CTI Jelentés

Adathalász csalások, visszaélések a bankok nevében

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996

NEMZETI KIBERVÉDELMI INTÉZET

KiberPajzs
Védelem a pénzügyekben

Tartalom

Mi is az az adathalászat?

Az adathalász támadások célja, hogy az áldozattól a kiberbűnözők bizalmas adatokat tulajdonítsanak el, oly módon, hogy a felhasználót személyes adatok, jelszavak, bankkártyaadatok és más egyéb érzékeny információk felfedésére veszik rá. Fontos megemlíteni, hogy a támadások különféle eszközök felhasználásával próbálnak meggyőzőnek, hitelesnek tűnni.

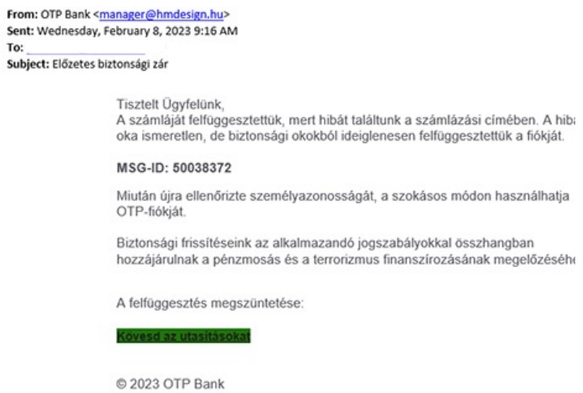
Amennyiben szeretne még több információt olvasni a kibertérből érkező fenyegetésekről, látogassa meg a nemrégiben indult KiberPajzs weboldalát!

A KiberPajzs együttműködés célja a lakosság pénzügyi tudatosságának erősítése, illetve segítséget nyújtani a pénzügyi kiberkockázatok minél hatékonyabb kezeléséhez.

Az adathalász csalások különböző típusai

E-mail alapú adathalászat

Az e-mail alapú támadás az adathalászat leggyakoribb és legelterjedtebb formája. Az e-mail alapú technika során a támadó mindig próbál valamilyen „hivatalos" kinézet mögé bújni. Azt, hogy az e-mailben a támadók épp milyen történettel, melyik intézményt megszemélyesítve állnak elő, azt sajnos nem tudni előre, mivel a lehetőségek tárháza szinte végtelen. A kiberbűnözőkre jellemző, hogy mindig alkalmazkodnak az aktuális trendekhez, igyekeznek kihasználni a nagy népszerűségnek örvendő témákat. Szerencsére még is van néhány jellemző, amelyek alapján könnyebben felismerhetővé válnak az adathalász levelek. Az álcázott levelek érkezhetnek akár egy közmű szolgáltató, akár egy online szolgáltatás (Apple, Google, Microsoft) vagy éppen bankok nevében is. Az ilyen üzeneteknél figyelni kell az ékezetek, írásjelek használatára, illetve a nyelvtani megfogalmazásokra.



From: OTP Bank <manager@hmdesign.hu>
Sent: Wednesday, February 8, 2023 9:16 AM
To: _____
Subject: Előzetes biztonsági zár

Tisztelt Ügyfelünk,
A számláját felfüggesztettük, mert hibát találtunk a számlázási címében. A hib
oka ismeretlen, de biztonsági okokból ideiglenesen felfüggesztettük a fiókját.

MSG-ID: 50038372

Miután újra ellenőrizte személyazonosságát, a szokásos módon használhatja
OTP-fiókját.

Biztonsági frissítéseink az alkalmazandó jogszabályokkal összhangban
hozzájárulnak a pénzmosás és a terrorizmus finanszírozásának megelőzéséh

A felfüggesztés megszüntetése:

Kövesd az utasításokat

© 2023 OTP Bank

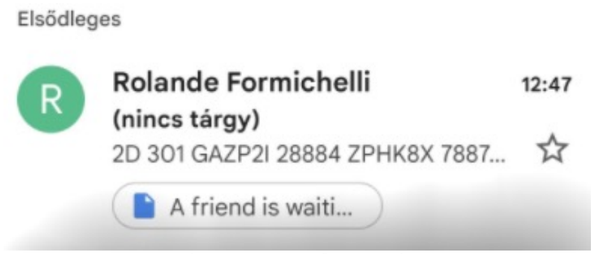
Adathalász e-mail az OTP Bank nevében (Forrás: https://www.otpbank.hu/)

