
NET/VÉSZ
Az internet veszélyeiről
dfmvk
DEÁK FERENC MEGYEI
ÉS VÁROSI KÖNYVTÁR

Tartalomjegyzék

A jó és a rossz jelszó

A NordPass nevű weboldalon minden évben közzéteszik a leggyakrabban használt jelszavak listáját.

Ami a megdöbbentő, hogy évek óta az első három helyezett az 123456, az 123456789 és az 12345. De az első 10 között egyébként is csak olyan jelszó szerepel, aminek a feltörési ideje kevesebb, mint 1 másodperc. Emberek milliói „védik" az adataikat olyan jelszavakkal, amik még egy ingyenes kódfeltörő programot sem izzasztanának meg különösebben.

Ha nem szeretnél abba a hibába esni, hogy gyenge védelemmel látod el és ezáltal könnyű prédává teszed például az internetes levelezésedet, a banki adataidat vagy éppen az online ügyintézés miatt a neten található hivatalos, illetve egészségügyi adataidat, jó ha betartod az alábbi néhány szabályt.

Ne használj olyan információt jelszavadként vagy annak részeként, amit könnyű megszerezni!

Ilyen a felasználónév, a születési dátum, a lakhely, a telefonszám, a családtag vagy házikedvenc neve, a kedvenc csapat, film- vagy könyvszereplő neve. Semmilyen személyes, közismert, vagy könnyen kideríthető adatot nem érdemes belefoglalni egy jelszóba.

Ne használd a billentyűzeten egymás után következő karaktereket ugyanabban a sorrendben!

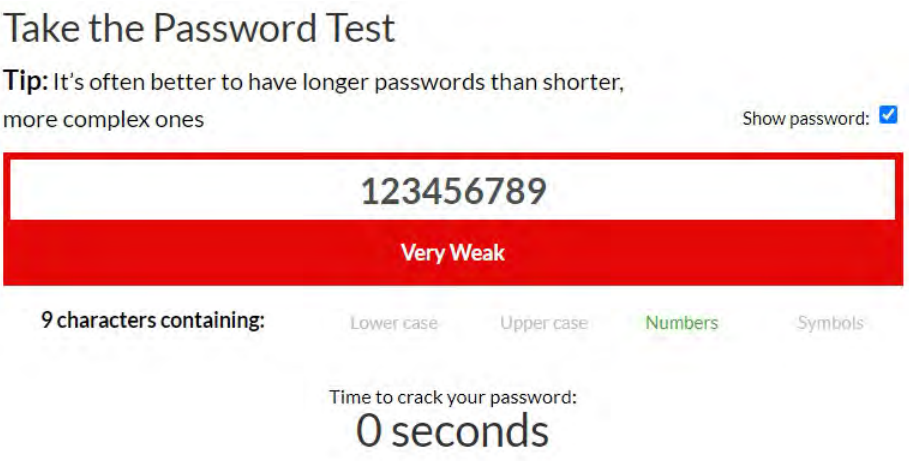
Ilyen az 12345, a qwert vagy éppen az asdf. Ha valaki manuálisan áll neki feltörni a fiókodat, valószínűleg ezek lesznek az elsők, amiket megpróbál. Ha pedig programot használ, egy másodperc töredéke kell csak hozzá, hogy bejusson a fiókodba.

De mitől lesz jó egy jelszó?

Azon felül, hogy elkerüljük a fentieket, jó ha megfelel néhány egyéb kritériumnak, feltételnek is.

Legyen legalább 8-10 karakter hosszú!

Minél hosszabb egy jelszó, annál tovább tart feltörni. Ez viszont csak egy alap kritérium, fontos az is, hogy ezen túl milyen karaktereket tartalmaz, hiszen az 123456789 számokat tartalmazónak megfelel a hossza, de mégis egy igen gyenge jelszó.



Használj minél többféle karaktert!

Sok oldalon már eleve csak olyan jelszót választhatsz

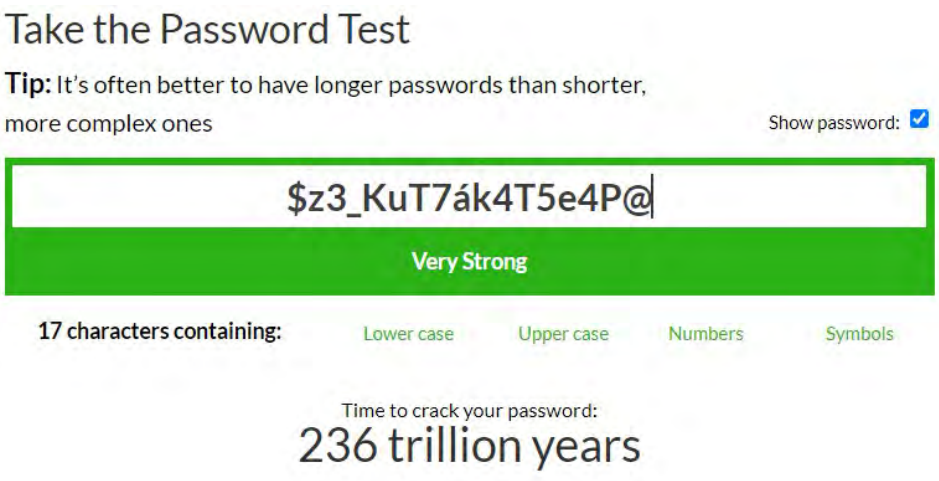
a regisztrációnál, amiben szerepel kis- és nagybetű, szám és különleges karakter is. Nem véletlenül, ugyanis minél összetettebb, annál nehezebb feltörni.

Persze ilyenkor merül fel az a probléma, hogy ha bonyolult a jelszó, mi magunk sem fogjuk tudni megjegyezni. Erre egy jó megoldás a mondatjelszó: kitalálsz egy mondatot, majd azt átvariálod úgy, hogy egy igen bonyolult jelszó legyen belőle, amit viszont te könnyen meg tudsz jegyezni az eredeti ismeretében.
Nézzünk erre egy példát:

Szeretek kutyákat sétáltatni a parkban.

Ezt a mondatot átalakíthatod úgy, hogy egyes betűket nagyként írsz, másikakat számmá formálsz, teszel bele szóközt (ahol ez nem megengedett, ott egy alulvonást használhatsz helyette), sőt pár egyedi karaktert is beleszúrhatsz:

$z3_KuT7ák4T5e4P@



Egyes számok az interneten való kommunikációban eleve használatosak bizonyos betűk helyett, ilyenek pl: 1 = i, 4 = a, 5= s stb.
Használhatod ezeket, de akár saját asszociációkat is kitalálhatsz, a lényeg, hogy te meg tudd jegyezni, melyik mit takar pontosan.

A mondatjelszó kigondolásánál használhatunk akár egy fényképet is, az a fontos, hogy "le lehessen olvasni" róla egy olyan mondatot, amiben valaki valahol valamit csinál. (Ez a PAO-módszer, ami az angol Person-Action-Object, vagyis személy-cselekvés-tárgy szavakból nyerte a nevét.)

Ajánlott minden oldalon más jelszót használni. A mondatjelszóval könnyen alkothatunk hasonló vagy ugyanolyan alapra sok különféle jelszót. A fenti példát használva, a kutya szót kicserélhetjük kutyafajtákra. Pl. a bank oldalán labradort, az e-mail fiókunknál németjuhászt, a facebookon meg huskyt írunk:
$z3_l4Br4DoRt5e4P@,
$z3_N3mJu8a5e4P@,
$z3_8uS2kYt5e4P@.
Máris van három különböző, de számunkra mégis könnyen megjegyezhető erős jelszavunk. Arra figyeljünk, hogy nem elég, ha csak 1 vagy 2 karakterben különböznek egymástól a jelszavak, és természetesen sokkal nagyobb biztonságot ad, ha minden oldalon teljesen más jelszót használunk.

Néhány egyéb tanács:
Ne írd fel könnyen látható helyre, és ne mondd el senkinek!
Ha mindenképpen tárolni akarod valahol, arra az esetre, ha elfelejtenéd, jobb ha nem a teljes jelszót írod le, inkább csak valamit, amiről biztosan eszedbe fog jutni.
Ha a mobilod biometrikus azonosítással van védve (ujjlenyomatot, arcképet, hangot ismer fel), jó lehet a tárolásra, de ebben az esetben sem ajánlott a teljes jelszót leírni.
A fenti példa alapján megjegyeztethetjük mobilunkkal, hogy a bank labrador, a facebook meg husky. Vagy éppen az eredeti alapmondatot.

Bizonyos időközönként cseréljük!
Mindenki mást ajánl annak kapcsán, hogy mikor érdemes lecserélni a jelszavakat, de azzal minden szakértő egyetért, hogy

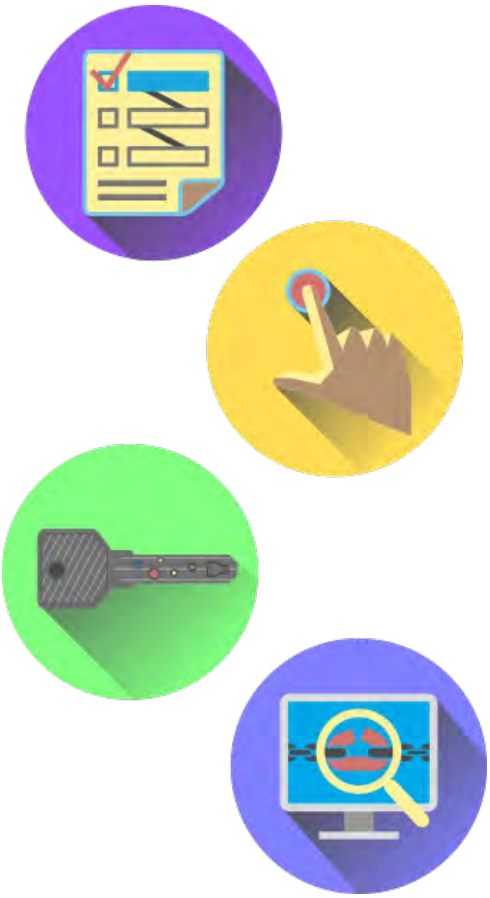
időnként meg kell változtatni őket. Megtehetjük havonta, negyedévente, félévente, évente vagy háromévente, a lényeg, hogy ha már úgy érezzük, túl régóta nem változtattuk meg, bátran írjuk át. Ha még sosem tettük meg, akkor most épp itt vanráatökéletesalkalom.

