A személyes adataink 5 legnagyobb ellensége

Sajtóközlemény – 2021.01.27./PResston PR

Az Európai Tanács kezdeményezésére 2007 óta minden év január 28-a az adatvédelem nemzetközi napja, amely adataink védelmére, és az ehhez kapcsolódó ismeretek fontosságára hívja fel a figyelmünket. Az idei világnap mégis más, mint a többi, hiszen az elmúlt egy évben az életterünk még inkább az online világ köré fonódott. A megnövekedett digitális jelenléttel egyenes arányban nőtt a kibertámadások száma is, amelyek során illetéktelen kezekbe kerültek a felhasználók érzékeny adatai. Ezt támasztja alá az ESET kiberbiztonsági jelentése is, mely szerint globális szinten 37%-kal nőtt az otthoni munkavállalókat érő kibertámadások száma.

„Soha nem volt még ennyire fontos számítógépeink, adataink biztonsága. Az intenzív és folyamatos online jelenlét, a tömeges otthoni munkavégzés és online oktatás komoly kihívás elé állította az emberiséget. ***Az egyedi kártékony kódok, vírusok száma idén meghaladta az 1.1 milliárdos számot, míg a Have I Been Pwned adatbázisában mára már több, mint 10.4 milliárd feltört, kiszivárgott jelszó található.*** *Az ESET 2021-es Kiberbiztonsági Trendekről szóló jelentéséből is látszik, ahogy a munkánk és a magánéletünk egyre nagyobb része kerül át a digitális térbe, úgy az idei évben a kiberbiztonságnak életünk legfontosabb alappillérévé kell válnia. Ehhez pedig a korszerű, hatékony védelmi megoldások mellett a folyamatosan fejlesztett biztonságtudatos hozzáállásunk is kulcsfontosságú lesz."*- hívja fel a figyelmet **Csizmazia-Darab István**, az ESET megoldásokat forgalmazó Sicontact Kft. IT biztonsági szakértője.

Ahogy egyre több digitális eszköz vesz körül bennünket, érdemes még nagyobb figyelmet szentelnünk az érzékeny adataink védelmére is. A biztonság felé vezető út egyik legfontosabb lépése, hogy tisztában legyünk azokkal a kockázatokkal, amelyekkel az adataink biztonságát veszélyeztethetjük.

Az alábbi adatvédelmi „mumusok" elkerülésével és a szakértői tanácsok megfogadásával sokat tehetünk saját magunk és adataink biztonsága érdekében:

1. **Elhanyagolt adatvédelmi beállítások**
   Az online jelenlétünket érdemes néha karbantartanunk. Időnként nézzük át a különböző webes szolgáltatások és közösségi média fiókok biztonsági és adatvédelmi beállításait, mert általában rendszeresen frissítik, bővítik őket. A közösségi oldalakon állítsuk be, hogy csak az ismerőseink láthassák a posztjainkat – ha van rá lehetőség, készíthetünk egyedi listákat is, például a tágabb ismerősi és a szűkebb, közeli baráti körünkről. Legyünk saját magunk

moderátorai: csak olyan tartalmakat tegyünk közzé, osszunk meg és csak úgy szóljunk hozzá mások posztjaihoz, hogy azok ne hozhassanak minket kínos helyzetbe még az eredeti környezetből kiragadva sem. Gondoljunk bele: bár mi döntjük el, hogy mit osztunk meg magunkról, azt nem tudjuk befolyásolni, hogy mások mihez kezdenek ezzel az információval.

2. **Alábecsült jelszavak**

Erős és egyedi jelszavak használatával nagyban megnehezítjük, hogy illetéktelen személyek feltörjék a fiókjainkat, és többek között a személyes vagy akár banki adatainkhoz hozzáférjenek. Érdemes megnéznünk a legrosszabb jelszavak toplistáját, melyben remek példákat találhatunk arra, hogy milyen jelszót ne válasszunk. A 2020-as év legtöbbször használt jelszavai például a kevesebb, mint 1 másodperc alatt feltörhető "123456", "123456789" és a "picture1" voltak.

A jelszó hosszát illetően jó, ha tudjuk, hogy jelenleg 12 karakter felett ugrik egy nagyságrendet a feltöréshez szükséges idő. Minden fiókunkhoz más kódot adjunk meg, és kerüljük a hozzánk köthető szavak, információk (pl. kisállatunk neve, születési dátumunk) használatát. Ahol pedig lehet, használjunk többfaktoros hitelesítést is, amely plusz védelmi réteget ad a fiókjaink számára. Ez az extra réteg lehet egy ellenőrző kód, értesítés az okostelefonunkon vagy akár ujjlenyomatos azonosítás is.

