Bevezető

Minden jelszó feltörhető, de nem mindegy, hogy feltöréséhez néhány percre vagy több száz évre van-e szükség a napjainkban elérhető számítógépek segítségével.

Tudtad-e?

Miért ne használjuk a személyes adatainkat a jelszavainkban?

Ha egy általad használt közösségi oldalon megadtad az adataidat, és ismerősid is ezt tették, akkor az adataitok nyilvánosan elérhetők. Ezeket ne használd a jelszavaidban, mert könnyen kitalálhatók!

Miért ne tároltassuk el közösen használt böngészőkön a belépési adatainkat?

„Alkalom szüli a tolvajt" – szól a mondás. Ha valaki közösen használt eszközökön a **böngészővel** megjegyezteti egy profilja belépési adatait, akkor saját maga kínálja fel a betörés lehetőségét. Ilyenkor néha azok is visszaélnek a helyzettel, akik korábban erre nem is gondoltak.

KIBERTÉR

A kibertér **informatikai rendszerek világméretű** (globális) **hálózatban történő összekapcsolásával létrejövő virtuális hely,** ahol adatok tárolódnak, **online kommunikáció és adatforgalom** zajlik. Virtuális (látszólagos), mert sosem tudhatjuk, hogy adataink és üzeneteink a világban éppen merre vannak. Sokszor még azt sem, hogy éppen kivel kommunikálunk.

KIBERBŰNÖZÉS

A kiberbűnözés (számítógépes bűnözés) a számítógépek megjelenésével egyidős. Már az internet elterjedése előtt is létezett.

A valós életben is találkozhatunk bűnözőkkel, akik átverik, megkárosítják vagy bántalmazzák áldozataikat. A **kiberbűnözők** mindezt informatikai eszközök segítségével teszik. A világháló elterjedésével **kihasználják a hardverek és szoftverek biztonsági réseit** (olyan hibáit, amelyek sebezhetővé teszi őket), de **legfőképpen a felhasználók hiszékenységére és figyelmetlenségére alapozva** követnek el a bűncselekményeket.

Néhány gyakori, az interneten megvalósított bűncselekmény:

Kiberbűnöző

- **Adatlopás:** a megszerzett adatok értékesítése a feketepiacon vagy felhasználásuk további bűncselekményekhez.
- **Internetes zaklatás:** megvalósulhat üzenetek útján vagy akár közösségi oldalakon nyilvánosan.
- **Jogosulatlan eszközhasználat:**
  - ilyenkor a felhasználó tudta nélkül a számítógépe kéretlen leveleket küldözget;
  - más eszközök vagy honlapok elleni támadásban vesz részt;
  - esetleg egy kiterjedt robothálózat részeként egyéb tevékenységeket folytat.
- **Csalás:** mások megtévesztése anyagi haszonszerzés céljából.
- **Zsarolás:** informatikai eszközök vagy adatok zárolása vagy képek, adatok közzétételével való fenyegetés váltságdíj reményében.
- **Kémkedés:** állami, katonai, céges vagy személyes információk megszerzése.
- **Lehallgatás:** a felhasználók eszközei kamerájának vagy mikrofonjának bekapcsolásával végzett megfigyelés, de a hálózati adatforgalom is lehallgatható.
- **Rongálás:** informatikai eszközöket, hálózatokat, webhelyeket tesznek használhatatlanná.

Hogyan védekezhetünk a kibertámadások ellen?

A kiberbűnözők gyakran a szoftverek biztonsági réseit veszik célba. Ha megtalálnak egy szoftverhibát, akkor annak felhasználásával indítanak támadást az informatikai eszközök (bármely okoseszköz) ellen. A szoftverfejlesztők folyamatosan javítják a kiberbűnözők által feltárt hibákat, és a javításokat frissítések formájában juttatják el a felhasználóknak. Aki rendszeresen frissíti szoftvereit, annak kevésbé kell félnie attól, hogy kibertámadás áldozatává válik.

MALWARE, AVAGY ROSSZINDULATÚ SZOFTVER

A malware (malicious software, ejtsd: málver; melisösz szoftver; magyarul: rosszindulatú szoftver) olyan programokat jelent, melyek célja **kárt okozni a számítógépben, kényes adatokat gyűjteni,** a megfertőzött eszközt tulajdonosa tudta nélkül saját céljaira felhasználni.

Naponta újabb és újabb rosszindulatú szoftverek jelennek meg. Gyakori fajtáik:

- **Vírusok:** olyan kártevő programok, amelyek saját másolataikat helyezik el más, végrehajtható programokban vagy dokumentumokban. Rendszerint nem megbízható forrásból származó programok juttatásával fertőzik meg a számítógépet.
- **Férgek** (worms; ejtsd: vörmsz): önálló rosszindulatú programok. Általában számítógépes hálózaton terjednek a szoftverek sérülékenységeit kihasználva. Redszeres szoftverfrissítéssel és tűzfalprogrammal védekezhetünk ellenük.
- **Trójai** (trojan; ejtsd: trójön) **programok:** nem megbízható forrásból származó szoftverek, amelyek gyakran nem csak az elvárt feladatokat látják el. Sokszor más káros programok és az internetes támadó számára elérhetővé teszik a számítógépet.
- **Kémprogramok** (spyware; ejtsd: szpájver): interneten terjedő szoftverek, melyek célja a felhasználók adatainak megszerzése. Ezeket utána a bűnözők vagy a feketepiacon értékesítik, vagy bűncselekményekhez használják fel.
- **Reklámprogramok** (adware; ejtsd: ádver): sok szoftverrel együtt telepíthetünk reklámprogramokat. Céljuk termékek, számítógépes programok vagy cégek reklámozása.
- **Böngészőeltérítők** (browser hijacker; bráuzör hájdzsekör): céljuk a webböngésző beállításainak kéretlen változtatása.
- **Rootkitek** (rootkit; ejtsd: rutkit): behatolnak a rendszerbe, és elrejtik a behatolókat vagy rosszindulatú programokat. A számítógéphez korlátlan hozzáférést biztosíthatnak a támadónak.
- **Zsarolószoftverek** (ransomware; ejtsd: ránszomver): blokkolják az eszközt, vagy titkosítják a rajta tárolt adatokat váltságdíj reményében.
- **Billentyűzetfigyelők** (keylogger; ejtsd: kílágör): titokban telepített programok, amelyek a billentyűzet leütéseit figyelik, és minden begépelt szöveges tartalmat rögzítenek. Lehetővé teszik jelszavak, személyes adatok és minden más begépelt információ megszerzését.