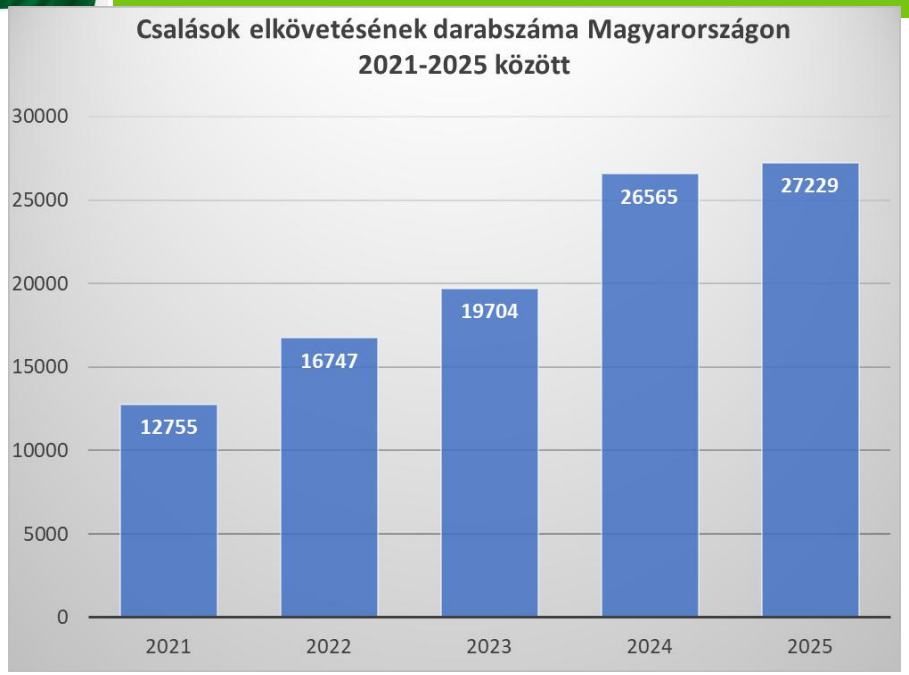
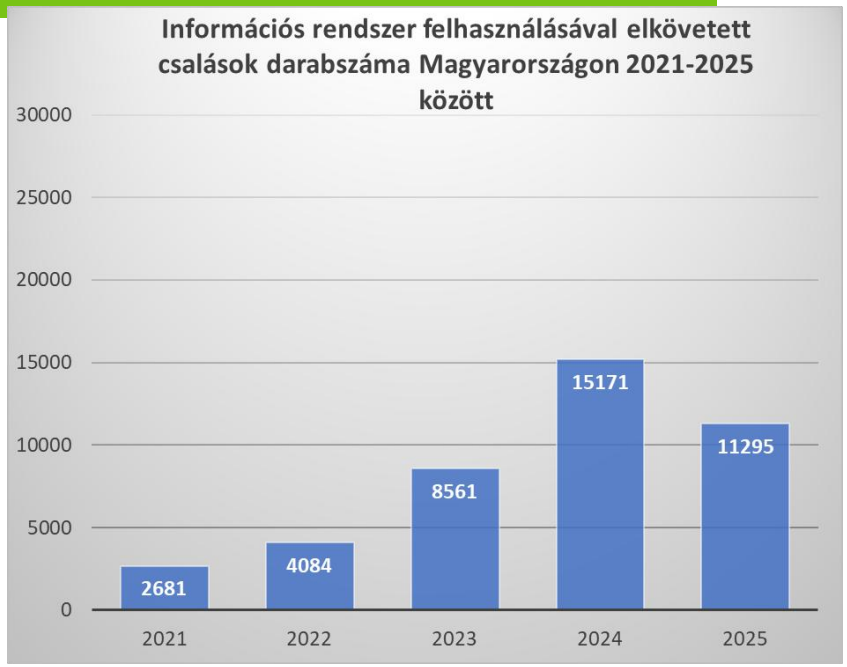
Az online csalások elkövetési módszerei, hogyan védekezzünk és hogyan előzzük meg őket: a megelőzés dimenziói

