

**ÖNTEVÉKENY CIVIL ÖSSZEFOGÁS
MECSEKSZABOLCSÉRT EGYESÜLET**

Közbiztonság, vagyonvédelem Pécs-keleten

Idősekre leselkedő veszély a digitális térben



Kedves Olvasó

Impresszum

A digitális világ veszélyei – Miért fontos az óvatosság?

Az internet és a digitális világ rengeteg előnyt kínál, legyen szó kapcsolattartásról, vásárlásról, ügyintézésről vagy szórakozásról. Azonban ezekkel a lehetőségekkel együtt jelentős veszélyek is megjelentek. Az idősebb korosztály – akik kevésbé ismerik a technológiai trükköket és sokszor jóhiszeműen közelítenek a digitális eszközökhöz – különösen sebezhető célpontjai lehetnek az online csalóknak.

Az internetes csalások leggyakoribb célja, hogy pénzt, személyes adatokat vagy érzékeny információkat szerezzenek a gyanútlan áldozatoktól. Az adathalásztattól kezdve a hamis nyereményjátékokon át egészen a zsarolóprogramokig a csalások számos formát ölthetnek, de mindegyik közös vonása, hogy a bizalmat és a figyelmetlenséget használják ki.

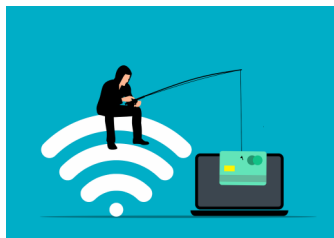
Az idősebbek gyakran kevésbé jártasak az online biztonság területén, ezért könnyebben bedőlhetnek a csalók által alkalmazott módszereknek. Gyakori példák erre a hamis banki értesítések, amelyek sürgős adatmegadást kérnek, vagy a megható történetekkel operáló álnok „jótékonyági” kampányok. Más esetekben hamis technikai segítségnyújtás ürügyén próbálnak hozzáférni az áldozat számítógépéhez, banki adatainak megszerzéséhez vagy személyes információihoz.

A csalók a technológia mellett az emberi természet gyengeségeit is kihasználják. Sok esetben az áldozatok félelmét, jóindulatát vagy tapasztalatlanságát veszik célba. Például egy e-mail, amely azt állítja, hogy a számítógépen vírus van, azonnali reakciót válthat ki, és egy gyanútlan felhasználó könnyen követheti az utasításokat anélkül, hogy ellenőrizné azok hitelességét.

A digitális világ veszélyei elleni védekezés alapja a tudatosság. Ismernünk kell a tipikus csalási módszereket, hogy felismerhessük őket, és mindig legyünk óvatosak, amikor személyes adataink vagy pénzünk forog kockán. A csalók törekvéseivel szemben a legjobb fegyverünk a biztonságtudatos viselkedés: gondolkodjunk, mielőtt kattintunk, és ha valami túl szép ahhoz, hogy igaz legyen, akkor valószínűleg nem is az.

Fontos, hogy mindig gyanakvóan kezeljük a váratlan üzeneteket, ajánlatokat és kéréseket. A tudás és a megelőzés kulcsszerepet játszanak abban, hogy elkerüljük a digitális világ csapdait, és biztonságban használhassuk az internet adta lehetőségeket.

Adathalászat: Hogyan védhetjük meg személyes adatainkat?



Az adathalászat (angolul phishing) az online csalók egyik leggyakoribb módszere, amely során megtévesztő üzenetekkel vagy weboldalakkal próbálnak meg személyes adatokat, például jelszavakat, bankkártyaadatokat vagy más érzékeny információkat megszerezni. Az ilyen adatok birtokában a csalók pénzügyi visszaéléseket követhetnek el, hozzáférhetnek online fiókjainkhoz, vagy akár teljesen eltulajdoníthatják személyazonosságunkat. Az idősek, akik kevésbé jártasak az online biztonsági intézkedésekben, különösen veszélyeztetettek lehetnek.