Mivel ezek a levelek sokszor valamilyen online fordító segítségével születnek, általában tartalmaznak nyelvtani hibákat is. Ezekben a levelekben a csalók valamilyen módon megpróbálnak rávenni bennünket arra, hogy gépeljünk be különböző érzékeny adatokat (felhasználónév/jelszó párost, esetleg a bankkártyán szereplő adatokat) egy weboldalon vagy küldjük el azokat számukra üzenetben. A levelekben sokszor befizetetlen havidíjra, „csekkre" vagy bankok esetében zárolt folyószámlára, letiltásra kerülő kártyára, ellenőrizetlen tranzakcióra hivatkoznak. Annak érdekében, hogy gyors cselekvésre kényszerítsenek minket, az a jellemző, hogy rövid határidőket fogalmaznak meg a levélben, továbbá gyakran egy visszaszámláló órát is elhelyeznek az üzenetben, fokozva ezzel a sürgetést. Ilyenkor az idő rövidsége miatt sokan áldozatul esnek ezeknek a leveleknek és online „befizetik" a kért összeget, megadva személyes adataikat, illetve bankkártyaadataikat. Természetesen a háttérben nem történik semmiféle befizetés vagy tranzakció, hanem az általunk megadott érzékeny adatok továbbítódnak a csaló felé.

Kártevő alapú adathalászat

A kártevők segítségével végrehajtott csalások napjainkban nagyon elterjedtek. Ez a módszer szorosan kötődik a fentebb leírt e-mail alapú adathalászathoz. Általánosságban elmondható, hogy ebben az esetben is valamilyen vállalatot személyesítenek meg az üzenetben, illetve a levélhez mellékelve találhatunk egy, a témához illő csatolmányt. Ezeket megnyitva, még ha esetleg elsőre csak egy szöveges fájlnak vagy táblázatnak tűnnek is, a felszín alatt, a tudomásunk nélkül hajtanak végre különböző káros parancsokat. Ezeknek a káros programoknak többféle súlyossági foka is lehet. Adott esetben csak azon a számítógépen

fut le a program, ahol azt megnyitották, ám az is előfordul, hogy egy vállalati környezetben szétterjed az informatikai infrastruktúrában, és még több célgépet képes megfertőzni. A programok ilyenkor megpróbálják a lehető legtöbb adatot elküldeni a csalók felé, hogy azok később lehetőség szerint visszaélhessenek velük. Erre láthatunk példát egy, a közelmúltban felfedezett adathalász-kampány esetében. A kiberbűnözők egy DBatLoader elnevezésű rosszindulatú programmal terjesztették a Remcos RAT és Formbook nevű malwareket.

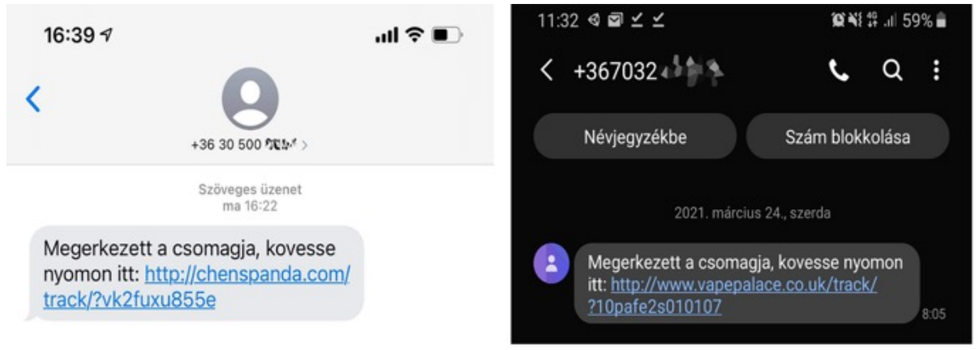


Csatolmánnyal rendelkező adathalász e-mail

SMS-alapú adathalászat

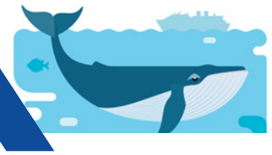
Az SMS alapú adathalászat során – az e-mail alapú csalásokhoz hasonlóan – a kiberbűnözők nagy tömegeket érhetnek el, rengeteg SMS-t kiküldve a készülékekre. Ezeket sok esetben úgynevezett SIM-farmok segítségével hajtják végre. A SIM-farm egy olyan rendszer, mely nagyszámú SIM kártya segítségével rengeteg SMS-t képes kiküldeni egyszerre. Ezek a farmok általában olyan országokban találhatóak, ahol a mobilszolgáltatók díjai olcsóbbak, illetve a bűnözők regisztrációs folyamatok nélkül képesek ezeket megvásárolni, beszerezni.

Az üzenetek témája változó, azonban a legtöbb esetben az SMS valamilyen futárszolgálat értesítő üzenetét tartalmazza (pl.: 2022-es FluBot-kampány), amiben arra kérnek bennünket, hogy egy linken keresztül erősítsük meg a csomag átvételét a személyes adataink megadásával, különben a csomagunk nem fog megérkezni. Sok esetben különböző streaming szolgáltatók üzeneteinek álcázott SMS-ek is fogadhatnak minket, melyben arról tájékoztatnak, hogy előfizetésünk záros határidőn belül lejár, ha az elküldött hivatkozás segítségével nem újítjuk meg azt. A megszokott módon a személyes-, illetve a bankkártya adatinkra vadásznak a csalók. Ahogy fentebb az e-mail alapú támadásnál említettük, itt is figyelni szükséges az üzenetek esetlegesen furcsa megfogalmazására.



A FluBot kampány során kiküldött SMS-ek (Forrás: https://kiber.blog.hu/)

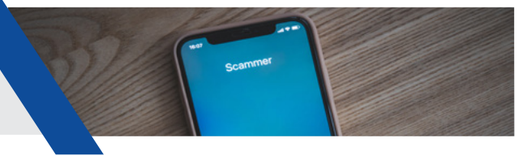
Célzott adathalászat, bálnavadászat



A legtöbb esetben, ha adathalászatról beszélünk, akkor a csalók technikája a minél nagyobb tömeg elérése és átverése. Célzott adathalászatnak nevezzük azt a támadási formát, amikor a kiberbűnözők egy konkrét személy vagy kisebb létszámú csoport adatait próbálják eltulajdonítani. Bálnavadászatnak pedig azt a támadási jelenséget

nevezzük, amely során egy fontosabb személy ellen irányul az adathalász támadás, pl.: cégvezetők, közéleti szereplők stb. Az ilyen típusú támadásokat általában hosszas előkészület, akár megfigyelés is megelőzheti, hogy a csalók megpróbálják megtalálni a lehető legesélyesebb pillanatot az adatok ellopására.

Telefonos adathalászat



A telefonos adathalászat az egyik legidősebb átverési technika. Ezzel a csalási módszerrel már az internet elterjedése előtt is találkozhattunk. A csalók általában valamilyen ügyfélszolgálat vagy kormányzati szerv nevében telefonálnak, sok esetben az általuk már előre megírt „forgatókönyvet" járják végig. A bűnözök megpróbálják a hívott félt stresszes szituációba hajszolni, sürgető mondatokkal, pszichológiai manipulációval. Ezen átveréseknél sem szabad elfelejteni, hogy a csalóknak itt is csak egy céljuk van: az, hogy rávegyenek minket arra, hogy minél több személyes és értékes információt osszunk meg velük. Az, hogy ezt milyen módon próbálják elérni, szintén nagyon különböző lehet. Előfordul, hogy egyszerűen a telefonon keresztül elmondjuk az adatainkat, de arra is akad példa, hogy valamilyen applikációt próbálnak letöltetni velünk a telefonunkra, amelyen keresztül később saját magunk gépeljük be a követelt információkat. Fontos megjegyezni, hogy létezik egy úgynevezett "Caller ID spoofing" technika, amely lehetővé teszi a csalók számára, hogy a hívás forrásának látszó telefonszámot manipulálhassák. Más szóval képes lehet egy csaló arra, hogy a bankunk valódi telefonszámát jeleztesse ki a fogadó fél telefonján, ezért nagyon fontos, hogy ha még fejből tudjuk is a bankunk ügyfélszolgálatának a számát, ne jussunk arra a következtetésre, hogy biztosan a bankunk keres.

Csalások és adathalászat a banki szektorban

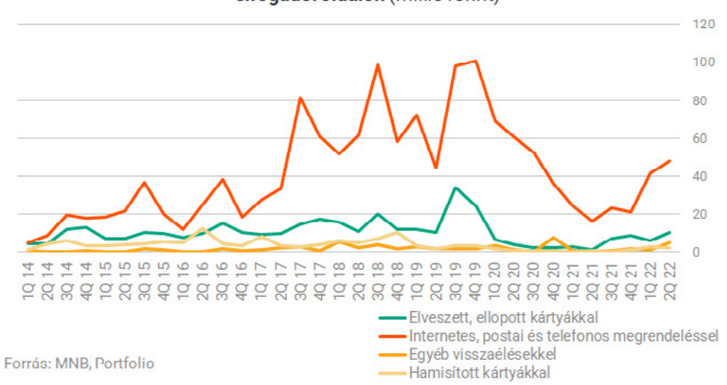
Milyen banki adatokat próbálnak megszerezni a csalók?

