OUCH! 2023. november

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Feltörték a fiókomat. Mit tegyek most?

Lehet, hogy meghackeltek?

Sokaknak nehéz lépést tartani az Internet folyton változó világával és az újabbnál újbb technológiákkal. Akármilyen óvatosak is vagyunk, előbb vagy utóbb mi is könnyen áldozatul eshetünk egy hackertámadásnak. Minél hamarabb felismerjük, hogy valami nincs rendben, és minél hamarabb reagálunk rá, annál könnyebben tudjuk minimalizálni az okozott kárt. Alább olyan ismertetőjeleket mutatunk be, amelyek arra utalnak, hogy hackertámadás áldozatává váltunk.

Nyomok, amik arra utalnak, hogy meghackelték egy online fiókunkat.

- Családunk vagy barátaink szokatlan üzeneteket vagy például meghívókat kapnak tőlünk, amelyekről tudjuk, hogy nem mi küldtük őket.
- A jelszavunk nem működik, pedig biztosra vesszük, hogy jót adunk meg.
- Belépésről szóló emlékeztetőket kapunk különböző webhelyekről, amikor nem is jelentkeztünk be.
- E-mail értesítést kapunk az online profilunkkal kapcsolatos változásokról vagy azok megerősítéséről (például e-mail cím vagy jelszó csere), amelyeket nem mi kezdeményeztünk.

Arra utaló nyomok, hogy feltörhették a számítógépünket vagy mobilunkat.

- Az antivírus szoftver riasztást küld arról, hogy rendszerünk fertőzött. Először is győződjünk meg arról, hogy valóban a víruskereső 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 programot, és ellenőrizzük, hogy a számítógép valóban fertőzött-e!
- Böngészés közben a böngésző gyakran olyan oldalakra irányít minket, amelyeket nem is akartunk meglátogatni, vagy új, nem kívánt oldalak jelennek meg.
- Egy felugró ablak jelenik meg, amely azt állítja, hogy a számítógépünk titkosítva van, és váltságdíjat kell fizetnünk a fájlok helyreállításáért.

Ismérvek, amik arra utalnak, hogy megszerezték a bankkártya adatainkat, vagy feltörték a mobilbankunkat.

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

Mit tegyünk ilyenkor? - Szerezzük vissza az irányítást!

Ha azt gyanítjuk, hogy hackertámadás áldozatai lettünk, maradjunk nyugodtak! Meg fogjuk tudni oldani. Ha mindez

munkahellyel kapcsolatos, ne próbáljuk meg egyedül megoldani a problémát! Jelentsük minél előbb az illetékes kollégák számára! Ha magánhasználatú rendszerről vagy fiókról van szó, kövessük az alábbi tanácsokat::

- **Online fiókok helyreállítása:** Ha még működik a jelszavunk, jelentkezzünk be egy olyan számítógépről, amit biztonságosnak tartunk (feltételezzük, hogy nem fertőzött), és változtassuk meg a jelszót! Lehetőleg egyedi, eddig sehol máshol nem használt jelszót állítsunk be – minél hosszabb a jelszó, annál jobb! Ha még nincs a fiókon kétfaktoros azonosítás (2FA) beállítva, akkor ez egy jó alkalom arra, hogy ezt megtegyük. Amennyiben már nem tudunk bejelentkezni a fiókba, vegyük fel a kapcsolatot az adott oldal üzemeltetőjével, és jelezzük, hogy átvették tőlünk a fiók irányítását! Ha van olyan fiók, amelyiken ugyanezt a feltört jelszót használjuk, annál is azonnal cseréljünk jelszót!
- **Számítógép és egyéb eszközök helyreállítása:** Ha a vírusirtó nem képes megszüntetni a fertőzést a számítógépünkön, vagy szeretnénk biztosra menni a rendszer biztonságát illetően, inkább telepítsük újra az operációs rendszert! Ha az eszköz már elég régi, lehet, hogy itt az ideje újat vásárolni.
- **Pénzügyi hatás:** Hitelkártyánkkal vagy bármilyen pénzügyi számlával kapcsolatos probléma esetén azonnal hívjuk bankunkat vagy a hitelkártya kibocsátóját. Minél hamarabb értesítjük a pénzintézetet, annál valószínűbb, hogy vissza tudják szerezni a pénzünket. Mindig a hivatalos, megbízható telefonszámon keresztül próbáljuk meg elérni a bankot, például a bankkártya hátoldalán feltüntetett, vagy a számlalevelekre nyomtatott telefonszámon, vagy keressünk rá a weboldalukra! Folyamatosan kísérjük figyelemmel bank- vagy hitelkártya-kimutatásainkat. Ha lehetséges, állítsunk be automatikus értesítést minden pénzügyi tranzakcióról, minden terhelésről és utalásról!

Mit tehetünk, hogy megelőzzük a kibertámadásokat?

Az OUCH havonta megjelenő biztonsági hírlevele pontosan arról szól, hogy hogyan biztosítsuk be magunkat a kibertérben. Lentebb az „erőforrások” szekcióban felsoroljuk a személyes kiberbiztonsággal kapcsolatos legfontosabb OUCH hírleveleket. Ezek az anyagok három fő lépésre fókuszálnak.:

1. Tartsuk minden rendszerünket és eszközünket naprakészen, a legfrissebb szoftver verziók telepítésével!
2. Használjunk erős és egyedi jelszavakat minden egyes fiókunkhoz, vagy használhatunk valamilyen jelszókezelő szolgáltatást! Ahol lehet, kapcsoljuk be a kétfaktoros hitelesítést!
3. Legyünk egy kicsit szkeptikusak – figyeljük olyan átverési módszerekre, mint az adathalász e-mailek!

A szerzőről

Sarah Morales (@SarahManley) a Google Privacy, Safety és Security csapatának szenior programmenedzsere. A külső kapcsolatokért felel, közösségépítéssel, együttműködési és partner kapcsolatok kialakításával a fókuszban. Emellett a Wicys igazgatósági tagja és aktívan támogatja a DEI törekvéseit a kiberbiztonsági közösségben.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
2FA: Egy egyszerű lépés fiókjaink biztonságossá tételéért: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Érzelmi triggerek – Így csapnak be minket a kibertámadók: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Egyre trükkösebbek az adathalász támadások: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

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