

Senki sincs biztonságban?



CSIZMAZIA-DARAB ISTVÁN
Az IT-biztonsági szakértő
helyzetértékelése és praktikus
tanácsai adataikra érzékeny
felhasználóknak.

szolgáltatásokban is. Mi a legegyszerűbb védekezési mód?

– Általánosságban szerintem az a fotó, az a dokumentum van a legnagyobb biztonságban, amelyet nem töltenek fel. Sokan nem gondolnak bele abba, mi van, ha elvesztik, ellopják a telefonjukat, vagy csak szervizbe kell vinni, mert elromlik. Nemcsak rengeteg személyes adat, hanem sokaknál kritikus céges információk is vannak az eszközön. Úgy vélem, manapság, mivel a támadók ropant felkészültek és leleményesek, egy okostelefont is ugyanúgy kell védeni, mint egy asztali Windows gépet – ezt a kártevők sokasága is jól reprezentálja. A jelenlegi nyilvántartott mobilos kártevőminták száma 2,5 millió, ez a 2012-es értékekhez képest mintegy hússzoros növekedést jelent. Ráadásul sokan már fizetnek is mobillal, és kihasználják az NFC chipes lehetőséget a közelérintéses pénztárcás fizetésre.

– Mi a legnagyobb kockázat?

– Lehetőleg ne készítsünk magunkról meztelen képet vagy szexvideót. Manapság 60 százalék feletti a válások aránya, de az együtt járás vagy az élettársi kapcsolatok sem tartanak minden esetben a sírig. Sajnos sok helyen a partner is visszaél később az ilyen felvételekkel, és bosszúból feltölti azokat az internetre. Emiatt például Németországban már törvényt hoztak arra, hogy az elvált másik félnek nincs joga ilyen fotókat birtokolni. Persze más kérdés, hogy sikerül-e ezt betartatni.

– Az adott botrány esetében a felhasználók vélhetően nem is tudták, hogy a felhőbe menti a képeket a telefon. Hogyan kellett volna cselekedniük?

– Nyilván ott se tároljunk intim képeket a telefonunkkal, ahol a fájlrendszer és a hálózatos mobilműködés beállításai miatt esetleg nem látjuk át, milyen másolatok vagy automatikus feltöltések keletkezhetnek. Ha nagyon muszáj, akkor egy külső memóriakártyás fényképező-

Az emberi tényező hogyan segíti a bűnözőket?

– Ha ismert emberek, közszereplők vagy éppen felelős beosztásban dolgozó döntéshozók vagyunk, akkor tudomásul kell venni azt is, hogy különösen vonzó célpont lehetünk, éppen ezért fokozott figyelemmel kell megelőznünk a biztonsági incidenseket. Ezt vagy saját magunknak kell megtenni, vagy megfelelő technikai segítséget szükséges kérni/alkalmazni hozzá. Mivel egy-egy híresség meztelen fotója akár több tízezer dollárt is érhet a bulvárlapoknak, ez komoly anyagi motiváció lehet a támadóknak, akiktől erkölcsi gátlást, becsületességet, korrektséget vagy könyörületet sose várunk. Természetesen nemcsak a hírességeknek, hanem mindenkinek érdemes

védekezni. Az elkövetők néha valóban célzottan, de sok esetben automatikusan támadnak minden védtelen, nem frissített eszközt. Például scriptekkel vagy megtévesztéssel (social engineering) azokat a felhasználókat célozzák, akik túlságosan hiszékenyek és nem elég biztonság tudatosak: mondjuk ingyenes nyeremény, előre kért lájk, mobilról bankolás vagy ismeretlen QR (Quick Response) grafikus kód beolvasása révén. Az is előfordul, hogy az ilyen támadásokat teszem azt Google vagy Facebook segítségével reklámozzák, és például ingyenes vírusirtók vagy népszerű programok, filmek ingyenes letöltésének ígéretébe csomagolják. Ezekkel legyünk különösen óvatosak.

– Ilyen esetek hallatán a felhasználók hite jogosan rendül meg a felhő-

A SZAKÉRTŐ TANÁCSAI

1. Ne töltsünk fel a netre bizalmas vagy szexuális tartalmakat, és ne tároljunk ilyeneket a telefonunkon sem!
2. Használjunk erős és mindenhol egyedi jelszót!

3. Ne kattintsunk ész nélkül mindenre!
4. Alaposan válasszuk meg, milyen alkalmazásokat milyen engedélyekkel és honnan telepítünk fel.
5. Használjunk antivírust, internetbiztonsági csomagot okostelefonon is.
6. A felhős tárhelyet is tekintjük egy olyan merevle-

meznek, amely akár el is romolhat, így ne az legyen életünk összes munkájának egyetlen őrzője, hanem csak egy extra lehetőség a lokális mentéseink mellett.

7. A felhős tárhelyet is tekintjük egy olyan merevlemeznek, amely ugyanúgy elveszhet vagy ellophatják, ezért bizalmas tartalmain-

kat – saját munka, személyes mentés, személyes fotók – csak és kizárólag titkosítva tároljuk ott.

