Általános jelszókezelési útmutató

Gyors Áttekintő Segédlet

Bevezetés

A számítógépes rendszerekben Ön is a születésnapját, gyermekei becenevét vagy kedvenc állata nevét állítja be jelszónak?

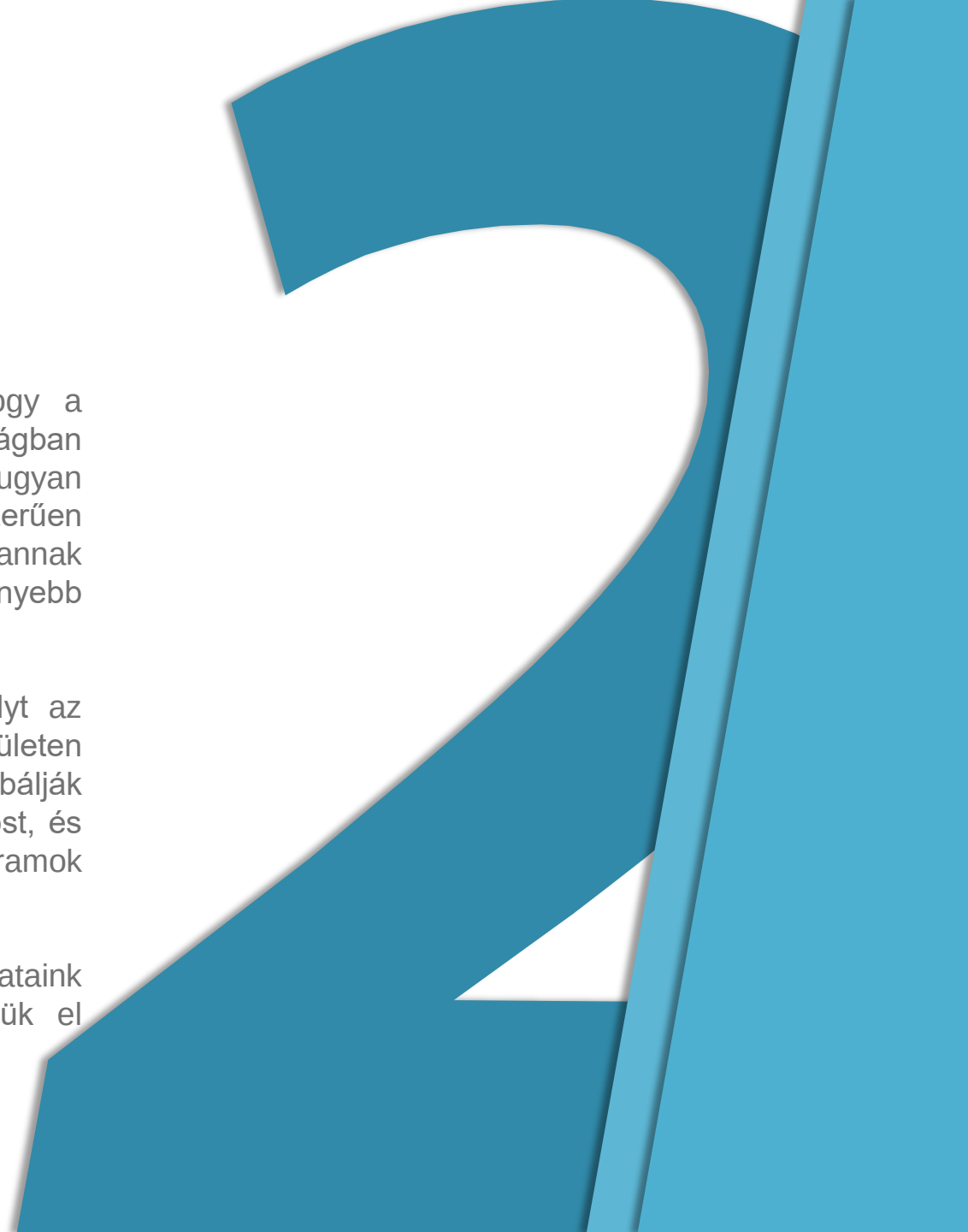
Ha ez az információ fenn van a Facebook-on, a LinkedIn-en, a Twitter-en vagy bármelyik más közösségi vagy ismerkedős oldalon, már el is lopták, és betörhettek vele nem csak saját postafiókjába, de nagy eséllyel akár iskolája, munkaadója rendszerébe is.

Rossz gyakorlatok:

A leggyakrabban elkövetett hiba, hogy a manapság minket körülvevő digitális világban mindenhol, vagy legalábbis sok helyen ugyan azt - az esetleg nagyon egyszerűen kitalálható/megfejthető - jelszót, vagy annak néhány változatát használjuk a könnyebb megjegyezhetőség miatt.

Ebben azonban a legnagyobb veszélyt az rejti, hogy ha a jelszavunk egy felületen kitudódik, a bűnözők sok felületen kipróbálják ugyan azt a felhasználónév/jelszó párost, és mindezt teljesen automatizált programok segítségével.

Akkor mit tegyünk, hogy adataink biztonságban legyenek és ne felejtsük el állandóan a bonyolult jelszavainkat?



