

Hogyan legyünk biztonságban a közösségi oldalakon?

Az ESET szakembereinek tanácsai a közösségi felületek biztonságos használatához

Az internetes jelenlétünk rengeteget változott az elmúlt években. Korábban az online böngészés a keresőmotorok használatát, konkrét tartalmak keresését vagy a kedvenc új weboldalaink olvasását jelentette. Ma már a közösségi média, az online videók és az azonnali üzenetküldés képezik az internetes felhasználói élmény alapjait, és ez a fiatalabb generációra különösen igaz. Azonban a barátokkal és az ismerősökkel való kapcsolattartás kényelmének ára van. Új kockázatok jelentek meg, és bár a közösségi felületek is igyekeznek megvédeni tagjaikat, mégis gyakran a felhasználók gondatlansága vezet a profilok veszélyeztetéséhez.

Az ESET szakembereinek összeállításából kiderül, hogyan védhetjük meg személyes adatainkat és profiljainkat a közösségi felületeken.

1. Frissítsük rendszeresen szoftvereinket és ügyeljünk eszközeink biztonságára

Rendszeresen frissítsük az operációs rendszerünket és egyéb szoftvereinket (különösen a böngészőket), valamint az okos eszközeinken található applikációkat. Emellett a támadások elkerülésének érdekében használjunk megbízható és naprakész biztonsági megoldást a számítógépünkön, vagy mobileszközünkön.

2. Használjunk erős jelszavakat

Ezt az alapvető szabályt nem pusztán a közösségi média, hanem minden online felület esetében érdemes betartani. Alkossunk hosszú jelszavakat, amelyek kis- és nagybetűket, speciális karaktereket, számokat is tartalmaznak, és ne használjuk több helyen őket, valamint, ha ez túl bonyolult, választhatunk jelszókezelő programot vagy jelmondatokat is.

3. Ellenőrizzük az adatvédelmi beállításainkat

Egy új profil létrehozása során az a legfontosabb, hogy elvégezzük a személyes adatainkkal kapcsolatos beállításokat. Ellenőrizzük, hogy posztjainkat tényleg csak a barátaink látják, illetve azok a csoportok, akiknek ezeket szántuk. Ha részletes adatokat adunk meg a profilunkban, akkor ne engedjük, hogy idegenek láthassák ezeket, így az online bűnözők sem tudják felhasználni adatainkat a jelszavaink kitalálásához, vagy ami még rosszabb: személyazonosságunk ellopásához. Ellenőrizzük rendszeresen a beállításokat, mivel a szolgáltatók hajlamosak időnként megváltoztatni ezeket.

4. Gondoljuk át kétszer is, hogy mit posztolunk

Ha rossz emberekben bízunk meg, akkor annak ellenére is kikerülhet az internetre egy képernyőfelvétel a profilunkról, hozzászólásunkról vagy valamelyik üzenetváltásunkról, ha adatainkat bizalmasan kezeljük és figyelünk a helyes beállításokra. Ezért mindig kétszer gondoljuk át, hogy mit,

kinek és hogyan posztolunk a közösségi felületeken, legyen szó egy véleményről, üzenetről, képről, vagy videóról, mert ami egyszer kikerült az internetre, azt már nem tudjuk később visszavonni.

5. Legyünk kétkedők

Általános szabály, hogy ami túl jó, hogy igaz legyen, az általában átverés. Ezért, ha valaki új autót, számítógépet, vagy okos telefont ajánl valamilyen személyes információért cserébe (születési hely, idő, személyi igazolvány száma stb.), az szinte biztosan csapda. Ezeket az adatokat ne adjuk ki, illetve mielőtt rábízunk személyes információinkat valakire, győződjünk meg az ajánlat vagy a személy hitelességéről.

6. Kerüljük az idegeneket

Egy csinos hölgy, vagy úr üzenetet küldött nekünk valamelyik közösségi felületen? Ha nem ismerjük az illetőt, nem találkoztunk vele még személyesen, akkor legyünk nagyon óvatosak. A kibertérben sok a rejtőzködő, illetve a hamis személyazonossággal rendelkező egyén, akik az álcákat az áldozatok manipulálására használják fel, és olyan dolgokra veszik rá a felhasználókat, amelyeket alapesetben nem tennének meg. Ha biztonságban szeretnénk lenni, akkor csak olyan embereknek engedélyezzük, hogy kapcsolatba léphessenek velünk, akiket személyesen is ismerünk.

**

Az ESET-ről:

A több mint 25 éves, díjnyertes NOD3228 technológiát kifejlesztő ESET a proaktív védelem úttörője, az üzleti és otthoni biztonságtechnikai szoftvermegoldások nemzetközi szállítója. A vállalat piacvezető a fenyegetések észlelésében és megelőzésében. Az 1987-ben megjelent ESET NOD32 Antivirus világszerte az elnyert Virus Bulletin "VB100" díjak számát tekintve, illetve a vizsgálatok 1998-as fennállása óta eddig minden szabadon terjedő vírust vagy férget észlelt és kivédett. Az ESET NOD32 Antivirus, ESET Smart Security és az ESET Cyber Security (biztonsági megoldás Mac-re), valamint a mobiltelefonok és táblagépek védelmét biztosító ESET Mobile Security a legajánlottabb biztonsági megoldások közé tartoznak, a termékekben milliók bíznak meg világszerte. A vállalat központja Szlovákiában, Pozsonyban található, regionális terjesztési központokkal rendelkezik San Diegóban (USA), Buenos Airesben (Argentína) és Szingapúrban, valamint irodái vannak São Paulóban (Brazília) és Prágában (Csehország). Az ESET több mint 180 országban, köztük Magyarországon, rendelkezik kiterjedt partneri hálózattal. További információ: www.eset.hu

A Sicontactról:

A Sicontact Kft. az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor. Mottója és küldetése, ami köré termékportfólióját kialakította: „biztonság a digitális világban”. A Sicontact Kft. Magyarországon az ESET NOD32 technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő. A cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact kizárólagos magyarországi disztribútora a Unified Threat Management (UTM) hálózatbiztonsági eszközök terén piacvezető Cyberoam termékeinek, valamint portfóliójában megtalálható a helyi és távoli rendszerdiagnosztika, a hálózatfigyelés, a távvezérlés és a licenccsere terén kiemelkedő képességekkel rendelkező AIDA64 szoftver is.

A Sicontact Kft. több ízben elnyerte a kitüntetett Business Superbrands díjat. Az ESET Smart Security programcsomagot többször is az év antivírus megoldásának választották. A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban kínálja. Az ESET biztonsági szoftverek licencelése során a gyorsan változó körülményeket is figyelembe veszi, így például az ESET szoftverek a licencidőszak alatt bármikor újratelepíthetők az adott számítógépre, továbbá az unilicenc konstrukció keretében a munkaállomásokon a megvásárolt ESET licenccel egyaránt használhatók a Windows, Linux és Mac operációs rendszerre fejlesztett ESET termékek, így az operációs rendszer cseréje esetén nem szükséges új licenct vásárolni. A Sicontact Kft. az ESET szoftverekhez és a Cyberoam termékeihez díjmentes terméktámogatást és távsegítséget biztosít, mind az otthoni, mind a vállalati felhasználók számára, így az ügyfelek jelentős időt és pénzt takarítanak meg.

Sicontact Kft. 1023 Budapest Sajka u. 4. tel: 1/346 7040 fax: 1/346 7050 www.sicontact.hu