Dr. Tarpai Lajos Tamás*:
Az online termékértékesítés csapdái

Már nem használt termékeink értékesítéséhez kiváló lehetőséget biztosítanak az online piacterek. Különösen nagy öröm, ha a meghirdetett termékre szinte rögtön jelentkezik egy vevő, esetleg több is. Előfordulhat azonban, hogy innentől már csak éberségünk dönti el, hogy megkönnyebbült eladók leszünk vagy csalás áldozataként súlyosan megkárosítanak.

Régen a zsúfolt piacon gondosan figyeltünk arra, hogy a pénztárcánk a táska mélyén legyen és azt szorosan fogjuk. Alaposan körbenéztünk, nehogy meglopjanak bennünket. Ma már pénztárca nélkül, bankkártyával, mobiltelefonnal vagy okosórával szinte bárhol könnyen és gyorsan fizethetünk. Magabiztosan és sokszor rutinból használjuk ezeket az eszközöket, és a működésükhöz szükséges hitelesítő adatokat is. Pedig ugyanúgy kellene vigyáznunk rá, mint, ahogy régen a pénztárcánkkal tettük. Netbanki belépéshez, banki mobilalkalmazás regisztrációjához szükséges adataink ugyanis a ***személyes hitelesítő elemeink***! Ennek megfelelően az értékük és jelentőségük is sokkal nagyobb annál, hogy pusztán technikai műveletként tekintsünk például az SMS-ben érkező betű- és számkombinációra.
Tény, hogy a digitalizáció alapvetően változtatta meg a pénzünk kezelésével kapcsolatos hozzáállásunkat.

A manipuláció lélektana
Az online termékértékesítés kapcsán elkövetett visszaélés célja, hogy a csalók minél több banki azonosító adatot szerezzenek meg a gyanútlan ügyfelektől. Ez a módszer alapvetően az ügyfél manipulációjára épül.
A meghirdetett termékre szinte azonnal jelentkező vevő, a gyors és sikeres eladás lehetőségét kínálja az eladónak, így már önmagában óvatlanná teszi. Az, hogy ilyen esetekben a vevő intézi a szállítást és csak e-mailt *és nem banki adatokat kér*, még szintén nem teszi gyanússá az ügyletet. Különösen akkor nem, ha látszólag valamilyen közismert szállítást végző cég (pl. Foxpost, GLS, DHL) is bekapcsolódik a folyamatba. A szállítás véglegesítéséről, a vételár átvételéről érkező e-mail üzenet képi és színvilága is meggyőző lesz, mivel nagyon hasonlít az általuk valóságban is alkalmazott színvilágra. Minden esetben ellenőrizni kell azonban a küldő e-mail címét, ugyanis ilyenkor ez nem kötődik sem a szállítást végző céghez, sem az online piactérhez, ez azonban sajnos sokszor elmarad.
A Pénzügyi Békéltető Testület (PBT) elé kerülő ilyen ügyek szinte mindegyikénél az tapasztalható, hogy ha az ügyfélben a vevő jelentkezésekor nem merült fel gyanú az ügylet valódiságával kapcsolatban, akkor bármilyen további levelezés történik, bármilyen kódokat kell kiadnia, részt vesz a folyamatban, mindent automatikusan végigcsinál. Még akkor sem változtat a döntésén, ha több nyilvánvaló jel mutat arra, hogy visszaéléssel van dolga, és már sejti, hogy valami nem „kerek”.
Inkább legyen indokolatlan a gyanú bank felé történő bejelentése, a bankkártya- vagy netbanki fiók letiltása, mint, hogy akár több milliós kárt szenvedjünk. ***Tanulság, hogy bármikor lehet nemet mondani egy ilyen ügylet során***.

Kódjátszma – óvatosan az SMS-sel és a QR-kóddal!

Az online termékértékesítés kapcsán elkövetett visszaélés kulcsmozzanata, amikor az ügyfelet egy olyan oldalra irányítják, ahol ki kell választania a saját bankjának ikonját, majd be kell lépnie a netbanki felületére. A csalók kihasználják, hogy az emberek többsége megszokásból cselekszik. Sokan automatikusan belépnek ilyenkor, anélkül, hogy végiggondolnák: miért is van erre szükség? Nem ellenőrzik, hogy a megjelenő banki weboldal elérési útvonala egyezik-e bankjuk valódi weboldalával. Az ilyenkor megjelenő banki oldalak azonban ***adathalász oldalak, minden ide beírt adat, jelszó, kód, idegen kézbe kerül és ezeket felhasználva megkárosítják az ügyfeleket***.

