

**JELSZAVAK KEZELÉSE**

Amiből mindenkinek van

Régebben a katonáknak és a titkos társaságoknak volt jelszavuk. Emlékezzünk, hogy a Pál utcai grundra is a palánk ajtaján való négy egymás utáni szabályos koppantás azonosította, hogy nem idegen érkezik. Ma viszont mindenkinek van jelszava, nem is egy, hanem akár tucatnyi. De hogyan tudjuk kezelni őket?



A jelszavak ma már minden hétköznapi embert kétségbe ejtenek.

Ha lakótelepen lakunk, kapunk egy általában fix kapukódot, amivel igazolhatjuk a jogosultságot, magyarul, az adott számkombináció bebillentyűzésével nyithatjuk ki a kaput. Ha mobiltelefonunk van, a hangpostafiókunkhoz jár egy alapértelmezett jelszó. Ha internetszolgáltatóhoz tartozunk, illetve elektronikus postafiókunkba akarunk belépni, ezekhez is mind egy választott jelszó birtokában férhetünk hozzá. A munkahelyünkön is kódokat kapunk a városi telefonhívásokhoz, a csoportmunkához, a hálózati belépéshez. Ha ezekhez egyedi, erős

JELSZAVAK MEGJEGYZÉSE 1.**TÖRJÜK SZÉT, ÉS ASSZOCIÁLJUNK!**

149289665 – igen hosszú számsor, igaz? Viszont remek jelszó lenne. Megjegyezni nem könnyű, ha azonban széttördeljük, akkor rögtön barátságossá válik. 1492... mi sem könnyebb, Amerika felfedezésének dátuma: elég, ha annyit jegyzünk meg, hogy a számsor ezzel a dátummal kezdődik. 89665... nem túl barátságos, bontsuk tovább... 89. Hát ez semmire sem jó, egyelőre hagyjuk. 665: superkönnyen megjegyezhető szám, hiszen majdnem azonos a 666-tal, amit az Ómen filmekből jól ismerünk, csak éppen eggyel kevesebb. Eddig tehát van egy ilyen képletünk: Amerika felfedezése, +89, +ómen mínusz egy. Most már csak a 89-et kell „számszerűleg” megjegyeznünk (ha esetleg van egy eseményünk vagy születésnapunk 1989-hez, akkor még könnyebb dolgunk van) – az összes többi elemet asszociációk segítségével tároltuk el a fejünkben, ergó elfelejteni nagyon nehéz: készen is vagyunk! Máris memorizáltuk a nem túl egyszerű 149289665 számsort! A folyamat elméletileg bármeddig folytatható, persze mindenkinek megvannak a saját korlátai, de egy kis gyakorlással, ezzel a módszerrel legalább tizenhat-tizennyolc számjeggyel elboldogulunk.



cserélt jelszavakat választunk, amelyekre később emlékezni is akarunk, alaposan felköthetjük a felkötendőt. A jelszavak ma már minden hétköznapi embert kétségbe ejtenek.

Katasztrófális fantáziátlanság

Sokféle hibát követhet el egy átlagfelhasználó: például az operációs rendszeréhez könnyen kitalálható jelszót választ. Sokan vannak, akik elhosszabbítják a boltból a WiFi routert, kicsomagolják, és az adminisztrációs jelszót sem változtatják meg azonnal, azután csodálkoznak, illetve, ami még talán rosszabb, észre sem veszik a következményeket. Routers esetében mindig érdemes azonnal új adminisztrációs jelszót választani – ne a szomszéd vagy egy utcáról netező zárjon ki minket a saját hálózatunkból, valamint a titkosítást is érdemes a viszonylag erős WPA2-re beállítani. A jelszóválasztási fantáziátlanság az emberek többségénél világszerte katasztrófális. Az Errata Security vizsgálatának eredménye szomorú képet fest elénk. Az „123456” és a „password” a leggyakoribb választott jelszók. De a top10-es lista további elemei sem jobbakk, például: „qwerty”, „12345”, „12345678”, „1234”, „test”, „123”. Pedig hát egy jól kitalált karaktersorozat ingyen van, és nem letudni vagy kipipálni való nyugnek, hanem adatainkat védő, minket szolgáló eszköznek kellene felfogni a jelszóválasztási procedúrát. E téma gyakran szóba került a Conficker féreg kapcsán, hiszen ott a támadás egyik módszere éppen a hálózati gyenge jelszavak elleni szótáralapú támadás.

