

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A jelszókezelők ereje

Frusztált a jelszavak miatt?

A legtöbb emberhez hasonlóan valószínűleg Ön is megterhelő feladatnak találja a különféle jelszavak létrehozását, kezelését és észben tartását. Úgy tűnik, mintha minden webhely különböző jelszósabályokkal rendelkezne, emellett ezek sok esetben további biztonsági intézkedést is igényelnek, mint például biztonsági kérdések beállítását. Nem lenne nagyszerű, ha lenne egyetlen megoldás, amely gondoskodik minden jelszóproblémáról? Létezik ilyen megoldás. Jelszókezelőnek hívják.

A jelszókezelők leegyszerűsítik és biztonságossá teszik digitális életünket.

A jelszókezelők olyan szoftvermegoldások, amelyek egy biztonságos adatbázisban tárolják a jelszavainkat, amit gyakran tárolónak is neveznek. A jelszókezelő titkosítja a tároló tartalmát, és azt egy ún. elsődleges jelszóval vagy más néven „mesterjelszóval” védi, amelyet csak a jelszókezelő tulajdonosa ismer. Amennyiben szükségünk lenne valamelyik jelszavunkra, a tárolót egyszerűen feloldhatjuk ezzel a mesterjelszóval. A jelszókezelő integrálódhat a webböngészőnkbe, amely automatikusan lekérdezi a helyes jelszót, majd biztonságosan bejelentkeztet a webhelyre. Az egyedi jelszóhasználat kritikus fontosságú digitális életünk biztonságának megőrzéséhez, ez a megoldás pedig egyszerűen megoldást nyújthat erre.

Továbbá a legtöbb jelszókezelő képes az eszközök közötti automatikus szinkronizálásra. Ezáltal, amikor frissítünk egy jelszót az egyik eszközünkön, ahhoz egy másikon is hozzáférhetünk. Végezetül, a legtöbb jelszókezelő képes érzékelni, ha egy új online fiókot regisztrálunk, amihez elkészíti és tárolja az új egyedi jelszavunkat.

Az egyetlen jelszó, amelyet meg kell jegyeznünk, az a jelszókezelő eléréséhez szükséges mesterjelszó. Nagyon fontos, hogy ez a jelszó hosszú és egyedi legyen. Azt javasoljuk, hogy mesterjelszóként egy ún. „passphrase-t” – vagyis egy több szóból vagy kifejezésből álló hosszú jelszót – alkalmazzunk. Amennyiben lehetséges, használjunk többfaktoros hitelesítést is! Végezetül létfontosságú, hogy ne felejtjük el a mesterjelszavunkat, ezzel elkerülve, hogy kizárjuk magunkat a saját fiókunkból!

A jelszókezelő kiválasztása

Számos jelszókezelő közül választhatunk. A hírlevél „Források” részében található hivatkozások segítséget nyújthatnak a jelszókezelők áttekintéséhez. Miközben megpróbáljuk megtalálni a legmegfelelőbbet, tartsuk szem előtt a következőket:

- A jelszómenedzser legyen egyszerűen kezelhető! Amennyiben a kiválasztott alkalmazást túl bonyolultnak találjuk, keressünk egy másikat, amely jobban illeszkedik az igényeinkhez!
- Egy jó jelszókezelő kompatibilis az összes eszközünkkel és képes szinkronizálni az adatainkat.
- Kizárólag jól ismert és megbízható jelszómenedzsereket használjunk! Legyenünk óvatosak azon termékekkel, amelyek nem régóta léteznek, illetve amelyekről nincs, vagy csak kevés közösségi visszajelzés érhető el!
- Mindig a legfrissebb verziót használjuk, valamint győződjünk meg arról, hogy a gyártó folyamatosan frissíti az általunk használt jelszókezelőt!
- A jelszómenedzsernek lehetőséget kell biztosítania arra, hogy más érzékeny adatokat is tároljunk benne, mint például a titkos biztonsági kérdésekre adott válaszainkat, a hitel- vagy törzsvásárlói kártyáink adatait.
- Legyünk óvatosak azokkal a jelszókezelőkkel, amelyek lehetővé teszik a mesterjelszó visszaállítását, vagy módosítását a technikai háttértámogató személyzet (support) számára!

Érdemes lehet leírni, illetve zárt borítékban, védett helyen tárolni elsődleges jelszavunkat, arra az esetre, ha véletlenül elfelejténénk.

A jelszókezelőket nem nekünk találták ki?

Van akinek a jelszómenedzserek használata bonyolultnak tűnhet. A biztonságunk megőrzése érdekében azonban minden fiókhoz egyedi jelszóra van szükségünk. Hogyan emlékezhetünk biztonságosan az összes egyedi jelszavunkra? Az egyik lehetőség, hogy leírjuk a jelszavainkat. Azonban a munkával kapcsolatos jelszavaink esetében ez nem jó megoldás. Ellenben ez egy jó alternatíva lehet a személyes fiókjaink jelszavainak a tárolásához, amennyiben a jelszóséf használata nem opció. A legfontosabb lépés a lejegyzett jelszó biztonságba helyezése. Amennyiben mi vagy akár egy családtagunk jegyzetfüzetet használ a jelszavak tárolásához, győződjünk meg arról, hogy azt biztonságos helyen tároljuk és csak olyanok férhetnek hozzá, akikben megbízunk!

A szerzőről

Noureen Njoroge hatalmas tapasztalattal rendelkező kiberbiztonsági vezető mind az állami, mind a magánszektorban. Stratégiai gondolkodású, aki vezetői tapasztalattal rendelkezik a feltörekvő technológiákkal kapcsolatos kérdésekben. Noureen vezető típus, akinek szenvedélye mások mentorálása. LinkedIn: <https://www.linkedin.com/in/noureennjoroge/>.



Források

Jelszókezelő áttekintés: <https://www.pcmag.com/picks/the-best-password-managers>

Több faktoro autentikáció: <https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/>

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

OUCH! A Sans Security Awareness részleg által közzétett és a [Creative Commons BY-NC-ND 4.0 licenz](https://creativecommons.org/licenses/by-nc-nd/4.0/) alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. Szerkesztette: Walter Scrivens, Phil Hoffman, Alan Wagoner, Les Ridout, Princess Young.