KIBERPAJZS

SZERZŐ: BIRÓ GABRIELLA A MAGYAR NEMZETI BANK INFORMATIKAI FELÜGYELETI FŐOSZTÁLY VEZETŐJE, AZ (ISC)2 HUNGARY CHAPTER ELNÖKSÉGI TAGJA ÉS A WITSEC ALAPÍTÓ ELNÖKSÉGI TAGJA

A KiberPajzs projekt keretében alapító tagként a Magyar Nemzeti Bank (MNB), a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság (NMHH), a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság átfogó oktatási programot indított az ügyfelek digitális pénzügyi tudatosságának fejlesztése érdekében.

KiberPajzs
Védelem a pénzügyekben

A projekt célja, hogy egységes arculatú, folyamatos kommunikációval felhívja az ügyfelek, a fogyasztók figyelmét a biztonságos digitális pénzügyek alapvető tudnivalóira és segítse őket a csalások idejében történő felismerésében, megakadályozásában, hatékony kezelésében. Erről az öt szervezet 2022. november 7-én együttműködési megállapodást írt alá és ezzel egy időben elindult a www.kiberpajzs.hu honlap is.

Az együttműködési megállapodás megkötését hosszú hónapok előkészítő munkája előzte meg, amelynek során számos egyeztetést, tapasztalatcserét tartottak az aláíró szervezetek szűkebb és szélesebb körben, a kereskedelmi bankok, a kártyatársaságok, különböző rendőri szervek, a fogyasztóvédelem és az adatvédelmi hatóság szakembereinek bevonásával. Minden résztvevő megerősítette, hogy egyre több és egyre kifinomultabb visszaéléssel találkoznak az online térben, ezért a KiberPajzs együttműködés szükséges és időszerű.

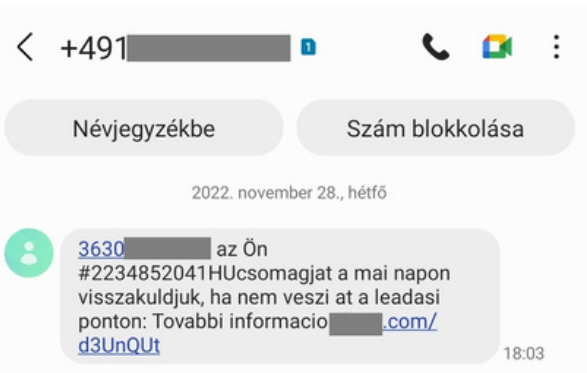
A kommunikációs kampány mellett a kezdeményezés másik nagyon fontos hozadéka a szakértők közti tudásmegosztás, a csalások forgatókönyveinek, elkövetési módjainak, ismérveinek és trendjeinek elemzése, a megelőzés és védekezés folyamatainak hatékonyabbá tétele. A szakértői egyeztetések, megbeszélések mellett eddig két szélesebb körű tudásmegosztó eseményt is rendeztünk 2022 májusában és októberében,

melyek során az előadók esettanulmányokat és elemzéseket mutattak be a visszaélésekkel, hatósági eszköztárral és kommunikációs lehetőségekkel kapcsolatban. A résztvevők visszajelzései alapján nagyon hasznos az eltérő megközelítéseket - a felügyeletek (MNB, NMHH), a bűnüldöző szervek, a bankok és a Pénzügyi Békéltető Testület tapasztalatait - egyben látni és megismerni a munkájuk során alkalmazott különböző megközelítéseket. Úgy tervezzük, hogy a továbbiakban is évente két alkalommal rendezünk hasonló tudásmegosztó alkalmakat hibrid módon, online és személyes részvétellel a projekt résztvevői és támogatói számára.

A projekt egyeztetései során a résztvevőktől kapott adatok alapján is látható, hogy az utóbbi időben felerősödtek azok a támadások, amelyek az erős banki-pénzügyi biztonsági rendszerek helyett -megtévesztés vagy/ és pszichológiai manipuláció révén - közvetlenül az ügyfeleket célozzák. Már az amúgy pénzügyekben járatos, pénzügyileg tudatos banki ügyfelek is áldozatul eshetnek a csalóknak, akik az utóbbi időszakban egyre kifinomultabb technikákat alkalmaznak. Néhány gyakori példa, a teljesség igénye nélkül:

Mostanában gyakori az az SMS-ben érkező üzenet, amely egy honlap felkeresésére vagy alkalmazás letöltésére és adatai megadására kéri a címzettet annak érdekében, hogy átvehessen egy csomagot. Mivel a karácsonyi időszak közeledtével a szokásosnál is többen és több árut rendelnek online, sajnos sokan jóhiszeműen áldozatul esnek ennek a fajta csalásnak.

