17. tétel

Az internet veszélyforrásai 1.

Mutassa be az internet leggyakoribb veszélyforrásait: a kéretlen reklámlevelet, a hoax-ot, és az adathalászatot, valamint az ellenük való védekezést! Térjen ki a webáruházas csalásokra is!

Nagyjából az internet tömeges elterjedésétől (1990-es évek) lehet számítani a kiberbűnözés megjelenését is. Nézzük a legfőbb formáit!

Az 1990-es évektől, az internet tömeges elterjedésétől lehet számítani a kiberbűnözés megjelenését is. Legfőbb formái:

1. Kéretlen levelek
A termékek reklámozására ideális az internet, mert olcsó, és nagyon sok felhasználót lehet egyszerre megszólítani. A reklámozás egyik módja, hogy a cég kéretlen leveleket küld a felhasználóknak, melyben termékeit kínálja megvételre. A felhasználók az e-mail-címük megadásával (pl. a felhasználási feltételek elfogadásával) lehetőséget adnak a reklámtartalmú levelek fogadására. Erről a levelekről le lehet iratkozni, de olvasás nélkül is törölhetők vagy fenntartható számukra egy ingyenes, másra nem használt e-mail-cím is.

✓ 1 PONT

2. Nigériai levelek (internetes csalás)
A nigériai levél, más néven a „419-es átverés" az egyik leggyakoribb átveréses bűncselekmény. Nevét a nigériai Büntető Törvénykönyv vonatkozó paragrafusáról kapta. Kezdetben hagyományos postai úton, illetve faxon terjedt, de az internet elterjedésével az e-mail lett a leggyakoribb közege. Forrás: USA, Egyesült Királyság, Nigéria, Dél-afrikai Köztársaság, Elefántcsontpart, Benin, Togo, Oroszország, Pakisztán, India, Hollandia és Spanyolország.

Megjegyzés: Nem kell ilyen részletesen felsorolni.

✓ 1 PONT

A nigériai levelek az 1980-as években alakultak ki. A csalás elkövetési módja általában egy e-mail, melyet látszólag egy kiválasztott címzettnek küldenek (valójában mások is megkapják), amelyben segítségért cserébe hatalmas összeget ígérnek a címzettnek. Léteznek hivatalosnak látszó profilok is a közösségi oldalakon, hogy hitelesebbnek tűnjenek a körülmények. Az e-mail tárgya gyakran „XY ügyvéd asztaláról", „Az Ön segítségére van szükségem", stb. lehet. Legtöbbször egy kormányzati vagy banki tisztviselő van megadva feladóként, aki sok pénzről vagy aranyról tud, melyhez nem fér hozzá, és a címzettől kér egy kisebb összeget pl. a kiutaláshoz szükséges előlegre. Bár a levelek túlnyomó részére nem érkezik válasz, mégis akadnak olyan emberek, akik a nyilvánvaló beugratás ellenére is küldenek pénzt.

✓ 1 PONT

3. Átverő hírek/hírlevelek (angolul: hoax)

- „Bill Gates (vagy más milliárdos) elosztogatja a vagyonát és aki ezt a levelet továbbküldi, az kap belőle."
- „Egy gyanús számot nem szabad felvenni, mert több ezer eurós mobilszámlát generál."
- „Sürgősen „A" Rh negatív vért keres egy leukémiás kisfiúnak a vérellátó szolgálat."
- „Ezzel a biztos befektetéssel évi 45%-os kamatot realizálhat."

A felsorolt négy üzenetben az a közös, hogy egyik sem igaz. A legtöbb hoax egyszerűen leleplezhető ha figyelmesen végigolvassuk és gondolkodunk. Pl. hazánkban jelenleg évi 45%-os kamat nem reális. Mint ahogy a semmiért több ezer eurós fizetés ígérete sem az, vagy – amire igen sok beteg ember érzékeny – a sajtó által eltitkolt gyógyító csodaszerek sem reálisak. A hihető hoaxot érdemes többszörösen ellenőrizni. A kiemelkedő híreket átveszik a fontosabb hírportálok, így ha azokon nem fordul elő, akkor legyünk kritikusak! Ne tájékozódjunk csak egyetlen forrásból, nézzük meg az ellenkező beállítottságú (hír)oldalt is! **Egyetlen kivétel van** ez alól:

április 1., amikor az olyan komoly hazai és nemzetközi hírportálokon is, mint pl. az angol The Guardian (lap), vagy a Google (kereső) megjelennek a komolytalan, átverős „hírek".

✓ 2 PONT

4. Tárolt adatokhoz való hozzáférés, visszaélés, adathalászat

Az e-mail-cím sokat ér, pl. 5000 valós e-mail-címért a hírlevél-küldők vagy a kéretlen levelek feladói 5-8 $-t is fizethetnek. Ugyancsak értékes pl. egy cég fizetési/juttatási listája egy konkurens cégnek vagy egy fejvadásznak. Az adathalászatot nehéz elkerülni, de tehetünk óvintézkedéseket. **Csak akkor adjuk meg az adatainkat, ha az feltétlenül szükséges!** Érdemes fenntartani egy olyan e-mail-címet is, amit akkor adunk meg, ha az elkerülhetetlen. A személyi igazolvány szám, a TAJ-szám vagy a bankkártya adatai kiemelten fontosak. Csak nagyon indokolt esetben és csak megfelelő biztonsággal rendelkező cégnek adjuk meg! Sajnos az adatbázisok időnként sérülhetnek, és kiszivároghatnak a biztonságban hitt adataink, képeink (ilyenek pl. a celebek nem nyilvánosságnak szánt fotói is). A kiszivárogtatást elvégezheti „jószándékú" ismerősünk, ha kezébe jut az okos telefonunk, vagy egy hacker, aki ismeri a szoftverek biztonsági hibáit.