Hogyan működik az adathalászat?

Az adathalász támadások jellemzően e-mailben, SMS-ben vagy közösségi média üzenetben érkeznek, és sürgős cselekvésre buzdítanak. A csalók gyakran úgy tesznek, mintha egy megbízható szervezet, például egy bank, közüzemi szolgáltató, népszerű online áruház vagy akár egy állami szerv képviselői lennének. Az üzenetek azt állíthatják, hogy:

- Szokatlan tevékenységet észleltek a fiókunkban.
- Azonnal frissíteni kell az adatainkat, különben zárolják a fiókunkat.
- Nyereményt nyertünk, amelynek átvételéhez csak néhány adatot kell megadnunk.

Az üzenetek gyakran tartalmaznak egy linket, amely egy hamis weboldalra vezet, amely külsőre megtévesztően hasonlít az eredeti, ismert weboldalra. Amint a gyanútlan áldozat itt megadja az adatait, azok azonnal a csalók kezébe kerülnek.

Hogyan ismerhetjük fel az adathalász kísérleteket?

- **Sürgető hangnem és fenyegetések** A csalók az idő sürgetésével próbálnak pánikot kelteni, például azzal, hogy ha nem cselekszünk azonnal, elveszíthetjük a fiókunkat vagy a pénzünket. Az ilyen nyomásgyakorlás gyakori jele annak, hogy csalással van dolgunk.
- **Gyanús e-mail-címek és linkek** A csalók általában olyan feladónévet használnak, amely megtévesztően hasonlít egy ismert cég nevére, de az e-mail-címük már gyanús lehet (például info@bank-neve.com helyett info@bankneve-security.com). A linkek mögötti címetek mindig érdemes ellenőrizni, mielőtt rákattintunk.

- **Hibás fogalmazás vagy szokatlan stílus.** Az adathalász üzenetek gyakran tartalmaznak nyelvtani hibákat, furcsa szóhasználatot vagy olyan kifejezéseket, amelyeket egy valódi cég sosem alkalmazna.
- **Kérések bizalmas információk megadására.** Egyetlen hiteles szervezet sem fog e-mailben vagy üzenetben kérni jelszavakat, bankkártyaadatokat vagy más érzékeny információkat.

Hogyan védekezhetünk az adathalászzal szemben?

- **Soha ne adjunk meg érzékeny adatokat üzenetben!** Ha valaki ilyet kér, különösen egy váratlan üzenetben, mindig legyünk gyanakvók. Ellenőrizzük az üzenet hitelességét az adott szervezet hivatalos ügyfélszolgálatán.
- **Legyünk óvatosak a linkekkel és csatolmányokkal!** Egy link kattintás előtt vigyünk főle az egérkurzort, hogy megnézzük, hova vezet. Ha a cím gyanús, ne kattintsunk rá! Ismeretlen feladótól érkező csatolmányokat pedig soha ne nyissunk meg.
- **Frissítsük rendszeresen az eszközeinket és használjunk vírusirtót!** Az operációs rendszer és a böngészők frissítése segít a biztonsági rések megszüntetésében. Egy megbízható vírusirtó program képes felismerni és blokkolni az adathalász oldalakat.
- **Kétlépcsős azonosítás használata.** Az olyan extra biztonsági intézkedések, mint a kétlépcsős azonosítás, megnehezítik, hogy a csallók hozzáférjenek fiókjainkhoz még akkor is, ha megszerezték jelszavainkat.
- **Tanuljunk a figyelmeztető jelekről!** Ismerjük meg a gyakori adathalász módszereket, hogy időben felismerhessük azokat.

Mit tegyünk, ha adathalász áldozatává váltunk?

