PÁRBESZÉD

Civil Érték Szövetség CIVILÉSZ

JÓ SZOLGÁLAT
EGÉSZSÉG
KULTÚRA
KÖRNYEZETTUDAT
BIZTONSÁG

Adathalászat
Hogyan védekezzünk?
Hamis ajánlatok…
Vegyük észre!
Telefonos csalók
Gondolkodjunk!
Bevásárlás a neten
Csak óvatosan…
Banki átverések
Párkeresés
Csak lassan…
E-mail
Veszélyes lehet!

Közbiztonság, vagyonvédelem Pécs-keleten

Idősek az online térben!

K e d v e s O l v a s ó !

Abban a reményben ad ki az egyesület három időszaki kiadványt közbiztonsági témakörben, hogy az idősebb korosztályt segítse a biztonságot érintő információk közreadásával. Az áldozattá válás elkerülésére, csalások felismerésére, vagyon elleni bűncselekmények megakadályozására, valamint az egyesület által végzett közbiztonsági tevékenységek bemutatására szolgáló kiadványok széles körben kerülnek kiosztásra. Az internet segítségével tovább növekszik az információval elérhető személyek száma. Fontos lenne, hogy a Tisztelt Olvasó megszavazza számunkra a bizalmat, hogy időt szán a kiadványban megjelenő információk befogadására, önnön biztonsága érdekében. Pécs keleti városrészében, ahol az egyesület végzi tevékenységét, magas a hátrányos helyzetben élők és a szenior korúak száma, ezért a szervezet kiemelt figyelmet fordít biztonságuk megerősítésére. Arra szeretnénk motiválni Önöket, hogy a kiadványokban megjelenített SZEM - Szomszédok Egymásért Mozgalom – értékrendjét követve legyenek SZEM-esek, figyeljenek oda szomszédaikra is, hiszen akkor várható a viszont segítség, ha a társadalom maga is nyitott a segítségnyújtásra. Cikkeinkhez kiváló alapot nyújtott a Magyar Rendőrség honlapja, valamint online vagyonvédelmi oldalak.

A kiadványban szereplő illusztrációk a https://pixabay.com oldalról származnak!

Érdemes lapszámainkat figyelmesen átböngészni, mert az itt közreadott információk által elkerülhető a sértetté válás lehetősége.

Jó szórakozást kívánunk!

I m p r e s s z u m

Időszakos kiadvány. 2024. IV. negyedév, I. évfolyam 2. szám. ISSN 1217-8594.
Az **Pécs Megye Jogú Város Önkormányzat** támogatásában, az
ÖCÖM **Öntevékeny Civil Összefogás Mecsekszabolcsért Egyesület** gondozásában.
Kiadja: a **Pécs-Baranyai Origó-Ház Egyesület, Párbeszéd Kiadója**,
7629 Pécs, Komlói út. 94-98. Tel.:72/238-888, 06-20/923-8888 E-mail:
origo@origo-haz.hu
Főszerkesztő: Kis Varga István, **Design:** Palotás Károly, **Lektor:** Kis Varga István
Szerkesztők: Palotás Károly, Sziva Gyula, Várkonyi Judit
Tördelés: REED Soft Bt.

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 adathalászattól 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 „jótékonysági” 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 csapdáit, és biztonságban használhassuk az internet adta lehetőségeket.

Adathalász csalások a digitális térben – Útmutató Időseknek

Az internet számos előnyt kínál, de sajnos veszélyeket is rejt magában. Az egyik leggyakoribb online fenyegetés az adathalászat, amely során a csalók megtévesztő módszerekkel próbálnak meg személyes adatokat megszerezni. Az idősek különösen sebezhetőek lehetnek ezekkel a támadásokkal szemben, ezért fontos, hogy tisztában legyünk a leggyakoribb adathalász módszerekkel és a védekezési lehetőségekkel.

Mi az adathalászat?

Az adathalászat olyan csalási módszer, amely során a bűnözők megtévesztő üzenetekkel próbálnak meg személyes adatokat, például jelszavakat, bankkártya adatokat vagy egyéb érzékeny információkat megszerezni. Ezek az üzenetek gyakran e-mailben, SMS-ben vagy közösségi média platformokon keresztül érkeznek.

Leggyakoribb adathalász módszerek:

Hamis e-mailek és weboldalak: A csalók gyakran küldenek olyan e-maileket, amelyek látszólag megbízható forrásból, például bankoktól vagy ismert szolgáltatóktól érkeznek. Az e-mailekben található linkek hamis weboldalakra vezetnek, ahol az áldozatokat arra kérik, hogy adják meg személyes adataikat.

Telefonos csalások (vishing): Ebben az esetben a csalók telefonon keresztül próbálnak meg adatokat szerezni. Gyakran banki alkalmazottnak adják ki magukat, és azt állítják, hogy sürgős adatellenőrzésre van szükség.

SMS csalások (smishing): Az SMS-ben érkező adathalász üzenetek hasonlóak az e-mailekhez. Az üzenetek gyakran tartalmaznak linkeket, amelyek hamis weboldalakra vezetnek, vagy arra kérik az áldozatokat, hogy válaszoljanak az üzenetre személyes adataikkal.

Közösségi média csalások: A csalók gyakran használják a közösségi média platformokat is, hogy megtévesztő üzeneteket küldjenek. Ezek az üzenetek lehetnek nyereményjátékok, hamis állásajánlatok vagy egyéb vonzó ajánlatok, amelyek célja az adatok megszerzése.

Hogyan védekezhetünk az adathalászat ellen?

Legyünk óvatosak az e-mailekkel és üzenetekkel: Soha ne kattintsunk gyanús linkekre, és ne adjuk meg személyes adatainkat ismeretlen forrásoknak. Ha egy üzenet gyanúsnak tűnik, ellenőrizzük a feladót, és keressük fel közvetlenül a hivatalos weboldalt vagy ügyfélszolgálatot.

Használjunk erős jelszavakat: Az erős jelszavak használata és a rendszeres jelszócsere segíthet megvédeni fiókjainkat. Kerüljük az egyszerű, könnyen kitalálható jelszavakat.

Telepítsünk biztonsági szoftvereket: A vírusirtó és egyéb biztonsági szoftverek használata segíthet felismerni és blokkolni a kártékony üzeneteket és weboldalakat.

Legyünk óvatosak a közösségi médiában: Ne osszunk meg túl sok személyes információt a közösségi média platformokon, és figyeljünk arra, hogy csak megbízható ismerősöket fogadjunk el.

Rendszeres ellenőrzés: Rendszeresen ellenőrizzük banki és egyéb online fiókjainkat, hogy időben észleljük a gyanús tevékenységeket.

Mit tegyünk, ha adathalászat áldozatai lettünk?

Azonnali lépések: Ha úgy gondoljuk, hogy adathalászat áldozatai lettünk, azonnal változtassuk meg az érintett fiókok jelszavait, és értesítsük a szolgáltatót vagy a bankot.

Jelentés a hatóságoknak: Jelentsük az esetet a rendőrségnek vagy a megfelelő hatóságnak. Magyarországon a rendőrség hivatalos honlapján találhatunk információkat és segítséget.

Figyelmeztessük ismerőseinket: Osszuk meg tapasztalatainkat ismerősein kel, hogy ők is tisztában legyenek a veszélyekkel és elkerüljék azokat.

Összegzés

Az adathalászat komoly veszélyt jelent az online térben, különösen az idősek számára. Azonban megfelelő óvintézkedésekkel és tudatossággal jelentősen csökkenthetjük a kockázatokat. Legyünk mindig óvatosak, és ne adjuk meg személyes adatainkat ismeretlen forrásoknak. Ha gyanús üzenetet kapunk, mindig ellenőrizzük a feladót, és kerüljük a gyanús linkekre való kattintást. Ezzel megvédhetjük magunkat és adatainkat a csalóktól.

Hamis ajánlatok és nyereményjátékok az interneten

Az internetes csalások folyamatosan fejlődnek, és a csalók egyre kifinomultabb módszereket alkalmaznak. A hamis ajánlatok és nyereményjátékok különösen veszélyesek, mivel a megtévesztés hatására az áldozatok önként osztanak meg érzékeny adatokat, vagy veszélyes tranzakciókat hajtanak végre. Az idősek, akik kevéssé tapasztaltak az online térben, különösen veszélyeztetettek. Az alábbiakban részletesen bemutatjuk, hogyan működnek ezek az átverések, milyen jelekre kell figyelni, és hogyan védekezhetünk hatékonyan.

A csalások mögötti pszichológia

A hamis ajánlatok sikeressége a manipulációra és a pszichológiai trükkökre épít. A csalók gyakran ígérnek valami rendkívül vonzót – például luxuscikkeket, vagy pénzjutalmat –, hogy a felhasználók elveszítsék kritikai érzéküket. A sürgősség érzésének megteremtése („Most kattints, hogy ne maradj le!”) szintén gyakori taktika, mivel az emberek ilyenkor kevesebb hajlamosak alaposan átgondolni döntéseiket.

Hogyan működnek a hamis nyereményjátékok?

A hamis nyereményjátékok sokszor úgy indulnak, hogy egy „hivatalosnak” tűnő üzenetet kapunk. Ebben azt állítják, hogy egy ismert cég nevében nyereményjátékot hirdetnek, vagy azt, hogy megnyerjük egy értékes ajándékot. Például az utóbbi időben több híradás szólt arról, hogy az ismert áruházláncok nevével élnek vissza, és hamis weboldalakon kérnek adatokat a „nyeremény” átvételéhez. Az ilyen oldalak azonban csak az áldozatok adatait gyűjtik, amelyek később további csalásokhoz használnak fel.

Az idősek gyakran tapasztalatlanok az online technológiák terén, és hajlamosabbak hinni a megtévesztő ajánlatoknak. Sokan nem használnak megfelelő védelmet eszközeiken, mint például tűzfalakat vagy modern vírusirtókat. Emiatt célzottan támadják őket adathalász e-mailekkel és hamis hirdetésekkel.

A gyanús jelek felismerése

- **Túl szép, hogy igaz legyen:** Egy ajánlat, amely rendkívül olcsó terméket vagy hatalmas pénznyereményt ígér, szinte biztosan csalás.
- **Sürgősség érzése:** Ha az üzenet sürgető (Csak ma érvényes!"), érdemes elgondolkodni az ajánlat hitelességén.
- **Ismeretlen feladó:** Ha az üzenet küldője ismeretlen, vagy az e-mail cím furcsa, érdemes gyanakodni.

Adatok bekérése: A hiteles cégek nem kérnek jelszavakat, banki, vagy más érzékeny adatokat egy játék, vagy promóció során.

Védekezési stratégiák

1. **Ellenőrzés:** Mindig vizsgáljuk meg az üzenet hitelességét. Ha egy ismert cég nevében küldik, keressünk rá a hivatalos weboldalon, vagy hívjuk fel az ügyfélszolgálatot.
2. **Biztonsági beállítások:** Használjunk vírusirtót és tűzfalat, valamint kapcsoljuk be a kétlépcsős azonosítást.
3. **Tudatosság növelése:** Osszuk meg tapasztalatainkat családtagjainkkal és ismerőseinkkel, különösen az idősebbekkel, hogy ők is tisztában legyenek a veszélyekkel.
4. **Ne kattintunk gyanús linkekre:** Ismeretlen forrásból származó linkeket soha ne nyissunk meg, még akkor sem, ha az üzenetnek látszik.

Adatvédelem: Ne osszunk meg személyes adatokat semmilyen promóciós felhívás által felajánlott linken, közösségi oldalakon vagy nyereményjátékra létrehozott platformon.

A csalások következményei

Az adathalászat és a hamis ajánlatok nagy károkat okozhatnak. Nemcsak pénzügyi veszteséget jelenthetnek, hanem az áldozatok személyes adataival további károkat is okoznak, például személyazonosság-lopást. Ezért különösen fontos, hogy mindenki tisztában legyen ezekkel a veszélyekkel, és körültekintően járjon el.

Összegzés

A hamis ajánlatok és nyereményjátékok az internetes bűnözés egyik legelterjedtebb formája. Az ilyen csalások ellen a legjobb védekezés a tudatosság, a biztonsági eszközök használata és a körültekintés. Az idősek külön figyelmet igényelnek, mivel ők a legkiszolgáltatottabbak ezeknek a trükköknek. A tudatos információ megosztás és a digitális készségek fejlesztése mind hozzájárulhatnak ahhoz, hogy csökkenjen az áldozatok számát.

Intő példák a hamis promóciók világából:

Autó, mindössze 699 forintért! Minden évben számos autó halmozódik fel a területeinken. A Posta Biztosító Zrt. Szabályai szerint ezeket az autókat el kell távolítani, de tökéletesen működnek és biztonságosak a vezetéshez, ezért úgy döntöttünk, hogy egyedüli ajánlatot teszünk mindösssze 699 forintért. Bárki kaphat autót, ha kitölti az űrlapot a weboldalon. A mennyiség korlátozott!
Ki ne szeretne 699 forintért autót nyerni? A kis ördög azért ott bujkál a leendő áldozat fejében, de arra gondol, hogy ennyiért megér egy próbát. No és csak korlátozott a mennyiség, nincs idő senkivel konzultálni! Ó, hogy fognak örülni. Nosza gyorsan irány a megadott weboldal - hisz ez a felület ismerős is - már CSAK az adatokat kell beírni, bankkártyával a 699 forintot átutalni, és már kész is. Esetünkben a csalók a befizetett 699 forinton felül az érzékeny adatokhoz is hozzáfértek!

Az Amazon továbbra is felszabadítja raktárait, a már több mint 2 éve ott tárolt termékektől mindössze 749 forintért azoknak, akik válaszolnak négy kérdésre!
Ismét egy potom összegért hirdetett promóció, mely nagy értékű ajánlattal kecsegtet adatainkért cserében.

S még egy gyöngyszem a közösségi médiában az arcunkba ordító hamis, megtévesztő hirdetések, átverő nyereményjátékok közül.
Szia, Catherina Maria vagyok a Honkongi HR osztályról. Önéletrajza alapján örömmel meghívjuk Önt egy munkára, ami napi 10-20 percet vesz igénybe és 70-300 EUR közötti keresetet biztosít. A fizetés aznap elszámolásra kerül és átutalják a számlájára. Ha érdekli, kérem lépjen kapcsolatba a régiós képviselővel.
Na ez szép! 10-20 perc munkával 300 EUR? Ez pont nekem való! Ámbár nem emlékszem, hogy küldtem volna önéletrajzot, milyen szerencse, hogy így is rám találtak. Nyílván csak az adatokat kell bediktálnom, és már indulhat is a pénzkereset!
Mindig megfontoltan, kétszer is megrágva döntsön!

Telefonos csalások – hogyan védekezzünk?

A telefonos csalások számos formában jelentkezhetnek, különösen veszélyeztetve az idősebb korosztályt, akik kevésbé jártasak a modern technológiákban és gyakran jóhiszeműek. Három gyakori csalási módszer emelhető ki: **nem banki szolgáltatók nevével történő visszaélés**, **wangiri (visszahívásos) csalások**, valamint **hívószám-hamisítás (spoofing)**.
Az alábbiakban részletesen bemutatjuk ezeket a módszereket, és tanácsokat adunk a megelőzéshez.

Nem banki szolgáltatók nevével történő visszaélés

A csalók gyakran olyan pénzügyi szolgáltatók, biztosítók vagy közműcégek, telekommunikációs, kábelszolgáltató, csomagküldő vagy futárszolgálat nevében hívják az áldozatokat, amelyek nem rendelkeznek banki engedéllyel. Ilyenkor hamis ajánlatokkal vagy fenyegetésekkel próbálják rávenni az áldozatokat személyes adataik, például bankszámlaszámuk vagy jelszavaik kiadására. Például egy "biztosító" képviselőjének álcázva azt állítják, hogy az ügyfél adósságot halmozott fel, amelyet azonnal ki kell egyenlíteni, különben jogi következményekkel kell szembenéznie. De nem ritka a fizetési késedelem ,adategyeztetés, hátralékkal, csomagokkal kapcsolatos ügyintézés, online vásárlással kapcsolatos megkeresések álcája mögé bújt átverés kísérlet.

Az ilyen hívások célja, hogy pánikot keltsenek, és gyors cselekvésre késztessék az áldozatot, mielőtt felismernék a csalást. Az áldozatoknak mindig érdemes közvetlenül felhívniuk az állítólagos szolgáltatót egy ismert telefonszámon, hogy ellenőrizzék a hívás hitelességét.

Wangiri – a visszahívásos csalás

A wangiri csalás során a bűnözők automata rendszerekkel tömeges hívásokat generálnak, amelyek mindössze egy-két csengés után megszakadnak. A cél az, hogy az áldozatok kíváncsiságból visszahívják a számot, amely általában drága nemzetközi vonalra irányul. A visszahívás során a hívásdíjat prémium tarifával számolják fel, így a csalók közvetlen anyagi haszonhoz jutnak.
A legjobb védekezés, ha ismeretlen külföldi számot nem hívunk vissza, különösen akkor, ha nem várunk ilyen hívást. Egyes mobiltelefon-szolgáltatók

lehetővé teszik a gyanús előhívószámok vagy országkódok csoportos letiltását, ami hatékony módszer lehet a hasonló csalások megelőzésére.

Hívószám-hamisítás (spoofing)

A hívószám-hamisítás során a csalók olyan technológiát használnak, amely lehetővé teszi számukra, hogy a hívott fél kijelzőjén egy hamis szám jelenjen meg. Gyakran valamilyen hivatalos szervezet, például a rendőrség, bank vagy közműcég számát tüntetik fel, így növelve a hívás hitelességét. Ezek a hívások különösen veszélyesek, mert a megszokott ellenőrzési módszerek – például a hívószám ellenőrzése – hatástalanok.

A csalók gyakran arra kérik az áldozatokat, hogy adják meg az online banki azonosítójukat, jelszavaikat, vagy töltsenek le távoli hozzáférést biztosító szoftvereket. Az áldozatoknak soha nem szabad személyes adatokat megadniuk telefonon keresztül, és érdemes azonnal megszakítani a hívást, ha gyanús kérdéseket kapnak.

Mit tehetünk a megelőzés érdekében?

- **Legyünk gyanakvóak:** Soha ne adjunk ki érzékeny adatokat telefonon, és ne hajtsunk végre pénzügyi tranzakciókat egy hívás alapján. Kezelje óvatosan, fenntartással a kéretlen üzeneteket vagy telefonhívásokat!
- **Presszió:** Mint minden online térben elkövetett csalásra, a telefonos próbálkozásokra is jellemző a sürgető hangnem.
- Pénzt soha ne utaljunk telefonos felszólításra, ne használja a hívó által megadott hitelesítő telefonszámot.
- **Használjunk online keresést:** Egy gyanús számot könnyen ellenőrizhetünk az interneten, ahol gyakran találhatók figyelmeztetések más áldozatoktól.
- **Konzultáljunk szakértőkkel:** Ha kétségeink vannak, forduljunk a rendőrséghez vagy a szolgáltatónkhoz, és kérjünk tanácsot.

