KIBERBIZTONSÁGI TIPPEK

8. BIZTONSÁGBAN A KÖZÖSSÉGI OLDALAKON

A közösségi oldalak kiváló lehetőséget biztosítanak az ismerőseinkkel való kapcsolattartásra, arra, hogy a velünk kapcsolatos információkat, eseményeket, élményeket barátainkkal, családtagjainkkal megosszuk. Segítségükkel a kommunikáció könnyebbé vált, a megosztott személyes információk mennyisége ugrásszerűen megnőtt. A közösségi oldalak az előnyök mellett ugyanakkor kockázatot is jelentenek a felhasználóknak.

SZEMÉLYES ADATOK MEGOSZTÁSA

- A közösségi oldalak lehetőséget biztosítanak a **SZEMÉLYES ADATAINK** megadására, amelyek nem megfelelő biztonsági beállítások esetén mások, akár idegen részére is **LÁTHATÓAK** lesznek.
- Mindig mérlegelje, hogy milyen személyes adatot ad meg, és azt is, hogy azt ki láthatja!
- A személyes adatok, mint a születési hely, idő vagy lakcím, családi kapcsolatok visszaélésre adnak lehetőséget, így ezeket láthatóságát érdemes **KORLÁTOZNI**.

AMIT BIZTOS NE OSSZON MEG!

- teljes születési dátum,
- aktuális helyzet, különösen nyaralás vagy hosszabb távollét esetén,
- lakcím, telefonszám
- családi állapot és családi kapcsolatok,
- képek a gyermekekről, különösen névvel megjelölve,
- képek földrajzi hely információval,
- utazási tervei,
- olyan információk, amiket nem osztana meg családjával, munkatársaival vagy a szomszédjaival,
- munkájával kapcsolatos aktualitások.

BEJEGYZÉSEK MEGOSZTÁSA

- Egy bejegyzés, fénykép, szintén tartalmazhat olyan információt, ami **VISSZAÉLÉSHEZ VAGY ZAKLATÁSHOZ** vezethet. Gondolja végig, hogy tényleg **SZÜKSÉGES-E** a bejegyzést, fényképet megosztani, illetve, hogy azt **KIVEL OSZTJA MEG**!
- Több közösségi oldalon lehetőség van arra, hogy a bejegyzést csak az **ISMERŐSEI EGY RÉSZÉVEL** (pl. közeli családtagok) ossza meg.
- A feltöltött információ, fénykép interneten történő terjedését nem tudjuk kontrollálni, így az **ELJUTHAT IDEGENEKHEZ** is.

INTERNET ONLINE ÉS BIZTONSÁGBAN TUDATOSAN

KIBERBIZTONSÁGI TIPPEK

FELHASZNÁLÓI FIÓKOK BIZTONSÁGA

A felhasználói fiókok (pl. közösségi oldalak, levelezési fiókok) védelme az ott tárolt **ADATOK, INFORMÁCIÓK,** fényképek videók miatt különösen fontos. Ha illetéktelen személy lép be a felhasználói fiókba, az ott tárolt információkat ugyanúgy **LÁTHATJA**, még akkor is, ha azokat a profil tulajdonosa nem osztotta meg. A megszerzett információkkal **VISSZAÉLHETNEK**, nagy nyilvánosság részére **KÖZZÉ TEHETIK** vagy akár **ZSAROLHATJÁK** is vele az áldozatot.

Az illetéktelen hozzáférés megelőzése érdekében válasszon **MEGFELELŐ JELSZÓT**, amely nem kapcsolódik a személyéhez. A különböző oldalak többféle lehetőséget biztosítanak a felhasználói fiókok védelmére. Ismerje meg ezeket, válassza ki az Önnek megfelelőt!

A nem kizárólagosan használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig **JELENTKEZZEN KI** a felhasználói fiókból, a böngésző bezárása nem elegendő, mivel az oldal újbóli megnyitása esetén belép az utoljára használt felhasználói fiókba. Az ilyen számítógépeken a felhasználói nevét és jelszavát soha ne jegyeztesse meg a böngészővel!

BIZTONSÁGI TANÁCSOK

- **NE LEGYEN NYILVÁNOS** a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- **CSOPORTOSÍTSA** ismerőseit és ezáltal korlátozhatja, hogy ki mit láthat!
- Állítsa be, hogy a **JÓVÁHAGYÁSA** után jelölhessék meg egy posztban!
- Korlátozza az **IDŐVONALA LÁTHATÓSÁGÁT**, és azt is, hogy ki tehet tartalmat közzé rajta!
- Ismerősei körét **IDEGENEK** ne láthassák!
- Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során ellenőrizze, hogy az oldal vagy alkalmazás milyen személyes adatához **FÉR HOZZÁ**. (születésnap, e-mail cím, ismerőseinek köre, stb.)!
- Szükség esetén **MÓDOSÍTHATJA** az elérhető információk körét. A hozzáférést az adatvédelmi beállításokban ellenőrizheti, visszavonhatja vagy módosíthatja!

ZAKLATÁS

Az egyszerű kommunikációnak köszönhetően a közösségi oldalak színterei lehetnek az online zaklatásnak. A zaklatás megvalósulhat **BÁNTÓ, FENYEGETŐ, GÚNYOLÓDÓ** személyes üzenetek vagy egy csoportban írt hozzászólások formájában. Az ilyen bejegyzéseket **JELENTENI** lehet az oldal üzemeltetőjének. Javasoljuk, hogy készítsen róluk **KÉPERNYŐMENTÉST, SZAKÍTSA MEG A KAPCSOLATOT** a zaklatóval, tiltsa le, hogy ne léphessen kapcsolatba Önnel! Ha folytatja (más felhasználói fiókkal vagy más csatornán), forduljon a **RENDŐRSÉGHEZ**!

INTERNET ONLINE ÉS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság

KIBERBIZTONSÁGI TIPPEK

CSALÁSOK

A közösségi oldalak lehetővé teszik, hogy **IDEGENEK** is kapcsolatban lépjenek velünk. A rólunk közzétett információk alapján könnyen **CSALÓK CÉLTÁBLÁJÁVÁ** válhatunk. Tipikus elkövetési forma, hogy nagyon kedvező **ÜZLETI LEHETŐSÉGET** kínálnak, minimális befektetéssel lehet szert tenni jelentős haszonra, vagy külföldi, jól fizető munkát ajánlanak némi közvetítői díjért cserébe. Óvakodjon az ilyen ajánlatoktól, mert ezek jellemzően csalóktól érkeznek!

A csalások másik formája az **ONLINE NYEREMÉNYJÁTÉKKAL** kapcsolatos. A csalók azzal keresik meg a kiszemelt áldozatot, hogy valamilyen nyereményjátékon nyert, de a nyeremény véglegesítéshez szükség van arra, hogy feltöltse egy **TELEFONKÁRTYA EGYENLEGÉT** vagy egy **ÜZENETET KÜLDJÖN** el egy telefonszámra (ez szintén egyenleget tölt fel a saját számlánk terhére). Ne dőljön be az ilyen ajánlatoknak!

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE ÉS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság