Aggasztóan sok a netes banki csalás, de megúszhatjuk az átverést pár egyszerű szabály betartásával

Telex https://telex.hu/gazdasag/2023/10/11/banki-csalasok-mnb-unokazos

Itthon is elszaporodtak az adathalászatra épülő banki lenyúlások, a helyzet annyira súlyos, hogy a kereskedelmi bankok, a Magyar Nemzeti Bank és a rendőrség is lépett. Mindazonáltal a legtöbbet még mindig maguk az ügyfelek tehetik. Cikkünkben átvert áldozatok élményeit közvetítjük, bemutatjuk a leggyakoribb elkövetői technikákat, a bankok gyakorlatát, végül megosztjuk a legfontosabb tippeket, amelyekkel elkerülhetjük a bankszámlánk kiürítését.

A kifizetések, banki műveletek fokozatosan áttevődtek a digitális térbe, így ma már sokkal több értéket tulajdonítanak el bűnözők egy távoli laptop mögül, mint zsebmetszéssel, pajszerrel, vagy akár fegyveres rablással. Legutóbbi, banki csalásokról szóló cikkünk megjelenése után sok levelet kaptunk: részben áldozatoktól, akik tudják, hogy hibáztak, áldozatoktól, akik nem is értik, hogy pontosan mi történt velük, de olyan olvasóktól is, akik egy gyanús ponton megállították a csalási kísérletet és szívesen segítenek másoknak a tapasztalataikkal.
Olvasói élmények gyűjtése mellett beszéltünk kereskedelmi bankosokkal is, illetve megismertük a friss jegybanki ajánlásokat. Mindezek alapján több tanulság is kirajzolódik, és ha betartunk néhány alapvető szabályt, nagy valószínűséggel elkerülhetjük, hogy effajta bűncselekmények áldozatává váljunk.

„Pedig még gyanút is fogtam”

Olvasónkat, Ildikót (akinek nem ez az igazi neve) a csalók az OTP nevében keresték meg, ami nem ritka eset, a piacvezető lakossági bank ügyfélszáma a legnagyobb, ezért logikus, hogy a csalók az OTP nevében mutatkoznak be. Ildikó nem ügyfele ugyan a banknak, de a vonal másik végén gyorsan reagáltak. Azzal folytatták, hogy egy az OTP-nél feketelistás IP-címről, Kecskemétről, egy iPhone-ról kísérelték meg feltörni a számláját (ez a szöveg teljesen sematikus, bankosoktól tudjuk, hogy egy éve még csak Kecskemét említésén sem variálnak a csalók), ezért segítenek neki, most azonnal átkapcsolják a CIB-hez.
Ildikó ezután hibázott, félelmében személyes adatokat adott át. Hozzá hasonlóan többen is elmesélték, hogy igen, már menet közben is gyanút fogtak, de a nagy veszteségtől félve, a pszichés nyomás hatására mégis megtörtek, a helyzet felülírt minden józan gondolkodást.

Hibáztam, de a bank és a rendőrség sem segített

Miután aztán valóban az ügyfél közreműködésével megtörtént a visszaélés, Ildikónak az fájt, hogy bár „minden tőle telhetőt megtett azért, hogy csökkentse a kárát”, a rendszer ebben nem segítette: mint meséli, a bank, a NAV és a rendőrség is nagyon passzív volt az eset feltárásában, a károsult támogatásában, arról nem is beszélve, hogy sehol nem találkozott olyan szervezett segítséggel, amely a traumatikus élmény feldolgozásában segítette volna.
Pedig ő úgy érzi, hogy a jobb prevenció, a több tájékoztatás és az utólagos támogatás a bankoknak is érdekük lehetne, hiszen
„csalódott és kétségbeesett károsultak bolyonganak különböző Facebook-csoportokban, és mindenféle bankok elleni összeesküvés-elméleteket gyártanak”.
Mint Ildikó meséli, ő mára elfogadta a veszteségét, igyekszik pszichésen nem rámenni az esetre, tudatosan kedves maradt az emberekkel, az önmarcangolást abbahagyta, de bízik abban, hogy a jövőben több támogatást kapnak a károsultak.

Van, hogy lebuktatják magukat

De miért lett csalódott Ildikó? Amikor bejelentést szeretett volna tenni a bankjánál, értékes percek vesztek el az idegölő tájékoztató géphangok és menüpontok között, nem volt forródrót. Amikor a rendőrségre ért, már le volt tiltva a banki alkalmazása, az ügyfél nem tudta megnézni, hogy hova ment pontosan a pénze, a banktól nem kapott nyomtatott számlakivonatot az utalásokról.
A rendőrség bagatell, felderíthetetlen ügyként kezelte az esetet a jegyzőkönyv felvételénél, Ildikónak frusztráló volt, hogy az intézkedő rendőr többször megszakította a jegyzőkönyv felvételét, kiment, vélhetően párhuzamosan más ügyekkel is foglalkozott. Bizonyos fontosnak tűnő adatokat nem írt le, mondván azt majd a bank úgyis megadja. Gyakorlatilag úgy tűnt, hogy az elkövetői oldalt nem is igazán vizsgálják, mert reménytelen nyomozásként tekintettek az ügyre.
Ezen a ponton fontos közbevetni, hogy releváns, de névtelenséget kérő beszélgetőpartnerünktől tudjuk:
annak ellenére, hogy valóban nincs sok visszhangjuk az ilyen ügyeknek, valójában napi rendszerességgel buknak le a csalók.
Az ATM-eknél kihelyezett kamerák felveszik azt, aki gyors telefonos értesítésre várva már az automatánál lebzsel, majd másodperceken belül készpénzt vesz fel. De olyan elkövetők is akadnak, akik átkokat kezdenek szórni, ha a beszélgetés nem úgy alakul, ahogy várták, például a kiszemelt áldozatnak leesik, miről van szó, és nem ad adatot, vagy akár elkezdi felvenni a beszélgetést. Olyan is akad, hogy a bűnözőt az bosszantja fel, hogy csak kisebb összeg van a lehúzni kívánt ügyfél számláján. Ilyenkor a bűnözőt nyilvánossá tett dialektusa, a szavajárása segíthet beazonosítani. Forrásunk szerint jellemzően nem digitális zsenikről van szó ilyen esetekben sem, gyakori, hogy tanulatlan, unokázós csalással foglalkozó bűnbandák utaznak a banki csalásokban is.

Kamuvállalkozás kulcsszerepben

Ildikó esetében később kiderült, hogy az a számla, ahová a pénzt utalták, egy isten háta mögötti, kis település faluvégi romhalmazának címére bejegyzett, több vármegyében is eljárások, például NAV-végrehajtás alá vont fantomcéghez ment, feltételezhetően egy szerencsétlen és tanulatlan strómant használtak fel a csalók.
A NAV azonban nem adhatott ki információt, az ügyintéző deklarálta, hogy addig nem tud segíteni, amíg nem érkezik hozzájuk hivatalos rendőrségi megkeresés.
Sajnos kiderült, hogy egy ilyen rovott cég számlája – legalábbis az eljárások közben – a bankok szempontjából még lehet utalási célpont.
Sőt, még azzal is megijesztették Ildikót, hogy mivel a cég ellen inkasszót nyújtottak be, az sem kizárt, hogy még ha meglenne is a pénze, abból először egyéb tartozásokat egyenlítenek ki.
Az ügyfélben sok kérdés merült fel: miért nincs erről a veszélyről több tájékoztatás, gyorsabb banki reakció, ügyfélközpontúbb esetkezelés? Biztosan sokan gondolják úgy, hogy „aki áldozattá vált, az meg is érdemli”, de ez semmiképp nem ilyen egyszerű: lehet, hogy valaki naiv, túlságosan jóhiszemű, pénzügyileg képzetlen, esetleg könnyen megijeszthető, de ezeknek a hibáknak nem lehet többévnyi munkabér az ára.
Ildikó egyébként később jelezte nekünk, hogy nagyon hasznosnak találta a Magyar Nemzeti Bank (MNB) videóját (https://www.youtube.com/watch?v=p8ZRq4UNYjA&t=24s) , amelyben nagyjából 8 perc bevezető után találhatók a tartalmi elemek, jó tanácsok.

Mit tesznek a kereskedelmi bankok?

A hazai kereskedelmi bankosokkal beszélgetve érezhető, hogy a bankok minden tőlük telhetőt szeretnének megtenni azért, hogy a csalási eseményeket feltárják, hiszen a bizalom megőrzése vagy helyreállítása alapérdekük. A bankok ezért fejlesztik a biztonsági rendszereiket, a szűréseiket, növelik az ezzel foglalkozók létszámát.
A magyar csalási esetszám nemzetközi összehasonlításban még mindig alacsony, ugyanakkor az mindenki számára ijesztő, hogy egy ember életének megtakarítása pár másodperc alatt elillanhat.
De abban azért lehet bízni, hogy prevenció mellett vagy az ügyfél tevőleges közreműködése nélkül ennek nagyon kicsi az esélye. A bankok mindenesetre 24 órán keresztül megerősített humánerőforrás-csapattal védekeznek, de sajnos a bank nevében telefonáló csalók sokszor éppen arra építenek, hogy a legtöbb ügyfél már kapott olyan banki telefont, amiben jelzi az ügyintéző, hogy blokkolta az ügyfél kártyáját, amíg meg nem erősíti, hogy tényleg ő használta a kártyát Thaiföldön. Ilyenkor két eset lehetséges: az ügyfél vagy azt mondja, hogy nem ő volt, ami letiltáshoz vezet, vagy jelzi, hogy igen, éppen Bangkokban nyaral, csak ezt nem jelentette be. Nagyon fontos, hogy

