Hírlevél

A Veszprémi Rendőrkapitányság Bűnmegelőzési kiadványa – 2023. 7. szám

TARTALOM

A vagyon elleni bűncselekmények jelentős minőségi változáson mentek keresztül az elmúlt években. Ezt a tényt advent időszakában is érdemes szem előtt tartani. Míg korábban a legtöbb kárt a lopások okozták a sértetteknek, napjainkban már egyre inkább a csalásokra tolódik át a súlypont. Természetesen nem a hagyományos csalásokra kell gondolni, hanem azok online verzióira, továbbá azokra melyek már eleve internetes alapon jöttek létre.

A klasszikus advent időszakában elkövetett bűncselekmények bemutatása mellett ezért az év utolsó Hírlevelében folytatjuk az online csalások fajtáinak bemutatását. Az év utolsó számában az online befektetési csalásokat, ezen belül elsősorban a kriprovalutás befektetési csalást vesszük górcső alá.

AZ ÜNNEPEK BIZTONSÁGA

Az online és az offline bevásárlás során is érdemes óvatosnak lenni

A karácsonyhoz közeledve egyre inkább tetőzik a forgalom a piacokon, bevásárló központokban. Ennek eredményeként jellemzően kialakul az a „kritikus tömeg”, ami kedvező helyzetet terem a zsebtolvajoknak. Az elmúlt években a belvárosok, üzletsorok, forgalmas bevásárlóközpontok és azok parkolói visszatérő helyszínei voltak a különféle adománygyűjtő akcióknak. Az adventi időszakban fokozódik ez a tevékenység, mivel ilyenkor a legnagyobb a forgalom az üzletek környékén, és a szeretet ünnepének közeledtével növekedik az adakozókedv a lakosságban. Ezt használták ki azok a csalók is, akik valamilyen karitatív célból történő gyűjtésre hivatkozva pénzt gyűjtenek a járókelőktől. Advent időszakában napirenden lehetnek az alkalmi lopások, mivel a vásárlók figyelme ilyenkor erősen megosztott, kevésbé kontrollálják értékeiket, ezért az átmenetileg valahova (pl. pultra, kasszaszalagra) letett vagy valahol (pl. próbafülke) ottfelejtett táskáknak, pénztárcáknak hamar lába kellhet. Érdemes az időseknek fiatalabb családtagjaik kíséretében üzletbe, áruházba menni, hiszen ilyenkor a hozzátartozó nem csak fizikai segítséget tud nyújtani, hanem éberségével az értékek megóvását is biztosíthatja. Az internetes vásárlók, eladók sincsenek biztonságban. Az „offline” tanácsok mellett az online karácsonyi vásárlásokhoz különösen fontos megszívlelni az alábbi tanácsokat.

AZ ÉRZELMEINKRE HATNAK

Az online csalások lélektana az áldozatok szemszögéből

Az online csalások mindennapossá válásának jelentőségét nem lehet túlbecsülni, az a bűnözés történetében új korszakot nyitott. A minőségi ugrást azoknak a módszereknek a megjelenése jelentette, amelyekkel az áldozatot már minden vagyonából ki lehet forgatni, sőt adott esetben még hitel felvételére is rábírhatják, melynek összege szintén az elkövetőkhöz kerül. A sértettek pedig csak sorjáznak. A probléma lényege, hogy az áldozatok bár rutinszerűen használják az internetet, ez a rutinjuk azonban gyakran csak technikai jellegű. A „hogyannal" tisztában vannak, azonban azt, hogy pontosan mit csinálnak, ők maguk sem látják előre. E veszélyes jelenségről szóló napi híradások egyelőre nem késztetnek tömeges önvizsgálatra. A sértettek között vannak, akik fordítóprogramokon keresztül leveleznek idegenekkel, mások a csalók által előadott történetek hatására hozzáférést biztosítanak netbankos, mobilappos azonosítóikhoz, jelszavaikhoz, amivel végső soron megszegik a bankjuknál aláírt általános szerződési feltételeket. Mindezek alapján megállapítható, hogy a sértettek nem érzik át kattintásaik súlyát, lehetséges veszélyeit, mert nem tudatosították magukban, hogy az elektronikus banki szolgáltatások igénybevételével mekkora felelősséget vettek magukra, szemben azzal, ha pénzügyeiket továbbra is bankfiókjukban intéznék a sorszámhúzást követően. A kényelem és a lényegében korlátlan szabadság a bankolás terén veszélyes vizekre vezethet. Amíg ezt nem ismeri fel a társadalom, addig a csalók hatalmas bevételekre fognak szert tenni.

