Dr. Tarpai Lajos Tamás*:

Hogyan akadályozzuk meg a bankszámlánkkal vagy bankkártyánkkal történő visszaélést?

A jogosulatlan fizetési műveletek kapcsán egy dologgal mindenképpen szembe kell nézni: a visszaélések eddig ismert változatai minden esetben az ügyfeleket célozzák meg. Az általuk kiszolgáltatott adatok, információk és hozzáférések teszik lehetővé, hogy a csalások eredményesek legyenek. A célzott támadások különböző formákban jelenhetnek meg, mint például SMS, e-mail, WhatsApp, telefonhívások, hirdetések vagy éppen hamis banki oldalként. Előbb vagy utóbb várhatóan mindenki találkozni fog a bizalmas adatainak megszerzésére irányuló kísérlettel. Érdemes tehát erre felkészülni. A Pénzügyi Békéltető Testület (PBT) tapasztalatai azt mutatják, hogy az ügyfelek sokat tehetnek azért, hogy ez a rémálom lehetőleg sohase következzen be.

Pár ezer forintos vásárlásból milliós kár

A megszokás, a rohanó világ elaltatja az ügyfelek figyelmét, a csalók pedig pontosan ezt használják ki. A kis összegű szállítási költség vagy éppen a szokásosnak mondható közüzemi számla megfizetésekor például az ügyfelek rutinból járnak el: megadják a bankkártya adataikat a felületen, illetve az SMS-ben érkező internetes vásárlás jóváhagyó kódját. A megszokás, esetleg a túl korai vagy késői időpont miatt nem gondolják végig van-e folyamatban rendelésük, esetleg fizetendő közüzemi számlájuk.

Előfordul, hogy a sikertelen vásárlás oka, hogy nem a bankkártyás vásárlás jóváhagyó kódja szerepel az ügyfélhez érkezett sms-ben, hanem egy új eszköz aktiváló kódja. A csalóknak már ennyi adat elegendő lehet, hogy az ügyfél bankkártyáját digitalizálják a saját telefonjukra letöltött mobilfizetéses (pl.: Apple Pay, Google Pay) szolgáltatásba, majd azzal vásárlásokat hajtsanak végre a világ egy távoli pontján. Így egy látszólag 1499 Ft-os sikertelen bankkártyás műveletből több milliós nagyságrendű kár lehet.

A mindennapi, rutinos netbanki belépés is tartogathat veszélyeket. Például az ügyfelek legtöbbször egy internetes keresőbe írják be a bankjuk nevét és a felhozott találatokból, rendszerint az első kiválasztott oldalon kísérelnek meg netbanki belépést. Az internetes keresőből, e-mailben vagy egyéb üzenetben kapott linkről megnyitott honlapok azonban veszélyesek lehetnek! Csak a bank által meghatározott módon, az elérési útvonalat közvetlenül beírva szabad megnyitni a netbanki felületet.

Számos esetben fordult elő, hogy az ügyfelek az említett netbanki felületeken kezdeményeztek belépést és rutinból adták meg az sms-ben kapott kódot azon a bűnözők által kialakított áloldalon. Ez az üzenet azonban nem a netbanki belépés kódját, hanem a bank mobilalkalmazásának regisztrációs kódját vagy éppen a QR alapú belépés jóváhagyásának, esetleg az átutalási limit módosításának a kódját tartalmazta. Az ügyfelek legtöbbször a sikertelen próbálkozások -azaz az egymás után érkező kódok rutinszerű kiadása - után feladták a belépésre tett kísérleteket. Ezzel párhuzamosan azonban a csalók a megszerzett adatokkal, az ügyfél bankszámlájához kapcsolódóan mobilalkalmazást telepítettek a saját telefonjukra. Így a már megemelt limit mellett, jóváhagyás nélkül számos nagyösszegű fizetési műveletet végeztek el.

Csalók és szemfényvesztők

Fontos tudni, hogy az online világban kapott hitelesítő adatok és kódok azonosítják az ügyfeleket a bankok részére. A többlépcsős hitelesítéseket (például SMS-ben kapott kódok,

