DE IBK

IT biztonsági tippek nyárra

Rendkívül fontos, hogy a nyaralási szezonban is kellő figyelmet szükséges fordítani az IKT eszközök és alkalmazások védelmére, valamint a biztonságtudatos magatartásra, ezért javasolt az alább leírtakat megfogadni.

1. Csak biztonságos Wi-Fi hálózatokat használj, és az automatikus csatlakozási lehetőséget kapcsold ki!

- Szinte már-már közhely, hogy a nyilvános, nem biztonságos Wi-Fi hálózatok kockázatot jelenthetnek. Gyakorlatilag bárki csatlakozhat egy ilyen hálózathoz, beleértve a rosszindulatú hackereket és csalókat is, akiknek viszont a felhasználó adataira és pénzére fáj a foga.
- Az egyik módja annak, hogy ez ne történhessen meg, az az, hogy kerülni kell a nyilvános Wi-Fi hálózatok használatát, különösen, ha azok nem rendelkeznek például jelszavas védelemmel. Mindezek mellett a szállodai Wi-Fi hálózatra sem a legjobb ötlet felcsatlakozni, főleg ha a felhasználónév és jelszó páros egy mindenki által jól látható és könnyen elérhető helyen van kifüggesztve.
- Ha mégis csatlakozunk egy nyilvános Wi-Fi hálózathoz: soha, de tényleg soha ne lépjünk be pl. a netbankunkba, vagy egyéb érzékeny személyes információkat kezelő felületre!

2. Keresd a HTTPS-t!

- Ha egy weboldal HTTP protokollt használ, akkor az nem a legjobb előjel, ugyanis az ilyen oldalak nem képesek megvédeni a továbbított információkat.
- A HTTPS – bár HTTP kapcsolatot jelöl – viszont a titkosításra támaszkodik, annak érdekében, hogy a támadók ne tudják a webhely és látogatóik között továbbított adatokat megismerni.
- Annak ellenőrzése, hogy a meglátogatott webhely HTTPS-t használ-e, nagyon egyszerű: elég egy gyors pillantást vetni a címsorra. A HTTP-weboldalakon a „Nem biztonságos” megjelölés jelenik meg, míg a HTTPS-weboldalakon az URL-cím mellett egy lakat ikon látható.
- Szóval csak olyan oldalakat keress fel, amelyek rendelkeznek biztonsági tanúsítvánnyal.

3. Kapcsold be az MFA-t!

- Online fiókjaid és a támadók közé további biztonsági rétegek „felhúzása” sosem rossz ötlet. Ezért érdemes engedélyezned és konfigurálnod a kétfaktoros (2FA), vagy többfaktoros hitelesítést (MFA) a fiókjaidon.
- Többféle MFA-típus is elérhető, ezért válaszd a legmagasabb biztonsági szintet nyújtó típust, például biometrikus, fizikai biztonsági kulcsot vagy hitelesítő alkalmazásokat.
- Ne feledd, a biztonsági ellenőrző kérdések gyakran hátrányt jelenthetnek, mivel a social engineering segítségével relatív könnyen kijátszhatók, ezért használatuk MFA-ként nem javasolt.

4. Használj jelszókezelőt!

- Nem árulunk el nagy titkot, hogy az emberek többsége nem szereti a jelszavakat, főleg nem szereti őket megjegyezni. Ezért hajlamosak lehetünk több fiókhoz is ugyanazt a jelszót használni (tisztelet a kivételnek), ami nem túl jó és nem túl biztonságos.
- A legkézenfekvőbb megoldás, ha minden fiókhoz más jelszót használtok. Na és ebben lehet segítségetekre egy-egy jelszókezelő, vagy jelszószéf.
- A jelszómenedzserek segítségével az összes jelszót és jelszókifejezést egyetlen biztonságos helyre teheted, és egy univerzális, ún. mesterjelszóval védheted, vagyis csak ezzel a mesterjelszóval férsz hozzá a többihez.

5. Kapcsolj ki és frissíts!

- Amennyiben nem használod, akkor érdemes kikapcsolni a Wi-Fi és Bluetooth kapcsolatokat, és minden egyéb szolgáltatást is tilts le az eszközeiden, amelyeket az adott időszakban nem használsz (ezért még az eszközöd aksija is hálás lesz).
- Ami ennél is fontosabb: győződj meg arról, hogy eszközeid és alkalmazásaid naprakészek-e, vagyis rendelkeznek-e a legfrissebb biztonsági javításokkal, frissítésekkel.
- És tényleg kapcsolódj ki! Ne posztolj a nyaralás alatt (ráér utána is). Ne tegyél közzé semmi olyan információt, ami megkönnyíti a bűnözők dolgát.