Ha tetszett ez a cikk, kövess minket a Facebookon is!

raketa.hu/hogyan-ne-doljunk-be-a-telefonos-csaloknak-akik-hiteles-banki-alkalmazottnak-tunnek

Több alkalommal írtunk már a Rakétán arról, hogy a csalók egyre kifinomultabb módszerekkel próbálkoznak, ha a pénzünk eltulajdonításáról van szó. Mostanában épp OTP-s banki ügyintézőnek adják ki magukat, és azzal az ürüggyel hívják fel áldozataikat, hogy gyanús tranzakciókat észleltek a számláján, a jelek szerint épp most próbálják ellopni a pénzét. Csizmazia-Darab Istvánt, az ESET/Sicontact IT biztonsági szakértőjét kérdeztük arról, hogy mégis hogyan ismerjük fel a csalókat, ha teljesen hitelesnek tűnnek.

Csizmazia-Darab István szerint a számítógépes vírusok, kártevők mellett sajnos gyakoriak a profi és amatőr csalók próbálkozásai is. Ezek sokszor adathalász weboldalra irányítanak minket, ahol például egy igazinak tűnő, de valójában hamis weblapon kell megadnunk azonosítóinkat és a jelszavunkat, amivel aztán a bűnözők már a nevünkben be tudnak lépni a valódi weboldalon, különféle károkat és bosszúságot okozva ezzel tulajdonosának.

Miért esünk könnyen áldozatul az SMS csalásoknak? A koronavírus-járvánnyal kapcsolatban a biztonsági szakemberek már többször említették, hogy a kiberbűnözők nagyon kreatív módon igyekeznek kihasználni az aktuális híreket, körülményeket. Nincs ez másképp most sem: az elmúlt időszakban a

webshopos vásárlások számának növekedéséhez igazodva futárszolgálatok nevében küldenek üzeneteket a csalók.

Az utóbbi időben viszont egyre gyakoribbak a kéretlen telefonhívások, ahol hivatalos szervezetek, pénzintézetek nevében jelentkeznek a csalók, és igyekeznek a gyanútlan, óvatlan felhasználóktól minél több személyes adatot kicsalni. Ezek segítségével pedig megszemélyesítve a naiv, pórul járt áldozatot, mérhető anyagi kárt képesek okoznak neki, például ellopják a számláján lévő összes pénzt.

A legutóbbi ilyen esetben az OTP bank biztonsági munkatársainak adták ki magukat csalók. Egy 70-es számról hívogattak véletlenszerűen embereket azzal a mesével, hogy állítólag éppen most, pár perce próbálták megcsapolni az ügyfél bankszámláját, és emiatt telefonálnak. Egy állítólagos *"Nagy Ludmilla"* kilencven-, illetve százötvenezer forintot próbált meg leemelni az ügyfél OTP-s számlájáról, ezért a telefonáló *"bankbiztonsági szakember"* szerint azonnal le kell tiltani ezt a számlát és a számlához kapcsolt bankkártyát. Ehhez pedig tőlünk kérik be a kártyaszámot, a kártyán szereplő nevet, a kártya lejáratát, a számlán szereplő egyenleget és persze a háromjegyű biztonsági CVC kódot is. A szakértő szerint

> óriási felelőtlenség ezeket az adatokat illetékteleneknek megadni, hiszen ezek birtokában egyszerűen ellophatják, elkölthetik a pénzünket.

A csalók továbbá arra kérik gyanútlan áldozatataikat, hogy a hívásuk fogadása után nagyjából tizenöt percig ne használják a netbankjukat, mert az állítólagos letiltás azt nem engedné. A valóságban viszont azért mondták ezt, hogy közben legyen idejük zavartalanul megcsapolni az adott bankszámlát.

A csalásban szereplő *+36 70/3666-000* számra rákeresve a telefonszamkereses.hu weboldalon már számos jelzést, figyelmeztetést olvashatunk, hogy erről a számról tört magyarsággal próbálják átverni a hívottakat adathalászok. Szerencsére a kommentelők közül sokan gyanút fogtak, és megszakították a beszélgetést.

> Fontos tudni, hogy a bankok sosem kérik el az ügyfelek PIN kódját, jelszavát, kártyájuk lejárati idejét, biztonsági kártyakódját,

ezek csak csalók lehetnek. Gyanú esetén legjobb, ha telefonon vagy személyesen keressük fel bankunkat és azonnal jelentjük az esetet. A bankkartya.hu weboldalon az összes magyarországi bank hivatalos elérhetősége megtalálható, a hozzájuk tartozó valódi telefonszámokkal együtt.

Védelem és megelőzés

A proaktív védelem érdekében használjunk olyan neves, megbízható biztonsági vírusvédelmi megoldást, ami dedikált védelmet tud nyújtani az adathalászat ellen, és a biztonságos online bankoláshoz is. Ne felejtsük el védeni az androidos eszközeinket sem, hiszen sokan már ezen bankolnak.

Az összes megtakarítását elveszítette, mert rossz alkalmazást töltött le a telefonjára Phillipe Christodoulou csak egy kriptotárcához tartozó alkalmazást töltött le az App Store-ból, de néhány pillanat alatt az összes bitcoinja felszívódott. A férfi 180 millió forintnak megfelelő összeget vesztett el, és nem ő volt mostanában az egyetlen, aki így járt.

De emellett nem nélkülözhetjük az óvatosságot, az egészséges gyanakvást, a biztonságtudatos hozzáállást sem. Legyünk óvatosak, hogy hol lépünk be a fiókunkba, hiszen a nyilvános Wi-Fi a kedvenc kávézónkban, vagy a főtéren elérhető hálózat nem feltétlenül a legjobb opciók arra, hogy megnézzük számlaegyenlegünket, vagy kifizessük számláinkat. Tartsuk operációs rendszerünket mindig naprakészen.

Hasznos, ha mindig folyamatosan figyeljük online egyenlegünket. Ezt legkönnyebben úgy tehetjük meg, ha bankunktól SMS értesítést kérünk az összes számlánkon zajlódó pénzmozgásról, így azonnal és sokkal könnyebben felfigyelhetünk az esetleges gyanús tevékenységekre, pénzmozgásokra.