CSALÁSTÍPUSOK

A digitalizáció ugrásszerű térnyerése a bővülő pénzügyi szolgáltatási kör mellett az ügyfelek oldalán is egyre nagyobb nyitottságot eredményezett. A fogyasztói és digitális szokások változása és a digitalizációs folyamatok átalakulása miatt egyre nagyobb hangsúly helyeződik az elektronikus pénzforgalomra. Mindezzel párhuzamosan fokozatosan növekszik a digitális térben elkövetett pénzügyi visszaélések száma is. Mivel a hazai pénzügyi rendszer biztonságosan működik, a kibertámadások – jellemzően a megtévesztésen és pszichológiai manipuláción alapuló visszaélések, valamint az adathalászat különböző formái – főként az ügyfeleket célozzák, nem pedig az informatikai rendszereket. Emiatt a piaci szolgáltatók technikai védelme mellett kiemelten fontos az Ügyfeleink pénzügyi tudatosságának erősítése is.

Az ügyfelek megtévesztésére vagy manipulálására épülő kibertámadások egyre elterjedtebbek, és gyakran megkerülik a hagyományos, technikailag jól védett pénzügyi infrastruktúrákat. Ezek a támadások nem a rendszerek gyengeségeit célozzák, hanem az emberi tényezőre építenek – arra a sérülékenységre, amely a technológiai fejlődéssel nem mindig képes lépést tartani. A digitalizáció gyors üteme és a kibertérben folyamatosan változó kockázatok különösen azokat teszik sebezhetővé, akik nem fektetnek kellő figyelmet a tudatosság és a felkészültség fejlesztésére.

A kiberbűnözők ezt a helyzetet kihasználva egyre kifinomultabb módszerekkel élnek – hamis ajánlatokkal, manipulatív kommunikációval vagy pszichológiai nyomásgyakorlással próbálnak érzékeny adatokhoz jutni vagy a célzott személyeket káros döntések meghozatalára rávenni. Kiemelten fontos felismerni, hogy mindez nem csupán fogyasztókat érint, a vállalati ügyfelek is egyre gyakrabban kerülnek célkeresztbe. Hiába rendelkeznek a cégek stabil belső rendszerekkel,

TYPES OF FRAUD

The surge in digitalisation has led to a widening range of financial services and a growing openness on the part of customers. Changes in consumer and digital habits and digitalisation processes have led to an increasing focus on electronic payments. In parallel, financial fraud in the digital space is gradually increasing. Given the security of the domestic financial system, cyber-attacks, typically based on deception and psychological manipulation and various forms of phishing, mainly target customers rather than IT systems. For this reason, in addition to the technical protection of market service providers, it is of paramount importance to raise the financial awareness of our Customers.

Cyber-attacks that rely on deceiving or manipulating customers - rather than breaching technical safeguards - have become increasingly prevalent. These attacks often circumvent secure financial infrastructures by targeting the human element, which is typically more susceptible to exploitation. While any individual or organisation can fall victim, those that struggle to keep pace with the rapid advancements in digitalisation and the evolving nature of cyber risks are particularly exposed.

Criminals are adept at exploiting these gaps, using tactics such as false offers, misleading communications, or high-pressure techniques to obtain sensitive information or induce harmful actions. Importantly, even corporate customers - despite operating within robust institutional frameworks - are not immune. Cybercriminals are increasingly focusing on employees within organisations, recognising that a single lapse in

ha a munkatársak nem megfelelően felkészültek a manipuláció felismerésére, egyetlen téves lépés is súlyos anyagi és reputációs következményekhez vezethet.

judgment or awareness can open the door to significant financial and reputational damage.

A támadók gyakran hiteles forrásnak álcázzák magukat, vagy sürgető, nyomást gyakorló helyzetet teremtenek, hogy befolyásolják az emberi döntéshozatalt. Ilyen esetekben a legkorszerűbb technikai védelem is hatástalan lehet, ha a felhasználók nem ismerik fel a fenyegetést. Éppen ezért az ügyfeleknek (függetlenül attól, hogy fogyasztó ügyfelek vagy jogi személyek) nem csupán informatikai rendszereik biztonságára kell koncentrálniuk, hanem legalább ilyen hangsúlyt kell fektetniük a csalásmegelőzést célzó tudatosságra és a kiberbiztonsági tudatosság erősítésére is.

These attackers often employ sophisticated social engineering strategies, impersonating trusted contacts or creating a false sense of urgency to manipulate decision-making. In such cases, well-established technical controls may be rendered ineffective if human vulnerabilities are successfully exploited. As a result, customers (either consumer customers or legal entities) must place equal emphasis on strengthening their digital defences and fostering a culture of cyber-awareness in order to ensure that vigilance becomes an integral part of daily operations.

A fentiek alapján a csalások megelőzése a digitális világban már nem csupán technikai védekezést jelent, legalább ilyen fontos szerepe van a kibertudatosságnak is. Még a legmegbízhatóbb technikai védelem is hatástalan lehet, ha valaki egy manipuláció hatására bizalmas adatokat ad ki. Tipikus eszközök a hamis e-mailek, megtévesztő weboldalak vagy sürgető hangvételű üzenetek, amelyek célja, hogy a felhasználót hibás döntésre késztessék.

In today's digital environment, fraud prevention goes far beyond securing systems - it also requires strong cyber awareness. Even the most advanced security infrastructure can be bypassed if a person is manipulated into disclosing confidential information. Phishing emails, fake websites, and urgent-sounding messages are just some of the tools criminals use to trick victims.

Ezért kiemelten fontos, hogy minden ügyfél – legyen magánszemély vagy vállalkozás – tudatosan és körültekintően viszonyuljon az online megkeresésekhez. Ne adjon meg bizalmas információkat gyanús forrásból érkező kérésekre, és minden szokatlan megkeresést ellenőrizzen hivatalos csatornán keresztül. Gondoskodjon arról, hogy eszközei naprakészek legyenek, és használjon erős, egyedi jelszavakat.

That is why staying alert and informed is a critical part of staying safe online. Customers—whether individuals or businesses—should treat unexpected requests for sensitive information with caution and verify their legitimacy through official channels. It is also important to keep software and devices updated and to use strong, unique passwords.

A digitális éberség kialakítása és fenntartása kulcsfontosságú a biztonság érdekében. A kibertudatosság nem egyéni kérdés, hanem közös felelősség – csak együtt, odafigyeléssel és tudatos viselkedéssel tudunk valóban biztonságos pénzügyi környezetet teremteni.

By developing a habit of digital vigilance, you can significantly reduce the risk of falling victim to fraud. Cyber awareness is not just a technical matter - it's a shared responsibility. Together, through informed and cautious behaviour, we can build a safer financial environment for all.

Felkészültséggel, odafigyeléssel és előrelátással csökkenthető annak az esélye, hogy az Ügyfelek ilyen típusú bűncselekmény áldozatává váljanak: legjobb védekezés az éberség! Az alábbiakban a Kiberpajzs (www.kiberpajzs.hu) kezdeményezés segítségével összegyűjtöttük a legtipikusabb csalási formákat. Ezúton szeretnénk felhívni Ügyfeleink figyelmét arra, hogy a Kiberpajzs weboldalon elérhető csalásmegelőzési tájékoztatók és ismert csalásmintázatok folyamatosan frissülnek. Annak érdekében, hogy mindig naprakész információkkal rendelkezzenek, javasoljuk a Kiberpajzs weboldalon közzétett tartalmak rendszeres nyomon követését. Kérjük, fordítsanak kellő figyelmet és időt az egyes csalástípusok megismerésére, elősegítve ezzel saját pénzügyi biztonságuk védelmét!

Bármilyen kérdés vagy észrevétel esetén, továbbá akkor ha gyanús tranzakciót észlel, kérjük bizalommal forduljon Bankunkhoz a Bank elérhetőségein!

With preparedness, vigilance and foresight, our Customers can reduce the chances of becoming a victim of this type of crime: the best defence is vigilance! Below, with the help of the CyberShield / Kiberpajzs (www.kiberpajzs.hu) initiative, we have compiled a list of the most typical forms of fraud. We kindly request our Customers to take the time to study these types of fraud! We would like to draw our clients' attention to the fact that the fraud prevention information and known fraud patterns available on the Cybershield/Kiberpajzs website are continuously updated. In order to always have up-to-date information, we suggest to regularly monitor the content published on the Kiberpajzs site. Please take the time to familiarize yourselves with the various types of fraud, thereby enhancing the protection of your financial security!

If you have any questions, concerns, or notice a suspicious transaction, please do not hesitate to contact the Bank through our official channels!

1. HAMIS BANKI TELEFONHÍVÁS (VISHING)

A vishing (az angol „voice” és „phishing”, vagyis hang és adathalászat szavak kombinációja) olyan telefonos csalás, amelynél a támadó megpróbálja személyes, pénzügyi vagy biztonsági információi megosztására vagy pénz átutalására rávenni az áldozatokat, akik általában banki ügyfelek. A vishing tipikus formája, amikor a csaló az adathalász hívás során megpróbálja elhitetni a felhasználóval, hogy ténylegesen egy banki alkalmazottal beszél, és egy pénzügyi tranzakció során fellépett hiba vagy csalásgyanú miatt telefonál.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!

1. FALSE BANK PHONE CALL (VISHING)

Vishing (a combination of the English words "voice" and "phishing") is a type of telephone scam where the attacker tries to convince victims, usually bank customers, to share personal, financial, or security information or to transfer money. A typical form of vishing is when the scammer, during the phishing call, tries to persuade the user that they are actually speaking with a bank employee and that there has been an error or suspicion of fraud during a financial transaction.

What can you do to avoid becoming a victim of such scams?

- Handle unsolicited phone calls with caution!

- Minél sürgetőbb a hívás, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- Gyanús telefonhívás esetén ne adjon meg személyes adatokat, és szakítsa meg a beszélgetést!
- Ha a kijelzett telefonszám valóban a Bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a Bank telefonszámát (a weboldalán vagy online kereséssel), és lépjen a Bankkal kapcsolatba közvetlenül!
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták.
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét a Bank ügyintézője adja meg, a válaszok másik felét pedig az ügyfél!
- Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy egyszer használható, második hitelesítési kódot! A bankok sosem kérik ezeket az információkat!
- Soha ne telepítsen mások kérésére programot számítógépére vagy telefonjára! A csalók sokszor vírusvédelmi megoldásnak beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- Soha ne utaljon pénzt telefonon érkező kérésre! A Bank sosem kér ilyet.
- A csalási szándékú hívásokat azonnal jelentse a Banknak!

- The more urgent the call, the more suspicious it is! Slow down and carefully consider what is being asked of you!
- Do not provide personal information during suspicious phone calls, and terminate the call!
- Even if the displayed phone number is indeed the bank's customer service number, it is not a guarantee that the call is legitimate. To verify if the caller is truly who they claim to be, find the organization's phone number (on their website or through online search) and contact them directly!
- Do not use the phone number provided by the caller for verification! The number may be fake or specifically created for the scam.
- Scammers can easily obtain basic information about you or the company you work for on the internet, for example, by using social media profiles. Do not trust the caller just because they know this information.
- If you believe the phone call is legitimate, still request cross-verification, where the representative of the Bank provides half of the answers to the questions (e.g., mother's maiden name), and the customer provides the other half!
- Never disclose your debit or credit card PIN, CVV code, online banking password, or one-time, second authentication code! Banks never ask for this information!
- Never install software on your computer or phone at someone else's request! Scammers often try to persuade their victims to install software that can be used for abuse, disguising it as antivirus solutions.
- Never transfer money in response to a phone request! The Bank never asks for this.
- Report fraudulent calls to us immediately!

2. HÍVÓSZÁM-HAMISÍTÁS (SPOOFING)

A hívószám-spoofing, azaz hívószám-hamisítás a vishing (hamis banki hívások) adathalász tevékenységek egyik speciális elkövetési technikája. Lényege, hogy az elkövetők módosítják a hívószámot, amely a hívott fél telefonjának kijelzőjén megjelenik, ezzel elrejtve a valódi hívó fél azonosságát. Vagyis híváskor nem a hívást kezdeményező igazi telefonszáma jelenik meg a potenciális áldozatok készülékén, hanem egy másik, jellemzően olyan, ami ismerős: például egy banké, ezáltal még inkább hitelesnek beállítva a hívást.

Az ilyen hívások célja elsősorban a bizalom kiépítése, illetve az adathalász támadások elsőszámú védvonalának, az óvatosságnak a kiiktatása: ha az áldozat ismerős telefonszámot lát, amikor hívják, kevésbé lesz gyanakvó, és megnő az esélye annak, hogy teljesíti, amit a hívó fél kér tőle. Akár a személyes, bankszámla- vagy bankkártyahitelesítő adatait is megadja, telepít a csalóknak távoli hozzáférést biztosító alkalmazást, esetleg ráveszik arra, hogy utalja el a pénzét egy „védett” számlára (valójában a csalóknak) vagy hagyja jóvá az általuk megadott utalást.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!
- Minél sürgetőbb a hívás és az üzenet, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- Gyanús telefonhívás esetén ne adjon meg személyes adatokat, és szakítsa meg a beszélgetést!
- Ha a kijelzett telefonszám valóban a Bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát (például a böngésző könyvjelzőjébe elmentett banki

2. CALLER ID SPOOFING (SPOOFING)

Caller ID spoofing is a specific technique used in phishing activities, particularly in vishing (fake bank calls). Its essence lies in modifying the caller ID displayed on the called party's phone screen, thereby hiding the identity of the actual caller. This means that during the call, the real phone number of the initiator is not displayed on the potential victim's device, but rather another number, typically one that seems familiar, such as a bank's, thus making the call appear even more authentic.

The primary goal of such calls is to build trust and bypass the first line of defense against phishing attacks: caution. If the victim sees a familiar phone number when they receive a call, they are less likely to be suspicious, increasing the chances of complying with the requests of the caller. They might provide personal, banking, or credit card authentication data, install remote access applications for the scammers, or even authorize a transfer to a "secure" account (actually controlled by the scammers) or approve a transfer provided by them.

What can you do to avoid becoming a victim of such scams?

- Handle unsolicited phone calls with caution!
- The more urgent the call and the message, the more suspicious it is! Slow down and carefully consider what is being asked of you!
- Do not provide personal information during suspicious phone calls, and terminate the call!
- Even if the displayed phone number is indeed the Bank's customer service number, it is not a guarantee that the call is legitimate. To verify if the caller is truly who they claim to be, find the organization's phone number (e.g., saved

weboldalán), és lépjen vele kapcsolatba közvetlenül!

- Fontos, hogy az ügyfélszolgálat felé a kapcsolatfelvételt, hívást Ön kezdeményezze az ismert telefonszámon, ne hagyatkozzon visszahívásra vagy átkapcsolásra, amit a csalók felajánlanak.
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet, vagy létrehozhatták kifejezetten a csaláshoz.
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adja meg, a válaszok másik felét pedig az ügyfél!
- Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy egyszer használható, második hitelesítési kódot! A bankok, banki ügyintézők sosem kérik el ezeket az információkat!
- Soha ne telepítsen mások kérésére programot számítógépére vagy telefonjára! A csalók sokszor vírusvédelmi megoldásnak beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- Soha ne utaljon pénzt telefonon érkező kérésre! A Bank sosem kér ilyet.
- A csalási szándékú hívásokat jelentse a Banknak!

in your browser bookmarks) and contact them directly!

- It's important to initiate contact with customer service using the known phone number; do not rely on callbacks or transfers offered by scammers.
- Do not use the phone number provided by the caller for verification! The number may be fake or specifically created for the scam.
- Scammers can easily obtain basic information about you or the company you work for on the internet, for example, by using social media profiles. Do not trust the caller just because they know this information.
- If you believe the phone call is legitimate, still request cross-verification, where the representative of the institution provides half of the answers to the questions (e.g., mother's maiden name), and the customer provides the other half!
- Never disclose your debit or credit card PIN, CVV code, online banking password, or one-time, second authentication code! Banks, bank representatives never ask for this information!
- Never install software on your computer or phone at someone else's request! Scammers often try to persuade their victims to install software that can be used for abuse, disguising it as antivirus solutions.
- Never transfer money in response to a phone request! The Bank never asks for this.
- Report fraudulent calls to the Bank immediately!

3. HAMIS ONLINE WEBÁRUHÁZAK, AJÁNLATOK

A fogyasztók és a vállalkozások egyre többet vásárolnak és adnak el az interneten. Az online

3. FALSE ONLINE STORES, OFFERS

Consumers and businesses are increasingly buying and selling online. Online offers are often

ajánlatok sokszor valóban kedvezőek, de óvakodjon a csalóktól! Bizony, van olyan, hogy valami túl szép, hogy igaz legyen!

genuinely favorable, but beware of scammers! Something can indeed be too good to be true!

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Ha lehet, belföldi kiskereskedelmi webhelyeken vásároljon, így nagyobb valószínűséggel kerülheti el, illetve oldhatja meg az esetleges problémákat!
- Nézzen utána a dolgoknak: vásárlás előtt keressen rá a hirdetőre, olvasson értékeléseket, ismertetőket az adott termékről!
- Kizárólag biztonságos fizetési szolgáltatásokkal fizessen! Gyanakodjon, ha pénzküldési szolgáltatás használatát kérik!
- Bank vagy kártyatársaság alkalmazásán kívül a kártyánkat ne rögzítsük!
- Mérlegeljük minden esetben az előre történő fizetés kockázatait és az utánvétel költségét, és inkább válasszunk utánvételt, különösen nagyobb összegű vásárlás esetén (hibás, késedelmes teljesítés esetén más a reklamációs lehetőség, ha már fizettünk; továbbá nagyobb a pénz visszaszerzésének az esélye reklamáció esetén, ha utalás helyett webkártyával fizettünk)!
- Csak biztonságos internetkapcsolat használatakor fizessen, ne használjon ingyenes vagy nyilvános wifi-hálózatokat!
- Csak biztonságos készülékről fizessen! Gondoskodjon az operációs rendszer és a biztonsági szoftverek folyamatos frissítéséről!
- Óvakodjon a hihetetlenül jó ajánlatokat kínáló reklámoktól vagy a csodát ígérő termékektől!
- Ha olyan felugró ablak jelenik meg a képernyőn, amely nem várt nyereményről tájékoztatja Önt, jusson eszébe, hogy ez nagy valószínűséggel egy rosszindulatú program!
- Ha nem érkezik meg a termék, vegye fel a kapcsolatot az eladóval! Ha nem válaszol,

What can you do to avoid becoming a victim of such scams?

- If possible, shop on domestic retail websites, as this may help you avoid or resolve potential issues more easily!
- Research things: before making a purchase, search for the advertiser, read reviews, and descriptions of the product!
- Only pay with secure payment services! Be suspicious if they ask you to use a money transfer service!
- Apart from using the Bank or card company's application, do not save your card!
- Consider the risks of advance payment and the cost of cash on delivery in each case, and choose cash on delivery instead, especially for larger purchases (the possibility of recourse is different in case of faulty or delayed performance if we have already paid; also, the chance of getting our money back is higher in case of complaint if we paid with a web card instead of a transfer)!
- Pay only when using a secure internet connection, do not use free or public Wi-Fi networks!
- Pay only from a secure device! Ensure that the operating system and security software are continuously updated!
- Beware of ads offering unbelievably good deals or promising miraculous products!
- If a pop-up window appears on the screen informing you of an unexpected prize, remember that this is most likely a malicious program!
- If the product does not arrive, contact the seller! If they do not respond, contact your bank and the operator of the online marketplace!
- Set daily and transaction limits for your account and card, online purchase limits

vegye fel a kapcsolatot a bankjával és az online piactér üzemeltetőjével!

- Állítson be számlájához és kártyájához napi és tranzakciós limiteket, online vásárlási limitet vagy korlátozást, továbbá kártyájához geolokáció korlátozást (ha van rá lehetőség)!

or restrictions, and, if possible, geolocation restrictions for your card!

4. SZEMÉLYESADAT-LOPÁS A KÖZÖSSÉGI MÉDIÁBAN

A csalók különböző módszerek alkalmazásával (például egy munkaajánlattal) megpróbálják elérni, hogy Ön megadja személyes adatait (név, e-mail-cím, jelszó, hitelkártyaszám stb.). Annak ellenére is megteszik ezt, hogy Ön megfelelő védelmet alkalmaz, ha közösségimédia-fiókjainak tartalmát nem láthatja mindenki, vagy ha óvatosságból nem oszt meg túl sok információt a profiljában (olyanokat, amelyekkel ellophatják a személyazonosságát). Az adatok birtokában aztán jóvá nem hagyott vásárlásokat hajthatnak végre az Ön hitelkártyájával; személyes adataival bankszámlát nyithatnak; telefon-előfizetést vásárolhatnak; hitelt vehetnek fel; illegális üzleti tranzakciókat hajthatnak végre; eladhatják adatait más csalóknak.

4. PERSONAL DATA THEFT IN SOCIAL MEDIA

Scammers, using various methods (such as a job offer), try to get you to provide personal information (name, email address, password, credit card number, etc.). They do this even if you have applied proper protection, such as making sure that the content of your social media accounts is not visible to everyone or not sharing too much information in your profile (information that can be used to steal your identity). With this data, they can conduct unauthorized transactions with your credit card; they can open a bank account with your personal data; they can buy a phone subscription; they can take out a loan; they can conduct illegal business transactions; they can sell your data to other scammers.

Mit tegyen személyes adatai védelme érdekében?

- Rendszeresen tekintse át közösségimédia-fiókjai adatvédelmi és biztonsági beállításait! Áldozzon némi időt annak megismerésére, hogy mit mutat a profilja Önről a külvilág számára!
- Gondolja át alaposan, mennyi információt és fényképet oszt meg a közösségimédia-oldalakon! Felhasználásukkal a csalók hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.
- Végezzen online kutatást! Keressen rá az adott termék nevére vagy a munkaajánlatra, és nézze meg, mit mondanak mások! Használjon olyan szavakat a keresőkifejezésben, mint „felülvizsgálat”, „panasz” és „csalás”!

What can you do to protect your personal data?

- Regularly review the privacy and security settings of your social media accounts! Spend some time understanding what your profile shows about you to the outside world!
- Carefully consider how much information and photos you share on social media pages! Using them, scammers can create false identities or try to trick you.
- Do online research! Search for the product name or job offer and see what others are saying! Use words like "review," "complaint," and "scam" in your search query!
- Report to the operators of social media platforms profiles that you suspect were created for fraud! Block them if they are

- Jelentse a közösségimédia-platform üzemeltetőinek azokat a profilokat, amelyekről azt gyanítja, hogy csaláshoz hozták létre őket! Tiltsa le őket, ha az ismerősei vagy a követői, és szakítson meg velük minden kapcsolatot!
- Ha valódi ismerőseitől kap szokatlan vagy gyanús üzenetet, illetve lát általuk közzétéve furcsa posztot, gyanakodjon és jelentse a közösségimédia-platform üzemeltetőjének!
- Ellenőrizze rendszeresen a és a betéti kártyája kivonatait! Ha olyan termékért, szolgáltatásért terhelték meg a számláját, amelyet nem Ön rendelt meg, vegye fel a kapcsolatot a bankkal és a kártyatársasággal!
- Állítson be számlájához és kártyájához napi és tranzakciós limiteket, online vásárlási limitet vagy korlátozást!

your friends or followers and break all connections with them!
- If you receive unusual or suspicious messages from your real acquaintances or see strange posts posted by them, be suspicious and report them to the operator of the social media platform!
- Regularly check the statements of your debit card! If your account is charged for a product or service you did not order, contact the bank and the card company!
- Set daily and transaction limits for your account and card, online purchase limits or restrictions!

