Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

A generációs szakadék áthidalása

Áttekintés

A mai technológiák biztonságos használata mindannyiunk számára okozhat nehézségeket, ám az olyan családtagok számára, akik nincsenek hozzászokva a technológiához, mindez különösen nagy kihívás jelenthet. Emiatt szeretnénk megosztani néhány kulcsfontosságú jó gyakorlatot, hogy segítsünk megvédeni azon családtagokat, akik esetleg küzdenek a technológiával, és félreérthetik a használatával járó kockázatokat.

Koncentráljunk az alapokra

Mások védelmét gyakran azzal segítjük elő a legjobban, ha a biztonságot a lehető legegyszerűbbé tesszük számukra. Koncentráljunk azokra a lépésekre, amelyekkel a legnagyobb hatást tudjuk elérni.

1. **Pszichológiai manipuláció:** A pszichológiai manipuláció az egyik legalapvetőbb támadási forma, ami legtöbbünket érinthet. Magyarázzuk el, hogyan dolgoznak a csalók és a szélhámosok évezredek óta, és hogy az egyetlen különbség most az, hogy a rosszfiúk az Internetet használják arra, hogy becsapjanak bennünket. Hozzunk fel konkrét példákat, mint az adathalász e-mailek, amelyek olyanok, mintha a banktól érkeztek volna, a hamis csomagértesítők, illetve az olyan csalók, akik technikai támogatásnak vagy kormányzati szervnek adják ki magukat. Győződjünk meg arról, hogy a családtagok megértették: nem szabad másnak megadniuk jelszavaikat, személyes – például hitelkártya adataikat – vagy hozzáférést engedniük a számítógépükhöz. Emlékeztessük őket: minél sürgetőbb egy üzenet, annál valószínűbb, hogy támadásról van szó. Léteznek olyan bűnözők, akik a gyengédségre vágyó szeretteinket próbálják kihasználni, és álmaik párjának adják ki magukat. Végül, tudatosítsuk szeretteinkben, hogy ha kényelmetlenül érzik magukat, esetleg kérdésük lenne egy emailről vagy telefonhívásról, akkor először hozzánk forduljanak.
2. **Otthoni Wi-Fi Hálózat:** Bizonyosodjunk meg arról, hogy szeretteink otthoni Wi-Fi hálózata jelszóval védett, és az alapértelmezett rendszergazdai jelszó megváltoztatásra került. Fontoljuk meg a Wi-Fi hálózat konfigurálását biztonságos DNS használatával, például az ingyenesen használható https://www.opendns.com segítségével. A biztonságos DNS-szolgáltatások nem csupán a fertőzött weboldalak ellen nyújthatnak védelmet, általuk azt is meghatározhatjuk, hogy mely weboldalak lehetnek meglátogathatóak és melyek nem. Mindez különösen fontos lehet a gyermekekre nézve.
3. **Frissítés:** Hangsúlyozzuk, hogy a rendszerek, szoftverek és eszközök naprakészen tartása sokkal nehezebbé teszi a bűnözők számára, hogy eszközeinket kompromittálhassák. Ennek biztosításának legegyszerűbb módja az automatikus frissítés engedélyezése mindehol, ahol az lehetséges.

Amennyiben olyan régi eszközzel vagy rendszerrel rendelkezünk, amit már nem lehet frissíteni, azt javasolt lecserélni egy újabbra, amelyhez még érkeznek frissítések.

4. **Jelszavak:** Az erős és biztonságos jelszavak használata a kulcs az eszközeink és fiókjaink védelméhez. Beszéljük át családtagjainkkal, miként alkothatnak megfelelően hosszú jelmondatokat. A jelmondatok használata és megjegyzése lehet a legegyszerűbb a számukra. Egy másik ötlet egy jelszókezelő szoftver telepítése, valamint használatának megtanítása. Ez lehetővé teheti szeretteink számára, hogy az Internetet egyszerűen és biztonságosan használhassák, hiszen csupán egyetlen jelszóra kell emlékezniük a jelszótároló feloldásához. Az adott szoftvertől függően akár mi is elvégezhetjük helyettük az adminisztrációt távolról. Ha ez nem működik, akkor kérjük meg őket arra, hogy írják be jelszavaikat egy könyvbe, majd tárolják azt egy kényelmes és biztonságos helyen. Bármely kritikus online fiókokhoz – például bankszámlákhoz – érdemes kétlépcsős azonosítást is beállítani. Bizonyosodjunk meg arról, hogy az online fiókok tekintetében is rendelkezünk örökítési tervvel, ugyanúgy mint a materiális javak esetében.
5. **Biztonsági mentések:** Ha minden más kudarcot vall, a mentések még megoldást jelenthetnek. Győződjünk meg arról, hogy a családtagok rendelkeznek egyszerű, megbízható biztonsági mentéssel. Sokak számára gyakran a felhőalapú megoldások jelentik a legegyszerűbb megoldást.

Ha úgy érzi a biztonsági intézkedések családtagjai számára túlságosan leterhelőek, segítsen nekik azáltal, hogy csak az alapokra összpontosít, és a lehető legegyszerűbben kezeli a biztonságot. Emellett legyünk türelmesek, adjunk időt és teret a hibák elkövetésére, azonban segítsünk másoknak abban, hogy ezeket ne ismételjék meg. Végül fontoljuk meg a SANS OUCH! hírlevélre történő feliratkozásukat.

A szerzőről

Chris Dale (Twitter @chrisadale) egy európai biztonsági tanácsadó cég, a River Security egyik főtanácsadója és tanúsított SANS oktató (https://www.sans.org/profiles/chris-dale/).
Chris a LinkedInen: https://www.linkedin.com/in/chrisad/

Források

Pszichológiai Manipuláció: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Jelszókezelők: https://www.sans.org/security-awareness-training/resources/password-managers-0
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
Digitális öröklés: https://www.sans.org/security-awareness-training/resources/digital-inheritance

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