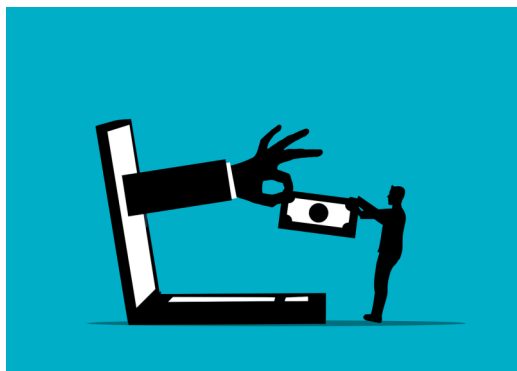


Ha úgy érezzük, hogy gyanús üzenetre válaszoltunk vagy megadtuk az adatainkat, azonnal változtassuk meg a fiókunk jelszavát, és értesítsük az érintett szervezetet. Banki adatok esetén azonnal lépünk kapcsolatba bankunkkal, és jelezzük a problémát. Továbbá tegyünk bejelentést az illetékes hatóságoknál,

hogy másokat is figyelmeztethessenek a csallók tevékenységére.

Az adathalászat elleni védekezés kulcsa a tudatosság és az óvatosság. Ha odafigyelünk a részletekre és követjük a biztonsági javaslatokat, jelentősen csökkenthetjük az áldozattá válás kockázatát.

Hamis ajánlatok és nyereményjátékok az interneten



Az interneten gyakran találkozhatunk olyan ajánlatokkal vagy nyereményjátékokkal, amelyek túl szépnek tűnnek ahhoz, hogy igazak legyenek - és általában nem is azok. Ezek a hamis promóciók az emberek kíváncsiságát, kapzsiságát vagy jóhiszeműségét használják ki, hogy pénzt vagy személyes adatokat csaljanak ki tőlük. Az idők különösen

kiszolgáltatottak lehetnek, mivel gyakran kevésbé ismerik az ilyen csalások működését.

Hogyan ismerhetjük fel a hamis ajánlatokat és nyereményjátékokat?

Túl szép, hogy igaz legyen

- Az olyan ígéretek, mint „Garantált nyeremény!”, „Milliós nyeremény egy kattintással!” vagy „Küldje el adatait, és máris az Öné egy új autó!”, szinte mindig csalások. A valódi nyereményjátékoknál általában világos szabályok és részletek vannak, nem pedig hihetetlenül könnyű nyerési lehetőség.

Váratlan üzenetek és ajánlatok

- Ha olyan nyereményről vagy lehetőségről kapunk értesítést, amelyért nem is jelentkeztünk, szinte biztos, hogy csalásról van szó. Senki sem nyerhet úgy, hogy nem vett részt semmilyen játékban.

Azonnali adatmegadási vagy fizetési kérések

- A hamis ajánlatok és nyereményjátékok gyakran azzal kezdődnek, hogy azonnal meg kell adnunk személyes adatainkat (például név, lakcím, telefonszám) vagy pénzt kell utalnunk „adminisztrációs költség” vagy „szállítási díj” címén. Ez egyértelmű jele annak, hogy csalásról van szó.

Gyanús weboldalak és linkek

- A csalók gyakran hamis weboldalakat hoznak létre, amelyek hasonlítanak egy ismert cég oldalára. Ezek az oldalak azonban általában rossz minőségűek, tele vannak helyesírási hibákkal, és az URL-jük is eltér az eredetitől (például www.ceg-neve.hu helyett www.cegneve-winner.com).

Milyen veszélyeket rejtene ez az átverés?

A hamis nyereményjátékoknak és ajánlatoknak sok kockázata van. A csalók:

- **Pénzügyi kárt okozhatnak**, ha például bankkártyaadatokat szereznek meg, vagy arra készítetnek, hogy pénzt utaljunk nekik.
- **Személyes adatainkkal visszaélhetnek**, például más csalásokhoz használhatják azokat.

Kártevő programokat telepíthetnek az eszközeinkre, ha kattintunk a hamis oldalakra vagy letöltünk egy csatolmányt.

Hogyan védekezhetünk?

Mindig legyünk skeptikusak az irreális ajánlatokkal szemben!

