

# ***BŰNMEGELŐZÉSI HÍRLEVÉL 2019. január***

## **BIZTONSÁGOS INTERNETHASZNÁLAT I.**



A technikai fejlődés következtében az internet a mindennapok része lett. Használatával könnyebbé, egyszerűbbé tehetjük életünket. A virtuális tér azonban valós veszélyeket is jelent. Digitálisan tárolt személyes és pénzügyi adataink megfelelő védelem hiányában illetéktelen személyekhez

kerülhetnek. Az elkövetők módszerei időről-időre változnak, de az ajánlott biztonsági intézkedések és magatartási szabályok tudatos betartásával jelentősen csökkenthetőek a felmerülő kockázatok.

### **BIZTONSÁGOS KÖRNYEZET**

A technikai megoldások, akár csak az otthonunk védelmében, jelentik az első lépcsőt. Gondoskodjunk arról, hogy a számítógépünk és az otthoni hálózatunk is biztonságos legyen. Ennek érdekében:

- Rendszeresen telepítse számítógépén az operációs rendszer és a felhasználói programok frissítéseit. Mobileszközein is frissítse az alkalmazásokat!
- A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt vírusirtó program telepítése és frissítése!
- Számítógépén a felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) a felhasználó engedélyére legyen szükség!
- Ne állítsa a böngésző biztonsági beállításait az „ajánlott” szint alá!
- Ismeretlen eredetű szoftvereket ne telepítsen!



### **TUDATOS INTERNETHASZNÁLAT**

A legjobb zár és riasztó sem ér semmit, ha a tulajdonos átadja a kulcsot és a kódot, vagy nyitva hagyja az ajtót és nem kapcsolja be a riasztót. Az interneten keresztül érkező veszélyek néhány egyszerű szabály betartásával elkerülhetőek:

- Csak ismerős feladó által küldött e-mail mellékletét nyissa meg!
- Soha ne adjon meg jelszót, PIN kódot e-mailben küldött kérésre!
- Belépéskor mindig gépelje be az URL címet, ne a kapott linkre kattintva lépjen be az oldalra!
- Online történő bankkártyás fizetésnél mindig győződjön meg arról, hogy valódi bank oldalon adja meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adja meg azokat!

· Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (https előtag) oldalon adjon meg!

### **ADATAINK FOKOZOTT VÉDELME**

Otthon az értékeink (készpénz, ékszer) védelmére további megoldásokat (értéktároló, széf) használunk. A digitálisan tárolt adataink védelme érdekében is fokozott körültekintéssel járunk el: egyrészt, hogy illetéktelen személyek ne férjenek hozzá, másrészt elvesztésük (pl. technikai probléma, szándékos károkozás) esetén is vissza tudjuk állítani őket:

· Ne adja meg senkinek felhasználói nevét és jelszavát!



- Közöségi oldalon ne legyen nyilvános a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- Csoportosítsa ismerőseit és ezáltal korlátozhatja, ki mit láthat!
- Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során ellenőrizze, hogy az oldal vagy alkalmazás

milyen személyes adatához fér hozzá. (születésnap, e-mail cím, ismerőseinek köre stb.)!

Szükség esetén módosíthatja az elérhető információk körét.

· Más által is használt számítógépen – ha befejezte az internet használatát – minden esetben jelentkezzon ki a közösségi oldalról, levelezéséből! A böngésző bezárása nem elegendő.

· Rendszeresen készítsen biztonsági másolatot fontos adatairól. Erre alkalmas lehet egy külső merevlemez, amit csak a biztonsági mentés idejére csatlakoztatunk a számítógéphez vagy olyan online tárhely, amely tárolja a fájlok korábbi verzióját is.

**100%-os biztonság nincs!**

**DE!**

**A biztonságos környezet megteremtésével, tudatos internethasználattal és adatainak fokozott védelmével biztonságosabbá tehetjük az internethasználatot.**

**Heves Megyei Rendőr-főkapitányság**

**Bűnmegelőzési Alosztály**

Általános segélyhívó: 112

Forrás: [www.police.hu](http://www.police.hu)

Képek forrása: internet