Tornai Annamária Natália*:

Banki kibercsalások útvesztője, avagy hogyan ne sétáljunk csapdába? – 1. rész

A bankolásnál ma már nem csak a díjak és kamatok számítanak, hanem elvárássá vált a gyors és egyszerű digitális ügyintézés is. A rutinszerű mobilos vagy okosórás fizetésnek azonban megvannak a maguk veszélyei. Nem csak azért, mert sokszor megszokásból cselekszünk vagy kapkodunk, hanem legfőképp azért, mert az online térben kevésbé vagyunk óvatosak és gyanakvóak. Pedig figyelni kellene a hamis banki weboldalakra, a nem valós kereskedőkre és a kémprogramok esetleges letöltésére is.

A bankok, kártyatársaságok, egyéb kapcsolódó hatóságok és szervezetek csalásmegelőző rendszereket működtetnek és figyelik a tranzakciókat az uniós szabályok és hazai jogszabályi előírások alapján, melyhez a bankok számára a Magyar Nemzeti Bank (MNB) elvárásai és iránymutatásai is segítségül szolgálnak. A tapasztalat szerint azonban a legtöbb online csalás sikerességéhez az ügyfelek aktív közreműködése is hozzájárul, így azok megakadályozásában az ő részvételük is elengedhetetlen. Legyen éber, óvatos és körültekintő! Pénzügyeit csak akkor kezelje, ha kellő ideje van rá, hiszen a csalók azt próbálják kihasználni, hogy az emberek elfoglaltak, felületesen olvasnak, sietnek és gyorsan döntenek, megszokásból cselekszenek. A csalás során a szélhámosok igyekeznek számukra ideális körülményeket teremteni, a kiszemelt áldozat számára pedig ez vagy teljesen szokványosnak tűnhet, vagy épp kényelmetlen. Ezért alkalmaznak olyan különféle **pszichológiai módszerek**et, mint a megtévesztés, sürgetés, ráijesztés, vagy akár a félelemben tartás.

Ezt támasztják alá az MNB-hez beérkező fogyasztói panaszok is, melyek jelentős részében azt állapította meg a számlavezető intézmény, hogy az ügyfél nem volt elég körültekintő, azt hitte, hogy megfelelően járt el és úgy adta ki az adatait a csalóknak, hogy az nem is tudatosult benne.

Az egyik panaszos ügyfél például hiába volt meggyőződve arról, hogy a banki mobilalkalmazásában nem adott engedélyt semmire, mégis egy telefonhívás során a csalók elhitették vele, hogy a bankjából telefonálnak, és hamis utalásokat akarnak visszafordítani. Ehhez telepíttettek a károsulttal egy távoli hozzáférést biztosító alkalmazást (pl. AnyDesk), amin keresztül hozzáférést adott a telefonjához, így a netbankjába való belépését nyomon követték az elkövetők, és egy push üzenetes jóváhagyással még egy kártyadigitalizáció is történt.

A csalók közben megnyugtatták, hogy nem kérnek tőle sem személyes-, sem kártyaadatokat és biztonsági kódokat sem. Az ügyfél ugyan gyanút fogott, bontotta a hívást, de a csalók visszahívták, mondván, hogy azért nem kapott sms-kódokat, mert a csalók átirányították a mobilját, de ezt most ők visszavonták. A károsult ezt is elhitte, hiszen hirtelen sms-eket kapott, amikről – a csalók kérésére – még képernyőképet is készített. Ezek a kódok kellettek végül ahhoz, hogy valóban megtörténhessenek az utalások.

Hogyan védekezhet ez ellen? A sürgető vagy fenyegető hívás hangneme mindig legyen gyanús! Ne kapkodjon, hanem gondolja át alaposan, hogy mit is kérnek valójában! Ne telepítsen ismeretlen alkalmazást a telefonjára, ne engedjen hozzáférést és ne adjon irányítási lehetőséget másnak a mobilja fölött és ne adjon ki bizalmas információkat!

Több esetben is előfordult, hogy az ügyfelek hamis, banki internetbanknak vagy valamelyik szolgáltató fizetési felületének álcázott weboldalon adták meg az azonosítóikat, melyekkel aztán a csalók visszaéltek. Az egyik károsult online piactéren szerette volna eladni már nem használt ruháit.

A csalók felvették vele a kapcsolatot, e-mailben küldtek neki egy linket azzal az ürüggyel, hogy eladóként ott adja meg az áruk kifizetéséhez szükséges számlaszámot. A gyanútlan ügyfél a linkre kattintást követően kiválasztotta a megjelenő listából a számlavezető bankját, majd megadta a belépési adatait, beírta az sms-ben kapott kódot is.

Az ügyfél még visszaigazoló e-mailt is kapott, melyben megköszönték neki a szolgáltatás igénybevételét, és tájékoztatták, hogy hamarosan megkapja az áruért járó összeget. Ehelyett azonban a csalók a hamis oldalon keresztül megszerezték az ügyfél banki azonosítóit, a háttérben a valós banki weboldalon keresztül beléptek az ügyfél netbankjába, és az ott lévő pénzt el is tüntették a számláról.

Volt olyan ügyfél is, aki épp csomagot várt külföldről, ezért elhitte, hogy a „csomagod a vámnál van" címmel érkezett e-mail valós, és annak átvételéhez szükséges párszáz forintos vámkezelési díjat fizetheti be, ezért rákattintott a fizetés gombra. Egy postaszolgáltatónak tűnő oldalon megadta a kártyaadatait és az sms-ben kapott kódot is annak ellenére, hogy abban az szerepelt, hogy az egyszer használatos jelszó egy mobiltárca regisztrációhoz szükséges, nem pedig az utaláshoz. Ezt követően már nem kapott semmilyen értesítést, üzenetet, mégis több vásárlás történt a kártyájával a tudta nélkül.

