CTI Jelentés

Kulcs a digitális élethez – a biztonságos jelszókezelésről

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

A digitális világ számos előnye mellett, sok esetben nem kevés kockázatot jelent a személyes kapcsolat hiánya.

Vegyük például a hivatalos ügyintézést, amihez elegendő besétálni egy kormányablakba, igazolni magunkat egy személyazonosításra alkalmas okmánnyal, és már el is indíthatjuk az ügyintézést. Ilyen esetben a kormányablakban dolgozó ügyintéző a saját szemével és az okmányaink segítségével győződik meg arról, hogy mi valóban azok vagyunk, akiknek állítjuk magunkat, és hogy jogosultak vagyunk-e az adott ügyintézésre.

Számos ügyintézési folyamatot online is lefolytathatunk, méghozzá az Ügyfélkapu segítségével. Ilyenkor is be kell bizonyítanunk, hogy jogosultak vagyunk az ügyintézésre, amit legegyszerűbben egy felhasználónév és jelszó párossal tehetünk meg. Míg a felhasználónévvel azt állítjuk, hogy kik vagyunk, addig a jelszavunkkal megerősítjük, vagyis hitelesítjük, hogy valóban azok vagyunk, akiknek mondjuk magunkat.

Minél több online szolgáltatást veszünk igénybe, feltehetően annál több jelszavunk lesz, ami jelentős kockázatot jelent a digitális életünk biztonságára nézve. Hogy miért? Mert legtöbbször a számítógépes bűnözők célja, hogy jelszavainkat megszerezve hozzáférjenek a felhasználói fiókjainkhoz, eszközeinkhez vagy a munkahelyi szervezetünk rendszereihez. Sikeres hozzáférés megszerzése esetén a támadók további rosszindulatú műveleteket hajthatnak végre ellenünk vagy akár a nevünkben, például kizárhatnak minket a fiókunkból, megzsarolhatnak minket az adatainkért cserébe, de káros programokat is terjeszthetnek a fiókjainkkal.

Jelen dokumentumban igyekszünk bemutatni a jelszavainkra leselkedő veszélyeket és gyakorlati példákkal szemléltetni, hogy milyen következménye lehet annak, ha kompromittálják a jelszavainkat, illetve ismertetjük azokat a védelmi intézkedéseket is, amelyekkel jelentős mértékben csökkenthetők a jelszóhasználatból eredő kockázatok.

Mitől lesz rés a pajzson?

Erre a legrövidebb választ a gyenge jelszavak jelentik, de mit jelent az, hogy egy jelszó „gyenge"?

Gyenge jelszónak tekintjük a túl rövid, kizárólag egy karaktertípust – vagyis csak betűket vagy csak számokat – tartalmazó, a felhasználó személyéhez erősen kötődő jelszavakat, amiket ráadásul egynél több felhasználói fióknál is alkalmaznak.

Bár a weboldalak többsége általában a minimum 8 karakter hosszú jelszavakat követeli meg a regisztráció során, erősen javasolt a legalább 12 karakter hosszúságú jelszavak használata. Emellett ajánlott több karaktertípusból összeállítani a jelszavakat, például – kis-és nagybetűkből, számokból és speciális karakterekből (+,!, #, &,@, stb.). Minderre azért van szükség, mert minél hosszabb és minél több karaktertípusból áll a jelszó, a kiberbűnözőknek annál több időre van szükségük annak feltöréséhez.

A következő oldalon lévő Hive Systems táblázata alapján például jól látható, hogy míg a rövid, csak számokból vagy csak betűkből álló jelszavakat a számítógépes bűnözők azonnal képesek feltörni, addig a hosszabb, kis-és nagybetűket, számokat és szimbólumokat is tartalmazó jelszavak esetén ez már komoly kihívást jelent.

Különböző hosszúságú és karaktertípusokból álló jelszavak feltörési ideje 2022-ben

Tovább ront a helyzeten, amikor a felhasználók egy általuk erősnek, biztonságosnak vélt jelszót egyszerre több fiókjukhoz is beállítanak.

Ez olyan mintha az otthonunkhoz, az autónkhoz és a széfünkhöz, amiben az értékeinket tarjuk, külön-külön, de ugyanolyan kulcsot használnánk. Ha a három kulcs közül egyet elveszítünk vagy ellopják, akkor nem csak egy tulajdonunkhoz szerezhetnek hozzáférést a kulcs által, hanem mindháromhoz.

Azoknál a felhasználóknál, akik egyszerre több fiókjukhoz is ugyanazt a jelszót állítják be, jelentősen nő annak a kockázata, hogy az egyik fiókjuk kompromittálásával a támadók hozzáférnek a többi fiókjukhoz is.

Végül a gyenge jelszavak negyedik ismérve – amitől szintén könnyen kitalálhatóvá válhatnak – az, ha olyan szavakból állnak, amelyek erősen köthetők a felhasználó személyéhez. Ez a közösségi médiaoldalak elterjedésével együttesen kialakuló „információközlő társadalom" hatására vált kockázattá. A közösségi oldalak aktív felhasználói ugyanis sok esetben előszeretettel osztanak meg magukról olyan bensőséges, személyes vagy a személyükhöz szorosan kapcsolódó információkat, amelyekkel mások visszaélhetnek.

Ha egy közösségi oldal felhasználója például a kis házikedvence nevét és annak születési dátumát állítja be jelszónak (pl.: Cirmi2006 vagy Cirmi0314) és a megosztásai között szerepel egy vagy több olyan bejegyzés is, ami Cirmiről szól, felfedve a nevét, netán megemlékezés a születésnapjáról, úgy egy rutinos támadó könnyen kitalálhatja az adott felhasználó jelszavát.

Éppen ezért érdemes törekedni arra, hogy tartsuk meg magunknak az ilyen jellegű információkat, illetve érdemes kerülni a személyünkhöz szorosan kapcsolódó vagy személyünkkel összefüggésbe hozható jelszavak használatát.

Egy titok, amit őrizni kell

A jelszavunk kulcs a digitális magánszféránkhoz, amivel illetéktelen személyek komoly károkat okozhatnak nekünk. A biztonságos jelszókezelés egyik legalapvetőbb elvárása, hogy a jelszavak ne kerüljenek szándékosan megosztásra más felhasználókkal, beleértve az ismerőseinket, barátainkat és rokonainkat. Nem feltétlenül arról van szó, hogy ezzel a másik fél szándékosan élne vissza — bár ez sem zárható ki teljesen —, de elképzelhető, hogy nem járna el olyan körültekintően a jelszavainkkal, mint mi magunk, és gondatlanságból vagy figyelmetlenségből okozna számunkra fejfájást. Különösen magas kockázatot jelent jelszavaink megosztása, ha esetleg azokat más fiókoknál is használjuk.

Sajnos több felmérés is azt bizonyítja, hogy a felhasználók gyakran kiadják jelszavaikat, ami különösen igaz az online streaming szolgáltatások tekintetében. A Netflix például közel 100 millióra teszi azok számát, akik előfizetés nélkül, jogtalanul férnek hozzá a tartalmaihoz, és bár a szolgáltató már tett lépéseket ezügyben, a jelszómegosztásra vonatkozó gyakorlaton sajnos ez nem változtat.

Munkahelyi jelszavak kezelésével kapcsolatban a szervezet saját információbiztonsági szabályzatában (IBSZ) meghatározott rendelkezések a mérvadók, ami nagy valószínűséggel tiltja, hogy jelszavainkat más tudomására hozzuk, ezért a legjobb, ha az IBSZ-ben foglaltak szerint járunk el.

Hogyan szerezhetők meg a jelszavak?

Jelen fejezetben bemutatásra kerül néhány olyan gyakori módszer, amivel a támadók megszerezhetik a felhasználók jelszavait. Bár a jelszavak megszerzésére számos módszer létezik, csak az 5 leggyakoribb támadási módszer kerül általunk bemutatásra.

Brute force

A brute force, más néven kimerítő próbálgatáson alapuló támadási módszer, ami szisztematikus próbálgatást jelent. Lényege, hogy a támadók a különböző karakterek (betűk, számok, speciális karakterek) lehetséges kombinációjából próbálják összeállítani a jelszót. Ez a technika jellemzően csak a rövid, egyszerű jelszavak esetén célravezető.

Szótár alapú támadás

Ez a támadási módszer a brute force egyik fajátja, ahol a támadók a karakterkombinációk helyett értelmes szavakkal és gyakran használt jelszavakkal próbálnak meg bejelentkezni. Az ilyen jellegű támadásokhoz olyan adatbázisokat használnak, amelyekben egyszerű kulcsszavak, korábban kiszivárgott jelszavak és mindezek ún. „leetspeak" kombinációi szerepelnek.

Leetspeak: az egyes betűk más karakterekkel, például számokkal vagy speciális karakterekkel történő helyettesítése. A „Jelszó" szónak a leetspeakje lehet például J3lsz0, j3152ó, _|3152ó, stb. Léteznek ilyen online is elérhető fordító programok, például a md5decrypt.net.

Az ESET biztonsági cég szerint ezek a 20 leggyakrabban használt jelszavak 2023-ban:

Position	Password	Position	Password
1	password	11	1234567
2	123456	12	1234
3	12123456789	13	1234567890
4	guest	14	000000
5	qwerty	15	555555
6	12345678	16	666666
7	111111	17	123321
8	12345	18	654321
9	col123456	19	7777777
10	123123	20	123

A fenti táblázatban szereplő jelszavak akár brute force, akár szótár alapú technikával szinte azonnal feltörhetők, ugyanis amellett, hogy általában egy karaktertípusból állnak és rövidek, nagy valószínűséggel szerepelnek a támadók adatbázisaiban.

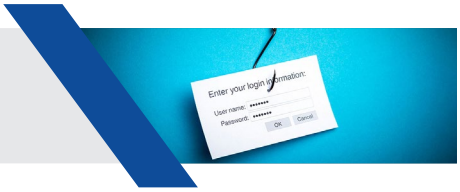
Password spraying

Másnéven jelszóspray-támadás, amiszintén egyre gyakoribb módszer a jelszavak feltörésére. A módszer lényege, hogy a támadók a felhasználónevekhez gyakran használt jelszavakat párosítanak, hogy megtalálják az összetartozó felhasználónév + jelszó párost. Ezzel a módszerrel – a brute force technikához képest – sokkal nagyobb felhasználói bázis vehető célba kevesebb próbálgatással, aminek köszönhetően a támadók képesek elkerülni a brute force elleni fiókvédelmi megoldásokat (például a bejelentkezési kísérletek számának korlátozását).

