Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Közösségi oldalak

Áttekintés

A Facebook, a Twitter, az Instagram, a LinkedIn és hasonló közösségi oldalak nagyszerű lehetőséget biztosítanak ahhoz, hogy a világ bármely pontján élőkkel ismerkedjünk meg, tartsunk kapcsolatot vagy akár különböző dolgokat osszunk meg velük. Azonban a lehetőségek kockázatokat is hordoznak magukban, amelyek nem csak ránk, hanem a családunkra, barátainkra vagy akár a munkatársainkra is leselkedhetnek. Az OUCH! e havi kiadásában bemutatjuk ezeket a kockázatokat, illetve azt is, hogyan használhatjuk a közösségi oldalakat biztonságosan.

A szerzőről

Tanya Beccam rutinos biztonsági szakértőnek számít, aki több mint egy évtizede számos SANS kurzus szerzője és oktatója. A Twitter-en **@tbaccam** néven található meg a csatornája.

Adatvédelem

A közösségi oldalakkal kapcsolatos általános aggodalom a személyes adatok védelme. A lehetséges veszélyek az alábbiak:

- **Hatással lehet a jövőre**: egyes szervezetek, cégek a háttérellenőrzések során megnézik a közösségi oldalakat is. A kínos vagy kellemetlen fotók, hozzászólások – nem számít milyen régiek – megakadályozhatnak egy előléptetést vagy álláspályázatot. Gyakran az adatvédelmi beállítások sem segítenek ilyen helyzetben, mert a szervezetek kérhetik azt, hogy a jelentkező „like”-olja az oldalukat, így hozzáférhetnek a korábbi posztokhoz, de előfordulhat, hogy sok hozzászólást egyéb oldalakon archiváltak.
- **Ellenünk irányuló támadások**: a kiberbűnözők képesek felhasználni a hozzászólásainkat azzal a céllal, hogy rólunk vagy a munkahelyünkről információkat szerezzenek. Például az általunk megosztott információkból megpróbálhatják kitalálni a „titkos kérdés”-re adandó válaszunkat, így vissza tudják állítani a jelszavunkat, célzott támadást indíthatnak ellenünk email-eken keresztül, vagy felvehetik valakivel a kapcsolatot a munkahelyünkön, azt tettetve, hogy mi vagyunk a vonal másik végén. Továbbá, az is előfordulhat, hogy a támadást kiterjesztik a valódi életünkre, behatárolva, hogy hol lakunk vagy dolgozunk.
- **Véletlenül veszélybe sodorjuk a munkaadónkat**: a bűnözők vagy a versenytársak felhasználhatják az általunk nyilvánosságra hozott információkat a munkahelyünk vagy a kollégáink ellen. Arról nem is beszélve, hogy a hozzászólásaink rossz fényt vethetnek a munkahelyünkre. Mindig ellenőrizzük a munkahelyünk ide vonatkozó előírásait, mielőtt bármit is leírunk, és számoljunk azzal a lehetőséggel, hogy maga a munkahely monitorozza a közösségi oldalakon végzett tevékenységünket.

A legjobb védekezés az, hogy saját magunk határoljuk be magunknak, hogy mit osztunk meg a közösségi oldalakon. Igen, az adatvédelmi beállítások segíthetnek valamelyest, de többször lehetnek megtévesztőek, és gyakran a tudtunk nélkül is

Közösségi oldalak

változhatnak. Amiről azt gondoljuk, hogy csak a szűk körű címzettek fogják látni, gyorsan nyilvánossá válhat számtalan ok miatt. Azt se felejtsük el, hogy a posztjainkat akár a címzettek maguk is továbbíthatják. Minél több emberrel osztunk meg információkat, annál valószínűbb, hogy nyilvánosságra kerül. Azt kell feltételeznünk, hogy bármit is osztunk meg, az előbb vagy utóbb nyilvános lesz, és örökre az Internet része marad.

Végül pedig legyünk tisztában azzal, hogy a barátaink miket posztolnak rólunk. Ha valami olyat töltenek fel egy közösségi oldalra, ami kényelmetlenül érint bennünket, akkor kérjük meg őket, hogy távolítsák el azt. Amennyiben figyelmen kívül hagyják a kérésünket, vagy nem vesznek rólunk tudomást, akkor keressük meg a közösségi oldal üzemeltetőjét, és őket kérjük meg a tartalom törlésére. Ezzel egy időben pedig tartsunk tiszteletben másokat saját posztjainkban.

A közösségi oldalak nagyon szórakoztatóak és sokoldalúak, de kétszer is gondoljuk meg, hogy kivel és mit osztunk meg!

