Dr. Szente Krisztina*

Így nem válunk telefonos adathalászat áldozatává

Ma az interneten, számítógép, okostelefon, okosóra használatával bankolunk, fizetünk, a telefonos adathalászok pedig az ezekhez használt azonosító kódjainkat akarják megszerezni A csalók megtévesztéssel, pszichológiai befolyásolással próbálkoznak pénzünk ellopására. A védekezéshez be kell tartanunk néhány egyszerű szabályt.

A telefonos csalásoknak egyik típusa, amikor a csalók magukat banki alkalmazottnak kiadva, gyanús tranzakciók, folyamatban lévő visszaélés miatt keresnek meg bennünket. A hívás nem egyszer olyan bank nevében érkezik, ahol nem is vezetünk számlát. Amint ez kiderül a csaló azonnal „intézkedik" és „átkapcsol" a számlavezető bankhoz. A csalók a pénzünk visszaszerzése, a tranzakciók megakadályozása, visszahívása, a kár bekövetkezésének elkerülése, a bűncselekmény elkövetőinek kézre kerítése érdekében kérik közreműködésünket. Valódi szándékuk azonban a személyes és banki adataink, a fizetési művelet jóváhagyásához szükséges kódok megszerzése. Arra is volt példa, hogy az általunk kiadott adatainkkal online személyi kölcsönt igényeltek.

A telefonhívások többségében egy távoli hozzáférést biztosító alkalmazás (jellemzően AnyDesk, TeamViewer, RustDesk) telepítését is kérik tőlünk a bankolásra használt eszközünkön, hogy hozzáférjenek bankszámlánkhoz, banki adatainkhoz. Legtöbbször arra hivatkoznak, hogy ez a bank vírusirtója vagy biztonsági programja, mellyel segítenek bennünket a gyanús tranzakció megakadályozásában.

A valós cél az, hogy a távoli hozzáférés engedélyezésével a csaló hozzáférjen az adott eszközön elérhető adatokhoz, közreműködésünkkel az általa szándékolt fizetési műveletek, átutalások kezdeményezésére kerüljön sor, ami a folyószámlánkon lévő pénzösszeg mellett egyéb megtakarításainkat, érték-papírszámlánkat, lekötött betéteinket is érintheti. Ha az alkalmazást okostelefonunkra is letöltöttük, a csaló számára a banktól sms-ben érkező jóváhagyó kódokat is láthatóvá tesszük.

A károsultak elmondása szerint a csalók sokszor azt is kérik, hogy az alkalmazás letöltését követően menjünk át a másik szobába, távolodjunk el az eszközünktől, mert „a vírusírtás csak így végezhető el sikeresen". Gyakori az is, hogy a csaló azzal hiteget bennünket, hogy a gyanús tranzakció összegét másnap vagy egy későbbi időpontban visszakapjuk, addig ne keressük sem a bankunkat, sem a rendőrséget. Előfordult olyan eset is, hogy a csaló azt hitette el az áldozattal, hogy banki ügyintézők, rendőrök is érintettek a csalásban, és ügy felderítése érdekében tilos bárkivel is beszélnie a történtekről. A valódi cél azonban az, hogy minél később tegyünk bejelentést a bankunknál és a rendőrségen.

A Pénzügyi Békéltető Testület (PBT) elé került egyik esetben a kérelmezőt az egyik bank nevében keresték telefonon, hogy végzett-e utalást külföldre, mert a bank biztonsági rendszere jelzett. A kérelmező közölte a hívóval, hogy másik banknak az ügyfele, erre azt mondták neki, hogy átkapcsolják számlavezető bankja biztonsági szolgálatához. A telefonhívás, a beszélgetés több órán keresztül tartott, melynek során a csalónak sikerült meggyőznie a kérelmezőt arról, hogy banki alkalmazott és azért jár el, hogy segítsen átutalni a pénzét egy biztonságos számlára, ahonnan azt majd

később visszakapja. A banki azonosítás a kérelmező elmondása szerint ugyanolyan tartalmú volt, mint a valódi banknál szokott lenni. A kérelmező a csaló kérésére telepítette készülékére az AnyDesk távoli elérést biztosító programot, majd több tranzakcióval közel 7 millió Ft-ot utalt át a csalók által megadott „biztonságos" bankszámlaszámokra, amit többé nem látott viszont.