A visszaélés során arra is ráveszik az ügyfeleket, hogy megadják a telefonjukra SMS-ben érkező kódokat, valamint a bankkártyaadataikat. Külön probléma, hogy az SMS-ben érkező kódok nemcsak a netbanki belépés kódjait, hanem banki mobilalkalmazás regisztrációs kódját vagy egyéb műveletek, például bankkártya telekód lekérdezés kódját is tartalmazzák. A megszerzett adatokkal a csalók a saját telefonjukra mobilbank alkalmazást regisztrálnak. Így pedig már könnyen és gyorsan hozzáférnek az ügyfél számlájához és teljesen kiürítik azt.

Előfordulhat, hogy az ügyfelektől a QR-kód beolvasását kérik, amelynek a netbanki belépés, illetve a fizetési művelet jóváhagyásában van szerepe. Ezekben az esetekben a QR-kódot e-mail vagy chat üzenetben küldik meg az ügyfeleknek azzal, hogy a vételár átvétele, „a pénz visszatérítése" miatt olvassák be a banki mobilalkalmazásukkal. ***Ha az ügyfél ezt megteszi, saját maga hagyja jóvá a már előkészített, nagy összegű átutalást.***

Hogyan ismerjük fel a csalókat?

Az online piactéren előforduló ilyen csalás csak egy formája a számtalan trükknek. Bármilyen visszaélést el lehet azonban kerülni, ha felkészülten, figyelmesen és kellő körültekintéssel járunk el. A csalók, mivel a banki rendszerek biztonságosak, így mindig az ügyfelek felől próbálnak a számlához hozzáférni, csupán a módszerek „csomagolása" változik. Ezért mindig kellő gyanakvással fogadjuk, ha bármilyen formában banki adataink kiadására vagy banki műveletek elvégzésére akarnak rávenni bennünket. ***A banki adatok és a hozzájuk kapcsolódó biztonsági elemek a számlánkat, pénzüket őrzik. Védjük őket ennek tudatában!*** Sose járjunk el rutinból, megszokásból, automatikusan! Mindig átgondoltan intézzük pénzügyeinket! Ne dőljünk be az online termékértékesítés során a sürgetésnek és az ügylethez szükségtelen adatok megadásának!

A visszaélések sajátossága a sürgetés. A csalók arra alapoznak, hogy az ügyfelek szeretnének minél hamarabb megszabadulni az eladás gondjától. A csaló azzal is nyomást gyakorolhat, hogy kifizette a vételárat és így már nem lehet másképp véghez vinni az ügyletet, csak jelentős késedelemmel. Előfordulhat, hogy a gyanútlan eladó látszólag a szállító cég vagy online piactér ügyfélszolgálatával is kommunikál, chat üzenetben. Természetesen ez is a csalás része. A chat üzenetekben is megerősítik, hogy az adásvétel, a pénz átvétele csak a megjelölt módon hajtható végre, minden más csak késedelmet okoz vagy egyszerűen lehetetlen.

A csaló üzenetek nyelvezete is gyanúra adhat okot: több esetben magyartalanok, keveredik benne a magázódás és a tegeződés. Az üzenetek tartalma is alapvetően eltér a valódi ügyfélszolgálatok chat üzeneteitől. Utóbbiakban nem találkozunk olyan mondatokkal, mint például „Mi egy nagyvállalatot képviselünk és nem lopunk pénzt a felhasználóinktól.", vagy „Szeretnénk segíteni és

megkönnyíteni a visszatérítési folyamatot, nem pedig átverni Önt.” Az ilyen mondatok már önmagukban gyanúsak.

Sokan gondolják, hogy ők egy ilyen visszaélésnek sohasem dőlnének be. A PBT-n tapasztaltak azonban azt mutatják, hogy ez hamis illúzió. Kortól, nemtől és iskolai végzettségtől függetlenül bárki lehet ilyen vagy más típusú visszaélés áldozata. Hogy ne így legyen, fogadjuk meg a bankok, illetve a Kiberpajzs együttműködés honlapján elérhető hasznos tanácsokat. **Ne üljünk fel a *sürgetésnek, a gyanús nyelvezetű, magyartalan üzeneteknek. Tájékozódjunk és legyünk óvatosak! Minden szempontból megéri!***

** A szerző a Magyar Nemzeti Bankon belül működő Pénzügyi Békéltető Testület tagja*

„Szerkesztett formában megjelent 2024. június 5-én a VG.hu oldalon.”