✓ 1 PONT

Csak akkor adjuk meg az adatainkat, ha az feltétlenül szükséges! Érdemes fenntartani egy „muszáj megadni" típusú e-mail-címet is. Más téma a személyi igazolvány száma, a TAJ-szám vagy a bankkártya adatai. Ezek kiemelten fontosak! Ezekre nagyon kell vigyázni! Csak igen indokolt esetben és csak megfelelő biztonsággal rendelkező cégnek! Sajnos az adatbázisok is időnként sérülnek, így kiszivároghatnak a biztonságban hitt adataink/képeink. Elég pl.: a celebek nem nyilvánosságnak szánt, de kiszivárgott fotói (Brad Pitt, Ariana Grande, Rihanna, Miley Cyrus, Orlando Bloom, Katy Perry,...) Ehhez elég pl. a telefonunkat kiadni a kezünkből egy „jószándékú" ismerősnek vagy elég a hackereknek kihasználni a szoftverek biztonsági hibáit. De sokat érhet pl. a cégünk fizetési/juttatási listája egy konkurens cégnek vagy egy fejvadásznak.

✓ 1 PONT

5. Csaló webáruházak

- „200 000 Ft-os notebook negyed áron, márkás póló alig 1000 Ft-ért" – csak két példa tipikus internetes átverésre. A külföldi internetes áruházakban rengeteg termék érhető el kedvező áron, de a megrendelés előtt ellenőrizni kell a biztonsági feltételeket. Ezek a következők:
- A weboldal megbízhatósága: háttérinformációk, vélemények, fórumok, reklamációs lehetőség, közönségszolgálat, **nyelvtudás** stb.
- Kevés informatikai ismerettel is lehet webáruházat nyitni, ezért az „IstiPisti kisboltja" vagy a hasonló érdekes nevű áruházak kínálatát kritikusan vizsgáljuk.
- A csalódások elkerülése érdekében **csak hivatalos helyről rendeljünk!** A hazai nagy cégeknek általában cégnév.hu típusú webhelyük van, míg a külföldieknek leggyakrabban nagymárka.com típusú a címük.

- Vásárlásra csak biztonságos https-protokoll-lal működő weboldalt használjunk, amit a weboldal címe előtt egy kis zöld lakat jelez! Így az adatfolyam megfelelő titkosítással halad az interneten keresztül.
- A saját gépre vírusirtó, tűzfal és egyéb biztonság is kell a lehető legfrissebb verzióval és adatbázissal.
- A biztonsági adatainkat ne adjuk meg egy nyílt hálózatra kötött gépen (pl. egy webkávézóban ne vásároljunk vagy bankoljunk)!
- **Bankkártya adatokat csak a biztonság ellenőrzése után adjuk meg!** Bármilyen bizonytalanság esetén álljunk el a vásárlástól!
- Az EU területén nincsenek vámok. A nem EU-s címről (pl. Kína, USA) rendelt áruk után értéktől függően (általában 50 $ felett) kell vámot, ÁFÁ-t fizetni. A jelenlegi magyar szabályozás szerint létezik a vásárlástól való elállás joga. Az interneten rendelt áruk esetén a vevő egyoldalúan visszaléphet, és a termék (hiánytalan) visszaküldése után kérheti az ár visszafizetését – általában 14 naptári napon belül. (Lásd magyar fogyasztóvédelmi szabályozás.)
- Külföldi megrendelés esetén bizonyosodjunk meg a jótállásról, illetve a garanciáról!

✓ 3 PONT

6. Bankszámla adatok (adathalászat újra)

Legyünk körültekintőek a bankkártyánk, vagy a bankszámlánk adataival! Pl. havonta 1-2 alkalommal 300 Ft levonása a bankszámláról nem tűnik soknak, de pl. 10 000 ilyen bankszámla-tranzakcióval már tetemes összeg halmozódhat fel.

Az adathalászok sokszor próbálkoznak azzal, hogy hamis weboldalakra irányítják a figyelmünket, melyben pl. az áramszolgáltató kéri az adatainkat ellenőrzésre. Ehhez küldenek egy hivatalosnak tűnő levelet és a háttérben működik egy hivatalosnak tűnő weboldal is. Sajnos sokszor a bankok oldalát is hamisítják. Egy bank, éppen az adathalászat miatt, soha nem kéri e-mailen az ügyfelei adatait és/vagy bankkártya számát, ezért ne reagáljunk az ilyen e-mailben érkező kérésekre!

✓ 1 PONT

+1. Jogi háttér:

Az Európa Tanács 2001. november 23-án Budapesten fogadta el a Számítástechnikai bűnözésről szóló egyezményt. Az egyezmény 2004. július 1-jén lépett életbe, miután az Európa Tanács 5 tagállama – köztük hazánk – ratifikálta azt. 2011. október 1-ig az Európa Tanács 31 tagja és az Egyesült Államok ratifikálta az egyezményt.

Az egyezmény védeni kívánja a számítástechnikai rendszerek, hálózatok, adatok hozzáférhetőségének sérthetetlenségét, az ilyen rendszerek titkosságát; biztosítani a rendszerek, hálózatok, adatok visszaélésszerű használatának megelőzését. Az egyezmény bűncselekménnyé nyilvánítja az ilyen eseteket. Továbbá meghatározza a kiberbűnözés elleni hatékony fellépést lehetővé tevő felderítést, nyomozást és üldözést nemzeti és nemzetközi szinten biztosító jogköröket és rendelkezéseket.

Megjegyzés: Nem kell ilyen pontosan ismertetni a jogi hátteret.

✓ 1 PONT