Nagyon elterjedt visszaélési típus az is, amikor telefonon hívnak magánszemélyeket és úgy tesznek, mintha a bankjuk nevében tájékoztatnák őket. A csalók elmondják, hogy gyanús utalási vagy bankkártyás vásárlási kísérleteket észleltek a számlákról, illetve a bankkártyákkal. Emiatt, úgymond egy (hamis) „technikai számlára” továbbküldve azonnal biztonságba kell helyezni az ügyfél megtakarítását. A telefonos azonosításhoz szükséges pár személyes azonosítón túl pl. „további adategyeztetésre”, „netbanki letiltásra” hivatkozva a bizalmas banki adatokat (számla vagy/és kártyaszám, a PIN és netbanki belépési kód) is elkérik,



vagy a csalók számára távoli hozzáférést biztosító alkalmazás telepítését kérik, és az így megszerzett információkat felhasználva ellopják az ügyfél szálmájáról az ott lévő összeget. Egyre gyakrabban tapasztaljuk azt is, hogy az ilyen hívások hamisított számról, azaz látszólag a tényleges banki ügyfélszolgálati telefonszámról érkeznek.

Ehhez kapcsolódóan a legújabb gyakorlat, hogy a bűnözők nem csak a bankszámlát ürítik ki, hanem a megszerzett adatokkal visszaélve az ügyfél nevében személyi kölcsönt is igényelnek.

További új bűnözői módszer, amikor a fogyasztók internetes portálon hirdetnek eladásra egy árut, és a csalók vevőként jelentkeznek. Azt kérik az eladótól, hogy egy csomagküldő szolgálat internetes oldalán banki azonosítóik megadásával indítsanak fizetési kérelmet feléjük, s akkor ott kifizetik az árut. Csakhogy az általuk megküldött csomagküldő weboldal hamis, s az azon szereplő internetes banki linkeket is ők alakították ki, így a banki adataikat begépelve az ügyfelek maguk adják meg az információkat a csalóknak.
Az elsősorban cégeket, intézményeket érintő úgynevezett számlaváltásos csalások (vagy angolosan Business Email Compromise visszaélések) is egyre gyakoribbak. Ezeknél az eseteknél a bűnözők egy várható költséggel kapcsolatban azt a látszatot keltik, mintha a számla jogosultjának megváltozott volna a számlaszáma és kérik, hogy másik bankszámlára utalja át az összeget. Jellemzően csak akkor derül fény a bűncselekményre, mikor a számla fizetési határideje letelik és a pénz jogos várományosa keresi az összeget.

Bár összességében rendkívül biztonságos a hazai elektronikus pénzforgalom, s a visszaélések aránya elenyésző, mégis jól láthatóan emelkedik a kibercsalások száma, és mostanra szinte mindenki találkozott egy-egy esettel a fent felsorolt példák közül is. Ezért is fontos - a szabályozás/adminisztratív védelem és a technikai eszközök alkalmazása mellett - a fogyasztók biztonságtudatosságának fejlesztése, a figyelemfelhívás. Az MNB a KiberPajzs kezdeményezés mellett is sokat tett és tesz azért, hogy a problémára felhívja a figyelmet: több szakmai cikket jelentetett meg a témában, a fogyasztók tájékoztatására megújította Pénzügyi Navigátor oldalának digitális biztonsággal kapcsolatos fejezetét.

A jegybank mellett a pénzügyi intézmények, hatóságok és különböző szervezetek is folytatnak figyelemfelhívó kampányokat: teljesen világos, hogy csak összefogással, a résztvevők eszközeinek együttes alkalmazásával léphetünk fel hatékonyan. A novemberben indított első kampány során a plakátokon három olyan „mindennapi példakép” személyiséget jelenítettünk meg, akik élethelyzete hasonlít a legtöbb pénzügyi fogyasztóéhoz. Terveink között szerepel, hogy további karaktereket mutatunk majd be, illetve a jövőben szeretnénk kampányfilmekben, rádiókban, valamint egyéb csatornákon is ismertetni a főbb csalási formákat.