**Információ technológiai biztonság alapjai:**

Ismertesse a hálózati biztonságot fenyegető külső és belső veszélyek alapvető jellemzőit!

Ismertesse a számítógépes károkozók legismertebb formáit (vírus, trójai, féreg, adware, spyware, spam)!

Hogyan lehet hatékonyan védekezni a kártékony szoftverek ellen?

Hogyan tudjuk biztonságosabbá tenni hálózati forgalmunkat?

Mi a jelentősége az operációsrendszer frissítéseknek, illetve a szoftver frissítéseknek?

* **Ismertesse a hálózati biztonságot fenyegető külső és belső veszélyek alapvető jellemzőit!**
  + Számítógépes veszélynek tekintünk minden olyan programot, ami ártó szándékkal készült, és fenyegeti a számítógép és a felhasználója biztonságát.
  + Mindkettő esetben a hálózatkezelés lelassul.
  + Felhasználók problémákat tapasztalnak.
* **Ismertesse a számítógépes károkozók legismertebb formáit (vírus, trójai, féreg, adware, spyware, spam)!**
  + Vírus:
    - Legrégebbi vírusforma, futtatható állományokhoz épül hozzá.
    - Akkor aktivizálódik amikor futtatjuk a vírus által fertőzött programot.
  + Trójai:
    - Mást kap a felhasználó, mint amit ígér a program.
    - Kívülről hasznos programnak látszik, esetleg valamilyen híres programnak adja ki magát.
    - Nem sokszorosítja magát, időzített bombaként viselkedik.
  + Féreg:
    - Felhasználók közreműködése nélkül terjed
    - Másolatokat terjeszt a hálózaton
    - Felemésztik a memóriát és a sávszélességet
  + Adware:
    - Freeware programok
    - Megjelennek a szponzorok, támogatók reklámjai
  + Spyware:
    - Kémprogramok, céljuk adatokat gyűjteni személyekről vagy szervezetekről.
    - Ellophatják bankszámla adatinkat, jelszavainkat, személyes adatainkat.
  + Spam:
    - Elárasztják az e-mail fiókunkat fölösleges levelekkel, ezzel terhelve az e-mail szolgáltatást, és feltöltve a fiókunk tárhelyét.
* **Hogyan lehet hatékonyan védekezni a kártékony szoftverek ellen?**
  + Összességében elmondható, hogy külső forrásból érkeznek a vírusok többsége.
    - Ezt úgy tudjuk orvosolni, ha a bejövő adatforgalmat minél szigorúbban ellenőriztetjük.
    - Bizonytalan eredetű, illegális szoftvereket kerüljük
    - Vírusírtót használjunk
      * Rendszer indulásakor végezze el a memória, merevlemezek, bootszektorok és rendszerfájlok ellenőrzését.
      * Figyeli a futó alkalmazásokat.
      * Ellenőrizheti a beérkező e-mailokat.
      * Rendszeresen futtat víruskeresést.
    - Felhasználói azonosítás felhasználónév és jelszóval történik (esetleg 2 lépcsős azonosítás)
    - Rendszerfájlok módosításának tiltása
* **Hogyan tudjuk biztonságosabbá tenni hálózati forgalmunkat?**
  + Tűzfal használatával:
    - Olyan hálózatvédelmi eszköz ami figyeli és korlátozza az internetes adatforgalmat.
    - Visszautasítja az olyan IP címekről érkező küldeményeket, ahonnan kérés egyébként nem történt.
    - Megakadályozza az esetleges kémprogramoknak, hogy a felhasználó nem publikus adatait továbbítsa a hálózaton kívülre.
* **Mi a jelentősége az operációsrendszer frissítéseknek, illetve a szoftver frissítéseknek?**
  + Mint minden szoftver és operációs rendszer, emberek által készül. Ez magában hordozza a hibalehetőségeket is.
    - Előfordulhatnak biztonsági rések a programokban, vagy az újabb operációsrendszer frissítésekben.
      * Ezt kihasználhatják a bűnözők, és lehetőségük lesz bejutni a számítógépünkbe.
      * Vannak fizetett etikus hackerek, akik ilyen biztonsági réseket keresnek.
    - A programozók ezeket a biztonsági réseket elég hamar be szokták foltozni, és a következő frissítésnél publikálják a felhasználóknak.