



BŰNMEGELŐZÉSI HÍRLEVÉL

2022. január



BOLDOG ÚJ ÉVET KÍVÁN a Komárom-Esztergom Megyei Rendőr-főkapitányság

Új év, régi problémák, új trükkök. A csalóknak mindig sikerül újabb és újabb ötletekkel előállni amikor az emberek átveréséről van szó. 2022. első hírlevelében egy új csalási módról szeretnénk hírt adni, és tanácsokkal látni el Önöket, hogy elkerülhessék az áldozattá válás t. Továbbra is legyenek óvatosak és körültekintőek az internetes vásárlások kapcsán, a telefonos banki kapcsolattartás során.

Ne adjunk esélyt a bűnözőknek!



FIGYELEM!

AZ OTP BANK NEVÉBEN TELEFONÁLÓ
EGYIK CSALÓ FELHÍVTA AZ ORFK
BŰNMEGELŐZÉSI OSZTÁLY
KIBERBIZTONSÁGI
SZAKVONALVEZETŐJÉT.



A BESZÉLGETÉS RÉSZLETEI ÉS A
BIZTONSÁGI TANÁCSOK A
BEJEGYZÉSBEN!

TELEFONOS CSALÓ

Ma reggel a +36 1 636 6666 számról hívott az OTP Bank nevében telefonáló egyik – férfi – csaló. Mivel a beszélgetés nagyon tanulságos volt, megosztjuk annak legfontosabb tapasztalatait.

„A csaló azért hívott, mert a bankkártyámmal gyanús online tranzakciót akartak végrehajtani az Alza webáruházában. A telefonhívás alatt próbált nagyon profinak tűnni, de érződött rajta, hogy nem igazi ügyfélszolgálatos. A beszélgetés közben sokszor megakadt, bizonytalan volt. A technikai, jogi, szakmai kifejezéseket rosszul használta. Ez persze nem mindenkinek tűnik fel, számomra azonban kifejezetten szórakoztató volt. Hangsúlyozta, hogy semmilyen személyes adatot nem kér, bele tudna nézni a banki anyagomba de az engedélyem nélkül nem teszi, ezzel is próbálta elnyerni a bizalmamat. Mivel mindenben nagyon együttműködőnek mutatkoztam és a feltett kérdésekre válaszoltam, javasolta, hogy egy alkalmazást telepítsek az eszközöm, hogy azzal tudjam elvégezni a kétfaktoros hitelesítést, amivel fokozhatom a biztonságot. Ez egy távoli asztal elérést biztosító program lett volna, amivel hozzáfértek volna minden, a készüléken tárolt információhoz. Ezt a kérését természetesen már nem teljesítettem.”

(orfk)



A napokban a fenti csaláson kívül egy másik módszerrel is próbálkoztak csalók: Az OTP és Takarékbank nevében is indítottak hívásokat a bankok bankkártya hátoldalán is látható telefonszámokról, és egy biztonságosabb bankkártya ígéretével kecsegtetve átutaltatott nagyobb összegeket erre a fiktív bankszámlára, több milliós kárt okozva ezzel a felhívottaknak.



Legyünk nagyon óvatosak, ha bank nevében telefonál valaki, még akkor is, ha a bank telefonszámáról kapjuk a hívást!

A beszélgetés elején kérdezzük meg, hogy kit keres, és ha nem tudja a pontos nevünket, akkor szakítsuk meg a hívást!

Semmilyen programot ne telepítsünk, még a bank nevében telefonáló személy kérésére sem!

Személyes vagy banki adatot, ideértve a bankkártya-adatokat és a bankszámla adatokat is, ne osszuk meg senkivel telefonon!

Ha valóban a bank ügyintézője telefonál, ő ismeri a szükséges adatokat!

Banki ügyintézés legbiztonságosabb formája a személyes ügyintézés!

6 TANÁCS A BIZTONSÁGOS VÁSÁRLÁSHOZ

1

Kevésbé ismert webáruház esetén ellenőrizze az üzemeltető adatait, a kapcsolattartási adatokat és a vásárlási feltételeket! Nézzon utána a webáruház értékelésének az interneten!

2

Felhasználói fiókjai védelmében minden oldalon másik jelszót használjon, továbbá kapcsolja be a kétfaktoros azonosítást, ahol lehet!

3

Rendeléskor és fizetéskor mindig ellenőrizze a böngésző címsorában, hogy valóban a megfelelő oldalra (webáruház, bank, fizetési közvetítő)!

4

Csak a rendelés teljesítéséhez szükséges személyes adatokat adja meg: név, számlázási és szállítási cím, e-mail cím, telefonszám!

5

Csak megbízható webáruházban fizessen előre bankkártyával vagy utalással! A legbiztonságosabb a személyes átvétel és fizetés.

6

Bankkártya-adatait csak banki oldalon, fizetési közvetítő oldalán vagy alkalmazásában adja meg!



INTERNET
ONLINE IS BIZTONSÁGBAN
TUDATOSAN

Országos Rendőr-főkapitányság

AZ ONLINE VÁSÁRLÁS VESZÉLYEI

(ORFK)

Az internethasználat széles körű elterjedésével egyre többen intézzük vásárlásainkat, pénzügyeinket online. A kényelmes ügyintézés azonban veszélyeket rejthet magában, ezért a kockázati tényezőkre érdemes figyelmet fordítani.

Az internetes vagy másnéven online kereskedelem mind a vásárlók, mind az eladók számára számos előnnyel jár. A potenciális vevők otthonról vásárolhatnak, lehetőségük nyílik az árak összehasonlítására, majd a megrendelést követően a futár házhoz hozza az árut. Mivel azonban a felek a legtöbb esetben nem találkoznak egymással, a vevő a fizetést megelőzően nem látja élőben a terméket és ez a helyzet kockázattal járhat, amelyet a csalók kihasználhatnak. Bár nem kell egyből a legrosszabbra gondolni, a rendelés során érdemes kellő körültekintéssel eljárni. Az internetes vásárlásnak alapvetően két fajtája van: történhet webshopokon keresztül és aukciós portálokon. A webshopokban a kereskedők jellemzően új terméket árulnak, számlával, jótállással, míg az aukciós portálokon sok esetben használt termékek szerepelnek, számla és jótállás nélkül. Ennél fogva az áruk alacsonyabb, de az ezzel járó esetleges kockázatot ajánlott szem előtt tartani.

Személyes átvétel: Az online vásárlás legnagyobb veszélye, hogy a megrendelő megkapja-e a pénzért a kiválasztott árut, illetve azt kapja-e, olyan minőségben, amit kiválasztott. A webshopokon és az aukciós portálokon keresztül történő vásárlásoknál többnyire lehetőség van a termék személyes átvételére, a helyszínen történő kifizetéssel. Ez a tranzakció legbiztonságosabb formája, hiszen a fizetés előtt alkalom nyílik az áru megtekintésére és ha az nem az elképzelésnek megfelelő, a vevő elállhat a vásárlástól. Aukciós portál esetében ennek lehetnek negatív következményei, ezért a licitálás előtt érdemes megfelelő tájékoztatást kérni a termékről, s amennyiben az nem felel meg a valóságnak, még mindig van lehetőség a visszalépésre.

Csomagküldés: A termék személyes átvétele nem minden esetben megoldható (távolság miatt, üzlet-helyiség hiányában), ilyenkor a postai út járható. A megrendelés (licitálás) előtt ajánlott tájékozódni a jótállás feltételeiről, a szállítási költségekről és a szállítás idejéről. Webshop esetében nézzük meg, hogy ki az oldal üzemeltetője. Ez lehet cég vagy magánszemély (egyéni vállalkozó), de az oldalon mindenkor fel kell tüntetni a címet, az adószámot és cégjegyzékszámot, illetve a csomagküldésre jogosító nyilvántartási számot. A webshopok és aukciós portálok használatához általában regisztráció szükséges, ilyenkor fontos a kért adatok (mint szállítási cím, e-mail, telefonszám) pontos megadása, hiszen ezek elengedhetetlenek a tranzakció sikeres lebonyolításához.