5. HAMIS TRANZAKCIÓK JÓVÁHAGYÁSA

A bankok az online belépéshez és a tranzakciók jóváhagyásához kétlépcsős hitelesítést követelnek meg: az ügyfélnek a jelszón kívül egy másik módon is azonosítania kell magát. Ez az azonosítás történhet az ügyfél birtokában lévő kódgenerátorral, az ún. tokennel (ahogyan ez a Bank esetében is történik!), amely a sorozatszámától és a használat időpontjától függően egy egyszer felhasználható, rövid ideig érvényes kódot szolgáltat, történhet az ügyfél mobilalkalmazása által a telefonján megjelenített push-üzenetben szereplő kóddal, vagy az ügyfél által megadott telefonszámra érkező SMS-ben szereplő szám megadásával.

Ezek a jóváhagyási kérelmek megjelenhetnek az ügyfél telefonján akkor is, ha nem személyesen maga az ügyfél, hanem a bankszámlája felett rendelkező más személy kezdeményezte a belépést vagy a tranzakciót. Ha egy csaló próbál belépni vagy hamis tranzakciót indítani, az ügyfélnek ugyanúgy meg kell adnia a másodlagos hitelesítési adatokat ahhoz, hogy a belépés vagy a tranzakció sikeres legyen.

5. HAMIS TRANSACTIONS APPROVAL

Banks require two-step authentication for online access and transaction approval: besides the password, the customer must also authenticate themselves in another way. This identification can be done with a code generator, a so-called token (which is used also by our Bank!), held by the customer, which provides a one-time, short-lived valid code depending on its serial number and the time of use, or through a push message displayed on the customer's phone via the mobile application, or by providing the number in an SMS sent to the customer's provided phone number.

These approval requests may appear on the customer's phone even if the login or transaction initiation was not personally initiated by the customer but by another person with access to their bank account. If a scammer attempts to log in or initiate a false transaction, the customer still needs to provide the secondary authentication data for the login or transaction to be successful.

Mit tegyen, ha hamis azonosítási folyamatot észlel?

- Mindig ellenőrizze, hogy a belépési kísérletet vagy a tranzakciót, melyre jóváhagyást kér a Bank, valóban Ön kezdeményezte! Sose hagyjon jóvá ismertlen kérést!
- A banki műveletek jóváhagyásához használt tokent sose hagyja felügyelet nélkül!
- Használjon a mobiltelefonján képernyőzárat!
- Csak saját ujjlenyomatait regisztrálja a telefonjába!
- Állítsa be úgy a mobiltelefonját, hogy a push-üzenetek és az SMS-ben kapott üzenetek, értesítések tartalma csak a képernyőzár feloldása után legyen látható!

What should you do if you notice a false identification process?

- Always verify that the login attempt or transaction for which the bank is requesting approval was indeed initiated by you! Never approve unknown requests!
- Never leave the token used for approving banking transactions unattended!
- Use a screen lock on your mobile phone!
- Only register your own fingerprints on your phone!
- Set up your mobile phone so that the content of push messages and messages received in SMS is only visible after unlocking the screen!

6. MEGHAMISÍTOTT BANKI OLDALAK

Az adathalász banki e-mailekben (phishing) található hivatkozások gyakran egy meghamisított banki weboldalra vezetnek, ahol a célszemélyt a pénzügyi és személyes adatai megadására kérik. Ezek a webhelyek – ahogy mondani szokás – megtévesztésig hasonlítanak a mintának használt valódi oldalhoz. Emellett tartalmazhatnak felugró ablakot, amely a banki hitelesítő adatok megadását kéri. Gyanús lehet továbbá a gyenge minőségű grafika, valamint a sürgető hangvételű üzenetek, tartalmak. A valódi bankok nem használnak ilyen ablakokat, tartalmakat.

6. FORGED BANKING WEBSITES

Phishing bank emails often contain links that lead to a forged banking website where the recipient is asked to provide their financial and personal data. These websites closely resemble the real page used as a template. Additionally, they may contain pop-ups requesting banking authentication data. Suspicious indicators may include low-quality graphics and urgent tone of messages and content. Real banks do not use such windows or content.

Mit tegyen, ha adathalász banki e-mailt kapott?

- Ne kattintson üzenetekben lévő hivatkozásokra, és ne nyissa meg a mellékleteket! A webes bejelentkezések címeit inkább manuálisan gépelje be, vagy mentse el a böngésző könyvjelzőjébe a hivatalos banki, szolgáltatói oldalt, és csak onnan nyissa meg!

What should you do if you receive a phishing bank email?

- Do not click on links or open attachments in messages! Instead, manually type web login addresses or save the official bank or service provider page to your browser bookmarks, and open it from there!
- Use a browser that allows you to block pop-ups!

- Használjon olyan böngészőt, amely lehetővé teszi a felugró ablakok blokkolását!
- Az előugró ablakok általában bizalmas adatokat kérnek Önről. Ne kattintson rájuk és ne adjon meg személyes adatot az ilyen oldalakon!
- Amennyiben a bank szeretné felhívni a figyelmet valamilyen fontos dologra, a figyelmeztetést az online banki felületen, vagy a banki applikációban jeleníti meg.
- Vizsgálja meg alaposan az e-maileket! Keressen következetlen, értelmetlennek tűnő dolgokat, például: furcsa nyelvezet, helyesírási hibák, sürgető hangnem, nem várt csatolmány, a megjelenített névtől eltérő hivatkozás (amelyet az egérmutató fölé mozgatásával ellenőrizhetünk). A csalók leggyakrabban valami rendkívüli jutalommal kecsegtetnek, sürgetnek, büntetéssel vagy a szolgáltatásból történő letiltással, kizárással fenyegetnek, illetve a kíváncsiságunkra próbálnak hatni.
- Keressen nehezen észrevehető különbségeket a feladó címében: a nulla például „o” betűnek tűnhet! Vesse össze a küldő e-mail-címét a Bank korábbi üzeneteivel!
- Legyen különösen körültekintő a mobileszközök használatakor! Telefonon vagy táblagépen nehezebb lehet észrevenni az adathalász kísérleteket. Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót. Bár ujjal hosszan rábökve a mobiltelefon megmutatja a hivatkozást, és rákérdez, hogy mit tegyen vele, mégis a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb felfedezni.
- A gyanús e-maileket jelentse bankjának, szolgáltatójának: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a bankját, szolgáltatóját!
- Mindig tartsa naprakész állapotban szoftvereit, beleértve a böngészőt, a vírusirtó programokat és az operációs rendszert!

- Pop-up windows typically request confidential data about you. Do not click on them and do not provide personal information on these websites!
- If the bank needs to alert you to something important, the warning will appear on the online banking interface or in the banking app.
- Thoroughly examine emails! Look for inconsistencies, nonsensical elements such as strange language, spelling errors, urgent tone, unexpected attachments, or links different from the displayed name (which can be checked by hovering over them with the mouse cursor). Scammers often promise something extraordinary, rush you, threaten with penalties or service suspension, or try to pique your curiosity.
- Look for subtle differences in the sender's address: for example, a zero may appear as the letter "o"! Compare the sender's email address with previous messages from the bank or service provider!
- Be particularly cautious when using mobile devices! It may be harder to detect phishing attempts on phones or tablets. You can't hover over suspicious links with the mouse. Although tapping and holding on the mobile phone will reveal the link and ask what to do with it, the smaller screen makes it harder to spot obvious mistakes.
- Report suspicious emails to your bank or service provider: every company appreciates information about such attacks. If in doubt, call your bank or service provider!
- Always keep your software up to date, including your browser, antivirus programs, and operating system!

7. HAMIS BANKI SMS (SMISHING)

A smishing (az angol „SMS” és „phishing”, vagyis SMS és adathalászat szavak kombinációja) olyan csalás, amelynél a támadók SMS segítségével próbálnak megszerezni személyes, pénzügyi vagy biztonsági adatokat, információkat. Megbízható forrásnak álcázzák magukat, úgy tesznek, mintha egy bank, kártyakibocsátó, futárszolgálat, közműszolgáltató vagy valamilyen egyéb szolgáltató képviseletében jelentkeznének. Az üzenet arra kéri a címzettet – általában sürgető módon –, hogy nyisson meg egy weboldalra vezető hivatkozást, telepítsen egy alkalmazást, vagy hívjon fel egy telefonszámot például 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.

A csalás célja olyan információk megszerzése, amelyek segítségével aztán ellophatják az óvatlan ügyfél pénzét.

Mit tegyen, ha hamis banki sms-t kapott?

- 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!
- Ne hagyja, hogy siettessék! Végezze el a megfelelő ellenőrzést, bármennyi időbe kerüljön is!
- Ha ismerős számról érkezik az SMS, az sem garancia arra, hogy megbízható. Lehetséges, hogy egy ismerőse már áldozatul esett a csalóknak, így fel tudják használni az ő telefonszámát és adatait.
- Soha ne válaszoljon olyan SMS-re, amely a PIN-kódját, az online banki jelszavát vagy

7. SMISHING (FAKE BANK SMS)

Smishing (a combination of "SMS" and "phishing") is a scam in which attackers try to obtain personal, financial, or security information and data through SMS. They masquerade as a reliable source, pretending to represent a bank, card issuer, courier service, utility provider, or other service provider. The message asks the recipient - usually in an urgent manner - to open a link to a website, install an application, or call a phone number, for example, for account verification, update, or reactivation. The link points to a fake website, and the phone number is answered by a scammer pretending to be a representative of the company.

The goal of the scam is to obtain information that can be used to steal the unwitting recipient's money.

What should you do if you receive a fake bank SMS?

- Do not click on links, attachments, or images in unsolicited text messages without verifying the sender's identity! For verification, search for the number on the internet (if it's a scam, you probably won't be the first), or compare the number with the official phone number of the relevant organization!
- Do not let yourself be rushed! Perform the necessary checks, no matter how long it takes!
- If an SMS comes from a familiar number, that is not a guarantee of reliability. It is possible that someone you know has already fallen victim to scammers, so they can use their phone number and data.
- Never respond to an SMS requesting your PIN code, online banking password, or any other security identification data!

bármilyen más biztonsági azonosítóadatát kéri!
- Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy válaszolt egy smishing üzenetre és megadta banki adatait!

- Immediately contact your bank if you suspect you have responded to a smishing message and provided your banking details!

8. ADATHALÁSZ BANKI E-MAIL (PHISHING)

Ez az adathalász csalási forma olyan, banki ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet.

Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák.

Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha valaki nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra.

A kiberbűnözők arra építenek, hogy az emberek elfoglaltak: felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen banki e-maileket!
- Minél sürgetőbb a levél hangvétele, legyen annál gyanúsabb!
- Legyen különösen éber, ha egy „banki” e-mail bizalmas információkat kér, például az online banki jelszavát! A bankok kizárólag biztonságos módon, az online banki felületen vagy mobilapplikációban kommunikálnak az ügyfelekkel, sosem kérnek bizalmas adatokat ilyen formában!
- Ne kattintson az üzenetben lévő hivatkozásokra, és ne nyissa meg a mellékleteket, a webes bejelentkezések

8. PHISHING BANK EMAIL

This phishing scam is an email with fraudulent intent targeting bank customers, attempting to persuade the recipient to share personal, financial, or security information.

These emails may appear identical to messages sent by legitimate banks: scammers replicate the logos, appearance, and style of real emails, sometimes even including details of previous (fake or real) correspondences.

They typically have an urgent tone, threatening with penalties if the recipient doesn't respond, but may also request downloading an attachment or clicking a link.

Cybercriminals rely on people being busy: at a glance, these fake emails seem genuine. As a result, the recipient is more likely to take them seriously and act as instructed.

What should you do to avoid falling victim to such scams?

