OUCH! | 2014. augusztus

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

**Ebben a kiadványban...**

- **Mi az a titkosítás?**
- **Helyi titkosítás**
- **Adatátvitel titkosítása**

# A titkosításról

## Mi az a titkosítás?

Mindannyian hallottunk már a titkosításról, valamint arról, hogy ennek segítségével meg tudjuk védeni saját magunkat és adatainkat, azonban sokak számára nem egészen egyértelmű maga a titkosítás koncepciója, illetve az, hogy ez sem véd meg bennünket mindentől, mivel ennek is megvannak a maga korlátai. Az OUCH! ehavi számában bemutatjuk, hogy mit is jelent a titkosítás, miért érdemes használni, és hogyan lehet megfelelően beállítani.

**A szerzőről**

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) tanácsadóként dolgozik Washington DC-ben. A SANS Institute Mobile Device Security and Ethical Hacking (SEC575) kurzusainak vezető oktatója, illetve Incident Response Team Management (MGT535) kurzus tananyagának szerzője.

Hatalmas mennyiségű bizalmas információ gyűlhet össze az általunk használt mobil eszközökön (pénzügyi adatok, képek, email-ek, egészségügyi információk, stb.). Ha elveszítjük vagy ellopják tőlünk az eszközt, akkor ezek az érzékeny információk idegen kézbe juthatnak. Ezen kívül végezhetünk olyan online tranzakciókat is, amelyeket szintén nem szeretnénk idegenekkel megosztani. Márpedig ha egy kiberbűnöző képes megfigyelni ezeket a műveleteket, akkor könnyedén megszerezheti az online banki fiókunk vagy a hitelkártyánk, bankkártyánk adatait. A titkosítás segít abban, hogy illetéktelen személyek ne tudjanak hozzáférni és ne tudják módosítani a bizalmas információkat.

Amikor az információ nincs titkosítva, akkor azt úgy nevezzük, hogy egyszerű vagy sima szöveg (plain text). Ez azt jelenti, hogy bárki könnyedén hozzáférhet és elolvashatja. A titkosítás az ilyen sima szöveget nem olvasható titkosított szöveggé (cipher text) alakítja át. A titkosítási folyamat összetett matematikai műveletek és egy egyedi kulcs segítségével alakítja át az információt titkosított szöveggé. Az egyedi kulcs segítségével lehet zárolni vagy feloldani az információt, pontosan úgy, mint egy valódi kulcs esetén az ajtókat. Általában jelszót használunk kulcsnak, így csak az a személy férhet hozzá a titkosított adatokhoz, aki birtokában van a megfelelő jelszónak. Ahhoz, hogy megvédjük a titkosított adatainkat, meg kell védenünk a kulcsot. Általánosságban azt mondhatjuk, hogy a titkosítások kétféle módon működnek. Egyrészt meg kell védenünk a helyben tárolt adatokat (pl. egy laptop merevlemezén), illetve az adatátvitel közben (pl. egy internetes adattovábbítás esetén).

## Helyi adatok titkosítása

A helyi adatok titkosításának elsődleges célja az, hogy ha esetleg elvész vagy ellopják a mobil eszközt, az azon lévő adatok ne kerüljenek illetéktelen kezekbe. Tizenöt éve ez még nem jelentett problémát, mivel az akkori számítógépek főleg nagy, asztali gépek voltak, amelyeket nem volt könnyű hordozni. A manapság gyakran használt laptopok alig néhány kilósak, míg a mobil eszközök pedig csak néhány dekagrammot nyomnak. Ezek az eszközök

