

BIZTONSÁGOS INTERNETHASZNÁLAT

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.

100%-OS BIZTONSÁG NINCS! DE!

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

A BIZTONSÁGOS KÖRNYEZET MEGTEREMTÉSE

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 **FRISSÍTÉSÉIT!** 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 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 BANKI OLDALON** adja meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adja meg azokat!
- Felhasználói nevet és jelszót **CSAK TANÚSÍTVÁNYNYAL** rendelkező (https előtag) oldalon adjon meg!

ADATAINK FOKOZOTT VÉDELME

Otthon az értékeink (késpénz, ékszer) védelmére további megoldásokat (értéktároló, széf) használunk. A **DIGITÁLISAN TÁROLT ADATAINK** védelme érdekében is fokozott körültekintéssel járjunk 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!

INTERNET TUDATOSAN

ONLINE IS BIZTONSÁGBAN

- Közöseti oldalon **NE LEGYEN** nyilvános a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- **CSOPORTOSÍTSA** ismerőseit és ezáltal korlátozhatja, hogy ki mit láthat!
- Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során **ELLENŐRIZZE**, hogy az oldal vagy alkalmazás milyen személyes adataához 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 **JELENTKEZZEN KI** a közösségi oldalról, levelezéséből! A böngésző bezárása nem elegendő.
- Rendszeresen **KÉSZÍTSEN** biztonsági másolatot fontos adataikról. 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.