

OUCH!

A Havi Biztonsági Tudatosságról szóló hírlevele

Kiberbiztonságos otthon

Áttekintés

Néhány évvel ezelőtt egy otthoni hálózat kiépítése nem állt másból, mint egy vezeték nélküli router és néhány számítógép telepítéséből. Mivel manapság sokan dolgozunk, tartunk kapcsolatot vagy tanulunk otthonról, nagyobb figyelmet kell szentelnünk egy erős, kiberbiztonságos otthon létrehozására. Ebben segít a következő négy egyszerű lépés.

Az Ön vezeték nélküli hálózata

Szinte minden otthoni hálózat kiépítése egy vezeték nélküli (vagy Wi-Fi) router üzembehelyezésével kezdődik. Ez teszi lehetővé, hogy eszközei csatlakozzanak az Internethez. A legtöbb otthoni vezeték nélküli hálózatot az internetes router, vagy egy külön, dedikált vezeték nélküli hozzáférési pont vezérel. Mindkét eszköz hasonló módon működik: vezeték nélküli jeleket sugároznak, amelyek lehetővé teszik az otthoni eszközök számára, hogy csatlakozzanak az internethez. Ez azt jelenti, hogy a vezeték nélküli hálózat biztonságossá tétele kulcsfontosságú otthonának védelme szempontjából. A következő lépéseket javasoljuk a biztonság növelése érdekében.

- Változtassa meg az otthoni hálózatot vezérlő router, vagy a vezeték nélküli hozzáférési pont alapértelmezett adminisztrátori jelszavát. Az adminisztrátori felhasználói fiókkal lehet a vezeték nélküli hálózat beállításait módosítani.
- Bizonyosodjon meg arról, hogy csak azok az eszközök csatlakozhatnak a vezeték nélküli hálózathoz, amelyekben Ön megbízik. Ezt erős védelmi beállítások alkalmazásával érheti el. A kapcsolódáshoz használjon jelszót és titkosítsa online tevékenységét a kapcsolat létrejötte után.
- Győződjön meg arról, hogy a csatlakozáshoz megfelelően erős jelszót választott, amely különbözik az adminisztrátori jelszótól. Ne feledje, hogy ezt a jelszót csak egyszer szükséges megadnia minden csatlakoztatott eszköz esetén, mivel azok emlékezni fognak rá.

Ha nem biztos benne, hogyan kell végrehajtani ezeket a lépéseket, ellenőrizze internet szolgáltatójának, vagy az eszköz gyártójának weboldalát.

Jelszavak

Használjon erős, egyedi jelszót minden eszközhöz és online felhasználói fiókjához. A hangsúly itt az **erősön** és az **egyedin** van. Minél hosszabb a jelszava, annál erősebbnek számít. Próbálja meg könnyen megjegyezhető szavak sorozatát használni, például **napsütés-fánk-boldog**.

Az egyedi jelszó azt jelenti, hogy más-más jelszót használ minden eszközhöz és felhasználói fiókjához. Az erős jelszavak megjegyzése érdekében használjon jelszókezelőt, azaz egy olyan megbízható programot, amely biztonságosan tárolja összes jelszavát egy titkosított, virtuális széfben.

Ezenkívül, ahol csak lehet, engedélyezze a kétlépcsős azonosítást, különösen az online felhasználói fiókok esetében. Ez a jelszavát használja, de hozzáad egy második lépést is, például egy okostelefonra küldött, vagy alkalmazás által generált kódot. Valószínűleg ez a legfontosabb lépés, amit megtehet, ráadásul sokkal könnyebb, mint azt gondolná.

Az Ön eszközei

A következő lépés annak feltérképezése, hogy milyen eszközök csatlakoznak a vezeték nélküli otthoni hálózatához, majd ezen eszközök megbízhatóságának és biztonságosságának ellenőrzése. Ez régebben, amikor csak egy számítógéppel rendelkezett, egyszerű volt. Napjainkban azonban szinte bármilyen eszköz képes csatlakozni az otthoni hálózatához, értve ezalatt az okostelefonokat, TV-ket, játékkonzolokat, babafigyelőket, nyomtatókat, hangszórókat vagy akár az autókat is. Miután azonosította az otthoni hálózatához csatlakoztatott összes eszközt, ellenőrizze le, hogy azok biztonságosak-e. A legjobb módszer erre az alapértelmezett jelszavak megváltoztatása, és lehetőség szerint az automatikus frissítés engedélyezése.

Biztonsági mentések

Időnként, függetlenül attól, hogy mennyire óvatos, előfordulhat, hogy feltörik a rendszerét. Ebben az esetben, gyakran az egyetlen út, hogy személyes adatait visszanyerje, a biztonsági mentésből történő helyreállítás. Bizonyosodjon meg róla, hogy rendszeresen készít biztonsági mentést a fontos adatokról és ellenőrizze le, hogy vissza is tudja-e állítani őket. A legtöbb mobil eszköz támogatja a felhőbe történő automatikus mentést. A legtöbb számítógép esetében előfordulhat, hogy meg kell vásárolnia bizonyos típusú adatmentő szoftvert vagy szolgáltatást, amelyek viszonylag olcsók és egyszerűen használhatók.

A szerzőről

Randy Marchany a Virginia Tech információbiztonsági vezetője. Randy a SANS egy tapasztalt instruktora, aki a SEC566 és a SEC440 (Kritikus Biztonsági Kontrollok -CIS- implementálása és auditálása) tanfolyamok oktatásáért felelős. **Kövesse Randy-t: @randymarchany.**



Források

Egyszerű jelszókezelés: <https://www.sans.org/security-awareness-training/resources/making-passwords-simple>

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>

Eszközök alapértelmezett jelszavai: <https://www.routerpasswords.com/>

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

OUCH! A Sans Security Awareness részleg által közzétett és a Creative Commons BY-NC-ND 4.0 licenz alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. Szerkesztette: Walter Scrivens, Phil Hoffman, Alan Wagoner, Cheryl Conley