Jelszó titokban tartása

A jelszó te vagy!

Ha odaadja másnak, Ő az Ön nevében járhat el!

- írhat egy felmondólevelet a főnökének
- megfertőzheti vírussal vagy módosíthatja fájljait, iskolai dokumentumait
- jegyeket írhat be a tanulóknak, vagy éppen törölheti azokat

Ne írjuk fel!

Sok jelszót nehéz vagy nem lehet megjegyezni, de:

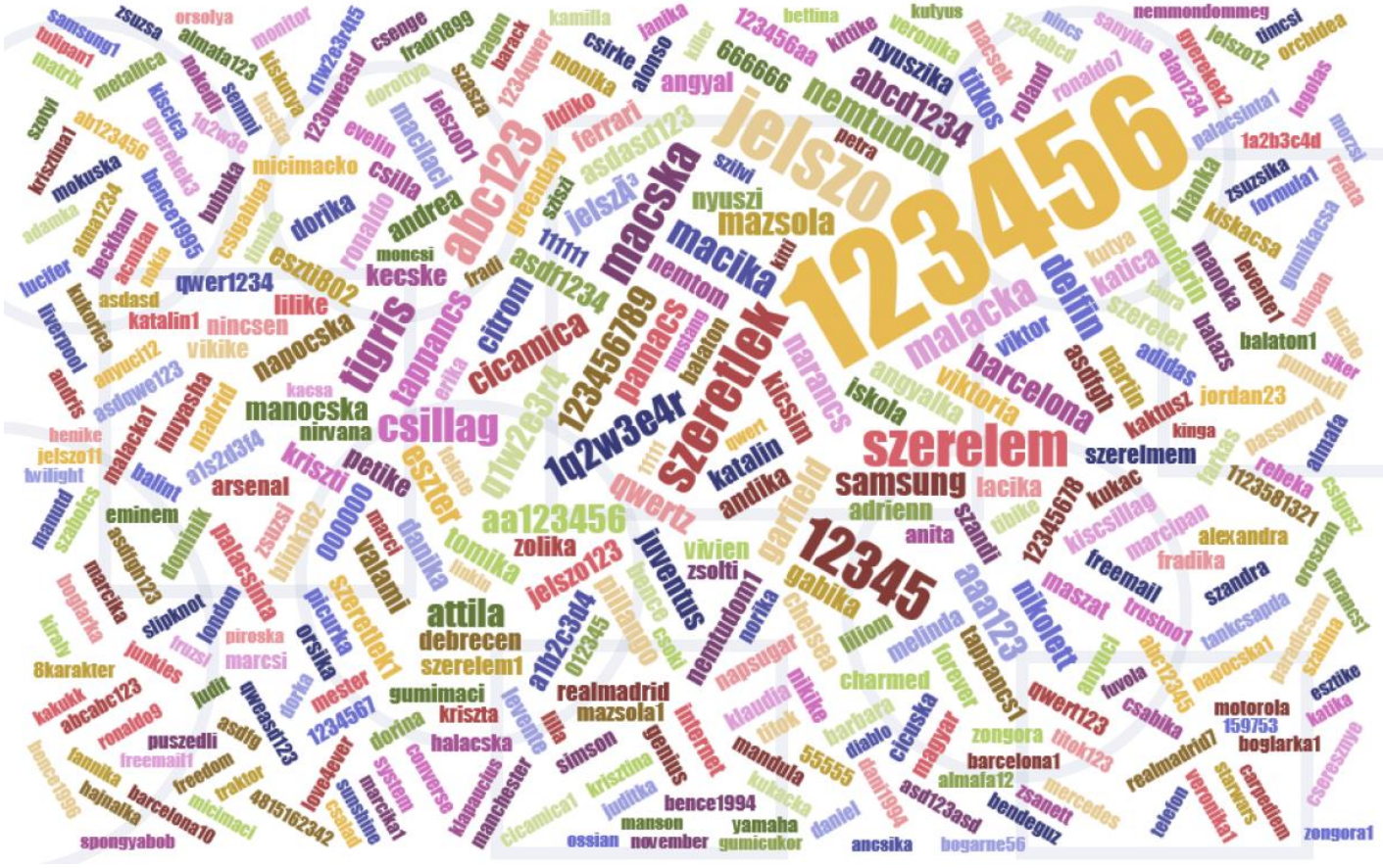
- ne írjuk fel egy fájlba, word dokumentumba gépünkön
- ne írjuk fel cetlire, monitor mellé, asztalunkra
- ne írjuk be a mobilunkba

Kezeljük külön!

Intézményi jelszavakat külön kezeljék a belépési adatoktól!

- felhasználónév kiosztása
- jelszó külön, akár nem is elektronikus úton történő kiosztása a Pedagógusoknak
- alapjelszavak (akár rendszeres) módosítása mindenkinek saját felelőssége

Jelszavunk ugye nincs a képernyőn?



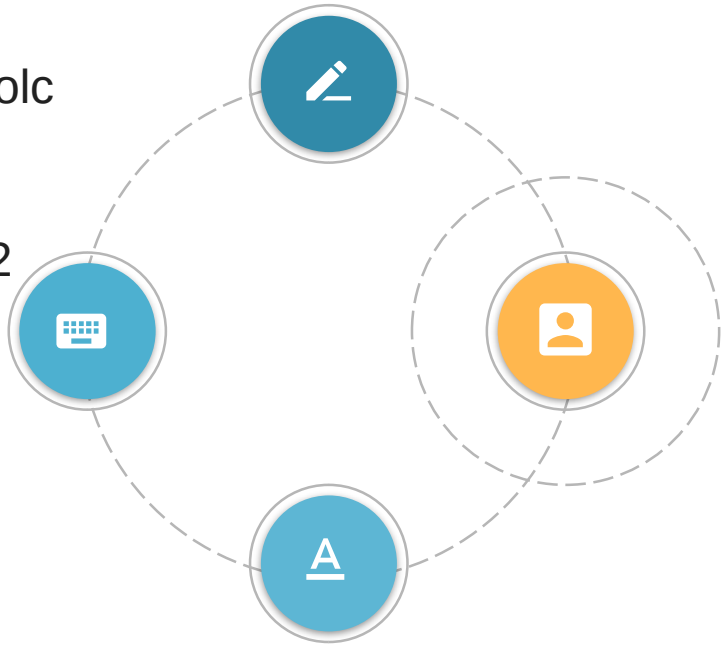
Feltört, magyarországi adatbázisok jelszó összesítése jelszó gyakoriság szerint

Rossz jelszóalkotás:

- szeretlek
- Szeretlek
- sz3r3tl3k
- Szeretlek123456
- Szeretlek!
- Zolika88
- Z0l1k@

Mi sem így alkotunk jelszót, ugye?

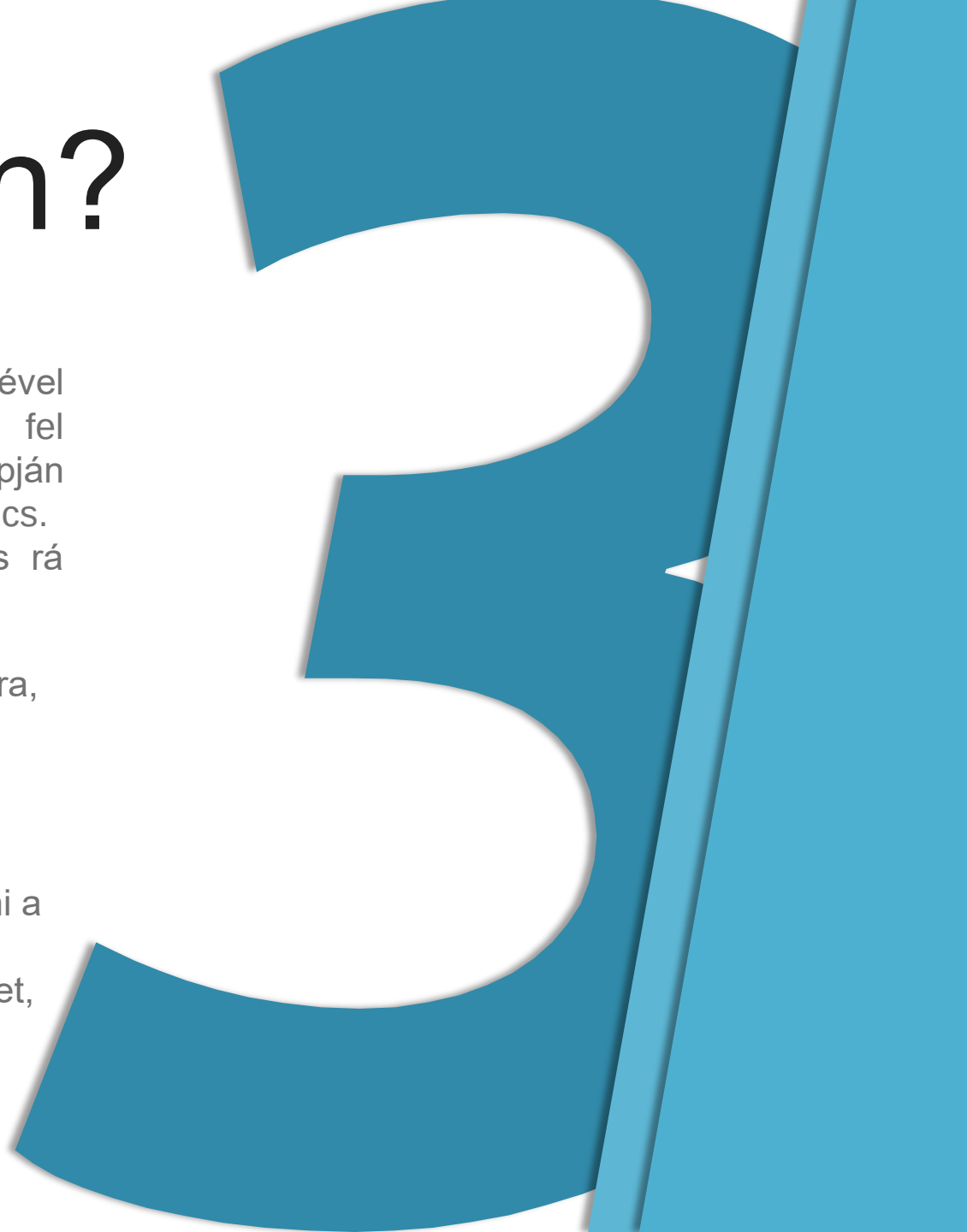
„jelszó” + szám:	Jelszó123, Jelszo1988, Jelszo!
gyerek/családtag neve + szám:	Zita3, Pisti98, 123Juli
saját keresztnév + szám:	Mate1988, 88Máté, Pál123
becenév + szám:	Petike88, Gabi98, 65Gabika, Zitus1
kedvenc virág + szám:	Tulipan12, 12Orchidea, Hóvirág9
kedvenc állat + szám:	Kutya33, Cica78, 16Bundás, Cirmi8
billentyűzet:	Qwertz123, qweASDyxc, 123qwe
születési dátum:	2001Januar15, 20010115
hónap neve + szám (dátum):	Január15, Februar2
város + szám:	Budapest2, 3500Miskolc
kedvenc ital + szám :	Unicum12, Bud2015
kedvenc film + szám:	Wasabi34, 99Wasabi
telephely, lakcím:	Maros19, KossuthTer2
projekt kód:	Támop113, Kofop435



