

Hogyan védjük meg az idősebb generációkat a kiberbűnözéstől?

Sajtóközlemény – 2019.12.16./PResston PR

A közvélekedés szerint az idős embereket nagyobb valószínűséggel verik át csalók, mint gyermekeiket vagy unokáikat. Ami a számokat illeti, csak az Egyesült Államokban évente közel 3 milliárd dollárt csálnak ki az idősök pénztárcájából különféle módszerekkel a kiberbűnözők – ezek között szerepelnek az internetes átverések is.

Ráadásul az ilyen statisztikák vélhetően csak a töredékét képviselik a tényleges károknak, mivel sok áldozat inkább hallgat, mert attól tart, nevetségessé válik, ha beismeri saját tudatlanságát, óvatlanságát.

De vessünk egy közelebbi pillantást a kérdésre, és vizsgáljuk meg, miért különösen sebezhetőek az idős emberek az online csalásokkal szemben! A csalók többek között kihasználhatják az idősök hiszékenységét, illetve egyes esetekben az öregedés okozta kognitív-képesség-romlást. Mondanunk sem kell, hogy az efféle bűnözők arra alapozzák tevékenységüket, hogy a kiszemelt áldozatok nem úgy nőttek fel, hogy ez a technológia körülvette volna őket. Nagy valószínűséggel ugyanis soha nem vettek részt még a legalapvetőbb kiberbiztonsági képzéseken sem. Nézzünk most pár praktikus tanácsot, melyekkel felvértezve az idősök is jóval nagyobb eséllyel szállhatnak szembe az online csalókkal.

Legyünk szkeptikusak!

Soha ne feltételezzük, hogy egy idegen személy az interneten megbízható! Sőt, minden váratlan üzenetet tekintsünk átverési kísérletnek! Akkor is óvatosan kell eljárunk, ha az üzenet egy ismerősünktől érkezik (vagy legalábbis úgy *tűnik*, hogy tőle érkezik) -- ez egyaránt vonatkozik az e-mailben, a Messenger-jellegű applikációkon keresztül és a közösségi médiában továbbított üzenetekre. Vigyázzunk, ha valami szokatlant veszünk észre akár az üzenetben, akár a feladóval kapcsolatban: lehet, hogy egy kiberbűnöző átvette az irányítást barátunk online fiókja felett, és most azt használja rosszindulatú spam-üzenetek küldésére. Ha kétség merül fel bennünk, inkább töröljük az üzenetet!

Ne kattintsunk!

Az adathalász támadás az egyik legelterjedtebb online visszaélés, és általában egy kéretlen e-maillal vagy közösségi médiás üzenettel kezdődik, amelyben a csaló egy számunkra ismert személynek adja ki magát, elhítelve velünk, hogy megbízhatunk benne. Aztán megpróbál meggyőzni minket arról, hogy adjuk ki neki érzékeny adatainkat, mint például hitelkártya-adatokat vagy online bejelentkezési adatokat. Sok csaló már jóval túlhaladta a rossz helyesírással megírt és csak szöveges tartalomra építő adathalász üzeneteket: konkrétan egész weboldalakat és Facebook-oldalakat hoznak létre átverő-kampányaikhoz. Soha nem szabad automatikusan feltételeznünk, hogy a váratlanul kapott anyagok hitelesek, függetlenül attól, hogy mennyire hivatalosnak néznek ki. Nagy körültekintéssel kattintsunk csak linkekre vagy nyissunk meg e-mailes csatolmányokat, még akkor is, ha az üzenet látszólag ismert, megbízható forrásból származik!

Mondjunk nemet az ingyenes dolgokra!

A fentiekhez hasonlóan a csalók e-mailt küldhetnek nekünk, hogy gratuláljanak a lottón vagy egy olyan nyereményjátékban elért „sikerünkhöz”, amelyben soha nem is vettünk részt. Annak érdekében, hogy a nyereményt „felszabadítsák” számunkra, kérni fogják a személyes adatainkat és/vagy előleg kifizetését egyfajta "előleges átverés" formájában. Általában az üzenetek sürgető jellegűek, próbálják azt az érzetet kelteni, hogy ha nem cselekszünk azonnal, akkor kimaradunk valamiből. Ne felejtjük el azonban, hogy a legitim lottók soha nem követelik meg a nyertesektől, hogy bármiféle díjat fizessenek a nyereményeik átvétele érdekében!

Soha ne utaljunk pénzt idegeneknek!

A romantikus indíttatású átverés volt a második legkártékonyabb csalási forma 2018-ban: a minden korosztályt megcélózó trükk-kategória (melyben egy lehetséges romantikus partneri viszony ígéretével csalnak ki pénzt vagy személyes információt az áldozatokból) összesen 362 millió dollár értékű kárt okozott. Ami még ennél is rosszabb: az FBI legfrissebb, internetes bűnügyekkel foglalkozó jelentése azt is megállapította, hogy becslések szerint a romantikus csalások áldozatainak csaknem egyharmadát ún. money mule-nak (pénzöszvérnek) használták, magyarul pénzmosó bűncselekmények gyanútlan részesévé tette őket. A romantikus átverések már évek

óta szerepelnek az időskorúak ellen elkövetett leggyakoribb átverések listáján, ami nem meglepő amiatt, hogy a magány az egyik leggyakoribb probléma, amellyel sok idős embernek szembe kell néznie.

Párbeszéd

Az utolsó tipp elsősorban a fiatalabbaknak szól: tartsuk fenn a folyamatos párbeszédet szüleinkkel és nagyszüleinkkel, és úgy magyarázzuk el nekik az alapvető kiberbiztonsági gyakorlatokat, hogy számukra a leginkább érthető legyen, illetve köthető saját tapasztalataikhoz!

Már azzal sokat segítünk, ha az interneten leselkedő veszélyekre felhívjuk a figyelmüket és átbeszéljük velük, mire kell vigyázniuk.

Érdeemes a figyelmükbe ajánlani olyan oldalakat, ahol IT biztonsággal kapcsolatos fontos tudnivalókról olvashatnak: <https://www.eset.com/hu/it-biztonsagi-temak/>

Amellett, hogy így jobban megértik majd az online világot és annak árnyoldalát, sokkal kevésbé érzik majd magányosnak magukat, ami végső soron segíthet abban is, hogy a világháló biztonságosabbá váljon a számukra.

+1 tipp

A fenti óvintézkedéseken túl mindig jól jön egy technikai védőháló is, melyet például olyan termékek szolgáltatnak, mint az ESET Internet Security. A több mint 110 millió felhasználóval rendelkező és a vírusvédelemmel kiemelten foglalkozó ESET most lehetővé teszi, hogy valami igazán hasznosat adjunk szeretteinknek karácsonykor: ha szeretnénk szüleiket, nagyszüleiket is biztonságban tudni az interneten, akkor most érdemes lecsapni az „egyet-fizetsz-hármat-vihetsz” akcióra. Ennek keretein belül 2020. január 6-ig 3-felhasználós licenc jár a bármilyen számítógépre (Windows, Macintosh, Linux) és okoseszközre (Android) telepíthető 1 éves, 1-felhasználós ESET Internet Security áráért.

Bővebb információ: karacsony.eset.hu

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 képviselét, 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 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 törekvések 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 tanácsadó** | **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