OUCH! 2021. március

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Így védjük meg magunkat a személyazonosság-lopástól

Mi az a személyazonosság-lopás?

Megszemélyesítéses csalásnak vagy személyazonosság-lopásnak nevezzük, amikor bűnözők az áldozat személyes adatait ellopva, azok felhasználásával csalást követnek el, például az adott személy nevében jogosulatlanul álláskeresési járadékot, adó-visszatérítést, hitelt vagy bankkártyát igényelnek. Ha nem hozunk óvintézkedéseket, előfordulhat, hogy olyan termékekért, vagy szolgáltatásokért fizetünk, amelyeket valójában nem mi vásároltunk meg, és biztosak lehetünk abban, hogy ez sok fejfájást fog okozni nekünk.

Személyes információink számos helyen megjelennek az interneten. Minden alkalommal, amikor böngészünk, vagy valamit online vásárolunk, megnézünk egy videót, ellátogatunk a háziorvoshoz, vagy megnyitunk egy alkalmazást a telefonunkon, információ keletkezik rólunk, ami valahol gyűjtésre kerül. Ezeket az adatokat a cégek sok esetben teljesen legálisan értékesíthetik egymás közt. Ha ezek közül csak egy is hacker támadás áldozatává válik, a bűnözők hozzáférhetnek személyes információinkhoz. Tételezzük fel, hogy a rólunk szóló információk egy része e pillanatban is a bűnözők rendelkezésére áll, és gondoljuk át, mit tehetünk annak érdekében, hogy észrevegyük és megakadályozzuk az adatainkkal történő visszaélést.

Észlelési tippek

- Időközönként nézzük át a bankszámlakivonatunkat és a banki fiókjainkon végrehajtott műveleteket, olyan terhelések után kutatva, amelyeket esetleg nem mi kezdeményeztünk. Ennek egyszerű módja, hogy a pénzügyi tranzakciókról automatikus e-mail vagy SMS értesítést állítunk be. Figyeljük a csalásra utaló jeleket!
- Járjunk utána azoknak a szituációknak, amikor egy kereskedő elutasítja kredit- vagy bankkártyánkat! Vizsgáljuk meg a fizetési felszólításokat, különösen bankkártyás vásárlások, orvosi számlák vagy hitelek tekintetében!
- Legyünk figyelmesek azokra a megkeresésekre, amelyek – minden előzmény nélkül – munkanélküli járadék vagy más állami támogatás igénylésével kapcsolatosan érkeznek!
- Évente egyszer javasolt hitelképesség-ellenőrzést végeznünk. Az Amerikai Egyesült Államokban például évi egy alkalommal ez ingyenesen kérhető.

Mit tegyünk, ha baj történik?

- Vegyük fel a kapcsolatot az érintett szervezettel! Például, ha tudomást szerzünk arról, hogy valaki a nevünkben igényelt egy hitelkártyát, azonnal értesítsük az adott pénzintézetet a problémáról. Ugyanígy, amennyiben valaki minket megszemélyesítve adó-visszatérítést, vagy álláskeresési járadékot igényelt, vegyük fel a kapcsolatot az érintett kormányzati szervezettel!

- Tegyünk rendőrségi feljelentést, hogy hivatalos nyoma is legyen a csalásnak! Erre sok esetben online is lehetőségünk van. Az Egyesült Államokban például a https://identitytheft.gov címen elérhető weboldalon keresztül tehetjük ezt meg. (Az NBSZ NKI megjegyzése: Magyarországon az elektronikusan intézhető rendőrségi ügyekkel kapcsolatos szabályok a https://ugyintezes.police.hu/e-ugyintezessel-kapcsolatos-szabalyzatok weboldalon tekinthetőek meg.)
- Amikor eljárunk egy csalás ügyében, rögzítsünk minden érintett szervezettel váltott üzenetet, valamint vegyük számba minden részünkről felmerült költséget, ugyanis ezekre később még szükségünk lehet.
- Értesítsük a biztosítónkat! Előfordulhat, hogy biztosítási csomagunk személyazonosság-lopás ellen is védelmet nyújt.

Hogyan védekezhetünk?

A következőkben olyan egyszerű tippeket ismerhetünk meg, amelyekkel csökkenthető a személyazonosság-lopás esélye:

- Korlátozzuk a rólunk elérhető információk mennyiségét az online platformokon és weboldalakon!
- Használjunk erős egyedi jelszót minden online fiókunk esetében, és extra védelem gyanánt alkalmazzunk kétfaktoros hitelesítést!
- Korlátozzuk, hogy ki férhet hozzá hitelekkel kapcsolatos adatainkhoz! Az Egyesült Államokban például van lehetőség arra, hogy befagyasszuk a hitelkártyánkat, így ha valaki kártyát igényelne, vagy hitelt venne fel a nevünkben, előbb fel kell oldania a zárolást!
- Érdeklődjünk a biztosítónknál, hogy van-e lehetőség biztosítást kötni a minket megkárosító megszemélyesítéses csalások esetére!

A szerzőről

Lenny Zeltser informatikai vezető az Axoniusnál, egy kiberbiztonsági eszközkezelő társaságnál. Emellett malware-ek elleni védekezést oktat, valamint publikál a SANS Intézetnél. Lenny a Twitteren is aktív: @lennyzeltser és egy biztonsági blog szerzője a zeltser.com-on.

Források

Pszichológiai Manipuláció: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Azonosítólopások bejelentése: : https://www.identitytheft.gov
Hitelszámla befagyasztás: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Identitás lopás: személyes tapasztalatok: https://zeltser.com/unemployment-fraud-and-identity-theft/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)