mobilalkalmazásban történő hitelesítés) a banki műveletek biztonságának növelése érdekében vezették be. A bankok ezáltal tudják ellenőrizni, hogy a fizetési műveletet valóban a számlatulajdonos kezdeményezte. Nagyon fontos, hogy az ügyfelek a saját adataik felhasználásával körültekintően járjanak el, hiszen minden egyes adat kiadásával gyengítik a biztonságukat jelentő védelmi vonalat. Olyan ez, mintha az ügyfél először csak a lakásába engedné be a csalót, aztán megmutatná neki a széfet, megadná a kódját, majd illedelmesen elfordulna, hogy a bűnöző szabad kezet kapjon a fosztogatáshoz.
A fenti példák rámutatnak arra, hogy ha az ügyfél a kapott SMS tartalmát valamilyen okból nem tudja értelmezni, akkor érdemes felhívnia a bankját, egyeztetni az üzenet tartalmát és általa végzett tevékenységet. Inkább kételkedjünk, mint hogy utólag szaladjunk a pénzünk után!
A csalók nemcsak üzenetekkel, hanem telefonhívásokkal is próbálják megszerezni a banki jelszavainkat és kártyaadatainkat. Tipikus példa, amikor az adathalász hívás során megpróbálják elhitetni velünk, hogy ténylegesen egy banki alkalmazottal beszélünk, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonálnak.
Szintén veszélyes, ha az online bankolásra használt eszközre távoli hozzáférést biztosító program telepítését javasolják (melyekre a csalók általában vírusirtóként hivatkoznak), vagy éppen bankbiztonsági okra hivatkozva bankkártya adatok, netbanki belépéshez szükséges adatok kiadását kérik. Legyen gyanús, ha limitemelést, fizetési műveletek törlése érdekében kódok kiadását vagy biztonsági számlára történő utalást kérnek. Fontos tudni: ha a bankok észlelik is a visszaélést és telefonon felveszik az ügyfelekkel a kapcsolatot, sosem kérnek a fentiekhez hasonlókat az ügyféltől. Amennyiben az ügyfél jelzi és megerősíti a visszaélést bankjának, akkor az korlátozza a számlához történő hozzáférést, tiltja a visszaéléssel érintett bankkártyát, mobilalkalmazást vagy éppen a netbanki fiókot. Nincs biztonsági számla, nem kell törölni a visszaélés megakadályozása érdekében semmilyen fizetési műveletet.

Óvatosan a személyes adatokkal!
Előfordul olyan visszaélési módszer is, amikor az ügyfél vélt befektetését kezelő személy kér hozzáférést az ügyfél netbankjához távoli hozzáférést biztosító alkalmazáson (pl. AnyDesk, TeamViewer stb.) keresztül. A PBT tapasztalatai szerint az ügyfelek sokszor kontroll nélkül teszik elérhetővé saját netbanki fiókjukat harmadik személy részére.
Több esetben előfordult, hogy kétségek nélkül nézték végig, ahogy egy harmadik személy távoli hozzáférésen keresztül fizetési tranzakció indít netbankjukban. Az is előfordult, hogy az ügyfél hosszabb időn át nem látta netbanki felületét, távoli hozzáférésen keresztül elrejtették előle arra hivatkozva, hogy egy alacsony összegű tranzakcióval tesztelni kell a netbanki fiók kapcsolódását a befektetést kezelő rendszerrel.
Sok ügyfél nem tette fel a jogos kérdést: vajon miért nem elég a bankszámlaszám megadása a befektetés kifizetéséhez? S miért kell a befektetett összeget egy teljesen ismeretlen magánszemély részére átutalni? Az érintett ügyfelek szerint azért, mert ezt mondták nekik a „banki tanácsadók”. Egyébként pedig alacsony volt az átutalás összege, így alacsony a kockázat, különben is minden fizetési műveletet erős ügyfélhitelesítéssel meg kell erősíteni. Csakhogy az erős ügyfélhitelesítés alól vannak kivételek. Ilyen eset, amikor olyan, elmentett partner (úgynevezett megbízható kedvezményezett) részére utalunk ismét, akinek azt már egyszer erős ügyfélhitelesítés mellett megtettük. Lehet, hogy az első ügyfél által jóváhagyott utalás csak 1 forint volt, de a következő már több milliós lesz, nem kellett hozzá külön jóváhagyás és a bűnözők számláján landol.

Minden olyan kérés gyanús tehát, ami a netbankunkhoz vagy mobilbankunkhoz kér hozzáférést.

Az alapkészségek elsajátítása mellett jó, ha a tudásunkat folyamatosan frissen tartjuk. Ehhez nyújtanak segítséget a bankok által küldött, illetve a honlapon megosztott visszaélésekkel kapcsolatos figyelmeztetések, információk, továbbá a Magyar Nemzeti Bank (MNB), számos hatóság, szervezet visszaélésekkel kapcsolatos biztonsági tanácsai.
A kiberbiztonsági kockázatok megelőzése érdekében az MNB, a Magyar Bankszövetség, a pénzpiac szereplői, illetve több egyéb hatóság nemrég KiberPajzs néven közös oktatási kampányt indított az elektronikus pénzügyi szolgáltatásokat igénybe vevő ügyfelek támogatására. Ennek kapcsán megújult az MNB Pénzügyi Navigátor oldalának digitális biztonsággal kapcsolatos fejezete is, mely további hasznos információval szolgál a témában.

** A szerző a Magyar Nemzeti Bank mellett működő Pénzügyi Békéltető Testület tagja*

„Szerkesztett formában megjelent 2023. június 7-én az Origo.hu oldalon."