Az idősek biztonságának érdekében a csalásmegelőzésben a tudatosság a legfontosabb. Ha egy hívás gyanúsnak tűnik, mindig az óvatosság legyen az elsődleges szempont. Általánosan kijelenthetjük, hogy a telefonos csalások megelőzésére érvényes az összes óvintézkedés,
mely az online biztonságot szolgálja!
Csalás esetén mindig értesítse a szolgáltatóját, tegyen bejelentést a hivatalos szerveknél és értesítse családtagjait, ismerőseit!

Biztonságos online vásárlás lépései

Az online vásárlás az idősebb generáció számára is egyre népszerűbbé válik, hiszen kényelmesen, otthonról elérhetik a szükséges termékeket. Ugyanakkor az internetes vásárlás számos kockázatot is rejt, amelyek különösen veszélyesek lehetnek azok számára, akik kevesebb tapasztalattal rendelkeznek a digitális technológiák világában. Az internetes vásárlás során a legnagyobb kockázatot a csaló webáruházak, az adatlopások és a rejtett költségek jelentik. A következő tanácsok segíthetnek abban, hogy az idősek biztonságban érezzék magukat az online térben.

Az alábbiakban részletes útmutatót adunk, amely nemcsak az online vásárlás előnyeit és veszélyeit tárgyalja, hanem a biztonságos vásárlás legfontosabb lépéseit is bemutatja, kiegészítve hivatalos források (kiberpajzs.hu, police.hu, MNB) aktuális tanácsaival.

Az első és talán legfontosabb lépés a megbízható webáruházak kiválasztása. Csak ismert, hivatalos oldalakon vásároljunk, amelyek rendelkeznek tanúsítvánnyal, például HTTPS protokollal. Ez azt jelzi, hogy a weboldal titkosított, így az adataink védve vannak a külső hozzáféréstől. A biztonságos weboldalak url címe előtt kis lakat jelenik meg. A csaló oldalak gyakran kínálnak irreálisan alacsony árakat vagy rendkívül jó ajánlatokat, amelyek túl szépnek tűnnek ahhoz, hogy igazak legyenek. Ilyen esetekben mindig érdemes gyanakodni és utána olvasni az adott áruház hitelességének. A police.hu szerint érdemes megnézni az oldal általános szerződési feltételeit, kapcsolat felvételi adatait, valamint az elérhető vásárlói véleményeket.

Az online fizetés az egyik legérzékenyebb pont. Az MNB javasolja, hogy mindig ellenőrizzük a fizetési oldal valódiságát. Soha ne adjuk meg bankkártya adatainkat ismeretlen oldalakon, és kerüljük azokat az ajánlatokat, amelyek közvetlenül e-mailben kérnek pénzt. Ha lehetséges, használjunk virtuális bankkártyát, amely limitált keretet biztosít, és kizárólag online vásárlásokra alkalmas. Ez egy extra védelmi réteget jelent, hiszen még adatlopás esetén is minimális kár érhet minket.

Az utánvétel biztonságos alternatívát jelent, hiszen a termék átvételekor

fizetünk, így biztosak lehetünk abban, hogy megkapjuk a megrendelt árut. A p olice.hu kiemeli, hogy ilyen esetekben mindig ellenőrizzük a csomag épségét, és győződjünk meg róla, hogy a megrendelt terméket kaptuk meg. Ha a csomag sérült, ne vegyük át, hanem jelezzük a problémát az eladónak.
Fontos tudni, hogy a fogyasztókat jogi védelem is segíti. Az online vásárlásokra is érvényes a 14 napos elállási jog, amely lehetővé teszi, hogy indoklás nélkül visszaküldjük a terméket. Ez különösen fontos, ha a termék nem felel meg az elvárásoknak vagy hibás. A kiberpajzs.hu és az MNB figyelmeztet, hogy mindig alaposan olvassuk el a vásárlás feltételeit, különös tekintettel a szállítási és visszaküldési szabályokra.
Az adatvédelem szintén kiemelten fontos. Soha ne adjunk meg több információt, mint amennyi feltétlenül szükséges, és kerüljük az olyan regisztrációkat, amelyek gyanúsan sok adatot kérnek. Az e-mailben érkező linkek, amelyek látszólag megbízható cégektől érkeznek, gyakran adathalász támadások részei lehetnek. Ilyen esetekben ne kattintsunk a linkekre, és mindig közvetlenül a cég hivatalos oldalát látogassuk meg.
Az idősebb korosztály számára az egyik legnagyobb kihívást az ismeretek hiánya jelenti, amelyet megfelelő tájékoztatással lehet orvosolni. Az online biztonsági ismeretek bővítése, például a kiberpajzs.hu oldalán található útmutatók tanulmányozása, jelentősen csökkentheti a kockázatokat. Emellett érdemes családtagokat vagy ismerősöket megkérni, hogy segítsenek a vásárlás során, ha bármilyen bizonytalanság merül fel.

Összegzésként elmondható, hogy az online vásárlás kényelmes és biztonságos módja lehet a termékek beszerzésének, ha tudatosan és körültekintően járunk el. A megbízható források kiválasztása, a biztonságos fizetési módok használata és a jogaink ismerete mind hozzájárulnak ahhoz, hogy elkerüljük az online tér veszélyeit. Az idősebb generáció számára különösen fontos a tájékozottság és a segítségkérés, hiszen a digitális világ lehetőségei így válnak valóban hasznossá és biztonságossá.

Banki csalások és megtévesztések az interneten

A digitális tér rohamos fejlődése számos előnnyel jár, azonban az idősebb generáció számára különösen fontos, hogy tisztában legyenek az online banki csalások kockázataival. A csalók egyre kifinomultabb módszerekkel próbálják meg kihasználni a tapasztalatlanabb felhasználók bizalmát, különösen azokat, akik kevésbé ismerik a modern technológiák veszélyeit. Az alábbiakban összefoglaljuk a legfontosabb tudnivalókat és tanácsokat a banki adatok és pénzügyi biztonság védelmében.