- Ha valami túl jó ahhoz, hogy igaz legyen, valószínűleg nem is igaz.

Ellenőrizzük az ajánlat forrását!

- Ha egy ismert cég nevében érkezik az ajánlat, keressük fel a cég hivatalos weboldalát, vagy kérdezzük meg az ügyfélszolgálatot, hogy valódi-e a promóció.

Soha ne adjunk meg személyes adatokat vagy bankkártyainformációkat ismeretlen weboldalon!

- Egy megbízható nyereményjáték nem kér banki adatokat az igényléshez.

Kerüljük a gyanús linkekre való kattintást!

- Ha egy e-mailben vagy üzenetben található link furcsának tűnik, ne kattintsunk rá.

Használjunk biztonsági szoftvereket!

- Az antivírus és az anti-phishing programok segítenek kiszűrni a gyanús weboldalakat és tartalmakat.

Mit tegyünk, ha áldozatává váltunk?

Ha úgy érezzük, hogy egy hamis nyereményjáték vagy ajánlat csapdájába estünk:

- Azonnal értesítsük bankunkat, ha pénzügyi adatainkat adtuk meg.
- Jelentsük a csalást a rendőrségnek vagy a fogyasztóvédelmi hatóságnak.
- Ha gyanús weboldalra léptünk be, ellenőrizzük eszközünket vírusirtóval, hogy eltávolítsuk az esetleges kártevőket.

A hamis ajánlatok és nyereményjátékok elleni védekezés kulcsa az óvatosság és a tudatosság. Ne hagyjuk, hogy a csalók jóhiszeműségünket kihasználják, és mindig gondolkodjunk, mielőtt cselekszünk!

Hamis telefonhívások: Az úgynevezett „unokázós csalás”

A telefonos csalások az egyik legelterjedtebb módszert jelentik, amellyel csalók idősebb embereket próbálnak megtéveszteni. Az áldozatok jóhiszeműségét és segítőkészségét kihasználva a csalók jelentős anyagi károkat okozhatnak. Az egyik legismertebb és sajnos gyakori módszer az „unokázós csalás”, amely során a csalók az áldozat hozzátartozójának adják ki magukat. Emellett számos más telefonos átverés is létezik, amelyek célja a pénzszerzés vagy az érzékeny információk megszerzése.



Az „unokázós csalás” működése:

Ebben a csalási formában a csalók általában egy idős embernek telefonálnak, és azt állítják, hogy az unokája vagy más közeli hozzátartozója bajba került. Az ürügyek változatosak lehetnek:

- Balesetet szenvedett, és sürgősen pénzre van szüksége a kórházi kezeléshez.
- Rendőrségi ügybe keveredett, és óvadékra van szükség.
- Külföldön tartózkodik, és ellopták az iratait vagy pénzét.

A csalók gyakran érzelmi nyomást gyakorolnak az áldozatra, és időhiányra hivatkozva sürgetik, hogy adjon át pénzt egy „megbízottnak”, aki elmegy érte. Az idős emberek jóhiszeműségét és családjuk iránti felelősségérzetét kihasználva gyakran sikerrel járnak.

Egyéb telefonos csalási módszerek

Hamis szolgáltatók vagy hatóságok

- A csalók közüzemi szolgáltatók, banki alkalmazottak vagy hatóságok képviselőinek adják ki magukat, és azt állítják, hogy az áldozatnak elmaradása van, vagy gyanús tevékenységet észleltek a számláján. Azonnali intézkedést sürgetnek, például egy bizonyos összeg átutalását vagy személyes adatok megadását kéri.

Nyereményjátékok és ajándékok

- A hívók azt állítják, hogy az áldozat nyert egy értékes díjat (például autót vagy pénzt), de annak átvételéhez előbb „adminisztrációs díjat” kell fizetni.