Miért pont én?

Nagyon sokan a jelszavak kezelésével kapcsolatban számos kérdést tesznek fel magukban, és a rá kitalált válaszaik alapján megnyugszanak, hogy semmi teendőjük nincs. Azonban gondoljuk át a következőket, és rá fogunk jönni, hogy ez nem így van!

- Miért van szükségem biztonságos jelszóra, hiszen kit érdekelne a jelszavam?
- Miért szeretné azt valaki megszerezni?
- Miért pont az Én jelszavamat szeretnék feltörni?
- Nincs is semmi, amivel vissza tudnak élni a tanáriban lévő számítógépen!
- És ha valaki megszerzi az e-mail címemet, úgy sem tud vele mit kezdeni!



Miért pont Én?

1

Miért van szükségem biztonságos jelszóra, hiszen kit érdekelne a jelszavam?
Miért szeretné a jelszavamat valaki megszerezni?

A legtöbb támadás nem célzott, mindenki célpont, a nagy számok törvénye alapján dolgoznak az adathalászok is.

2

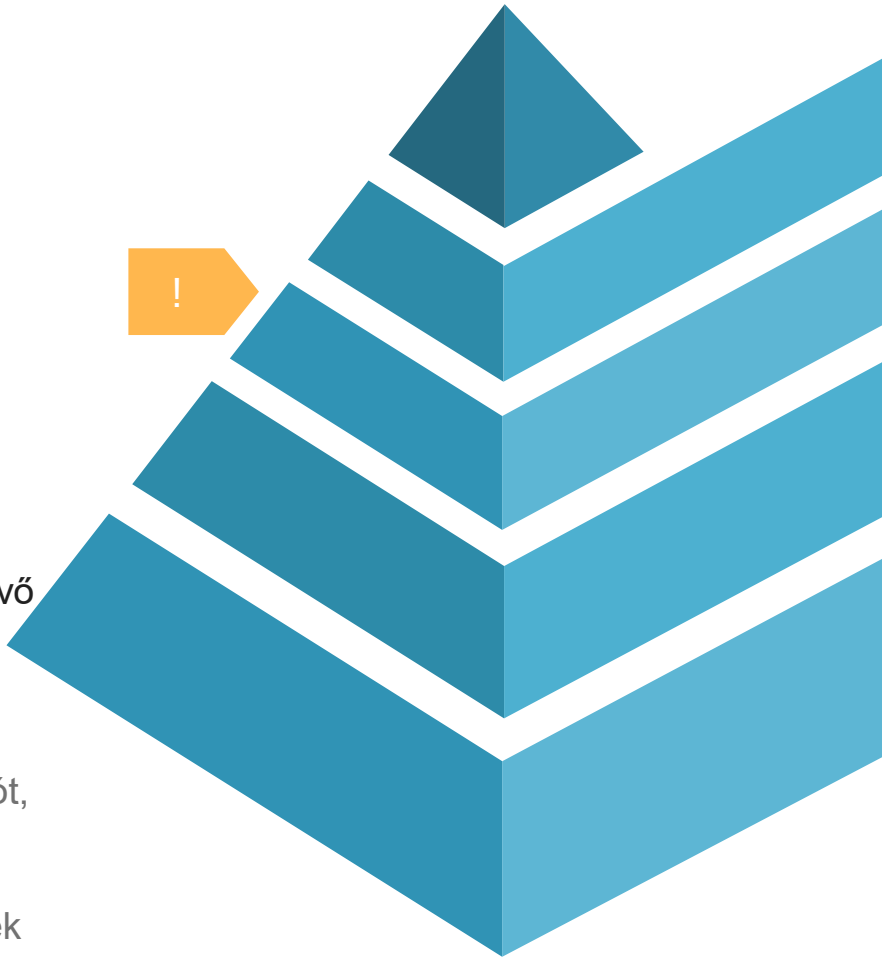
Miért pont az Én jelszavamat szeretnék feltörni?

