

Hamis wifi-hálózat létrehozása (Evil twin phishing)

Ennél az elkövetési módnál a támadók egy ismert, legitim vezeték nélküli (WiFi) hozzáférési ponttal azonos nevű hamis hozzáférési pontot hoznak létre.

A támadók ezután ráveszik az áldozatokat, hogy csatlakozzanak rá az eszközükkel, majd megfigyelik, lehallgatják az óvatlanul a hálózatra csatlakozó felhasználók online forgalmát. Így érzékeny adatokhoz, például felhasználónevekhez és jelszavakhoz férhetnek hozzá.

A felhasználók gyakran észre sem veszik, hogy támadás áldozatául estek.

Mit tegyen?

- Kerülje a „nem biztonságos” -nak jelzett vezeték nélküli hálózatokat!
- Lehetőség szerint kerülje a nyilvános WiFi-hálózatokhoz való csatlakozást!
- Kizárólag saját mobilinternetet vagy megbízható (pl. otthoni) hálózatot használjon a webes böngészéshez, közösségi média használatához vagy banki ügyintézéshez!
- Ne használja a telefonja, eszköze „automatikus kapcsolódás WiFi-hálózatokhoz” funkcióját!
- Nyilvános WiFi-kapcsolat használatakor ne lépjen be olyan oldalra, ahol meg kell adnia felhasználónevét és jelszavát!
- Az autentikációt (hitelesítést) alkalmazó oldalak esetén használjon többfaktoros autentikációt – amennyiben van erre lehetőség!