1 ÖN MAGUNK VÉDELME
A kiberbűnözők tudják, hogy legkényebbé úgy tudnak megszerezni valamit, ha elérkik azt lőveink. Ilyen esetekre a jól szervezett és félreítve védekezés. Ha egy üzenet vagy egy telefonhívás túl csábítónak vagy gyakran tőkők, akkor az valószínűleg átverés, mint az alábbi példákban is:

Az adatadás email-eket azért küldik, hogy az adatadat megnyisa az abban lévő kéros szoftverrel fertőzött csatornánnyi vagy fertőzött weboldalra mutató hivatkozást. Az ilyen email-ek nagyon csáblik lehető, mert látszólagos barátok vagy egy, az adatát átadta a szerverezettél érkezik, Elfordít, hogy a kiberbűnözők a közösségi oldalról szereznek olyan információkat, amelyeket felhasználnak az adatadási támadáshoz.

Telefonhívás érkezik az internetes szolgáltató úgyfeljegyződata nevében. Azt állítják, hogy a számítógépünk fertőzött, pedig a hívő csak egy kiberbűnöző, aki hozzáférést akar szerezni a rendszertünk, vagy egy harmis antivírus szoftver akár eladni.

2 AZ OTTHONI HÁLÓZAT VÉDELME
A Wi-Fi router (más néven Wi-Fi Access Point - AP) egy fizikai eszköz, amely szabályozni tudja, hogy ki férhet hozzá az otthoni Wi-Fi hálózathoz.

Változtassuk meg a gyártás beállított adminisztrátoriaknul, és lehetőleg egy erős, bonyolult jelszót válasszunk!

Ügy állítsa be a Wi-Fi router, hogy jelszót kérjen a csatlakozásokor! Ezen kívül érdemes mindig a legjobb titkosítási módszert (ez jelen esetben az WPA2) beállítani alapértelmezettének.

Legyünk tisztában azzal, hogy milyen eszközök csatlakoznak a Wi-Fi hálózatunkhoz (lapok, okostelefon, játékkonzol, TV, és akár az autó is).

3 SZÁMÍTÓGÉPEK ÉS ESZKÖZÖK VÉDELME
Az alábbiakban segítünk megvédni a Wi-Fi hálózatra csatlakozott eszközöket:

Győződjünk meg arról, hogy minden eszközét erős jelszót vagy PIN kód véd, valamint a lepőjeléből szoftvert futtatjuk!

Ha van rá lehetőség, legtöbb két számítógép legyen otthon: egy a szükségek, egy a gyerekeinknek! Ha együtt számítógépen kell oszlozni, akkor mindenknél legyen saját felhasználói főjöv, és a gyerek ne kapjon rendszergazdai jogokat!

A számítógépeken mindig legyen naprakész vírusirtó és tőzfal program, és ezek folyamatosan fussenek!

Mielőtt lecsérélünk egy számítógépet vagy egy hordozható eszközt, mindig törljük le róla minden személyes adatait, mobil telefonokat ezt egyszerűen megoldhatjuk a készülékeknél alapeltető állásával (ilyen adatok visszaállítása).

4 FELHASZNÁLÓI FIÓKOK BIZTONSÁGA ÉS JELSZAVAK
Elfordítható, hogy nagyon sok online felhasználó fiókhoz és számítógéphez/mobil eszközökhez kell megjegyeznünk jelszavakat. Az alábbi tanácsok ezek védelmélben segíthetnek:

Hasznájunk hosszú jelszavakat, amelyeket nehez kitalálni! Ha lehetőség van rá, akár használhatunk egész mondatokat is (jelmondat, például „Hol van a kávézm?”).

Ha nem tudunk annyit jelszót fejlenkenni, akkor használjunk jelszókezelő programokat, amely biztonságos módon, titkosítva kapcsoló azokat!

Használjunk különböző használati, amikor lehetőség van rá! Az ilyen esetekben mindig elég a jelszó ahhoz, hogy bejelentkezünk a felhasználó fiókba, mert szükség van egy másodlagos kódra is, amit például a telefonra küldhet a szolgáltató!

Köszönés ölelet a családokért, amit nyugodtan vallátban foglalkozunk, mert elfordítunk, hogy a szülőknél vagy kollégánknál is létejük azokat!

5 MIT TEGYÜNK, HA MEGTÖRTÉNT A BAJ?
Nem számít, mennyit foglalkozunk a biztonságiunkkal, bár látóképpen lehet áldozat.

Remintsenken készítsünk biztonsági mentőt az adatankról! Ha feljebb a számítógépünket vagy mobil eszközünket, akkor lehet, hogy csak a biztonsági másolatunkból tudunk visszaszerezni fontos személyes dologkat.

Ha feltörtünk valamilyen online felhasználói fióknak, akkor azonnal lépjünk bele, és egy erős, egyedi jelszóra cseréljük a jelentős használatot!

Amennyiben nem tudunk belépni, akkor vegyük fel a kapcsolatot a szolgáltatóval!

Köszönsük nyomon a bankkártyáinkat forgalmát! Ha olyan tranzakciókat látunk, amelyet nem kívánunk az esetében, vegyük fel a kapcsolatot a bankunkkal!

A POSZTERRŐL
A Poszter egy közösség kezdeményezése, amelynek a létrehozásában az alábbi biztonsági szakemberek működték közre:


© SANS Institute - You are free to print, distribute and post as many copies as you like; the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingshuman.org/resources/posters