Az 5 legfontosabb lépés a biztonságos otthoni munka érdekében

Tudjuk, hogy az otthonról végzett munka néhányunknak újdonság lehet, talán nyomasztó, ahogy az új környezethez kell alkalmazkodni. Az egyik célunk lehetővé tenni, hogy a lehető legbiztonságosabban dolgozhassanak otthonról. Alább öt egyszerű lépész ismerhetnek meg a biztonságos munkavégzéshez. A legjobb ezekben a lépésekben, hogy nem csak a munkát teszik biztonságosabbá, hanem az ön és családja számára is növelik otthona kiberbiztonságát.

Ön: Az első és legfontosabb, hogy a technológia önmagában nem képes megvédeni – ön a legjobb védelem. A támadók megtanulták, hogy céljaikat legkönnyebben úgy érik el, ha önt veszik célba, nem pedig a számítógépét vagy egyéb eszközét. Ha a jelszavát, a munkahelyi adatait vagy a számítógépe irányítását akarják megszerezni, megpróbálják önt rászedni, hogy megadja nekik, gyakran a sürgősség érzetét keltve. Például felhívhatják önt, a Microsoft műszaki támogatásának adva ki magukat, azt állítva, hogy a számítógépe megfertőződött. Vagy esetleg e-mailben küldenek figyelmeztetést, hogy egy csomagot nem lehetett kézbesíteni, így becsapva önt, hogy egy rosszindulatú hivatkozásra kattintson. A pszichológiai manipulációs támadások leggyakoribb jelei:

- Nagyon sürgető érzést keltenek, gyakran félelem, megfélemlítés, válsághelyzet, esetleg fontos határidő formájában. A kibertámadók meggyőző üzeneteket képesek összerakni, amelyek úgy tűnnek, mintha megbízható szervezettől érkeztek volna, például bankoktól, kormányzati vagy nemzetközi szervektől.
- Nyomásgyakorlás, hogy megkerülje vagy figyelmen kívül hagyja a szabályokat vagy eljárásokat, vagy olyan ajánlat, ami túl szép, hogy igaz legyen (nem, nem nyert a lottón)!
- Baráttól vagy munkatárstól érkező üzenet, amelyben az aláírása, hangneme vagy szövegezése mégsem úgy hangzik mintha tőlük származna.

Végső soron ön a legjobb védelem ezen támadások ellen.

Otthoni hálózat: Majdnem minden otthoni hálózat egy vezeték nélküli (más néven Wi-Fi) hálózattal indul. Ez teszi lehetővé, hogy eszközeivel az internetre csatlakozzon. A legtöbb otthoni vezeték nélküli hálózatot az internetes router vagy egy különálló, erre szolgáló vezeték nélküli hozzáférési pont vezérli. Mindkettő ugyanúgy működik: vezeték nélküli jeleket bocsátanak ki, amire az otthoni eszközök csatlakozhatnak. Ez azt jelenti, hogy a vezeték nélküli hálózat biztonságossá tétele otthona védelmének kulcsfontosságú része. Az alábbi lépéseket javasoljuk a biztonsághoz:

- Változtassa meg a vezeték nélküli hálózatot irányító eszköz alapértelmezett adminisztrátori jelszavát. Az adminisztrátori fiók teszi lehetővé, hogy a vezeték nélküli hálózat beállításait megváltoztassa.
- Győződjön meg róla, hogy csak olyanok csatlakozhatnak a vezeték nélküli hálózatához, akikben megbízik. Ezt az erős biztonság bekapcsolásával érheti el. Ezt bekapcsolva mindenkinek jelszóra lesz szüksége, hogy a vezeték nélküli hálózathoz csatlakozhassanak, és miután csatlakoztak, az online tevékenységük titkosított.
- Győződjön meg róla, hogy a vezeték nélküli hálózathoz használt jelszó erős, és nem azonos az adminisztrátori jelszóval. Ne feledje, csak egyszer kell megadnia a jelszót minden egyes eszközön, mivel azok eltárolják és megjegyzik a jelszót.

Nem biztos benne, hogyan tegye meg ezeket a lépéseket? Kérdezze meg internetszolgáltatóját, nézze meg a weboldalukat, olvassa el a vezeték nélküli hozzáférési ponthoz kapott dokumentációt vagy a gyártó weboldalát.

Jelszavak: Ha egy weboldal azt kéri öntől, hozzon létre egy jelszót: találjon ki erős jelszót, minél több karakter szerepel benne, annál erősebb. Egy jelmondat használata a legjobb módja, hogy biztosítsa az erős jelszavát. A jelmondat nem más, mint egy több szóból álló jelszó, mint például *„hangya eper bourbon.”* Az egyedi jelmondat azt jelenti, hogy minden eszközhöz és online fiókhoz különbözőt használ. Így ha az egyik jelmondata kompromittálódik, a többi fiókja és eszköze még biztonságban marad. Nem tud minden jelszót fejben tartani?

Használjon jelszókezelőt, ami olyan speciális program, amely biztonságosan tárolja az összes jelmondatát titkosított formában (és még számos más remek szolgáltatást is kínál!). Végül, alkalmazza a kétlépcsős azonosítást (más néven két- vagy többfaktoros hitelesítést) amikor csak lehetséges. Ez az ön jelszavát használja, de mellette egy második lépést is, például az okostelefonjára küldött kódot vagy alkalmazást, amely kódot generál önnek. A kétlépcsős azonosítás valószínűleg a legfontosabb lépés, amit megtehet online fiókjainak védelméért, és sokkal könnyebb használni, mint gondolná.

Frissítések: Győződjön meg róla, hogy minden számítógép, mobileszköz, program és alkalmazás a legfrissebb változatot használja. A kibertámadók folyamatosan keresik az új sebezhetőségeket az ön által is használt szoftverekben és eszközökben. Ha sebezhetőséget találnak, speciális programokkal kihasználják, és feltörik az ön által használt eszközöket. Eközben az adott eszközhöz a szoftvert készítő cég a frissítések kiadásával keményen dolgozik rajta, hogy kijavítsa. Ha gondoskodik róla, hogy a számítógépeire és mobileszközeire azonnal telepítve legyenek ezek a frissítések, jelentősen megnehezíti, hogy bárki feltörje azokat. Hogy naprakész maradjon, egyszerűen csak kapcsolja be az automatikus frissítéseket, amikor lehetséges. Ez a szabály vonatkozik szinte minden, a hálózatra csatlakozó technológiára, beleértve nem csak a munkával kapcsolatos eszközeit, hanem az internetre csatlakozó TV-t, bébiőrt, biztonsági kamerákat, otthoni routert, játékkonzolokat vagy akár az autót.

Gyerekek / vendégek: Ha valami miatt nem kell aggódnia a munkahelyén, akkor az, hogy a gyerekek, vendégek vagy egyéb családtagok használják az ön laptopját vagy egyéb munkával kapcsolatos eszközét. Győződjön meg róla, hogy a családja és a barátai megértik: nem használhatják az ön munkaeszközeit, mivel véletlenül törölhetnek vagy módosíthatnak rajta adatokat, vagy ami még rosszabb, véletlenül megfertőzhetik az eszközt.