Havi biztonságtudatossági hírlevél számítógép-felhasználók számára

OUCH!

Ebben a kiadványban...

- **Áttekintés**
- **Adatvédelem**
- **Biztonság**

Közösségi oldalak biztonságosan

VENDÉG SZERKESZTŐ

Mostani kiadásunk vendég szerkesztője Ted Demopoulos, aki régóta dolgozik biztonsági tanácsadóként, és egy évtizede oktat SEC401/501 vagy MGT414/512 SANS tanfolyamokon. További információ Ted-ről a http://demop.com weboldalon olvasható.

ÁTTEKINTÉS

Az olyan közösségi oldalak, mint a Facebook, a Twitter, a Google+, a Pinterest és a LinkedIn nagyon népszerűek és lehetővé teszik számodra, hogy emberekkel ismerkedj meg, kommunikálj és információkat ossz meg velük. Azonban mindezen lehetőségek mellett kockázatokat is hordoznak; nem csak rád, de a családodra, a barátaidra és a munkáltatódra nézve is. Hírlevelünkben áttekintjük, melyek ezek a veszélyek, és hogy hogyan lehet használni ezeket az oldalakat nagyobb biztonsággal.

ADATVÉDELEM

Általános probléma a közösségi oldalakkal kapcsolatban az adatvédelem, azaz a személyes adataid és mások bizalmas információinak védelme. A lehetséges veszélyek a következők:

- **Befolyásolja a jövődet:** Számos munkahely használja a közösségi oldalakat háttér információk begyűjtésére. A kínos vagy terhelő megjegyzések, függetlenül attól, hogy azok milyen régiek, megakadályozhatják, hogy egy pozícióra felvegyenek vagy előléptessenek. Továbbá Amerikában, számos egyetem is végez hasonló ellenőrzéseket a náluk tanulni szándékozókkal kapcsolatban. Az adatvédelmi beállítások nem feltétlenül segítenek, mivel például az amerikai munkahelyek kérhetik, hogy „Like”-oljuk vagy csatlakozzunk az ő oldalukhoz a jelentkezési folyamat előtt.

- **Ellened irányuló támadás:** A kiberbűnözők begyűjtik a személyes adatainkat amelyeket ellened irányuló támadásokhoz használnak fel. Például felhasználhatják személyes adataidat ahhoz, hogy a „emlékeztető kérdés”-eidre kitalálják a választ és így átállítsák online jelszavad, célzott adathalász - más néven „spearphishing” támadásokat vagy nevedet felhasználva hitelkártyacsalásokat hajtsanak végre. Továbbá ezek a támadások a fizikai világban is megjelenhetnek, például kideríthetik, hogy hol dolgozol vagy azt, hogy hol élsz.

- **Kárt okozhatsz a munkáltatódnak:** A bűnözők vagy a versenytársak bármilyen a munkahelyedről közzétett bizalmas információt felhasználhatnak a munkáltatód ellen. Továbbá a meggondolatlan bejegyzéseiddel te magad is ronthatod munkáltatód hírnevét. Ügyelj arra, hogy ellenőrizd a munkahelyed szabályzatát, mielőtt bármit közzéteszel a munkáltatóddal kapcsolatban.

Közösségi oldalak biztonságosan

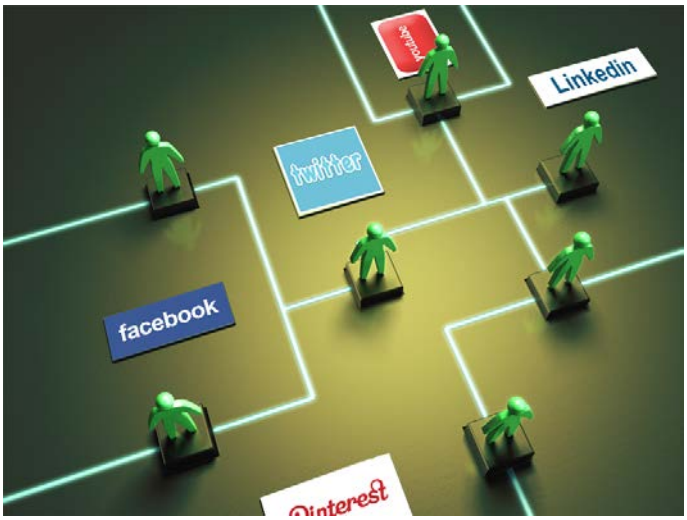
A legjobb védelem, ha korlátozod a közzétett információkat. Igen, az adatvédelmi beállítások némi védelmet biztosítanak, azonban ne feledd, hogy az adatvédelmi beállítások gyakran zavarosak, és megváltozhatnak a tudtod nélkül. Amiről azt gondoltad, hogy magánjellegű, egyszer csak nyilvánossá válhat különböző okok miatt. Továbbá, az adataid védelme csak annyira biztonságos, mint azok az emberek, akikkel megosztottad ezeket. Minél több ismerőssel osztunk meg személyes információt, annál valószínűbb, hogy ezek nyilvánosságra kerülnek. Továbbá, az adataink bizalmasságának megőrzése nagyban függ attól, kikkel osztjuk meg azokat. Végső soron a következő szabály betartása a legjobb módszer a magánjellegű adatok megvédésére: „ha nem szeretnéd, hogy a szüleid vagy a főnököd lássa megjegyzéseidet, akkor ne tedd közzé azokat”.

