IT-biztonsági tippek az ünnepekre

Sajtóközlemény – 2019.12.04./PResston PR

Az ünnepek közeledtével a szokásosnál is nagyobb figyelmet kell fordítanunk adataink védelmére és otthonunk, családunk digitális biztonságára. Utazás alatt különösen óvatosnak kell lennünk.

Hogy nagyobb sikerrel vehessük fel a harcot a kiberbűnözőkkel, ajánlatos megfogadni az alábbi „mit ne tegyünk / mit tegyünk" tanácsokat.

Mit NE tegyünk:

- Bármekkora is az öröm és az izgalom az ünnepi utazások miatt, a közösségi médiában ezt ne osszuk meg! Ha közzétesszük, hogy éppen elutaztunk, akkor ez az információ felhasználható egy betörés megtervezésére és kivitelezésére.

- Ne osszunk meg a közösségi médiában repülőjegyeket ábrázoló fényképeket!

- Miután nyilvános helyen befejeztük a netezést, ne felejtsük el törölni azokat a hálózatokat, amelyekhez csatlakoztunk, hogy elkerüljük a későbbi automatikus csatlakozást, és a támadásokat! Ne felejtsük el kikapcsolni a Bluetooth-t és a wifi-t, ha már nem használjuk őket!

- Számos nyilvános wifi hálózat megköveteli, hogy megosszuk email címünket és személyes adatainkat, mielőtt engedélyeznék nekünk az internethez való csatlakozást. Próbáljuk meg nem megosztani a valós adatainkat és nem megadni a mindennapi email címünket! Hozzunk létre már előre egy eldobható email címet csak az ilyen esetekre! Így a fő email címünk és érzékeny adataink nagyobb biztonságban maradnak.

Mit TEGYÜNK:

- Korlátozzuk a digitális eszközeinkhez való fizikai hozzáférést. Minden elektronikus eszközünkön állítsunk be PIN-kódot, jelszót, biometrikus azonosítást vagy feloldási mintát. Ne feledjük azonban, hogy a feloldási minta könnyen kitalálható, tehát a biztonságos jelszó vagy az ujjlenyomatunk sokszor jobb megoldás.

- Ha lehetséges, telepítsünk egy biztonsági megoldást is. A fejlettebbek (mint pl. az ESET Mobile Security for Android) a hatékony vírusvédelem mellett lehetővé teszik

az eszköz távoli kezelését, lopás vagy elvesztés esetén a készülék megtalálását, riasztások aktiválását és a távolból történő törlést is.

- Sok esetben a készülékeken lévő adatok bírnak a legnagyobb értékkel. Utazás közben mindig próbáljunk minden elektronikus eszközt magunknál, a zsebünkben vagy a kézipoggyászban tartani.

- Ha lehet, titkosítsuk adathordozóinkat!

- Legyünk óvatosak az USB-töltőhelyeken, pl. repülőtereken és más nyilvános helyeken! A feltört töltőportokon keresztül rosszindulatú adatlopó szoftverek és kártevők települhetnek az eszközeinkre.

- Ha nyílt wifi hálózatokat használunk nyilvános helyeken, pl. éttermekben, kávézókban, szálláshelyeken, akkor az adataink védelme érdekében használjunk VPN szolgáltatást -- ezek egy része ingyenes, és ami a legfontosabb, növelhetik adataink biztonságát az adatátvitel pillanatában. De még a fizetős VPN szolgáltatások – amelyek sebessége sokkal gyorsabb az ingyenes, változatokénál, például ExpressVPN, Nord VPN, SurfSharkNet- is bőven a megfizethető kategóriában találhatóak.

- Mindig használjuk az ún. kétfaktoros hitelesítést (2FA), mert ez hatékonyan növeli fiókjaink és adataink biztonságát!

- Rendszeresen ellenőrizzük bankszámláinkat és közösségi oldalainkat, hogy megbizonyosodjunk arról, nincs-e szokatlan tevékenység. Ha bármi gyanúsat észlelünk, azonnal változtassuk meg bejelentkezési adatainkat! Az ilyen adatok kezelésének legjobb módja egy olyan eszköz, amely erős és egyedi jelszavakat hoz létre minden fiókhoz. (Ilyen pl. az ESET Password Manager is.)

- Védjük online vásárlásainkat! Ha lehetséges, bankkártya helyett hitelkártyát vagy virtuális bankkártyát használjunk! Ha bankkártyánk adatait ellopják, fennáll a veszély, hogy hirtelen egy üres bankszámlával találjuk szembe magunkat, ami az ünnepek alatt és egy utazás kellős közepén senkinek sem hiányzik. erre jó kiegészítő megoldás, ha minden pénzmozgásról SMS értesítést kérünk, így azonnal feltűnhet, ha valami gyanús tranzakciót indítanak a nevünkben.

- Legyünk óvatosak, mikor ATM-ből veszünk fel pénzt! Ellenőrizzük, hogy a kártyaolvasónak nincsenek-e laza vagy könnyen eltávolítható részei! Ezek gyanúsak, kamerát rejthetnek vagy eltömítik a pénzkiadó nyílást! A legbiztonságosabb ATM a bank ügyfélterében lévő automata.

- Netes információküldés előtt ellenőrizzük, hogy a kapcsolat titkosítva van-e HTTPS-sel – ezt könnyű felismerni, mert általában egy lakat szimbólum jelzi a meglátogatott website címe előtt, hogy biztonságban vagyunk. Ha nincs, akkor az egy komolytalan, illetve nem elég biztonságos webshop, webhely.

- Az utazók az IT-támadások gyakori célpontjai, mert a kiberbűnözők tudják, hogy az útra kelők online keresik a legjobb ajánlatokat. Célszerű ezért egy átfogó, hatékony biztonsági megoldást használni otthonra, amely többféle támadási lehetőség ellen is védelmet nyújt, mint pl. az ESET Internet Security.

Adjunk biztonságot karácsonyi ajándékba

Az ünnepekhez közeledve jó ötlet lehet igénybe venni egyet az ilyenkor szokásos akciók közül. A vírusvédelmi-szakértő ESET hazai forgalmazójának (Sicontact Kft.) felmérése alapján, Magyarországon a 18-59 éves lakosság háromnegyede használ vírusirtót számítógépén vagy okoseszközén, míg 18% egyáltalán nem használ ilyen programot. 35%-uk vált már valamiféle vírustámadás áldozatává: sokaknak csak kéretlen felugró reklámablakok és weboldalak jelentek meg, de az áldozatok közel felének vírus támadás miatt nem indult el az eszköze, illetve minden ötödik áldozat nevében küldtek már kéretlen üzeneteket, leveleket vírusok.

Az ESET igyekszik támogatni a felhasználókat a támadások elkerülésében, így december 2 és január 6 között 3 felhasználós licencet biztosít a mindenfajta számítógépre (Windows, Macintosh, Linux) és okoseszközökre (Android) telepíthető 1 éves, 1 felhasználós ESET Internet Security áráért. Ebben a konstrukcióban nem egy, hanem három eszközre szóló licenc jár egy áráért.

Bővebb információ: karacsony.eset.hu

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