**Nyitott könyv az életünk, de vajon a személyes adataink is benne vannak?**

5 figyelmeztető jel, amely arra utal, hogy személyazonosság-lopás áldozataivá váltunk

Sajtóközlemény – 2022.01.20./PResston PR

**Lassan már észre sem vesszük, hogy milyen sok időt töltünk a digitális térben. Mindenképpen elgondolkodtató, hogy a legújabb előrejelzések szerint 2022 végére a felhasználók átlagos képernyőideje meghaladhatja a napi 8 órát is. Ez azt is jelenti, hogy egyre több adatot fogunk online kezelni, ami növeli az adathalász támadások kockázatát.**

**Mit is jelent a személyazonosság-lopás?**

Személyazonosság-lopásról akkor beszélünk, ha valaki megszerzi személyes adatainkat, és valamilyen visszaélést követ el vele, megkárosítva bennünket ezzel. A kibertámadók rendszerint olyan érzékeny adatokat tulajdonítanak el, mint az elektronikus jelszavaink, hitelkártya- és társadalombiztosítási számaink, melyekkel tranzakciókat indíthatnak a nevünkben, online vásárlásokat kezdeményezhetnek, vagy akár tudtunk és beleegyezésünk nélkül hitelt is igényelhetnek különböző platformokon keresztül. Valljuk be, már önmagában a gondolat is nagyobb óvatosságra ösztönöz bennünket a digitális világban.

Az **ESET kiberbiztonsági szakértői** összegyűjtötték, hogyan ismerhetjük fel az identitás lopás jeleit, illetve mit tehetünk annak érdekében, hogy minimalizáljuk a ránk leselkedő veszélyeket.

1. **Indokolatlan levonások a bankszámlánkról**

Az egyenlegünk legkisebb mértékű változása is gyanúra adhat okot, ugyanis a csalók gyakran alacsony értékű próbavásárlásokkal ellenőrzik az ellopott kártyák érvényességét. Ha bármi szokatlant észlelünk, érdemes azonnal felvenni a kapcsolatot a bankunkkal, és letiltani a bankkártyánkat!

1. **Letiltott fiókok**

Ha a kibertámadóknak sikerül megszerezniük bejelentkezési adatainkat, fontos tudnunk, hogy első dolguk a jelszóváltoztatás lesz, hogy maximálisan kizárjanak minket a saját fiókjainkból, digitális identitásunkból.

Amennyiben a mobilszolgáltatónknál próbálkoznak, és sikerül megoldaniuk, hogy telefonszámunkat egy másik (a támadók tulajdonában lévő) eszközre irányítsák át, SIM- cserés támadást is végrehajthatnak. Ennek jele, ha váratlanul elnémul a mobilunk, lekapcsolódva a mobilhálózatról.

Ez különösen veszélyes, ugyanis így közvetlen hozzáférésük lesz például a bankok által használt egyszeri SMS hitelesítéshez érkező jelszavakhoz is, melyek segítségével már gond nélkül hozzáférnek számláinkhoz. Gyanú esetén azonnal lépjünk kapcsolatba a mobilszolgáltatónkkal és a bankunkkal.

1. **Hamis adóvisszatérítési értesítések**

Egy másik gyakori módszer a kiberbűnözők körében, hogy adóvisszatérítésre hivatkozva próbálják megszerezni az áldozatok személyes adatait. Hazánkban a Nemzeti Adó- és Vámhivatal (NAV) is figyelmeztetést adott ki hasonló támadásokkal kapcsolatban 2021 novemberében. A kibertámadók sms-ben, e-mailben, de akár telefonon is megkereshetnek bárkit, hogy megszerezzék a bankkártyaadataikat. Soha ne dőljünk be az ilyen próbálkozásoknak, ugyanis a NAV-nak csakis bankszámlaszámra vagy postacímre van szüksége a visszatérítések kiutalásához!

1. **Fals orvosi számlák**

Okkal gyanakodhatunk arra, hogy személyazonosság-tolvajok áldozatává váltunk abban az esetben is, ha olyan orvosi ellátásról kapunk számlát, amit sosem vettünk igénybe. Az ilyen jellegű támadások különösen népszerűek azokban az országokban, amelyekben magánegészségügyi szolgáltatások érhetők el.

1. **Adósságbehajtók megkeresései**

Ha a személyes adataink illetéktelen kezekbe kerültek, és különböző visszaélések áldozatai lettünk, sajnos rövid időn belül számíthatunk arra, hogy adósságbehajtók jelentkeznek nálunk a kiegyenlítetlen számlákkal. Bizonyára ez már a rendőrség hatásköre, így mielőbb vegyük fel velük a kapcsolatot.

**Hogyan védjük meg magunkat a személyiség-tolvajoktól?**

Az alábbi biztonsági lépések betartásával csökkenthetjük a kockázatát annak, hogy identitás lopás áldozatává váljunk:

* Minden online fiók esetében éljünk a többfaktoros hitelesítés lehetőségével
* Használjunk erős és egyedi jelszavakat, a biztonságos tárolásukra pedig alkalmazzunk professzionális jelszókezelő programokat
* Minden eszközünket lássuk el naprakész, megbízható biztonsági szoftverrel, és kapcsoljuk be az automatikus hibajavító frissítéseket
* Csak hivatalos áruházakból töltsünk le alkalmazásokat
* Kerüljük a nyilvános Wi-Fi hotspotok használatát
* Csakis HTTPS (a böngésző címsorában kis lakattal jelzett) webhelyeket látogassunk
* Kidobás előtt semmisítsünk meg minden régi dokumentumot olyan módon, hogy a személyes adataink ne legyenek belőle összerakhatóak

A gyors digitális fejlődés a kibertámadások gyakoriságát is felgyorsította, ezért mindennapi életünket sokkal tudatosabban kell élnünk az online térben is, hogy semmiképp se kerüljünk a csalók hálójába.

Összefoglalásul, az ESET kiberbiztonsági szakértői azt tanácsolják, hogy legyünk éberek és tudatosak, hogy megelőzhessük, illetve időben felismerjük a figyelmeztető jeleket és felkészülhessünk a megfelelő védekezésre az érzékeny adatainkra vadászó csalók esetében. Érdemes tájékozottnak lenni a lehetséges kockázatokkal kapcsolatban, a veszélyekről pedig tájékoztassuk barátainkat és családtagjainkat is, kiemelten ügyelve az idősek tapasztalatlanságára, akik gyakori áldozatai a csalásoknak.

**A Sicontact Kft.-ről röviden:**

A Sicontact Kft. hazánkban az egyik legjelentősebb **IT biztonsággal foglalkozó** cég, az ESET termékek kizárólagos magyarországi forgalmazója.

Mottója és küldetése, ami köré termékportfolióját kialakította: „**biztonság a digitális világban**”. A Sicontact Kft. Magyarországon az **ESET NOD32** technológiára épülő termékeivel mind a lakossági, mind a vállalati szegmensben meghatározó piaci szereplő.

A Sicontact Kft. több ízben elnyerte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 30 éve biztosít védelmet a digitális világ fenyegetéseivel szemben. Egy kicsi és dinamikus vállalatból mára egy több mint 100 millió felhasználót számláló és 202 országot és területet lefedő globális márkává nőtte ki magát.

Rengeteg minden változott, de az alapvető törekvéseik és a hozzáállásuk változatlan maradt, továbbra is céljuk egy biztonságosabb digitális világ felépítése, amelyben mindenki élvezheti a biztonságos technológia előnyeit.

**További információ és interjúegyeztetés:**

**Terdik Adrienne| Ügyvezető igazgató | PResston PR | Rózsadomb Center |
1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 |
M +36 30 257 60 08 |** adrienne.terdik@presstonpr.hu **|www.presstonpr.hu**

**Szekeres Nikoletta | PR vezető | PResston PR | Rózsadomb Center |
1025 Budapest | Törökvész u. 87-91. | T + 36 1 325 94 88 | F +36 1 325 94 89 |
M +36 30 831 64 56 |** nikoletta.szekeres@presstonpr.hu **|** www.presstonpr.hu