Credential Stuffing

A támadások során a hitelesítő adatok automatizált kitöltése a korábban kiszivárgott vagy ellopott felhasználónév és jelszó párosokat tartalmazó adatbázisokkal történik. Az ilyen támadások sajnos 2%-os sikerarránnyal működnek.

Adathalászat



A korábbiakban felsorolt módszerekkel ellentétben, az adathalászat során a támadók nem feltörik a felhasználók jelszavait, hanem valamilyen megtévesztéssel ráveszik őket, hogy maguk adják át azokat. Ezt általában azzal érik el, hogy a megkeresések során megszemélyesítenek valakit vagy valamilyen szervezetet. Mindezt leggyakrabban e-mail, SMS vagy közösségi média hálózaton keresztül küldött üzenet formájában teszik, de előfordulhat az is, hogy telefonon keresik fel az áldozatokat. Az adathalászatról egy korábbi, Adathalászat – a leghatékonyabb kiberfegyver című kiadványunkban olvashatnak bővebben.

Amiről a felhasználó nem tehet - kiszivárgott jelszavak

Egyre gyakrabban fordul elő, hogy a kiberbűnözők a jelszavak megszerzése érdekében nem közvetlenül a felhasználókat, sokkal inkább az online szolgáltatókat veszik célba. Ilyenkor az elkövetők különféle támadási módszerekkel hozzáférést szereznek a weboldalak infrastruktúráihoz, beleértve a különféle adatokat, például a felhasználói bejelentkezési információkat tartalmazó adatbázisokat is.

Adatszivárgásnak nevezzük azokat a biztonsági eseményeket, amelyek során valamilyen váratlan esemény hatására a védett, bizalmas adatok kikerülnek védett közegükből, így azokhoz arra nem jogosultak is hozzáférhetnek.

Sajnos az adatszivárgások ellen nem sokat tehetnek a felhasználók, hiszen ők csak közvetetten érintettek az ilyen jellegű támadásokban.

Érdemes figyelemmel kísérni az adatszivárgásokról szóló híreket, különösen azon platformok esetén, amelyeken mi magunk is rendelkezünk felhasználói fiókkal. Amennyiben arról értesülünk, hogy adatszivárgás történt az egyik online szolgáltatónknál, ajánlott mielőbb lecserélni az adott oldalon használt jelszavunkat, illetve azoknál a felhasználói fiókjainknál is, ahol – az ajánlások ellenére mégis – ugyanazt a jelszót használjuk. Fontos, hogy a jelszóváltoztatás során törekedjünk az egyediségre, így minden felhasználói fiókunkhoz más és más jelszót állítsunk be!

Az Európai Unió Általános Adatvédelmi Rendeletének (GDPR) értelmében a szolgáltatók például kötelesek tájékoztatni az érintetteket az adatvédelmi incidensről, „ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül". A GDPR-ról bővebben olvasható az „Ezeket érdemes tudni a GDPR-ról és a webes sütikről" című korábbi elemzésünkben.

Mihez kezdhetnek a számítógépes bűnözők az ellopott jelszavakkal?

Máig vannak olyan felhasználók, akik azt állítják, hogy ők nem bánják, ha más is hozzáfér akár az e-mailjeikhez, telefonjukhoz vagy egyéb felhasználói fiókjaikhoz, mert nincs mit titkolniuk. A következőkben néhány példán keresztül bemutatásra kerül, hogy milyen következményekkel jár egy-egy felhasználói fiók kompromittálódása, valamint milyen további károkat okozhatnak mindezzel az elkövetők ránk, ismerőseinkre, barátainkra, családunkra és más felhasználókra nézve.

Kompromittált e-mailfiókok

Talán az egyik legkritikusabb online szolgáltatás az e-mailfiók, hiszen a beérkezett levelek között nem csupán a személyes és hivatalos megkeresések, ügyintézéssel kapcsolatos információk találhatók meg, hanem olyan levelek is, amik más weboldalakra történő regisztrációról vagy egyéb online szolgáltatás igénybevételéről szólnak. Ilyen lehet például egy közösségi oldal vagy internetbanki regisztrációt megerősítő e-mail, egy webáruházban leadott rendeléssel kapcsolatos tájékoztató üzenet stb. Éppen ezek miatt, ha arra nem jogosult személyek hozzáférést szereznek az e-mailfiókunkhoz, gyakorlatilag az összes tárolt információhoz is hozzáférnek.

Továbbá bárki számára levelet küldhetnek a nevünkben, akár hivatalos szerveket is megkereshetnek vagy például pénzt is kérhetnek az ismerőseinktől, barátainktól és családtagjainktól, de használhatják káros kódok terjesztésére is a levelező fiókunkat.

Ezen kívül további következményekkel is lehet számolni, például azzal, hogy kizárnak minket a fiókjainkból. A legtöbb online szolgáltatás igénybevétele során e-mail címet és jelszót kell megadniuk a felhasználóknak, amikkel a későbbiekben hozzáférhetnek majd a profiljukhoz. A weboldalak biztosítanak egy „Elfelejtettem a jelszavam" lehetőséget, arra az esetre, ha a felhasználók nem emlékeznének a jelszavukra. A weboldalak általában ilyenkor a regisztráció során megadott e-mailcímre küldenek egy linket, amire kattintva a felhasználók megadhatják majd az új jelszavukat. Ha illetéktelenek hozzáférnek a levelezésünkhöz, és látják milyen oldalakra regisztráltunk korábban, könnyen elvégezhetik az előbbiekben leírt műveletet, ellehetetlenítve számunkra a weboldalakra történő belépést. Sőt, azt is megtehetik, hogy további weboldalakra regisztrálnak a nevünkben, például társkereső vagy pornóoldalakra.