ilyen alkalmakkor tényleg csak ennyiből áll az ügyintézővel folytatott a beszélgetés, nincs mese habbal, hogy ki, hol, milyen eszközről, hányszor próbált meg belépni, és az ügyfél-azonosításon túl nincs adatkérés.

Elkövetők és módszereik

Hagyjuk most egy pillanatra a bankokat, és vizsgáljuk meg a helyzetet az elkövetők oldaláról! Velük nem beszéltünk, de mint az őket üldözőktől hallottuk, ahogy tíz éve az unokázós csalás, úgy az adathalászat is egy egyszerű séma, amelynek know-how-ját ugyanolyan bűnbandák fejlesztik, majd értékesítik egymásnak. Az elkövetői csoportok sokszor átfedésben vannak a 2014-től elterjedt csoportokéival, csak itt még könnyebb dolguk van, hiszen nem kell személyesen odamenni a nagyihoz. (Az unokázós csalás ötletgazdáiról, Arkadiusz Lakatosz és Marcin Kolompar történetéről ebben a HVG-cikkben lehet bővebben olvasni.)
Az adathalászathoz minimális informatikai tudás kell, általában nem ők a legfifikásabb elkövetők a bűnözői világban. Valójában nyugodtabb körülmények között az ügyfeleknek is feltűnne, hogy a csalók nem jól fejezik ki magukat, olyan mondatokat és úgy ejtenek ki, ahogyan az egy valódi banki ügyintézőnél nem fordulna elő. Bizonyos elemek azonban erősítik a hihetőséget, így például a call centeres háttérzajokat jól imitálják a bandák, amelyek tagjainak leggyakoribb trükkjei mostanában ezek:

- Rábírják az ügyfelet, hogy a veszély miatt adjon meg adatokat, például CVC-t (a bankkártya hátoldalán található biztonsági kódot) is, mert az kell ahhoz, hogy a bank letiltsa a kártyát, megállítsa a csalást.
-
- Arra veszik rá, hogy irányítsa át a pénzét egy biztonsági számlára, ami persze nem létező fogalom, a számla a csalók felügyelete alatt van;
- Esetleg rábeszélik, hogy telepítsen egy általuk „biztonsági vírusirtónak” nevezett programot, ami valójában számukra kínál távoli hozzáférést az ügyfél gépéhez (AnyDesk, Teamwiewer, Rustdesk). Ezeknek a programoknak lehet létjogosultságuk kollégák között, vagy ha valaki távsegítséget kér, de a csalók felügyelete alatt minden jelszó vagy sms támadás alatt állhat.
-
- Emellett eléggé jellemző, hogy az ügyfeleket hamis weboldalra tereli a csaló, például ha népszerű árucserés oldalakon (a litván Vinted vagy a magyar Jófogás is ilyen) valamit el akar adni az áldozat, akkor a vevő az utaláshoz kér adatokat, vagy javasol valami remek csomagküldési megoldáshoz egy letöltést, ahol gyorsan és költségmentesen lebonyolítható az utalás. Természetesen a kattintás már a kamuoldalra terel.

- De azok a kattintásra ösztökélések is gyakran betalálnak, amelyek egy csomag nyomon követésével, egy főtávos késedelemmel, egy nyereménnyel, egy szexvideóval, vagy egy kérdőívvel kérnek kattintást.

  Akinek nincs akkora egyenlege, azt sokszor tranzitszámlának használják, ráutalják a pénzt, onnan valamilyen külföldi (nem ritkán fintech vagy bitcoinos cégekhez tartozó) számlára továbbítják. Fontos tudni, hogy jellemzően egy rossz helyre klikkeléssel még nem kerül bajba az ügyfél, de ha a kattintás után még fizetési megerősítéseket, adatokat is kér a kamuoldal, ott már tényleg meg kell állni.

