

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Az otthoni Wi-Fi biztonságossá tétele

Áttekintés

Egy biztonságos otthoni hálózat létrehozásának első lépése a Wi-Fi hozzáférési pont (legtöbbször Wi-Fi router) biztonságossá tétele. Ez az eszköz határozza meg, hogy ki vagy mi csatlakozhat az otthoni hálózathoz. A következőkben bemutatott öt egyszerű lépés segítségével biztonságossá tehetjük otthoni Wi-Fi hálózatunkat.

Koncentráljunk az alapokra

A Wi-Fi eszköz konfigurálásához csupán csatlakoznunk kell az otthoni hálózathoz. A böngésző segítségével navigáljunk el az eszköz kézikönyvében megadott IP címre (például: <https://192.168.1.1>), vagy használjuk a gyártó által biztosított segédprogramot vagy appot.

1. **Változtassuk meg az admin jelszót:** A legtöbb Wi-Fi hozzáférési ponton egy alapértelmezett jelszóval érhetjük el az adminisztrátori fiókot, amelyen keresztül változtathatunk az eszköz beállításain. Ezek az előre beállított jelszavak azonban bárki számára ismertek lehetnek, akár az Interneten is közzétételre kerülhettek. Használjunk egyedi, erős jelszót az admin fiókhoz, hogy ehhez csak mi férhessünk hozzá. Amennyiben az eszköz lehetőséget biztosít rá, az admin fiók felhasználónevét is változtassuk meg.
2. **Hozzunk létre egy hálózati jelszót:** Állítsuk be a Wi-Fi hálózatot, amit szintén védjünk egyedi, erős jelszóval (ügyelve arra, hogy ez különbözzön az admin jelszótól). Ezáltal biztosíthatjuk, hogy csak azok képesek csatlakozni az otthoni hálózatunkhoz, akikben megbízunk. Fontoljuk meg egy jelszókezelő program használatát egy erős jelszó kiválasztásához és jelszavaink nyomon követéséhez.
3. **Firmware frissítés:** Engedélyezzük az automatikus frissítést a Wi-Fi hozzáférési pont firmware-én, azaz operációs rendszerén. Így biztosíthatjuk, hogy eszközünk a lehető legbiztonságosabb legyen, és rendelkezzen a legújabb biztonsági megoldásokkal. Ha az automatikus frissítés nem engedélyezhető, rendszeres időközönként lépünk be az eszközre és ellenőrizzük az elérhető frissítéseket. Ha az eszköz már nem rendelkezik gyártói támogatással, fontoljuk meg egy új készülék vásárlását, hogy rendelkezésre álljanak a legújabb biztonsági szolgáltatások.

4. **Használjunk vendéghálózatot:** A vendéghálózat egy virtuálisan elkülönített hálózat, amelyet a Wi-Fi hozzáférési ponton hozhatunk létre. Ez azt jelenti, hogy az eszközön valójában két hálózat létezik egy időben. Az *elsődleges* hálózat az, amelyhez a megbízható eszközeink csatlakoznak, például számítógépünk, okostelefonunk vagy tabletünk. A *vendég* hálózat pedig az, amelyhez a nem megbízható eszközök csatlakozhatnak, például látogatóink eszközei, vagy az otthoni okoseszközeink. A vendéghálózathoz csatlakozó eszközök nem láthatják az elsődleges hálózaton történő kommunikációt.
5. **Használjunk DNS szűrést:** A DNS egy internetes szolgáltatás, amely a weboldalak neveit fordítja le numerikus címekké. Ez az, ami biztosítja, hogy számítógépünk csatlakozni tud egy weboldalhoz, amelynek nevére rákeresünk. A Wi-Fi hozzáférési pontok általában az internetszolgáltató által biztosított, alapértelmezett DNS szervert használják, de több biztonságosabb ingyenes alternatíva is létezik, mint például az [OpenDNS](#), a [CloudFlare for Families](#) vagy a [Quad9](#), amelyek extra biztonságot nyújthatnak a nem biztonságos weboldalak blokkolásával. Lépünk be eszközünk menüjébe és változtassuk meg a DNS szerver beállítást egy biztonságosabb alternatívára.

Az otthoni Wi-Fi hozzáférési pont biztonsága az első és az egyik legfontosabb lépés a biztonságos otthoni hálózat létrehozásához. A Wi-Fi hozzáférési pont biztonságával kapcsolatos további információkért tekintsük át az eszköz kézikönyvét, vagy ha az internetszolgáltatónk biztosította a Wi-Fi eszközt, vegyük fel velük a kapcsolatot a biztonsági funkciókkal kapcsolatos további információkért.

A szerzőről

Joshua Wright (Twitter @joswr1ght) a Counter Hack Challenges, LLC igazgatója, illetve a NetWars és a Holiday Hack Challenge kiberversenyeinek koordinációját és fejlesztését vezeti. Josh a LinkedInen: <https://linkedin.com/in/joswr1ght>.



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>

OpenDNS beállítási tanácsok: <https://www.opendns.com/setupguide/#familyshield>

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, Les Ridout, Princess Young