OUCH! | 2017. szeptember

Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

Jelszókezelő programok

Áttekintés

Az egyik legfontosabb dolog, amit tehetünk az online védelmünk érdekében, hogy egyedi és erős jelszót használunk az összes fiókunkhoz és applikációnkhoz. Sajnos valószínűleg lehetetlen, hogy az összes jelszavunkra emlékezzünk, amiket a különböző fiókjainkhoz használunk. Ez az oka annak, hogy sokan ugyanazt a jelszót használják több helyen is. Ugyanazon jelszó több fiókhoz történő használata veszélyes, mert ha egyszer valaki feltöri a jelszavunkat, akkor hozzáférése lesz minden olyan fiókunkhoz, amihez ezt a jelszót használjuk. Egyszerű megoldás a jelszókezelő programok (más néven: jelszó trezor) használata. Ezek olyan programok, amik biztonságosan tárolják az összes jelszavunkat megkönnyítve ezzel, hogy minden fiókunkhoz különböző jelszóval rendelkezzünk. Ezt teszik egyszerűvé a jelszókezelő programok, mert ahelyett hogy minden egyes jelszavunkra emlékeznünk kellene, csak a jelszókezelő programhoz tartozó mester jelszót kell tudnunk.

A szerzőről

Chris Christianson 20 év tapasztalattal és számos technikai tanúsítvánnyal rendelkező információbiztonsági tanácsadó Kaliforniában. Különféle konferenciákon adott elő és számos iparági cikk szerzője. Elérhetőségei: **@cchristianson**, **https://ismellpackets.com**.

Jelszókezelő programok működése

A jelszókezelő programok egy adatbázisba tárolják az összes jelszavunkat, amit néha trezornak is neveznek. A jelszókezelő titkosítja a trezor tartalmát és egy olyan mesterjelszóval védi, amit csak mi tudunk. Amikor szükségünk van egy jelszavunkra, hogy belépjünk az online banki felületre, vagy hozzá akarunk férni az emailjeinkhez, akkor egyszerűen csak beírjuk a mester jelszavunkat a jelszókezelő programba, hogy kinyissuk a trezort. Számos esetben a jelszókezelő program automatikusan előveszi a jelszót és biztonságosan belép nekünk. Ezzel egyszerűen lehet akár több száz egyedi és erős jelszavunk úgy, hogy azokra nem kell emlékeznünk.

Egyes jelszókezelő programok a trezorunkat a számítógépünkön vagy mobileszközünkön helyezik el, míg mások felhőben tárolják. Továbbá, a legtöbb jelszókezelő képes az általunk felügyelt eszközök trezorjai közötti automatikus szinkronizációra. Így ha frissítjük az egyik jelszavunkat a laptopon, ez a változás az összes egyéb eszközünkre szinkronizálva lesz. Az adatbázis tárolásának helyétől függetlenül a használathoz a jelszókezelő alkalmazást a rendszerünkre vagy eszközünkre fel kell telepíteni.

Jelszókezelő programok

A jelszókezelő első használatakor meg kell adnunk manuálisan vagy importálnunk kell a bejelentkezési adatainkat és jelszavainkat. Később – nyitott trezor esetén – a jelszókezelő fel tudja ismerni, hogy új online felhasználó fiókot próbálunk regisztrálni vagy egy létező profilunkhoz tartozó jelszót frissítünk és automatikusan frissíti a trezort ennek megfelelően. Ez azért lehetséges, mert a jelszókezelőnk kéz a kézben működik a web böngészőnkkel. Ez az integráció lehetővé teszi, hogy automatikuson be is léptessen minket a weboldalra.

Elengedhetetlen, hogy a mester jelszó, amit a jelszókezelő program tartalmának megvédéséhez használunk, erős legyen és mások nehezen tudják kitalálni. Valójában javasolt, hogy mester jelszóként egy jelmondatot használjunk, ami az egyik lehetséges legerősebb jelszótípus. Ha a jelszókezelő programunk támogatja a kétlépcsős hitelesítést, akkor azt használjuk mesterjelszóként. Végül legyünk biztosak abban, hogy emlékezni fogunk a mester jelszavunkra. Ha elfelejtjük, akkor nem fogunk hozzáférni a többi jelszavunkhoz.

Jelszó kezelő programok használatával egyszerűen és biztonságosan tárolhatjuk jelszavainkat.

Jelszókezelő program kiválasztása

Számos jelszókezelő program közül választhatunk. A források szekcióban szereplő linkek egyike a jelszókezelő programok áttekintéséről szól. Az alábbi szempontokat vegyük figyelembe, amikor a nekünk megfelelő jelszókezelőt próbáljuk megtalálni:

- A jelszókezelő programunk használata legyen számunkra egyszerű. Ha a megoldást túl összetettnek találjuk, akkor keressünk egy másikat, ami jobban megfelel a tapasztalatainknak és a stílusunknak.
- A jelszókezelő programnak minden olyan eszközön működnie kell amin jelszavakat használunk. Legyen egyszerű a jelszavaink szinkronizálása az összes eszközünkre.
- Csak ismert és megbízható jelszókezelőt használjunk. Legyünk óvatosak az olyan termékekkel, amik nem régóta elérhetőek illetve nincs vagy csak kevés a közösségi visszajelzés róluk. A kiberbűnözők létrehozhatnak hamis jelszókezelőket, hogy ellopják az információinkat. Legyünk gyanakvóak bármelyik olyan eladóval, aki azt állítja, hogy saját titkosítási megoldást fejlesztett ki.
- Kerüljük el az olyan jelszókezelő programokat, amik azt ígérik, hogy képesek visszaállítani a mester jelszavunkat számunkra. Ez azt jelenti, hogy tudják a mester jelszavunkat, ami túl nagy kockázatot jelent nekünk.
- Bármely megoldást választjuk, legyünk biztosak abban, hogy a gyártó rendszeresen ad ki frissítéseket és javításokat a jelszókezelő programhoz. Továbbá győződjünk meg arról, hogy mindig a legfrissebb verziót használjuk.

Jelszókezelő programok

- A jelszókezelő programnak legyen olyan funkciója, amely automatikusan generál erős jelszót, illetve mutassa meg az általunk választott jelszó erősségét.
- A jelszókezelő program tegye lehetővé, hogy más érzékeny adatokat is tudjunk benne tárolni, mint a titkos biztonsági kérdésekre adandó válaszokat vagy a hitelkártya és törzsutas adatokat.

A jelszókezelő program használata megfelelő megoldás az összes jelszavunk és az érzékeny adataink biztonságos tárolására. Mivel fontos információkat védenek, bizonyosodjunk meg arról, hogy egyedi és erős mester jelszót használunk, amit nemcsak a támadónak nehéz kitalálni, de számunkra könnyen megjegyezhető.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

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.

Hivatkozások

2017 Top jelszókezelő programjai:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Jelmondatok:	https://securingthehuman.sans.org/ouch/2017#april2017
Két lépcsős azonosítás:	https://www.securingthehuman.org/ouch/2015#september2015
Zárja le bejelentkezését:	https://www.lockdownyourlogin.org/
SANS a nap biztonsági tippje:	https://www.sans.org/tip-of-the-day

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita

