Internetbiztonság

# Közösségi hálózatoK

* 3 milliárd tag
* 14 % hamis fiók
* 350 millió kép/nap
* 81% csak mobilról használja
* Megosztott Információk (post, komment, videó, fotó, állapotfrissítés) átgondolatlanul
* Erotikus önportré, Családi képek gyerekekről 🡪 Következmények
  + Pornográf képek (18 év alatt bűncselekmény)
    - megszerez, tart
    - készít
    - nagy nyilvánosságra hoz
* Letörölhetetlen
* A helyes jelszó képzése (pl.: **EmAkTYk#21** – **E**j, **M**i **A** **k**ő! **TY**úkanyó, **k**end) – Így elegendő a mondóra és a képzési szabályra emlékeznünk.

# Megosztott információk

* Az arckép, munkahely és telefonszám ismerete már elegendő lehet zaklatáshoz
* A sok megosztott információ „személyiséglopás”-hoz vezethet
* A közösségi oldalak elérhetőségével komoly károkat is lehet okozni
* Adatokat, arcképet, hangot, videót könnyedén lehet hamisítani akár ingyenes online programokkal is.

# Megosztott képek – GPS

* A okos telefonnal készített képek GPS koordinátákat is tárolhatnak a kép meta információi között
* Ez pl. Meta (exif) adat online keresővel meg is tekinthető
* Így meghatározható, hogy a kép hol készült
* A meta információk eltávolítására vannak programok, de az operációs rendszerekbe is beépítik a lehetőséget napjainkban
* Vagy kikapcsolt GPS-el kell fényképezni a megosztani kívánt képeket
* A közösségi oldalak (Facebook, Instagram, Twitter stb…) törli ezeket a felhasználó helyett, de pl. egy tömörített csomagban vagy e-mail mellékletkét csatolta tartalomban benne maradnak az információk.

# Phishing – Adathalászat

* Telefonon
  + a bank csalásellenes osztálya nevében vagy éppen a rendőrség nevében telefonálnak
  + azt állítják, hogy gyanús aktivitást észleltek a bankszámlánkon
  + Hívószám hamisítás (Spoofing) – Bárki nevében hívhatnak, a bank hivatalos számáról is.
  + Elkérik a bankkártya adatokat és "ellenőrzésképpen" bekérik a PIN kódunkat is vagy
  + „Vírusírtó” programot (pl. **AnyDesk**) telepíttetnek (Ez egy távoli elérésre alkalmas program és teljes uralmat szereznek vele az eszközünk felett)
  + Ürítik a bankszámlánkat a netbankuk használatával.
* E-mail / SMS
  + Az elkövető felveszi a kapcsolatot termék eladójával azon legendával, hogy megvásárolta a terméket és intézi a szállítást.
  + Az elkövető email címet kér a sértettől, amelyre meghamisított-utánzott (fake) banki, szállítmányozó **(Foxpost, GLS, DHL**) vagy kereskedelmi oldalak (Vinted, Marketplace, Jófogás) cég nevében adathalász weboldalra vezető weblinket küld.
  + Amelyet megnyitva a sértett megadja a banki adatait és engedélyezőkódokat.
* Online kérdőíves csalás
  + Hamis online ajánlatok (pl kérdőív kitöltéséért pénzt fizetnek, amely során meg kell adnia bankkártyájának adatait
  + Hamis munkalehetőség
  + Hamis társkeresés

# VIRTUÁLIS RANDI

* Internetes társkeresésbe oltott átverés
* Néhány jól sikerült virtuális randi után a várva várt első személyes találkozó váratlanul elmarad
* "baleset", egy család tag hirtelen "betegsége" vagy állítólagos halála felborítja a terveket
* A behízelgő modorú "áldozat" anyagi elsősegélyt kér az újdonsült párjától
* Védekezési lehetőség:
  + TinEye - fordított képkeresés, segítségével megnézhetjük, hogy egy kép hol, milyen weboldalon fordul elő az interneten.