- **Személyes adatok** (név, születési hely és idő, személyi igazolvány szám stb.)
- **Az adott bank internetes felületéhez, internetbankjához használt belépési azonosítók**
- **Bankkártya adatok** (Bankkártya száma, tulajdonos neve, lejárati dátum, PIN kód, CSC/CVC/CVC2/CVV/CVC2 – a megnevezés a kártya típusától függ, de mindig a kártya hátulján található)

A banki csalásokról további érdekes információkat tudhat meg a témát feldolgozó Kibertámadás! Podcast adásunkból:

A bankkártyás visszaélések értéke típusonként a kibocsátói oldalon (millió forint)

A bankkártyás visszaélések értéke típusonként az elfogadói oldalon (millió forint)



Forrás: MNB, Portfolio

Az elfogadói és a kibocsátói oldal kifejezések nem konkrét bankokra utalnak, hanem arra, hogy a bankok hol helyezkednek el egy tranzakciós folyamatban. Az elfogadói oldal a tranzakció kereskedői oldalán lévő bank, a kibocsátói oldal pedig a kártyabirtokos vagy az ügyfél bankja. A bankok mindkét szerepet betölthetik és általában be is töltik. A fentiekhez kapcsolódó tipikus átverések szoktak előfordulni, amikor olyan „munkát" ajánlanak nekünk, amiben egy idegen bankszámláról különböző összegeket utalnak a saját bankszámlánkra. Ezután megkérnek minket arra, hogy az átutalt összeget továbbítsuk egy harmadik, szintén ismeretlen bankszámlára.

Milyen jelei vannak a banki csalásoknak?

E-mail felhasználásával történő csalás esetén

- Az egyik legszembetűnőbb jel, ha a levél már eleve a levélszemét (spam) mappánkban landol. Ilyen esetben az általunk használt levelezőszolgáltató szűrője valamilyen gyanús elemet észlelt a levélben, ezért ilyen esetben legyünk kifejezetten óvatosak az üzenettel kapcsolatban.
- Vizsgáljuk meg alaposan, hogy a kapott levél milyen e-mail címről érkezett.
- Győződjünk meg arról, hogy a használt e-mail cím ténylegesen az adott szervezet e-mail címe. Előfordulhat, hogy az eredetihez nagyon hasonló e-mail címet próbálnak használni, ehhez akár elég csak egy karakter különbség is. pl.: **titkarsag@nki.gov.hu** helyett **titkarsag@enki.gov.hu**.
- Az eredeti, korábban kapott levelektől eltér a levél kinézete, felépítése.
- A levél szövegében furcsa weboldalakra mutató linkeket találunk.
- A fentebb már említett technika, a levél általában úgy van megfogalmazva, hogy sürgető legyen.

SMS felhasználásával történő csalás esetén

- Az üzenetben olyan megszólítást, megfogalmazást használnak, mely eddig nem volt jellemző. A szövegben ékezetek nélküli szavak, rossz magyarsággal megírt mondatok szerepelnek.
- Az SMS-ben szereplő linkek nem a bank oldalára mutatnak, a hivatkozás furcsa karakterekből áll.
- A hangvétel itt is általában sürgető, sokszor nyereményjátékra vagy valamilyen majdnem lejárt határidőre hivatkozva.

Telefon felhasználásával történő csalás esetén

- Gyakran használt trükk, hogy a telefonáló csaló valamelyik bank nevében, mint ügyfélszolgálati munkatárs mutatkozik be és olyan eseményre hivatkozik (külföldről való belépés, gyanús tranzakció stb.), mely során szükséges a bankszámlánkon tárolt összeget egy biztonsági számlára áthelyezni.
- A hívás során a „banki munkatárs" nem csak személyes adatokat, hanem a bankkártyánk adatait, illetve az internetbankhoz szükséges belépési adatokat is elkéri tőlünk.
- A telefonáló megpróbál minket rávenni arra, hogy töltsünk le valamilyen másik banki alkalmazást.
- Az ügyintéző elkezd minket sürgetni határidőkkel, mielőbbi választ és cselekvést várva tőlünk. Ezáltal egy olyan helyzetbe próbálja hozni az áldozatot, hogy ne legyen ideje elgondolkodni vagy esetleg utánakeresni az adott ügyintézési folyamatnak.