Ezen felül meg kell győződni arról is, hogy az ismerőseid milyen információkat tesznek közzé rólad. Káros lehet, ha az ismerőseid tesznek közzé rólad bizalmas információkat vagy kínos fotókat. Győződj meg arról, hogy az ismerőseid tisztában vannak vele, milyen információkat oszthatnak meg rólad és milyeneket nem. Ha neked nem tetsző információkat osztanak meg, kérd meg őket, hogy távolítsák el azokat. Ugyanakkor neked is tekintettel kell lenned másokra.

BIZTONSÁG

Az adatvédelmi aggályok mellett, a közösségi oldalakat a kiberbűnözők felhasználhatják ellened vagy eszközeid ellen irányuló támadásokhoz. Néhány lépés, amivel megvédheted magad:

- **Bejelentkezés:** A közösségi oldalhoz tartozó felhasználói fiókodat védd erős jelszóval és azt senkinek ne add meg, valamint ne használd fel más oldalakhoz ugyanazt a jelszót. Továbbá, bizonyos közösségi oldalak erősebb hitelesítési mechanizmust is támogatnak, mint például a 2 lépcsős hitelesítés. Ha lehetséges, mindig engedélyezd az erősebb hitelesítési mechanizmust.



A közösségi oldalak népszerűek és szórakoztatóak, de légy óvatos, hogy mit teszel közzé és kiben bízol meg.

- **Titkosítás:** Több közösségi oldal lehetővé teszi azt, hogy titkosítást használj - más néven HTTPS - az oldalhoz történő biztonságos kapcsolódás érdekében. Több oldal, mint a Twitter és a Google+ alapértelmezetten ezt használják, míg más oldalak esetében neked kell engedélyezned a HTTPS használatát a felhasználói fiók beállításainál. Ha lehetséges, használj HTTPS-t.
- **Email**: Légy gyanakvó azokkal a levelekkel szemben, amelyek látszólag egy közösségi oldalról jönnek. Ezek gyakran egy hamisításos támadás részeként érkeznek a kiberbűnözőktől. A legbiztonságosabb módja az ilyen levelek megválaszolására, ha bejelentkezünk az adott közösségi oldalra, és ott megvizsgáljuk az üzeneteinket, értesítéseket.
- **Rosszindulatú linkek/csalások**: Legyünk óvatosak a közösségi oldalakon közzétett gyanús hivatkozásokkal és potenciális csalásokkal. A kiberbűnözők közzétehetnek rosszindulatú hivatkozásokat, és ha

Közösségi oldalak biztonságosan

ráklikkelsz, olyan weboldalakra kerülhetsz, amelyek megpróbálják megfertőzni a számítógépedet. Továbbá attól, hogy egy bejegyzés látszólag egy ismerősödtől származik, nem biztos, hogy valóban ő készítette, mivel a felhasználói fiókját fel is törhették. Ha egy családtag vagy egy ismerős szokatlan üzenetet tesz közzé, amit nem tudunk ellenőrizni (pl. hogy elrabolták és pénzre van szüksége tőled), hívjuk fel az üzenet megerősítése érdekében.

- **Alkalmazások**: Néhány közösségi oldal lehetővé teszi, hogy harmadik féltől származó alkalmazásokat lehessen telepíteni vagy hozzáadni, például játékokat. Tartsd szem előtt, hogy minimális vagy gyakorlatilag semmilyen minőségi ellenőrzésen nem mennek keresztül ezek az alkalmazások; esetleg teljes hozzáféréssel rendelkezhetnek a felhasználói fiókodhoz és személyes adataidhoz. Csak olyan alkalmazásokat telepíts, amelyekre szükséged van és jól ismersz, megbízható oldalakról származnak, valamint ha már nincs rájuk szükséged távolítsd el.

A közösségi oldalak népszerűek és szórakoztató módon biztosítják a világgal való kommunikációt. Ha követed az itt leírt ajánlásokat, egy sokkal biztonságosabb online élményben lehet részed. További információk a közösségi oldalak biztonságos használatával és a jogosulatlan tevékenységek jelentésével kapcsolatban az adott weboldal biztonsággal kapcsolatos ismertető oldalain találhatóak.

HIVATKOZÁSOK

Az alábbi hivatkozások közül néhány a TinyURL szolgáltatással került rövidítésre, hogy könnyebben olvasható legyen. Az esetleges biztonsági problémák miatt az OUCH! mindig a TinyURL előnézeti funkcióját használja, amely megmutatja a hivatkozás valódi célját, valamint engedélyt kér mielőtt továbblép a weboldalra.

11 Biztonsági Tanács az Online Közösségi Oldalakhoz:
http://preview.tinyurl.com/b28a525

FB Biztonság:
https://www.facebook.com/safety

A te FB biztonsági beállításaid:
https://www.facebook.com/settings?tab=security

Általános Biztonsági Feltételek:
http://preview.tinyurl.com/6wkpae5

SANS Napi Biztonsági Javaslata:
http://preview.tinyurl.com/6s2wrkp

Biztonságos Internet:
http://preview.tinyurl.com/arhv37c

TUDJON MEG TÖBBET

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

A nemzeti/kormányzati CERT szerepet Magyarországon 2005 óta a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ látja el. A PTA CERT-Hungary Központ közhasznú feladatként támogatja a magyar társadalom felkészülését az internet minél tudatosabb és biztonságosabb használatára. További információ a http://www.cert-hungary.hu oldalon olvasható.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy

Fordította: Birkás Bence, Benyó Pál