# mobil keresés (google, samsung)

* Helymeghatározás (GPS alapján)
* Hívás
* Zárolás
* Tartalom törlése
* Akkumulátor élettartamának meghosszabbítása
* Naplók letöltése
* Gyámok beállítása
* Készülék feloldása

# FORDÍTOTT KÉPkeresés (TinEye, google)

* Képek előfordulásának keresése az interneten.
* Hamis termékek vagy személyek kutatása

# HACKER

Cél:

* + Behatolás
  + A rendszer megértése
  + Biztonsági veszélyek felfedése
  + Figyelmeztetés
  + Finomhangolás
  + Szórakozás
* Nem okoznak kárt
* Ha cégek megbízásából is dolgozhatnak (penetráció-tesztelők)

# HACKER verseny

* Számítógép HACKER verseny (Pwn2Own – Pwnium, Vancouver, évente)
  + Több százezer dollár összdíjazás (Plusz például a feltört Tesla)
  + A legutolsó patch-ekkel ellátott Adobe Reader, SharePoint, Tesla Gateway, Tesla Infotainment System, Ubuntu desktop, macOS, Windows 11, Oracle VirtualBox, Microsoft Teams feltörése a cél.
  + A fent említettek általában 10-20 perc vagy néhány óra alatt alatt feltörésre kerülnek a még be nem foltozott biztonsági réseken keresztül.

# CRACKER

* Rossz szándékú hacker
* Jól képzett

Cél:

* + Behatolás
  + Szándékos károkozás
  + Milliós károk

# SCRIPT KIDDIE

* Behatolás kész programokkal (Hacker Tool)
* Károkozás tudatlanul
* Cél nélkül keresik a gyenge pontokat
* Kihasználják, „kiteregetik” azokat
* Sokszor nem is tudják, hogy mekkora károkat okoznak

# VÍRUSOK

Ransomeware – zsaroló típusú

* + Az összes fontos állományt (\*.jpg, \*.bmp, \*.png, \*.doc, \*.docx, \*.xls, \*.xlsx, \*.ppt, \*.pptx, \*.pdf, stb…) lekódolja…
  + Az alkalmazott titkosítás gyakorlatilag lehetetlenné teszi, hogy visszaszerezzük a fájljainkat
  + Az asztal hátterét megváltoztatva egy figyelmeztető üzenetet jelenít meg
  + Fizetésre 72 órát, azaz 3 napot kapunk
  + A feloldó kulcsért BITCOIN-t követelnek (1 Bitcoin ≈ 22 millió forint)
  + A 72 órás határidő elteltével megduplázódik a váltságdíj összege

# Okostelefonok

* Telepített alkalmazások megfontolandó engedélyei:
  + Mikrofonunk távoli használata
  + Kameránk távoli ki-be kapcsolása
  + GPS pozíciónk
  + WiFi adataink továbbítása
  + SD adathordozónk írása, olvasása, formázása
  + Címjegyzékünk harmadik féllel való megosztása
  + Emelt díjas számok értesítés nélküli hívása
* Védelem:
  + Jelszavas
  + Feloldó minta (Látszhat a kijelzőn)
  + Újlenyomat
  + Retina scan

# DEEPWEB | DARKWEB | TOR Project – Anonim hálózatOK

* Black Market
  + Drogok
  + Fegyverek
  + Robbanószerek
  + Anonim bankkártyák
  + Hamis pénz
  + Betiltott könyvek
  + Mérgek
  + Pedofil pornográf tartalmak
  + Szolgáltatások:
    - Anonim bankszámla (anonim kártyával)
    - Hackerek bérelése
  + A félelem legkisebb jele nélkül web shopként üzemeltetik
  + Van kosár, pénztár, és fizetési lehetőség is
  + Az egész világra vállalnak házhozszállítást
* Teljes anonimitást ígér, bár az utóbbi években az FBI többször beazonosította és leállított közülük néhányat

# BITCOIN

* Decentralizált (Központi kibocsátó helyett a számítógépek hálózata tartja a fenn a rendszer működését)
* Blokklánc (az átutalások főkönyve amit minden résztvevő birtokol így hamisíthatatlan)
* Bányászat (Az átutalásokat 10 percenként bonyolult kriptográfiai feladat megoldásával (egy blokk létrehozásával) hitelesítik, amihez komoly számítási kapacitás szükséges. >> Bánya)
* Privát kulcs bármiből képezhető (Mondat, kép, hangállomány, stb.) Ennek (vagy a számla létrehozásakor megjegyzendő 12 szóból ) bármikor helyreállítható a számla
* Anonim pénzműveleteket tesz lehetővé 🡪 Pénzmosás, szervezett bűnözés, terrorizmus.
* Az eladó félnek semmi kockázata nincs: anonim a szerver, anonim helyre megy a kifizetett vételár is
* A postai szállítmány is feladó nélkül, vagy hamis feladóval érkezik
* A vevő nem anonim. Postacímre szükség van
* Léteznek olyan bankok, bank automaták, amelyek valódi pénzt Bitcoinra és vissza váltanak
* Ügyvédnél, fodrásznál, webáruházban, stb. is lehet vele fizetni.

Szeged, 2025. április 28.

Szabó Tamás

CSCSVMRFK GVO