OUCH! | 2020. február

OUCH!
A Havi Biztonsági Tudatosságról szóló hírlevele

# Adatvédelem a közösségi médiában

## Áttekintés

A legtöbb ember soha sem tudná elképzelni, hogy besétál egy zsúfolt szobába és az ott lévő összes idegennek hangosan elmondja magánéletének minden részletét — egészségügyi állapotától kezdve a családja és a barátai nevén, életkorán át egészen munkahelyének vagy iskolájának címéig. Azonban ugyanezek az emberek gyakran kétszer sem gondolják meg, hogy ezeket az információkat a közösségi médiában közzétegyék. A túl sok információ megosztásának következményei nemcsak a személyes és szakmai életre, hanem a család és a barátok életére is kihathatnak.

A közösségi média remek hely a kapcsolatteremtésre, a megosztásra és a tanulásra. Azonban pusztán a közösségi média adatvédelmi beállításainak megszigorításával nem tudja megvédeni magát. Amint egyszer valamit online közzétesz, elveszíti az irányítást felette. Meg kell értenie, hogy mi kerül összegyűjtésre, valamint az hogyan kerül felhasználásra. Íme néhány adatvédelmi aggály, amelyekkel a közösségi média használatakor szembe kell néznie:

**Adatvédelmi beállítások:** Figyelmesen állítsa be és gyakran vizsgálja felül az összes közösségi média fiókjának adatvédelmi beállításait, különösen akkor, ha változások történnek a szolgáltatás és az adatvédelmi irányelvek vonatkozásában. Ne felejtse el, hogy még ha be is állította, hogy ki láthatja az Ön posztjait, az összes információ összegyűjtésre, elemzésre és tárolásra kerül a közösségi média platform szerverein — talán örökre.

**Adatvédelmi fa:** A közösségi média beállításai nem tudják megvédeni Önt azoktól a barátoktól, rokonoktól és munkatársaktól, akik megnézik az Ön posztjait, majd megosztják ezeket a hozzászólásokat saját baráti körükkel és így tovább.

**Családi adatok megosztása:** Mindenki szeret mesélni barátairól és családjáról. Azonban a születésnapi tortáról készült buta képek, illetve az egészségügyi és viselkedési problémák megosztása megfélemlítéshez vezethetnek, különösen a fiatalabbak számára, ráadásul életüket is befolyásolhatják.

**Információ megosztás:** Ha egy szolgáltatás „ingyenes”, akkor Ön a termék. Kutatások kimutatták, hogy az Ön online tevékenységének adatait másoknak akár el is lehet adni.

**Helymeghatározó szolgáltatások:** A bejelentkezési adatokat más személyes adatokkal összevetve profil készíthető az életéről és a szokásairól, amely lehetőséget ad arra, hogy megfigyeljék Önt, valamint sérülékennyé tehetik más zaklató tevékenységekkel szemben. Mindemellett legyen óvatos a posztolt képeken vagy videókban szereplő, tartózkodási helyére vonatkozó információkkal.

**Mesterséges intelligencia:** Az MI (mesterséges intelligencia), a közösségi média és a marketing a tökéletes kombináció. A hirdetők manapság az Ön online szokásaiból összegyűjtött információkat használják arra, hogy a legutóbbi keresésének vagy vásárlásának megfelelő hirdetéseket mutassanak Önnek, egyre több és több ismeretet szerezve.

**Digitális halál:** Ha valaki meghal, akkor online jelenléte sebezhetőbbé válik a rosszindulatú személyekkel szemben, főként ha az örökösök nem gondozzák vagy szüntetik meg online fiókjait. Az egyén magánélete nemcsak a személyét érinti; hanem hatással lehet a családjára és a barátaira is.

**Nem szándékos közzététel:** Az önmagáról megosztott információk felfedhetik élettörténetének nagy részét, és így választ adhatnak a titkos biztonsági kérdésekre.

Az adatvédelem sokkal több, mint pusztán a közösségi média fiókok adatvédelmi beállításainak megadása. Minél több információt oszt meg, és minél többen osztanak meg információt Önről, annál több információt gyűjtenek és használnak fel a vállalatok, kormányok és más szereplők. Az egyik legjobb módja annak, hogy megvédje magát az, ha átgondolja és korlátozza azt, amit megoszt magáról, és amit mások osztanak meg Önről, függetlenül az Ön által használt adatvédelmi beállításoktól.

## 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

***Cathy Click*** *több mint 14 éves tapasztalattal rendelkezik egy Fortune 500-as globális vállalat biztonsági tudatossági programjának fejlesztésében. Cathy szeret bonyolult technikai témákkal foglalkozni, és azokat könnyen érthető formában tolmácsolni, amivel segíthet az embereknek saját online biztonságuk erősítésében.*

## Források

Digitális öröklés: http://www.sans.org/u/Z2G

Átverés a közösségi médián keresztül: http://www.sans.org/u/Z2L

Rendelkezik biztonsági mentéssel?: http://www.sans.org/u/Z2Q