Előzzük meg a kiber térben történő csalásokat!

Országosan, így a Gárdonyi Rendőrkapitányság illetékességi területén is megszaporodtak a kibertérben elkövetett bűncselekmények, amelyek több válfaja is ismertté vált az elmúlt időszakban. A két leggyakoribb a pénzintézetek nevében elkövetett, illetve az adathalászattal elkövetett csalások.

A pénzintézetek nevében elkövetett csalások módszere a következő.

A sértetteket telefonon azzal hívják fel az elkövetők – megtévesztésként olyan telefonszámot használnak, ami azonos lehet egy hitelintézet hívószámával (VOIP interneten kigenerálható számok)-, hogy a számláján folyamatban vannak tranzakciók, amiket a „bankbiztonság" ellenőriz, hogy a hívott fél kezdeményezte-e. Ezt követően a sértettől kikérdezéssel megszerzik a netbank belépési adatait, vagy a bankkártya adatait - bankkártya száma, lejárati dátuma, illetve annak hátoldalán található CVC kódot -, aminek birtokában hozzá tudnak férni a sértett bankszámlájához. A következő lépésben a banki adatok ismeretében bármilyen műveletet el tudnak végezni a bankszámlán, így utalni is lehetőségük nyílik a számlán levő összegekből. Általában más magyar, vagy külföldi bankszámlára, illetve kriptovaluta számlára utalják tovább a megszerzett összegeket.

A sértetté válás megelőzésének, elkerülésének lehetőségei:

Köztudott, hogy a bankok nem kérnek az ügyfelektől bankszámla, ill. bankkártya védelmét szolgáló adatokat, így CVC kódot, számlaszámot, bankkártya számot, egyéb ügyfél adatokat mivel az előttük ismert.

Az ügyfeleknek ilyen jellegű hívás kapcsán semmi esetben nem szabad személyes, ill. banki adatokat közölni, kiadni telefonon keresztül. Ugyanezt a magatartást kell követni, ha elektronikus levélben kérnek be ilyen azonosító adatokat, pl. emailben, vagy egy honlapra történő átnavigálás kapcsán. Kerülni kell a bizonytalan kapcsolatfelvételek során kért netbankos belépéssel kapcsolatos információk megosztását, így elkerülhető a bankszámla információk, bankkártya adatok illetéktelen kezekbe kerülése, valamint a bankbiztonsági rendszerben alkalmazott többlépcsős védelmi rendszerek (megerősítő sms) kikerülése az ügyfél birtokából.

Az elkövetők csak abban az esetben tudják megszerezni a számlához férési adatokat, ha az ügyfél megtévesztése sikeres és ő átadja a saját biztonsági adatait.

Ezen elkövetéshez köthető cselekmény, melynek során az ügyfelekkel letöltetnek egy olyan alkalmazást, mely teljes hozzáférést ad az ügyfél számítógépéhez, mobiltelefonjához, mint pl.: az Anydesk, Rustdesk, Teamviewer. Az elkövetők így át tudják venni az irányítást a megkeresett ügyféltől, a számítástechnikai eszközein tárolt adatokat így megszerezhetik és konkrét tranzakciókat kezdeményezhetnek az ügyfél gépéről, telefonjáról, ami károkozáshoz vezet.

Az elkövetők csak abban az esetben vehetik át a kontrollt az ügyfél eszközén, ha a távoli belépésre szolgáló szoftvert letelepítik, illetve erre engedélyt biztosítanak számukra.

Az adathalászat vagy más néven „phising” jellegű csalások is több féle elkövetési módszerrel történnek.

Ilyen módszer, ha a Vinted, Facebook marketplace stb. online felületen hirdetünk egy terméket, melyre a leendő vásárló üzenetváltás során felajánlja, hogy küld egy emailt Vinted, Gls, Dpd, Foxpost csomagfeladásra hivatkozva, ahol a gombra kattintva egy ilyen honlapra átnavigálja az eladót. Itt kiválasztható a számlavezető bankja, utána egy eredeti oldalhoz hasonló felületre kerül, ahol az eladó belép az „ál” netbank felületre, majd a kapott megerősítő kódok megadása után beírja a megerősítést, mellyel tulajdonképpen jóváhagyja a napi limit beállítást, utalást, illetve egyéb tranzakciókat.

Ezen bűncselekmények úgy előzhetők meg, hogy a különböző adás-vételek során csak a szükséges adatokat adjuk meg, az eladásnál ne adjunk meg többlet adatokat. Amennyiben email címet is kérnek eladásnál, ill. tovább navigálnak egy csomagküldő oldalra, már feltételezhető a csalási szándék.

Egy másik adathalász módszer, mikor különböző hirdetések jelennek meg termékekről, melyek túlzottan kecsegtető árral szerepelnek, és arra rákattintva bizonyos összeg befizetése szükséges a termék megvásárlásához.

Fontos megjegyezni, hogy előfordul olyan eset is, mikor a Posta, Nav, illetve egyéb hivatalos szervtől érkezik email, melyben valamilyen tartozás rendezésére szólítanak fel, vagy csomag érkezik. Ezen esetekben is bankkártya használattal történő összegek befizetésére hívnak fel. Az emailben rákattintva a jelzett linkre ugyancsak adathalászat áldozatai lehetünk.

A sértetté válás elkerülése érdekében ilyen esetekben mindig ellenőrizni kell a feladó email címet, ugyanis sokszor tele vannak hibákkal, nem magyaros megfogalmazásúak, ill. nem „.hu” kiterjesztésűek. Kerüljük az ilyen díjtartozások online rendezését!

Új elkövetési magatartásként értékelhető, amikor a Posta, Gls, illetve egyéb csomagküldő szolgáltató cégek nevében küldenek emailt, melyben át nem vett csomagokat lehet nagyon jutányos áron megvásárolni.

Szükséges tájékozódni a szolgáltató cégeknél, hogy van-e ilyen akciójuk, szolgáltatásuk, mielőtt utalnánk!

Jelenleg alacsonyabb számban fordulnak elő a Jófogás, illetve más aukciós portálokon hirdetett vásárlásokkal kapcsolatos csalások, melyek során előre utalásként kérik a termékek kifizetését, azonban vagy nem küldik meg azokat, vagy üres dobozt, esetleg más terméket küldenek meg.

Javasolt mindig utánvétes fizetés beállítása, ne utaljunk előre, amíg nem győződtünk meg átvételkor a csomag helyes tartalmáról. Az online webáruházak tekintetében is előfordulhatnak csalások, melyek elkerülése érdekében olyan helyről rendeljünk termékeket, amik ellenőrzöttek, megbízhatóak, a kapcsolat felvehető az áruházzal.