Használjunk többlépcsős azonosítást!
Sok weboldal, főleg azok, amik személyes adatokat tárolnak (például bankkártya adatokat), felajánlja a több lépcsős azonosítást. Ez állhat abból, hogy küldenek egy e-mailt vagy sms-t egy kóddal a bejelentkezéshez, de akár külön applikációt is igénybe vehetnek erre a célra.

Lehetőség szerint ne lépjünk be nyilvános számítógépekről!
Nem csak azért kerülendő ez, mert léteznek szoftverek, amik megjegyzik a billentyűleütéseket, de véletlenül el is menthetjük a jelszavunkat vagy kifigyelhetik azt akár a hátunk mögött állva is.

Ne adjuk meg sem írásban, sem szóban a jelszavunkat senkinek!
Egyetlen szolgáltató sem fogja elkérni a jelszavunkat, a bankunk meg aztán pláne nem. Ha egy hivatalosnak tűnő e-mailt kapunk azzal, hogy szeretnék megtudni a bejelentkezési adatainkat, inkább hagyjuk figyelmen kívül.

A jelszavak becsült feltörési idejét ábrázoló képek forrása a https://www.passwordmonster.com/.



6

Hazug/megtévesztő e-mailek (adathalászat)

Az adathalászat nem újkeletű találmány, már az 1980-as években is ismert technika volt, és mára a kiberbűnözők egyik leggyakrabban alkalmazott támadásává vált.
Ennek során egy megtévesztő e-mailt küldenek az áldozatnak, amiben megpróbálják rávenni, hogy adjon meg bizonyos adatokat (pl jelszót) vagy kattintson rá egy linkre, aminek következtében kü-

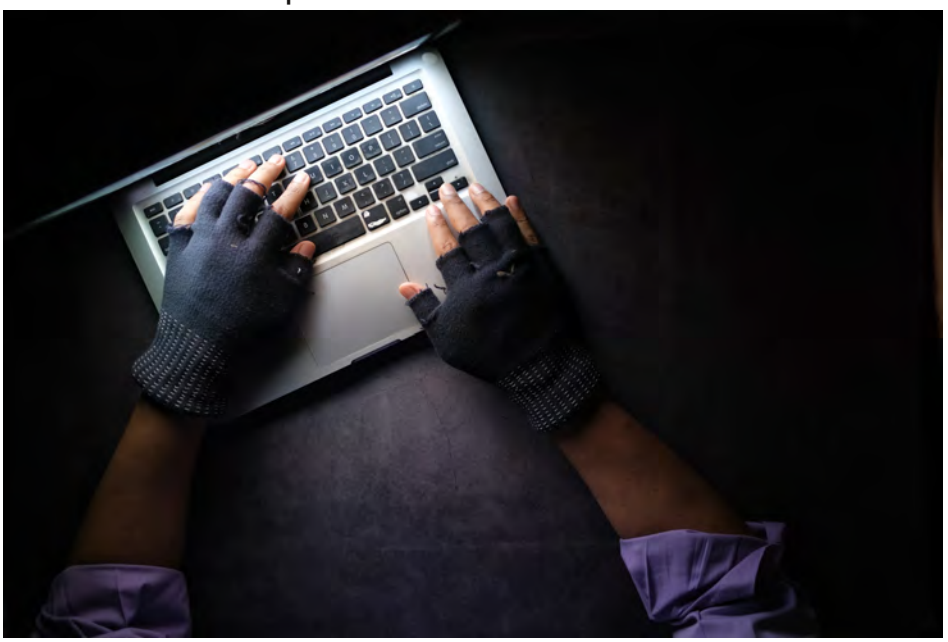
lönféle rosszindulatú programokat telepítenek a gépére.

Az e-mailek általában próbálnak hasonlítani egy hivatalos levélre, ezért felhasználják a cég logóját, színeit, egyéb arculati elemeit. Néhány alapvető dologra figyelve azonban könnyen észrevehetjük, ha egy üzenet hamisított.

Fontos megnézni a küldő e-mail címét, ami egészen biztosan nem fog megegyezni a bankunkéval (vagy az éppen lemásolni próbált egyéb szolgáltatóéval), akkor sem, ha egyes elemeiben hasonlít rá.
De még ezen túl is gyanúsan túl bonyolult és egyáltalán nem tűnik professzionális e-mailnek. Ha egy cím gyanús, eleve rá se kattintsunk az üzenetre.
Ha szeretnénk ellenőrizni, keressük fel az eredeti cég oldalát, a kapcsolat menüpont alatt biztosan fel lesz tüntetve a hivatalos e-mail cím is.

A megszólítás sem mindegy. Ha egy hivatalos üzenetben azt írják, hogy "Szia" vagy éppen, hogy "Tisztelt Felhasználó", akkor ott már problémák vannak. A legtöbb esetben vagy a neveden vagy a felhasználóneveden fognak szólítani, de minimum ügyfélnek vagy partnernek.

Gyanús lehet a magyartalan szöveg is. Egy-egy gépelési hiba bárkivel megeshet, de azt, hogy egy mondatnak ne legyen értelme vagy éppen teljesen magyartalan legyen, egy szolgáltató sem engedheti meg magának. Ha a bankodtól olyan e-mailt kapsz, amiben ilyen mondat van: "Meg kell nyitni a fiókot velünk.", inkább töröld az e-mailt vagy kérdezz rá telefonon vagy e-mailben, de fontos hogy ezeket a kapcsolattartási adatokat a bank vagy egyéb szolgáltató eredeti oldalán keresd le,



és semmiképpen ne kattints rá arra a linkre, ami a gyanús e-mailben látható!

Furcsa, ha sürgetnek egy hivatalos e-mailben. Az előfordulhat, hogy adnak határidőt, de az kevéssé valószínű, hogy azt írják, hogy ha három napon belül nem teszel meg valamit, akkor annak már komoly következményei lesznek (pl. kikapcsolják az áramot, ha éppen az áramszolgáltató nevében írnak).
Mielőtt tényleg tennének valami hasonlót, több felszólítást is küldenek, az esetek többségében megpróbálják az illetőt postai úton vagy telefonon is elérni. Ha egy hivatalos e-mailben sürgetnek, legyen gyanús. Az adott szolgáltató oldalán pedig keress elérhetőséget, és kérdezz rá, hogy ezt biztosan ők küldték-e.

Általános jó tanács, hogy semmilyen e-mailben ne kattints rá a linkre, bár körülményesebb, de el tudod érni azt a weboldalt úgy is, ha külön megnyitod az eredeti szolgáltató weboldalát, és akkor a támadóknak nincs esélyük átirányítani téged egy olyan oldalra, ami bár hasonlít (gyakran egészen megdöbbentően) az eredetire, de mégsem az.
Ezen a hamis oldalon aztán követni tudják mit csinálsz. Ha megbízol az e-mailben és mégis kattintani szeretnél, ellenőrizd előbb a linket úgy, hogy ráviszed a kurzort. Az ablak bal alsó sarkában meg fogja jeleníteni azt a webcímet, ahova átirányít, ha rákattintasz. Ha ismeretlen vagy furcsa, inkább ne kattints!

Egy plusz tipp! Mindenképpen legyen gyanús, ha az üzenetben nem szerepelnek ő és ű betűk. Nagyon sok betűtípus nem tartalmazza ezeket, mert a kettős éles ékezet a latin ábécét használó nyelvek közül csak a magyarban található meg. Szóval, ha egy magyar hivatalos levélben ezek rosszul (pl o, u betűként vagy több karakter halmazaként) vagy egyáltalán nem jelennek meg, akkor, ha nem is dobjuk az üzenetet egyből a kukába, azért legyünk extra figyelmesek.

A folyton figyelő szem

Nem kell ahhoz összeesküvés hívőnek lenni, hogy tudjuk, az interneten folyamatosan megfigyelnek minket. Gyűjtik az adatainkat: mit nézünk, mire keresünk rá, mire kattintunk. Aztán ezeket arra használják, hogy számunkra releváns(nak gondolt) hirdetéseket tegyenek elénk akkor és ott, amikor és ahol a korábban feltérképezett szokásaink szerint a legvalószínűbben észrevesszük.

Azt azonban kevesebben tudják (vagy legalábbis kevesebben használják ki), hogy vannak eszközeink arra, hogy meghatározzuk ki gyűjthet rólunk adatokat, ki követheti az online tevékenységünket.

Az egyik ilyen például a Ghostery, ami egy ingyenes és nyílt forráskodú böngésző bővítmény. Nem csak a hirdetéseket tudja blokkolni, de a követést is szabályozza az általunk megadottak alapján. Hasonlóan megoldást jelenthet a sokak által ismert és használt Adblock vagy éppen a Privacy Badger nevű bővítmény.

A Google is előszeretettel jegyzi meg kereséseinket, kattintásainkat, tartózkodási helyünket (sőt, ha engedélyeztük neki, akkor azt is elmenti, hogy mikor merre jártunk).
A fiókunk beállításainál viszont megtekinthetjük és megadhatjuk, milyen adatokat gyűjtsön és tároljon rólunk. Az Adatok és adatvédelem menüpont alatt részletesen testre szabhatjuk mennyire ”közelről” követhet minket.

Ha a Google nem is menti el a tartózkodási helyünket, mi magunk is gyakran eláruljuk, amikor megosztjuk Facebookon vagy Instagramon, hogy merre járunk éppen. A legjobb, ha soha nem adjuk meg ilyen esetekben a pontos tartózkodási helyünket, de ha mégis erős késztetést érzünk rá, tegyük utólag és ne akkor, amikor éppen ott vagyunk.

Ne tölts fel képet személyes iratokról, végzettséget igazoló okmányokról, számlákról vagy egyéb hivatalos iratokról! Mindenki gratulálni fog a diplomádhoz akkor is, ha csak a bőrkötéses borítóját látják, viszont legalább nem lopják el a benne szereplő személyes adataidat.

Ne nyiss meg olyan csatolmányokat, mellékleteket, amik nem tudod mik lehetnek és ki küldte őket! Ha furcsa a fájl neve és/vagy nem ismered a címzettet, inkább ne kattints! Eleve gyanús lehet, ha a fájlnak többszörös kiterjesztése van, pl: fajlnev.pdf.gz

Ha nem használsz reklámblokkolót, legalább ne kattints rá mindegyik hirdetésre, felugró ablakra. Akkor se, ha csak itt, csak most, csak neked ajánlattal kecsegtetnek. Sőt, akkor pláne ne! Óvd az adataidat, ne add ki pusztán figyelmetlenségből!

Kitől vásárolj és kitől ne?

Manapság szinte mindent könnyebb online elintézni, és ez alól a vásárlás sem kivétel.
Viszont mivel ebben az esetben a terméket majd csak akkor látjuk, amikor már kiszállították nekünk (ha egyáltalán megkapjuk a rendelésünk), fontos lenne, hogy felismerjük a csaló oldalakat.

Vannak, amik már egy létezőt próbálnak másolni, és esetenként elég meggyőzően teszik ezt. Ezeknél alaposan meg kell nézni a webcímet, előfordulhat, hogy a név csak egy betűvel tér el a valódi cég vagy márka nevétől. Például gyakran az m-t az rn betűk kombinációjával írják. Ha ehhez jó betűtípust választanak, alig tűnhet fel a különbség.

A nagyon nagy akciók és hihetetlen ajánlatok szintén megszólaltathatják a vészcsengőket. Ha valamit több, mint 60%-kal leáraznak, az már feltébb gyanús, de ha 90%-kal olcsóbban adják, az már biztosan átverés.

Akkor se bízzunk benne, ha nem csak hatalmas leárazásokkal reklámozza magát, de még viszonylag fiatal is az oldal. A

> „A 90%-os akció biztosan átverés"

https://web.archive.org/ oldal többek között weboldalakat archivál, rákeresve az url címre megnézhetjük egy adott oldal korábbi verzióit, és egyben azt is megtudhatjuk, hogy mióta létezik.

Nem árt, ha megnézzük a kapcsolat menüpont alatt található információkat.

Ahol nincs elérhetőség megadva, onnan vásárolni sem érdemes, hiszen nem tudunk senkihez fordulni, ha netán bármi panaszunk lenne a szolgáltatással vagy termékkel kapcsolatban.

Ha találunk elérhetőséget, de azon nem érünk el senkit, vagy eleve furcsának, amatőrnek tűnik (pl. véletlenszerű karakterek halmaza az e-mailcím vagy a székhely címén nem az található, aminek kellene lennie), szintén éljünk a gyanúval, és ha egy hely nem tűnik megbízhatónak, inkább ne költsük ott a pénzünk.

Ha csak bankkártyát fogadnak el és az adatokat ráadásul a saját oldalukon kell megadni (nem pl. egy olyan felületen keresztül, mint a SimplePay), szintén felejtsük el a vásárlást.

Nem növeli a bizalmat, ha a termékekről vagy nincs visszajelzés, vagy minden komment ötcsillagos és abszolút pozitív. Még a legkiválóbb termékeknél és szolgáltatásoknál is akad egy-egy elégedetlen vásárló.

Ha tudod, hogy a cég magyar, a legegyszerűbb, ha rákeresel a cégjegyzékben. Ha nem létezik, törölték vagy csődeljárás zajlik ellene, azt ott látni fogod. Ugyanígy az egyéni vállalkozók nyilvános adatait is le tudod kérdezni.
Külföldi cég esetében például a Google Biztonságos Böngészés - webhelyállapot oldalán indíthatunk egy keresést, vagy a ScamAdviser oldalán.

Az internet népe

A Facebook már több milliárd hamis fiókot törölt, de ez nem akadályoz meg senkit abban, hogy újabbakat hozzanak létre. Ez a probléma azonban nem korlátozódik csak a Facebookra. Minden olyan oldalon, ahol mint valós személyek kommunikálunk egymással, legyen az közösségi média oldal vagy éppen társkereső application, előfordulnak álprofilok.

Ezeknek egy része azért születik, mert a mögötte álló ember fél felvállalni magát, biztonságosabbnak érzi egy hamis profil mögé bújni, de akadnak köztük olyanok is, akik rosszindulatúak: az álprofilokat használják csalásra, adathalászatra, zaklatásra is.

Az álprofil nem minden esetben csak egy netről levadászott kép és egy véletlenszerűen választott név némi adattal, amitől valósnak tűnhet, van amikor egy valós személy képeit, nevét és adatait használják fel. Extrém esetben az is megtörténhet, hogy a hamis profil jelenti a valódi profilt az oldal üzemeltetőjének, és előfordulhat, hogy végül utóbbi lesz letiltva.

Mielőtt parttalan vitába kezdünk valakivel a Facebookon, érdemes megnézni, hogy egyáltalán

”valódi” emberrel van-e dolgunk vagy csupán egy trollal, akinek szórakozást jelent, ha sikerül felidegesíteniük a célpontjukat; esetleg egy üzleti megfontolásból létrejött álprofillal, aki a vita generálásával akarja növelni a poszt/oldal hozzászólásait, nézettségét, látogatottságát.

Na, de miről lehet felismerni egy álprofilt?

