Lakossági Tájékoztató

Tisztelt Lakosság!

A Mátészalkai Rendőrkapitányság óvatosságra inti a lakosságot az interneten terjedő nyereményjátékokkal kapcsolatban

Aki rendelkezik okostelefonnal, számítógéppel és internettel, függetlenül attól, hogy mennyi ideje is használja, jóhiszeműségéből adódóan bármikor a csalók áldozatává válhat! Az internet veszélyei közül az egyik legelterjedtebb fenyegetés, amivel minden felhasználó találkozni szokott, az a ***hamis nyereményjátékok.*** Itt a felhasználók megadják a személyes adataikat abban a hiszemben, hogy egy nyereményjátékra iratkoztak fel. Kiszolgáltatott adatainkkal könnyedén visszaélnek, és bűncselekmény áldozatává válhatunk.

Dr. Bakos Olivér r. ezredes

kapitányságvezető

A csalók sokszor nagyon egyszerű és általános módszerekkel verik át az embereket! Felhívjuk a figyelmét mindenkinek arra, hogy egyre több nyereményjáték jelenik meg az online térben. Az interneten, a közösségi oldalakon, telefonokon és egyéb applikációk segítségével, a játékot szervezők ismert, neves cégek, kereskedelmi üzletláncokra (Penny, Tesco), vállalatokra, vagy épp márkanevekre hivatkoznak, illetve arculatukat a megtévesztésig lemásolva hirdetik garantált nyereményeiket.

Ajándékjegyeket, utazást ígérnek, cserébe „csak” egy regisztrációt kérnek.

Egy egyszerű példa a **<u>Hamis ajándékjegyekkel kapcsolatos csalás tekintetében:</u>**

A csaló célja, hogy a webes platformokon kéretlen fizetős szolgáltatások igénybe vételére kényszerítse a megtévesztett felhasználót, aki abban a tudatban, hogy „online játékban” vesz részt a sorsoláson való részvétel érdekében teljesíti a feltételeket, amit részére meghatároztak.

Kérdőíveket tölt ki, megoszt, lájkol, véleményt nyilvánít, stb. Máris feltételes nyertesként sorsolták ki (kérdés csak az, hogyan lehetséges, ha nem jelentkezett?) Miután megtette a felhasználót máris átirányítják egy másik oldalra, ahol megvásárolhat bizonyos szolgáltatásokat annak érdekében, hogy megkaphassa a „feltételes nyereményét".

A regisztrációk során számos esetben személyes, vagy bizalmi adatok rögzítését, feltöltését is kérik, mint például személyi igazolvány száma, netalán fényképes igazolvány, bankkártya adatok.

Ezek az oldalak úgynevezett adathalász oldalak, és az adatok begyűjtése során nagyon rövid időn belül megszűnnek, így a rendelkezésre bocsátott adatokat a későbbiekben felügyelni nem lehet.

Áldozattá válás megelőzése érdekében kérem, fogadják el tanácsainkat:

Jótanácsok:

Mindig ellenőriznie kell a weboldalon a cég elérhetőségeit (e-mail, telefon, postai cím) FONTOS tudni, hogy a valós intézményi honlapok esetén a böngésző alsó sávján/felső címsorában szerepel a biztonságos kapcsolat meglétet jelző kis lakat ikon továbbá az ilyen oldalak elérésekor és használatakor a normál **http helyett https** védett kapcsolat épül fel az ügyfél gépe és az intézmény webszervere között.

- E-mail fogadás, olvasás során ne kattintsunk ismeretlen linkre (gyakran irányít át olyan oldalakra, vagy alkalmazásokra amelyek látszólag akár egy banki oldallal megegyezik)
- A megtévesztő szándékkal küldött e-mailek - akár magyar, akár idegen nyelvű - gyakran sürgős adatmegadásra, aktualizálásra szólítanak fel, esetleg valamilyen fenyegetést is megfogalmaznak. Minden esetben ellenőrizze a feladó címét – e nélkül sem a csatolmányra sem a hivatkozásra ne kattintson rá!
- **Legyünk mindig gyanakvóak**, ha olyan e-mailt/üzenetet kapunk, melyben arról tájékoztatnak minket, hogy az intézmény szolgáltatásaihoz használt adatainkat adjuk meg e-mailben küldött linkre kattintva vagy egy telefonszámon. Ezt sose tegyük, helyette haladéktalanul **értesítsük számlavezető szolgáltatónkat.**

A bankok sem e-mail sem telefon vonatkozásában adatokat nem kérnek, és nem is szolgáltatnak, kizárólag személyesen.