Utánvétel: Az áru kifizetése többféleképpen történhet. Az egyik az utánvétellel történő kifizetés, ilyenkor a postásnak vagy a futárnak kell fizetni. Ez általában pluszköltséget jelent a szállítási díjon felül. Ebben az esetben a csomagot szinte biztosan megkapjuk. Mindig ellenőrizzük, hogy a csomag bontatlan és ép. Ha felbontották vagy sérült, akkor ne vegyük át, hanem küldjük vissza a feladónak. Ha van rá lehetőségünk, nyissuk ki és ellenőrizzük, hogy tényleg a megrendelt árut tartalmazza.

Átutalás, bankkártya használat: Utánvétel helyett lehetőség van az áru előre történő kifizetésére. Ez történhet átutalással, ekkor kapunk egy előleghszámlát, amin a számlaszám és az átutalandó összeg szerepel. Ezt akár személyesen a bankunkban vagy az interneten keresztül is átutalhatjuk. Fizethetünk bankkártyával is, szintén az interneten keresztül. Ehhez általában dombornyomott kártyára van szükség, de vannak olyan nem dombornyomott kártyák is, amelyekkel lehet így fizetni. A bankkártyás fizetésnél meg kell adni a kártya adatait (mint bankkártya típusa, száma, tulajdonos neve, lejárat ideje és a hátoldalon található biztonsági kód). Ezen adatok illetéktelen kézbe kerülése visszaélésre adhat alkalmat, ezért praktikus eszköz az egyes bankok által kibocsátott úgynevezett virtuális kártya, amelyre a kívánt összeget a vásárlás előtt fel tudjuk tölteni és azt követően nem marad rajta pénz. A további veszélyek elkerülése érdekében lényeges, hogy csak bank által működtetett, biztonságos oldalon adjuk meg az említett adatokat. Több bank is működtet ilyet, a kereskedő döntése, hogy melyikkel köt szerződést. Az eladó ekkor nem kerül kapcsolatba az adatokkal, hanem átirányítja a potenciális vásárlókat egy bank által működtetett oldalra és a kártyaadatok ott kerülnek feldolgozásra. Mindig ellenőrizzük, hogy az oldal rendelkezik-e tanúsítvánnyal, ugyanis ennek megléte garانتálja, hogy az oldalt tényleg a bank üzemelteti, illetve, hogy a kapcsolat megfelelően titkosított (az elküldött adatok visszafejtésének elkerülése érdekében).

A bankkártya-adatokat soha ne adjuk meg e-mailben vagy más, nem banki úrlapon keresztül!

Paypal

A bankkártyán túl az elektronikus fizetésnek van más módja is. Ez az úgynevezett Paypal fizetési rendszer. A Paypal oldalán kell regisztrálni és megadni a kártyaadatokat, majd a hitelesítési folyamatot követően már használatba is vehető. A vásárlások során a Paypal fizetési módot választva a Paypal oldalára jutunk, ahol belépve jóvá tudjuk hagyni a megadott tranzakciót. Ez a vásárlók számára ingyenes. Ellenőrizzük ilyenkor is a https meglétét, hiszen elképzelhető, hogy álooldalra irányítanak, hogy megszerezzék a belépési adatokat. A paypalos fizetés a bankkártyát terheli, de annak adatait az eladó nem látja.

Az interneten történő vásárlás alkalmával mindenkor legyünk körültekintőek az alábbiak tekintetében:

ha lehet, válasszunk személyes átvételi módot;

ellenőrizzük az eladót korábbi visszajelzések, közzétett adatok alapján;

bankkártya-adatainkat csak a bank online fizetésre létrehozott oldalán adjuk meg (e-mailben soha);

ellenőrizzük, hogy a fizetésre használt oldal rendelkezik-e tanúsítvánnyal!



Segélyhívó szám: 112

Készítette: Komárom-Esztergom Megyei Rendőr-főkapitányság

Bűnügyi Osztály Bűnmegelőzési Alosztály

bunmeg@komarom.police.hu