OUCH! | 2021. február

Feltörték a fiókomat. Mit tegyek most?

Lehet, hogy meghackeltek?

Nem számít, mennyire vagyunk biztonságtudatosak, bármikor előfordulhat, hogy meghackelnek bennünket. Az alábbiakban olyan figyelmeztető jelekről olvashatunk, amelyek arra utalhatnak, hogy hackelés áldozatává váltunk, illetve megtudhatjuk, hogy ilyen esetben mi a teendő.

Online fiókok

- Családunk vagy barátaink szokatlan üzeneteket vagy például meghívókat kapnak tőlünk, amelyekről tudjuk, hogy nem mi küldtük őket.
- Jelszavunk nem működik, pedig biztosak vagyunk benne, hogy jól adtuk meg.
- Belépésről szóló emlékeztetőket kapunk különböző webhelyekről, amikor nem is jelentkeztünk be. Ne kattintsunk az ilyen értesítésekben található linkekre; amennyiben ellenőrizni szeretnénk fiókunkat, írjuk be a webhely címét a böngészőbe, használjunk egy korábban elmentett könyvjelzőt, vagy mobilalkalmazáson keresztül jelentkezzünk be a fiókba.

Számítógépek vagy mobil eszközök

- Az antivírus szoftver riasztást küld arról, hogy rendszerünk fertőzött. Először is győződjünk meg arról, hogy valóban a víruskereső szoftver generálja a riasztást, és nem egy előugró ablak egy webhelyről, ami arra igyekszik rávenni minket, hogy felhívjunk egy telefonszámot, vagy telepítsünk egy programot. Amennyiben elbizonytalanodtunk, nyissuk meg az antivírus és ellenőrizzük, hogy a számítógép ténylegesen fertőzött-e.
- Megjelenik egy felugró ablak, amely azt állítja, hogy a számítógépünk titkosítva van, és váltságdíjat kell fizetnünk a fájlok helyreállításáért.
- Az alkalmazások véletlenszerűen leállnak vagy nagyon lassan töltődnek be.
- Böngészés közben a böngésző gyakran olyan oldalakra irányít minket, amelyeket nem is akartunk meglátogatni, vagy új, nem kívánt oldalak jelennek meg.

Pénzügyi

- Olyan gyanús vagy ismeretlen terheléseket találunk a bankszámlakivonatunkon, amelyekről tudjuk, hogy nem mi kezdeményeztük.

Mit tegyünk ilyenkor? - Szerezzük vissza az irányítást

Ha úgy véljük, feltörték egy fiókunkat, maradjunk nyugodtak, túl fogunk jutni rajta. Ha mindez munkahellyel kapcsolatos, ne próbáljuk meg egyedül megoldani a problémát, azonnal jelentsük azt. Ha személyes rendszerről vagy fiókról van szó, kövessük az alábbi tanácsokat:

- **Online fiókok helyreállítása:** Amennyiben még hozzáférünk a fiókhoz, lépjünk be egy megbízható, általunk vírusmentesnek tartott számítógépről, és cseréljünk jelszót! Amint bejelentkeztünk, állítsunk be egy új, egyedi és erős jelszót – minél hosszabb, annál jobb. Ne feledkezzünk meg arról, hogy minden egyes fiókunkhoz különböző jelszót használjunk! Ha már nem tudjuk észben tartani a jelszavainkat, javasolt egy jelszókezelő program használata. Továbbá, ha lehetséges, engedélyezzük a többlépcsős hitelesítést (MFA), így biztosítva, hogy a számítógépes támadók ne léphessenek be újra a fiókunkba. Amennyiben már nem férünk hozzá a fiókhoz, vegyük fel a kapcsolatot az adott oldal üzemeltetőjével és jelezzük, hogy átvették tőlünk a fiók irányítását!
- **Számítógép és egyéb eszközök helyreállítása:** Ha a vírusirtó nem képes megszüntetni a fertőzést számítógépünkön, vagy szeretnénk biztosra menni a rendszer biztonságát illetően, inkább telepítsük újra az operációs rendszert! Ez gyakran azzal jár, hogy törölni vagy cserélni kell a merevlemezt, ezt követően lehet újrainstallálni és frissíteni az operációs rendszert. Ne telepítsük újra az operációs rendszert biztonsági mentésből! A biztonsági mentést csak személyes fájlok helyreállítására célszerű használni. Ha nem vagyunk biztosak abban, hogy hogyan kell elvégezni az újratelepítést, fontoljuk meg, hogy egy szakszervíz segítségét kérjük. Ha a számítógép vagy eszköz már elég régi, lehet, hogy itt az idő újat vásárolni.
- **Pénzügyi fiókok helyreállítása:** Hitelkártyánkkal vagy bármilyen pénzügyi számlával kapcsolatos probléma esetén azonnal hívjuk bankunkat vagy a hitelkártya kibocsátóját! Kizárólag hivatalos, megbízható telefonszámon keresztül próbáljuk meg elérni őket, például a bankkártya hátoldalán feltüntetett vagy a számlalevelekre nyomtatott telefonszámon, vagy látogassunk el a weboldalukra. Folyamatosan kísérjük figyelemmel bank- vagy hitelkártya-kimutatásainkat! Mindezek mellett, ilyenkor célszerű lehet az érintett számlák befagyasztása is.

Ha anyagi kárt ért bennünket, vagy bármilyen módon fenyegetettnek érzzük magunkat, jelentsük az esetet a helyi bűnüldöző szerveknek!

A szerzőről

Maxim Deweerdt (Twitter @alfasec) a SANS Intézet oktatója, főleg kibervédelmi tanfolyamokat vezet. Emellett az NVISO főtanácsadójaként fenyegetés detektálással, incidenskezeléssel és SOC érettségi projektekkel foglalkozik.

Források

A frissítés ereje: : https://www.sans.org/security-awareness-training/resources/power-updating
Biztonsági mentések: https://www.sans.org/security-awareness-training/resources/got-backups
Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Zsarolóvírusok: https://www.sans.org/security-awareness-training/resources/ransomware
Azonosítólopások bejelentése: https://www.identitytheft.gov
Hitelszámla befagyasztás https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)