Az első ellenfél, amivel a bankszámla-tulajdonosnak meg kell küzdenie, az önmaga. Védtelenül és felkészületlenül áll az online csalókkal szemben, óriási az információs deficitje velük szemben. Amíg ezt a hátrányát nem faragja le, addig esélytelen marad. Tovább bonyolítja a helyzetet a módszerek sokszínűsége. Erre figyelemmel teljes immunitással csak az az internethasználó rendelkezik, akinek az élet minden területén naprakész a tudása, beleértve a bűnözés által teremtett kihívásokat is. Ilyen emberek azonban csak rendkívül kis számban létezhetnek. A többségről az mondható el, hogy egy bizonyos körben tájékozott, ami pedig azon kívül esik, abban nem. Itt jön a második nagyon fontos elem, a korlátok felismerése és hogy ami azokon túl van, ahhoz a legnagyobb alázattal és elővigyázatossággal kell közelíteni. Az online csalások megelőzésében az informatikának (vírusírtó, tűzfal stb.), komoly jelentősége van. Ennek speciális területe a bankbiztonság, mely a legkülönfélébb technikákkal (tranzakciós limitek, kétlépcsős azonosítás stb.) törekszik megnehezíteni a bűnelkövetők dolgát, illetőleg mérsékelni az ügyfelek esetlegesen bekövetkező kárát.

A csalók a céljaik elérését nehezítő akadályokat általában úgy kerülik ki, hogy a „védelmi vonal” leggyengébb láncszemét az embert veszik célba megtévesztéssel, csellel, fortéllyal. Leggyakrabban négy pszichológiai tényezőre alapozzák a sikert. Ezek mindegyikében közös, hogy rontják a potenciális áldozat tisztánlátását, megnehezítik, hogy higgadt maradjon és gátolják abban, hogy felismerjék az őket fenyegető veszélyt, illetőleg érzékeljék, hogy milyen irányból kell számítani rá.

ÖRÖM, EUFÓRIA

Az elkövető az áldozatban pozitív érzelmeket indukál: váratlan lehetőség reményét kelti az anyagi gyarapodásra (nyereményjáték, nigériai ajánlat, kriptovalutába történő befektetés) vagy a társra találás esélyét villantja fel (romantikus csalás).

FÉLELEM, RETTEGÉS

Az elkövető az áldozatban negatív érzelmeket indukál: félelmet kelt súlyos anyagi veszteség bekövetkezésével fenyegetve (bank alkalmazottjának kiadva magát telefonál) vagy az ismerősök előtti megszégyenülés lehetőségét előre vetítve (zsaroló e-malt küld).

IDŐZAVAR, KAPKODÁS

Az elkövető az áldozatot azonnali kármentő cselekvésre ösztönözi (bank alkalmazottjának kiadva magát telefonál) vagy azt a „félelmet” alakítja ki az áldozatban, hogy ha nem lép haladéktalanul, akkor lemarad egy kedvező lehetőségről (nyereményjátékból származó vagyoni előny, termék áron alul történő megvásárlása, vagy alku nélküli azonnali eladása).

GÉPIES CSELEKVÉS

Az internethasználók mindennapi tevékenységük során kialakítják azokat az időt spóroló technikákat (sütik használatának automatikus elfogadása, hírlevélre feliratkozás azonnali elvetése a felugró ablakok szövegének elolvasása nélkül), melyek beidegződéssé válását ki tudják használni a csalók. Az online vásárlások során automatizmussá rögzülhet a bankkártya adatok visszatérő beírása az arra kialakított felületek rovataiba. Az áldozat később egy ezzel éppen ellentétes szituációban (pl. termékeladás online piactéren) esetleg nem is mérlegeli már, hogy ténylegesen szükség van-e ezeknek az adatoknak a megadására.

Amennyiben a fenti érzelmi hatások valamelyikét vagy azok kombinációját érzékeli magán a potenciális áldozat, akkor valószínűsítheti, hogy az online csalás már kísérleti szakba lépett. Ekkor még rendelkezésre áll a lehetőség a szituációból való kilépésre és az anyagi veszteség elkerülésére, azaz a megkezdett bűncselekmény nem válik befejezetté.

ÍGY KERÜLHETŐ EL A„KRIPTO” CSALÁS

A közelmúltban megszaporodtak a befektetési csalások

Az elkövetők különböző online hirdetési felületeken osztanak meg rendkívüli hozamokat ígérő befektetési lehetőségről szóló hirdetéseket. Teszik ezt jellemzően híres magyar közéleti személyiségek arcképét ábrázolva, és ezzel azt a látszatot keltve, hogy a csalinak kihelyezett hirdetésben szereplő „celebek” is befektettek a kihagyhatatlan ajánlatba.

A csalások közös pontja jellemzően az, hogy egy kezdeti, relatíve alacsony összeg befektetését kérik, amely azonban folyamatosan emelkedhet a befektető (és egyben a későbbi sértett) fizetési hajlandósága szerint. Az elkövetők sokszor hamis cikkeket is közzé tesznek az interneten, mellyel megpróbálják hitelesebbé tenni a kriptovalutás befektetési formákat. Fontos azonban tudni, hogy a hivatkozott automatikus kriptovaluta-kereskedő rendszerek nem léteznek, így ilyenekbe érdemben befektetni sem lehetséges. Bár a különböző elkövetések során a befektetést kínáló alkalmazás-csomag elnevezése is változó lehet, legtöbbször a bitcoin-loophole angol kifejezésre hivatkoznak, melyet a hivatkozott szoftver kihasznál, ezáltal hatalmas összegekre tehet szert a felhasználó. Mivel bitcoin loophole nem létezik, így befektetési formának is alkalmatlan.

A kriptovaluta „befektetési rendszerek” esetében a csalók tapasztalt befektetéskezelőknek adják ki magukat. Azt állítják, hogy speciális módszerüknek köszönhetően dollármilliókat kerestek a kriptopénzekbe való befektetéssel. Majd azt ígérik áldozataiknak, hogy nekik is sok pénzt fognak keresni. Ehhez a csalók előzetesen díjat kérnek, ezután egyszerűen ellopják a befolyó pénzeket.

Kriptovalutába fektetni nem lehetséges a befektetési forma ismerete nélkül. Sőt, ennek a befektetési fajtának a lényege pont az, hogy közvetítő cégek, személyek nélkül működik.

A csalók kriptovalután kívül egyéb kecsegtető üzleti ajánlatokkal is megtalálhatják áldozataikat: részvények, kötvények, tengeren túli ingatlan-befektetések, ritka fémek, vagy alternatív energia – mind olyan hívószavak, amelyek alkalmasak arra, hogy az emberek leginkább elhiggyék róla jövőbeli gazdaságuk forrása lehet.

KIBERPAJZS

Összefogás a digitális pénzügyi bűnözőkkel szemben

KiberPajzs néven közös oktatási és kommunikációs együttműködésről döntött a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, az Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, illetve az ORFK 2022-ben**.** A kezdeményezéshez 2023. szeptember 7-én a Gazdaságfejlesztési Minisztérium és a Magyar Államkincstár is csatlakozott. A KiberPajzs projekt egyik legfontosabb célja a tájékoztatás, az edukáció, az ügyfelek és felhasználók figyelmének felhívása az online tér pénzügyi biztonságot veszélyeztető kockázataira. Az alapítók célkitűzése, hogy az elsajátított ismeretek segítségével a lehető legteljesebb pénzügyi tudatosság alakuljon ki a digitális pénzügyi szolgáltatásokat használó lakosság körében, ezzel csökkentve annak esélyét, hogy online csalás áldozatává váljanak.

Az együttműködés alapján létrejött honlap a **www.kiberpajzs.hu**, amely mindig naprakész információval szolgál olvasóinak az aktuális online csalási módszerekről. A KiberPajzs abban is segíti a látogatóját, hogy idejekorán felismerje, ha a sérelmére bűncselekményt kísérelnek meg elkövetni.

Ezen bűncselekmények felderítése, sértettjeik kártalanítása még bizonytalan, az egyedül hatékony megoldásnak a megelőzés tűnik. A támadások elhárítására pedig csak azok képesek, akik kellőképpen felkészültek a témában. A Veszprém vármegyei rendőrség elnevezésű Facebook oldalon a Veszprém Vármegyei Rendőrfőkapitányság Sajtószolgálata rendszeresen megosztja az aktuális híreket, közleményeket, a legújabb online csalási módszereket. Ezek között az online csalások is szerepelnek, továbbá az azok megelőzését segítő információk.

Információkéréssel forduljon hozzánk bizalommal!

Veszprémi Rendőrkapitányság
8200 Veszprém, Bajcsy-Zsilinszky utca 2.
Tel: 06-88/428-022
E-mail: **rauszi@veszprem.police.hu**

A kiadásért felel: Rausz István r. ezredes rendőrkapitány

Tájékoztatjuk, hogy a Rendőrségi Adatvédelmi Nyilvántartás szerinti adatvédelmi tájékoztató a következő linkről letölthető:

http://www.police.hu/hu/a-rendorsegrol/adatvedelem/altalanos-informaciok

Tájékoztatjuk továbbá, hogy amennyiben a jövőben nem kívánja hírlevelünket megkapni, a Veszprémi Rendőrkapitányság rauszi@veszprem.police.hu e-mail címre küldött üzenetével kérheti e-mail címe törlését.