## A titkosításról

gyakorlatilag komplett számítógépek, és rendkívül sok bizalmas adatot hordozhatnak, viszont nagyon könnyen elveszíthetők. Ezen kívül vannak még egyéb adathordozók is, amelyeken bizalmas információkat tárolunk (pendrive, CD-ROM). Az ilyen esetben szokás használni a Full Disk Encryption (FDE) módszert, azaz a lemezen lévő összes tartalom automatikusan titkosításra kerül, nem szükséges nekünk dönteni arról, hogy most akarunk-e valamit titkosítani vagy sem. Manapság a legtöbb operációs rendszer ismeri az FDE módszert, nekünk legfeljebb csak engedélyezni kell. Például a Mac OS X része a FileVault nevű alkalmazás, a Windows egyes verziói pedig tartalmazzák a Bitlocker nevű titkosító programot. Mindenképp javasolt ezen funkciót használni, amennyiben a számítógépünk képes erre. Érdemes tudni azt is, hogy a legtöbb mobil eszköz képes a belső tároló eszköz is teljes egészében titkosítani valamilyen FDE módszerrel. Például az iOS rendszereket használó iPhone-ok és iPad-ek a teljes háttértárat titkosítják, miután egyszer beállítottuk a jelszavas védelmet. Érdemes megkérdezni a rendszergazdát vagy az ügyfélszolgálatot, hogy az általunk használt eszközök képesek-e FDE titkosítást használni. Saját tulajdonú eszköz esetén pedig a gyártó weboldala segíthet ennek a kérdésnek a megválaszolásában.

*A titkosítás egy megfelelő módszer arra, hogy biztonságba helyezzük az adatainkat, de ez csak annyira biztonságos, mint amennyire erős a titkosítás feloldását szolgáló kulcs.*

## Adatátvitel titkosítása

Az információ akkor is veszélyben van, amikor egyik helyről a másikra küldjük át. Amennyiben nincs titkosítva, akkor egy esetleges lehallgatás során könnyen hozzá lehet férni. Ezért meg kell bizonyosodnunk arról, hogy az olyan bizalmas online adatátvitelek titkosítva vannak-e, mint például webbankba történő bejelentkezés, online vásárlás, de akár még a közösségi oldalak felé irányuló kommunikáció is. Erre a leggyakoribb módszer a HTTPS protokoll használata, ami azt eredményezni, hogy a böngészőnk és a weboldal közti adatátvitel automatikusan titkosításra kerül. Abból tudhatjuk, hogy aktív az adatforgalom titkosítása, hogy a weboldal címe így kezdődik: https://, vagy ha egy zárt lakat van a cím előtt, esetleg a teljes címsor zöld színűre változik. Ezek mind a titkosított kommunikáció jelei, amelyek külön-külön, vagy akár együtt is megjelenhetnek internethasználat közben. Amennyiben nyílt WiFi elérést kell használnunk, akkor győződjünk meg arról, hogy használjuk a titkosítást, amennyiben lehetőségünk van rá! Végezetül pedig ne feledkezzünk meg arról, hogy ha email kliensből küldünk vagy fogadunk levelet, akkor azt mindig titkosított csatornán keresztül tegyük meg! A legtöbb email kliens külön eszköz nélkül is tudja kezelni a titkosítást, és talán az internetszolgáltató is tud segíteni a beállításban.

## Megfelelő titkosítás beállítása

Függetlenül attól, hogy milyen titkosítási eljárást vagy mire használunk, szinte minden eljárásban azonos lépéseket kell megtenni a megfelelő beállítások érdekében:

## A titkosításról

- A titkosítás csak annyira erős, amennyire a titkosító kulcs. Amennyiben valaki kitalálja vagy feltöri az általunk használt kulcsot, akkor hozzáférhet az adatainkhoz. Védjük meg a saját kulcsunkat!
- Amennyiben jelszót használunk a kulcshoz, akkor az legyen hosszú és biztonságos jelszó, és ne felejtsük el, mert különben nem férünk hozzá a saját adatainkhoz!
- A titkosítás csak annyit ér, amennyire biztonságban van a számítógépünk. Amennyiben feltörik, vagy káros szoftverrel fertőződik meg a rendszerünk, akkor a támadó megkerülheti a titkosítást. Ezen kívül gondoskodjunk arról is, hogy az eszközt fizikailag is biztonságban tartsuk!
- Amennyiben különböző titkosítási módszerek közül választhatunk, akkor mindig a legerősebbet válasszuk!

## 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

| | |
|---|---|
| Mac OS X Filevault: | http://support.apple.com/kb/ht4790 |
| iOS titkosítás: | http://support.apple.com/kb/ht4175 |
| Android titkosítás: | http://www.androidauthority.com/how-to-encrypt-android-device-326700/ |
| Windows titkosítás: | http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7 |
| 7 lépés a számítógép védelme érdekében: | http://www.securingthehuman.org/ouch/2012#december2012 |
| Jelszókezelő megoldások: | http://www.securingthehuman.org/ouch/2013#october2013 |



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



 