

OUCH!

Havi biztonság tudatossági hírlevél mindenkinek

# A legjobb tippek a közösségi média biztonságos használatához

## Áttekintés

Az olyan közösségi média oldalak, mint a Snapchat, Facebook, Twitter, Instagram és a Linked in hihetetlen erőforrások, melyek lehetővé teszik, hogy az egész világon tudjunk más emberekkel ismerkedni, interakcióba kerülni és megosztani. Azonban ezen erők kockázatokkal is járnak nem csak számunkra hanem a családunk, barátaink és munkáltatónk számára is. Ebben a számban bemutatjuk azokat a kulcsfontosságú lépéseket, amelyek lehetővé teszik, hogy a közösségi média a lehető legbiztonságosabb legyen.

## Posztolás

Legyünk óvatosak és gondoljuk át mielőtt posztolunk. Bármilyen közlést, amit publikusan elérhetővé fog válni, befolyásolva a hírnevünket és a jövőnket, beleértve azt is, hogy hova mehetünk iskolába vagy milyen munkát kaphatunk. Ha nem akarjuk, hogy a családunk vagy a főnökünk lássa a posztot, akkor valószínűleg nem kellene közzé tennünk. Ezen felül kövessük figyelemmel, hogy mások miket osztanak meg rólunk. Őket megkérhetjük, hogy távolítsák el azokat, amiket megosztottak rólunk.

## Adatvédelem

Majdnem minden közösségi média oldal erős adatvédelmi lehetőségekkel rendelkezik, lehetőleg engedélyezzük azokat. Például tényleg szükséges, hogy az oldal követni tudja a tartózkodási helyünket? Továbbá, az adatvédelmi lehetőségek kuszának tűnhetnek és gyakran változhatnak is. Válasszon rutinszerűvé ezek ellenőrzése, győződjünk meg róla, hogy azok a mi elvárásainknak megfelelnek.

## Jelmondatok

Tegyük biztonságossá a közösségi média fiókunkat egy hosszú egyedi jelmondattal. A jelmondat egy több szóból álló jelszó, amit nekünk könnyű megjegyezni és begépelni de a kibertámadók számára nehéz kitalálni.

## Zárjuk a fiókunkat

Még jobb, hogy ha engedélyezzük a kétfaktoros autentikáció használatát az összes fiókunknál. Ez kiegészíti egy egyszeri kóddal a jelszavunkat, amikor be kell lépni a fiókunkba. Tulajdonképpen ez nagyon egyszerű és az egyik legerősebb módja a fiókunk védelmének.

## Csalások

Csak úgy, mint az email esetén, a rossz fiúk megpróbálnak becsapni vagy bolonddá tenni minket a közösségi média üzenetek segítségével. Például megpróbálhatják kicsalni a jelszavunkat vagy bankkártya adatainkat. Legyünk óvatosak,

hogy mire kattintunk rá: ha egy barátunk látszólag egy furcsa üzenetet küld nekünk, vagy nem úgy hangzik mintha ő írta volna akkor lehet, hogy egy kibertámadó tesz úgy mintha a barátunk lenne.

## Felhasználási feltételek

Ismerjük meg az oldalak felhasználási feltételeit. Bármilyen, amit megosztunk vagy feltöltünk az oldal tulajdonává válhat.

## Munka

Ha bármit szeretnénk megosztani a munkánkkal kapcsolatban, akkor ellenőriztessük le először a vezetőnkkel, hogy az publikusan megosztható-e.

Kövessük ezeket a tippeket, egy sokkal biztonságosabb online élmény érdekében. Ha többet szeretnénk megtudni a közösségi média oldalak biztonságos használatáról vagy a jogosulatlan tevékenységek bejelentéséről akkor ellenőrizzük a közösségi média oldalak biztonsági szabályait.

## 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.

## A szerzőről

**Jessica Barker** világszerte a kiberbiztonság humán területén. Tanácsadói szolgáltatásokat nyújt ügyfeleinek világszerte a [Redacted Firm](#) nevű cégnél, melynek társalapítója, valamint előadóként is ismert. A [@drjessicabarker](#) azonosítón követhető Twitteren.



## Források

Jelmondatok:	<a href="https://www.sans.org/u/B6E">https://www.sans.org/u/B6E</a>
Kétlépéses autentikáció:	<a href="https://www.sans.org/u/B6J">https://www.sans.org/u/B6J</a>
A mai online gyerekek biztonsága:	<a href="https://www.sans.org/u/B6O">https://www.sans.org/u/B6O</a>
Biztonságos bejelentkezés:	<a href="https://www.lockdownyourlogin.org/">https://www.lockdownyourlogin.org/</a>

## License

Az OUCH! a Sans Securing The Human részleg által közzétett és a [Creative Commons BY-NC-ND 4.0 licenz](#) alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. A Fordításért vagy további információért lépjen kapcsolatba velünk a [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter) címen. Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Fordította: Tikos Anita