Több panaszos ügyfél is kapott felszólító e-mailt valamelyik szolgáltatótól lejárt számlával kapcsolatban, a kapott linken pedig „befizették" a kért összeget attól tartva, hogy kikapcsolják náluk a szolgáltatást. Egyiküknek még az sem volt gyanús, hogy az általa használt telefontól teljesen különböző operációs rendszerű fizetési mód regisztrációját hajtotta végre.

Kifejezetten elterjedt visszaélési módszernek számít, amikor a csalók **az ügyfél bankkártyáját digitalizálják**. Ha az ehhez szükséges kódot megadja az áldozat, akkor a mobiltárca vagy okoseszköz későbbi használatakor már nem érkezik megerősítő kód, így a további tranzakciók sokszor csak a számlakivonatból derülnek ki. Az úgynevezett tokenizáció pedig épp a biztonság érdekében annak elkerülésére szolgál, hogy a kereskedő megkapja a kártyaszámunkat. A tokenizációt használó mobiltárcák úgy működnek, hogy a kártya regisztrálásakor a kártyaszámot egyedi, véletlenszerűen képzett számokkal helyettesítik, a kártyaadatokat ezáltal kicserélik egy helyettesítő tokenre.

Vásárláskor az eszközünk így már nem a tényleges kártyaszámot használja, hanem csak az adott tranzakcióra vonatkozó fizetési token kódot. Fizetéskor tehát nem a kártyaadatokat, hanem ezt a hivatkozást kapja meg a kereskedő, és a tokenszolgáltató tudja visszafejteni, kizárólag egy arra megfelelő feloldó kulccsal. Mivel ilyenkor nem ténylegesen a kártya használata történik, nem is kell PIN-kódot megadni, és az erős ügyfélhitelesítés sem elvárt az egyes vásárlásokhoz, csak magához a tokenizációhoz. Tehát ha óvatlanul megadja az ehhez szükséges kódot, azzal lényegében korlátlan hozzáférést enged a kártya digitális használatához.

Hogyan védekezhet? Legyen óvatos a mások által kezdeményezett kapcsolatfelvételekkel, ne kattintson az üzenetben lévő hivatkozásokra, és ne nyissa meg a mellékleteket, inkább használja a hivatalos (esetleg a kedvencek közé elmentett) banki oldalt! A jóváhagyáshoz kapcsolódó sms-ben vagy push üzenetben szereplő információkat olvassa el és értelmezze, ne adjon engedélyt olyan esetben, ha a jóváhagyó kód nem a szándékai szerinti tranzakcióra vonatkozik! Ha például a netbankjába akar belépni, de mobiltárca regisztrációról szól az sms/push üzenet, **azonnal szakítsa meg a folyamatot és vegye fel a kapcsolatot a bankjával**!

A csalók gyakran próbálkoznak azzal a módszerrel, hogy egy ismert e-mail címben vagy internetes oldal címében egy-egy karaktert kicserélnek egy nagyon hasonlóra. A kis- és nagybetűk is könnyen összetéveszthetőek, a nulla például nagy „o" betűnek tűnhet (0 ≠ O), a kis „L" és a nagy "i" is nagyon

hasonló (l ≠ I), de lehet benne egy plusz kötőjel vagy a .hu helyett .com is. Ilyen linket kapott egy csomagot váró ügyfél is, egy másik hasonló esetben pedig egy futárcéges üzenetnek álcázott sms-ben érkezett egy **rövidített link**.

Egy esetben a gyanútlan ügyfél elhitte, hogy csak a hibás címadatot kell javítania, és akkor sem fogott gyanút, amikor banki belépési adatokat kellett megadnia a linkről megnyíló felületen. A linkrövidítés több esetben is hasznos, és nem csak a csalók, hanem megbízható szolgáltatók is használják, ha pl. korlátozott karakterszám áll rendelkezésre vagy marketingcélból egy több soros linket átláthatóvá, szebbé kell varázsolni. A rövidített URL-ek elfedhetik a valós weboldalt, a teljes URL azonban link rövidítő alkalmazással (link shortener) visszafejthető, ezáltal megvizsgálható, hogy valóban meg akarjuk-e látogatni.

A kiberbiztonsági kockázatok megelőzésére, csökkentésére 10 állami intézmény, köztük az MNB és pénzpiac szereplői **KiberPajzs** néven közös kommunikációs és edukációs kampányt folytatnak, továbbá elemzik a folyamatokat, lehetséges intézkedéseket az elektronikus pénzügyi szolgáltatásokat igénybe vevő ügyfelek támogatására, védelmére.

KiberPajzs
Védelem a pénzügyekben

Az egyes csalástípusokról, ismertető jegyeikről, teendőkről a KiberPajzs oldalán további információkat talál (Ön felismerné az összes csalástípust? | KiberPajzs), emellett érdemes felkeresni az MNB Pénzügyi Navigátor weboldalának digitális biztonsággal kapcsolatos oldalát is, amelyen szintén hasznos információk találhatók a témában. Ugye megnézi a szöveg mögötti linket mielőtt kattint?

** A cikk szerzője az MNB fogyasztóvédelmi munkatársa*

„Szerkesztett formában megjelent 2024. szeptember 11-én a VG.hu oldalon.”