

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 megfelelő működését is akadályozhatja.

Honnan kaphatunk vírusokat?

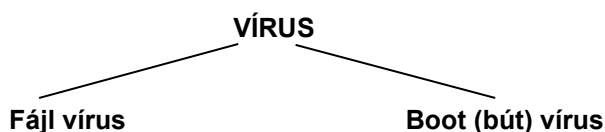
Bizonytalan eredetű lemezekről, pendrive-ról, **internetről**, vagy akár **elektronikus levelekből**.

Csak ismert, megbízható forrásokból származó lemezek tartalmát töltsük gépeinkre. Lehetőleg ellenőrizzük valamilyen vírusirtó programmal.

Hogyan ismerhetjük fel a vírusfertőzést?

Szokatlan, megmagyarázhatatlan események jelentkeznek.

- különös sosem látott üzenetek
- gyakori lefagyások
- tartalomjegyzék összekeveredése
- a winchesteren a szabad helyek eltűnnek
- 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 ott minden futtatott (azaz a memóriába betöltött) programot megfertőz. Ezek tovább fertőznek.

(A nem használt programjaink épen maradhatnak.)

A vírus ebben az esetben csak akkor kerül a memóriába, ha indítunk egy fertőzött állományt.

Boot vírus:

A sz. gép rendszerállományait fertőzi. A rendszerállományok minden egyes gépindításkor betöltődnek a memóriába, 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.

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 megnyitásakor 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 pl. egy jópofa animációnak. Nem foglalkoznak direkt módon maguk terjesztésével, a programok másolásával ez úgyis megtörténik. A programok elindításával az vagy vírust telepít a gépre, vagy valamilyen módon rongálja a winchester tartalmát.

Hoax (Kacsa)

A hoax (angol eredetű vándorszó, jelentése: „beugratás”, „megtévesztés”, „átverés”, „álhír” vagy „kacsa”) leggyakrabban az e-mailben terjedő álhírek, kacsa-lánclevelek 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 („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.

A vírusok ellen vírusfigyelő, ill. irtó programokkal védekezhetünk.

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

Vírusirtó programok pl.: Microsoft Security Essential, NOD32, AVAST, VIRUSBUSTER, NORTON ANTIVIRUS, PANDA, Windows defender

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.