Az elkövetett online csalások dinamikája



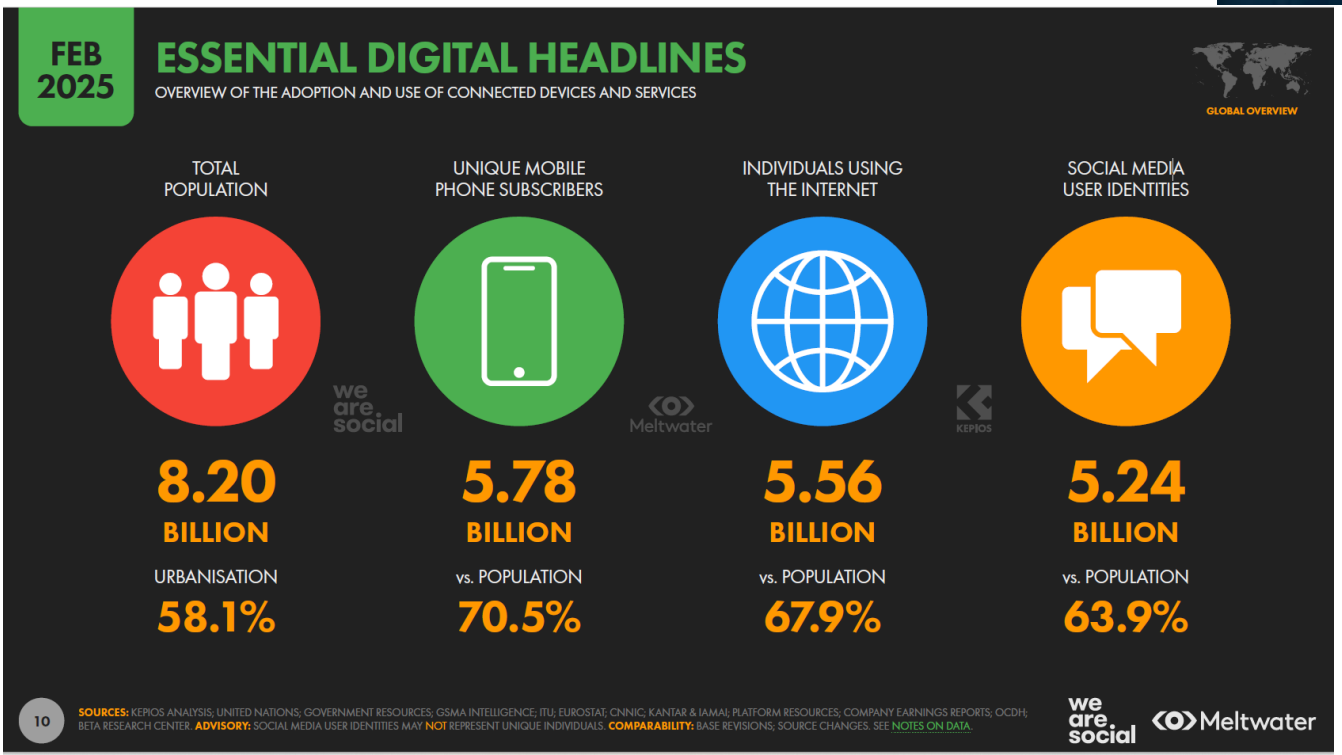


A csalások és azon belül is az információs rendszerek felhasználásával elkövetett csalások száma az elmúlt években folyamatosan nőttek, azonban 2025. évben mintegy 20 %-os csökkenés figyelhető meg.