Az online visszaélésekhez a csalóknak meg kell szerezniük a kártyaszámot, a lejárati dátumot és a kártya hátoldalán szereplő biztonsági számot. Az online csalások ellen is van védelem. Több magyar banknál is lehetőség van arra, hogy kártyás vásárlást csak egy SMS-ben történő azonosítás után lehessen indítani. Ilyenkor hiába szerezték meg a kártyaadatokat, a tulajdonos telefonja nélkül nem tudnak visszaélni ezekkel. Bankkártyáját soha ne a hozzá tartozó PIN-kóddal együtt tárolja! A napi limitet, lehetőség szerint vásárlási szokásaihoz igazítsa! A tranzakciókról kérjen értesítést üzenetben, így azonnal értesül a pénzforgalomról, illetve a kártya használatának pontos helyszínéről!

Amennyiben a szolgáltató nevében megtévesztő módon érkezett e-mailre/üzenetre már megadtuk azonosítónkat, jelszonkat, mihamarabb tiltassuk le azokat, és kérjünk információt pénzügyi intézményünktől.
Ha a bankkártyája elveszett, ellopták, illetve bármilyen módon kikerült ellenőrzése alól, vagy ha az adataival visszaélve fizettek azonnal tiltassa le a banknál!

- LEGYEN gyanús, ha magyar nyelvű oldalról idegen nyelven próbálnak velünk kommunikálni

- A magyar telefonszolgáltatók SMS üzenetei is keltsenek bennünk gyanút, ha az idegen nyelven érkezik a szöveg
- Mindig vizsgáljuk meg a telefonszámot mielőtt visszahívnánk! : a telefonszám legelején, a + jel után látható szám (például +256) az előhívó, ez mutatja meg, hogy milyen országból hívtak minket amelyben rákeresve rögtön kideríthetjük, hogy a +256-as előhívóról érkező hívás valójában melyik országból érkezett
- Ne adja ki a belépési adatait. Még akkor se, ha úgy tűnik, hogy ezt maga a szolgáltató követeli. A távközlési cégek ugyanis nem szokták elkérni egyetlen ügyfél belépési azonosítóját és jelszavát sem.
- **Valótlan nyereményjáték a trükkös** csaló a telefontársaság munkatársának nevében, ***hívószámkijelzés*** nélkül hívja fel az ügyfelet, hogy nyert valamit, majd ***az örömhír közlése után hozzáteszi:***

nyereményét csak akkor tudja átvenni, ha „a technikai költségeinek fedezéséhez” egy kisebb/nagyobb összeget tölt fel egy adott telefonszámra.

Nyeremények miatt ne tölts fel egyenleget, ne végezz banki tranzakciókat (hiszen a nyereményjátékoknál nem szokás ilyen feltételeket szabni). Ne faxoljon, scannelje, diktáljon be adatokat kedvező ígéretek miatt! Járjon utána, hívja, fel a céget mielőtt kiszolgáltatja adatait, hiszen előfordulhat, hogy adatainak birtokában az Ön terhére vásárol a csaló okostelefont.

- Állítsunk be spam szűrőt, védjük eszközeinket tűzfallal.
- Használjon erős jelszót, melyet legalább 2 havonta változtasson meg (az erős jelszó legalább 7 karakter, kis és nagybetűket, valamint számokat is tartalmaz).

Fontos a tudatosság és az óvatosság! Minél informáltabb valaki egy témában annál nehezebb megtéveszteni, megvezetni, netalán becsapni.

Az online csalás formái rendkívül változatosak. Fellelhető a nyereményjáték, ingyenes menetjegyek, lottó nyeremény, távoli rokontól érkező örökség, és sorolhatnánk a végtelenségig.

A lényeg ugyanakkor a készpénz, bankszámlaadatok, az online hozzáféréshez szükséges adatok (belépési kódok, jelszavak,PIN – kódok megszerzése.

Amennyiben trükkös csalók próbálkoznak az Ön megtévesztésével, vagy áldozatául esik, azonnal értesítse a rendőrséget a 112-es ingyenesen hívható segélyhívó számon, vagy tegyen bejelentést bármely rendőrnél, vagy rendőri szervnél!

Elérhetőségeink:

Cím: 4700 Mátészalka, József A. u. 1-3, Posta cím: 4701 Mátészalka Pf.: 40.

Telefon: 44/312-033., Fax: 44/312-033.,

E-mail: mateszalkark@szabolcs.police.hu