- Handle unsolicited bank emails with caution and skepticism!
- The more urgent the tone of the email, the more suspicious it should be!
- Be particularly vigilant if a "bank" email requests confidential information, such as your online banking password! Banks only communicate with customers securely, through online banking platforms or mobile apps, never asking for confidential data in this way!
- Do not click on links in the message or open attachments; manually type in web

címeit inkább manuálisan gépelje be, vagy használja a hivatalos (esetleg a kedvencek közé elmentett) banki oldalt!

- Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvételekkel szemben, amely során nem tud minden kétséget kizáróan megbizonyosodni a másik fél identitásáról! Különösen igaz ez az elektronikus kommunikációra: ne válaszoljon a gyanús e-mailekre!
- Vizsgálja meg alaposan az e-mailt! Keressen furcsaságokat, következetlenségeket és értelmetlennek tűnő dolgokat, például a következőket: furcsa nyelvezet, helyesírási hibák, sürgető hangnem, szokatlan formátumú csatolmány (.zip stb.).
- Keressen nehezen észrevehető különbségeket a feladó címében: a nulla például nagy „o” betűnek tűnhet: 0 vs. O! Vesse össze a küldő e-mail-címét a Bank korábbi üzeneteivel!
- Legyen különösen körültekintő a mobileszközök használatakor! Telefonon vagy táblagépen nehezebb lehet észrevenni az adathalász kísérleteket. Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót, és a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb beazonosítani.
- A gyanús e-maileket jelentse bankjának: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a Bankot!
- Mindig tartsa naprakész állapotban szoftvereit, beleértve a böngészőt, a vírusirtó programokat és az operációs rendszert!

9. "NIGÉRIAI TÍPUSÚ" CSALÁSOK

A „nigériai típusú” csalás a megtévesztés egyik legrégebbi, 19. század végén elterjedt formája, amelyet nigériai levélként vagy 419-es átveréseként is említenek. Kezdetben hagyományos, postai úton vagy faxon terjedt, de a telekommunikációs eszközök fejlődésével, valamint az internet és az e-

login addresses or use the official (perhaps bookmarked) bank website!

- Always be wary of contact initiated by others, especially when you cannot be absolutely sure of the other party's identity! This is particularly true for electronic communication: do not respond to suspicious emails!
- Thoroughly examine the email! Look for oddities, inconsistencies, and nonsensical elements, such as strange language, spelling errors, urgent tone, or unusual attachment formats (.zip, etc.).
- Look for subtle differences in the sender's address: for example, a zero may look like a capital "o": 0 vs. O! Compare the sender's email address with previous messages from the bank!
- Be extra cautious when using mobile devices! It may be more difficult to detect phishing attempts on phones or tablets. Mouse-over for suspicious links may not be possible, and smaller screens make it harder to identify obvious errors.
- Report suspicious emails to your bank: every company welcomes information about such attacks. If in doubt, call the Bank!
- Keep your software up to date, including your browser, antivirus programs, and operating system, at all times!

9. "NIGERIAN-STYLE" SCAMS

The "Nigerian-style" scam is one of the oldest forms of deception, dating back to the late 19th century, also known as the Nigerian letter or 419 scam. Initially spread through traditional mail or fax, with the development of telecommunication

mail terjedésével ennek a csalástípusnak is az online tér vált a fő platformjává.

A nigériai csalások során az elkövetők valamilyen megtévesztő kommunikációval – jellemzően e-mailben – pénz utalására veszik rá az áldozatukat, vagyis ezekben az esetekben az ügyfelek önszántukból utalnak! A hamis levelekben, megkeresésekben általában segítséget kérnek az elkövetők: menekültek vagyonának vagy jogtalanul elvett örökség visszaszerzéséhez, valamilyen okból átmenetileg hozzá nem férhető összeg megszerzéséhez stb. Közösségimédia-oldalakon, online társkereső portálokon terjed a nigériai csalás azon változata, amelynél az elkövető romantikus kapcsolatot épít fel leendő áldozatával, mielőtt valamilyen megható történettel pénzt kér tőle. A megtévesztő történetet valódinak látszó, de hamis közösségimédia-profillal és eredetinek tűnő, de szintén fiktív iratokkal igyekeznek alátámasztani. Hogy a történet hihetőbb legyen, előfordulhat, hogy a csalók nemzetközi átutalást kezdeményeznek, amelyet aztán visszavonnak, így mutatva, hogy az összeg valójában rendelkezésre áll, csak a levélben jelzett adminisztratív nehézség áll a kifizetés útjában. A levélben kért segítség kizárólag egy bizonyos pénzösszeg átutalását jelenti. Mindezért későbbi busás jutalmat ígérnek, amelyet azonban a károsultak végül nem kapnak meg, de a befizetett összeget elveszítik. Az is egy bevett forma, hogy a vagyon kimenekítéséhez a címzettnek meg kell adnia a bankszámlaadatait, aminek az eredménye természetesen nem az, hogy pénzösszeg érkezik rá, ellenkezőleg: az elkövetők immár hozzáférnek a bankszámlához, így akár le is nullázhatják azt.

Mit tegyen, hogy megelőzze a bajt?

- Semmilyen körülmények között ne adjon meg bizalmas információkat, banki adatokat vagy azonosító és hitelesítő információkat e-mailben vagy más úton érkező felkérésre!
- Ne kezdeményezzen fizetést levélben kapott felszólításra!

tools, the internet, and email, this type of fraud has also become prevalent in the online space.

In Nigerian scams, perpetrators use deceptive communication – typically via email – to convince their victims to make a money transfer. In these cases, customers transfer money voluntarily! The false letters or requests usually ask for help: to recover the wealth of refugees or unlawfully taken inheritance, to acquire temporarily inaccessible funds, etc. On social media platforms or online dating portals, a variant of Nigerian scams spreads where perpetrators build romantic relationships with their potential victims before asking for money with some touching story. They try to support the deceptive story with seemingly genuine but fake social media profiles and documents. To make the story more believable, scammers may initiate international transfers, then withdraw them, showing that the amount is indeed available, only administrative difficulties mentioned in the letter are hindering the payment. The assistance requested in the letter only means transferring a certain amount of money. For this, they promise generous rewards later, which the victims never receive, but they lose the deposited amount. Another common tactic is to request the recipient's bank account details to evacuate the wealth, which naturally does not result in money being transferred to them; on the contrary, perpetrators gain access to the bank account, so they can zero it.

What should you do to prevent trouble?

- Under no circumstances should you provide confidential information, bank details, or identification and authentication information in response to email or other requests received!
- Do not initiate payment in response to a letter received by mail!

- Kéretlen levél esetén figyelje a nyelvezetet: a „nigériai” levelekre jellemző a pongyola megfogalmazás, a számtalan nyelvtani és stilisztikai hiba. Ám sok esetben épp ez támasztja alá a történetet: a „tört magyarság”, a megtévesztő történetben szereplő külföldi levélíró kísérlete, hogy magyarul próbáljon meg segítséget kérni. Ha ilyen levelet kap, legyen megfontolt és gyanakvó!
- Ne legyen hiszékeny: ne higgyen e-mailben érkező, már-már romantikus történeteknek!
- Ha egy történet „túl szép, hogy igaz legyen”, akkor az nem igaz, hanem csalás, átverés!
- Nem reális, hogy ismeretlenek a könnyű meggazdagodás lehetőségét ajánlják fel másoknak. Ha ilyen tartalmú levelet kap, gyanakodjon!

- In the case of unsolicited mail, pay attention to the language: the "Nigerian" letters are characterized by sloppy phrasing, numerous grammatical and stylistic errors. However, in many cases, this supports the story: the "broken Hungarian", the attempt of the foreign letter writer appearing in the misleading story to seek help in Hungarian. If you receive such a letter, be prudent and suspicious!
- Do not be gullible: do not believe in email-received, almost romantic stories!
- If a story is "too good to be true," then it's not true but a scam, a fraud!
- It is not realistic for strangers to offer easy wealth opportunities to others. If you receive such a letter, be suspicious!

10. ELŐFIZETÉSES CSALÁS

A Magyar Nemzeti Bank adatai szerint 2025 elejétől újfajta csalástípus terjed több – jellemzően külföldi – weboldalon. Ezeken vonzó áron terméket vagy szolgáltatásokat kínálnak úgy, hogy a kereskedők, szolgáltatók a felületen található ügyféltájékoztatókban elrejtik, hogy az ügyfelek vásárlásukkal együtt azt is jóváhagyják, hogy egy – esetleg a termékhez egyáltalán nem kötődő – ismétlődő előfizetést is igényelnek.

A vásárlási, erős ügyfélhitelesítéssel jóváhagyott tranzakciók után (akár több héttel) az ügyfelek azt tapasztalják, hogy rendszeresen, akár hetente néhány ezer, tízezer forinttal megterhelik számlájukat. Az első, erős ügyfélhitelesítéssel végrehajtott vásárlással jóváhagyott ismétlődő terhelések – bejelentés hiányában – ugyanis ennek hiányában akadálytalanul teljesülhetnek.

10. SUBSCRIPTION FRAUD

According to the information of the Hungarian National Bank, as of 2025 a new type of fraud is spreading on several websites, mostly abroad. On these sites, products or services are offered at attractive prices, with vendors and service providers hiding in the customer information leaflets on the site that customers agree to a recurring subscription - possibly not related to the product at all - along with their purchase.

After purchases approved with strong customer authentication, clients experience that their accounts are regularly debited — sometimes weekly — with amounts ranging from a few thousand to tens of thousands of forints. Following the initial purchase, which was approved using strong customer authentication, recurring charges can be executed without further strong authentication, provided that no objection is raised.

Az új csalástípus azért is lehet hatékony, mert a mindennapok részévé váltak a szolgáltatásokra történő elektronikus előfizetések: az ügyfelek sokszor bankkártyával, hitelkártyával fizetnek elő például streaming- vagy tárhelyszolgáltatásra. Igényléskor az első időszakra vonatkozó díjat bankkártyával, erős ügyfélhitelesítés mellett róják le. A szolgáltatóval történő szerződés részeként az ügyfelek ilyenkor azt is elfogadják, hogy előbbi az előfizetés keretében rendszeresen megterhelje bankszámlájukat, immár további külön megerősítés nélkül.

Amennyiben az ügyfél számláját megterhelik a fizetési megbízás összegével, és a fizetést követően a terméket ő nem kapja meg, illetve nincs valós teljesítés a megújuló szolgáltatás (előfizetés) mögött, úgy neki lehetősége van a kártyatársasági szabályok szerint ún. chargeback eljárást kezdeményezni. Ennek lényege, hogy az ügyfél visszakövetelheti a vásárlás ellenértékét, abban az esetben is, ha külföldi a kereskedő. A visszatérítést a kártyát kibocsátó banknál kell kezdeményezni (ez a számlavezető bank), ennek során meg kell adni a tranzakció adatait – kereskedő/szolgáltató neve, vásárlás dátuma, a vásárlás ellenértéke, a kártya száma stb. Meg kell továbbá indokolni a visszatérítés okát, amely ezekben az esetben a szolgáltatás nem teljesítése (nem kapott az ügyfél árut, szolgáltatást). A bankoknak joguk van bekérni a csalárd kereskedővel folytatott kommunikációt is.

Fontos!

- Amennyiben a fentiekhez hasonló tranzakciókat tapasztal, haladéktalanul jelezze a bankjának!
- Mindig körültekintően vásároljanak - különösen az eddig ismeretlen - weboldalakon! Gyanakvásra adhat okot, ha a termék vagy szolgáltatás ára az átlagos piaci árakhoz képest irreálisan kedvező.
- A vásárlást megelőzően nézze meg az adott webshop fogyasztói értékelését is a közösségi médiában vagy az interneten!
- Esetleges nemfizetéssel nem feltétlenül szűnik meg automatikusan a csalásos

The new type of fraud can also be effective because electronic subscriptions to services have become part of everyday life: customers often subscribe to streaming or hosting services, using a credit or debit card. When a subscription is requested, the first period is charged by credit card with strong customer authentication. As part of their contract with the service provider, customers also agree to have their bank account debited regularly by the service provider as part of the subscription, now without further confirmation.

If the amount of the payment order is debited from the customer's account and the customer does not receive the product after the payment or there is no real performance behind the renewed service (subscription), the customer has the possibility to initiate a chargeback procedure under the card scheme rules. This means that the customer can claim back the value of the purchase, if the merchant is foreign. The refund must be initiated with the bank that issued the card (this is the account-keeping bank), providing details of the transaction - name of the vendor/service provider, date of purchase, value of the purchase, card number, etc. The reason for the refund must also be given, which in these cases is non-performance of the service (the customer did not receive the goods or services). Banks also have the right to request communications with the fraudulent merchant.

Important!

- If you experience transactions similar to the above, please report them to your bank immediately!
- Always shop carefully, especially on unfamiliar websites! Suspicion may be aroused if the price of a product or service is unrealistically low compared to average market prices!
- Before you buy, check consumer reviews of the shop on social media or online!
- A possible non-payment does not necessarily automatically end the fraudulent service. In some cases, the charges may continue until you cancel the

szolgáltatás. Bizonyos esetekben a díjterhelések addig folytatódhatnak, amíg – a szolgáltatóval kötött szerződésben rögzítettek szerint – le nem mondjuk a szolgáltatást. Ezért rendszeresen ellenőrizzük a bankkártyás, illetve a bankszámlát érintő tranzakcióinkat!

service, as set out in your contract with the service provider. So check your credit card and bank account transactions regularly!

11. LÁNDZSÁS ADATHALÁSZAT (SPEAR PHISHING)

A spear phishing, vagy lándzsás adathalászat egy új csalási technika, amely során a támadók személyre szabott üzenetekkel próbálják tőrbe csalni a potenciális áldozatot. Az ilyen támadások gyakorisága növekvő tendenciát mutat, mert a támadók folyamatosan finomítják módszereiket, és egyre több személyes információhoz férnek hozzá a közösségi média és egyéb online platformok révén.

A hitelesség látszatát a kiberbűnözők az úgynevezett social profiling módszert alkalmazva építik fel: a leendő áldozatról nyilvánosan elérhető adatokból, részletes elemzést követően összeállítják annak profilját és elkészítik a személyre szabott félrevezető üzenetet. Ezek az üzenetek általában olyan információkat tartalmaznak, mint a személy neve vagy munkahelyének neve stb.

Árulkodóak lehetnek a gyanús linkek és mellékletek is – nagyon fontos, hogy ezekre ne kattintsunk rá, mert a hivatkozások rosszindulatú weboldalakra irányíthatnak, a mellékletek pedig kártékony szoftvereket tartalmazhatnak.

Mit tegyen, ha már megtörtént a baj?

Ha személyre szabott online adathalász csalás áldozatává vált, a gyors cselekvés a legfontosabb. A kiberbiztonsági szakértő a következő lépéseket javasolja:

- Jelentse az esetet a rendőrségen, és vegye fel a kapcsolatot jogi szakértővel, aki

11. SPEAR PHISHING

Spear phishing is a new fraud technique where attackers use personalised messages to lure potential victims into a trap. The frequency of such attacks is on the rise as attackers continue to refine their methods and gain access to more and more personal information through social media and other online platforms.

Cybercriminals use a method known as social profiling to build up the appearance of authenticity: they use publicly available data about the prospective victim to compile a profile and create a personalised misleading message, after a detailed analysis. These messages usually contain information such as the person's name, workplace, etc.

Suspicious links and attachments can also be a giveaway - it is important not to click on them as links can lead to malicious websites and attachments can contain malicious software.

What should you do if the problem has already happened?

If you've been a victim of a personalised online phishing scam, acting quickly is key. Cybersecurity experts recommend the following steps:

- Report the incident to the police and contact a legal professional who can help

támogatást nyújthat pénze – vagy jó híre – visszaszerzésében.
- Azonnal értesítse a bankját, hogy ideiglenesen le tudják állítani a tranzakciókat vagy visszatéríteni a csalás során átutalt összeget.
- Változtasson jelszót, optimalizálja fiókja adatvédelmi beállításait.
- Értesítse ismerőseit – különösen akkor, ha a csalók az Ön nevében próbált másokat félrevezetni.
- Dokumentálja, amit csak lehet: jegyezzen fel minden kommunikációt, eseményt és tranzakciót. Ide tartoznak a banki kivonatok, e-mail üzenetek és minden egyéb dokumentum, amely a csalással összefüggésbe hozható. Ha a csalók telefonon újra próbálkoznak, rögzítse a hívást!

you recover your money - or your reputation.
- Contact your bank immediately so they can temporarily stop transactions or refund the amount transferred in the scam.
- Change your password, optimise your account privacy settings.
- Inform your friends - especially if fraudsters have tried to mislead others on your behalf.
- Document what you can: record all communications, events and transactions. This includes bank statements, email messages and any other documents that can be linked to the fraud. If the fraudsters try again by phone, record the call.

Mit tegyen személyes adatai védelme érdekében?

- Nézze át közösségi média adatlapjait egy kiberbűnöző szemével! A támadók számára a Facebook, Instagram, LinkedIn, TikTok, Twitter profilok igazi aranybányaként szolgálhatnak. Szelektáljon és töröljön olyan adatokat, amelyek tálcán kínálják a lehetőséget annak, aki rossz szándékkal közelít! (pl. pontos születési dátum, telefonszám, személyes e-mail cím, lakcím, banki adatok, gyerekek személyes adatai, érzékeny munkahelyi információk)
- Utazások alkalmával különösen figyeljen arra, hogy ne osszon meg repülőjegyeket, szállásfoglalási adatokat, részletes útiterveket.
- Módosítsa az adatvédelmi beállításokat!
- Állítsa privátra a profil láthatóságát. Az a legbiztosabb, ha a közösségi média adatlap lényegi része csak a visszaigazolt ismerősök, engedélyezett követők számára látható.
- Korlátozza posztjai láthatóságát, és kerülje a helymegosztás használatát.

What should you do to protect your personal data?

- Look at your social media profiles through the eyes of a cybercriminal! For attackers, Facebook, Instagram, LinkedIn, TikTok, Twitter profiles can be a real goldmine. Select and delete data that offers a platter of opportunities to anyone who approaches you with malicious intent! (e.g. exact date of birth, phone number, personal email address, home address, bank details, children's personal details, sensitive work information)
- When travelling, be particularly careful not to share airline tickets, hotel booking details, detailed travel plans.
- Change your privacy settings!
- Set your profile visibility to private. It is safest if the core part of your social media profile is only visible to confirmed friends and authorised followers.
- Limit the visibility of your posts and avoid sharing space.
- Make unauthorised access difficult with strong passwords and multi-factor authentication.

- Az illetéktelen belépést nehezítse meg erős jelszóval és többfaktoros azonosítással.
- Gondolja át alaposan, mennyi információt és fényképet oszt meg a közösségimédia-oldalakon! Felhasználásukkal a csalók hamis személyazonosságot hozhatnak létre, vagy megpróbálhatják átverni.

- Think carefully about how much information and photos you share on social media sites. Fraudsters may use them to create a false identity or try to trick you.

12. VISSZAHÍVÁSOS TELEFONOS CSALÁS (WANGIRI)

A Japánból származó wangiri a mobiltelefonoknak köszönhetően vált az egyik legelterjedtebb csalástípussá. Lényege, hogy a csalók tömegesen generált számítógépes hívások részeként ismeretlen, általában külföldi – jellemzően 2-essel kezdődő országhívószámmal rendelkező afrikai, vagy 5-össel kezdődő országhívószámmal rendelkező közép-amerikai – számról hívják fel áldozataikat, ám a hívást egy-két csöngés után bontják a visszahívás reményében. A visszahívás azonban a belföldinél magasabb tarifán zajlik, és a csalás akkor is eredményes, ha a hívás látszólag sikertelen: például folyamatosan kicsöng, vagy épp nem csöng ki, hanem vonalszakadást vagy folyamatosan foglaltat jelez.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen, különösen a külföldi számról indított telefonhívásokat!
- Ne vegye fel a telefont, ha híváskor ismeretlen külföldi hívószámot jelez ki a telefonja, és ne is hívja vissza rögtön – először ellenőrizze azt!
- Különösen legyen óvatos akkor, ha olyan külföldi számról hívják, ahol nem él ismerőse vagy ahonnan nem vár hívást, illetve ha az országhívó 2-essel vagy 5-össel kezdődik (afrikai és közép-amerikai azonosítók)!
- Egy internetes kereséssel utánajárhat annak, hogy az adott telefonszámmal kapcsolatban felmerül-e a csalás gyanúja:

12. CALLBACK PHONE FRAUD (WANGIRI)

Wangiri, originating in Japan, has become one of the most widespread types of fraud thanks to mobile phones. In essence, fraudsters use mass-generated computer calls to call their victims from an unknown number, usually abroad, typically an African country code starting with 2 or a Central American country code starting with 5, but then disconnect the call after one or two rings in the hope of a callback. However, the callback is charged at a higher rate than national calls, and the scam is effective even if the call appears to be unsuccessful: for example, it rings continuously, or does not ring but indicates a disconnection or a busy signal.

What should you do to avoid becoming a victim of such fraud?

- Handle unsolicited phone calls, especially from abroad, with caution and reservation.
- Don't answer the phone if you receive a call from an unknown foreign number, and don't call back immediately - check it first!
- Be especially careful if you are being called from a foreign number where you do not know someone or from where you do not expect a call, or if the country code starts with 2 or 5 (African and Central American identifiers)!
- You can check whether the number you are calling is suspected of being fraudulent by doing an internet search: if

ha igen, nagy valószínűséggel talál ezzel kapcsolatos információt a világhálón.

- Az ismeretlen előhívószámokról érkező külföldi hívások egyedileg és csoportosan is letilthatók. Az egyedi hívószámokat a készülék beállításaiban lehet letiltani, míg az előhívószámok csoportos letiltása a szolgáltató ügyfélszolgálatán kérhető.

so, you are likely to find information on the web.

- Calls from unknown dialling codes abroad can be blocked both individually and in groups. Individual numbers can be blocked in the device settings, while group blocking of dialling codes can be requested from your operator's customer service.

13. ELADÓK ÁTVERÉSE AZ ONLINE PIACTEREKEN

Az egymás közötti adásvételt egyszerűen és ingyenesen lehetővé tévő internetes felületek, azaz online piacterek egyre több csalót vonzanak. Pár éve még a vevők megkárosítása volt a jellemző, manapság azonban már az eladók is a visszaélések céltáblájává válhatnak. Az óvatlan eladót úgy verik át, hogy a piactéren értékesített áruért járó ellenérték fogadásához vagy az áru kiszállításához valamilyen szokatlan, további teendőt várnak el.

Hogyan ismerheti fel az ilyen átveréseket?

Az eladó megkárosításának egyik leggyakoribb módjánál a vevő azzal hívja fel őt, hogy kifizette a meghirdetett terméket, ám arra kéri az eladót, hogy valamilyen távoli hozzáférést biztosító programot (például AnyDesk, TeamViewer) telepítsen a gépére vagy telefonjára annak érdekében, hogy „biztosítva legyen az átutalás fogadása”.

Az online piactereken alkalmazott csalások egy másik típusánál az eladó egy sms-t kap, amelyben arról tájékoztatják, hogy a termékét kifizették, de „fogadnia kell az összeget” az üzenetben küldött link segítségével, vagy a termék kiszállításához ajánl a „vevő” egy csomagküldő szolgálatot, ismert, jogszerűen működő cégek nevével visszaélve (pl.: Foxpost, DHL, DPD, MPL), és rájuk hivatkozva küld adathalász linket tartalmazó üzenetet vagy e-mailt. Amikor az eladó gyanútlanul rákattint, akkor egy, a csalók által készített hamis weboldalon találja magát, ahol bankkártyaadatait kérik (amivel ezután a csalók

13. SCAMMING SELLERS ON ONLINE MARKETPLACES

Internet platforms, or online marketplaces, that make it easy and free to sell to each other are attracting more and more fraudsters. While a few years ago it was the buyers who were being victimised, nowadays sellers can also be the target of fraud. Fraudsters deceive unsuspecting sellers by demanding unusual additional actions to receive payment for the sold goods or to receive the delivery of the goods.

How can you recognize such fraud?

In one of the most common ways of defrauding a seller, the buyer calls the seller saying that they have paid for the advertised product, but asks the seller to install some remote access software (e.g. AnyDesk, TeamViewer) on their computer or phone to “ensure that the transfer is received.”

In another type of online marketplace scam, the seller receives a text message informing them that their product has been paid for but they need to “accept payment” via a link in the message, or the “buyer” recommends a parcel delivery service to deliver the product, misusing the names of known legitimate companies (e.g. Foxpost, DHL, DPD, MPL) and sending a message or email containing a phishing link referring to them. When the seller unsuspectingly clicks on it, they are taken to a fake website created by the fraudsters, where they are asked for their credit card details (which the fraudsters can then abuse, for example to make a

vissza tudnak élni, például vásárolhatnak vele) vagy ki kell választania a számlavezető bankját, és arra kattintva megadni a saját banki belépési adatait. Utóbbi esetben az eladó érzékeny netbanki belépési adatai kerülnek illetéktelen kezekbe. Mivel ez a hamis oldal a valódi banki oldalnak továbbítja az adatokat, az óvatlan ügyfél (eladó) megkapja az egyszer használható bejelentkezési kódot (pl. SMS-kódot), és azt is begépeli a hamis oldalon. Így a csalók bejutnak az ügyfél banki profiljába, és a számlán lévő pénzhez is hozzáférnek, amelyet azonnal elutalhatnak, ellophatnak.

purchase) or they have to select their account bank and click on it to enter their own bank login details. In the latter case, the seller's sensitive online banking login details fall into the wrong hands. As this fake site forwards the data to the real bank site, the unwary customer (seller) receives a one-time login code (e.g. SMS code) and enters it into the fake site. This allows fraudsters to access the customer's banking profile and gain access to the money in the account, which they can then immediately transfer or steal.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Soha ne utaljon pénzt, ha Ön az eladó (mert például csomagküldéssel próbálhatják rászedni)!
- Legyen tisztában azzal, hogy eladóként Ön pénzt csak fogad, nem küld.
- Online piactereken vagy más, interneten keresztüli értékesítésnél az a legbiztonságosabb, ha a fizetést a bankszámlánkra kérjük a nevünk és bankszámlaszámunk (vagy másodlagos azonosítónk) megadásával.
- Legyen éber! Ahhoz, hogy bankszámlájára pénzt utaljanak, Önnek nincs szüksége semmilyen programra, és netbanki profiljába se kell bejelentkeznie!
- Soha ne adjon meg további bankszámlaadatokat, felhasználóifiók-azonosítókat, jelszavakat e-mailben, sms-ben vagy telefonon érkező kérésre!
- Soha ne töltsön le ismeretlen programot vagy applikációt számítógépére, mobiltelefonjára, főleg ne egy linkre kattintva!
- A csalás és a tényleges jogosulatlan átutalás között akár napok is eltelhetnek, ezért amint azt észleli, hogy csalás áldozatává vált, azonnal, késlekedés nélkül jelentse az esetet bankjánál, és tegyen feljelentést a rendőrségen!

What should you do to avoid becoming a victim of such fraud?

- Never transfer money if you are the seller (because they may try to trick you into sending parcels, for example)!
- Be aware that as a seller you are only receiving money, not sending it.
- For online marketplaces or other online sales, it is safest to ask for payment to our bank account by providing your name and bank account number (or secondary identifier).
- Be vigilant! You do not need any software to get money transfered to your bank account, nor do you need to log in to your online banking profile!
- Never provide additional bank account details, usernames, user IDs, passwords by email, SMS or phone when asked!
- Never download any unknown program or application to your computer or mobile phone, especially by clicking on a link!
- It can take days between fraud and the actual unauthorised transfer, so as soon as you realise that you have been a victim of fraud, report the incident to your bank immediately and without delay and report it to the police.

14. HAMIS BEFEKTETÉSI LEHETŐSÉGEK

A befektetésekkel kapcsolatos legelterjedtebb csalásoknál olyan területeken kínálnak vonzó lehetőségeket, mint például a részvények, a kötvények, a kriptovaluták, a ritka fémek, a tengerentúli ingatlanok vagy az alternatív energia. Ezeket a befektetési lehetőségeket gyakran – a tudtuk és beleegyezésük nélkül – közismert emberek, sportolók, modellek képeivel és ajánlásával hirdetik.

Mit tegyen, ha ilyen ajánlatot kapott?

- Ne vegye fel a telefont, ha híváskor ismeretlen külföldi hívószámot jelez ki a telefonja, és ne is hívja vissza rögtön – először ellenőrizze azt! Különösen legyen óvatos akkor, ha olyan külföldi számról hívják, ahol nem él ismerőse vagy ahonnan nem vár hívást, illetve, ha az országhívó 2-essel vagy 5-össel kezdődik (ld. fentebb: afrikai és közép-amerikai azonosítók)!
- Egy internetes kereséssel utánajárhat annak, hogy az adott telefonszámmal kapcsolatban korábban felmerül-e a csalás gyanúja: ha igen, nagy valószínűséggel talál ezzel kapcsolatos információt a világhálón.
- Az ismeretlen előhívószámokról érkező külföldi hívások egyedileg és csoportosan is letilthatók. Az egyedi hívószámokat a készülék beállításaiban lehet letiltani, míg az előhívószámok csoportos letiltása a szolgáltató ügyfélszolgálatán kérhető.

- Mindig gyanakodjon, ha
  - az a megérzése támad, hogy az ajánlat „túl szép, hogy igaz legyen”;
  - folyamatosan kapja a kéretlen e-maileket;
  - a közösségi médiában újra és újra találkozik ezekkel a hirdetésekkel;
  - gyors megtérülést ígérnek és biztosítják arról, hogy a befektetés biztonságos;

14. FAKE INVESTMENT OPPORTUNITIES

Some of the most common investment scams offer attractive opportunities in areas such as shares, bonds, cryptocurrencies, rare metals, overseas real estate and alternative energy. These investment opportunities are often advertised - without their knowledge or consent - with pictures and recommendations of well-known people, athletes and models.

What should you do if you receive such an offer?

- Don't answer the phone if you get an unknown foreign number displayed on your phone, and don't call it back straight away - check it first! Be particularly wary if the call is from a foreign number where you do not know or expect to be called, or if the country code starts with 2 or 5 (see above: African and Central American identifiers)!
- An internet search can help you to find out whether the number you are calling has been suspected of fraud: if so, you are likely to find information on the web.
- Calls from unknown dialling codes abroad can be blocked both individually and in groups. Individual numbers can be blocked in the device settings, while group blocking of dialling codes can be requested from your operator's customer service.

- Always be suspicious if
  - you get the feeling that the offer is "too good to be true";
  - you keep receiving unsolicited emails;
  - you keep seeing these ads on social media;
  - you are promised a fast return and assured that your investment is safe;

    - az ajánlat csak korlátozott ideig él, kimaradhat, lemaradhat róla;
    - az ajánlat csak Önnek érhető el, és megkérik, hogy senkinek se szóljon róla!
- Utasítsa el/tiltsa le a befektetési lehetőségekkel kapcsolatos kéretlen e-maileket, telefonhívásokat, bármilyen egyszerű és könnyű pénzszerzésről, meggazdagodásról szólnak is!
- Pénz átadása vagy befektetése előtt mindig kérjen pénzügyi tanácsot egy független féltől, szakértőtől!
- Ha olyan felugró ablak jelenik meg a képernyőn, amely nem várt nyereményről tájékoztatja Önt, jusson eszébe, hogy ez nagy valószínűséggel egy rosszindulatú tartalom!
- Óvakodjon a jövőbeli csalásoktól! Ha egyszer már befektetési csalás áldozatává vált, a csalók valószínűleg újra megkeresik, vagy eladják adatait más bűnözőknek!
- Értesítse a rendőrséget, ha gyanakszik!

15. HAMIS MNB ÜGYFÉL-ELÉGEDETTSÉGI KÉRDŐÍVVEL TÁMADNAK A KIBERCSALÓK

A közelmúltban feltárt online vásárlásos rejtett előfizetési csalás után a Magyar Nemzeti Bank (MNB) fogyasztói jelzések alapján ismét egy új kibercsalási módszerről értesült. A bűnözők az elmúlt napokban a jegybank nevében keresték meg telefonon az ügyfeleket, azt állítva, hogy a hazai bankokra vonatkozó ügyfél-elégedettségi kérdőíves felmérést végeznek. A beszélgetés során az adott ügyfelektől megtudakolták azok számlavezető hitelintézeteinek nevét, illetve rögzítették e-mailes elérhetőségüket is.

Az állítólagos „felmérést” követően nem sokkal az érintett ügyfelek egy része olyan adathalász e-mailt kapott az MNB nevében, amelynek mellékelt hivatkozását (linkjét) megnyitva a csalók számára számítógépéhez távoli hozzáférést biztosító alkalmazás (ez lehet AnyDesk vagy egyéb program is) töltődött le. Más ügyfeleket rövidesen saját

    - the offer is only for a limited time, you may miss it, you may miss out;
    - the offer is only available to you and you are asked not to tell anyone about it!
- Reject/unsubscribe to unsolicited emails, phone calls about investment opportunities, however simple and easy they are about making money, getting rich!
- Always seek financial advice from an independent party, an expert, before transferring or investing money!
- If a pop-up window appears on your screen telling you about an unexpected prize, remember that it is most likely malicious content!
- Beware of future scams! If you have already been a victim of an investment scam, the scammers will probably contact you again or sell your details to other criminals!
- Notify the police if you suspect fraud!

15. CYBER FRAUDSTERS ATTACK WITH FAKE MNB CUSTOMER SATISFACTION QUESTIONNAIRE

Following the recently discovered online shopping hidden subscription fraud, the Hungarian National Bank (MNB) has again become aware of a new cyber-fraud scheme based on consumer signals. Criminals have been contacting customers by phone in recent days on behalf of the central bank, claiming to be conducting a customer satisfaction survey on domestic banks. During the conversation, the customers were asked for the names of their credit institutions and their e-mail contact details.

Shortly after the alleged 'survey', some of the customers concerned received a phishing e-mail on behalf of the MNB, which contained a link that downloaded an application (could be AnyDesk or other software) that allowed the fraudsters to remotely access their computers. Other customers were soon contacted by cybercriminals

bankjuk nevében hívtak fel a kiberbűnözők, és – a korábban megismert csalási mintázattal azonos módon – arról értesítették, hogy gyanús tranzakciókat látnak bankszámláján. A csalók ezekre hivatkozva és „banki segítséget” ajánlva próbálták megtudni az adott fogyasztók bizalmas banki azonosítóit, belépési jelszavait.

on behalf of their own bank and, in a similar pattern to the fraudulent activity we have seen before, were informed that they were seeing suspicious transactions on their bank accounts. The fraudsters referred to these and offered "banking assistance" in an attempt to obtain the consumers' confidential bank identifiers and login passwords.

Az MNB nem végez semmiféle ügyfél-elégedettségi kérdőíves felmérést az ügyfelek között, a kiberbűnözők a jegybank nevének ismertségével élnek vissza. A kereskedelmi bankok soha semmilyen kommunikációs csatornán (sem telefonon, sem e-mailben vagy sms-ben) nem kérik el az ügyfelek bizalmas azonosítóit és nem töltetnek le azok gépére „vírusírtó” alkalmazásokat, vagyis a valóságban kémprogramokat.