A legegyszerűbb módja, ha a Google képkeresőjében indítunk egy keresést az illető profilképére (amennyiben az embert ábrázol, de az álprofilok általában igyekeznek minél hihetőbbek lenni, emiatt ritka, hogy kiscicás képet használnának profilképként). Ha a Google megtalálja máshol, más néven vagy éppen ugyanazon a néven, de egy sokkal valódibbnak tűnő profilon, akkor máris tudhatjuk, hogy itt valami nem igazán stimmel.

Gyanús lehet, ha kevés az ismerőse. Az persze előfordulhat, hogy új profil, de jobb ha ilyenkor azért megpróbálunk elővigyázatosak lenni.

Megtekinthetjük az idővonalát, tevékenységeit is. Ha egy profil egy bizonyos célra (pl.: üzleti vagy politikai) lett létrehozva, az látszani fog abból, hogy mit oszt meg, mihez (és hogyan) szól hozzá.

Ha nem ismerünk valakit, ne jelöljük vissza! Ha úgy érezzük, hogy valahonnan ismerős, de nem tudjuk honnan, inkább kérdez-

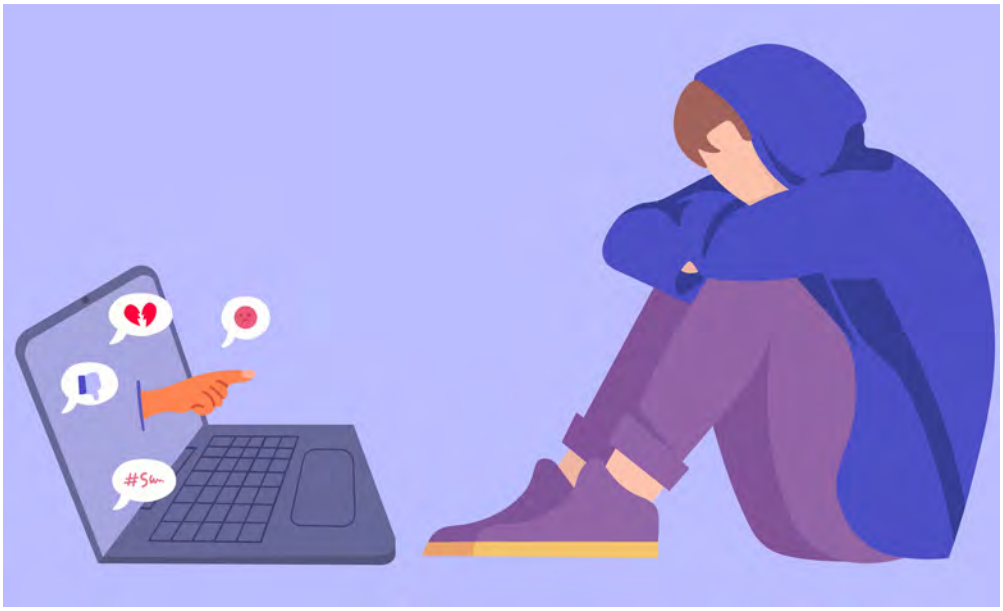
Részletesebben a témáról: https://people.inf.elte.hu/szlavi/InfoDidact18/Manuscripts/HCs.pdf

Cyberbullying, zaklatás a neten

Az online vagy internetes zaklatás, eredeti nevén cyberbullying olyan infokommunikációs technológiát használó szándékos, ismétlődő tevékenység, aminek célja mások bántalmazása.

Bár a zaklatás, gúnyolódás, iskolai kiközösítés az internet használatának tömeges elterjedése előtt is létezett, a cyberbullying komolyabb problémát jelent, mert nem ér véget a tanítási idővel és nem szünetel a vakáció alatt sem. A "hagyományos" zaklatást sokszor meg lehet szüntetni költözéssel, másik iskolába való átiratkozással, és ilyen módon tiszta lappal lehet kezdeni, de az internetes zaklatásnak sem földrajzi, sem időbeli korlátai nincsenek. Ráadásul az internet nem felejt: ha valakiről felkerült a netre egy személyes (akár intim) fotó, azt bárki lementheti és akár évekkel később is újra előkerülhet. Az online zaklatásnak sokszor nagyobb a "nézőközönsége" is, ezért az áldozat hatványozottan nagyobbnak érzi a megaláztatást.

> "A bántást nem lehet megérdemelni. A bántás mindig a bántóról szól."
>
> Tisza Kata



A cyberbullyingnak sok fajtája van, például a zaklatók terjeszthetnek pletykát az áldozatról, gúnyolódhatnak, élcelődhetnek rajta, megoszthatnak róla kompromittáló képeket vagy videókat, de mindezt egy az áldozat nevében regisztrált álprofilról is megtehetik.