Az elkövetett bűncselekmények vizsgálati szempontja és megértése

A bűncselekmények vizsgálata (kiberbűnözés és online csalás)

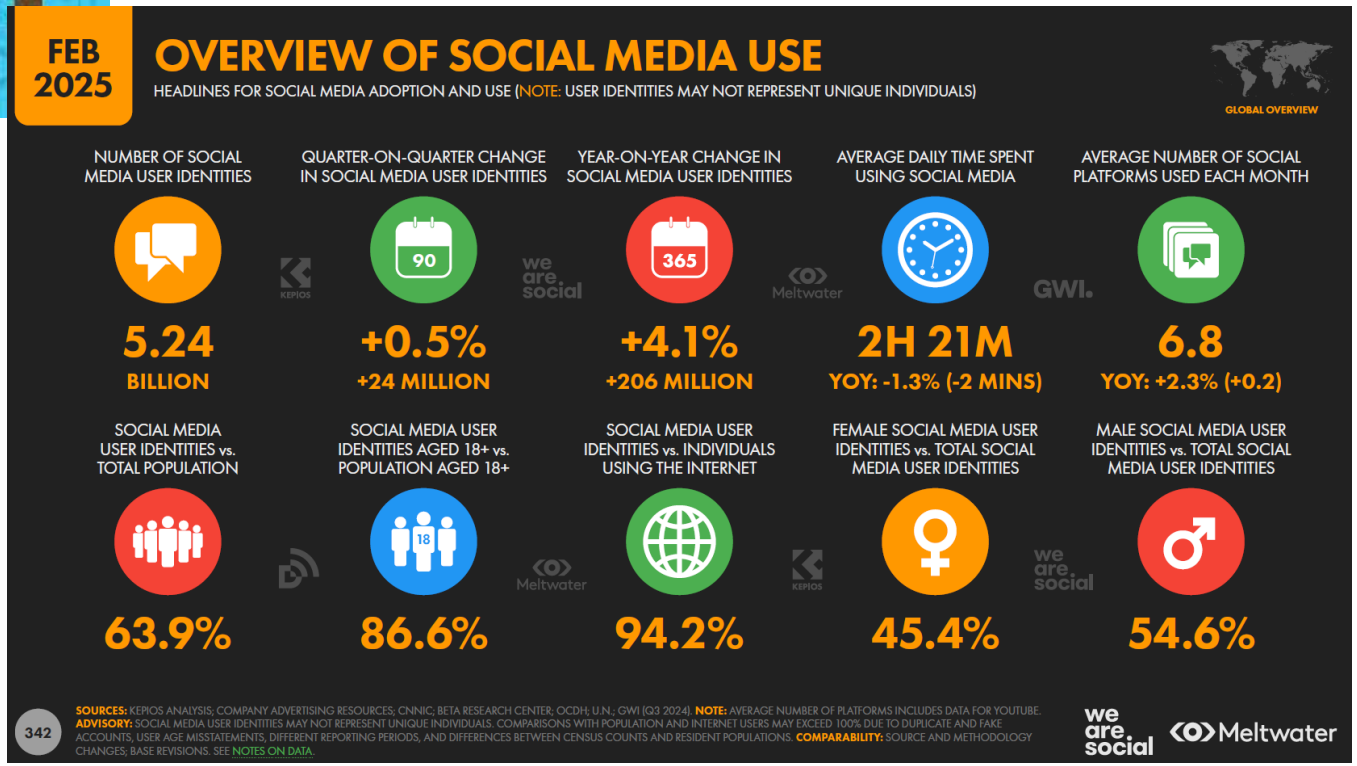
-elkövetői oldal
- sértetti oldal
-pénzintézeti oldal
- állami társadalmi szerepvállalás



Sértettioldal:

