Bűnmegelőzési hírlevél

Ne linkeskedjen!

Bátran kijelenthetjük, hogy mára talán az egyik legnépszerűbb vagyon elleni bűncselekménnyé lépett elő a csalás. Az emberek nagy része még mindig túl jóhiszemű, még mindig túl „jól nevelt", egyszerűen fel sem tételezi, hogy egy másik ember szánt szándékkal képes becsapni, hazudni, a pénzét kicsalva megkárosítani, különösen ha a csaló hivatalos, valamilyen szervezet (rendőrség, bank, önkormányzat stb) képviselőjének adja ki magát, vagy az igazira a megszólalásig hasonlító ál weboldalt hoznak létre, de igaz ez akkor is, ha tisztességes, becsületes módon magánemberek egyeznek meg valamiben, vagy legalábbis azt hiszik….

Nagyon sok bűncselekmény történik az online térben, mindegyik más és más, ami viszont általánosságban megállapítható a csalások esetében, hogy a cél, az anyagi haszonszerzés, a kivitelezéshez pedig meg kell szerezni a kiszemelt áldozat személyes és/vagy banki adatait.
Az adatokat sok esetben ellopják, de nagyon sokszor előfordul, hogy maguk a sértettek szolgáltatják ki a csalónak a csaló által megküldött linkre kattintással, vagy a csaló által ajánlott applikáció letöltésével, amely legtöbbször egy adatlopó vírus, vagy egy olyan program, amely távoli hozzáférést engedélyez a számítógépükhöz, mobil eszközükhöz.

Tudatos és felelős internet használattal az online térben elkövetett csalások jó eséllyel megelőzhetők az alábbi szempontok figyelembe vételével:

Biztonság 3 lépésben!

1. Ne „linkeskedjen”!

- **Ne kattintson automatikusan a felkínált linkekre, de ha mégis megtörténne, ne adja meg se a személyes, se a banki adatait!**
- **Ha nem tudja pontosan egy alkalmazásról, mire használható, ne telepítse sem a számítógépére, sem egyéb mobil eszközre, különösen mások kérésére ne tegyen ilyet!**
- **Üzenetben – e-mailben - kapott linkről, vagy ismeretlen telefonáló által javasoltak alapján, még ha pénzintézeti alkalmazottnak is mondja magát, soha ne töltsön le és telepítsen alkalmazást!**

2. Ellenőrzés

- **Minden esetben külön keressen rá az adott cég, vagy szervezet hivatalos weboldalára és ott bejelentkezve ellenőrizze a kapott üzenet valóságtartalmát.**

3. Személyes adatok védelme

- **Használjon egyedi, összetett jelszót minden online fiókjához, és fontolja meg a jelszókezelő használatát!**
- **Gondosan vizsgálja felül adatvédelmi és biztonsági beállításait, és korlátozza a látható és megosztható lehetőségeket! Utólag is ellenőrizze a már telepített webszolgáltatások és alkalmazások adatvédelmi és biztonsági beállításait**
- **Tiltsa le az ön által nem használt alkalmazásokat és funkciókat!**
- **Kapcsolja ki a követési és a helymeghatározó szolgáltatásokat, amikor éppen nem használja, és konfigurálja a böngészőt úgy, hogy rendszeresen törölje a sütiket!**
- **Számos alkalmazás hozzáférést kér a személyes adatokhoz, például a földrajzi helyhez, a névjegyzékhez és a fényképalbumhoz, mielőtt igénybe vehetné a szolgáltatásaikat. Óvakodjon az olyan alkalmazásoktól, amelyek hozzáférést igényelnek a kínált szolgáltatáshoz szükségtelen információkhoz!**