The MNB does not carry out any customer satisfaction surveys among its customers, and cybercriminals are taking advantage of the name recognition of the central bank. Commercial banks never ask for customers' confidential identities through any communication channel (telephone, e-mail or SMS) and never download 'anti-virus' applications, in reality spyware, onto their computers.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!
- Ha sürgető hangnemű telefonhívást kap, legyen mindig szkeptikus! Minél sürgetőbb a hívó fél, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- Amennyiben felmerül Önben a kétely, hogy csalóval beszélhet, mielőbb szakítsa meg a hívást, és keresse fel az érintett intézményeket a további lépésekkel kapcsolatban (pl. banki megkeresésnek álcázott hívás esetén saját bankunkat)!
- Gyanús telefonhívás esetén ne adjon meg személyes adatokat, és szakítsa meg a beszélgetést!
- Soha ne telepítsen mások kérésére programot számítógépére vagy telefonjára! A csalók sokszor vírusvédelmi megoldásnak beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- AnyDesk szoftvert használva soha ne írja be személyes érzékeny adatait sehova,

What should you do to avoid becoming a victim of such fraud?

- Handle unsolicited phone calls with care and caution!
- If you receive an urgent phone call with an urgent tone, always be sceptical! The more urgent the caller, the more suspicious you should be! Slow down and think carefully about what they are really asking for!
- If you suspect that you may be talking to a fraudster, disconnect the call as soon as possible and contact the relevant institutions for further action (e.g. your bank in case of a call disguised as a bank inquiry)!
- If you receive a suspicious phone call, do not give any personal details and disconnect the call!
- Never install software on your computer or phone at the request of others! Scammers often use the disguise of an anti-virus solution to try to persuade their victims to install an abusive program.
- When using AnyDesk software, never enter your personal sensitive data anywhere, as it can be easily stolen by criminals once they take control!

hiszen az irányítás átvételével könnyen ellophatják azokat a bűnözők!

- Jelenjen meg „piros jelzés” Önben, ha idegenek azt kérik, hogy lépjen be privát banki felületére!
- Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát (a weboldalán vagy online kereséssel), és lépjen vele kapcsolatba közvetlenül a bankkal!
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet, vagy kifejezetten a csaláshoz is létrehozhatták.
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről vagy a vállalatról, amelynek dolgozik, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adja meg, a válaszok másik felét pedig az ügyfél!
- Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy egyszer használható, második hitelesítési kódot! A bankok sosem kérik ezeket az információkat!
- Soha ne utaljon pénzt telefonon érkező kérésre! Egy bank sosem kér ilyet.
- A csalási szándékú hívásokat azonnal jelentse a bankjának!
- Ha netán mégis megkárosítottak bennünket, jelentsük a Rendőrségen az esetet!

- Be alerted if strangers ask you to log in to your private banking interface!
- Even if the phone number displayed is indeed the bank's customer service number, there is no guarantee that it is from there. To verify that the person is who they say they are, look up the organisation's phone number (on their website or by searching online) and contact the bank directly!
- To verify, do not use the phone number provided by the caller! The number may be fake or may have been created specifically for fraud.
- Fraudsters can easily obtain basic information about you or the company you work for online, for example by using your social media profiles. You cannot trust a caller just because they know this information.
- Even if you think the phone call is authentic, ask for a cross-identification, whereby the institution's administrator gives half of the answers to the questions asked (e.g. mother's name at birth) and the client gives the other half.
- Never give out your debit or credit card PIN, CVV code, online banking password or one-time use second authentication code! Banks never ask for this information!
- Never transfer money when asked to do so by phone! A bank will never ask for this.
- Report fraudulent calls to your bank immediately!
- If you become a victiom of a fraud, report it to the police!

16. CEO FRAUD, ÜZLETI E-MAIL KOMPROMMITÁCIÓ

A CEO csalás – más néven üzleti e-mail kompromittáció (*Business Email Compromise*, röviden BEC) – a kibertámadások egy kifinomult formája, amely során bűnözők magas rangú vállalati vezetők, például a vezérigazgató (CEO), a pénzügyi igazgató (CFO) vagy más megbízható vezető személyazonosságát hamisítják meg. Céljuk, hogy a vállalat alkalmazottait – leggyakrabban üzleti, pénzügyi, HR vagy adminisztratív területen dolgozó munkatársakat – megtévesszék annak érdekében, hogy pénzösszegeket utaljanak át, bizalmas információkat adjanak ki, vagy jogosulatlan műveleteket hajtsanak végre.

A csalók rendszerint alapos előkészítő munkát végeznek: feltérképezik a szervezeti felépítést, azonosítják a kulcsfontosságú személyeket, megfigyelik a vállalati partnereket, a folyamatban lévő projekteket, sőt a vezetők kommunikációs stílusát is tanulmányozzák. Ez a részletes háttérmunka lehetővé teszi számukra, hogy rendkívül meggyőző, hitelesnek tűnő üzeneteket készítsenek.

Ezek a támadások célzottak, nehezen felismerhetők, és súlyos pénzügyi veszteségeket, valamint jelentős hírnévbeli károkat okozhatnak, legyen szó akár kisvállalkozásról, akár nemzetközi nagyvállalatról.

Tipikus figyelmeztető jelek

A CEO csalás megelőzésének alapfeltétele a korai figyelmeztető jelek felismerése. A leggyakoribb intő jelek közé tartoznak:

- Szokatlan vagy sürgős kérések: A támadó azonnali intézkedést sürget, gyakran arra hivatkozva, hogy "rendkívüli helyzet" miatt a szokásos jóváhagyási folyamatot nem szükséges betartani.
- Titoktartásra való felhívás: Az üzenet hangsúlyozza, hogy az ügy szigorúan

16. CEO FRAUD, BUSINESS EMAIL COMPROMISE

CEO fraud — also known as Business Email Compromise (BEC) — is a sophisticated type of cyberattack where criminals impersonate high-ranking company officials such as the CEO, CFO, or another trusted executive. The aim is to deceive employees, typically those in business, finance, HR, or administration, into transferring funds, sharing sensitive corporate information, or carrying out unauthorized actions.

Fraudsters often spend significant time researching their target, learning about the organization's hierarchy, key individuals, partners, ongoing projects, and even the CEO's communication style. This reconnaissance enables them to craft convincing and targeted emails or messages that appear legitimate.

These attacks are highly targeted, difficult to detect, and can cause significant financial and reputational damage to organizations of all sizes, from small businesses to multinational corporations.

Typical Warning Signs

Recognizing the early signs of CEO fraud is crucial for prevention. Common indicators include:

- Unusual or Urgent Requests: Emails or messages claiming urgent action is needed, often asking to bypass standard processes "due to exceptional circumstances."
- Pressure for Secrecy: The attacker stresses that the matter must remain

bizalmas, és más kollégák vagy osztályok bevonása nem kívánatos.
- Gyanús e-mail címek: A feladó címe első ránézésre valósnak tűnhet, de apró eltéréseket tartalmazhat (például plusz karakterek, módosított domainek, elgépelések).
- Ismeretlen számlaszámok: A kérés új, ismeretlen – gyakran külföldi – bankszámlára történő utalásra szólít fel.
- Szokatlan nyelvezet vagy stílus: Az üzenet nyelvtani hibákat tartalmazhat, vagy a megszokottól eltérő hangnemben íródhat.
- Rossz időzítés: A csalók gyakran akkor támadnak, amikor a vezetők üzleti úton vannak, ünnepnapokon, hétvégéken vagy munkaidőn kívül, amikor a szokásos ellenőrzések nehezebben megvalósíthatók.

confidential and should not involve other colleagues or departments.
- Strange Email Addresses: The sender's email address may look similar but will have minor differences (e.g., extra characters, a different domain, or spelling errors).
- Unfamiliar Payment Details: Requests to transfer funds to new, unverified bank accounts, especially those located abroad.
- Odd Language or Tone: The message may have minor grammatical mistakes, or the tone may seem slightly off compared to the executive's usual style.
- Poor Timing: Requests often arrive when executives are traveling, during weekends, late at night, or around public holidays when verification may be more difficult.

Hogyan előzhető meg a CEO csalás?

A CEO csalás elleni védekezés hatékonysága a technikai megoldások, a munkatársak tudatossága és a szigorú belső eljárásrendek együttes alkalmazásán múlik. A legfontosabb megelőzési lépések:

- Ellenőrzési mechanizmusok bevezetése: Minden érzékeny vagy pénzügyi kérés esetében kötelező a független csatornán történő visszaellenőrzés – például ismert belső telefonszámon történő telefonhívással, nem pedig az e-mailben megadott elérhetőségen keresztül.
- Munkafolyamatok szétválasztása: Nagyobb értékű pénzügyi tranzakciók esetében több személy jóváhagyására legyen szükség, így egyetlen munkatárs sem dönthet egyedül jelentős kifizetésekről vagy érzékeny adatok kiadásáról.
- Folyamatos oktatás és tudatosságnövelés: Minden munkatársat – különösen a pénzügyi és adminisztratív területeken dolgozókat – rendszeresen oktatni kell a phishing támadások, a társadalmi

How to Prevent CEO Fraud?

Preventing CEO fraud requires a combination of technical controls, employee awareness, and strict internal procedures. Recommended measures include:

- Verification Procedures: Always verify sensitive or financial requests through an independent communication channel. For example, confirm via a phone call using a known internal number, not the number in the suspicious email.
- Segregation of Duties: Implement multi-step approval processes for financial transactions. No single individual should have authority to authorize large payments or sensitive actions alone.
- Employee Training and Awareness: Regularly train all employees, especially those handling finances or sensitive information, to recognize phishing, social engineering tactics, and CEO fraud

manipuláció (social engineering) és a CEO csalás veszélyeire.

- E-mail biztonság megerősítése:
  - E-mail hitelesítési technológiák (SPF, DKIM, DMARC) alkalmazása a hamisított levelek kiszűrésére.
  - Külső forrásból érkező levelek egyértelmű megjelölése figyelmeztető üzenettel.
  - A vállalat domainjéhez hasonló domainek folyamatos monitorozása.
- Nyilvános információk korlátozása: Minimalizálni kell a nyilvánosan elérhető szervezeti és személyes információk mennyiségét (például szervezeti ábrák, vezetői bemutatkozók), hogy a támadók ne tudják ezeket felhasználni a megtévesztés előkészítésére.
- Incidenskezelési terv kialakítása: Fontos, hogy minden munkatárs pontosan tudja, hogyan kell jelenteni a gyanús üzeneteket, és a szervezet rendelkezzen kidolgozott, begyakorolt eljárásrenddel a hasonló incidensek gyors és hatékony kezelésére.

attempts.

- Strengthen Email Security:
  - Deploy email authentication protocols like SPF, DKIM, and DMARC to protect against email spoofing.
  - Mark external emails clearly with a warning banner.
  - Monitor for lookalike domains.
- Protect Public Information: Limit the amount of organizational and personal information available online (e.g., organizational charts, leadership bios) that can be used by attackers for social engineering.
- Establish an Incident Response Plan: Ensure employees know exactly how to report suspicious communications, and have a well-practiced protocol for responding to fraud attempts quickly.

17. SZÁMLACSALÁS

A számlacsalás egy kifinomult csalási forma, amely során elkövetők megtévesztik a vállalatokat, és ráveszik őket, hogy kifizetéseiket hamis bankszámlákra teljesítsék.

A támadók gyakran egy ismert szállító nevében lépnek kapcsolatba a céggel, vagy egy meglévő kommunikációs szálat eltérítve manipulálják a számlaadatokat. Céljuk, hogy a vállalatok jóhiszeműen, de hibásan, közvetlenül a csalók számláira utaljanak összegeket.

A bűnözők alapos előkészületeket végeznek: feltérképezik az üzleti kapcsolatokat, beszállítói

17. INVOICE FRAUD

Invoice fraud is a type of financial scam where criminals trick businesses into transferring funds to fraudulent bank accounts by manipulating legitimate invoicing processes.

