DE IBK

Így ismerhetjük fel a gyanús linkeket

Sokszor elmondjuk, hogy az üzenetekben érkező webes hivatkozásokkal legyünk óvatosak, inkább ne kattintsunk rá a kicsit is gyanúsnak tűnő linkekre. De mitől számít gyanúsnak egy link?

- tipikus csalási témák, amiket messziről fel lehet ismerni

Bizonyos témájú kéretlen üzeneteknél egyből gyanakodhatunk. Például, ha az üzenet látszólag **banktól**, egy **közmű- vagy streaming szolgáltatótól** érkezett, és linket tartalmaz. Az ilyen üzeneteknél mindig keressünk rá külön a szolgáltató weboldalára!

- Elírások a webcímben

Sok esetben a csaló weboldalakat a webcímben találhat tartománynév (domain) alapján is fel tudjuk ismerni, mert hasonlítanak az eredeti domainhez, attól csupán néhány karakterben térnek el. Az alábbi hivatkozás például nagyon hasonlít az OTP Bank hivatalos webcímére (**https://www.otpbank.hu/**), épp csak egy „a” betű hiányzik belőle:

Van, hogy egy támadó által készített káros webcím attól válik megtévesztővé, hogy szerepel benne egy valós domain név (pl: google.com), csak éppen nem a megfelelő helyen.

Előfordul, hogy olyan szándékos elírás szerepel egy webcímben, ami a *homográfiát* (a karakterek írásmódjának hasonlóságát) használja ki. Például a **gov[.]hu** helyett **qov[.]**hu (a „g” helyett „q” betű) szerepel a linkben.

Kattintás előtt mindig nézzük meg alaposan az URL-t!

- **Rövidített linkek**

A rövidített linkek (mint például: **https://tinyurl.com/8nv2paaf**) ún. URL rövidítő (shortner) szolgáltatással kerülnek formázásra, ezek nem önálló webhelyek, csupán átirányítást végeznek a megadott webcímre. Számos ilyen online szolgáltatás érhető el, a legismertebb talán a **bit.ly**, illetve a **tiny URL**. Hasznos eszköz a hosszú hivatkozások lerövidítésére, így azok átláthatóbbak, kezelhetőbbek, “elegánsabbak”. Ugyanakkor jó ha tudjuk, hogy a kiberbűnözők is előszeretettel használják ezeket a szolgáltatásokat arra, hogy a káros weboldaluk címét elrejtsék a biztonsági szoftvereink elől.

Ezeket a rövidített URL-eket ki lehet bontani, meg lehet tekinteni az eredeti URL-t, például a CheckURL nevű online eszköz segítségével. Nincs más dolgunk, mint átmásolni a rövidített URL-t, majd a “Long URL” résznél láthatjuk az eredeti webcímet. Ne kattintsunk rövidített hivatkozásra anélkül, hogy nem ellenőriztük, hogy az milyen webcímre irányít át!

- Gyanús URL-ek ellenőrzése

  Nem csupán az e-mailben érkező hiperlinkekkel kell óvatosnak lenni, hanem például **blogokon, fórumbejegyzésekben**, **közösségi oldalak kommentjeiben** posztolt hivatkozásokkal is. Ha mindenképp kíváncsiak vagyunk egy webes tartalomra, kattintás előtt legalább egy-két online URL ellenőrzővel vizsgáljuk meg a hivatkozást!

  Erre jó megoldás a VirusTotal, ám emellett számos további hasonló webes szolgáltatás érhető el, ilyenek például:

  - Google Safe Browsing
  - urlscan.io
  - Talos Reputation Lookup
  - Sucuri SiteCheck

  Ha piros jelzést látunk az ellenőrzés eredményei között, inkább ne kattintsunk!