A telefon okos, a felhasználó kevésbé

Egy ausztrál fiatalember visszaélve a feltört telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett SSH-jelszót felhasználva írt egy C nyelvű férget, amely távolról belépett mások telefonjába, lezárta az SSH-portot, és felmá-

JELSZAVAK MEGJEGYZÉSE 2.

FOGLALJUK TÖRTÉNETBE!

67000123 – szintén egy nehéz számsor, ráadásul nem biztos, hogy itt is működnek az egyértelmű asszociációk. Ilyenkor bontsuk szét a számot, és keressünk mintákat. Ezt a számot például elég két részre bontani: 6700 és 0123. A 0123 könnyen megjegyezhető, elég lesz a 6700-at memorizálnunk, és valahogy hozzákötni a 0123-at, de hogyan? Nos, kerekítsünk egy kis történetet köré! Például: „Egyszer félretettem 6700 dollárt a bankban... de sajnos elköltöttem mindet... és megint el kellett kezdenem gyűjteni... dollárról dollárra... a nulláról. Aztán egy dollár, két dollár, három dollár...”

Ma már nem szükséges a Yahoo-t vagy a Gmailt feltörni ahhoz, hogy valakinek a postafiókjába be lehessen jutni.

solt néhány állományt, többek közt lecserélte az iPhone-háttérképet Rick Astley fotójára. Kíváncsi volt, vajon hány ilyen sebezhető készüléket talál, és állítólag száz föléi darabszámba lett így rá. A 21 esztendő Ashley Towns úgy gondolta, csak egy ártalmatlan tréfa, amit tesz. Úgy tűnik, valóban

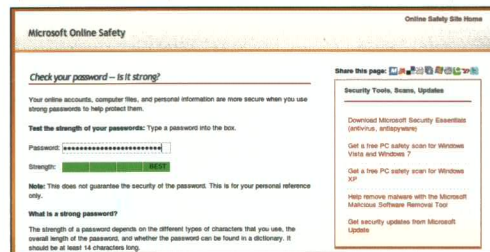
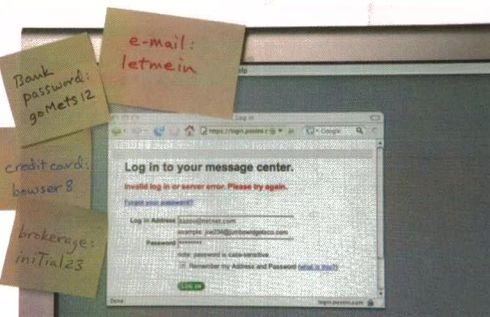
nem akart kárt okozni, és a feltűnően lecserélt háttérkép is ezt látszik igazolni. Csak azok a feltört telefonok voltak ilyen veszélyben, amelyeken fut ez az említett SSH-démon.

Sokan próbálnak különböző okok miatt megszabadulni a korlátozásoktól, és az ilyen esetek nyilván médiaértékűek az Apple-nek, hogy lám-lám, így jár, aki nem az egyenes utat választja. Azonban e támadás C programja nyilvánosságra is került, ezért várhatóan további,

kevesbé barátságos próbálkozások is megjelenhetnek majd. A védekezés egyébként egyszerű, nem más, mint egyedi SSH-jelszó beállítása.

Gyógymódok gyanú esetére

Ma már nem szükséges a Yahoo-t vagy a Gmailt feltörni ahhoz, hogy valakinek a postafiókjába be lehessen jutni. De legyen bármi is a módszer, mit tegyen az, aki gyanítja vagy éppen biztos benne, hogy a levelezését feltörték? A biztonsághoz való megfelelő hozzáállás az, hogy biztos információ nélkül, már pusztán gyanú esetén is úgy járjunk el, mintha biztosak lennénk a kompromittálódásban. Az okok keresésében és a teendők megválasztásában az alábbiak talán segíthetnek. – Az érin-