Technikai támogatás csalások

- A csalók azt állítják, hogy egy ismert cég (például egy szoftvergyártó vagy internetszolgáltató) ügyfélszolgálatáról hívnak, és azt mondják, hogy az áldozat eszközén biztonsági problémát találtak. A probléma „megoldásához” pénzt vagy távoli hozzáférést kérnek az eszközhöz.

Hogyan védekezhetünk?

Ne cselekedjünk azonnal érzelmi nyomásra!

- Ha egy hívás sürgető vagy nyomást gyakorol ránk, maradjunk higgadtak. Tegyük fel kérdéseket, és próbáljuk ellenőrizni a történetet.

Ellenőrizzük a történet hitelességét!

- Az „unokázós csalás” esetén hívjuk fel az érintett hozzátartozót egy másik telefonon, hogy megerősítsük, valóban ő van-e bajban.

Ne adjunk ki érzékeny adatokat telefonon!

- Egyetlen bank, szolgáltató vagy hatóság sem kér jelszavakat, PIN-kódokat vagy banki adatokat telefonon.

Ne utaljunk pénzt ismeretleneknek!

- Ha egy hívás során pénzátdásról van szó, mindig gyanakodjunk. Kérjünk időt az ügy átgondolására, és beszéljük meg családtagokkal.

Jegyezzük meg a telefonszámot és tegyünk bejelentést!

- Ha gyanús hívást kapunk, jegyezzük fel a hívó számát, és jelentsük a rendőrségnek vagy a helyi hatóságoknak.

Mit tegyünk, ha áldozattá váltunk?

Ha úgy érezzük, hogy telefonos csalók csaptak be:

- Azonnal értesítsük a rendőrséget, és tegyünk bejelentést.
- Ha pénzt adtunk át, próbáljuk megakadályozni az átutalást vagy a készpénz átadását, és értesítsük bankunkat.
- Hívjuk fel hozzátartozóinkat, hogy figyelmeztessük őket a csalók módszereire.

A telefonos csalások elleni védekezés kulcsa a tudatosság és a gyanakvás. Ha időben felismerjük a jeleket, megelőzhetjük, hogy csalók áldozataivá váljunk.

Biztonságos online vásárlás lépései



Az online vásárlás kényelmes, gyors és egyszerű, azonban számos veszélyt is rejthet. A csalók egyre kifinomultabb módszereket alkalmaznak, hogy pénzt vagy személyes adatokat csaljanak ki az interneten vásárlóktól. Ahhoz, hogy elkerüljük a kellemetlen meglepetéseket, érdemes körültekintően eljárni, és betartani néhány alapvető biztonsági lépést.

Vásárlás előtt: Mit érdemes ellenőrizni?

A weboldal hitelessége

- **Biztonságos kapcsolat:** Az oldal URL-jének *https://*-szel kell kezdődnie, és a böngészőben meg kell jelennie egy lakat ikonnak. Ezek a biztonságos adatátvitel jelei. Gyanús, ha a weboldal címe hibásan írt, furcsa kiegészítéseket tartalmaz, például *"-cheap"* vagy *"-deal"*.
- **Elérhetőségek és impresszum:** Egy megbízható áruház feltünteti a cég nevét, címét és kapcsolatfelvételi adatait. Ha ezek hiányoznak, az oldal gyanús lehet.

Vásárlói vélemények és hírnév

- Nézzünk utána a webáruház értékeléseinek független oldalakon vagy fórumokon. Ha az oldalról kevés információ érhető el, vagy sok a negatív visszajelzés, érdemes elkerülni.

Árak és akciók reális volta

- A túlzottan kedvező árak vagy irreális akciók gyakran figyelemfelkeltő trükkök a csalók részéről. Ha egy ajánlat túl szép ahhoz, hogy igaz legyen, valószínűleg nem megbízható.

Fizetési módok és adatvédelem

- Csak biztonságos fizetési módokat válasszunk, például bankkártyát vagy megbízható online szolgáltatásokat, mint a PayPal. Kerüljük azokat az oldalakat, amelyek kizárólag előre utalást fogadnak el.

