



Nyáron sokat vagyunk távol az otthonunktól – kávézók, szórakozóhelyek, repterek és külföldi szálláshelyek kínálják a hálózatukat. Mi pedig azonnal csatlakozunk, hiszen haza kell szólni, hogy rendben megérkeztünk, fotókat posztolunk, és információkat gyűjtünk. Csakhogy mindez nem veszélytelen...

INGYENES WIFIRŐL NETEZIK?

Egy átlagos egyhetes nyaralás során körülbelül 100-120 között van az internetes kereséseink száma. A legtöbbször nem mobilnetet használnak, hanem a szállásuk wifihálózatát, az étteremét, ahol épp vacsoráznak, vagy a közterületen elérhető nyilvános szolgáltató adta lehetőségeket.

– A nyilvános wifipontokhoz csatlakozva rengeteg adat juthat a hálózatokat rendszeresen monitorozó kiberbűnözőkhöz, és ha a felhasználó nem elég körültekintő, akkor könnyen áldozattá

válhat – mondja **Csizmazia-Darab István**, a Sicontact Kft. IT-biztonsági szakértője. – A publikus wifin zajló adatforgalom lehallgatásához a bűnözők részéről különösebb szakértelem sem kell, elég egy csali hotspot üzemeltetése, vagy akár csak egy egyszerű böngésző kiegészítő használata. A titkosítatlan wifihálózat látogatóitól a támadók igen könnyen lophatnak adatokat, jelszavakat, akár a teljes netes forgalmat rögzíthetik. A naplózott adatok birtokában követni

lehet, hogy mely weboldalakat látogattunk meg, és illetéktelenek láthatják a teljes levélforgalmunkat is.

Mi okozza a bajt?

Statistikák szerint a kártékony kódok legtöbbször valamilyen ellenőrizetlen letöltés, illetve telepítés útján kerülnek a gépünkre, így emiatt érdemes alaposan utánanézni, milyen programokat engedélyezünk. A legfontosabb, hogy minden eszközünkön használjunk vírusirtót. Ez alól az androidos tablet és a telefon sem ki-

vétel, ahogy számítógép esetében a Macintosh vagy a Linux sem sebezhetetlen. Érdemes olyan vírusvédelmi szoftvert alkalmazni, amely nemcsak a kártékony kódokat képes szűrni, de fejlett lopásvédelemmel is bír.

Mire figyeljünk?

Nyitott wifit csak általános böngészésre használjunk: hírolvasásra, időjárás-előrejelzés megtekintésére, programok keresésére.

– Hasznos óvatosság, ha étterem, kávézó, iskola, könyvtár nyitott wifijével nem lépünk be jel-

szóval védett fiókjainkba, innen nem bankolunk, és nem indítunk semmiféle vásárlást – hangsúlyozza a szakértő. – Emellett érdemes elolvasni a használat szabályait is, mert óvatlanságunk nagyon kellemetlen és sok pénzbe kerülő szituációt teremthet. Például külföldi komputázás esetén előfordulhat, hogy a hajótársaság saját műholdas szolgáltatást üzemeltet, amelynek tarifája kiemelten magas, így akár több százezer forintunk is bánhatja, ha innen netezünk.

P. N.



Csizmazia-Darab István, a Sicontact Kft. IT-biztonsági szakértője.

– A publikus wifin zajló adatforgalom lehallgatásához a bűnözők részéről különösebb szakértelem sem kell, elég egy csali hotspot üzemeltetése, vagy akár csak egy egyszerű böngésző kiegészítő használata. A titkosítatlan wifihálózat látogatóitól a támadók igen könnyen lophatnak adatokat, jelszavakat, akár a teljes netes forgalmat rögzíthetik. A naplózott adatok birtokában követni

5 MEGFONTOLANDÓ TANÁCS

1 Legyünk gyanakvók!

A személyzet segítségével ellenőrizzük, hogy a hálózat neve valódi. Győződjünk meg arról, hogy készülékünk adatmegosztási funkcióit kikapcsoltuk. Ha a szállásunk internetes kapcsolata azt kéri, hogy frissítsunk egy szoftvert a kapcsolódás érdekében, gyanakodjunk, és azonnal kapcsolódjunk le a hálózatról, illetve jelentsük szállásadónknak. Győződjünk meg róla, hogy eszközeink a legfrissebb operáci-

ós rendszer fut, és mielőtt útra kelünk, még itthon frissítsük alkalmazásainkat.

2 Zárjuk el a készülékét!

Soha ne hagyjuk felügyelet nélkül eszközeinket nyilvános helyen vagy kocsiban, amíg strandolunk. Ha van rá lehetőség, mindig tegyük a széfbe.

3 Ellenőrizzük alkalmazásainkat!

Kapcsoljuk ki a wifi- és a bluetooth-elérést alkalmazásainkban, amikor épp nem használjuk őket.

4 Maradjunk biztonság tudatosak!

Használjunk az oldalakhoz (Gmail, Facebook stb.) erős, egyedi (hosszú és bonyolult) jelszavakat. Ha zárván változtassuk meg őket.

5 Irtuk a vírust!

Ha nem tudjuk elkerülni a nyilvános hálózatok használatát, akkor alkalmazzunk VPN (Virtual Private Network) megoldást, hogy kommunikációnk titkos maradjon, és adataink ne kerüljenek illetéktelen kezekbe.