Typically, attackers either impersonate a known supplier or intercept genuine communications to alter payment details on invoices. Their goal is to deceive companies into unknowingly sending large payments to the attacker’s account instead of the legitimate supplier's.

Fraudsters often conduct thorough research to understand the relationships between companies

láncokat, és akár hosszabb ideig figyelik a levelezéseket is. Ezzel a háttérismerettel képesek rendkívül hiteles, a valódi számlákhoz szinte teljes mértékben hasonló hamis dokumentumokat előállítani.

and their vendors. They may monitor email correspondence, hack into supplier accounts, or send convincing fake invoices that closely mimic legitimate documents.

A számlacsalás jelentős anyagi veszteségeket és komoly reputációs károkat okozhat, függetlenül a cég méretétől vagy iparágától. Az elkövetők gyakran éppen a beszállítókkal kialakított többéves bizalmat használják ki.

Invoice fraud can cause substantial financial losses and damage to business relationships. It affects organizations of all sizes and sectors, often exploiting trust built up over years between companies and their regular partners.

Tipikus figyelmeztető jelek

A számlacsalás korai felismerése kulcsfontosságú a károk megelőzése érdekében. A leggyakoribb figyelmeztető jelek közé tartoznak:

- Bankszámlaadatok megváltoztatására irányuló váratlan kérések: Olyan üzenetek érkeznek, amelyekben a szállító új számlaszámot közöl, sürgetve az adatok azonnali frissítését.
- Kisebb eltérések a kommunikációban: A feladó e-mail címe kis mértékben eltér az ismerttől, vagy a megszokottól eltérő stílusban, furcsa szóhasználattal ír.
- Szokatlan fizetési instrukciók: Olyan átutalási utasítások, amelyek eltérnek a korábbi gyakorlattól, például új – különösen külföldi – bankszámlák megjelölése.
- Számlákban tapasztalható apró különbségek: A megszokott számlaképtől eltérő logó, cím, elérhetőség vagy formátum.
- Sürgetés és nyomásgyakorlás: Felszólítás azonnali kifizetésre, késedelmi díjak vagy üzleti kapcsolatok megszakításának kilátásba helyezésével.
- Kedvezőtlen időzítés: Az utalási kérések jellemzően akkor érkeznek, amikor a kulcsfontosságú munkatársak nincsenek elérhető közelségben – például ünnepek alatt, szabadságok idején vagy hónapzáráskor.

Typical Warning Signs

Recognizing the early indicators of invoice fraud is critical for effective prevention. Common warning signs include:

- Requests to Update Bank Account Details: An unexpected email or letter informing you that a supplier's bank account has changed, urging immediate updates.
- Slight Changes in Communication: Minor differences in the sender's email address, unfamiliar wording, or unusual urgency in payment requests.
- Unusual Payment Instructions: New payment destinations, especially international accounts, that differ from the ones previously used without proper justification.
- Invoice Discrepancies: Invoices that differ slightly from previous versions in terms of layout, logos, contact information, or reference numbers.
- Pressure for Immediate Payment: Messages insisting on urgent settlement of invoices to avoid supposed penalties or service interruptions.
- Poor Timing: Requests that arrive when key staff are unavailable, such as during holidays, business trips, or month-end processing rushes.

Hogyan előzhető meg a számlacsalás?

- A számlacsalás elleni védekezés átfogó megközelítést igényel, amely technológiai eszközöket, tudatosságnövelést és szigorú belső szabályokat is magában foglal. A legfontosabb megelőzési lépések:
- Bankszámlaváltozások független ellenőrzése: Minden számlaszám-módosítást kizárólag független, ismert csatornán (pl. telefonon, személyes megerősítéssel) szabad visszaigazolni – soha nem pusztán egy e-mail alapján.
- Beszállítói adatmódosítások hitelesítése: Hivatalos eljárásrend kidolgozása minden szállítói adatváltoztatás ellenőrzésére a fizetési folyamat előtt.
- Munkafolyamatok szétválasztása: A szállítói kommunikáció, a számlák jóváhagyása és a kifizetések lebonyolítása különböző munkatársakhoz tartozzon, így csökkentve a csalás kockázatát.
- Folyamatos munkatársi oktatás: A pénzügyi, beszerzési és adminisztrációs területeken dolgozó munkatársakat rendszeresen oktatni kell a csalási módszerek felismerésére és helyes kezelésére.

- E-mail biztonság erősítése:
  - E-mail hitelesítési protokollok (SPF, DKIM, DMARC) alkalmazása.
  - Külső forrásból érkező levelek egyértelmű figyelmeztető jelölése.
  - Hasonló domain-nevek figyelése és monitorozása.

- Pénzügyi tranzakciók rendszeres felülvizsgálata: A tranzakciók szúrópróbaszerű és rendszeres ellenőrzése segít kiszűrni a gyanús tevékenységeket.
- Beszállítói kapcsolatok tudatos kezelése: Részletes, naprakész beszállítói adatbázis

How to Prevent Invoice Fraud?

- Preventing invoice fraud requires vigilance, strong internal controls, and regular employee training. Recommended prevention measures include:
- Verification of Account Changes: Always independently verify requests for changes in bank account details, ideally through a known contact person and a trusted communication channel (never rely solely on email).
- Supplier Confirmation Procedures: Establish formal procedures for verifying the authenticity of any changes in supplier information before processing payments.
- Strict Segregation of Duties: Separate responsibilities so that different employees handle vendor communications, payment approvals, and payment processing.
- Employee Training and Awareness: Educate all staff involved in finance and procurement about invoice fraud tactics and how to spot suspicious invoices or payment requests.

- Email Security Measures:
  - Implement and enforce secure email protocols (SPF, DKIM, DMARC).
  - Flag external emails with a clear warning to increase awareness.
  - Monitor for suspicious domain registrations similar to trusted vendors.

- Monitor Financial Transactions: Regularly review financial transactions to identify unusual payments or anomalies.
- Supplier Management: Maintain up-to-date supplier records and establish clear, documented communication paths with key vendors.

fenntartása, és világos, előre meghatározott kommunikációs csatornák kijelölése.
- Gyors reagálás biztosítása: Minden munkatársnak pontosan ismernie kell, hogyan kell jelenteni a gyanús eseteket, és a szervezetnek rendelkeznie kell gyors és hatékony incidenskezelési protokollal.

- Incident Response Plan: Ensure that all employees know how to report suspected fraud attempts quickly, and have an action plan in place to minimize potential damages.

18.ÜZLETI IDENTITÁSLOPÁS

Az üzleti identitáslopás során csalók egy vállalkozás hivatalos adatait – például a cég nevét, cégjegyzékszámát, adószámát, bankszámlaszámát vagy logóját – jogosulatlanul használják fel saját bűncselekményeikhez.

A cél általában az, hogy a megtévesztett harmadik felektől árut, szolgáltatást, hitelt, támogatást vagy egyéb pénzügyi előnyt szerezzenek, úgy, hogy az igazi vállalkozás ne is tudjon róla, vagy ne járuljon hozzá.

Ez a típusú csalás az érintett vállalkozás számára súlyos anyagi károkat, jogi következményeket és komoly reputációs veszteséget okozhat.

Hogyan történik az üzleti identitáslopás?

Az elkövetők jellemzően:

- Nyilvánosan elérhető adatokat (pl. cégadatbázisok, hivatalos bejegyzések) gyűjtenek össze a cégről.
- Hamis weboldalakat, e-mail címeket vagy hivatalosnak tűnő dokumentumokat hoznak létre az eredeti cég nevében.
- Hamis megrendeléseket adnak le, szállítmányokat rendelnek meg, vagy hiteleket vesznek fel az eredeti cég nevében.
- Adót érintő visszaéléseket követnek el, például csalárd adóvisszatérítést igényelnek.

18. BUSINESS IDENTITY THEFT

Business identity theft occurs when criminals unlawfully use a company’s official information — such as its name, registration number, tax ID, bank account details, or brand identity — to commit fraud.

The goal is typically to obtain goods, services, loans, grants, or other financial advantages without the genuine company's knowledge or consent.

This type of fraud can cause severe financial losses, legal consequences, and significant reputational damage to the affected business.

How Does Business Identity Theft Happen?

Fraudsters typically:

- Collect publicly available information (e.g., from company registries or official filings).
- Create fake websites, email addresses, or documents that closely resemble the legitimate company’s communications.
- Place fraudulent orders, arrange shipments, or take out loans in the company’s name.
- Commit tax-related fraud, such as filing for false refunds.
- Deceive clients or partners by impersonating the original business.

- Ügyfeleket vagy partnereket tévesztenek meg az eredeti vállalkozás arculatával.

Tipikus figyelmeztető jelek

- Furcsa, ismeretlen megrendelések: A cég nevére vagy bankszámlájára történő, nem várt szállítási vagy pénzügyi tranzakciók.
- Értesítések új hitelekről vagy számlákról: Olyan banki, pénzügyi vagy szolgáltatói értesítések, amelyeket a vállalat nem kezdeményezett.
- Partnerek visszajelzései: Ügyfelek vagy szállítók jelzik, hogy gyanús üzeneteket kaptak a vállalkozás nevében.
- Hivatalos figyelmeztetések: Hatóságoktól érkező értesítések adótartozásról, hitelfelvételről vagy jogi eljárásról, amelyről a vállalat nem tud.

Hogyan előzhető meg az üzleti identitáslopás?

- Céginformációk tudatos kezelése: Csak a szükséges információkat osszuk meg nyilvánosan, például weboldalon, cégtárban.
- Digitális jelenlét védelme: A cég hivatalos weboldalát, e-mail címét, közösségi profiljait rendszeresen ellenőrizni és védeni kell.
- Domain nevek regisztrációja: A hasonló nevű domain-ek előzetes lefoglalása csökkentheti a visszaélés lehetőségét.
- Ügyfelek és partnerek tájékoztatása: Világosan kommunikálni kell, milyen hivatalos csatornákon történik a kapcsolatfelvétel.
- Számlázási és pénzügyi folyamatok védelme: Minden nagyobb tranzakció vagy partnerkapcsolat esetében javasolt független ellenőrzést végezni.
- Figyelőszolgáltatások igénybevétele: Cégfigyelő és hitelminősítő rendszerek segíthetnek időben észlelni a szokatlan aktivitást.

Typical Warning Signs

- Unexpected orders or transactions: Receiving shipments or financial notices for transactions the company did not initiate.
- New loans or accounts: Notifications about loans, credits, or services opened in the company's name without authorization.
- Feedback from clients or partners: Business partners report suspicious communications supposedly coming from the company.
- Official warnings: Notices from tax authorities, banks, or courts regarding activities the company was unaware of.

How to Prevent Business Identity Theft?

- Manage corporate information carefully: Limit the amount of sensitive business information shared publicly.
- Protect your digital presence: Regularly monitor and secure your company’s official website, email addresses, and social media accounts.
- Register similar domain names: Secure domains that resemble your company's name to prevent impersonation.
- Communicate clearly with clients and partners: Establish and publicize official communication channels.
- Secure financial and invoicing processes: Verify significant transactions and new partnerships through independent checks.
- Use monitoring services: Business monitoring and credit alert services can help detect unusual activity early.

- Gyors reagálás: Gyanú esetén azonnal értesíteni kell a hatóságokat, a partnereket és a pénzügyi szolgáltatókat.

Felhívjuk Ügyfeleink figyelmét, hogy a fenti csalástípusokon túl a Kiberpajzs honlapján (www.kiberpajzs.hu) további hasznos és folyamatosan frissülő információkat találnak!

- Respond quickly: In case of suspicion, immediately alert authorities, partners, and financial institutions.

Please note that in addition to the above types of fraud, you can find more useful and up-to-date information on the CyberShield/Kiberpajzs website (www.kiberpajzs.hu)!