DE IBK

Biztonságos kapcsolattartás a nyaralás alatt is – az eSIM kockázatai

Külföldi utazásaink során – különösen, ha más régióba készülünk – a szolgáltatók igen magas roaming díjat számolhatnak fel a külföldi mobilinternetezésért, ráadásul közel sem biztos, hogy ugyanolyan minőségű lesz ott is a hazai szolgáltatók lefedettsége, mint itthon. Ugyan kézenfekvő ötletlen tűnhet ilyenkor a helyi éttermek, kávézók és szállodák által biztosított ingyenes Wi-Fi hálózatok használata, de inkább ne tegyük!

Az ingyenes Wi-Fi hálózatokra hitelesítés nélkül bárki felcsatlakozhat, beleértve a kiberbűnözőket is, ráadásul komoly biztonsági kockázatoknak teszik ki eszközeinket és adatainkat azáltal, hogy nem titkosítják a rajtuk átmenő adatokat. Több támadási módszer is igyekszik kihasználni az „ingyen Wi-Fi” vagy „Free Wi-Fi” kiírások vonzerejét, például a Wi-Fi Pineapple-lel végrehajtott támadások vagy az ún. Evil Twin Phishing, amikor a támadók egy ismert és legitim Wi-Fi hálózattal azonos nevű, hamis Wi-Fi hálózatot hoznak létre, majd lehallgatják a hálózatra csatlakozó gyanútlan felhasználók internetes forgalmát, így jutva érzékeny információkhoz, például bejelentkezési adatokhoz.

Hogy elkerüljük az ingyen Wi-Fi kockázatait és a magas roaming díjakat, érdemes lehet megfontolni az egyre népszerűbb eSIM használatát.

- *Fontos megjegyezni, hogy ezen technológiával még nem kompatibilis minden eszköz, ezért mielőtt az eSIM használata mellett döntünk érdemes ellenőrizni, hogy készülékünk támogatja-e azt egyáltalán.*

Mi az eSIM?

A beágyazott előfizetői azonosító modul (embedded subscriber identity module – eSIM), a hagyományos SIM kártyák egy új evolúciós változata, amelyet szabványügyi testületek és technikai vállalatok fejlesztettek ki.

Az eSIM lehetővé teszi az eszközök számára, hogy fizikai SIM kártya nélkül csatlakozzanak a különböző mobilszolgáltatók hálózataihoz. A hagyományos SIM-kártyákkal ellentétben az eSIM közvetlenül az eszköz hardverébe van beágyazva, így nincs szükség fizikai kártyára, ráadásul kezelésük (pl.: aktiválás, deaktiválás, profilváltás) is digitálisan történik.

eSIM használatának előnyei

- **Kényelem:** eSIM használatával nincs szükség a fizikai kártyák cserélgetésére, ha szolgáltatót szeretnénk váltani, ugyanis a csomagaktiválás és a szolgáltatóváltás is általában egy alkalmazáson vagy online felületen keresztül történik. Továbbá egyszerűbben vásárolható és aktiválható külföldre utazáskor, így nem csupán a szolgáltatónk személyes felkeresésének idejét spórolhatjuk meg, hanem a magas roaming díjakat is elkerülhetjük.

- **Rugalmasság:** Könnyen váltogathatunk a szolgáltatók között, ráadásul egyetlen chipen több szolgáltató profilját is tárolhatjuk.

- **Biztonság:** Fizikai kártya hiányában, nehezebb elhagyni vagy klónozni magát a SIM kártyát, ráadásul azokban az okoseszközökben, ahol a készülék feloldása, illetve a tranzakciók biometrikus (pl.: arc-vagy ujjlenyomat) azonosításhoz kötöttek nehezebb az eSIM-ekhez való rosszindulatú hozzáférés, továbbá az ilyen eszközökben titkosítással is védhetők az eSIM előfizetői profilokhoz tartozó érzékeny adatok.

eSIM használatának kockázatai

Mint mindennek, az eSIM használatának is megvannak a maga velejáró kockázatai. Míg fizikai társa hardveres és szoftveres támadásoknak is ki van téve, addig az eSIM-et jellemzően szoftveres támadások fenyegetik.