Biztonság

Az adatvédelmi aggályok miatt az alábbi lépéseket érdemes betartani a közösségi oldalakon lévő felhasználói fiókunkkal és más internetes tevékenységünkkel kapcsolatban.

- **Bejelentkezés**: minden fiókunkhoz egyedi, erős jelszót használjunk, és azt ne adjuk meg senkinek! Ezen kívül a legtöbb közösségi oldal támogatja az olyan erős hitelesítési megoldásokat, mint a két lépcsős hitelesítés. Használjuk ezeket a lehetőségeket, ha van rá mód! Végezetül pedig soha ne használjuk a közösségi oldalon használt fiókunkat arra, hogy más oldalakra jelentkezzünk be vele, mert ha azt feltörik, akkor az összes fiókunk veszélybe kerül.
- **Adatvédelmi beállítások**: ha használunk adatvédelmi beállításokat, akkor rendszeresen nézzük át, és teszteljük is azokat! A közösségi oldalak gyakran változtatják a szabályaikat, és így könnyű hibát véteni. Ezen kívül számos olyan alkalmazás és szolgáltatás van, amely megjelöli azt, hogy éppen hol tartózkodunk, amikor posztolunk valamit (geotagging). Rendszeresen ellenőrizzük ezeket a beállításokat, ha nem akarjuk nyilvánosságra hozni, hogy hol tartózkodunk éppen.
- **Titkosítás**: a közösségi oldalak HTTPS kapcsolatot használnak annak érdekében, hogy biztonságosan tudjunk kapcsolódni. Vannak olyan oldalak, amelyek alapértelmezetten ezt használják, másoknál pedig nekünk magunknak kell gondoskodni erről. Ellenőrizzük ezt a fiókunk beállításainál, és állítsuk be alapértelmezettnek a HTTPS használatát!
- **Email**: mindig legyünk gyanakvóak az olyan levelekkel szemben, amelyek azt állítják, hogy a közösségi oldaltól érkeztek, mivel könnyen lehet, hogy ezeket kiberbűnözők hamisítják. Az ilyen üzenetekre mindig úgy válaszoljunk, hogy közvetlenül lépünk be a közösségi oldalra (pl. könyvjelző használatával), nem pedig a levélben kapott hivatkozásra kattintva, és ott olvassuk el, és válaszoljuk meg a kapott üzeneteket!
- **Káros tartalmú hivatkozások/átverések**: legyünk óvatosak a közösségi oldalakra posztolt gyanús hivatkozásokkal és potenciális átverésekkel szemben! A bűnözők is használják ezeket az oldalakat, mégpedig azért,

Közösségi oldalak

hogy az általuk kitervelt csalásokat széles körben tudják terjeszteni. Csak mert egy üzenet egy ismerősünktől érkezik, még nem biztos, hogy ő is küldte el, mert lehet, hogy csak feltörték a fiókját. Például ha egy rokonunk vagy barátunk furcsa üzenetet küld, amelyet nem tudunk ellenőrizni, miszerint kirabolták, és sürgősen pénzre van szüksége, akkor inkább vegyük fel vele a kapcsolatot a közösségi oldaltól független csatornán (pl. mobiltelefon), és győződjünk meg arról, hogy valóban ő küldte az üzenetet.

- **Mobilos alkalmazások**: a legtöbb közösségi oldal biztosít valamilyen okostelefonra készült alkalmazást, amely segítségével hozzá tudunk férni az online fiókunkhoz. Az ilyen alkalmazásokat csak megbízható forrásból töltsük le, és a készüléket is erős jelszóval védjük! Ha elveszítenénk a telefonunkat, miközben az nincs zárolva, akkor bárki tud a nevünkben posztolni a közösség oldalunkra.

A közösségi oldalak segítségével bármikor kapcsolatba tudunk lépni az ismerőseinkkel. Ha követjük a fenti tanácsokat, akkor biztonságban érezhetjük magunkat. Ha többet is akarunk tudni a közösségi oldalunk biztonságáról, vagy jelenteni akarunk valamilyen nem engedélyezett tevékenységet, akkor látogassuk meg az oldal biztonsággal foglalkozó részét!

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

A jelmondatokról:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
Kétfaktoros hitelesítés:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_hu.pdf
Mobil alkalmazások biztonságos használata:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_hu.pdf
Az internetes biztonsági oktatása gyermekeknek:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_hu.pdf
Facebook biztonság:	http://biztonsagosinternet.hu/tippek/adatbiztonsag-kozossegi-oldalakon

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