OUCH! 2023. március

OUCH!

SANS SECURITY AWARENESS

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Digitális „tavaszi nagytakarítás”, 7 egyszerű lépésben

Áttekintés

Gyakran halljuk a „tavaszi nagytakarítás” kifejezést, amely az évnek azon időszaka, amikor a közelgő nyárra készülve átnézzük holmijainkat, rendszerezzük a háztartásunkat és az életünket. Ez egy tökéletes alkalom digitális életünk éves áttekintésére is. A következőkben bemutatunk 7 egyszerű lépést, amelyeket évi egy alkalommal elvégezve máris sokat tehetünk azért, hogy biztonságosan hozhassuk ki a legtöbbet a technológia által kínált lehetőségekből.

FELHASZNÁLÓI FIÓKOK: Nézzük át minden egyes felhasználói fiókunkat! Ha minden fiókunkhoz megfelelően hosszú, egyedi jelszót használunk, azzal biztosítani tudjuk, hogy az egyik fiók feltörése esetén a többi továbbra is biztonságban maradjon. Nehéz fejben tartani az összes jelszót? Semmi gond, ezzel más is így van. Ezért javasolt a jelszókezelők használata, amelyekben biztonságosan tárolhatjuk a jelszavainkat, és egyúttal egyszerűbbé is teszik az életünket. Ahol csak lehet, engedélyezzük a kétfaktoros azonosítást (2FA), különösképp a személyes vagy banki fiókjainknál! Ez a lehető legfontosabb lépés, amit csak tehetünk online fiókjaink biztonsága érdekében. Ha esetleg van olyan felhasználói fiók, amire több mint egy éve nem jelentkeztünk be, akkor itt az idő törölni azt.

PROGRAMOK: Eszközeink és szoftvereink naprakészen tartásával kihasználhatjuk a legújabb biztonsági funkciókat, miközben az ismerté vált sérülékenységek is javításra kerülnek. Ennek a legegyszerűbb módja, ha engedélyezzük az automatikus frissítések futtatását a számítógépünkön, mobilkészülékeinken, illetve minden egyéb otthoni okoseszközünkön. Töröljünk minden olyan programot vagy alkalmazást a mobilkészülékeinkről és személyi számítógépeinkről, amit nem használunk! Egyes applikációk tárhelyigényesek, sérülékenységeket rejthetnek magukban és még le is lassíthatják a rendszert. Minél kevesebb alkalmazásunk van, annál biztonságosabb a rendszerünk, és ezáltal az adataink. Sok eszközön meg tudjuk nézni, hogy mennyi idő telt el mióta utoljára használtunk egy adott appot. Ha már egy éve nem nyitottunk meg egy alkalmazást, arra jó eséllyel nincs is szükségünk.

PÉNZÜGYEK Győződjünk meg arról, hogy a bankszámlánk, hitelkártya és nyugdíj-takarékszámlánk úgy legyen beállítva, hogy tranzakciók – különösen a nagy összegű vásárlások, vagy átutalások – esetén kapjunk figyelmeztetést. Ha értesítést kapunk a tranzakciókról, könnyebben vesszük észre a csalást vagy a jogosulatlan tevékenységet. Minél hamarabb sikerül kiszúrni a csalásokat, annál hamarabb leszünk képesek megállítani azokat és visszaszerezni a pénzünket. Csalás esetén az egyik leghatékonyabb lépés, amit tehetünk, a folyószámla letiltása, ami országtól függően érhető el.

SELEJTEZÉS: Idővel azon kaphatjuk magunkat, hogy egyre több olyan eszközünk gyűlt össze, amelyekre valójában már nincs is szükségünk – például régi okostelefonok vagy okosotthoni eszközök. Mielőtt kidobnánk ezeket az eszközöket, mindenképpen töröljünk le róluk minden személyes információt! A legtöbb készülék már rendelkezik beépített törlési funkcióval, amivel selejtezés előtt biztonságosan törölhetjük az eszközön tárolt személyes adatainkat (vagy visszaállíthatjuk az alapértelmezett gyári beállításokat).

BIZTONSÁGI MENTÉSEK Nem számít mennyire vagyunk biztonságtudatosak, nagyon valószínű, hogy egyszer szükségünk lesz biztonsági mentésere ahhoz, hogy visszaállíthassuk a számunkra fontos adatokat. Érdemes úgy beállítani az eszközt, hogy automatikus mentéseket készítsen a felhőbe. A biztonsági mentések ütemezése lehetővé teszi legfontosabb adataink visszaállítását.

SZÜLŐI FELÜGYELET: Szülőként vizsgáljuk felül a gyermekekre vonatkozó felügyeleti beállításokat is, hiszen a gyermekek is idősödnek, elképzelhető, hogy időszerűvé vált a beállítások módosítása..

KÖZÖSSÉGI MÉDIA: Tekintsük át a közösségi média fiókunk adatvédelmi beállításait is, hiszen ezek a személyes információk aranybányái. Ellenőrizzük, hogy nem hozunk-e nyilvánosságra érzékeny adatokat, mint például a születésnapunk, telefonszámunk, lakcímünk, bankkártya adataink vagy éppen tartózkodási helyünk a megosztott fotóinkon.

Ha csak minden évben pár órát ezekre a lépésekre fordítunk, máris sokat tettünk eszközeink és személyes információink védelméért.

A szerzőről

Ritu Gill (@OSINTtechniques) a SANS fejlesztő oktatója, hírszerzési elemző, aki a nyílt forrású információszerzésre (OSINT) specializálódott. Rituról bővebb információ itt https://www.sans.org/profiles/ritu-gill és itt érhető el https://www.osinttechniques.com.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
A frissítés ereje: https://www.sans.org/security-awareness-training/resources/power-updating/
Így szabaduljunk meg a mobilkészülékeinktől: https://www.sans.org/newsletters/ouch/disposing-mobile-devices/
Rendelkezünk biztonsági: https://www.sans.org/newsletters/ouch/backups/
Online biztonság gyermekeknek: https://www.sans.org/newsletters/ouch/online-security-kids/

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