Vásárlás közben: Mire figyeljünk?

Rendelési adatok ellenőrzése

- Győződjünk meg róla, hogy minden adat pontosan szerepel, és nincsenek rejtett költségek vagy díjak a végösszegben.

Adataink védelme

- Csak a vásárláshoz szükséges adatokat adjuk meg. Gyanús, ha egy webáruház felesleges információkat kér, például személyi igazolvány számot.

Visszaigazolás

- Egy megbízható webáruház azonnal küld e-mailben visszaigazolást, amely tartalmazza a vásárlás részleteit. Ha ez elmarad, érdemes gyanakodni.

Vásárlás után: Mi a teendő?

Csomag követése

- A legtöbb megbízható áruház lehetőséget biztosít a rendelés nyomon követésére. Ha ez nem elérhető, vagy a szállítás indokolatlanul késik, keressük fel az ügyfélszolgálatot.

Bankszámla ellenőrzése

- Vásárlás után figyeljük a bankszámlakivonatunkat, hogy csak a megrendelt összeg került-e levonásra. Ha gyanús tranzakciót észlelünk, azonnal értesítjük a bankot.

Reklamáció és visszaküldés

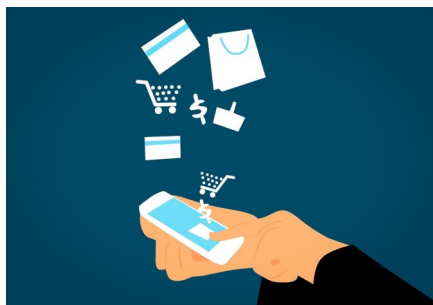
- Ha a termék hibás, vagy nem felel meg a leírásnak, élhetünk az elállási jogunkkal. Ellenőrizzük a webáruház visszaküldési szabályzatát.

Mit tegyünk, ha csalás áldozatává válunk?

- Azonnal értesítjük a bankunkat, hogy zárolják a kártyánkat, és próbáljuk visszahívni a tranzakciót.
- Jelentsük az esetet a rendőrségen vagy a fogyasztóvédelmi hatóságnál.

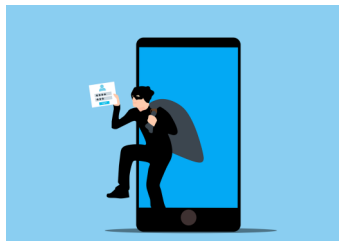
Osszuk meg tapasztalatainkat, hogy másokat figyelmeztessünk az adott oldal veszélyeire.

Összegzés



Az online vásárlás biztonságossága leginkább a tudatosságon múlik. A megbízható webáruházak kiválasztásával, reális ajánlatok keresésével és biztonságos fizetési módok alkalmazásával elkerülhetjük a csalásokat, és élvezhetjük az internetes vásárlás előnyeit.

Banki csalások és megtévesztések az interneten



Az online bankolás kényelme ma már sokak számára elengedhetetlen, azonban a digitális világ veszélyeket is rejt. Az online banki csalások az adatok ellopására és pénzügyi kártételre irányulnak, és a csálók egyre kifinomultabb technikákkal próbálják megtéveszteni az embereket.

Gyakori banki csalási módszerek

Hamis banki üzenetek és értesítések: A csálók gyakran küldenek e-maileket vagy SMS-eket, amelyek első ránézésre hivatalos banki értesítésnek tűnnek. Az üzenetek gyakran sürgős cselekvésre szólítanak fel, például "fiókja zárolásra kerülhet, ha nem lép be azonnal". Az üzenetekben található linkek azonban hamis weboldalra vezetnek, ahol a felhasználótól bizalmas adatokat kérnek.

Adathalászat (phishing) Az adathalász támadások célja, hogy megtévezzék az áldozatot, és megszerezzék banki belépési adatait, jelszavait vagy bankkártya-információit. Ez történhet e-maileken, hamis weboldalakon vagy akár telefonhívásokon keresztül.

Malware és kémprogramok Az interneten terjedő kártékony programok (malware) észrevétlenül települnek a felhasználók eszközeire. Ezek a programok képesek a billentyűleütések rögzítésére, képernyőfelvételek készítésére, vagy akár a banki belépési adatok eltulajdonítására.

Technikai segítségnyújtási csalások A csálók telefonon vagy e-mailben technikai támogatást színlelve próbálnak hozzáférni az eszközökhöz. A "segítségnyújtás" keretében a felhasználót ráveszik, hogy telepítsen egy programot, amivel távolról irányíthatják az eszközt, és hozzáférhetnek a banki információkhoz.

Banki mobilalkalmazások hamisítása Egyes csálók hamis banki alkalmazásokat hoznak létre, amelyeket letöltve a felhasználók önként adják meg adataikat.

Védekezési stratégiák

Hitelesség ellenőrzése

- Soha ne kattintsunk közvetlenül e-mailekben vagy SMS-ekben található linkekre. Mindig kézzel írjuk be a bank hivatalos weboldalának címét a böngészőbe.

- Ellenőrizzük az üzenetek küldőjét: gyanús e-mail címek vagy szokatlan telefonszámok intő jelek lehetnek.

Erős védelem használata

- Aktiváljuk a kétfaktoros azonosítást (2FA), amely további védelmet nyújt a belépési adatok mellett.
- Telepítsünk megbízható vírusirtót, és rendszeresen frissítsük azt.

Óvatos adatkezelés

- Soha ne osszunk meg bizalmas adatokat e-mailben, SMS-ben vagy telefonon, még akkor sem, ha a küldő látszólag banki dolgozónak tűnik.
- Ha gyanús telefonhívást kapunk, mindig ellenőrizzük a bank hivatalos ügyfélszolgálatán keresztül az információ hitelességét.

Nyilvános hálózatok kerülése

- Ne végezzünk banki tranzakciókat nyilvános Wi-Fi-hálózatokon. Ha elkerülhetetlen, használjunk virtuális magánhálózatot (VPN).

Számlakivonatok figyelése

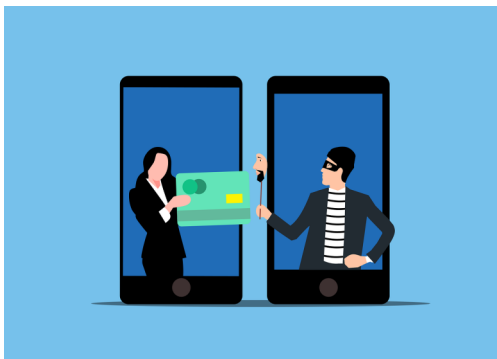
- Rendszeresen ellenőrizzük bankszámlánk forgalmát, hogy időben észlelhessük a gyanús tranzakciókat.

Mit tegyünk, ha áldozatokká válunk?

- Azonnal lépünk kapcsolatba a bankunkkal, és kérjük számlazárolást vagy kártyacsere szolgáltatást.
- Jelentsük az esetet a rendőrségen és a Nemzeti Kibervédelmi Intézetnél. Futtassunk átfogó víruskeresést az eszközeinken, és szükség esetén állítsuk vissza azok gyári beállításait.

Összegzés

A banki csalások és megtévesztések kivédésének kulcsa a tudatos magatartás. Ha óvatosan kezeljük a banki értesítéseket, csak hivatalos csatornákat használunk, és erős védelmi rendszereket alkalmazunk, minimalizálhatjuk annak esélyét, hogy áldozattá váljunk. Az elővigyázatosság nemcsak pénzügyi, hanem személyes adataink biztonságát is garantálja.



A kiadvány létrejöttét támogatta:

Pécs Megye Jogú Város Önkormányzata



További támogatóink:



MINISZTERELNÖKSÉG



**Nemzeti
Együttműködési
Alap**

