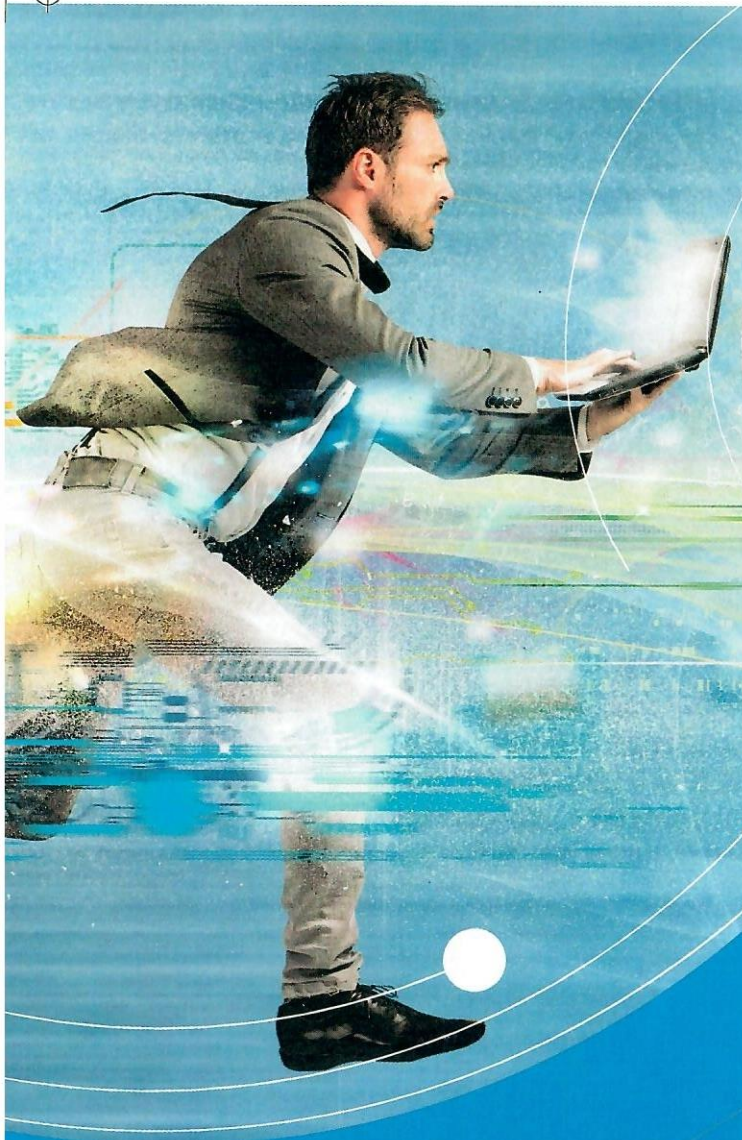


NEMZETI
KIBERVÉDELMI INTÉZET
GOVCERT

Az adatvédelem minden felhasználó alapvető érdeke, ezért a Nemzeti Kibervédelmi Intézet (NKI) az állami kibervédelem támogatásán, fenntartásán és fokozottabb működtetésén túl az egyéni felhasználók tudatosítására is egyre nagyobb hangsúlyt helyez.

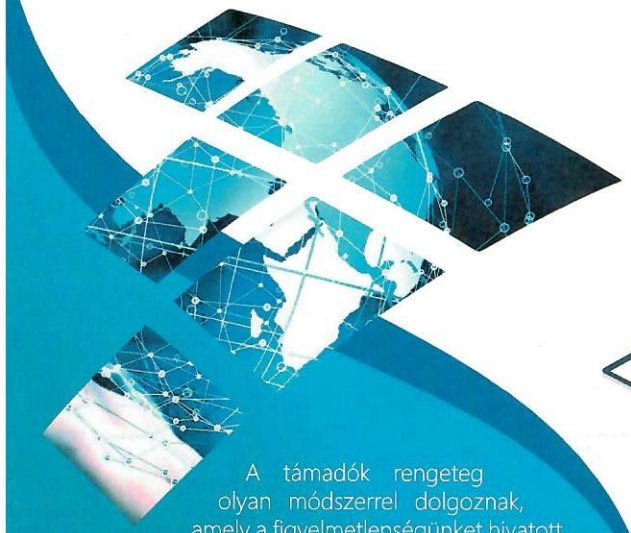
Az NKI célja, hogy az IT biztonságot érintő tematikus tájékoztatói segítségével a lehető legtöbb hasznos információt jutassa el a felhasználók részére.

