Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Jelszókezelő programok

Áttekintés

A saját magunk védelmében megtehető egyik legfontosabb lépés az, hogy minden egyes felhasználói fiókunkhoz erős és egyedi jelszót használunk. Sajnos a legtöbbünk olyan sok fiókkal rendelkezik, hogy szinte lehetetlen észben tartani az ezekhez tartozó jelszavakat. Erre a problémára egy egyszerű megoldás lehet a jelszókezelő programok használata (ezeket nevezik néha jelszó trezornak is). Ezeket az alkalmazásokat arra készítik, hogy biztonságosan tároljuk a felhasználói adatainkat. Ráadásul ezek használatával sokkal egyszerűbben lehet a weboldalakra, mobil vagy egyéb alkalmazásokba belépni.

A szerzőről

Lenny Zeltser az NCR Corp ügyfelei IT biztonságát felügyeli, valamint biztonsági szakértőket oktat a SANS Intézetben. A Twitter-en a **@lennzeltser** csatornán találkozhatunk vele, illetve cikkeket publikál a **zeltser.com**-on.

Hogy működnek a jelszókezelő programok?

A jelszókezelő programok úgy viselkednek, mint egy digitális trezor. Biztonságosan tárolja a felhasználóneveket, jelszavakat és egyéb bizalmas információkat. Amikor egy oldalon be kell jelentkezni a felhasználói fiókunkba, akkor a jelszókezelő automatikusan kiolvassa a jelszavunkat, és biztonságosan beléptet az adott weboldalra. Ez lehetővé teszi, hogy akár több száz erős, egyedi jelszót használjunk, mivel egyiket sem kell észben tartanunk.

A jelszókezelő program egy adatbázisban tárolja ezeket az információkat, pont úgy mint egy trezor. A program titkosítja a trezor tartalmát, és egy olyan mesterjelszóval védi, amit csak mi ismerünk. Amikor szükségünk van egy felhasználói fiók adataira, például ha be akarunk lépni az online banki vagy email fiókunkba, csak egyszerűen beírjuk a mesterjelszavunkat a jelszókezelő programba, és így ki tudjuk nyitni a trezort.

Egyes jelszókezelő programok a saját számítógépünkön vagy okostelefonunkon tárolják az értékeinket, mások pedig egy távoli adatbázisban, amit a program készítője működtet. Ezen kívül a legtöbb jelszókezelő fontos képessége, hogy képes a trezor tartalmát automatikusan szinkronban tartani számos eszközön keresztül, amelyeknek engedélyt adtunk erre. Így ha módosítunk egy jelszót a laptopunkon, a változások szinkronizálódnak az okostelefonunkra, tabletünkre vagy tetszőleges más, általunk használt számítógépre. Függetlenül attól, hogy az adatbázis hol tárolódik, a használathoz telepítenünk kell egy jelszókezelő programot a rendszerünkre.

Jelszókezelő programok

Első használatkor, a jelszókezelő programba kézzel kell felvennünk a meglévő felhasználói fiókjaink adatait, vagy importálnunk kell azokat. Ezután már a program képes észlelni, ha egy új online fiókot akarunk regisztrálni, vagy módosítani akarjuk egy meglévő fiók beállításait, ilyenkor automatikusan frissíti a jelszókezelő tartalmát. Ez azért lehetséges, mert a legtöbb jelszókezelő program együtt működik a böngészővel, és ez az integráció teszi lehetővé azt is, automatikusan jelentkezzünk be a weboldalakra.

A jelszókezelő programok egyszerű megoldást kínálnak a különböző jelszavaink biztonságos tárolására és használatára.

A jelszókezelő programokat úgy készítik, hogy biztonságosan tárolják a jelszavakat. Azonban rendkívül fontos, hogy a trezor tartalmát védő mesterjelszó nagyon erős, mások számára kitalálhatatlan legyen. Valójában azt javasoljuk, hogy a mesterjelszó egy jelmondat legyen, ami a jelszavak egyik legerősebb típusa. Ha a jelszókezelő támogatja a két lépcsős hitelesítést, akkor használjuk ezt is a mesterjelszóhoz! Végezetül pedig nagyon fontos, hogy semmilyen más fiókhoz vagy rendszerhez ne használjuk ezt a mesterjelszót! Így, ha egy hacker le tudja másolni a jelszókezelő tartalmát, még akkor sem tudja kitalálni a hozzá tartozó jelszót, és hozzáférni a tartalmához. Végezetül még egy fontos figyelmeztetés. Ne felejtsük el a mesterjelszót, mert különben nem fogunk tudni hozzáférni egyetlen, a jelszókezelőben tárolt jelszavunkhoz sem.

Jelszókezelő program kiválasztása

Számos ingyenes és fizetős jelszókezelő program közül választhatunk. Miközben megpróbáljuk megtalálni a nekünk legjobbat, az alábbiakat érdemes észben tartani:

- Győződjünk meg arról, hogy minden olyan rendszeren fut a program, amiről hozzá akarunk férni a jelszókezelőhöz. Ezzel a megoldással a jelszókezelő tartalmát is könnyen szinkronban lehet tartani a különböző eszközök között.
- Csak jól ismert és megbízható programot használjunk. Legyünk óvatosak az olyanokkal szemben, amelyek nem régóta vannak jelen, vagy nem található róluk közösségi visszajelzés. A kiberbűnözők nem csak hamis víruskereső programokat, hanem hamis jelszókezelőket is készítenek, hogy ellophassák a jelszavainkat.
- A programnak egyszerűnek kell lennie. Ha túl összetett, hogy megértsük, keresnünk kell egy alternatív megoldást, amely jobban megfelel a képességeinknek.
- Bármelyik megoldást is választjuk, mindig legyen naprakész, telepítsük a legfrissebb verziót és hibajavításokat is.
- A programnak lehetővé kell tennie, hogy könnyedén válasszunk erős jelszót a különböző fiókjaink számára, illetve tudnia kell automatikusan erős jelszót generálni.
- Képesnek kell lennie egyéb bizalmas információk tárolására is, mint például a titkos kérdésre adandó választ, bankkártyaszám, vagy egyéb más információ!

Jelszókezelő programok

- Tartózkodjunk az olyan programoktól, amelyek egyedi vagy ismeretlen módszert használnak a jelszókezelő titkosítására a jól ismert ipari szabványok helyett. Ha a gyártó azzal dicsekszik, hogy saját titkosító megoldást fejlesztett, akkor maradjunk távol tőlük.
- Felejtsük el azokat a programokat, amelyet azt állítják, hogy vissza lehet szerezni az elfelejtett mesterjelszavakat. Ez azt jelenti, hogy ismerik a mesterjelszavunkat, amely óriási kockázatnak tesz ki bennünket.

A jelszókezelők nagyszerű eszközök arra, hogy biztonságosan tároljuk a jelszavainkat és egyéb bizalmas információinkat. Mivel ilyen fontos adatokat bízunk ezekre, ezért körültekintően kell kiválasztani a programhoz tartozó mesterjelszót, amit nagyon nehéz kitalálni, de mi mégis könnyen meg tudunk jegyezni.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Jelmondatokról:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
A kétlépcsős hitelesítés:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201509_hu.pdf
A legjobb 5 jelszó kezelő (angolul):	http://lifehacker.com/5529133/five-best-password-managers
SANS napi biztonsági tipp (angolul):	http://www.sans.org/tip_of_the_day.php

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó