

## 2. SZÁMÍTÓGÉPÜNK VÉDELME

Az internet használata során számos veszély fenyegeti a felhasználókat és számítógépeiket. Ezekkel szemben a megfelelő biztonsági intézkedésekkel és magatartási szabályok tudatos betartásával lehet védekezni.

### A SZÁMÍTÓGÉP MEGFELELŐ BEÁLLÍTÁSA

A **ROSSZINDULATÚ SZOFTVEREK ÉS HACKEREK** a számítógépen futó szoftverek (operációs rendszer és egyéb programok) biztonsági hibáit használják ki. A szoftverek gyártói az ismertté vált hibákat rendszeresen javítják, és a javításokat **FRISSÍTÉSEK KIADÁSÁVAL** juttatják el a felhasználókhoz. A frissítések kiadásával az addig esetleg nem nyilvános hibákról is tudomást szerezhetnek a rosszindulatú szoftvereket készítő és a hackerek, így azok a rendszerek, amelyeken a hibákat javító frissítés nem történt meg, fokozottan veszélyeztetettek lehetnek.

Az operációs rendszer **AUTOMATIKUS FRISSÍTÉSÉNEK** bekapcsolásával biztosítható, hogy a számítógép a frissítés közzétételét követő legrövidebb időn belül megkapja a biztonsági frissítéseket. A felhasználói programok jelentős része szintén jelzi, hogy újabb verzió elérhető, ezek telepítése is ajánlott a fenti okok miatt.

### VÍRUSIRTÓ PROGRAMOK

A vírusok (és egyéb kártékony programok) elleni védekezés céljából feltétlenül javasolt **VÍRUSIRTÓ PROGRAM TELEPÍTÉSE**.

A hagyományos vírusirtó programok adatbázisok alapján azonosítják a káros programokat. Az adatbázist a vírusirtó szoftver gyártója **RENDSZERESEN FRISSÍTI**, a frissítéseket a legtöbb vírusirtó szoftver automatikusan letölti az interneten keresztül. Ez a reaktív védelem.

A modern vírusirtó programok beépített **ELEMZŐ ALGORITMUSOK** segítségével – a programok tevékenységének elemzésével – azonosítják a vírusokat. (heurisztikus védelem) Mivel egy új vírus megjelenése után több nap is eltelhet, amíg a vírusirtó program gyártója frissíti az adatbázist, addig a reaktív vírusirtó nem nyújt védelmet. A heurisztikus módszereket is alkalmazó modern vírusirtók viszont addig is védelmet nyújtanak a legtöbb kártevő ellen, amíg a frissítés megtörténik.

## TŰZFAL

A tűzfal célja a privát (otthoni/vállalati) és a nyilvános (internet) **HÁLÓZAT ELKÜLÖNÍTÉSE**, továbbá annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.

**HARDVERES TŰZFAL:** valamilyen fizikai eszköz, ami a privát és a nyilvános hálózat között monitorozza és szabályozza a bejövő és kimenő hálózati forgalmat a beállított tűzfalszabályoknak megfelelően. Korlátozott tűzfalként alkalmazható egy otthoni router is, megfelelően beállítva kellő védelmet nyújthat a külső támadások ellen.

**SZOFTVERES TŰZFAL:** a tűzfal szoftver a számítógépen fut. (pl. Windows beépített tűzfala), és a számítógép bejövő és kimenő hálózati forgalmát monitorozza és szabályozza. Alkalmazása akkor indokolt különösen, ha a számítógép közvetlenül - nem routeren keresztül - csatlakozik az internethez.

## BIZTONSÁGI MENTÉS

**RENDSZERESEN** készítsünk biztonsági másolatot fontos adatainkról. 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. **ONLINE TÁRHELY** esetében azért fontos a fájl verziók korábbi eltárolása, mert, ha zsarolóvírus támadás éri a gépet, akkor az automatikus szinkronizációnak köszönhetően a titkosított fájlok kerülnek az online tárhelyre is, de a vírus eltávolítását követően a legutolsó ép verziók visszaállíthatóak.

## BIZTONSÁGI TANÁCSOK

- Kapcsolja be az operációs rendszer és a felhasználói programok **AUTOMAIKUS FRISSÍTÉSÉT!**
- A felhasználói fiókok felügyeletén állítsa be, hogy a kritikus műveletekhez (pl. program telepítése) a **FELHASZNÁLÓ ENGEDÉLYÉRE** legyen szükség!
- Állítsa magasabb szintre a **BÖNGÉSZŐK BIZTONSÁGI BEÁLLÍTÁSAIT!**
- **ISMERETLEN EREDETŰ** szoftvereket ne telepítsen!
- Használjon **VÍRUSIRTÓ** programot!
- Kapcsolja be a **TŰZFALAT** a számítógépén vagy a routeren!
- Rendszeresen készítsen **BIZTONSÁGI MENTÉST** fontos adatairól!

## TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN



[www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag](http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag)



[www.facebook.com/internettudatosan](https://www.facebook.com/internettudatosan)