Milyen módszerekkel dolgoznak a csalók?

Az online csalások gyakori formája az adathalászat, amikor hamis e-mailekkel, SMS-ekkel vagy weboldalakkal próbálnak bizalmas adatokat megszerezni, például netbank jelszavakat vagy bankkártya adatokat. Sokszor egy banknak álcázott e-mail vagy telefonhívás sürgető hangnemben kér érzékeny adatokat, például azt, hogy erősítse meg a számlaadatait. Az ilyen megkeresések szinte mindig csalásra utalnak, mivel a valódi bankok soha nem kérnek ilyen információkat ilyen módon.

Egy másik jellemző trükk, hogy a csalók sürgetik az ügyfeleket, hogy pénzüket egy "biztonságos számlára" utalják át, vagy azt állítják, hogy azonnali lépés szükséges a számlabiztonság érdekében. Ezek a módszerek mind a pszichológiai nyomásgyakorlásra épülnek, hogy áldozatukat meggondolatlan cselekvésre késztessék.

Hogyan védekezhetünk?

Erős jelszavak használata: Soha ne használja ugyanazt a jelszót több szolgáltatásnál, és kerüljön minden olyan kombinációt, amely könnyen kitalálható, például háziállat neve vagy születési év. A jelszavak legyenek legalább 12 karakter hosszúak, tartalmazzanak nagy- és kisbetűket, számokat, illetve speciális karaktereket.

Kétlépcsős azonosítás bekapcsolása: Ez a funkció jelentősen megnöveli a biztonságot, hiszen a belépéshez nemcsak a jelszóra van szükség, hanem például egy telefonra küldött kódra is.

Banki értesítések bekapcsolása: Az MNB ajánlása szerint minden ügyfél szá-

mára érdemes beállítani az azonnali értesítéseket, amelyek figyelmeztetnek a számlán végrehajtott tranzakciókra vagy bejelentkezésekre. Ez azonnal jelzi, ha illetéktelen tevékenység történik a számlánkon.

Limit beállítása a tranzakciókra: Sok bank lehetővé teszi, hogy az ügyfél maga állítson be napi vagy havi átutalási limitet. Ez megakadályozhatja, hogy a csalók az összes megtakarítást egy tranzakcióval eltulajdonítsák.

Ne kattintson gyanús linkekre: Adathalász e-mailekben gyakran találhatók kattintásra csábító linkek. Ha ilyen üzenetet kap, mindig manuálisan írja be a böngészőbe a bank webcímét, vagy használja a korábban elmentett könyvjelzőt.

Mit tegyünk, ha csalás áldozatai lettünk?

Az első és legfontosabb lépés, hogy haladéktalanul értesítsük bankunkat, és kérjük a számla zárolását vagy a gyanús tranzakciók felfüggesztését. Emellett jelenteni kell az esetet a rendőrségnek, hiszen ez segítheti a csalók felderítését és további károk megelőzését. Mindenképpen értesítsük családtagjainkat, ismerőseinket a csalásról, hogy hasonló támadások elkerülhetőek legyenek. Érdemes a KiberPajzs (www.kiberpajzs.hu) ajánlásait követve alaposan ellenőrizni eszközeinket, és szükség esetén vírusellenőrzést végezni vagy újratelepíteni a rendszert.

További hasznos információk

Az MNB és a rendőrség weboldalai rendszeresen publikálnak figyelemfelhívó anyagokat, például a legújabb csalási módszerekről és megelőzési lehetőségekről. Ezek az oldalak (pl. police.hu, kiberpajzs.hu) megbízható források, amelyek segíthetnek az idősek és családtagjaik számára a tájékozódásban és a védekezésben.

Az online térben való biztonságos jelenlét nem csupán technikai kérdés, hanem tudatosságot is igényel. Ha bármilyen gyanús helyzettel találkozik, mindig inkább ellenőrizze kétszer, mielőtt cselekszik! Ez a legjobb módja annak, hogy elkerülje a kellemetlen és sokszor helyrehozhatatlan anyagi károkat.

Adathalász e-mailek áldozatai

Egy idős házaspár kapott egy e-mailt, amely látszólag a bankjuktól érkezett, és az azonnali fiókellenőrzés szükségességére hivatkozott. A levél egy linket is tartalmazott, amely a banknak álcázott hamis weboldalra irányította őket. Az oldalon megadták netbankos belépési adataikat, amit a csalók azonnal felhasználtak, hogy nagy összegű átutalásokat indítsanak a számlájukról. Az esetről a KiberPajzs is beszámolt, hangsúlyozva: **soha ne adjunk meg érzékeny adatokat e-mailben vagy hamis oldalon.**

Telefonos csalás és "biztonságos számla"

Egy nő banki ügyintézőnek kiadva magát hívta fel egy idős férfit, és arról tájékoztatta, hogy a számláját "illegális hozzáférés" fenyegeti. A csaló meggyőzte őt, hogy az összes megtakarítását utalja át egy "biztonságos számlára". Miután a pénz elutalásra került, a csaló eltűnt. Az ilyen trükkök mögött a sürgetés és a félelemkeltés áll, amit a csalók tudatosan alkalmaznak.

Mobiltelefonos adathalászat

Egy másik esetben egy idős nő SMS-ben kapott értesítést arról, hogy bankkártyáját letiltották. A levél tartalmazott egy linket, amely egy mobilbarát

adathalász oldalra irányította. A kisebb képernyő miatt nem vette észre, hogy egy hamis oldalra irányították. A csalók kifinomult technikával és egyre ügyesebben hamisítják a bankok felületeit, mely megszólalásig hasonlít az eredetire. Általános tanácsként írhatjuk, hogy nem csak a banki ügyintézésben, de egyéb területeken sem ajánlott semmiféle idegen embertől származó linkre rákattintani!

Az internetes barátkozás és párkeresés veszélyei

Az internetes párkeresés és barátkozás mára az idősebb generáció számára is egyre vonzóbb lehetőség. Az online világ kínálta kapcsolatteremtés kényelmes és gyors, és sokan az egyedüllét ellenszereként tekintenek rá. Azonban nem árt tisztában lenni az ezzel járó kockázatokkal, mert a jóhiszeműség és tapasztalatlanság könnyű célponttá teheti az idősebbeket.

