NEMZETI KIBERVÉDELMI INTÉZET

OUCH! | 2017. április

Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

Jelmondatok

Háttér

A jelszavak használata mindennapossá vált, az e-mailjeink vagy az online bankolástól kezdődően, egészen a termék vásárlásig vagy a mobiltelefonunkhoz való hozzáférésig. Azonban a jelszavak az egyik gyengepontunknak tekinthetőek, hiszen ha kitalálják vagy megtudják a jelszavunkat, akkor hozzá férést kapnak a fiókjainkhoz, megszerezhetik a pénzünket, elolvashatják a leveleinket, megszerezhetik a személyes adatainkat vagy ellophatják az identitásunkat. Ennek elkerülése érdekében elengedhetetlen az erős jelszavak használata. A jelszavak jellemzően zavarosak, nehéz megjegyezni és begépelni őket. Ebben a hírlevélben bemutatjuk, hogyan lehet könnyen megjegyezhető és begépelhető erős jelszavakat, más néven jelmondatokat létrehozni.

A szerzőről

My-NGoc Nguyen (kiejtve ME-Nop Wynn) minősített SANS oktató, valamint a Secured IT Solution ügyvezető igazgatója. A legmagasabb szintű tanúsítványokkal, valamint több, mint 14 év tapasztalattal rendelkezik kiberbiztonsági programok tervezése, fejlesztése terén különböző szektorokban és iparágakban. Twitter:**@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Jelmondatok

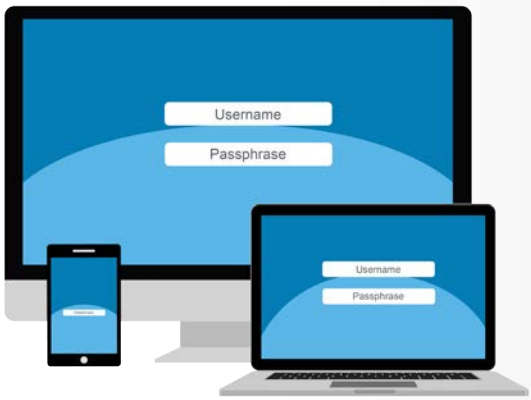
Mostanában azzal a kihívással szembesülünk mindannyian, hogy a kiberbűnözők kifinomult és hatékony módszereket fejlesztettek ki, arra, hogy megszerezzék a jelszavunkat az úgynevezett „brute force" azaz automatikus kipróbálás módszerével. Ez azt jelenti, hogy fel tudják törni a jelszavainkat, ha túl könnyen kitalálhatóak, gyengék. Önmagunk védelme érdekében nagyon fontos lépés az erős jelszó használata. Ez jellemzően komplex jelszavak létrehozásával érhető el, melyeket nehéz megjegyezni, zavarosak és nehéz begépelni. E helyett azt javasoljuk, hogy használjunk jelmondatot, szavak véletlenszerű sorozatát vagy egy mondatot. Minél több karaktert tartalmaz a jelmondat annál erősebb. Előnye, hogy ezeket sokkal könnyebb megjegyezni és begépelni, de ugyanakkor nehézséget okoz a kiberbűnözőknek a feltörése.
Két különböző példa a jelmondatra:

Fenntart- Könnyen- Bebörtönözni
Tea idő 1:23-kor

Nem csak a hosszúságuk teszi erőssé ezeket a jelmondatokat, hanem az, hogy tartalmaznak nagybetűket és szimbólumokat is (emlékezzünk: szóköz és írásjelek is szimbólumok). Ugyanakkor könnyű megjegyezni és begépelni is ezeket a jelmondatokat. A jelmondatot még erősebbé tehetjük, ha a betűket számokra vagy szimbólumokra cseréljük, mint például

Jelmondatok

az „a” betű kicserélhető a „@” szimbólumra, vagy az „o” betű a nullával. Ha egy weboldal vagy program limitálja a jelszóhoz használható karakterek számát, akkor használjuk fel a maximum karakterszámot a jelszavunkhoz.



A jelmondatok alkalmazása könnyű módja az erős és könnyen megjegyezhető jelszavak létrehozásának.

Jelmondatok biztonságos használata

A jelmondatok használatakor is óvatosnak kell lennünk, hiszen a jelmondat használata nem fog segíteni, ha a bűnözők könnyen ellophatják vagy lemásolhatják.

1. Minden felhasználói fiókhoz vagy eszközhöz használjunk különböző jelmondatot. Például ne használjuk ugyanazt a jelmondatot a munkahelyi vagy banki hozzáférésünkhöz, mint a személyes fiókjainkhoz (mint pl. a facebook, youtube vagy twitter). Így, ha valamelyik fiókunkat feltörték, akkor még a többi fiókunk továbbra is biztonságban van. Ha túl sok jelmondatot kell megjegyezni (ami elég gyakori) akkor megfontolandó egy jelszókezelő program használata. Ez egy speciális program, ami biztonságosan tárolja az összes jelmondatunkat. Így csak a számítógép és a jelszókezelő program jelszavára kell emlékeznünk.
2. Soha se osszuk meg senkivel - beleértve a munkatársainkat és a vezetőinket - sem a jelmondatainak vagy a stratégiánkat, hogy hogyan képezzük azokat. Ne feledjük, a jelmondat egy titok, ha bárki más megtudja a jelmondatunkat, akkor az már többé nem biztonságos. Ha véletlenül megosztjuk a jelmondatunkat valakivel, vagy ha úgy véljük, hogy a jelmondatunkat ellopták vagy kompromittálták változtassuk meg azonnal. Az egyetlen kivétel az lehet, hogy ha meg akarjuk osztani a fő személyes jelmondatunkat veszély esetére egy megbízható családtagunkkal. Így ha valami történik és segítségre van szükségünk, akkor a szeretteink hozzá férhetnek a főbb felhasználói fiókunkhoz.
3. Ne használjunk a felhasználói fiókjainkba való bejelentkezéshez olyan közösségi számítógépet, mint amik a hotelekben vagy internetkávézókban találhatóak. Mivel ezeket a számítógépeket bárki használhatja, előfordulhat, hogy fertőzöttek és minden billentyű leütést rögzítenek. Csak megbízható számítógépeken vagy mobil eszközökön jelentkezzünk be a felhasználói fiókjainkba.
4. Legyünk óvatosak az olyan weboldalakkal, amik személyes kérdéseket tesznek fel. Ezeket a kérdéseket elfelejtett jelszó esetén a visszaállításhoz szokás használni, létrehozni. Az a probléma ezzel, hogy a kérdésekre gyakran megtalálhatjuk a választ az interneten, vagy akár a facebook profilunkon is. Bizonyosodjunk meg róla, hogy ha személyes kérdésekre válaszolunk, akkor csak olyan információkat adjunk meg, amik nem publikusan elérhetőek vagy saját magunk által kitalált fiktív információk. Ha nem emlékszünk az összes biztonsági kérdésre adott válaszainkra, akkor válasszunk ki egy témát, mint például egy filmkarakter és arra alapozzuk a válaszainkat. A másik megoldási lehetőség ismét a jelszó kezelő program használata, melyek a legtöbb esetben képesek ezeket a kiegészítő információkat is tárolni.

Jelmondatok

5. Számos online fiók lehetővé teszi az úgynevezett kétfaktoros vagy kétlépcsős hitelesítést. Ebben az esetben a jelmondaton kívül további azonosító információra is szükség van a belépéshez, mint például a telefonra küldött hozzáférési kódra. Ez a módszer sokkal biztonságosabb, mint a jelmondat használata önmagában, ezért ha lehetséges mindig engedélyezzük és használjuk ezt az erős hitelesítő módszert.
6. A mobil eszközök gyakran igényelnek PIN kódot az illetéktelen hozzáférés ellen. Emlékezzünk arra, hogy a PIN nem más, mint egy jelszó. Minél hosszabb a PIN kód annál biztonságosabb. Számos mobil eszköz lehetővé teszi, hogy a PIN kód helyett jelmondatot vagy biometrikus azonosítást használjunk, mint pl. az ujjlenyomat.
7. Ha többé nem használunk egy felhasználói fiókot, akkor mindig zárjuk be, töröljük vagy tegyük inaktívvá.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Jelszókezelő:	https://securingthehuman.sans.org/ouch/2015#october2015
Két lépcsős azonosítás:	https://securingthehuman.sans.org/ouch/2015#september2015
Bejelentkezés zároló:	https://lockdownyourlogin.com
Öt napos képzés a kiberbiztonság alapjairól:	https://sans.org/sec301

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita