Bűnmegelőzési hírlevél
2023. január

Január 28. Az adatvédelem nemzetközi napja.

Az adatvédelem nemzetközi napját az Európa Tanács (ET) kezdeményezésére 2007-ben, az ET adatvédelmi konvenciója elfogadásának 25. évfordulóján rendezték meg először az Európai Bizottság támogatásával.

Az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozásával, az érintett személyek védelmével foglalkozik. Nevével ellentétben tehát nem elsősorban az adatokat védi, hanem azokat a személyeket, akikkel az adatok összeköthetők. Az adatvédelem vagy más néven az információs önrendelkezési jog az egyén azon joga, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról.

Az adatvédelem nemzetközi napja időszerű emlékeztető arról, milyen nagy mennyiségű adatot osztunk meg online – akár önként, akár véletlenül. Sok ember nem ismeri az online kockázatokat vagy a személyes adatai értékét. A legnépszerűbb közösségi fórumokon is (facebook, instagram, TikTok) videók, fényképek és adatok tömege kerül minden nap megosztásra.

A személyes adatok gondatlan megosztása vagy rossz kezekbe kerülése, a személyes adatokkal visszaélés nagyon is valós, komoly következményekkel járhat.

A pénzügyi következményektől az érzelmi következményekig, az online adatokkal való visszaélés nagyon sokféle hatással lehet, melyek még évekig is elhúzódhatnak, ezért nagyon komolyan kell vennünk azokat.

Az egyik **legnépszerűbb módja a csalásnak az adathalászat útján megszerzett adatokkal történő visszaélés.** Ál nyeremény játék, internetes vásárlás, internetezés során **csak egy linkre kell kattintaniuk**, esetleg kitölteni egy egyszerű kis kérdőívet, vagy válaszolni néhány egyszerű kérdésre, s míg ezt megteszik, ellopják az Ön adatait, amivel később különböző visszaéléseket követnek el. Az Ön által megadott adatokkal, vagy amelyeket elloptak az ide-oda kattintgatás során, **idegenek vásárolnak az interneten az ön pénzéből**, **megcsapolják a bankszámláját,** áruvásárlási kölcsönt vesznek fel, szerződést kötnek internet, mobil telefon előfizetésre, amiről a sértett már csak akkor szerez tudomást, amikor a szolgáltató jelentkezik az elmaradt részletek, előfizetési díjak követelésével.

A személyes adatok kézben tartása és a magánélet határainak megerősítése azonban sokkal könnyebb, mint ahogy az emberek gondolják.

Személyes adatainak védelme érdekében javasoljuk:

- 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!

Nagyon gyakori, hogy az elkövetők pénzintézetre, bankra hivatkozva csalják ki a számla vagy bankkártya birtokos személyes adatait, internetbanki belépéshez szükséges azonosítót, biztonsági kódot, jelszót vagy bankkártya adatokat. Viszonylag új módszer, hogy a csalók a bankok, pénzintézetek web oldalaihoz a megszólalásig hasonlító ál web oldalakat hoznak létre, ahová egy, a bank nevében e-mailben küldött linkre kattintva lehet jutni, vagy a keresőbe beírva a keresett bank nevét, a felkínált lehetőségek között szinte bizonyosan az elsők között fog szerepelni az ál banki oldal is.

- **Ne üzenetben kapott linkről lépjen a bankja web oldalára!**
- **Mindig ellenőrizze gondosan, hogy valóban a bankja hivatalos web oldalára lépett be!**
- **Üzenetben kapott linkről, vagy ismeretlen telefonáló által javasoltak alapján, még ha pénzintézeti alkalmazottnak is mondja magát, soha ne töltsön le és telepítsen alkalmazást!**

Az egyik leginkább elterjedt károkozó, „vírusírtónak” is titulált alkalmazás, az Anydesk elnevezést viseli, de vannak más alkalmazások is, amelyek távoli hozzáférést biztosítanak a kiszemelt áldozatok eszközeihez, és az azon tárolt összes fájlhoz, jelszóhoz.

- **Ha nem tudja pontosan egy alkalmazásról, mire használható, ne telepítse sem a számítógépére, sem egyéb mobil eszközre, különösen mások kérésére ne tegyen ilyet!**

- **Ha ilyen, vagy hasonló hívást kap, azonnal ellenőrizze vissza! Hívja fel Ön a számláját kezelő pénzintézetet, vagy érdeklődjön személyesen a bankjában!**

- **Egyeztessen a pénzintézettel az Ön számára legideálisabb védelemről!**

Ha minden elővigyázatosság, odafigyelés ellenére mégis bűncselekmény történne a sérelmükre, kérjük azonnal értesítsék a Rendőrséget!
112

Segítségért fordulhatnak az áldozatsegítő szolgáltatást nyújtókhoz is:

Egri Áldozatsegítő Központ
Eger, II. Rákóczi Ferenc utca 10.
Tel: +36 (30) 3752176
e-mail: askeger@im.gov.hu