Hamis profilok és érzelmi manipuláció

Az egyik leggyakoribb veszély az úgynevezett „romantikus csalás", amely során a csalók hamis profillal érzelmi kapcsolatot alakítanak ki áldozataikkal. Ezek a kapcsolatok gyakran szorosak, és az áldozat bizalmát kihasználva pénzügyi segítséget kérhetnek. Például egy idős hölgy arról számolt be, hogy egy külföldön dolgozó férfi, akivel egy társkereső oldalon találkozott, hónapokig udvarolt neki, majd egy „váratlan balesetre" hivatkozva pénzt kért sürgősségi műtétre. A nő átutalta a pénzt, de soha többé nem hallott a férfiról.

Az anonimitás veszélyei

Az online térben a másik fél valódi személyazonosságának ellenőrzése nehéz, és a csalók gyakran éppen erre építenek. Sok történet szól arról, hogy ártatlan beszélgetések során az áldozatok fokozatosan osztottak meg személyes információkat, például banki adatokat vagy lakcímet, amelyeket később visszaélésre használtak fel.

Álhírek és információs túlterhelés

Nemcsak a párkeresés, de az internetes barátkozás során is fontos figyelni az információk hitelességére. Az idősebb korosztály hajlamosabb lehet elhinni, hogy az online ismerős által küldött hírek, történetek vagy kérések igazak, miközben ezek mögött gyakran csalók állhatnak, akik kattintásra, adathalászatra vagy pénzügyi tranzakciókra ösztönöznek.

Hogyan védekezhetünk?

Lassan haladjunk: Soha ne osszuk meg személyes vagy pénzügyi adatainkat, különösen egy újonnan megismert online személlyel. Legyünk óvatosak az

érzelmileg túlfűtött üzenetekkel, amelyek túl hamar komoly kapcsolatot sugallnak.

Kerüljük a pénzügyi tranzakciókat: Ha valaki pénzt kér, az intő jel lehet. Még ha a történet hihető is, mindig ellenőrizzük, hogy valóban igaz-e, mielőtt segítenénk.

Ellenőrizzük a profilokat: Végezhetünk háttérkutatást, például megkérdezhetjük közös ismerőseinket, vagy használhatunk fordított képkeresést, hogy megnézzük, nem lopott fotóval van-e dolgunk.

Tartsuk meg a valós kapcsolatok egyensúlyát: Az online barátságok és párkapcsolatok mellett fontos, hogy a való életben is ápoljuk a kapcsolatainkat, hiszen ezek adhatnak valós támogatást és örömöt.

Az internet valóban segíthet az időseknek az elmagányosodás elleni küzdelemben, és új lehetőségeket nyit meg a kapcsolatteremtésre. Azonban a biztonságos internetezés alapelveit mindig szem előtt kell tartani, hogy ne váljunk a csalók áldozatává. A tájékozottság és a megfontoltság a legjobb védekezés az online tér veszélyeivel szemben.

Egy 67 éves nő, aki egyedül élt, elhatározta, hogy az internet segítségével próbál társra találni. Egy társkereső oldalon ismerkedett meg egy magát külföldön dolgozó mérnöknek mondó férfival. Hónapokig leveleztek, és a férfi szívhez szóló üzeneteivel gyorsan elnyerte a nő bizalmát. A beszélgetések során arról mesélt, hogy özvegy, és egy gyermeket nevel, akinek jobb életet szeretne biztosítani.

Egy napon a férfi arról írt, hogy egy váratlan baleset érte őt a munkahelyén, és sürgős orvosi kezelésre van szüksége, de a biztosítását nem tudja időben aktiválni. Segítséget kért, arra hivatkozva, hogy amint kilábal a helyzetből, azonnal visszafizeti a pénzt. A nő, a kapcsolatuk intimitása miatt, úgy döntött, hogy átutalja az összeget, de a férfi ezután eltűnt. Később kiderült, hogy az egész történet egy előre megtervezett csalás volt.

Ez az eset rávilágít arra, hogy az érzelmi manipuláció és a jóhiszeműség kihasználása gyakran célzottan az idősebb generációkat érinti, akik a társas kapcsolat reményében hajlamosabbak lehetnek bízni egy online ismeretlenben.

Közösségi média: Információink megosztásának kockázatai.

Az idősebb generáció egyre aktívabban vesz részt a közösségi média platformjain. Ezek a felületek remek lehetőséget kínálnak arra, hogy kapcsolatban maradjanak családjukkal és barátaikkal, valamint tájékozódjanak a világ híreiről. Ugyanakkor a közösségi média használata jelentős kockázatokkal járhat, különösen, ha a felhasználók nem kellően óvatosak személyes adataik védelmében.

Milyen veszélyek leselkednek az idősebbekre?

Adathalászat:

A csalók gyakran használják a közösségi média platformokat személyes adatok gyűjtésére. Egy nyilvános profilról megszerzett információk – például lakcím, születési dátum, családi kapcsolatok – könnyen felhasználhatók az áldozat megtévesztésére.

Személyazonosság-lopás:

Az idősebb korosztály gyakran kevésbé tudatos az adatvédelem terén, így könnyen előfordulhat, hogy túl sok személyes információt osztanak meg. Ezeket a csalók felhasználhatják, hogy az áldozat nevében pénzügyi tranzakciókat hajtsanak végre vagy visszaéljenek a hitelükkel.

Közösségi mérgezés és hamis információk terjedése:

Az idősebbek hajlamosabbak elhinni a közösségi médiában terjedő álhíreket vagy megtévesztő tartalmakat, amelyek nemcsak félrevezetik őket, hanem érzelmi manipulációra is alkalmasak lehetnek.

Hogyan előzhetjük meg a problémákat?

Profilbeállítások ellenőrzése:

Az idősebb generációnak fontos, hogy a közösségi média profilját ne tegyék teljesen nyilvánossá. Csak olyan emberek férjenek hozzá a megosztott tartalmakhoz, akiket személyesen is ismernek.

Ne osszunk meg túl sok információt:

Személyes adatokat, például lakcímet, telefonszámot, születési dátumot vagy bankszámlaadatokat semmiképp se osszunk meg. A csalók ezeket az

információkat könnyen felhasználhatják.

Legyünk óvatosak a fotókkal:

A képeinkből több információ derülhet ki, mint gondolnánk. Egy családi fotón például látszódhat a házunk címe, egy drága tárgy, vagy olyan információ, amely vonzóvá tehet minket a csalók számára.