3. **Kíváncsiskodó alkalmazások**

Érdemes időnként átnézni az eszközeinken futó alkalmazásokat, és felülvizsgálni, hogy melyek azok, amiket már nem használunk. Fontos, hogy a felesleges alkalmazásokat ne csak eltávolítsuk az eszközről, hanem a hozzá tartozó felhasználói fiókunkat - az összes rólunk tárolt információval együtt – is töröljük az applikációban!

A még használatban lévő appok esetében pedig figyeljünk arra, hogy rendszeresen frissítsük azokat, illetve kapcsoljuk ki az olyan adatgyűjtő funkciókat, mint például a helymeghatározás, amikor a program éppen nincs használatban. Az alkalmazások letöltése vagy frissítése előtt nézzük át, hogy pontosan mihez kérnek hozzáférést. Mielőtt gondolkodás nélkül rányomnánk a feltételek elfogadására, mérlegeljük az előnyöket és a hátrányokat, illetve érdemes átolvasnunk más felhasználók szöveges értékeléseit is.

4. **Trükkös e-mailek**

Adathalász támadásoknál a kiberbűnözők a netezők hiszékenységét próbálják kihasználni. Megkereshetnek minket egy ismert, megbízhatónak tartott szolgáltató nevében (bankok, hivatalok, csomagküldő szolgálatok, közösségi

média felületek), vagy valamilyen csalit, például pénz nyereményt vagy műszaki cikket kínálva. Általában a levél arra kér minket, hogy a megadott linkre kattintva adjunk meg különböző bizalmas adatokat magunkról. Mindig figyelmesen ellenőrizzük, hogy az e-mail valóban az adott szolgáltatótól érkezett-e, illetve ellenőrizzük azt is, hogy az üzenetben hivatkozott ügyfélkódunk helyes-e. Mindig tartsuk szem előtt, hogy a bűnözők igyekeznek kihasználni az aktuális eseményeket, így a koronavírus-járványt is. Már most is találkozhatunk vakcinákkal kapcsolatos kéretlen üzenetekkel, amelyek információt, a várakozási listában való előrébb jutást, vagy akár felár ellenében azonnali oltóanyagot ígérnek. Utóbbi esetben különösen veszélyes, hogy a gyanútlan áldozatok a személyes adataik ellopása és az anyagi károk mellett az egészségüket, de akár az életüket is kockáztathatják.

5. **Védtelen eszközök**

   Sok bosszúságtól kímélhetjük meg magunkat egy naprakész, modern vírusvédelmi szoftver használatával. Lehetőleg olyan programot válasszunk, amelynek van adathalászat elleni funkciója is, így védve leszünk azon káros weboldalak ellen, amelyek célja különböző érzékeny adatok eltulajdonítása. Érdemes ismert gyártók termékei közül választani. Az **ESET Internet Security** például hatékony védelmet nyújt az adathalászat mellett a hackerek, a rosszindulatú programok, zsarolóvírusok, valamint egyéb online fenyegetések ellen.

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 cég 2007-ben megszerezte az ESET ausztriai képviseletét, így azóta regionális piaci szereplőként tevékenykedik. A Sicontact Kft. több ízben elnyerte a kitüntető **Business Superbrands** díjat. Az ESET Smart Security programcsomagot többször is **az év antivírus megoldásának** választották.

A független tesztelő szervezet több díjjal is elismerte az otthoni ESET termékeket a 2019-es eredményeket összefoglaló riportjában:

- Arany díjat nyert a fejlett, célzott és fájlnélküli kártevő támadások kivédésében, amely új kategóriaként jelent meg 2019-ben. Az ESET volt azon két gyártó egyike, akik mind a 15 célzott támadást sikeresen blokkolták a tesztelés során.

- 2018-ban ezüst, majd 2019-ben arany díjat szerzett a rendszer gyorsaságára és teljesítményére gyakorolt hatást vizsgáló kategóriában, az ESET szoftverek alacsony erőforrásigényének köszönhetően.

- Bronz díjat nyertek el a téves riasztások kategóriájában, amelyek ugyanúgy gondot okozhatnak, mint egy valós fertőzés, ezért az elkerülésük kulcsfontosságú a biztonsági szoftvereknél.

A Sicontact Kft. az ESET szoftvereit a lehető legrugalmasabb konstrukciókban, magyar nyelvű terméktámogatással kínálja. Az ESET már több mint 25 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