A leggyengébb jelszavakat törik fel, és bárki nevével visszaélve, az Ő nevében járhatnak el akár egy internetes vásárlás, akár egy jegybeírás vagy intő rögzítése során.

3

Nincs is semmi, amivel vissza tudnak élni a tanáriban lévő számítógépen!
És ha valaki megszerzi az e-mail címemet, úgy sem tud vele mit kezdeni!

Legtöbbször nem azon az oldalon használják fel a jelszót, ahonnét megszerzik, hanem más oldalakon.
Akár az Én nevemben az ismerőseimnek vírusokat, adathalász, csaló leveleket, illetve üzeneteket küldhetnek az Én postafiókomból. Akár éveken keresztül. Nem lesznek boldogok az ismerőseim, az biztos.



Hogyan törhetik fel jelszavainkat?

Minden nap jelszavak elképzelhetetlen mennyisége kerül bűnözők kezére, és kezdik meg az adatok értékesítését, mintha csak a zöldségpiacon járnánk.

Az internet úgynevezett sötét oldalán fellelhető, szabadon elérhető és kereshető mintegy 1,4 milliárd (ebből 2,4 millió „.hu” végződésű) e-mail cím és a hozzá tartozó jelszó, s tanulmányok szerint ezen azonosítók és jelszavak 25%-a gond nélkül használható jelenleg is.

2017-ben kiszivárgott jelszavak (becsült érték):	
Vírus/billentyűzet leütést figyelő alkalmazás	788 000
Adathalászat	12 000 000
Feltört rendszerekből ellopott adatok	3 300 000 000

Belépési adataink titokban tartása

Ahogy a bankkártyánk PIN kódját is rejtve, másik kezünkkel eltakarva ütjük be, ugyan így járjunk el az e-Naplós jelszavunkkal is!

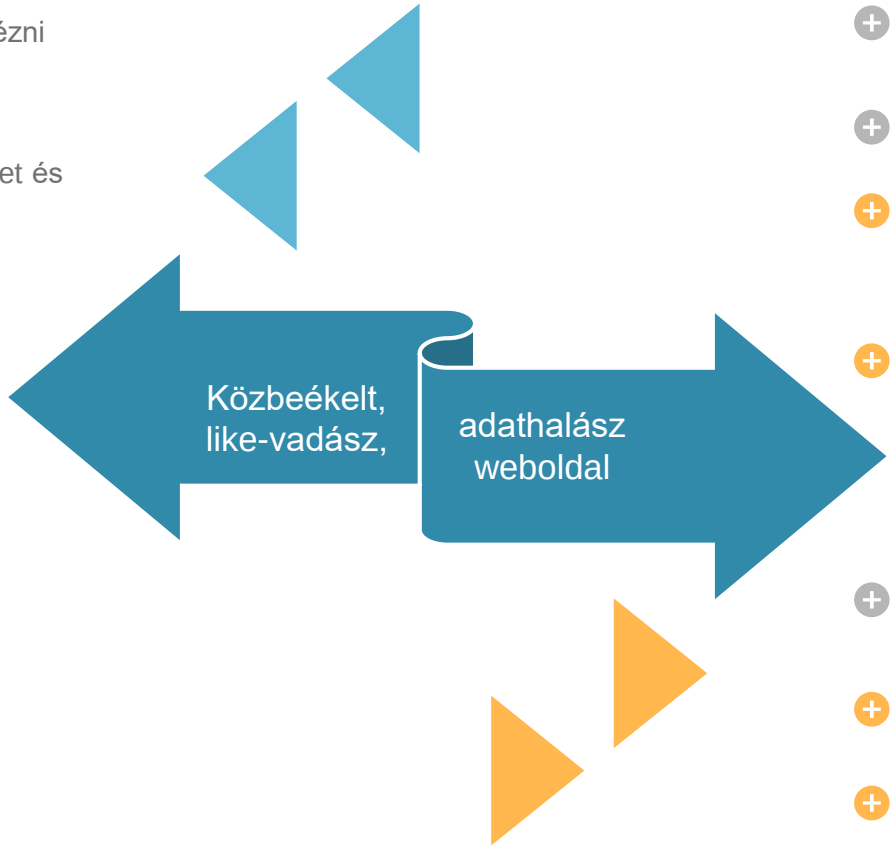
A mai tanulók a digitális korba születve különösen érzékenyek minden olyan eszközre és információra, ami „kütyü”-t érint. Ide tartozik az oktatás, a Pedagógusok és elektronikus eszközeik is, így nagyon fontos, ha tanuló jelenlétében jelentkezünk be bármilyen elektronikus rendszerbe, e-Naplóba, akkor a tanulókat kérjük meg, hogy lépjenek hátra, forduljanak el.
Hiszen a legegyszerűbb, ha valakinek leolvassuk a jelszavát, miközben azt beüti a számítógépe billentyűzetén keresztül.

