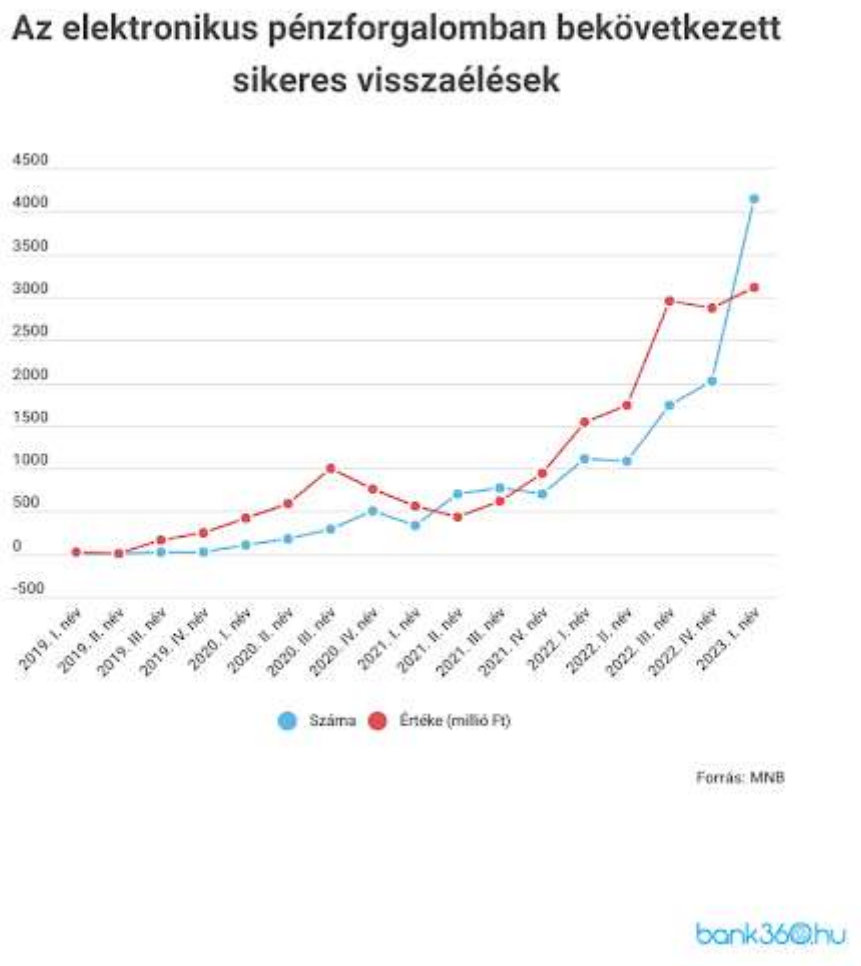
Tájékoztató a banki csalásokról

Rövid idő alatt többszörösére ugrott az ilyen csalások száma, a rászedett banki ügyfelek kára pedig milliárdokban mérhető. Új módszerekkel próbálkoznak a csalók, a telefonos, internetes manipulátoroknak bedőlők átlagosan több százezer forintot is bukhatnak - írja a Bank360.hu. Az adathalászok is egyre sikeresebbek, az óvatlan károsultak pedig fájdalmas tanulópénzt fizethetnek.

Drasztikus mértékben nő a bankszámlás, bankkártyás csalások száma a Magyar Nemzeti Bank (MNB) friss adatai szerint. 2023 első negyedévében minden korábbinál több alkalommal, összesen 4150 esetben jártak sikerrel a bűnözők, akik így 3,1 milliárd forintnál is több kárt okoztak a bankszámla- és bankkártya-tulajdonosoknak. Ennek a kárnak a döntő részét - **2,8 milliárd forintot az ügyfelek viselték**.

A csalók általában az **interneten vagy mobiltelefonon** keresztül cserkészik be az áldozataikat. Az internetes csatornákon keresztül több mint 1300 sikeres visszaélés történt három hónap alatt csaknem 2 milliárd forint értékben. Mobiltelefonon keresztül mintegy 2800 bűnöző járt sikerrel, ők csaknem 1 milliárd forint kárt okoztak.



A korábbi évekkel szemben azonban már nem az ellopott vagy elvesztett bankkártyák tulajdonosai vannak a legnagyobb veszélyben. Előfordulnak ugyan ilyen jellegű csalások is, de ezek száma és értéke marginális az erős ügyfélhitelesítés és a viszonylag könnyű lebukás miatt. Ha egy lopott bankkártyával vásárolnak, akkor a boltok kamerái vagy internetes vásárlásnál a rendelés helye alapján meg lehet találni az elkövetőt, aki amellett, hogy akár szabadságvesztéssel is számolhat, a Központi Hitelinformációs Rendszer (KHR) feketelistájára is felkerül. Ez aligha éri meg, főleg miután egy átlagos eltulajdonított bankkártyával csak 16,6 ezer forintnyi kárt okoztak az elmúlt negyedévben.

Az adathalászok és a manipulátorok okozzák a legnagyobb károkat

A bankkártyás visszaéléseknél sokkal nagyobb károk keletkeznek az adathalászok tevékenysége nyomán. Az idei első negyedévben a kibocsátói oldalon 39 447 esetben fordult ez elő, és több mint 1,1 milliárd forint volt az okozott kár. Nem véletlen, hogy a bankok szinte naponta figyelmeztetik az ügyfeleiket adathalász-támadásokra.

A pszichológiai manipulációval, megtévesztéssel operáló csalók által okozott károk száma 238 volt, sajnos ezekben az esetekben a bűnözők viszonylag nagy összeggel károsították meg az áldozatokat, az átlagos kár 256 ezer forint volt. Problémát jelent, hogy ilyenkor az ügyfelek maguk adják meg azokat az adatokat, hagyják jóvá azokat a tranzakciókat, amelyekkel a csalók megszerzik a pénzüket, emiatt általában **kártérítésben is hiába reménykednek** - hívják fel a figyelmet a Bank360.hu szakértői.

Az elfogadói oldalon is az adathalászok az egyik legkártékonyabb elkövetők, az első három hónapban 359 alkalommal 26,7 millió forint kárt okoztak. A kártyakibocsátó bankokra terhelt veszteség alapvetően nem növekszik, a kártyabirtokosok és az elfogadóhelyek azonban egyre több pénzt veszítenek a bűnözők miatt.

Cél az adataink és a belépési azonosítók megszerzése

A banki csalók célja, hogy bármely módon birtokába jussanak a **bankszámlánk** adatainak, és onnan elutalják vagy elutaltassák az ott tartott pénzösszegeinket. Ezt számos úton igyekeznek elérni, jellemzően megtévesztés útján csalják ki, szerzik meg ezeket az információkat.

Ahhoz, hogy elérjék céljukat, a személyes adatainkra (név, születési név, anyja neve, születési hely és idő, lakcím) és a bankszámlánk online vagy telefonos azonosítói, jelszavai szükségesek.

Ezen adatok egy részét az internetről, közösségi oldalakról, nyilvános adatbázisokból (cégnyilvántartás, egyéni vállalkozók nyilvántartása) is össze tudják gyűjteni, de minden szükséges adat általában nem lelhető fel a világhálón. Fontos, hogy tisztában legyünk azzal, hogy mely, ránk vonatkozó információk találhatóak meg harmadik személyek számára, és igyekezzünk ezen adatok mennyiségét csökkenteni.

A csalók, ha már pár adatot megszereztek, egy második kapcsolatfelvétel során ezekre hivatkozva könnyebben tudnak a bankszámlatulajdonos bizalmába férkőzni, hiszen nem feltételezzük idegenekről, hogy ismerik ezeket az adatainkat.

Új módszer: megtévesztő online hirdetés és a hamis banki honlap

A legújabb módszereik egyike, hogy jogosulatlanul Google, Facebook vagy más hirdetési felületen a bank nevében megtévesztő hirdetést tesznek közzé, ami a banki felületre nagyon hasonlító, de hamis, a bankhoz valójában nem kötődő weboldalra vezet.

A banki ügyintézési felületre belépést kínáló hamis aloldalon a gyanútlan felhasználó – azt gondolva, hogy a valós banki honlapon adja meg belépési adatait – önként adja át a bűnözők részére az azonosítóját, jelszavát, de még a mobiltelefonjára érkező, egyszeri SMS kódot is, ami után a bankszámlájához az elkövetők hozzáférnek.

A telefonos átverés

Régebbi megoldás, amikor telefonhívás útján megpróbálják elhitetni, hogy a bank munkatársai, további adatokat kérnek, vagy előadják, hogy az ügyfél bankszámláját veszély fenyegeti, ezért a hívás során meg kell adni részükre a belépési kódokat.

Az is előfordul, hogy a gyanútlan banki ügyfelet, miután sikerült meggyőzni, hogy a bankból telefonálnak, arra veszik rá, hogy maga utalja át a „veszély” miatt egy „biztonságos” számlára a saját pénzét.

Egy másik gyakori módszere a csalóknak, hogy arra kérik az áldozatot, hogy a telefonjára, számítógépére egy távoli elérést biztosító programot telepítsen (például az **AnyDesk szoftvert**), amelyen keresztül már könnyűszerrel átveszik az irányítást a telefon vagy a laptop felett, és maguk végzik el az utalásokat. Ha sikerült átutalniuk egy másik számlára az összegeket, akkor azokat jellemzően azonnal tovább is utalják egy távoli országba, vagy készpénzben felveszik, és emiatt szinte lehetetlen időben megállítani a folyamatot.

Ne dőlj be! Az MNB nevében levélben kérnek pénzt a csalók

Adathalászat emailben

A hozzáféréshez szükséges adatokat adathalász emailek (phishing) segítségével is igyekeznek megszerezni, amikor tömegesen küldik ki a megtévesztő emailcímről, banki logóval ellátott emaileket. Az emailben olyan internetes linket helyeznek el, ami megjelenésében, domain nevében a tényleges banki weboldalra hasonlító honlapra vezet. Ha ott begépeli az ügyfél a banki azonosítóit, már részben át is adta a bűnözők részére a hozzáférését. Ilyenkor már csak a belépési, biztonsági kódot igyekeznek kicsalni telefonon keresztül az ügyfélből, és ha ez sikerült, már be is jutottak a valós banki rendszerbe.

Ezek a hamis levelek sokszor furcsa nyelvtani hibákat, rossz szóhasználatot tartalmaznak, mert az elkövetők nem mindig az adott ország lakói, nem vagy nem jól beszélik a nyelvet, és csupán ellenőrizetlen gépi fordításokkal operálnak.

Ebben az esetben az eszközön tárolt minden adathoz hozzáférhetnek, akár kárt tehetnek bennük megsértve a bizalmasság, rendelkezésre állás és sértetlenség elvét, megszemélyesítést felhasználva okozhatnak kárt felhasználva a megszerzett adatokat.

A bankoknak is van felelőssége a csalások megelőzésében

Egy csalás kapcsán a **bank** felelősségét is meg kell vizsgálni. Ehhez tisztában kell lennünk a bankbiztonság kapcsán betartandó szabályokkal. Ha a bank ezeket megszegi, érdemes a károk megtérítését követelni.

Bankkártyás visszaélés áldozata lettél? Ilyen kártérítési lehetőségeid vannak

A pénzforgalmi szolgáltatás nyújtásáról szóló **2009. évi LXXXV. törvény** szabályozza, hogy milyen módon kell a bankoknak a pénzforgalmi szolgáltatáshoz kapcsolódóan kockázatmérséklési intézkedéseket és ellenőrzési mechanizmusokat kialakítani, vagyis a bankszámlánkat – akár a megtévesztésünk okozta tévedéseinktől is – megvédeni. Ennek részeként a pénzforgalmi szolgáltató köteles hatékony eseménykezelési eljárásokat kialakítani, fenntartani, a súlyosabb működési és biztonsági eseményeket felderíteni és osztályozni.

A banknak erről a tevékenységéről évente legalább egyszer aktualizált és átfogó értékelést kell küldenie a felügyeleti szervének a működési és biztonsági kockázatokról, a felismert kockázatok mérséklésére alkalmazott intézkedések és a kapcsolódó ellenőrzési mechanizmusok megfelelőségéről.

Ha bármilyen súlyosabb működési vagy biztonsági eseményt észlel, akkor a pénzintézet haladéktalanul köteles tájékoztatni a bankfelügyeletet. Ha az incidens, a biztonsági esemény sérti a bankszámlatulajdonos ügyfél érdekeit, a banknak erről késedelem nélkül tájékoztatnia kell az ügyfelet, és informálnia kell a lehetséges intézkedésekről, amelyet a káros hatások enyhítése érdekében meghozhatnak.

A törvény szerint a pénzforgalmi szolgáltatónak erős ügyfél-hitelesítést kell alkalmaznia, amikor a fizető fél online fér hozzá a fizetési számlájához, vagy elektronikus fizetési műveletet kezdeményez, illetve

bármely műveletet olyan távoli csatornán keresztül hajt végre, ami fizetéssel kapcsolatos csalásokra és más visszaélésekre adhat módot. Szintén erős ügyfél-hitelesítést kell alkalmaznia elektronikus távoli fizetési művelet esetén, ha a művelet egy előre meghatározott összeggel és egy adott kedvezményezettel dinamikusan összekapcsolódó elemeket tartalmaz.

A banknak olyan biztonsági intézkedéseket kell alkalmaznia, amelyek alkalmasak az ügyfelekhez tartozó személyes hitelesítési adatok bizalmasságának és integritásának megóvására.

A pénzintézetek a Magyar Nemzeti Bank ajánlását is figyelembe véve dolgozzák ki a biztonságos banki folyamataikat. (DORA Rendelet– új uniós kiberbiztonsági szabályozás)

A pénzintézet akkor lehet felelős, ha a rá irányadó, a bankbiztonságot célzó feladatait nem vagy nem jól teljesítette, ha nem tett meg minden elvárható intézkedést a csalás, a károkozás megakadályozására. Ha azért tűnik el a pénz a számlánkról, mert feltörték a bank adatbázisát, de ennek kapcsán nem volt semminemű közrehatásunk, akkor a bank rendszere nem volt jól védhető, és ez valószínűleg a bank felelősségét alapozza meg.

INTERNETEN KERESZTÜL CSAK BIZTONSÁGOS HELYRŐL INTÉZZÜK PÉNZÜGYEINKET!

- Ne adjunk lehetőséget arra, hogy elektronikus kódunkat más is láthassa! **Csak végső megoldásként használjunk nyilvános internetet**, vagy jelszóval nem védett Wi-Fi hálózatot bankügyeink intézésére. Ha mégis ezt tesszük, saját érdekünkben tartsunk be néhány fontos biztonsági szabályt!
- Ha nyilvános helyen intézzük pénzügyeinket, **célszerű ezt követően megváltoztatni a belépési jelszót.**
- **Ne válasszuk azt a lehetőséget, hogy a számítógép megjegyezze** a belépéshez szükséges jelszót!
- Tanácsos **törölni a böngésző tárolóját** is az internetes bankolás után, hogy illetéktelen személy ne tudjon adatainkkal visszaélni.
- Az internetes rendszerből **ne a böngésző bezárásával, hanem a kilépés gombbal jelentkezzünk ki!**
- Az internetbank használata közben a böngésző címsorában szereplő linket adatainak biztonsága érdekében ne küldjük tovább!

MOBIL NETBANK HASZNÁLATÁVAL KAPCSOLATOS TANÁCSOK

A mobil készülékek (pl. okostelefonok, táblagépek) – ugyanúgy, mint a számítógépek - célpontot jelentenek az on-line bűnözők számára, egyre nagyobb kockázatot jelent az ilyen készülékek felelőtlen, átgondolatlan használata.

Fontos, hogy tisztában legyünk az ilyen készülékek használatának veszélyeivel és a kockázatok csökkentésének lehetőségeivel.

Tanácsos **a beépített védelmek magas szinten történő használata**, a mobil készülékekre elérhető vírusvédő szoftverek alkalmazása, és speciális biztonsági szoftverek használata (például jelszótárolásra, mobilkövetésre).

Egyes kártevők képesek a többszintű/többcsatornás azonosítást is megkerülni. Például, ha az azonosításhoz a standard azonosító mellett egy ideiglenes, csak pár percig élő azonosító (amit SMS-ben kapunk meg az intézménytől) is szükséges, az okostelefont megtámadó szoftver mindkét azonosítót megszerzi a telefonból, jelentős károkat okozva ezzel.

Gyanús jel:

- Korábban a banktól (vagy szolgáltatótól) kapott sms-ek egy másik telefonszámról érkeztek.
- Az üzenet úgy van megfogalmazva, hogy sürgető legyen. Akár nyereményjátékot hirdet, vagy arra utal, hogy csak a link megnyitásával teljesül az sms-ben jelzett szolgáltatás

ÓVATOSAN KEZELJÜK A LETÖLTÉSEKET, ELLENŐRIZZÜK A FORRÁSOKAT!

A mobil fenyegetettségek egyik legfontosabb szeletét a rosszindulatú programok (malware) adják. A rosszindulatú programokat a támadók a PC világhoz hasonlóan számos módon juttathatják el a felhasználó okostelefonjára. Az egyik legjobb lehetőség számukra az alkalmazás-letöltési dömping kihasználása. Ezért fontos a közösségi hálózatokban való ésszerű és átgondolt részvétel, valamint a vezeték nélküli kapcsolatok biztonságos használata.

Ahogy internetbankolás esetében, úgy mobil netbankolás során is **a kilépés gombbal jelentkezzünk ki az internetes rendszerből**, továbbá a használat közben a böngésző címsorában szereplő linket **adatainak biztonsága érdekében ne küldjük tovább!**

Ha kétségei vannak, hívja fel számlavezető intézménye telefonos ügyfélszolgálatát információért, segítségért, és ehhez használja a bank hivatalos honlapját, az ott található elérhetőségeket!

Az adathalász módszer egyik változata, amikor a „hitelesítés" során Ön visszaigazoló SMS-t, rövid szöveges üzenetet kap a mobiltelefonjára, amely egyszer használatos kódot tartalmaz, és amit be kell írnia. Ebben az esetben az SMS-t valóban a bankja küldi Önnek, de legyen figyelmes: mihez ad engedélyt az SMS-kód? Előfordulhat, hogy a csalók egy banki applikációt, alkalmazást aktiválnak az Ön által megadott adatok segítségével, így hozzáférnek az Ön bankszámlájához. Az átutalásokat jóváhagyó üzeneteknek tartalmaznia kell a célszámlát és az összeget is - így feltétlenül olvassa el, hogy a visszaigazoló SMS milyen műveletet engedélyez, mielőtt azt bárhová beírná!

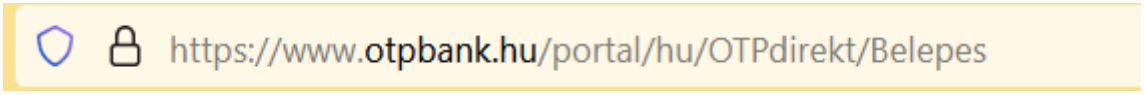
Jó tanács, hogy ne váljon online csalók áldozatává:

- Gondolja át a kapott üzenet tartalmát. Tisztázza magában, hogy a leírtak mennyire feleltethetőek meg a valóságnak. Lehet, hogy az adott szolgáltatásnak vagy banknak nem is az ügyfele? Egy olyan szolgáltatástól kap sms-t, ahol korábban nem adta meg a telefonszámát? Nem is rendelt semmit, mégis hogyan érkezhetne csomagja?
- Amennyiben nem tudja eldönteni egy üzenet valóságtartalmát, vegye fel a kapcsolatot a küldővel. Keresse fel például a szolgáltatója, a bankja vagy a hivatkozott csomagküldő szolgálat hivatalos honlapját, esetleg hívja fel őket a hivatalos telefonszámukon. Amennyiben egy közösségi oldalon privát üzenetet kap egy ismeretlentől? Hagyja figyelmen kívül. Azonban ha egy ismerőstől, kérdezzen vissza a linkre kattintás előtt, mit küldött Önnek az illető.
- Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvétellel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél kilétéről. Ne adja meg illetékteleneknek személyes, pénzügyi és biztonsági adatait! Ha egy gyanús üzenet egy linket vagy egy mellékletet tartalmaz, ne kattintson rá és ne is töltse le.
- Az esetek túlnyomó többségében az online térben működő bűnözők az emberi kíváncsiságot használják ki. Ne dőljön be egy ismeretlen feladótól kapott üzenetnek, ne akarjon csak most az egyszer kattintani, még akkor sem, ha az üzenet szerint egy videót talált Önről egy ismerőse. Egy nem várt és minden előzmény nélkül kapott linket vagy csatolmányt ne nyisson meg.
- Amennyiben adathalász-támadás célpontjává vált, jelezze munkahelyi vezetőjének, rendszergazdának, ismerőseinek, ezzel segítve az ő online biztonságukat. Nem volt elég szemfüles egy adathalász-üzenet kapcsán, és rákattintott az abban található linkre? Haladéktalanul vegye fel a kapcsolatot a számlavezető bankjával, és tegyen feljelentést a rendőrségen!
- Minden fontos kapcsolatában változtassa meg a jelszavát.
- Ne kattintson kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!

- Legyen körültekintő az üzenetekkel, emailekkel és telefonhívásokkal! Ismerje fel az árulkodó jeleket, tájékozódj rendszeresen a témában! A titkos adatokat pedig tényleg kezelje bizalmasan. Semmit sem ér egy titkos kód vagy jelszó, ha bárkinek elmondja.

- Mindig ellenőrizze le, hogy hová mutat egy URL, mielőtt kattintana! Könnyen meggyőződhet a valódiságáról, ha fölé viszi a kurzort, akkor látja, hogy mi a tényleges cím, ahová a link elnavigálja.
- Ahol lehet, mindig használjon kétlépcsős azonosítást, mert így egy plusz azonosítási kör is kell az érzékeny adatokat kezelő műveletek elvégzéséhez!

Fontos tudni, hogy a valós intézményi honlapok esetén a böngésző alsó sávján vagy felső címsorában szerepel a biztonságos kapcsolat meglétét jelző kis lakat ikon, továbbá az ilyen oldalak elérésekor és használatakor **a normál http helyett https (védett) kapcsolat épül fel az ügyfél gépe és az intézmény webszervere között**.



Ha áldozattá vált:

Rendőrségi feljelentést mindig csak maga a sértett tehet. Tehát, ha a csalás áldozata lett, csak ön tud feljelentést tenni a csalás kapcsán.

A rendőrségen szakértők foglalkoznak az internetes és mobilon keresztül bonyolított csalásokkal, így érdemes megtenni a feljelentést. Erre személyesen vagy e-mailben van lehetőség. Bővebb információért látogass el a www.police.hu weboldalra vagy keress rá a böngészőben a lakóhelyed szerinti rendőrkapitányságra a telefonos és e-mailes elérhetőségekért!

Amennyiben rendőrségi feljelentést tesz vagy bejelenti az esetet a szolgáltatónál, igyekezzen minél részletesebben átadni minden releváns információt, ezzel is segítve a vizsgálatot. Az itt részletezett csalások során az áldozatnak okozott kárért a szolgáltató nem tud felelősséget vállalni, de a beérkező visszaélésekkel kapcsolatos bejelentéseket kivizsgálják.

Hova fordulhat még

- Munkahelyen történt esetnél a felettes és a rendszergazda értesítése kötelező
- A csalásokat vagy csalási kísérleteket a Telekomnak a 1414 telefonszámon vagy a www.telekom.hu/irjonnekunk weboldalon tudod jelezni.
- Az egyes szolgáltatók ügyfélszolgálata
- Incidens Bejelentés | Nemzeti Kibervédelmi Intézet (gov.hu)

Források :

https://bank360.hu
E-banking biztonság (mnb.hu)
A Magyar Rendőrség hivatalos honlapja
https://nki.gov.hu/it-biztonsag/tudastar/
OTP bank.hu
Telekom.hu

Tájékozottságát mérheti: OTP Bank - Adatbiztonsági kvíz

Kelt: 2024.04.