Szabó Péter*:
65 év felettiek vigyázat, csalók!

A digitális világ gyors fejlődése különösen az idősebb korosztályt teszi kiszolgáltatottá a kibercsalásokkal szemben. Az adathalász támadások súlyos pénzügyi veszteségeket okozhatnak, veszélyeztetve a nyugdíjas évek anyagi biztonságát. Fontos, hogy az érintettek és hozzátartozóik tisztában legyenek a megelőzés lehetőségeivel.

Szinte mindenki ismer olyan valakit, aki már adathalász támadás áldozatává vált, vagy hallott hasonló esetekről a hírekben. A kibercsalások az általnál is súlyosabb következményekkel járhatnak, ha nyugdíjas az érintett, hiszen akár az életük során felhalmozott megtakarításaik, akár a nyugdíjból származó összegek is a csalók kezébe kerülhetnek, ezzel veszélyeztetve a nyugdíjas évek anyagi biztonságát.

A csalások áldozatai – még ha utólag rájönnek is, hogy hibáztak – gyakran úgy érzik, hogy bankjuknak többet kellett volna tennie a megelőzés érdekében, vagy a csalási folyamat megállítása céljából. Ez az érzés fokozottan jelentkezik a nyugdíjasok esetében. Ilyen esetekben a Pénzügyi Békéltető Testülethez (PBT) is fordulhatnak, amely a pénzügyi intézmények és ügyfeleik között kialakuló anyagi, elszámolási jogviták rendezésének lehetséges fóruma.

Bár minden korosztály érintett lehet a kibercsalásokban, az áldozattá válás módja és gyakorisága különbözik az életkori sajátosságok és az eltérő banki ismeretek miatt. A PBT eljárásainál minden negyedik (!) esetben nyugdíjas volt az áldozat. Ez a magas részarány indokolttá teszi az okok elemzését és a figyelemfelhívást a megelőzés lehetőségeire. Az idősek különösen veszélyeztetettek, mivel kevésbé jártasak a digitális világban. Természetesen vannak kivételek, de a többség számára a technikai újdonságok nehézségeket okozhatnak.

A megelőzés érdekében célszerű áttekinteni a kibercsalások tipikus folyamatát. Ez különösen fontos a nyugdíjas emberek esetében, akik – mivel nem „digitális bennszülöttek” – esetleg idegenkednek egyes digitális eszközöktől, nehezen értik a bank által használt, gyakran angol szóhasználatot. Az idős emberek gyakran nem is sejtik, hogy ha nem használnak digitális szolgáltatásokat, akkor is áldozattá válhatnak. Gyakori, hogy a bank figyelmeztető üzenetét vagy SMS-ét félreértelmezik, vagy nem tulajdonítanak neki jelentőséget.

Egy tipikus bankszámlát érintő csalási folyamat például három lépésből áll: először a csalók valamilyen adathalászati módszerrel megszereznek fontos adatokat (kártyaadat, jelszó stb.), majd ezekkel tranzakciókat kezdeményeznek. Az utolsó lépésben megszerzik az áldozataiktól még azokat az adatokat, kódokat is, melyekkel jóváhagyják a csalárd tranzakciót.

Idősebbek körében gyakori, hogy a csalók telefonhívással próbálkoznak, erős érzelmi hatást kiváltva, sürgetve az áldozatot az adatok megadására. Gyakran nyereményt vagy különleges

lehetőséget ígérnek, amit azonnali adatmegadással lehet „elérni”. Az óvatlanság következménye az ügyfél bankszámláján lévő teljes összeg eltulajdonítása is lehet. Máskor a csalók a bank nevében telefonálnak, bizalmat ébresztve és azt a látszatot keltve, hogy a hitelintézet ügyintézője figyelmeztet visszaélési kísérletre.

E bűnözői módszerek közös jellemzője, hogy a csaló átgondolatlan lépésre készteti az áldozatot. Mivel figyelmeztető hívás ténylegesen érkezhet a banktól is, nem egyszerű a valós hívás megkülönböztetése a hamistól. A valós banki ügyintéző azonban soha nem kér telefonon érzékeny személyes adatot, jelszót, kódot. Ha szokatlannak, gyanúsnak tűnik a hívás, célszerű megszakítani a vonalat és sürgősen hívni a banki ügyfélszolgálatot a hivatalos telefonszámán.

A csalók az ügyfelek bizalmas kártya- és személyes adatainak megszerzése révén gyakran élnek az adott bankkártyák digitalizálásával is. A megszerzett adatokkal például a GooglePay vagy Apple Pay fizetési szolgáltatásra alkalmas eszközre, a saját mobiltelefonjukra regisztrálják az áldozat kártyáját. A sikeres digitalizálást követően a csaló ugyanúgy tud fizetni a saját mobileszközével, mintha a kártyával fizetne. Ehhez azonban szükség van a kártya adataira és egy biztonsági kódra, melyet általában SMS-ben küld a bank. Ha a bűnöző ezt is megszerzi, akkor már a saját eszközén tudja hitelesíteni a fizetési műveletet, például saját ujjlenyomatával vagy arcfelismeréssel, tehát akár a kártya PIN kódja nélkül.

A PBT eljárásai során gyakran előfordult, hogy az idős ügyfelek megkapták a GooglePay vagy Apple Pay szolgáltatásokra vonatkozó banki figyelmeztető SMS-eket, el is olvasták, azonban nem ismerték a szolgáltatást, vagy úgy gondolták, hogy úgysem fogják használni, ezért nem tulajdonítottak neki jelentőséget. Pedig, ha valaki ilyen értesítést vagy kódot kap a bankjától anélkül, hogy szándékában állna a telefonjával fizetni, soha ne adja meg a kódot, és ne írja meg emailben vagy SMS-ben, illetve ne mondja be telefonon a bűnözőknek. Ehelyett sürgősen vegye fel a kapcsolatot a bankjával, mert biztosan visszaélésről van szó.

Gyakori az is, hogy a bűnözők a visszaélések megelőzése érdekében ráveszik a jóhiszemű idős áldozatukat, hogy telepítsenek egy távoli digitális hozzáférést biztosító alkalmazást, például az AnyDesk vagy a TeamViewer programot számítógépükre. A csalók gyakran arra hivatkoznak, hogy a bűnmegelőzés érdekében „vírusírtásra” vagy egyéb „biztonsági alkalmazás” telepítésére van szükség, éppen az állítólagos más bűnözők távoltartására. Fontos tudni, hogy egy bank sohasem kér efféle távoli hozzáférést az ügyféleszközökre. Az ilyen alkalmazások telepítése az ügyfél közreműködését igényli, de ha valaki ezt megteszi, a csalók hozzáférhetnek az internetbankjához érkező információkhoz, kódokhoz, jelszavakhoz, sőt akár teljes irányítást szerezhetnek a számítógép felett. Ha nem akarjuk, hogy mások hozzáférjenek az eszközeinkhez, ne működjünk együtt ilyen alkalmazás telepítése kapcsán a csalókkal, ne adjuk meg a kódokat, és ne hajtsuk végre az utasításaikat!

A bűnözők sokszor próbálnak mobilapplikációkat is telepíteni a megszerzett adatokkal, melyhez a bankok szintén üzenetet és kódot küldenek a bankszámla-tulajdonosnak. Probléma ebben az esetben is akkor adódik, ha az ezzel kapcsolatos szöveges üzenetet az ügyfél figyelmen kívül hagyja vagy nem értelmezi jól. Idősebb ügyfelek gyakrabban nem tudják, hogyan értelmezzék az olyan üzeneteket, mint például a *„Mobilalkalmazás regisztrációs igény érkezett a bankhoz”*. Ha a csalók telefonon keresztül próbálják meg félremagyarázni ezeket az értesítéseket, különösen fontos, hogy az ügyfél ne dőljön be e meséiknek.

A digitális világ gyors fejlődése mindenki számára kihívás, s különösen igaz ez az idősebb korosztály számos tagja esetében. A környezetünkben élő idősek – családtagok, barátok, szomszédok stb. - támogatása, figyelmeztetése és figyelemmel kísérése kulcsfontosságú annak érdekében, hogy elkerüljük, hogy adathalász csalás áldozatává váljanak.

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

„Szerkesztett formában megjelent 2024. december 31-én a VG.hu oldalon.”