Ugyan így fontos minden nyilvános, más által használható eszköz esetén jelszavaink mentésének megakadályozása, azaz **ne jegyeztessük meg** a böngészővel **bejelentkezési adatainkat kényelmi szempontból**, **mert az** igencsak **a biztonság rovására mehet**!

Adatlopás közbeékelt weboldal segítségével

az Áldozat, aki meggondolatlanul regisztrál egy weboldalon

- le szeretne tölteni egy file-t, megnézni egy videót egy weboldalon
- a weboldal regisztrációt kér (ehhez szükséges egy **e-mail cím**et és **jelszó**t megadnunk)
- biztonsági kérdésként megkérdezi tőlünk a weboldal kedvenc ételünk nevét, amit meg is adunk



az Áldozat igazi levelező rendszere

- a hamis oldal megpróbál belépni a megadott levelezési rendszerbe a megadott **e-mail cím** és **jelszó** segítségével
- ha nem sikerül a belépés simán, a levelezési rendszertől jelszó emlékeztetést kér nevünkben, akár az esetleges CAPTCHA biztonsági kép felhasználásával, ha lehet, biztonsági kérdés formát választva? (pl.: Mi a kedvenc ételünk?)
- a válasz birtokában új jelszót kap a levelezési rendszerünkben
- a címtárban szereplő, vagy a rendszeres levelezésben érintett címekre a nevünkben vírusos file-t, adathalász levelet, vagy „csak” SPAM leveleket küldhet a bűnöző

Ezért használjunk különböző jelszavakat minden elektronikus felületen és gondoljuk át on-line tevékenységünket!
Ha valami gyanús, zárjuk be a böngészőt, függesszük fel a regisztrációt/tevékenységünket!

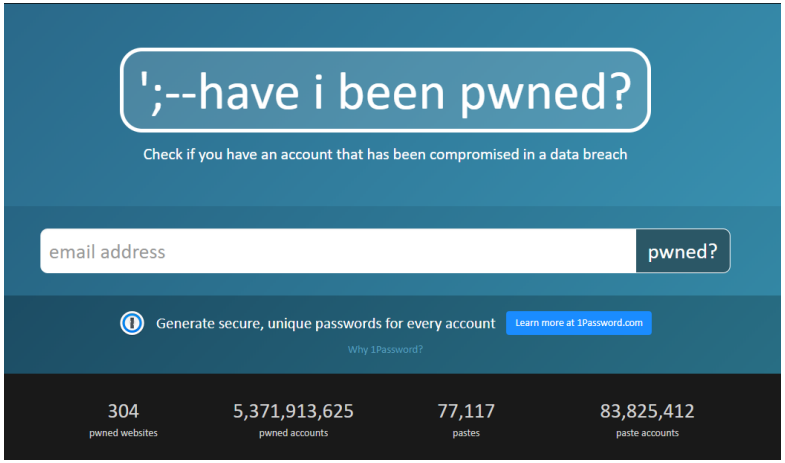

Badoo – gov.hu
675 db gov.hu végződésű e-mail cím, név, születési dátum és kódolt jelszó került ki az internetre a Badoo adatszivárogtatása során


LinkedIn – gov.hu
246 db gov.hu végződésű e-mail cím és kódolt jelszó került ki az internetre a LinkedIn adatszivárogtatása során

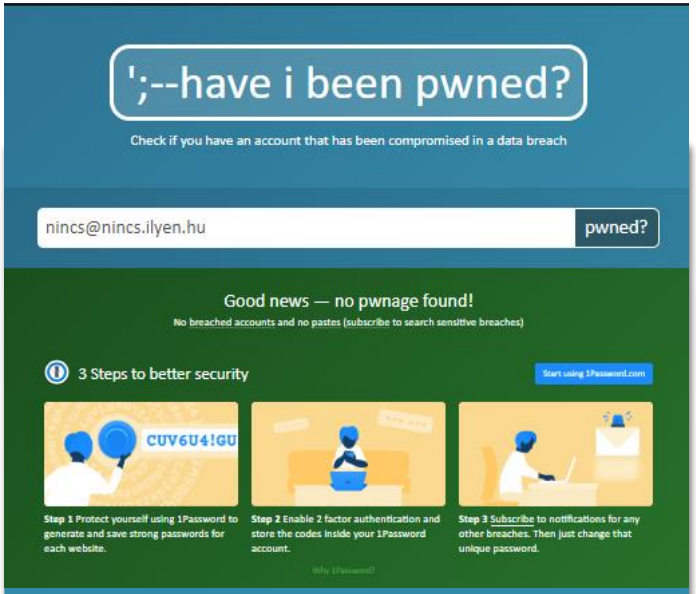
Érintett vagyok?

Az internet ebben is segíthet!

A https://haveibeenpwned.com/ weboldal segítségével másodpercek alatt kideríthetjük, hogy a jelenleg nyilvánosságra került adatbázisokban szerepelnek e akár hivatalos, akár magán jellegű e-mail címeink, felhasználó neveink!



