Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

A jelmondatokról

Háttér

A jelszavak használata mára mindenapossá vált: használjuk az email-ek letöltéséhez, az internetes vásárláshoz szükséges online banki hozzáféréshez, vagy akár az okostelefonunkhoz. Azonban a jelszavaink egyben komoly támadási felületet is biztosítanak a bűnözők számára, mivel ha meg tudják azokat szerezni, meg tudnak személyesíteni bennünket, megszerezhetik a pénzünket, vagy akár hozzáférhetnek a személyes adatainkhoz. Az erős jelszó használata alapvető követelmény ahhoz, hogy meg tudjuk védeni magunkat. Az OUCH! e havi kiadásában bemutatjuk, hogyan hozzunk létre könnyen megjegyezhető erős jelszavakat, más néven jelmondatokat (passphrase).

A szerzőről

Guy Bruneau az IPSSC Inc. elismert biztonsági szakértője, a SANS oktatója és ISC (Internet Storm Center) elemzője. Guy SANS GSE előadásokat tart, illetve elvégezte a SANS Cyber Guardian képzést is. A Twitter-en **@GuyBruneau** csatornán található meg, illetve a SANS weboldalán, a **handlers.sans.org/gbruneau** címen.

A jelmondatok

Manapság egyre gyakrabban szembesülünk azzal a problémával, hogy a kiberbűnözők olyan kifinomult módszereket fejlesztenek ki, amelyekkel viszonylag könnyen ki tudják „találni” a jelszavainkat pl. az ún „brute force” támadás segítségével. Ez a gyakorlatban azt jelenti, hogy fel tudják törni a jelszavainkat, ha azok túlságosan egyszerűek. Ez ellen úgy védekezhetünk, ha kellően erős jelszót állítunk be saját magunknak. Minél több karakterből áll a jelszavunk, annál nehezebben lehet találgatással megfejteni. Ennek azonban az a hátránya, hogy a hosszú és bonyolult jelszavakat nehéz megjegyezni. Ezért inkább azt javasoljuk, hogy használjunk ún. jelmondatokat, amik gyakorlatilag olyan kifejezések vagy akár teljes mondatok, amiket könnyű észben tartani, viszont nehéz feltörni. Lássuk az alábbi példát:

„Hol van Mátyás király?”

Mitől válik ez jó jelszóvá? Nem csak attól, hogy 22 karakter hosszú, hanem attól is, hogy van benne nagybetű és szimbólum is (a szóköz és az írásjelek tartoznak ide). Tovább fokozhatjuk a jelmondat erősségét azzal, hogy kicserélünk bizonyos betűket szimbólumokra (például az „a” helyett írhatunk „@” vagy az „o” helyett „0” jelet). Ha egy weboldal maximálja a jelszóban használható karakterek számát, akkor érdemes annyit használni, amennyire lehetőségünk van.

A jelmondatok biztonságos használata

Természetesen a jelmondatok használatakor ugyanolyan óvatossággal kell eljárni, mint az egyszerű jelszavak esetén, ugyanis a jelmondat sem ér sokat, ha a bűnözők könnyedén meg tudják szerezni.

A jelmondatokról

1. Használjunk minden egyes eszközhöz és online felhasználói fiókhoz külön jelmondatot. Példának okáért soha ne használjuk ugyanazt a jelmondatot otthoni felhasználásra (Facebook, Twitter, Youtube, stb.), mint amit a munkahelyen vagy az online banki hozzáférésünkhöz. Ha a kiberbűnözők mégis megszerzik az egyik jelmondatot, akkor a többi fiókunk még mindig biztonságban van. Ha túl sok jelmondatot kell észben tartani (és ez elég gyakori manapság), érdemes megfontolni egy jelszókezelő program használatát, amely az összes jelmondatot képes biztonságosan tárolni. Ebben az esetben elég két darab jelmondatra emlékeznünk: egyik ahhoz kell, hogy belépjünk a számítógépre, a másik pedig a jelszókezelő programhoz.

A jelmondatok használata az egyik leghatékonyabb lépés abba az irányba, hogy megvédjük magunkat és a személyes adatainkat.

2. Soha ne adjuk meg senkinek a használt jelmondatokat vagy azt, hogy milyen módszerrel készítjük el azokat. Tartsuk észben, hogy a jelmondat egy titok. Ha bárkinek elmondjuk, többé már nem lesz biztonságos, ha ennek ellenére véletlenül mégis megosztjuk valakivel a jelmondatot, vagy arra gyanakszunk, hogy valahogy kitudódott, akkor azonnal változtassuk meg azt.

3. Akárcsak a jelszavaknál, a jelmondat esetén is tartózkodjunk a könnyen kitalálható vagy általánosan használtaktól. Például a „Four score and seven years ago” (Abraham Lincoln gettysburg-i beszédéből ismert részlet) nem igazán jó, mert túlságosan ismert.

4. Ne használjunk nyilvános számítógépet (hotel, könyvtár) arra, hogy belépjünk például a munkahelyi hálózatra vagy az online banki fiókba. Mivel az ilyen számítógépeket bárki használhatja, előfordulhat, hogy olyan káros szoftverrel van megfertőzve, amely megjegyzi a billentyűzet leütéseket. Online banki felületre vagy céges hálózatba csak megbízható számítógépről vagy mobil eszközről jelentkezzünk be.

5. Legyünk óvatosak az olyan weboldalakkal, amelyek azt kérik, hogy személyes kérdésekre válaszoljunk. Ezek a kérdések akkor használatosak, ha elfelejtettük a jelmondatunkat, és vissza szeretnénk állítani azt. Az a probléma az ilyen kérdésekkel, hogy az Interneten gyakran megtalálhatók a válaszok, de talán meg a Facebook oldalunkra is ki van írva. Ha személyes kérdésekre kell válaszolni, akkor csak olyan választ adjunk meg, ami nem nyilvános, vagy akár olyat, ami mi saját magunk találtunk ki. A jelszókezelő programok segítenek ebben, mert képesek további információkat is tárolni.

A jelmondatokról

6. Az online felhasználói fiókok gyakran biztosítanak ún. két lépcsős (két faktoros) hitelesítési lehetőséget. Ebben az esetben nem elegendő csak a jelmondat ahhoz, hogy belépjünk egy weboldalra, hanem szükség van még egy plusz azonosító információra is, amit például a telefonunkra küldenek SMS-ben. Ez a módszer sokkal biztonságosabb, mint ha csak a jelmondatra hagyatkoznánk, ezért érdemes igénybe venni, ha van rá lehetőség.

7. A mobil készülékek gyakran kérnek valamilyen PIN kódot ahhoz, hogy használni tudjuk azokat. Tartsuk észben, hogy a PIN nem más, mint egy jelszó. Minél hosszabb a PIN, annál biztonságosabb. Számos mobil eszköz lehetőséget ad arra, hogy a PIN-t lecseréljük valamilyen jelmondatra.

8. Ha már nem használunk egy felhasználói fiókot, akkor ne feledkezzünk meg arról, hogy lezárjuk, töröljük, vagy tegyük inaktívvá.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Kétfaktoros hitelesítés: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_hu.pdf

Jelszókezelő megoldások: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_hu.pdf

A pszichológiai manipuláció: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf

Általános biztonsági kifejezések: http://biztonsagosinternet.hu/tippek

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó