Ne dőljön be! – Összefogás az online csalások visszaszorítása érdekében

Napjainkban egyre gyakrabban találkozunk az online térben elkövetett csalási módszerekkel, ezért az ilyen típusú bűncselekmények visszaszorítása érdekében KiberPajzs néven közös oktatási és kommunikációs együttműködésről döntött a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet és az Országos Rendőr-főkapitányság. A programról az alapítók még 2022. november 7-én beszámoltak.

A tapasztalat azt mutatja, hogy minden törekvés ellenére növekszik az interneten elkövetett csalások száma, és a módszerek is változnak. Annak érdekében, hogy a digitális térben se váljanak áldozattá az emberek, az ORFK, a Magyar Bankszövetség és a NBSZ Nemzeti Kibervédelmi Intézet 2023. március 7-én közös sajtótájékoztatón számolt be az újabb típusú online csalásokról és az áldozattá válás megelőzésének lehetőségeiről.

Oláh-Paulon László r. alezredes, az ORFK Bűnmegelőzési Osztály vezetője elmondta, az elmúlt egy évben közel háromszorosára növekedtek az online térben elkövetett bűncselekményeknek a számai. Ki lehet jelenteni, hogy legjobb módja az áldozattáválás elkerülésének, ha megismerjük a legújabb és legelterjedtebb elkövetési módokat. Felismerjük azokat a jeleket, amik utalhatnak a rosszindulatú elkövetőkre. Ezeket megismerve nem dőlünk be ezeknek a trükköknek. A KiberPajzs programnak azért lett alapítótagja a rendőrség, mert a rendőrség egyik fő feladata a bűnmegelőzés.

A közoktatási intézményekben folytatott rendőrség biztonságra nevelő programjainak egyik meghatározó alapelemévé vált az online biztonság oktatása. De nem csak iskolákban, hanem közösségi média felületeken illetve a rendőrség saját online felületén is rendszeres figyelemfelhívó közleményeket teszünk közzé. Ilyen volt elmúlt héten rendőri vezetők nevével visszaélve megküldött adathalász e-mailek, valamit online kereskedelmi oldalon regisztrált eladók tudatos megtévesztése témakörben kiadott közlemények.

Sütő Ágnes a Magyar Bankszövetség főtitkár-helyettese kitért arra, hogy 2023. március 6-10. között zajlik a PÉNZ7 program az iskolákban, több mint 1000 iskola közel 140 ezer diákja részvételével. Az idei pénzügyi téma a „Korszerű pénzkezelés és digitális biztonság”, ami lehetővé teszi, hogy általános- és középiskolai tanórákon önkéntes szakértők bevonásával tanuljanak a diákok pénzügyi digitális alapismereteket. A Magyar Bankszövetség Digitális Szimat Kihívást hirdetett, amelyben életkortól függetlenül tehetjük próbára tesztkérdésekkel a digitális biztonsági felkészültségünket, és kipróbálhatjuk „Okosabbak vagyunk-e mint egy hacker?”.

A programban egy ismert gamer és egy etikus hacker együtt segítik a felkészülést.

Simon Edina nb. százados, az NBSZ NKI szóvivője felhívta a figyelmet arra, hogy az adathalász-támadás, bármilyen csatornán is érkezzen, valójában egyfajta pszichológiai hadviselés az online térben. A felhasználó megtévesztésével a kiberbűnözők megpróbálják rávenni az áldozatot arra, hogy személyes adatokat, érzékeny információkat adjon át számukra, vagy egy vírussal megfertőzzék a számítógépét. Amíg azonban a korábbi években a támadások kevésbé előkészítettek voltak, és jobban magukon hordozták a felismerhető jeleket, amellyel a szemfülesek át tudtak látni rajtuk, addig napjainkban a támadások komplexek és sokkal inkább célzottak, jobban kihasználják a napi aktualitások okozta realitás erejét (legyen szó akár egy bank technikai leállásáról, vagy egy online streaming szolgáltatás által bejelentett felhasználói feltétel változásáról). A naprakész tartalmú támadással pedig hihetőbb keretet adnak a csalásnak.

A veszély forrása, az ilyen jellegű támadások közös pontja, pedig a szöveges üzenetben található link. A link, amelyre kattintva vagy egy adatlap, regisztrációs felület található (ahol a megtévesztett áldozat önként megadja a bizalmas adatait), vagy egy kártékony tartalom lakozik.

A sajtótájékoztatón a szakemberek ismertették az új elkövetési módszert. „Smishing" (az angol „SMS" és „phishing", vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadó SMS segítségével próbál megszerezni személyes, pénzügyi vagy biztonsági információkat. Jellemzően egy beágyazott link van az egyébként szokványosnak tűnő üzenetben (pl. csomagod érkezett). A küldő megbízható forrásnak álcázza magát, úgy tesz, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkezne. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot a fiókja ellenőrzése, frissítése vagy újraaktiválása érdekében. A hivatkozás hamis weboldalra mutat, a telefonszámon pedig egy csaló jelentkezik, aki az adott cég munkatársának adja ki magát. Célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az áldozat pénzét.

Néhány jó tanács, hogy ne váljon online csalók áldozatává:

1. Gondolja át a kapott üzenet tartalmát. Tisztázza magában, hogy a leírtak mennyire feleltethetőek meg a valóságnak. Lehet, hogy az adott szolgáltatásnak vagy banknak nem is az ügyfele? Egy olyan szolgáltatástól kap sms-t, ahol korábban nem adta meg a telefonszámát? Nem is rendelt semmit, mégis hogyan érkezhetne csomagja?
2. Amennyiben nem tudja eldönteni egy üzenet valóságtartalmát, vegye fel a kapcsolatot a küldővel. Keresse fel például a szolgáltatója, a bankja vagy a hivatkozott csomagküldő szolgálat hivatalos honlapját, esetleg hívja fel őket a hivatalos telefonszámukon. Amennyiben egy közösségi oldalon privát üzenetet kap egy ismeretlentől? Hagyja figyelmen kívül. Azonban ha egy ismerőstől, kérdezzen vissza a linkre kattintás előtt, mit küldött Önnek az illető.
3. Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvétellel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél kilétéről. Ne adja meg illetékteleneknek személyes, pénzügyi és biztonsági adatait! Ha egy gyanús üzenet egy linket vagy egy mellékletet tartalmaz, ne kattintson rá és ne is töltse le.
4. Az esetek túlnyomó többségében az online térben működő bűnözők az emberi kíváncsiságot használják ki. Ne dőljön be egy ismeretlen feladótól kapott üzenetnek, ne akarjon csak most az egyszer kattintani, még akkor sem, ha az üzenet szerint egy videót talált Önről egy ismerőse. Egy nem várt és minden előzmény nélkül kapott linket vagy csatolmányt ne nyisson meg.
5. Amennyiben adathalász-támadás célpontjává vált, jelezze ismerőseinek, ezzel segítve az ő online biztonságukat. Nem volt elég szemfüles egy adathalász-üzenet kapcsán, és rákattintott az abban található linkre? Haladéktalanul vegye fel a kapcsolatot a számlavezető bankjával, és tegyen feljelentést a rendőrségen!
6. Ne kattintson kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!
7. Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy egy smishing üzenetre válaszolt és megadta banki adatait.

Sajtókapcsolat:

- Sütő Ágnes
- suto.agnes@bankszovetseg.hu

© Magyar Bankszövetség

© Magyar Bankszövetség

Eredeti tartalom: Magyar Bankszövetség

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/?p=1422