≡ Érintett vagyok? - haveibeenpwned.com



nincs találat – JELENLEG ↑

az interneten jelenleg elérhető adatbázisokban a kereső nem találta meg felhasználó nevünket/e-mail címünket, ami nem azt jelenti, hogy nem tulajdonították el elektronikus adatainkat, „csak” még nem hozták nyilvánosságra az érintett értékeket

fel is iratkozhatunk, hogy az adataink megjelenéséről értesítést kapjunk

← találat – adataink szerepelnek kiszivárgott adatbázis(ok)ban

a listában megtekinthetőek azok az adatszivárogtatások, melyekben érintettek a keresett felhasználónév vagy e-mail cím adataink, így veszélyben lehetnek azok

javasolt lépések:

- az ezen rendszerekben lévő jelszavak cseréje
- nézzünk utána legalább kimenő postafiókunknak, nem használták e már most levélküldésre adatainkat
- figyeljük az érintett cég közleményeit az ügyben
- hasonló vagy azonos jelszavainkat más rendszerekben azonnal cseréljük le
- ha lehet, kapcsoljunk be kétfaktoros azonosítást (pl.: internetban – SMS)

6

Mégis mit tegyek?

Egyik lehetőségünk **jelszókezelő** alkalmazást használni, mely egy mesterjelszó védelmében az összes többi jelszavunkat tárolja, és a használat esetén automatikusan be is írja.

Ez kényelmes, és a minden felületen azonos jelszó használatánál sokkal biztonságosabb megoldás, azonban gépünk tényleges feltörése vagy a mesterjelszó kitudódása esetén ez sem tökéletes megoldás.

Másik lehetőségünk **jelmondat** használata.

Manapság sokkal biztonságosabbnak tekintik a szakértők, mint egy szimpla jelszót.

Mi az a jelmondat?

Jelmondat: Több szóból összerakott, mondatszerű biztonsági kód.

Miért biztonságosabb?

Napjainkra a bűnözők számára olyan programok, listák és adatbázisok állnak rendelkezésre, amikkel belátható rövid idő alatt ki tudják próbálni akár egy azonos szó különféle verzióit, még ha bizonyos karaktereket egyéb írásjelekre is cserélünk.
Ezért a szakemberek és kutatások már nem egy rövid, vagy viszonylag rövid, akár különleges karaktereket is tartalmazó jelszó használatát javasolják, amiknek megjegyzése is nehézkes a felhasználók számára, hanem olyan szavakból összetett, akár értelmes mondatokat alkotó jelmondatokat, melyek közvetlenül nem köthetőek hozzánk, minden felületen akár más verzióban is használhatjuk, és még a megjegyzésük sem okoz komolyabb megterhelést számunkra.

Példák szótár alapú jelszófeltörésre - howsecureismypassword.net

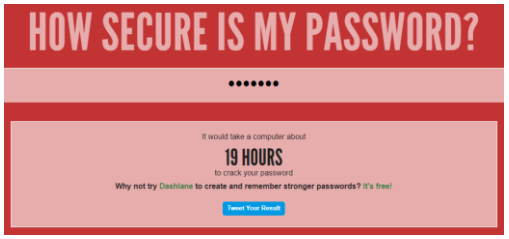
A jelszavak 50%-a szótár alapon feltörhető, és a megfelelő eszközök (elég nagy szótártábla, megfelelő számítógép) segítségével átlagosan 6 óra alatt visszafejthető egy 8 karakteres kód.
A több helyen is azonos jelszó használata csak fokozza a problémát!

1

123456

2013-ban a kitudódott magyar jelszavak toplistájának vezetője

feltörési idő: azonnal



feltörési idő: 19 óra

3

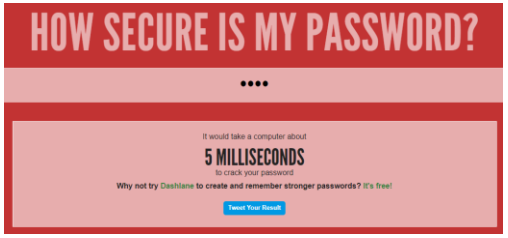
Jelszó!

Mondatszerű jelszó, de rövidsége miatt szintén nem okoz gondot a szótár alapú támadásnak, legfeljebb kicsit hátráltatja a feltörést

2

Áron

Párunk, gyermekünk neve, beceneve szintén a szótárak alapján elég gyorsan megfejthető



feltörési idő: 5 miliszekundum

feltörési idő: 7 milliárd év

4

Esik az eső!

Vegyesen használva különféle karaktereket a megfelelő hosszúságú, de értelmes mondat esetén

Milyen a jó jelszó?

Egy 32 millió jelszót érintő IT biztonsági kutatás arra jutott, hogy a vizsgált jelszavak 30%-a 6 vagy kevesebb karakterből állt, míg 60%-a csak betűket tartalmazott.

Az eddigiekben vázolt információk birtokában javasolt a jelenleg használt jelszavaink és azok kezelésének átgondolása, az esetleg szükséges változtatások megtétele, és az itt elhangzottak szem előtt tartása akár saját magunk, akár ismerőseink vagy munkahelyünk, de legfőképpen a tárolt adatok biztonságának érdekében.

Ellenőrzések

- Tartsuk titokban jelszavunkat, jelmondatunkat, ne írjuk fel cetlire, ne mentsük el egy file-ba vagy telefonunkba, használatakor takarjuk el kezünket
- Legyen könnyen megjegyezhető számunkra, de egyben ne legyen túl rövid, legalább 16 karakter javasolt (ez jelmondat esetén kb.: 3 - 4 szó)
- Ne használjunk olyan szavakat, adatokat, amik hozzánk köthetőek, elérhetőek közösségi vagy egyéb felületeken, használjunk akár véletlenszerű szavakat
- Használjunk minden felületen eltérő jelszót/jelmondatot
- Ha felmerül a gyanú, hogy jelszavunk kitudódott, cseréljük le azonnal!
- Ne hasonlítson semmilyen korábbi vagy máshol használt jelszavunkra

Ez minden?

A jelszavakkal kapcsolatos tudnivalókon kívül, bármilyen számítástechnikai eszközről is beszélünk, azért érdemes más dolgokat is átgondolni.

Ezeket nevezhetjük általános IT ismereteknek, vagy lassan a mindennapi élethez szükséges alapismereteknek, mint az olvasás, vagy írás.

Általános IT biztonság

számítástechnika ≠ számítógép

Sokan a számítástechnikát vagy informatikát a számítógéppel azonosítják, pedig az már rég több annál! Átfonja mindennapjainkat, és jelen van életünk minden percében.

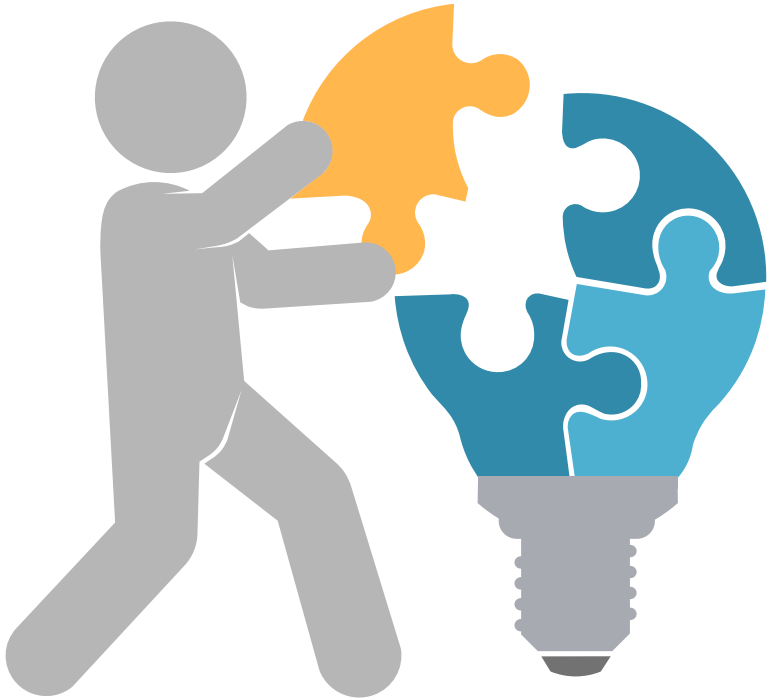
kiegészítők

A mai, modern okostelefonok nagyobb számítási kapacitással rendelkeznek, mint az első szuperszámítógépek, amik egész csarnokokat töltöttek meg. Az egyre népszerűbb okos órák és egyéb kiegészítők szintén IT eszközöknek számítanak!

Gondoljuk még át:

- egyre több helyen érhetőek el - akár ingyenesen használható - wifi lehetőségek, azonban a **nyilvános wifi hot-spot**-okon ne intézzünk banki ügyeket vagy olyan belépéseket, amik biztonsági kockázatot jelenthetnek, mert ezeken bárki könnyedén megfigyelheti adatainkat
- otthon kényelmes a gépünk/eszközünk megosztása a hálózaton, de egy **megosztott mappa** egy nyilvános hálózatban bárkinek betekintést enged adatainkba
- minden eszközön beállítható **jelszavas belépés**, **kód kérés**, elveszett vagy ellopott eszközök esetén ez nagy segítség lehet adataink védelmének érdekében
- eszközeink egy része állandó Bluetooth kapcsolatban van egymással, azonban az eszközök párosítása után javasolt annak **Bluetooth jel**ének **elrejtése**, nem csak energiatakarékosság, hanem a kártékony, szándékos belépéseket is megelőzendő

KRÉTA Tudásbázis



KRÉTA Tudásbázis

A KRÉTA Tudásbázis egy on-line webportál, ahol elérhetők a KRÉTA rendszerrel kapcsolatos valamennyi segédlet. A portál tartalmazza a KRÉTA rendszer különböző moduljainak részletes on-line felhasználói kézikönyveit, a fenntartók által – a különböző adatszolgáltatásokhoz - készített szakmai útmutatókat, a gyakran ismételt kérdésekre adott válaszainkat, továbbá számos videóval, tippek és trükkök bemutatásával is segítünk a KRÉTA rendszer használatában.

A Tudásbázis alábbi webcímen érhető el:
https://tudasbazis.ekreta.hu