u/OGi |