Gyanús felkérések elutasítása:

Az ismeretlen személyek barátkérési felkéréseit mindig utasítsuk el, mivel ezek mögött gyakran csalók vagy adathalászok állnak.

Erős jelszavak használata:

Minden közösségi média fiókhoz egyedi, erős jelszót használjunk, és lehetőség szerint kapcsoljuk be a kétlépcsős hitelesítést.

Álhírek felismerése:

Ha valamilyen tartalom túl szép vagy túl rémisztő ahhoz, hogy igaz legyen, érdemes először ellenőrizni a forrást, mielőtt tovább osztanánk.

Az idősebbek tudatosságának erősítése

Az idősebb generáció számára a közösségi média egyszerre áldás és veszélyforrás. A legnagyobb kihívást az jelenti, hogy felismerjék a kockázatokat, és megtanulják, hogyan védhetik meg magukat. Ebben a családtagok és a barátok sokat segíthetnek, például azzal, hogy tanácsokat adnak, vagy segítenek beállítani a biztonsági opciókat.

Összegzés

A közösségi média használata lehetőséget ad az idősebbeknek, hogy aktív részesei legyenek a digitális világnak, de az adatok védelme elsődleges fontosságú. A személyes információk felelős kezelése, az erős jelszavak és az óvatosság a legjobb eszközök a visszaélések megelőzésére. Egy kis odafigyeléssel és tudatossággal a közösségi média valóban a kapcsolatteremtés örömét nyújthatja, nem pedig a veszélyek forrását.

Számítógépes vírusok és zsarolóprogramok

Az idősebb generáció egyre gyakrabban használ számítógépeket és okoseszközöket, hogy tartsa a kapcsolatot családtagjaival, vagy intézze mindennapi ügyeit. Ez azonban kockázatokat is rejt magában, különösen a számítógépes vírusok és zsarolóprogramok formájában, amelyek komoly károkat okozhatnak.

Mik a számítógépes vírusok és zsarolóprogramok?

Számítógépes vírusok: Ezek kártékony szoftverek, amelyek a számítógépünk vagy eszközeink működését akadályozhatják, adatainkat ellophatják vagy törölhetik. Egy fertőzött fájl vagy program letöltésével terjednek.

Zsarolóprogramok: Ezek a vírusok titkosítják a számítógépünkön lévő adatokat, és pénzt követelnek, hogy újra hozzáférhessünk. Gyakran ijesztő üzenetekkel próbálnak nyomást gyakorolni, pl. hogy elveszíthetjük minden adatunkat, ha nem fizetünk.

Hogyan fertőződhetünk meg?

E-mail csatolmányok: Egy gyanús e-mailben érkező fájl megnyitása révén. Az idősebbek gyakran kevésbé gyanakvók az ismeretlen feladóktól érkező üzenetekkel kapcsolatban.

Gyanús weboldalak: Ha véletlenül egy fertőzött weboldalt látogatunk meg, az automatikusan letöltheti a vírust a gépünkre.

Hamis programok és frissítések: A csalók gyakran ajánlanak letöltésre "ingyenes vírusirtót" vagy "fontos frissítést", amelyek valójában kártékony szoftvert tartalmaznak.

Hogyan védekezhetünk?

Telepítsünk megbízható vírusirtót: Egy jó minőségű vírusirtó szoftver felismeri és blokkolja a fenyegetéseket. Fontos, hogy rendszeresen frissítsük a programot.

Legyünk óvatosak az e-mailekkel: Ne nyissuk meg az ismeretlen feladóktól érkező csatolmányokat, és ne kattintsunk gyanús linkekre.

Kerüljük a kétes forrásokat: Csak megbízható weboldalakról töltsünk le programokat.

Készítsünk biztonsági mentést: Rendszeresen mentsük el fontos adatainkat külső adathordozóra vagy felhőbe, hogy zsarolóprogram esetén se vesszenek el.

Használjunk naprakész rendszert: Az operációs rendszerek és programok frissítései gyakran tartalmaznak biztonsági javításokat, amelyek megvédhetnek a fenyegetésektől.

Összegzés

A számítógépes vírusok és zsarolóprogramok komoly veszélyt jelentenek, de tudatos viselkedéssel és megfelelő védelemmel megelőzhetők. Az idősebb korosztály számára különösen fontos, hogy óvatosak legyenek, és ha nem biztosak valamiben, kérjék családtagjaik vagy szakember segítségét. Ezáltal biztonságosan élvezhetik az online világ nyújtotta előnyöket.

Vigyázat, hamis jótékonysági felhívások!

Az idősebb korosztály különösen ki van téve az internetes csalások veszélyeinek, köztük a hamis jótékonysági felhívásoknak. Ezek az átverések gyakran érzelmekre hatnak, és az adományozók jóhiszeműségére alapozva próbálnak pénzt kicsalni. Az alábbiakban néhány tippet adunk, hogyan ismerhetjük fel a csalásokat, hogyan támogathatjuk biztonságosan a valódi szervezeteket.

Mire figyeljünk?

Hirtelen érzelmi nyomás: A csalók gyakran használják fel a tragikus történeteket, például természeti katasztrófákat vagy súlyos betegségeket, hogy gyors döntésre késztessék az embereket. Legyünk óvatosak, ha azonnali adományozásra buzdítanak!

Ismeretlen szervezetek: Ha egy jótékonysági szervezet nevét halljuk, érdemes utánanézni az interneten. Ellenőrizzük a szervezet hivatalos honlapját, és nézzük meg, hogy szerepel-e hiteles adatbázisokban, például a Magyarországon működő civil szervezetek nyilvántartásában.

Gyanús kommunikáció: A csalók gyakran e-mailben vagy közösségi média üzenetekben keresnek meg. Ha az üzenet túl személyes, helyesírási hibáktól hemzseg, vagy nem hivatalos e-mail címről érkezik, legyünk gyanakvóak.

Fizetési módok: Ha valaki arra kér, hogy banki átutalás helyett utalványon vagy kriptovalután keresztül fizessünk, az szinte biztosan csalásra utal.

Adományigazolás hiánya: A valódi szervezetek mindig adnak igazolást az adományról, amelyet az adóbevallás során felhasználhatunk. Ha ez elmarad, joggal gyanakodhatunk.

Hogyan támogassuk a valódi jótékonyságot?