http://www.phenoelit-us.org/dpl/dpl.html

Default Password List

Last updated: 02.22.2010

Vendor	Model	Version	Access Type	Username	Password	Privileges	Notes
3COM	ComBuilder	7000-6000-3000-2500	Telnet	debug	system		
3COM	ComBuilder	7000-6000-3000-2500	Telnet	tech	tech		
3COM	HPNetARC	v4.1.1	Telnet	admin	(none)		
3COM	LANtroller	2500	Telnet	debug	system		
3COM	LANtroller	2500	Telnet	tech	tech		
3COM	LinkSwitch	2000-2700	Telnet	tech	tech		
Huawei	E860			admin	admin	Admin	
3COM	NetBuilder		SNMP	admin	8141	Admin	
3COM	NetBuilder		Multi	admin	(none)	Admin	
3COM	Office Connect (EON)	5.0	Telnet	n/a	PASSWORD	Admin	
3COM	SuperStack II Switch	2200	Telnet	debug	system		
3COM	SuperStack II Switch	2700	Telnet	tech	tech		
3COM	OfficeConnect 812		Multi	admin	admin	Admin	
3COM	Wireless AP	400	Multi	admin	comconcent	Admin	Works on all 3com wireless
3COM	ComPlex	7000	Telnet	tech	tech	User	
3COM	ComPlex	7000	Telnet	admin	admin	Admin	
3COM	ComPlex	7000	Telnet	operator	(none)	Admin	
3COM	HPNetARC	v4.1.1	Telnet	admin	(none)	Admin	



tett szolgáltató azonnali értesítése (pl. Gmailnél Google) az incidensről. Később az ő rendszernaplóik segíthetnek a tisztázásban, felderítésben is. Ilyen esetekben a szolgáltatók igyekeznek minden megtenni, és segítőkészek.

■ Használtam-e másik postafióknál, webes szolgáltatásban ugyanazt a jelszót? Mert ha igen, gyakori forgatókönyv, hogy egy jelszó megszerzésekor végigpróbálgatják az illető egyéb levelező-, csevegő-, webes, FTP-eléréseit, és gyakran nem eredmény nélkül. Ha igen a válasz, akkor a feltört helyszínen mindenképpen, és az esetleges megegyező jelszavú helyeken úgyszintén azonnali jelszócsere szükséges.

■ Használtam-e túlságosan beszédes, könnyen kitalálható jelszó-émlékeztető kérdést? Ha igen, akkor azonnal meg kell változtatni. Ha esetleg ezzel egyező jelszó-émlékeztető kérdés van másik helyszínen, akkor azt is módosítani kell.

Ugyancsak nem célszerű ész nélkül minden személyes adatot túlzottan kiplakátolni a közösségi oldalakra. A módszer ugyanis gyakran nem feltörés, nem jelszótalálgatás, hanem új jelszó igénylése. A születési hely és idő megszerzése ilyenkor nem okoz gondot, a titkos ellenőrző kérdés pedig lehet valamilyen részlete az életünknek. Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit a bulvárlapok hetente megírnak, vagy valaki önként kiteszi például az iWiW-es lapjára.

■ Használtam-e a jelszavamat nyilvános helyen: kávézóban, hotspoton, kileshette-e valaki a vállam felett? Találtam-e a kocsim mellett (direkt-véletlenül nekem csalinak odahelyezett) USB-kulcsot vagy egyéb eszközt, amit a gépembe később bedugtam? Ha bármelyik kérdésre igen a válasz, érdemes a jövőben ezekre kiemelten figyelni.

■ Adatvagyonleltár felmérése. Milyen bizalmas



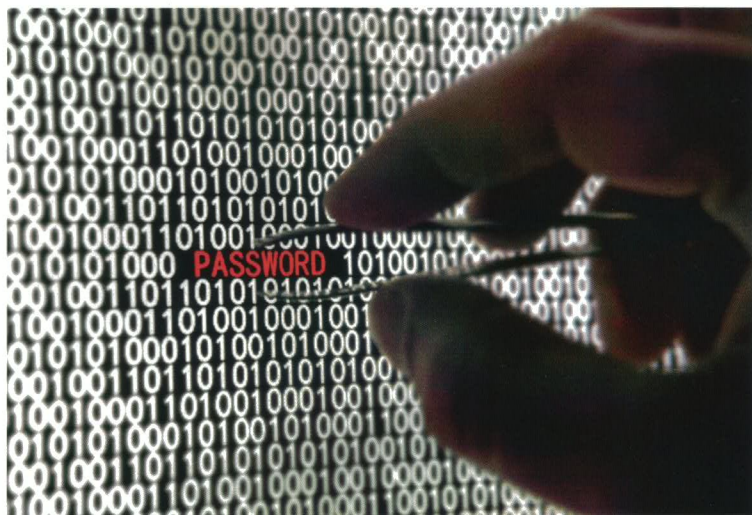
JELSZAVAK MEGJEGYZÉSE 3.

ÉNEKELJÜNK!

Ha nem boldogulunk a képzettársításokkal és a történetekkel, akkor énekeljünk! Meglepő tanács, de beválik: ha egy számsort vagy jelszót hangosan kimondva, esetleg énekelgetve memorizálunk, garantáltan eszünkbe fog jutni, még évek múlva is. A hangosan kimondott vagy elénekelt számok és szavak esetében az agyunk parancsot ad az állapotok izmainak, hogy formázzák meg a hangokat, és ha ezzel megvagyunk, a fülünk továbbítja a kimondott jelszót vissza az agyunkba. Ezzel jóval több helyen fordult meg a jelszó, mintha csak fejben próbáltuk volna meg memorizálni.



