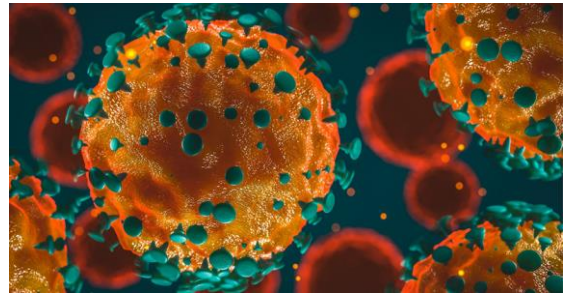


## Számítógép vírusok

A számítógép vírus olyan program, mely a gépre kerülve önmagát másolva szaporodik. Kárt tesz a számítógépen tárolt adatokban, vagy magában a számítógépben, illetve a számítógép és az egyes programok megfelelő működését is akadályozhatja.



## Honnan kaphatunk vírusokat?

Pendrivelről, internetről, vagy akár elektronikus levelekből.

## Hogyan ismerhetjük fel a vírusfertőzést?

Szokatlan, megmagyarázhatatlan események jelentkeznek.

- üzenetek megjelenése
  - gyakori lefagyások
  - a winchesteren a szabad helyek eltűnnek
  - tárolt adatok eltűnnek
  - tárolt adatokat letitkosítja a vírus és nem férünk hozzá
  - állományok méretének ok nélküli változása, stb.
  - a gép lassulása, nem megfelelő működése, különböző ablakok megjelenése
- 

## Fájl vírus:

A programok indítható állományait fertőzi többnyire. Ha a fertőzött állományt indítjuk, a vírus a memóriába kerül, s onnan tovább fertőzi a számítógép állományait. A vírus ebben az esetben csak akkor kerül a memóriába, ha indítunk egy fertőzött állományt. A gép megfelelő működését akadályozza.

## Boot vírus:

A sz. gép rendszerállományait fertőzi. A rendszerállományok minden egyes gépindításkor betöltődnek a memóriába (windows), így velük együtt a vírus is. Megfertőz minden használt állományt. Itt nincs esélyünk arra, hogy elkerüljük a vírus betöltődését a memóriába, mint az előző esetben, tehát a továbbfertőzés és egyéb galibák okozása elkerülhetetlen.

---

**A wormok**, vagy magyarul férgek e-mail-hez kapcsolódnak (csatolva), amit látszólag egy ismerőstől kapunk. A levél felhívja a figyelmet, hogy a lényeg a csatolt állományban van. A csatolt állomány megnyitáskor történik a fertőzés, amely során a vírus valamilyen módon rongálja a számítógépet. A vírus tovább küldi magát a címjegyzékben szereplő címekre is, vagy a kapott levelekre magától válaszokat küld, valami hasonló módon: "Megkaptam a leveled, én is küldök pár dokumentumot, kérlek, nézd meg őket!"

**Trójai programok**, amelyek valami másnak álcázzák magukat, ténylegesen használhatók valamire, de közben hozzáférhetővé teszik a gépet más számára, így azzal különböző visszaéléseket lehet tenni. Nem foglalkoznak direkt módon maguk terjesztésével, a programok

letöltésével ez úgyis megtörténik. A programok elindításával az vagy további vírust telepít a gépre, vagy valamilyen módon rongálja a gép tartalmát.

### **Hoax (Kacsa)**

A hoax (angol eredetű vándorszó, jelentése: „beugratás”, „megtévesztés”, „átverés”, „álhír” vagy „kacsa”) leggyakrabban az e-mailben terjedő álhírek, kacsa-láncclevelek különféle változatait jelöli, bár az átverés gyakran kiegészül honlapokkal. Nevezhetjük ártatlan tréfának is, de az elkövetőnek tudnia kell, hogy számos esetben nagyon vékony a határvonal a tréfa és a büntetendő cselekedet között. A számítógépes vírusok „automatikus” terjedésével ellentétben ez az emberi segítséget is igénybe veszi pl. („Küldd tovább 10 példányban!”). Nemzetközileg az internettel együtt terjedt el, minthogy a hálózat ideális terepe a kisebb-nagyobb átveréseknek. A népszerűbb hoaxok jelentős forgalmat generálhatnak, és ezzel komoly pluszköltségeket okozhatnak a szolgáltatóknak. A hoax írójának célja lehet, hogy a "szélnek eresztett" levél fejlécében rövid idő alatt rengeteg e-mail cím gyűlik össze, amelyek a levél többszörös továbbítása után hozzá is visszajutnak - így valós, működő címekhez juthat, melyeket értékesíthet a spammereknek (kéretlen levél, más néven levélszemét küldözgetőknek).

---

**Malware:** A számítógép működésére káros programok összefoglaló neve. Ide tartoznak a vírusok is.

**Spyware:** Kémprogram. Célja, hogy a felhasználó tudomása nélkül megszerezzék a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait.

**Tűzfal:** A számítógépre telepített tűzfal program nem védi a gépet a vírushatás ellen, nem jelzi a fertőzött fájlokkal való találkozást, mert nem ez a feladata. De a tűzfal az általa védett hálózat gépei között a háttérben észrevétlenül közlekedni próbáló vírusprogramok mozgását, behatolását megakadályozhatja. A tűzfal mellé víruspajzsra is szükség van a biztonsághoz.

---

### **A vírusok ellen vírusfigyelő, ill. irtó programokkal (víruspajzs) védekezhetünk.**

A vírusirtó programok adatbázisát rendszeresen frissíteni kell, hogy a legújabb vírusokat is felismerjék, és irtani tudják.

Vírusirtó programok pl.: NOD32, AVAST, VIRUSBUSTER, NORTON ANTIVIRUS, PANDA, KASPERSKY, MCAFEE

Windows defender (a Windows saját vírus pajzsa.)