Kérjünk segítséget! Ha nem vagyunk biztosak egy szervezet hitelességében, kérjünk tanácsot családtagjainktól vagy ismerőseinktől.

Adományozzunk közvetlenül! Keressük fel a szervezet hivatalos honlapját, és csak ott adjunk támogatást.

Kerüljük a közvetítőket! Ha valaki közvetítőként lép fel, inkább utasítsuk vissza a felkérést.

Ne hagyjuk, hogy jóhiszeműségünket kihasználják! Az odafigyeléssel és a megfelelő információk beszerzésével megvédhetjük magunkat a csalásoktól, és valóban segíthetünk azoknak, akik rászorulnak.

Hamis tech-támogatás: Soha ne adja ki jelszavát!

Az idősebb generáció tagjai gyakran válnak az úgynevezett „hamis tech-támogatási" csalások áldozatává, ahol a csalók informatikai problémák ürügyén próbálják megszerezni a jelszavakat vagy pénzt. Általában telefonon, emailben, internetes felugró ablakokon keresztül keresik meg áldozataikat.

Tipikus forgatókönyvek

Hamis figyelmeztetések: A képernyőn felugró ablakok arról tájékoztatják, hogy a számítógép „fertőzött", és azonnal lépjen kapcsolatba a „támogatással". Ezek az ablakok gyakran ijesztő üzeneteket tartalmaznak.

Telefonos megkeresés: Egy „informatikai szakember" azt állítja, hogy egy nagyvállalat (pl. Microsoft) nevében hív, és technikai problémát szeretne megoldani.

Hozzáférés kérése: A csalók megpróbálják rávenni az áldozatot, hogy telepítsenek egy programot (pl. Team Viewr, AnyDesk, vagy más távoli asztalkezelő szoftvert), hogy hozzáférjenek a számítógéphez.

Jelszó- és banki adatok kérése: A probléma „megoldásához" gyakran jelszavakat, banki adatokat vagy közvetlen fizetést kérnek.

Miért veszélyes ez?

A jelszó kiadása lehetővé teszi, hogy a csalók hozzáférjenek a személyes adatokhoz, például e-mail fiókokhoz, banki rendszerekhez vagy közösségi média profilokhoz. Ezzel pénzügyi károkat okozhatnak, vagy további csalásokat követhetnek el az Ön nevében.

Hogyan védekezhetünk?

Hivatalos támogatás ellenőrzése: Valódi technikai támogatás soha nem hívja Önt váratlanul. Gyanú esetén hívja fel a cég hivatalos ügyfélszolgálatát!

Ismeretlen szoftver: Ne engedélyezze távoli hozzáférést ismeretleneknek!

Soha ne adjon ki jelszót: A hivatalos szervezetek soha nem kérnek jelszavakat telefonon vagy e-mailben.

Frissítse rendszeresen jelszavait: Használjon erős, egyedi jelszavakat, és cserélje le azokat rendszeresen.

Beszéljen róla családjával: Ha gyanús megkeresést kap, beszéljen erről egy megbízható családtaggal vagy baráttal, mielőtt bármit tenne.

Ha bármilyen gyanús tevékenységet tapasztal, azonnal zárja le a beszélgetést vagy üzenetet, és értesítse a hatóságokat. A jelszavai az Ön biztonságának kulcsai – óvja őket!

Digitális csalások Totó – Tesztelje tudását!

1. **Honnan ismerhető fel egy hamis jótékonysági felhívás?** A) Nem kérnek sürgős adományozást. B) Nem tudnak hivatalos adományigazolást adni. C) Mindig postai úton küldenek tájékoztatót. **Helyes válasz: B**
2. **Miért veszélyes, ha jelszót adunk ki telefonon?** A) Ezzel egy számítógépes vírus terjedhet. B) A csalók hozzáférhetnek személyes adatainkhoz. C) Elveszíthetjük az internetkapcsolatot. **Helyes válasz: B**
3. **Hogyan lépnek kapcsolatba leggyakrabban a hamis tech-támogatási csalók?** A) Telefonon vagy felugró ablakokkal. B) Hivatalos postai levélben. C) Személyesen keresik fel az áldozatokat. **Helyes válasz: A**
4. **Mit tegyünk, ha egy ismeretlen számról családtagként mutatkozik be valaki?** A) Kérjünk tőle személyes információt, amit csak az ismerősünk tudhat. B) Azonnal utaljuk át a kért összeget. C) Ne szóljunk senkinek, hogy titokban tartsuk a beszélgetést. **Helyes válasz: A**
5. **Hogyan kerülhetjük el a hamis nyereményjátékokat?** A) Soha ne adjuk meg személyes adatainkat gyanús weboldalakon. B) Mindig elolvassuk a nyereményjáték szabályait. C) Csak nagyobb összeget fizetünk be, hogy növeljük az esélyeinket. **Helyes válasz: A**
6. **Mit tegyünk, ha egy ismeretlen „informatikai szakember" telefonál?** A) Adjunk meg neki minden kért információt. B) Telepítsünk egy távoli hozzáférési programot. C) Zárjuk le a hívást, és kérjük a cég hivatalos elérhetőségét. **Helyes válasz: C**
7. **Mi a teendő, ha gyanús e-mailben kattintásra buzdítanak?** A) Kattintsunk, hogy megtudjuk, mi történik. B) Töröljük az e-mailt, és ne kattintsunk semmire. C) Küldjük tovább egy barátunknak, hogy megbeszéljük. **Helyes válasz: B**
8. **Milyen fizetési módot kérnek gyakran a csalók?** A) Banki átutalást hivatalos számlára. B) Utalványokat vagy kriptovalutát. C) Postai csekket. **Helyes válasz: B**
9. **Mit tegyünk, ha felugró ablak jelzi, hogy „vírus van a számítógépen"?** A) Kattintsunk az ablakra a probléma megoldásához. B) Hívjuk fel a megadott telefonszámot. C) Zárjuk be az ablakot, és futtassunk saját víruskeresőt. **Helyes válasz: C**
10. **Hogyan ismerhetjük fel a hamis online áruházakat?** A) Gyakran kínálnak irreálisan olcsó termékeket. B) Csak készpénzben lehet fizetni. C) Csak hazai termékeket árusítanak. **Helyes válasz: A**

A kiadvány létrejöttét támogatta:

Pécs Megye Jogú Város Önkormányzata

További támogatóink: