A Havi Biztonsági Tudatosságról szóló hírlevele

Jelszókezelők

Áttekintés

Ahhoz, hogy megvédje magát, az egyik legfontosabb lépés az egyedi és erős jelszó használata minden fiókjánál és alkalmazásánál. Sajnos azonban szinte lehetetlen emlékezni az összes különböző jelszóra. Ráadásul tudjuk, hogy a jelszavak folyamatos beírása a különböző webhelyeken, az új jelszavak generálása, a biztonsági kérdésekre adott válaszok nyomon követése és még számos egyéb tényező időigényes feladat. Van azonban olyan megoldás, amely az életét sokkal egyszerűbbé és sokkal biztonságosabbá teszi - a jelszókezelők.

Hogyan működnek a jelszókezelők?

A jelszókezelők az összes jelszavát egy adatbázisban tárolják, amelyet néha tárolónak hívnak. A jelszókezelő titkosítja a tároló tartalmát, és egy mesterjelszóval védi, amelyet csak Ön ismer. Amikor szüksége van a jelszavára, például az online bankfiókjába vagy e-mail fiókjába való bejelentkezéshez, egyszerűen csak be kell írnia a mesterjelszavát a jelszókezelőbe a tároló feloldásához. A jelszókezelő automatikusan lekérdezi a helyes jelszót, és biztonságosan bejelentkezik a webhelyre. Többé nem kell megjegyeznie a jelszavait, vagy manuálisan bejelentkeznie a fiókjaiba.

Ezen felül a legtöbb jelszókezelő magában foglalja az automatikus szinkronizálás lehetőségét több eszközön keresztül. Így, amikor frissít egy jelszót a laptopján, a változás szinkronizálódik az összes többi eszközére. Végül, a legtöbb jelszókezelő érzékeli, amikor Ön új online fiókot hoz létre vagy meglévő fiókjának jelszavát módosítja, és automatikusan frissíti a tároló tartalmát.

Fontos, hogy a jelszókezelő védelmére használt mesterjelszó megfelelően hosszú és egyedi legyen. Leginkább azt javasoljuk, hogy mesterjelszavát jelmondatként adja meg, ami több szóból vagy kifejezésből áll. Amennyiben a jelszókezelő támogatja a kétlépcsős azonosítást, használja azt mesterjelszavához is. Végezetül, ügyeljen arra, hogy ne felejtse el mesterjelszavát. Ha mégis elfelejti, akkor nem fog hozzáférni a többi jelszavához.

Jelszókezelő kiválasztása

Számos jelszókezelő közül választhat. A „Források” részben hivatkozást talál a jelszókezelők áttekintéséhez. Miközben megpróbálja megtalálni az Önnek legmegfelelőbbet, tartsa szem előtt a következőket:

A jelszókezelő használatának egyszerűnek kell lennie. Ha túl bonyolultnak talál egy megoldást, keressen másikat, amely jobban megfelel az Ön elvárásainak és szakértelmének.

A jelszókezelőnek minden olyan eszközön működnie kell, amelyen jelszavakat használ. A jelszavak eszközök közötti szinkronizálásának egyszerűnek kell lennie.

Csak jól ismert és megbízható jelszókezelőket használjon. Legyen óvatos azon termékekkel, amelyek csak nem régóta léteznek, vagy amelyekről nincs, vagy csak kevés közösségi visszajelzés érhető el. A kiberbűnözők hamis jelszókezelőket is létrehozhatnak, hogy ellopják adatait. Legyen nagyon óvatos azokat a gyártókat illetően, akik azt reklámozzák, hogy saját titkosítási megoldást fejlesztettek ki.

Kerüljön el minden olyan jelszókezelőt, amely állítólag vissza tudja állítani a mesterjelszavát. Ez ugyanis azt jelenti, hogy ismerik a mesterjelszavát, ami túl nagy kockázatot rejt magában.

Győződjön meg arról, hogy bármilyen megoldást is választ, a fejlesztő továbbra is aktívan frissíti és javítja a jelszókezelőt, valamint különösen ügyeljen arra, hogy mindig a legújabb verziót használja.

A jelszókezelőnek lehetőséget kell adnia arra, hogy abban más érzékeny adatokat is tároljon, például a titkos biztonsági kérdésekre adott válaszokat, hitelkártya adatokat, vagy épp pontgyűjtő kártyák adatait.

Fontolja meg mesterjelszavának zárt borítékban történő elhelyezését, és zárt szekrényben, fizikai széfben vagy tárolóban való tárolását.

A jelszókezelők nagyszerű lehetőséget kínálnak jelszavainak és egyéb érzékeny adatok, például hitelkártya számok biztonságos tárolására. Ügyeljen azonban arra, hogy egyedi, erős mester jelmondatot használjon, és mindig használja az alkalmazás legújabb verzióját.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI 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 https://nki.gov.hu oldalon olvasható.

A szerzőről

Russell Eubanks *egy atlantai információbiztonsági vezető, aki több mint 20 éves szakmai tapasztalattal és számos biztonsági tanúsítvánnyal rendelkezik. A SANS Internet Storm Center egy munkatársa, aki közreműködik a Critical Security Controls (Kritikus Biztonsági Kontrollok) megalkotásában. Russell elérhető a @russelleubanks-on, valamint a https://www.securityeverafter.com weboldalon.*

Források

Egyszerű jelszókezelés:	http://www.sans.org/u/Y10
Digitális öröklés:	http://www.sans.org/u/Z10G
A legjobb jelszókezelők áttekintése:	https://www.wired.com/story/best-password-managers/