

HOGYAN VÁLASSZUNK MAGUNKNAK JELSZÓT?

Egyre több jelszó és PIN kód áraszt el bennünket a bankkártyától a számítógépes rendszereken át a mobiltelefonig. Sokaknak ehhez kell hozzávenni a háztartási eszközök, beléptetőrendszerek és riasztók vagy a gépjármű különböző kódjait. Hogyan kezelhető biztonsági szempontból optimálisan ez a része a mindennapi életünknek?

Az egyszerű kódok könnyen megjegyezhetők, így nagy a kísértés, hogy minél egyszerűbb kódot válasszunk. Ez addig jó, amíg az egyszerű kóddal más nem él vissza. A biztonságban a megelőzés jobb, mint a kezelés, így következzen néhány megelőzést segítő tanács a jelszóválasztáshoz és kezeléshez.

Milyen a rossz jelszó?

Előbb nézzük, milyen a **nem megfelelő jelszó**. Alaptanács, hogy ne válasszunk olyan jelszót, ami:

ránk jellemző (becenév, családtag vagy háziállat neve, kedvenc focicsapat, és hasonló)
könnyen tippelhető (számsorozat, mint az 1234 vagy karaktersorozat, mint a qwerty)
túl rövid (2-5 karakter hosszú), ha egyáltalán van hossza („elég enter-t ütni és belépsz!”)
tartalmaz olyan karaktereket, melyek nem biztos, hogy minden esetben elérhetők (pl. ékezetes betűk)
szótári vagy ismert szó bármilyen nyelv szótárában vagy nyelvében

Ez utóbbi esetben idegen nyelvkörnyezetben sem nyerő ötlet valami ízes magyar kifejezés alkalmazása, ami szerintünk nem szerepel egy akadémiai kiadó szótárában. Volt rá példa, hogy kutatók Internet oldalakról és hírcsoportokból gyűjtött cikkek alapján állítottak fel szótárakat úgy, hogy az adott nyelvet nem is ismerték. Az egyes szavak gyakoriságát vették alapul, így az obszcén szavak és a szleng kifejezések is bekerültek a jelszókitaláló alkalmazás számára gyűjtött szótárba. Az okosabb jelszó-kitaláló programok még azt is kipróbálják, hogy a szótári szó elején vagy végén van-e szám, tehát az 'alma' helyett az 'alma2' jelszó választása csak nekünk macerásabb, mert hosszabb, de egy jelszókitaláló programnak nem nagy feladat erre rájönni.

A másik véglet a minél véletlenebb és összefüggéstelenebb jelszó választása, mert kísérletek is igazolják, hogy ezeket könnyen elfelejtik a felhasználók, és az elfelejtett jelszó cseréjével járó kellemetlenségek a rendszergazdákat is feleslegesen terhelik

Milyen a jó jelszó?

Az előzők alapján azt a következtetést vonhatjuk le, hogy **a jó jelszó**:

nem szótári szó,
van benne vegyesen betű, szám és speciális karakter is, így megfelelő hosszúságú
nem köthető az egyénhez, és
könnyű megjegyezni, hogy
ne írjuk fel, mert nem tudjuk megjegyezni,
és nem tartalmaz speciális ékezetes betűket

Amíg nem terjednek el az intelligens kártyás biometrikus azonosítással működő rendszerek vagy az egyszerűhasználatos jelszavak (azért emlékezünk az 5 M-re: Mit old meg, Mennyire jól, Mik az új problémák, Mennyiért, Megéri-e?), addig a statikus jelszavak és PIN kódok világát kell optimális módon alkalmaznunk. Jelenleg a célra legalkalmasabb jelszótípus a kódmondaton alapuló jelszó.

Mielőtt kiválasztjuk a megfelelő kódmondatot, ismernünk kell a korlátokat. Ha az adott rendszerben a jelszavak bármilyen hosszúak lehetnek, mert úgyis csak az első néhány karaktert veszik figyelembe, vagy a kis- és nagybetűket nem különbözteti meg a rendszer (érdeklődjünk a rendszergazdánál!), akkor felesleges hosszabb és vegyes kis/nagybetűs jelszót használnunk.

Optimális megoldás

A következő lépés a kódmondat alapjának kiválasztása. Ez lehet egy kedvenc mű részlete („Mily becsben áll a rossz, ha kiderül, hogy van még rosszabb?” mondja Shakespeare Lear királya). Az első rész rövid változata ékezetek nélkül minden páros karaktert nagy betűvel írva: 'mBaR', és ebbe csempészhető számjegy is, mondjuk a közepére '42', az élet értelme (ld. Douglas Adams: Galaxis Útikalauz). Egy kis speciális karakterrel fűszerezve előáll az 'mB_42aR' sorozat, amit a kitaláló könnyen megjegyez, és az általános követelményeket is teljesíti. Az adott rendszer specifikumát is be lehet csempészni az algoritmusba (pl. az adott szerver nevének első betűje), így már csak a levezetésre kell emlékeznünk.

A felhasználó válassza a kódmondaton és algoritmuson alapuló jelszót, mivel ugyanolyan könnyen emlékezetbe véshető, mint a naivul kiválasztottak, de elég nehéz kitalálni, mint a véletlenszerűen generált jelszavakat. Az algoritmosos változat több rendszer esetén is jól használható (ha több szerveren van azonosítónk, nem tanácsos mindenütt ugyanazt a jelszót alkalmazni) és véd az ellen is, ha az egyik helyen felfedik a jelszavunkat. Emlékezzünk, a biztonság nem termék, hanem eljárás, tehát nem ér sokat az optimális választás sem, ha a vonal lehallgatható, és így a mintaszerűen megalkotott jelszavunkat megszerzi a támadó, de ez ellen is lehet védekezni (ld. a **Kódolt kommunikáció** című anyagot).

Ezek után már a megfelelő humorérzéssel tudjuk kezelni az ilyen szólásokat: „A jelszavam a kedvenc papagájom neve, és mivel hetente jelszót kell cserélnem, most úgy hívom a papagájomat, hogy fgxZC2&!0_oéok”.