Feltört közösségi oldalak

Közösségi oldalak esetén is igen súlyos következményekkel lehet számolni, ha valaki, aki arra nem jogosult, hozzáférést szerez a fiókunkhoz. Az e-mailekhez hasonlóan a támadók itt is elérhetik a profilunkhoz társított összes információt, beleértve a nyilvános és a mások elől elrejtett, privát adatokat is. Sőt, amennyiben úgy tartja kedvük vagy érdekük, módosíthatják is azokat, valótlan információkat tehetnek közzé rólunk az interneten, olyanokat is, amik számunkra akár kellemetlenek és kínosak lehetnek.

Ha mindennek a tetejében még ki is zárnak a fiókunkból, semmit sem tehetünk ezek megakadályozása érdekében azon kívül, hogy egy másik kommunikációs csatornán megkérjük az egyik ismerősünket, hogy a platformon jelentse a feltört fiókunkat.

Feltört közösségi profilok esetén is lehet számítani arra, hogy a nevünkben – különböző célzattal - felkeresik az ismerőseinket, például azzal a kéréssel, hogy kattintsanak egy rosszindulatú linkre vagy küldjenek pénzt, amit persze majd a nevünkben írogató csaló fog bezsebelni.

A közösségi oldalak biztonságos használatáról bővebb információk érhetők el a „Tanácsok a biztonságosabb Facebook és közösségimédia-használathoz" című elemzésünkben.

Jogosulatlan hozzáférés a netbank fiókhoz

Talán mindenki egyik legnagyobb félelme, hogy ellopják a megtakarítását, így - ha az előzőekben felsorolt következmények nem is - ez biztos eléri a megfelelő ingerküszöböt.

Szerencsére napjainkban a pénzügyi szolgáltatók szigorú védelmi előírásainak köszönhetően, olyan biztonsági intézkedések kerültek kikényszerítésre, amelyek jelentősen megnehezítik a támadók dolgát. Ezeknek az intézkedéseknek köszönhetően már nem elegendő, hogy a számítógépes bűnözők megszerezzék a felhasználók jelszavait, további ellopott adatra vagy megfertőzött eszközökre is szükségük van ahhoz, hogy hozzáférjenek a célszemély banki fiókjaihoz.

Amennyiben egy csaló mindezen védelmi intézkedések ellenére mégis hozzáférést szerez egy felhasználó netbankjához, úgy az ott lévő teljes összeget is ellophatja, jelentős anyagi károkat okozva ezzel a felhasználónak.

A banki, illetve más online vagy telefonos csalások elleni védekezéshez nyújt segítséget a KiberPajzs elnevezésű együttműködés, amely a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság együttműködésével jött létre.

Kiberpajzs kampánykép

Hogyan készítsünk erős jelszavakat?

Ebben a fejezetben ismertetésre kerül, hogy milyen tulajdonságoktól válik egy jelszó erőssé, illetve néhány olyan módszer is bemutatásra kerül, amelyekkel erős jelszavak hozhatók létre.

Erős jelszónak tekinthetjük az egyedi, minél hosszabb, de legalább 12 karakter hosszú, kis-és nagybetűket, számokat, valamint speciális karaktereket tartalmazó és a felhasználó személyéhez szorosan nem köthető jelszavakat.

Szavak helyett jöhetnek a jelmondatok

Hogy a jelszavunk megfeleljen a fenti kritériumoknak, érdemes számunkra könnyen megjegyezhető mottóban, szlogenben vagy legalább négy szó összefűzéséből álló jelmondatban gondolkodnunk. Jelmondatok alkotásakor kifejezetten előnyös a szleng kifejezések és becenevek használata.

Például:

pöpec mondat lesz a belépőm -> popecmondatleszabelepom

Még biztonságosabbá tehetjük az így alkotott jelszavunkat, ha egyes betűket számokra cserélünk és váltogatjuk a kis- és nagybetűket, valamint speciális karakterekkel is kiegészítjük a mondatot.

Például:

popecmondatleszabelepom -> p0p3c#m0Nd4t?lEsz!4_b3l3'P0"m

A fenti példában bemutatott jelszó bár erős, eléggé nehezen megjegyezhető, főleg, ha minden felhasználói fiókunkhoz hasonló nehézségű jelszót állítunk be. Megkönnyíthetjük a dolgunkat, ha a fenti folyamatot egy bizonyos szisztéma szerint végezzük el, például adott betűket mindig adott számokra cserélünk (pl.: a ->4, e ->3) vagy bizonyos rendszer szerint használjuk a speciális karaktereket (pl.: szavak elválasztása #-el vagy *-al stb.). Ezzel a módszerrel elég csak az eredeti jelmondatot észben tartanunk.

