Jelszavak és azok védelme

„Az a jó jelszó, amit rajtad kívül más nem ismer, és nem is tudják kitalálni!”

szerző: Dr. Albert Ágota, a MÁOK adatvédelmi tisztviselője

Ha már GDRP, akkor az adatvédelem mellett az adatbiztonság is terítékre kerül, hiszen **a ránk bízott adatokat** (meg nem utolsó sorban a saját és családunk adatait is) **kötelességünk gondos családapaként kezelni.** Ehhez pedig az egyik legkézenfekvőbb és legegyszerűbb megoldás **a jelszavaink helyes használata**.

Milyen a jó jelszó? Szakirodalom van bőven a témában, a felhasználók többsége viszont megelégszik az „almafa” típusú megoldásokat bízva abban, azt talán nem felejtik el. Számos alkalmazás azonban kifog rajtunk és speciális követelményekkel nyaggat minket (hosszúság, különleges karakter, szám, stb.), időnként akár az őrületbe is kergetve.

Azonban, ha az adott program nem kényszerít bennünket extra erőfeszítésre, még nem azt jelenti, hogy kényelmesen hátra dőlhetünk a „qwertz” vagy a „123456” sok-sok erőfeszítést igénylő kitalálása és bepötyögése után.

Már csak azért sem dőlhetünk hátra, mert a kamarai tagokon extra nagy felelősség van, hiszen nemcsak a saját maguk gyűjtögette adatokat kell óvniuk, hanem olyan nagy adatbázishoz is lehet hozzáférésük, mint a PetVetData, **a hanyag jelszókezelésük pedig komoly adatvédelmi incidenst is eredményezhet.**

Aki tehát úgy véli, hogy a jelenlegi jelszava nem elég erős, vagy meglehetősen régen élt utoljára a jelszóváltoztatás lehetőségével, válasszon most azonnal új jelszót!

Milyen a jó jelszó?

- ✓ legalább nyolc alfanumerikus karaktert tartalmaz (de van, aki a 12-re esküszik, mint minimum)
- ✓ kis- és nagybetűt is tartalmaz vegyesen,
- ✓ legalább egy számot tartalmaz,
- ✓ legalább egy különleges karaktert tartalmaz (például: ”+!%/=()#&@<>)

Az ékezetes betűkkel vigyázzunk, mert azok felismerése időnként még egy szimpla Windowsnak is erőn felüli kihívás, aztán hol beenged minket, hol nem, attól függően hogy emlékszik-e aktuálisan az általunk beállított magyar billentyűkiosztásra vagy sem.

És milyen a rossz jelszó?

- ✓ nyolcnál kevesebb karaktert tartalmaz,

- ✓ a jelszó szótárban megtalálható szóalak (nemcsak magyarul, hanem angolul, németül, stb.), és a szlengszótár sem ismeretlen a kódfeltöréssel foglalkozóknak,
- ✓ személyes információkat tartalmaz. Tipikusan gyakori példa erre
    - a családtagjaink születési dátuma (főleg ha még a Facebook-on is megtalálható az információ),
    - a házassági évfordulónk dátuma (bár biztos van egy-két házasságban élő, aki ezen a ponton feladná a párja jelszavának megfejtését),
    - kedvenc szuperhősünk neve (jedi, jamesbond, mylittlepony, stb.) illetve
    - a családtagjaink beceneve, hogy
    - olyan triviális megoldásokról ne is beszéljünk, mint négylábú kedvenceink neve (Buksi, Picur, Cirmi, Mici, stb.).

  Ha pedig akár mi, akár a családtagjaink a közösségi médiában éljük alternatív életünket, mindenképpen felejtsük el azokat a szavakat, amelyek a posztjainkban visszaköszönnek és bárki által megismerhetőek.
- ✓ munkánkhoz kapcsolódó információkat tartalmaz, például a rendelőnk nevét-címét, vállalkozásunk elnevezését, stb.
- ✓ népszerű szám- vagy betűmintákat tartalmaz (például aaabbb vagy 123321),
- ✓ gyakran használt tartalmaz még akkor is, ha előtte vagy utána számok állnak, esetleg fordított sorrendben szerepelnek a betűk (bond007, stb.).

Szakemberek javasolják, hogy **egyszerű szavak helyett operáljunk például kedvenc számunk, versünk, mondóként szövegrészletével**. Íme egy példa, a „nem minden szarka farka tarka”, alap jelszavasítva „nemmindenszarkafarka”. Ebből az alapból kedvünkre építhetünk fel variációkat, például

- „NemMindenSzarkaFarka”,
- „Nem1Minden2Szarka3Farka4”,
- „!Nem1Minden2Szarka3Farka4!”,
- a lustábbak meg koncentrálhatnak a kezdőbetűkre is „N1M2Sz3F4!”.

A lényeg, hogy elérjünk egy olyan ideális állapotot, amelyben még képesek vagyunk megjegyezni a betűk-számok-egyéb karakterek sorrendjét és ezzel egyidőben a jelszavunkra áhítozók dolgát is megnehezítjük. Persze az egész erőfeszítés semmit sem ér, ha utána a billentyűzetünk hátlapjára odaragasztjuk, biztos, ami biztos alapon.

Van, aki szerint a sok-sok általunk használt alkalmazás tekintetében úgyis képtelenek vagyunk megjegyezni melyik jelszót hova kell használnunk, így az egyetlen, nehezen megfejthető és általunk tökéletesnek ítélt jelszavunk mögé rakjunk kiterjesztést, hogy azért mégse használjuk mindenhol ugyanazt a pár karaktert, pl. „N1M2Sz3F4!@gmail”, „N1M2Sz3F4!@OTP”, „N1M2Sz3F4!@kamara”

A jelszó helyett a profik használhatnak jelkifejezést is, ezek nagyobb biztonságot nyújtanak a szótár alapú támadásokkal szemben, viszont kiváló emlékező képességet

igényelnek tőlünk (kivéve, ha például a szarkás verziót variáljuk át jelkifejezéssé). A jó jelkifejezés viszonylag hosszú és kis- és nagybetűk, numerikus és központozáshoz használt karakterekből áll, például „Az*?#>*@M7*&#!#tegnap Este.”

Vannak még egyéb követelmények is a biztonságos jelszóval szemben, például:

a) tilos ugyanazt a jelszót használni a kamarai fiókhoz, a PetVetDatához és más nem kamarai hozzáféréshez (például személyes használatú fiók, internetbank, aukciós oldal, stb.)
b) tilos a login nevünket jelszóként használni – meglepődnénk, egyes oldalakon hányan használják a login nevüket egyben jelszónak is, legalább mi ne tegyük ezt
c) **cseréljünk le időnként a jelszavunkat**, egyes vélemények szerint az ideális jelszó-változtatási intervallum minden negyedik hónap (az internetbankok például ki is követelik ezt és nem engedik a kettővel korábbi jelszavunkat sem újra használtatni)
d) **a jelszót tilos mással megosztanunk** (még akkor sem adhatjuk ki, ha szabadságra megyünk) és valamennyi jelszót érzékeny, bizalmas kamarai/praxis információként kell kezelnünk,
e) tilos a jelszavunkat e-mail üzenetben vagy az elektronikus kommunikáció egyéb formáiban elhelyezni, illetve telefonon keresztül se fecsegjük ki,
f) a jelszót ne írjuk le és ne tároljuk az irodában (rendelőben) és a mobilunkba se mentsük el. Ha mindenáron meg szeretnénk örökíteni, akkor lezárt borítékban helyezzük olyan helyre, amely a szokásosnál jobban védett (pl. széf), ebben az esetben egy esetleges illetéktelen hozzáférésről mindenképpen tudomást szerzünk.
g) **soha ne használjunk jelszó emlékeztetőt** (ha van ilyen lehetőség), mert annak segítségével igen könnyen feltörhető a fiókunk. A hol született kérdésre például hány honfitársunk írhatná be Budapestet? A kutyánk nevét meg pláne ne használjuk, ha a közösségi médiában rendszeren kiposztoljuk, Fifike milyen új kunsztokra képes. Arról meg ne is beszéljünk, ha nem akarunk banális választ adni a jelszó emlékeztetőre, hanem különlegeskedünk, az előre megadott emlékeztetős válaszunkat ugyanúgy el fogjuk felejteni, mint a jelszavunkat.

Ami pedig a legfontosabb, **bárki is garázdálkodik a mi jelszavunkkal, azért mi leszünk a felelősek,** hacsak be nem bizonyítjuk, mi mindent megtettünk a jelszavunk védelme érdekében.