Routerek esetében mindig érdemes azonnal új adminisztrációs jelszót választani – ne a szomszéd vagy egy utcáról netező zárjon ki minket a saját hálózataunkból.



adatok voltak a levelezésben, amelyek, ha illetéktelen kezekbe kerültek, bajt okozhatnak? További szolgáltatások, munkahelyi elérések belépő jelszavai, partnereinkkel folytatott levelezések, magánéleti dolgok, amiket nem szívesen látnánk a subba blogon vagy a szanalmas.hu oldalon. Teendő lehet a levelekben szereplő összes account haladéktalan megváltoztatása, fontosabb üzleti partnerek figyelmeztetése, ismerőseink, rokonaink, barátaink értesítése, hogy postafiókunk áldozatul esett, és ha x-től – y időtartamig a nevünkben levelet kaptak, ellenőrizték le annak tartalmát velünk külön egyeztetve. 2010 márciusában ismeretlen elkövetők például a tulajdonos Propeller.hu nevében beadtak egy törlési kérelmet is a Google-hoz.

■ Ha bankkártyaszámok, elektronikus fizetési adatok is szerepeltek, akkor a banki egyenleg, tranzakciók azonnali vizsgálata a kétes időszakra. Ugyanez vonatkozik a fizetős online játékokra is (például World of Warcraft és hasonlók).



JELSZAVAK MEGJEGYZÉSE 4.

Ha végképp nem boldogulunk egy számmal vagy jelszóval, tegyük napi rutinná, mondjuk egy hónapon keresztül, minden reggel ismétljük el háromszor a tükör előtt, például fogmosás után. Egy hónap múlva garantáltan „beég”, és még évtizedek múlva is elő tudjuk hívni az emlékezetünkéből.

Érdemes fokozott óvatossággal viselkedni Facebook-, iWiW-, Myspace-profilunk jelszó-émlékeztető kérdéseivel kapcsolatban.

Az „123456” és a „password” a leggyakoribb választott jelszó.

- Beléptünk-e bármilyen webes levelezésbe, szolgáltatásba, és kipipáltuk-e az „Emlékezz rám” vagy a „Maradjak belépve” opciókat? Ha igen, üssünk a kezünkre, és többet ne tegyünk ilyet.
- Érdemes lehet egy alapos vírus- és kémprogram-ellenőrzést is tartani a biztonság kedvéért.
- Feljelentést tenni a rendőrségen az ügyben. Indokolt esetben mind a Google központjától, mind az érintett IP-cím aktuális felhasználójának internetszolgáltatótól való kikérése megtörténhet a nyomozás folyamán.
- Végül bízni abban, hogy nem lesznek további kellemetlenségek, és megfogadni szent esküvéllel az erős jelszó használatát, mindenhol másikat alkalmazni, és ezeket rendszeres idő-

közönként cserélni, valamint Facebook-, iWiW-, Myspace-profilunk jelszó-émlékeztető kérdéseivel kapcsolatban fokozott óvatossággal viselkedni a jövőben.

Nem bosszantani akar

A jelszóval való törődés nem azért van, hogy bosszantson minket, hanem hogy sikerrel szolgáljon, védjen bennünket, amit meg is tesz, ha mi is gondosan állunk hozzá. Ha rendszeresen cseréljük, kellően erőset választunk, és nem ugyanazt használjuk mindenhol, máris sokat tettünk – saját magunkért.

Persze igaz, ezek az erőfeszítések, jelszócsere munkát, folyamatos törődést és odafigyelést igényelnek, de akárcsak a biztonsági mentések készítésénél, itt is megtérül a befektetés, ha legyőzzük a lustaságunkat.

CSIZMAZIA ISTVÁN

KAPCSOLÓDÓ CIKKEK



techline.hu

- ▶ <http://ajanlo.techline.hu/jelszavak>
- ▶ <http://ajanlo.techline.hu/jelszotarolas>
- ▶ <http://ajanlo.techline.hu/biztonsag>



Nyitva a holnapra

PC vagy Mac? Tablet vagy netbook? Okostelefon vagy más okos megoldások?

A legfrissebb trendek, események és termékek az információ és a kommunikáció világában. Tesztek, elemzések, vélemények a HVG Online infoportálján.

www.techline.hu



techline.hu

a HVG IT portálja