Nemzeti Kibervédelmi Intézet
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu

Biztonságos internet használat

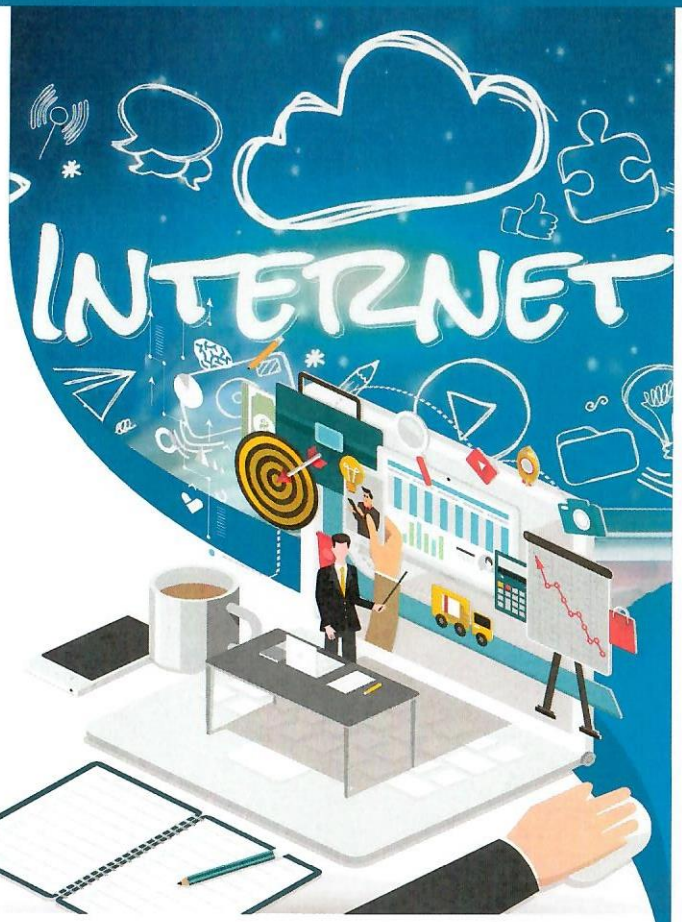
Készült a Nemzeti Kibervédelmi Intézet megbízásából, az Ön informatikai egészségének megőrzése érdekében.

Biztonságos internet-használat



A támadók rengeteg olyan módszerrel dolgoznak, amely a figyelmetlenségünket hivatott kihasználni: ilyenek az álweboldalakat és hamis e-mail-eket felhasználó támadások is. Ennek során a cél az, hogy átirányítsanak minket egy támadó weboldalra, vagy rávegyenek bennünket arra, hogy egy kártékony programot letöltve futtassuk azt számítógépünkön. E módszerek segítségével megszerezhetik hozzáférési adatainkat.

A támadók sokszor visszaélnek informatikai jártasságunk hiányával, és ezt kihasználva próbálnak minket befolyásolni. Sok támadás alapul a megfélemlítésen, illetve azon, hogy a támadók a támadást gyakran technikai folyamatnak próbálják álcázni (pl.: szoftverfrissítés).



Mit is jelent ez a hétköznapokban?

A mindennapok során mind a munkában, mind a magánéletben gyakran használunk online felületeket. Az ügyintézéstől az e-bank-on át a közösségi oldalakig szinte minden oldalon azonosítanunk kell magunkat a felhasználónevünkkel és jelszavunkkal.

Ahhoz, hogy ezek a hozzáféréseink biztonságosak legyenek, ismernünk kell mind a számítógépünkre leselkedő, mind az online felületeket érintő sebezhetőségeket.

Hogyan védekezzünk?!

A biztonságos internethasználat lényege, hogy ismerjük a ránk leselkedő veszélyeket, és próbáljuk meg elkerülni azokat. Az alábbi elveket követve a támadások többségét könnyen elkerülhetjük:

Weboldalakon való bejelentkezés előtt mindig ellenőrizzük, hogy valóban a kért weboldalon tartózkodunk-e (pl.: nincs a címben elírás, cég.com helyett cég.co)!

Bejelentkezés előtt ellenőrizzük az oldal biztonsági tanúsítványát, a címsor mellett bal oldalt a kis lakat ikonra kattintva. Ha itt piros figyelmeztetést látunk, ne jelentkezzünk be az oldalon!

Különböző oldalakon való azonosításhoz használjunk különböző jelszavakat;

Ne töltsünk le felugró hirdetésekben szereplő szoftvereket és böngésző kiegészítőket (pl.: az internet sebességét növelő szoftver)!