- **eSIM swapping:** Az eSIM-csere során a támadó megszerzi az áldozat adatait, majd jogosulatlanul kéri a szolgáltatónál az eSIM cseréjét, hogy saját készülékén aktiválja a profilt, ami a kapcsolat elvesztését okozza; emellett Simjacker típusú speciális SMS-ekkel is visszaélhet, amelyek rejtett parancsokat futtatva profilok törlését, személyazonosság-lopást, csalást, kártékony kód terjesztését vagy megfigyelést tesznek lehetővé, főleg ott, ahol nincs biometrikus védelem vagy titkosított kommunikáció.

- **Memory exhaustion:** A memóriakimerítés során a támadó addig tölti tele az eSIM chip memóriáját, például visszaigazolások megakadályozásával, amíg „árva” profildarabok maradnak, amelyekhez nincs aktív szolgáltató és nem törölhetők. Ismételt támadással a memória teljesen betelik, a készülék működésképtelenné válik, nem állítható helyre, és a támadás szinte nyom nélkül zajlik, mert csak egy elveszett üzenet utal rá.

- **Undersizing memory:** A támadó egy feltört vagy rosszindulatú SM-SR komponenssel hamis memóriaadatot küld a szolgáltatónak, például nullára állítja a szabad kapacitást, így a rendszer azt hiszi, hogy nincs hely új profilnak, ezért nem indul telepítés. Ez főleg régebbi készülékeken maradhat észrevétlen, és nem hagy közvetlen bizonyítékot maga után.

- **Inflated profile:** Ennél a módszernél egy feltört SM-DP vagy rosszindulatú szolgáltató szándékosan túl nagy méretű profilt telepít az eSIM-re, hogy elfoglalja a memóriát, és megakadályozza más szolgáltatók profiljainak létrehozását. Gyakori változata, amikor kevés helyet hagynak szabadon, ami már nem elég új profilhoz, így a készülék működőnek tűnik, de valójában nem bővíthető.

- **Locking profile:** A profilzárolás során egy szolgáltató szándékosan olyan szabályt állít be a profilban (például a *CannotBeDisabled* opciót), amely végleg a készüléket a saját hálózatához köti, és megakadályozza a profil törlését vagy letiltását. Ha ilyen profilt telepítenek, a többi profil automatikusan inaktiválódik, nem törölhető, a zárolás 4G hálózaton visszafordíthatatlan, és a módszert akár piaci vagy állami célból is kihasználhatják.

- **Protocol attacks:** Protokolltámadások során a támadó egy kártékony app-ot vagy fertőzött alkalmazást telepíttet a felhasználóval, amely rootolt eszközökön teljes hozzáférést szerezhet, például speciális protokollparancsokkal (APDU) kiolvashatja a biztonsági fájlokat és PIN-kódokat, így lehetővé válik a hálózat lehallgatása, személyes adatok ellopása vagy közbeékelődéses támadás indítása.

- Támadások a szolgáltatók és az ellátási láncok ellen: Ezek a támadások közvetlenül a mobilszolgáltatókat, fejlesztőket vagy beszállítókat célozzák, hogy bizalmas forráskódokhoz jussanak, kártékony folyamatokat építsenek be, vagy legitim app-okat fertőzzenek meg, ami bizalomvesztést, kártékony szoftverek terjedését és érzékeny adatok kiszivárgását okozhatja.

  Az eSIM-ről és az eSIM használatából eredő kockázatokról bővebb információ érhető el az ENISA által kiadott összefoglalóban.

Biztonságos eSIM használat

- Kizárólag jól ismert, megbízható szolgáltatónál váltsunk eSIM csomagot!

- eSIM alkalmazást csak hivatalos alkalmazásboltokból töltsünk le!

- Amennyiben lehet, kerüljük az appon belüli vásárlásokat! Ha előfizetői csomagunkat mégis az alkalmazáson belül kell kiegyenlítenünk, használjunk egy külön erre a célra használt virtuális bankkártyát!

- Mindig ellenőrizzük az alkalmazások hozzáféréseit, kövessük a legkisebb jogosultság elvét és tiltsuk az alkalmazások működéséhez nem szükséges funkciókat!

- Használjunk erős jelszavakat fiókjaink védelme érdekében és amennyiben módunkban áll, alkalmazzunk kétfaktoros azonosítást (2FA).

- Okoseszközeink zárolásának feloldásához, valamint a tranzakciók megerősítéséhez használjunk biometrikus (pl.: arc vagy ujjlenyomat) azonosítást!

- Tartsuk naprakészen eszközeinket azáltal, hogy rendszerese frissítünk!