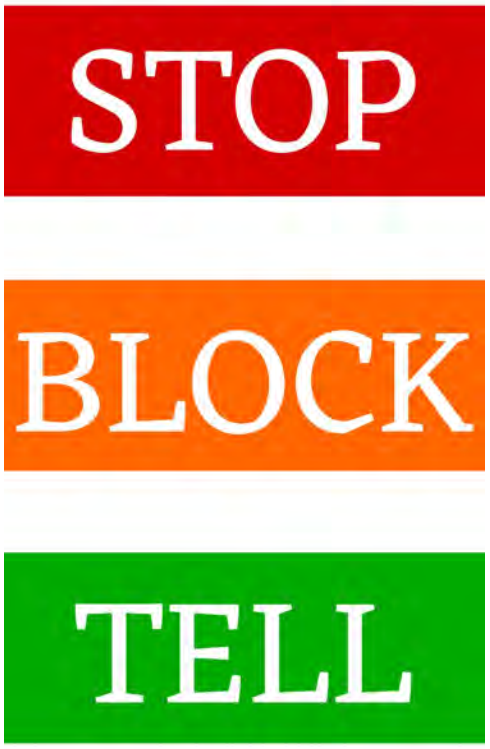
A következményei pedig gyakran súlyosak: önértékelési zavarokat, szorongást, stresszt okoz, és ha mindez hosszabb távon

Majd megöregszel és bánni fogod,
hogy bántasz, – azt, amire büszke vagy ma.
A lelkiismeret majd bekopog
s nem lesz emlék, melyben magadra hagyna.

József Attila

fennáll, mentális és fizikai tünetekkel, betegségekkel járhat, végső esetben akár öngyilkossági kísérletbe is torkollhat.

Nagyon fontos, hogy a gyerekek tudják, mi az internetes zaklatás és tisztában legyenek vele, hogy fordulhatnak problémáikkal az értük felelős felnőttekhez. Érdemes a zaklató üzeneteket menteni, mert bizonyítékok lehetnek abban az esetben, ha eljárás indul. A zaklatás ugyanis bűncselekmény, ezért ha rendőrségi feljelentés történik, büntetőeljárás indulhat, és a zaklató akár több év szabadságvesztéssel is büntethető.



Ha úgy gondolod, hogy te is internetes zaklatás áldozata vagy, alkalmazd a hármas szabályt:

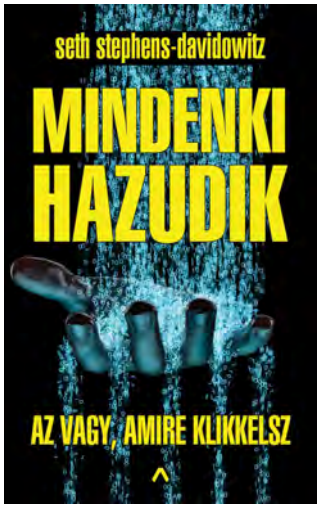
STOP! BLOCK! and TELL!

ÁLLJ MEG! Ne csinálj semmit, próbálj megnyugodni!

TILTS! Tiltsd le a zaklatót vagy limitáld a kommunikációdat a legközelebbi (megbízható) barátaidra, ismerőseidre!

és **MONDD EL!** Mondd el egy felnőttnek, akiben megbízol, nem kell ezt egyedül végigcsinálnod!

Könyvajánló



Hasznos oldalak

https://saferinternet.hu/

Az Európai Bizottság által indított Safer Internet Plus program tudatosságnövelő központként a gyermekek, szülők, tanárok és döntéshozók felvilágosítását, a program népszerűsítését tűzte ki célul.
Szeretné elérni, hogy az országban minél több internethasználó böngészhessen biztonságos körülmények között, illetve hogy probléma esetén az érintettek tudják, kihez fordulhatnak. Ennek érdekében számos eszközzel hívja fel a társadalom figyelmét a biztonságos internethasználat fontosságára. Konferenciák, rendezvények, kampányok során tudatosítja a világháló veszélyeit és bemutatja elkerülésük hatékony és egyszerű eszközeit. A Safer Internet program egyik fő tevékenysége a felhasználói tudatosság növelése.

https://www.gyermekmento.hu/

A Nemzetközi Gyermekmentő Szolgálat (NGYSZ) a hazai Safer Internet konzorcium Tudatosságnövelő Központjaként 2010 óta számos iskolában, művelődési házban és egyéb intézményben tartott Netezz biztonságosan! címmel térítésmentes oktatásokat. Az oktatások során olyan témákat érintenek, mint a személyes adatok védelme, az online zaklatás, netikett és a webes identitás. A gyerekek számára kisfilmekkel, olykor feladatokkal színesített programmal készülnek. Az oktatások alapját képező tananyag elkészítését, valamint a központi koordinációt a Nemzetközi Gyermekmentő Szolgálat látja el. Videók a témában: **Saferinternet Magyarország** csatornája és **Webidomár** csatornája.

https://kek-vonal.hu/

A Kék-Vonal Gyermekkrízis Alapítvány. Célja, hogy a gyerekek valódi odafigyelést, elfogadást, a bajban segítséget kapjanak, valamint hogy széles körű, gyors, ingyenes elérhetőséget biztosítson számukra.

https://unicef.hu/cyberbullying

Az Unicef internetes zaklatással foglalkozó oldalán a szervezet cyberbullyinggal kapcsolatos felméréseit, kampányait (pl.: #nemvagyegyedül, Együtt a sértő hangok ellen) követheted figyelemmel.