A bank szűr, olykor lép, olykor nem

Egy kereskedelmi banknak sok minden gyanús lehet. Ha valaki hirtelen külföldi IP-címről lép be a netbankba, ha új eszközt regisztrál, ha hirtelen sok számlára utalna, limitet szabadít fel, nyelvet vált, vagy új partnernek nagy összeget utalna.
Ugyanakkor azt is meg kell érteni, hogy a bankoknak nehéz dolguk van a bűnesetek szűrésekor.
A hazai bankok több százezres, esetleg milliós ügyfélszáma mellett ezek az események is gyakran életszerűek, tényleg van olyan, hogy egy ügyfél telefont cserélt, külföldre ment, új számlaszámra utal. Ha pedig túl sok ilyen, megerősítésre irányuló telefont kapnának az ügyfelek, az is elégedetlenséget szülne a bankot illetően. Az is eléggé jellemző, hogy az idősebb áldozatot a csaló szóval tartja, így a bankból érkező, érdeklődő hívást nem veszi fel az áldozat, mert még vonalban van.
Végül az AFR 2.0 is megnehezítette a bankok dolgát. Az utalások immár 4-5 másodpercen belül elmennek akár 20 millió forintos összegig, így a bűnözők akár 20 másodperc alatt már mindennel végeznek, adatot lopnak, vásárolnak, vagy kiveszik az ATM-ből a pénzt.
Ha megtörténik a baj, és bejelentést tesz az átvert ügyfél, a rutin a következő: a bank azonnal reagál, megkeresi a társbankot, olykor sikerül is megállítani az utalási láncot. A legtöbb banknál van olyan gyorsvonal, amelyen a bankok elérik egymást, de a nemzetköziekkel ez nehézkesebb, ott még van olyan, hogy elmegy a megbízás, az ügyfél jelez, van is idő az előző napi zárás és a másnapi nyitás között, mégsem tudja a bank a holt időszakban megfogni a pénzt. Amint hallottuk, ezen a téren van fejlődés, egyre többször gördülékeny az együttműködés a pénzintézetek között.

10 jótanács

Lássuk, hogy mi mit tanultunk meg a beszélgetésekből!

- Egy bank munkatársa mindig csak egyszerű ügyfél-azonosítást végez (név, anyja leánykori neve, lakcím, születési hely, idő), soha nem kér semmilyen titkolni való személyes adatot az ügyfele azonosításához (bankszámlaszámot, lejárati dátumot sem, de PIN-kódot, vagy a kártya hátán látható CVC-kódot semmiképpen). A valódi bankos nem hadoval, őt csak az érdekli egy gyanús utalásnál, hogy az ügyfél jóváhagyta-e az utalást, vagy sem. Ha pedig nem, a banknak van eszköze leállítani a csalást.

- A bank soha nem javasolja azt, hogy egy „biztonságos számlára” utalja el az ügyfél a pénzét, vagy ahhoz adjon meg adatokat.
- A bankoknak nincs idejük és pénzük, hogy 40 percen át győzködjék, nyaggassák az ügyfelet. Aki egy ilyen hosszú beszélgetésbe bonyolódik, biztos lehet benne, hogy csalóval van dolga.
- Egy bank (például az OTP) soha nem figyelmezteti úgy egy másik bank ügyfelét (például egy K&H-st), hogy felhívja, majd a másik bankhoz kapcsolja az ügyfelet.
- Ahogy a bankkártyára nem írjuk vagy ragasztjuk rá a PIN-kódot, mert attól tartunk, hogy nem tudunk 4 számjegyet megjegyezni, úgy a 21. században a netes jelszavakkal van azonos feladatunk. Ne ugyanazok legyenek a jelszavaink mindenféle alkalmazásban, illetve ne hagyjunk elöl, egyszerű fájlokba ne írjuk be simán a jelszavainkat, PIN-kódunkat, CVC-kódunkat!
- Ne töltsünk le felszólításra nyakló nélkül semmilyen alkalmazást. A javasolt „vírusirtó” ugyanis könnyen lehet, hogy kémprogram.
- Ne utaljunk külső noszogatásra ellenőrzés nélkül idegeneknek pénzösszegeket!
- Ha a banki weblapra szeretnénk belépni, akkor kézzel írjuk be a címet, vagy mentett könyvjelzőről lépjünk be, de ne kattintgassunk összevissza!
- Vessünk egy pillantást a banki oldalunk, vagy a webshop URL-jére, és ha gyanús a domén, meneküljünk! Nagyon egyszerű az amazon.com helyett amazoncom.hu, vagy hasonlókat lefoglalni.
- Figyeljünk a bank által küldött értesítő sms-ek szövegére, a bank hívásaira! Ha csak lehet, vegyük fel, főleg egy gyanús hívás közben vegyük át a hívást, ha a bankunk ügyintézője hív.

Tisztelettel:
BRFK Kommunikációs Osztály