8. Ahol rendelkezésre áll a kétlépcsős azonosítás (autentifikáció), például banki tokenes vagy SMS-visszaigazoló megoldások, ott használjuk is ki és éljük a lehetőségével.●

géppel vagy kamerával tegyük ezt, ahol sem az internetes csatlakozási lehetőség, sem pedig a véletlen megosztás nem zavarhat be. Emellett pedig a memóriakártyát később akár fizikailag is könnyen megsemmisíthetjük, vagy megfelelő segédprogrammal többszörösen felülírva a tartalmát biztonságosan és visszaálíthatatlanul letörölhetjük.

És lehetőleg ne töltsünk fel magunkról meztelen képet vagy szexvideót az internetre, mert nem lehetünk biztosak benne, hogy valójában nem örök időkre őrzik meg ezeket. Hiszen a világháló nem felejt, amit egyszer feltöltünk, az jó eséllyel ott is marad, és később esetleg megbánhatjuk, vagy akár állásle-

hetőségektől is eleshetünk miatta. Sok esetben bebizonyosodott már – például a Facebook vagy a Snapchat esetében –, hogy a töröltnek gondolt felvételek igazából fizikailag sosem tűnnek el teljesen.

– De ha már felkerültek a netre a képek, akkor utólag törölhetőek is, nemde?

– Hogy az utólagos törlés nem működik, sőt épp ellenkező hatást vált ki, erre a legjobb példa, amikor 2003-ban a Kelet–Nyugat Kosárlabdagalán Király Linda csúfosan belesült a Himnusz énekésébe, mert nem tudta a szövegét. Az ezt megörökítő kínos felvételt – amely bejárta a videomegosztó oldalakat – Linda

apja olyan módon próbálta meg 2014-ben eltüntetni az internetről, hogy megvásárolta és levédette a szerzői jogát nem kevés pénzért, majd ügyvédei útján perrel fenyegette meg a videomegosztó oldalakat, hogy azonnal távolítsák el az anyagot. Ezt a YouTube meg is tette, azonban ezzel mégis pont ellentétes hatást ért el, mert a felfokozott érdeklődés miatt sokan ismét kíváncsiak lettek rá, és néhányan a felvételt többek közt olyan egzotikus jogrendszerű országok videomegosztóira töltötték fel, mint Malajzia vagy Vietnam, ahol az Európában, illetve Amerikában ismert és alkalmazott szerzői jog már nem jelent semmit.

Az összeállítást készítette: Halaska Gábor

HIRDETÉS

ÜZLET, GAZDASÁG, TÁRSADALOM
FIGYELŐ

onlinemarketing.hu



FIGYELŐ ÜZLETFEJLESZTÉSI WORKSHOP 1.0

A FIGYELŐ három délutáni alkalommal igazi műhelybeszélgetésekkel egybekötött, üzletfejlesztési tippel tarkított workshopot tart. A témák elismert szakértői mellett neves előadók mesélik el, milyen utat jártak be, amíg vállalkozásukkal sikeresek lettek és jelentős eredményeket értek el. És persze példákkal tanítanak is!

IDŐPONTOK:

2014. szeptember 18., 25. és október 2. 14.00-18.00 óra

HELYSZÍN:

VENDEL KONFERENCIAKÖZPONT

A KONFERENCIA TÉMÁJA: AZ ÜZLET MOTORJAI

1. AZ ÖNINDÍTÓ

- ▶ Melyik piacon ténykedünk: B2B vagy B2C?
- ▶ SWOT és a célok összefüggése
- ▶ Célozzak vagy mindenki az ügyfelem?
- ▶ Mit keres a ROLEX óra a trafikban?
- ▶ Legyen márkánk, vagy csak adjuk el a termékünket?
- ▶ Termék/szolgáltatás portfólió kialakítása
- ▶ Miniben árképzés és értékesítési csatornák gyakorlatban

2. A KAROSSZÉRIA

- ▶ Arculat – hogyan alakuljon ki és frissítsük időről időre?
- ▶ Mit jelentenek a színek azon a piacon, ahol a cég dolgozik?
- ▶ Milyen a hatékony brosúra?
- ▶ Nyomda: költséghatékony megoldás?
- ▶ Hol és hogyan hirdessünk, mitől lesz költséghatékony egy hirdetés?

3. AZ ELEKTRONIKA

- ▶ Ami a dróton jön, az mára elsősorban az internet.
- ▶ Mit tegyünk, hogy jól működjön?
- ▶ Milyen kampányunk, weboldalunk lesz sikeres?
- ▶ Mit jelentenek az adatok?

ELŐADÓINK: Szabó Julianna, Berényi Konrád, Lambert Gábor, Schobert Norbert, Szalay Angelika, Lonkai Márton, Ómolnár Miklós (további előadók egyeztetés alatt)

Teljes árú díj: 99 900 Ft + áfa • Early Bird kedvezmény 2014. szeptember 15-ig történő jelentkezésre: 49 900 Ft + áfa

BEJELENTKEZÉS: www.figyelo.hu/konferenciak vagy konferenciak@figyelo.hu