Másra is bízhatjuk a jelszógenerálást

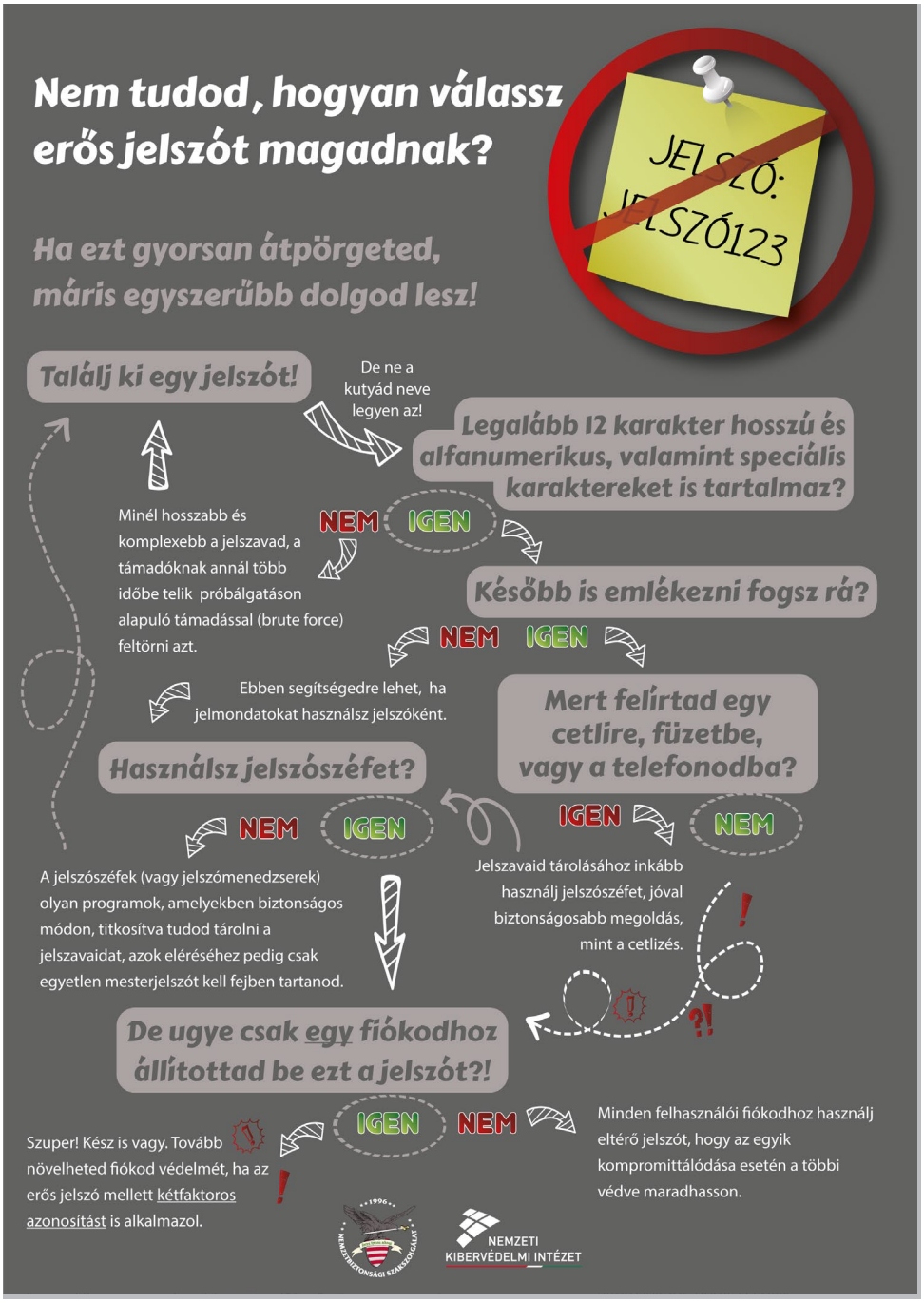
Számos lehetőség közül választhatnak a felhasználók, például letölthetnek és telepíthetnek jelszógenerátor alkalmazásokat vagy igénybe vehetik a böngészők és a különféle eszközök beépített funkcióit is.

A Microsoft Edge, Google Chrome és a Mozilla Firefox böngészőkkel például egyszerűen létrehozhatók erős jelszavak, csakúgy mint az iPhone beépített „Erős jelszó létrehozása új fiókhoz" funkciójával. Ezeken felül számos védelmi szoftver – például a jelszókezelők, amikről bővebben egy későbbi fejezetben lesz szó – is rendelkeznek beépített jelszógeneráló funkcióval.

Amennyiben harmadik féltől származó jelszógeneráló alkalmazás használatát tervezzük, kizárólag megbízható forrásból (Play Store, App Store, Microsoft Store stb.) szerezzük be azt, és a megvásárlás, illetve a letöltés előtt mindenképp olvassunk utána az adott szoftver funkcióinak, megbízhatóságának, valamint ismerjük meg más felhasználók véleményét is a programról!

Egyszerű jelszóalkotó folyamat

Az NBSZ NKI egy korábbi kiadványa segíthet az erős jelszavak létrehozási folyamatának elsajátításában anélkül, hogy ahhoz bármiféle bonyolultabb technikára szükség lenne.



Hogyan jegyezhetők meg az erős jelszavak?