A bankok ügyfélszolgálatai a valóságban nem kapcsolják át a hívást sem más bankhoz, sem a rendőrséghez. A banki ügyintéző, ha csalás gyanú miatt hív bennünket, nem több óra alatt, hanem azonnal letiltja internetbankunkat, bankkártyánkat, digitális szolgáltatásainkat, ha elmondjuk, hogy a gyanús műveletet nem mi végeztük. A bankoknak nincs „biztonsági" bankszámlája, amire a saját pénzünket átutalhatnánk. Amennyiben a hívó egy alkalmazás, program letöltését kéri tőlünk, szakítsuk meg a hívást!

Nem biztos, hogy a bank alkalmazottjával beszélünk, ha látszólag a számlavezető bank telefonszámáról érkezik a hívás. Ismert elkövetési mód ugyanis a hívószám-hamisítás (spoofing) útján elkövetett csalás is. Egy konkrét esetben látszólag a kérelmező számlavezető bankjától érkezett a hívás, a bank nevében eljáró ismeretlen személy azt közölte, hogy a bank rendszerében azt látja, hogy bankszámlájáról átutalásokat kezdeményeztek, s azt szeretné ellenőrizni, hogy azt a kérelmező kezdeményezte-e. A hívó azt mondta, hogy amennyiben ezeket nem az ügyfél indította, úgy további sms-ekben kódokat fog kapni, melyek visszaolvasásával a tranzakciók visszavonását tudja jóváhagyni.

Az ügyfél beolvasta telefonon az sms-ekben megjelenő kódokat, s mivel a csaló siettette és aggódott, hogy elveszik a pénze, csak a kódokra koncentrált. Mivel az sms-eket ugyanarról a telefonszámról kapta, mint korábban, emiatt fel sem merült benne, hogy csalásról lehet szó, erre csak akkor jött rá, amikor letette a telefont. Csak később szembesült azzal, hogy a kiadott kódokkal internetbanki belépést és egy nagyobb összeg átutalását hagyta jóvá.

A banki ügyintézők soha nem kérik az sms-ben kapott kódoknak a megadását. Ha ilyet kérnek tőlünk, azonnal szakítsuk meg a hívást. Ha az sms-ek szövegét elolvassuk, észlelhetjük a csalást.

A csalók sokszor sürgető, akár fenyegető hangnemet alkalmaznak. Azzal érnek célt, hogy pánikba esünk, pénzünk megmentése érdekében együttműködünk velük.

Bármilyen kétség esetén – mielőtt beszélgetésbe kezdenénk az ismeretlen féllel – ellenőrizzük a hívást, kérjük el a hívó azonosítóját, tegyük le a telefont és hívjuk fel mi a hívó felet bankunk központi telefonszámán keresztül.

Ha a bankunk hív fel bennünket, akkor a személyes adataink mellett csak néhány adatot kérnek el a beazonosításhoz (pl. milyen devizanemben vezetünk számlát, van-e társtulajdonos a számlán, rendelkezünk-e hitelkártyával, folyószámlahitellel stb.) de nem kérnek sem bankkártyaszámot, sem bankszámlaszámot, sem banki belépési adatokat, sem számlaegyenleget. A bank soha nem kéri semmilyen alkalmazás letöltését, nem kéri PIN kódunkat vagy, sms-ben küldött kódokat.

Ha mi keressük telefonon a bankot (pl. bankkártya-letiltás miatt) akkor annak több azonosító adatra van szüksége azonosításunkhoz.