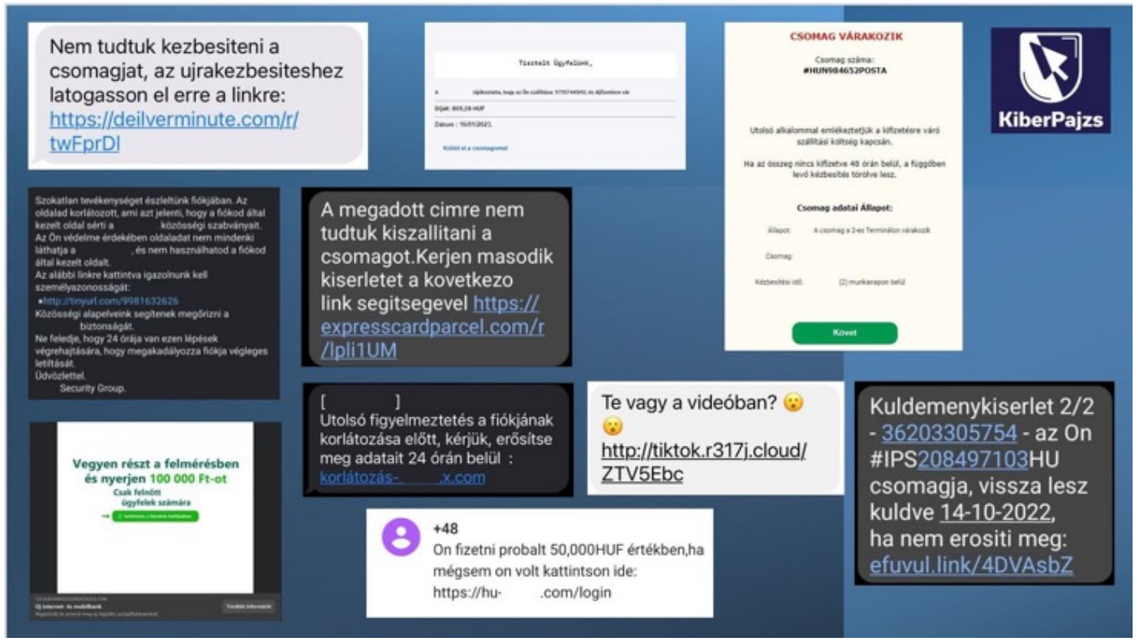
Weboldalak felhasználásával történő csalás esetén

- Hamis, az adott bank weboldalát lemásolva létrehozott weblapokkal általában a csalók által küldött e-mailekben vagy SMS-ken keresztül találkozhatunk.
- Esetekben találhatunk eltérő formázási elemeket vagy felépítést az eredeti banki oldalhoz képest.
- A weboldal URL címében furcsa dolgokat találunk. Oda nem illő számokat, betűket, írásjeleket vagy esetleg a webcím végén másik ország azonosítója szerepel.
- Nem találhatóak a biztonságos kapcsolat jelzései az általunk használt böngészőben. A címsorban ezt egy lakat ikon jelzi, illetve a webcím eleje nem „https://-el" kezdődik.

Mobilalkalmazások felhasználásával történő csalás esetén

- Ahogyan a weboldalak esetében, itt is általában a csalók által küldött e-mailekben vagy SMS-eken található hivatkozásokra kattintva töltődhet le hamis alkalmazás a telefonunkra.
- A telepítés során az alkalmazások engedélyeket kérnek bizonyos funkcióhoz. Itt nagyon érdemes megfigyelni, hogy pontosan milyen jogosultságokra lehet szüksége a programnak. Ha egyre több gyanús jogosultságot (pl.: névjegyek, mikrofon stb.) kér tőlünk a telefon, szakítsuk meg a telepítést.
- Az alkalmazás információi között nem találunk semmit vagy gyanús, magyartalan megfogalmazásokat.
- Az alkalmazásáruházban található app alatti felhasználói visszajelzések, kérdések, értékelés hiánya.

- Figyeljünk a kis számban letöltött alkalmazások esetében, ha 10 ezer alkalom alatti a letöltések száma, kezdjünk gyanakodni! A telefonunk a telepítésre kattintva nem megbízhatóként jelzi az alkalmazást.



Különöző típusú adathalász üzenetek

Hogyan védekezhetünk a banki csalások és adathalászat ellen?

Jelen tájékoztató szinte teljes egésze a kibertérben elkövetett csalásokról szól, azonban mindenképp szeretnénk megemlíteni egy nagyon egyszerű, „offline" módszert értékeink megóvásának érdekében. Amikor bármilyen publikus helyen szükséges megadnunk a bankkártyánk PIN kódját, törekedjünk arra, hogy az egyik kezünkkel takarjuk el a terminált az esetleges kíváncsiskodók elől! Ez egy nagyon egyszerű de hatásos mozdulat, azonban a mindennapi élet során sokan megfeledkeznek róla.

Telefonhívások, e-mail-ek és SMS-ek kezelése során, mindig legyünk résen, ha akármilyen indokkal elkérik tőlünk a fentebb említett banki adatokat, bejelentkezési azonosítókat. Azonnal jusson eszünkbe, hogy valószínűleg egy csalóval kommunikálunk!

Egy nagyon hatásos módszer, aminek nem lehet negatív következménye: amint felmerül bennünk bármi gyanú az adott telefonos beszélgetés során, köszönjünk el és tegyük le a telefont! Tárcsázzuk az adott bank hivatalos telefonszámát, ahol egy hivatalos ügyintézővel tudjuk folytatni a beszélgetésünket, meséljük el neki, hogy az imént kaptunk egy hívást, mondjuk el, hogy miről szólt a beszélgetés! Amennyiben valóban hiteles volt az előző beszélgetés, azt tudjuk folytatni az aktuális bank munkatársával, amennyiben pedig nem tudnak ilyenről, valószínűleg sikeresen elkerültünk egy csapdát.

Hasonló technikát lehet alkalmazni az e-mailekben és SMS-ekben kapott hivatkozásokra is. Amennyiben ezekben az üzenetekben felszólítanak minket, hogy adjunk meg adatokat, vagy lépjünk be a banki felületünkre a megadott linken, keressük meg bankunk eredeti weboldalát

és ott jelentkezzünk be! Így egyszerűen biztosíthatjuk magunkat, és elkerülhetjük, hogy a hivatkozások esetleg valamilyen hamis oldalra továbbítsanak minket.

Ne telepítsünk olyan alkalmazásokat, amelyek ismeretlenek számunkra, különösen ne hallgassunk olyanokra, akik külön kérik telefonon vagy üzenetben, hogy telepítsük valamilyen banki szoftvert számítógépünkre, okostelefonunkra!

A csalók gyakran olyan szoftverek telepítését kérik, amellyel távolról lehetőségük adódik átvenni az irányítást a számítógépünk vagy telefonunk felett. A csalók kérésére semmi esetre se telepítsünk ilyen jellegű alkalmazásokat illetve, ha használunk hasonló szoftvereket ne adjuk meg a csatlakozáshoz szükséges azonosítókat számukra!

Ne utaljunk pénzt a fentebb említett ismeretlen „biztonsági számlára"!

Tehetünk fel kérdéseket is az ügyintézőnek, amelyekre egy csaló nem tudja a választ, azonban a bankunk igen. Kérdezzük meg tőle a pontos nevünket, számlaszámunkat, mi volt az utolsó pár darab kártyás tranzakciónk! Ha az ügyintéző ezekre a kérdésekre nem tudja a választ, valószínűleg csalóval van dolgunk.

Amennyiben lehetőségünk van, használjuk az adott bank mobilapplikációját! A szoftver segítségével naprakész információkat kaphatunk számlánk részleteiről. A programon belül könnyebben elérhetjük a különböző biztonsági funkciókat is.

Bankkártyánkhoz állítsunk be a mindennapi életünkhöz igazodó napi összeglimitet!

Internetes vásárlás során részesítsük előnyben a bank által kiállított virtuális bankkártyát, így az interneten történő tranzakciók során nem szükséges megadnunk a fizikai bankkártyánk adatait!

Mit tehetünk, ha banki csalás áldozatává váltunk?

Ha csalás vagy adathalász támadás során feltételezhetően adataink a csalók kezébe kerültek, a lehető leghamarabb jelezzük azt a bankunk felé! Erre általában három féle módon van lehetőségünk: telefonon, e-mailben, illetve személyesen az adott bankhoz tartozó bankfiókban. Érdemes előre tájékozódni arról, hogy a bankunknál ennek mi a menete, így vész esetén csak a protokollt kell követni!

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!

2023