Mivel az erős jelszavak egyik kritériuma a felhasználói szintű egyediség, ami azt jelenti, hogy minden felhasználói fiókhoz más és más jelszót kell beállítani, így azok megjegyzése és fejben tartása egy bizonyos mennyiség után problémássá válhat. Bár jó megoldásnak tűnhet, ha kis cetlikre, egy füzetbe vagy esetleg a telefonunkon tárolt jegyzetek közé írjuk fel a jelszavainkat, hogy azokra a későbbiek során emlékezhessünk, ezek a megoldások nem tekinthetők biztonságosnak. Ezekhez a feljegyzésekhez ugyanis arra nem jogosult személyek is hozzáférhetnek, és így – mivel ez a fajta jelszótárolás semmilyen titkosítást nem alkalmaz – a bejelentkezési adatinkat illetéktelenek is könnyen megismerhetik. Azonban mindkét problémára megfelelő megoldást nyújthatnak a jelszókezelő alkalmazások.

A jelszókezelők vagy más néven jelszómenedzser (password manager) alkalmazások titkosított formában tárolják a jelszavakat, azok eléréséhez pedig egyetlen ún. mester jelszót kell észben tartani. A mesterjelszóból kerül leképezésre az a titkosító kulcs, amivel a hitelesítő adatokat (felhasználónév, jelszó) tároló adatbázis — esetlegesen további kriptográfiai komponensek bevonásával — titkosításra kerül.

A piacon számos ingyenes és fizetős jelszókezelő szoftver érhető el, például a 1Password, a KeePass, Dashlane, a LastPass, a Password Safe és persze vannak a beépített jelszókezelők is, mint a Microsoft Edge, Google Chrome és Mozilla Firefox böngészők jelszókezelői vagy az Apple mentett jelszavak funkciója.

Bár jelszavaink webböngészőkbe történő mentése meglehetősen kényelmes megoldásnak tűnik, nem árt tisztában lennünk az ezzel járó kockázatokkal. Ugyan a legtöbb böngésző ma már törekszik arra, hogy titkosítva tárolják a mentett jeszavainkat, a kimondottan erre a célra szánt jelszószéfekkel szemben még így sem fordítanak kellő figyelmet a biztonságra, ráadásul léteznek olyan támadási módszerek, is amelyekkel a támadók könnyen kinyerhetik jelszavainkat a böngészőkből, ráadásul a böngészők sérülékenységei további kockázatot jelentenek a jelszavak biztonsága tekintetében.

Érdemes azt is megemlíteni, hogy a jelszókezelők használata sem nyújt 100%-os védelmet, sőt használatuk újabb kockázatokat is jelenthetnek. Ilyen lehet például a szoftver sérülékenységeiből adódó fenyegetettségek vagy, ha nem rendelkezünk biztonsági mentéssel és elveszítjük a jelszókezelőt lokálisan tároló eszközünket, akkor nem fogunk hozzáférni a többi felhasználói fiókunkhoz sem. Ugyanez igaz akkor is, ha elfelejtjük a mester jelszavunkat.

Bőven elég fejfájást okoz, ha elveszítjük vagy ellopják eszközünket, amin tovább ronthat, ha még a felhasználói fiókjainkhoz sem tudunk már hozzáférni. Csökkenthetjük ennek kockázatát, ha olyan jelszókezelőt választunk, ami nem csupán lokálisan, az eszközünkön tárolja jelszavainkat, hanem egy bárhonnan elérhető, például felhőtárhelyen is.

Mielőtt letesszük a voksunkat egy jelszókezelő mellett, érdemes utánajárni annak előnyeinek és hátrányainak, hogy mire és meddig terjed ki a gyártói támogatás, illetve megismerni más felhasználók véleményét is az adott szoftverről.

Egy extra védelmi funkció – 2FA

A **kétfaktoros azonosítás (2FA)** egy olyan védelmi megoldás, ahol a felhasználók hitelesítése a klasszikus tudás alapú azonosítás (felhasználónév és jelszó) mellett további faktort is alkalmaz, például a birtoklás alapú (egy eszköz, amivel a felhasználó rendelkezik) vagy a tulajdonság alapú (a felhasználó egyedi tulajdonsága pl.: ujjlenyomat, arc, hang, írisz stb.) hitelesítést. A kétfaktoros azonosítás legelterjedtebb formája jelenleg, mikor a felhasználóknak a jelszavuk mellett egy kódot is meg kell adniuk a bejelentkezéshez. Több módja is van a kétfaktoros azonosításnak, például az SMS-alapú hitelesítés, a külső, például telefonra telepített hitelesítőalkalmazás (authenticator) vagy a biztonsági kulcs használata.

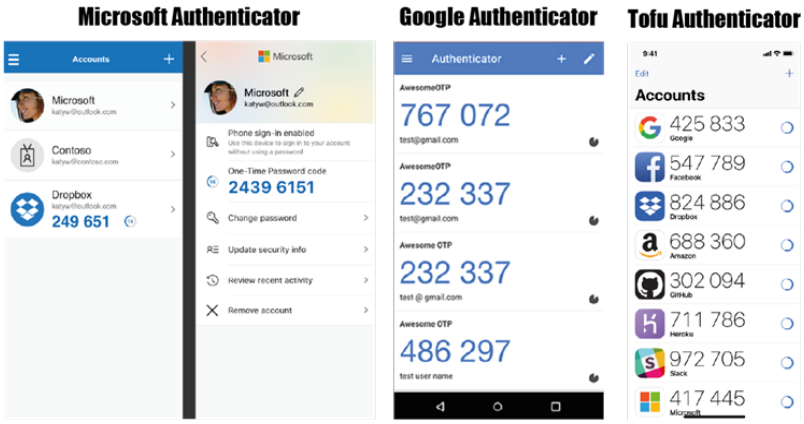
Többfaktoros azonosításról abban az esetben beszélhetünk, ha az előbbiekben említett faktorok közül többet is felhasználnak a hitelesítési folyamat során.

