Megvédeni magunkat, mikor a magánéletünk védelme lehetetlen

A csalfa hívás, ami túl valódinak tűnt

Minden egy teljesen átlagosnak tűnő telefonhívással kezdődött. “Hello, Mrs. Patel? Michael vagyok, a bankja csalásokkal foglalkozó osztályáról. Szokatlan aktivitásra lettünk figyelmesek a számláján. Vásárolt mostanában 1200 dollár értékben egy elektronikai szaküzletben?” Mrs. Patel szívében megállt az ütő. Nem vásárolt semmi ilyesmit.

Hogy még hitelesebbnek tűntesse fel a beszélgetést, "Michael" megerősítette Mrs. Patel lakcímét és születési dátumát - olyan információkat, amikről a nő úgy gondolta, csak a bankja tudhat. Michael azt mondta neki, ahhoz, hogy visszafordítsák a tranzakciót, Mrs. Patel-nek előbb hitelesítenie kell személyazonosságát, amit a bankkártya adatai és a banki alkalmazásának hitelesítő adatainak megadásával tehet meg. Mivel rendkívül nyugtalan volt, úgy tett, ahogy Michael mondta. A hívó megköszönte, és biztosította róla, hogy a problémát hamarosan megoldják. Néhány órával később azonban Mrs. Patel nem tudott belépni a bankfiókjába. Aztán értesítéseket kapott, hogy többezer dollárt utaltak a tengeren túlra számlájáról.

Amire Mrs. Patel nem gondolt az az, hogy a csaló egy korábbi adatszivárgásból megszerezte a személyes adatait, és ezt használta hitelességének növelésére. Az egész hívás hazugság volt. Őt pedig épp átverték.

Az adataink mindenhol ott vannak

A mai összekötött világban a magánélet az egyik legnehezebben megvédhető dolog. Minden alkalommal, amikor online vásárlunk, stream-elünk egy filmet, használjuk a bankkártyánkat, vezetünk az autópályán vagy bármilyen mobilalkalmazást használunk, az információinkat begyűjtik, analizálják és megosztják. Ezenfelül személyes adataink jelentős része közhiteles nyilvántartásokban is szerepelhet, például állami választói adatbázisokban, adónyilvántartásokban vagy lakásvásárlásokra vonatkozó adatokban. A modern autók kamerái miatt még egy olyan egyszerű dolog is, mint egy parkolóban való sétálás azzal jár, hogy felvétel készül rólunk.

Függetlenül attól, ki és milyen célból gyűjti az információkat, az eredmény ugyanaz: személyes információk hatalmas mennyisége van világszerte eltárolva különféle adatbázisokban. Olyan adatok, amelyek fölött semmilyen irányításunk nincs. És mivel az adat létezik, így el lehet lopni, el lehet adni vagy kártékony célokra is fel lehet használni. A valódi, teljeskörűen védett magánélet gyakorlatilag majdnem lehetetlen.

Csak azért, mert tudják kik vagyunk, még nem biztos hogy hitelesek

A csalók gyakran használják ezeket a "könnyen" elérhető információkat, hogy a csalásaikat hihetőbbnek tűntessék fel. Például:

1. Egy csaló felhívhat minket banki alkalmazottnak kiadva magát, aki előbb megerősíti az otthoni címünket, ezt követően pedig elkéri a belépési adatainkat és a számlaszámunkat.
2. Egy e-mail tartalmazhatja a teljes nevünket, telefonszámunkat és születési dátumunkat is, hogy hitelesnek tűnjön.
3. Egy SMS úgy látszódhat, az autó biztosítónktól származik, és tartalmazhatja az autónk márkáját, típusát - sőt, akár az évjáratát is.

Az igazság az, hogyha valaki személyes információkkal rendelkezik rólunk, az még nem teszi őt megbízhatóvá, csupán meggyőzőbbé. A váratlan üzeneteket, hívásokat és e-maileket mindig szkeptikusan kezeljük, függetlenül attól, mennyit tud rólunk a feladó, vagy mennyire sürgető az üzenet. Nyugodtan szakítsuk meg a hívást, és hívjuk vissza az adott intézményt egy megbízható telefonszámon, amiről tudjuk, hogy hivatalosan hozzájuk köthető.

Figyeljünk a pénzünkre - itt kezdődik a csalás.

Mivel az adatainkat nem tudjuk teljesen megvédeni, a második legjobb védekezés a **korai észlelés**. Pénzügyeink folyamatos figyelemmel kísérése kulcsfontosságú előnyt jelenthet: észrevehetjük a gyanús tevékenységet, mielőtt az komoly kárt okozna. Minél előbb veszünk észre egy csalárd terhelést, annál könnyebb visszafordítani és megelőzni a további veszteségeket. Néhány egyszerű lépés, amit bárki megtehet:

- **Állítsunk be értesítéseket!** A legtöbb bank, hitelkártya-kibocsátó és befektetési szolgáltató lehetővé teszi, hogy minden tranzakcióról, pénzfelvételről vagy bejelentkezési kísérletről azonnali szöveges értesítést kapjunk.
- **Rendszeresen tekintsük át fiókjainkat!** Az értesítések mellett szánjunk hetente néhány percet arra, hogy ellenőrizzük az egyenlegeinket és a legutóbbi tevékenységeket, és kiszűrjük az esetleges szokatlan jeleket. Vagy állítsuk be fiókjainkat úgy, hogy napi vagy heti összesítő jelentéseket küldjenek számunkra e-mailben.
- **Fagyasszuk be számlánkat!** Tartózkodási helytől és szolgáltatótól függően lehetőségünk lehet számlaegyenlegünk ideiglenes hozzáférhetetlenné tételére, így senki sem fizethet kártyánkkal még akkor sem, ha megszerzi, illetve hitelt sem vehet fel. Ezenfelül ingyenes vagy olcsó jelentéseket is igénybe vehetünk a hitelminősítő intézetektől. Figyeljünk az ismeretlen fiókokra, lekérdezésekre.

A mai világban a tökéletesen megóvott magánélet már nem elérhető. Mindig jusson eszünkbe, hogy attól, hogy valaki információkkal rendelkezik rólunk, még nem feltétlenül hiteles. Nem kell kiberbiztonsági szakértőnek lennünk ahhoz, hogy biztonságban maradjunk: csak legyünk éberek, tegyünk fel kérdéseket, és figyeljünk a fiókjainkra!

Vendégszerkesztő

Dr. Litany Lineberry, a WiCyS Oktatási és Képzési Partner titkára, mérnöki doktori (PhD) fokozattal rendelkezik, kiberbiztonsági fókuszú szakterületen. Információs rendszerek technológiája tárgyat oktat a Hinds Community College uticai campusán, és támogatja a WiCyS küldetését, amely a nők toborzását, megtartását és előmozdítását célozza a kiberbiztonság területén, minden szektorban. https://www.linkedin.com/in/litany-lineberry

Források

Hogyan használják ki a kiberbűnözők érzelmeinket: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
A Misztikum Feloldása: Hogyan lopják el a jelszavakat a kiberbűnözők?: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Ne hagyjuk, hogy a kiberbűnözők lenyúlják a megtakarításainkat: Zároljuk a pénzügyi számláinkat!: https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)

Többet találhat az Ouch!-ból A következő linken: https://www.sans.org/newsletters/ouch