Ha kételyünk van, éljünk akár a keresztazonosítás lehetőségével, aminek alkalmazását az MNB ajánlásában a telefonos vagy egyéb hangalapú kommunikáció során várja el a pénzügyi szolgáltatóktól. Ennek során legalább három kérdésre részben az ügyfél, részben a szolgáltató ügyintézője

válaszol a beszélgetésben, így mindkét fél azonosítható. Ez a gyakorlatban azt jelenti, hogy az ügyintéző által feltett biztonsági kérdésekre (pl. anyja neve) a válaszok egyik felét az ügyintéző adja meg, a válaszok másik felét pedig mi. Feltehetünk k olyan kérdéseket is, amelyekre a csalók nem tudhatják a választ, ezáltal meggyőződhetünk arról, hogy bankunk ügyintézője van a vonal másik végén.

Sokszor gyanúsan kedvező befektetési lehetőség, nyeremény ürügyén kezdeményeznek a csalók telefonos kapcsolatfelvételt. Ugyancsak telefonos megkereséssel indult az a csalás, amelynél az ügyfelet egy általa nem ismert társaság nevében hívták fel azzal, hogy nyert egy nyereményjátékon, és a nyeremény átvételéhez az ügyfél okostelefonjára le kell töltenie az AnyDesk távoli elérést biztosító alkalmazást.

A csaló az alkalmazás révén hozzáfért az ügyfél telefonjához. Habár a kérelmezőnek először kétségei voltak, mégis teljesítette a hívó fél utasításait, így telefonjáról belépett az internetbankjába is. A telefonhívás alatt az ügyfél bankszámlájáról a csaló több átutalást hajtott végre, amit a hívás közben látott is a netbankjában és furcsának is találta. Mégis elhitte a csalónak, hogy azért kerül sor először átutalásokra egy másik bank által vezetett számlára, mert ott „feldolgozzák az összeget" és onnan fogják átutalni részére a „nyereményt". Csak akkor fogott gyanút, amikor a személyi kölcsönt is igényeltek a nevében.

Egyik másik ügyben az ügyfél egy internetes oldalon bitcoin befektetés reményében regisztrált. Ezután a csalók telefonon hívták és rávették arra, hogy bankszámlája és bankkártyája adatait adja meg, valamint személyazonosító igazolványát, lakcímkártyáját, jövedelemigazolását és a bankkártyáját, azok mindkét oldalát fotózza le és küldje el. A csalók utasítására az AnyDesk alkalmazást is letöltötte a számítógépére és belépett az internetbakjába.

A csalók ezután az ügyfél adataival többmillió forint összegű online személyi kölcsönt igényeltek, majd az ügyfél számlájára folyósított kölcsönt a számlán lévő saját pénzével együtt elutalták. A kölcsönfelvételt, átutalást azt tette lehetővé, hogy az sms üzenetekben kapott banki megerősítő kódokat a csaló utasítására az ügyfél maga írta be az internetbanki felületre. Utóbbinak – habár látta, hogy távolból kezelik a laptopját és a netbankjához is hozzáfértek – csak az általa jóváhagyott utalást követően lett gyanús a történet.

Az adathalászat megelőzésére fontos a tájékozottság és az elővigyázatosság. Az ismert csalástípusok mellett bármikor újak jelenhetnek meg. Tájékozódjunk a bankok és más szolgáltatók honlapján, valamint a csalások visszaszorítása érdekében létrehozott KiberPajzs honlapon.

Ha mégis megtörtént a baj, haladéktalanul vegyük fel bankunkkal a kapcsolatot és tegyünk rendőrségi feljelentést. A rendőrség foglalhatja le azt a bankszámlát, amire a pénzünket átutalták, a bankunknak nincs ilyen jogosítványa.

** A szerző az MNB-n belül működő Pénzügyi Békéltető Testület tagja*

„Szerkesztett formában megjelent 2024. október 9-én a VG.hu oldalon."