A fent felsorolt lehetőségek közül az SMS-alapú hitelesítés minősül a legkevésbé biztonságos megoldásnak. Több támadási módszer is létezik az SMS forgalmak illetéktelen hozzáféréséhez, például a telefonos rendszerek által használt SS7 (vagyis Signaling System #7) protokoll sérülékenységeinek kihasználása vagy a SIM-csere támadás. Utóbbi ráadásul nem igényel különösebb technikai szaktudást, a támadás során ugyanis a támadók – átverve a mobilszolgáltatók ügyfélszolgálati dolgozóit – hozzárendeltetik saját telefonszámukat az áldozatok SIM kártyáihoz, így a támadók a saját készülékeiken képesek fogadni az áldozatok SMS-eit, beleértve a – általában egyszer használatos – hitelesítő kódokat is.

Egyszer használatos kódnak, ún. OTP-nek (One Time Password) nevezzük a második faktor szerepét betöltő azonosítókat, amelyek kizárólag egyszer és csak korlátozott ideig felhasználhatók, ezáltal jelentős mértékben korlátozva a támadók felhasználói fiókok feltörési kísérletére szánt idejét.

Érdemes megjegyezni, hogy bár nem az SMS-alapú hitelesítés a legjobb 2FA megoldás, még mindig jobb, mintha csak jelszóval védenénk a fiókjainkat.

A telefonos hitelesítőalkalmazások közül számos népszerű, ingyenes és fizetős verzió érhető el Android és iOS rendszeren, például a Microsoft Authenticator, a Google Authenticator és a Tofu Authenticator. Mielőtt letennénk a voksunkat egy adott alkalmazás mellett, érdemes előtte alaposan utánajárni, hogy az adott app milyen mértékben támogatott, hány platformon lehet használni, milyen pontos funkcionalitással rendelkezik és milyenek a felhasználói vélemények róla. Miután kiválasztottuk a számunkra legjobb megoldást, ügyeljünk rá, hogy kizárólag megbízható forrásból, például a gyártók hivatalos oldaláról vagy a Google Play Store vagy az Apple App Store alkalmazásboltokból szerezzük be az alkalmazást!



Képek forrása: a techcommunity.microsoft.com, googleauthenticator.net és a tofuauth.com

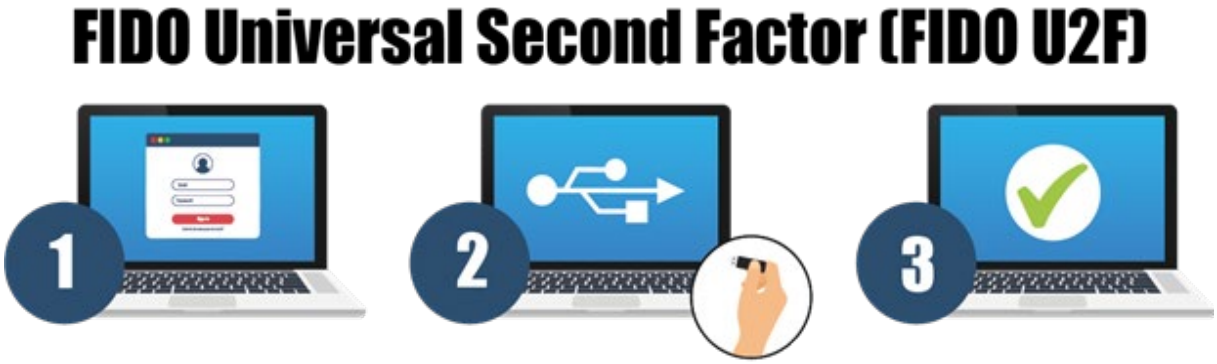
A biztonsági kulcsok vagy más néven hardverkulcsok, olyan kisméretű fizikai eszközök, amelyek kinézetüket tekintve hasonlítanak egy pendrive-hoz, és fizikai (USB-C) csatlakozással vagy rövid hatótávú kommunikációs technológiával (NFC - Near field communication) segítik a felhasználók kétfaktoros (2FA) bejelentkezését.

Hardverkulcsok esetén érdemes megemlíteni a FIDO Szövetség (FIDO Alliance) által évek óta fejlesztett FIDO protokollokat, amelyek használatával a regisztráció során két kulcs, egy publikus és egy privát kulcsból álló ún. kulcspár kerül létrehozásra. Míg a nyilvános kulcsok regisztrálásra kerülnek a szolgáltatónál, addig a privát kulcsok eltárolásra kerülnek a felhasználók eszközein, legyen az hardverkulcs vagy mobiltelefon.

Az éveken át tartó fejlesztéseknek köszönhetően jelenleg három ilyen protokoll létezik: az U2F, a FIDO UAF és a FIDO2.

FIDO Universal Second Factor (FIDO U2F):

A FIDO protokoll egy korai verziója, ami a hardverkulcsokra támaszkodik, és lényegében a hitelesítési folyamat második faktoraként szolgál, ezáltal növelve az egyszerű felhasználónév és jelszó párossal történő bejelentkezés biztonságát. Léteznek olyan U2F biztonsági kulcsok is, amelyek használatához - az eszközre történő csatlakoztatást követően – biometrikus azonosításra is szükség van, ami egy, a hardverkulcsba beépített ujjlenyomat szkennerrel oldható meg. Az ilyen biztonsági kulcsokkal történő hitelesítési folyamat során a tudás alapú azonosítás kiegészül a birtoklás és a tulajdonság alapú faktorokkal. (Kép forrása: yubico.com)



A Bluetooth és az NFC technológiának köszönhetően, ez a megoldás mobil verzióban is létezik. Ilyenkor az azonosítás második lépésénél nincs szükség az azonosításhoz szükséges eszköz csatlakoztatásához, elég csupán a közelben elvégezni a hitelesítést. A FIDO Universal Second Factor (FIDO U2F) időközben átnevezésre került Client to Authenticator Protocols (CTAP1) névre.

Mára már számos gyártó terméke érhető el a piacon, amelyeket szerencsére egyre több okoseszköz és platform is támogat. A legnépszerűbb hardverkulcsok közé tartozik például a YubiKey termékcsalád a Yubico gyártótól, illetve a Google által forgalmazott Titan biztonsági kulcs. A teljes hivatalos gyártói lista a FIDO Szövetség honlapján érhető el.

Egyenes az út a jelszómentességhez

Az előző fejezetben említett FIDO protokollok közül a másik két megoldással komoly lépéseket tettek a jelszómentesség irányába mobileszközök esetén. Mind a FIDO Universal Authentication Framework (FIDO UAF), mind pedig a FIDO2 lehetővé teszik a felhasználók számára, hogy az online szolgáltatásokhoz egy adott mobileszközt regisztráljanak, kiküszöbölve ezáltal a kézzelfogható hardverkulcsok szükségességét. Ettől függetlenül mindkét megoldásnak három használati módja van, egyrészt a jelszó és/vagy token nélküli használat, másrészt pedig a hardverkulccsal, illetve az NFC támogatású mobileszközökkel történő alkalmazás. Utóbbi esetén a felhasználó eszköze (például mobiltelefonja vagy táblagépe) kerül hitelesítőként használatra.

A FIDO2 a Word Wide Web Consortium (W3C) által kidolgozott WebAuthentication („WebAuthn") specifikációjából, illetve a Client to Authenticator Protocols (CTAP2) protokollból áll.

A WebAuthn egy, a böngészőkbe és különböző platformokba beépíthető szabványos webes API, ami lehetővé teszi a FIDO hitelesítés támogatását.

A CTAP2 lehetővé teszi külső hitelesítő eszközök (biztonsági kulcsok és mobileszközök) jelszó nélküli, második vagy többtényezős hitelesítési használatát a FIDO2-kompatibilis böngészőkben és operációs rendszereken.

FIDO Universal Authentication Framework (FIDO UAF) és FIDO2

Amennyiben a felhasználó egy UAF vagy FIDO2 protokollt támogató weboldalon szeretne bejelentkezni vagy tranzakciót kezdeményezni, úgy a weboldal WebAuthn API interakciót kezdeményez a weboldal és a hitelesítő eszköz között. Ilyenkor a felhasználó azonosítása a hitelesítő eszköz feloldásával, például ujjlenyomat- vagy arcszkenneléssel, vagy PIN kód megadásával valósul meg.

Passkey technológia

A FIDO Alliance, a Word Wide Web Consortium (W3C), az Apple, a Google és a Microsoft az elmúlt években közösen fejlesztették ki a Passkey nevű technológiát, amelynek célja, hogy a felhasználók hitelesítési folyamatából teljes mértékben eltávolítsák a jelszavakat, így csökkentve az azok kompromittálhatóságából eredő kockázatokat.

A Passkey a korábbiakban már ismertetett WebAuthentication API (vagy „WebAuthn") szabványra épülő hitelesítési folyamatot alkalmazza, így a felhasználók jelszavak helyett biometrikus azonosítással jelentkezhetnek be a fiókjaikba készülékeik segítségével. A Passkey technológia is egyedi kulcspárokat hoz létre működése során, amiket az alkalmazáshoz vagy a fiókhoz társít a regisztrációk alkalmával. Míg a kulcsokpárok közül a nyilvános kulcsok a szervereken kerülnek tárolásra, addig a privát kulcsok csak a felhasználók eszközein kerülnek előállításra.

A biztonságos jelszókezelésre vonatkozó javaslatok összegzése

- Soha, semmilyen körülmények között ne osszuk meg jelszavainkat másokkal!
- Minden felhasználói fiókunkhoz használjunk egyedi, minél hosszabb, kis-és nagybetűket, számokat és speciális karaktereke is tartalmazó jelszavakat, amelyek nem köthetők a személyünkhöz.
- Hogy ne felejtsük el az eltérő, erős jelszavainkat, használjunk megbízható jelszókezelő programot!
- Ahol csak módunkban áll, engedélyezzük a kétfaktoros azonosítás számunkra legmegfelelőbb formáját!


TIPS

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023