https://hop12.hu/

Az internet teljesen behálózza a hétköznapjainkat, ennek ellenére nem feltétlenül tudatosítjuk a veszélyeit. Ebben a virtuális térben naponta több százezer gyermek tűnik el, anélkül, hogy tisztában lennének a „netvilág" szabályaival. Ezért határozott úgy a Hegyvidéki Önkormányzat, hogy a Hegyvidéken élő vagy itt tanuló gyerekek védelme érdekében létrehozza a Hegyvidéki ONvédelem Programot. Kiknek szól? Elsősorban a szülőknek és pedagógusoknak, akik ezen az oldalon, illetve a programhoz tartozó képzések alkalmával megszerzett tudás segítségével képesek tájékoztatni a gyerekeket a lehetséges veszélyekről, illetve segíteni őket, ha támadás, zaklatás vagy egyéb atrocitás éri őket. Mi a célja? A szülők és pedagógusok ismereteinek bővítése, a gyerekek tudatos médiafogyasztásra nevelése, a problémákra koncentráló, gyakorlati megoldások bemutatása.

https://nmhh.hu/internethotline/

Az NMHH (Nemzeti Média- és Hírközlési Hatóság) keretében működő Internet Hotline egy jogsegélyszolgálat, amely bejelentések alapján segíti a neten talált jogsértő tartalmak gyors eltávolítását azért is, hogy a gyermekek minél kevesebb káros tartalommal találkozhassanak a neten. A honlap Tudástár és Hírek rovata fontos, részben az internethasználat jogi szempontjaival, részben a nagy nyilvánosságot leginkább érdeklő problémákkal kapcsolatos információkkal szolgál. Az Internet Hotline oldalról elérhető az NMHH fogyasztóknak/internet oldala (http://nmhh.hu/fogyasztoknak/internet); az NMHH kutatások oldala (http://nmhh.hu/kutatasok); az alkalmazások oldal, ahol a szűrőszoftverekkel kapcsolatos információk találhatók.

https://www.facebook.com/safety

A portál szülői és ifjúsági rovatai közvetlen, informativ és praktikus javaslatokat fogalmaznak meg, a szülői beszélgetések rovatban (https://www.facebook.com/safety/parents/conversations) pedig fontos kérdéseket járnak körül. A portál pozitív szemlélete segíti, hogy a gyerekek jobban megfontolják a kockázatokkal kapcsolatos javaslatokat is. A honlapra kerülő anyagok mögött nemzetközi szakértőkből álló biztonsági testület áll.

http://www.tabby.eu/

A T.A.B.B.Y. az interneten (Threat Assessment of Bullying Behaviour in Youth Online) projekt célja a fiatalok körében tapasztalható, kortárs online bántalmazás formáinak és nagyságrendjének felmérése és a jelenség megismertetése a pedagógusokkal, az iskolapszichológusokkal, az iskolavezetéssel, a szülőkkel, valamint a diákokkal. A program a digitális média – az internet, a mobiltelefonok és egyéb interaktív elektronikus kommunikációs formák – fiatalok általi használata kapcsán tapasztalt kihívásokra, ezen belül is leginkább az online fenyegetésre, megfélemlítésre és a szexuális tartalmú szöveges üzenetek problémáira irányul.

https://www.telekom.hu/rolunk/fenntarthatosag/edukacio/gyermekvedelem

Felelős nagyvállalatként feladatunk – olvasható a Telekom honlapján –, hogy „segítséget nyújtsunk az internet biztonságos használatához. Arra törekszünk, hogy minden korosztály okosan és tudatosan éljen a digitális világ lehetőségeivel és megszűnjön az ország egyes területei között fennálló digitális szakadék. 2017 novemberében a vállalatcsoport többi tagjához hasonlóan a Magyar Telekom is csatlakozott a Deutsche Telekom Teachtoday nevű kezdeményezéséhez, ezáltal lehetőséget teremtve az edukációs tartalmak online, széles körben való terjesztésére.

https://nane.hu/onlineeroszak/

A Nők A Nőkért Együtt Az Erőszak Ellen Egyesület online erőszakról szóló oldalán többféle tesztet, szituációs játékot végigpróbálva tanulhatjuk meg, mit jelent többek között az online zaklatás és mit tehetünk, ha ilyen helyzetbe kerülünk.

https://www.biztonsagosinternet.hu/

Itt bejelentheted, ha olyan weboldalra találsz, amit károsnak gondolsz, veszélyt jelenthet a gyermekek fejlődésére vagy megsért valamilyen jogszabályt.

http://mediatudor.hu/

Az Egyesült Királyságból származó Media Smart program magyar változata a Médiatudor nonprofit médiaismereti oktatási program 6–11 éves gyermekek számára, amely 2007-ben készült el. Az oktatási segédanyagok fejlesztésében szakértői bizottság működik közre, melynek elnöke dr. Kósa Éva pszichológus, egyetemi tanár. Az oktatási segédanyagok hazai készítését és működtetését a Media-Smart Hungary Oktatási Nonprofit Kft. végzi. Az eredeti program célja megtanítani a gyermekeket arra, hogy helyesen értsék, értékeljék és értelmezzék a reklámokat, felkészüljenek a kritikus, tudatos fogyasztói magatartásra. Közvetett célja, hogy a kritikus gondolkodás fejlesztésével a gyerekek megtanuljanak értékelve viszonyulni a média által közvetített tartalmakhoz.

A kiadványt a 2022-es Internet Fiesta program keretében a
Deák Ferenc Megyei és Városi Könyvtár készítette.
Szerkesztő: Deák Klaudia

DEÁK FERENC MEGYEI
ÉS VÁROSI KÖNYVTÁR