-A felgyorsult világ, információdömping és felületes értelmezés

- IKT rendszerek robbanásszerű fejlődése és az információ technológiai lemaradás



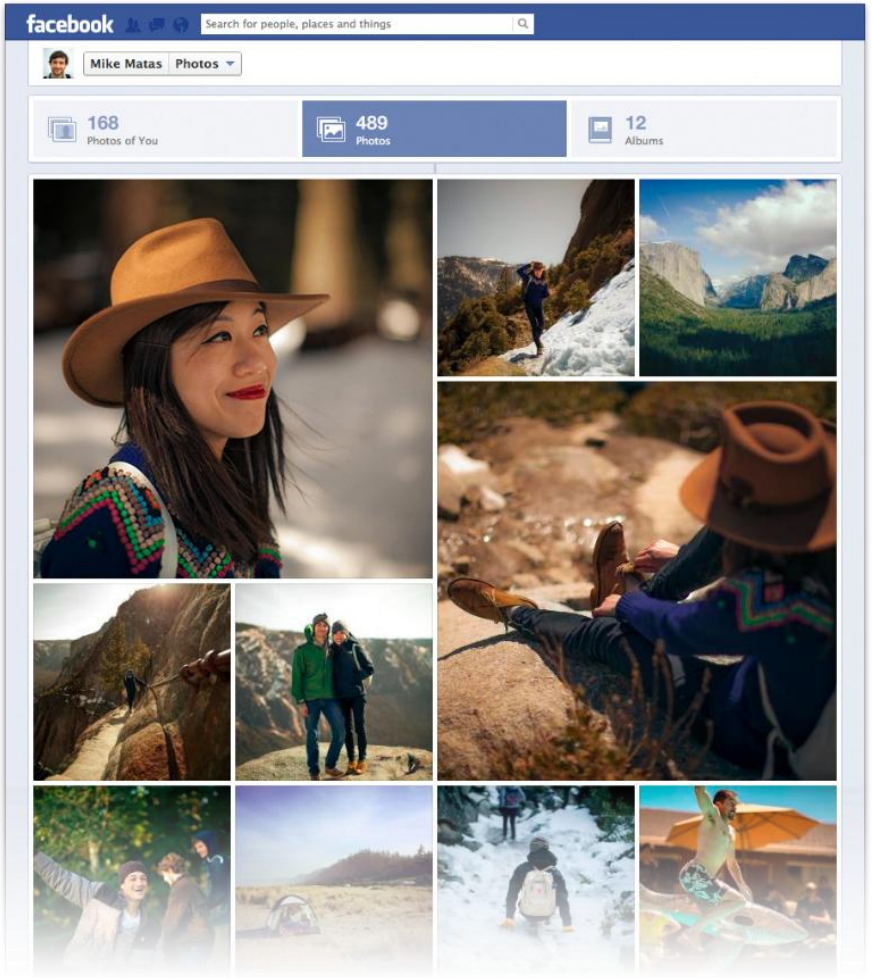
Sértetti oldal:

- kényelem és biztonság

- a közösségi média általi kitárulkozás és a határvonalak elmosódása:

- az online platformon és a közösségi médián által közvetített információk hitelessége

-manipuláció



Sértetti oldal:

- az emberi tényezők

- a jellemző emberi tulajdonságok

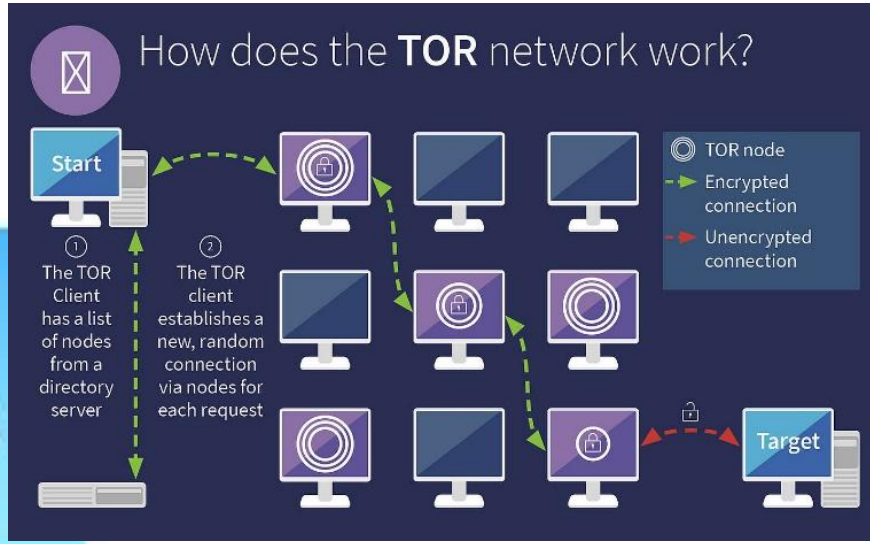
-az élethelyzetek

Elkövetői oldal:

- a bűnelkövetői csoportok törekvéseinek változása

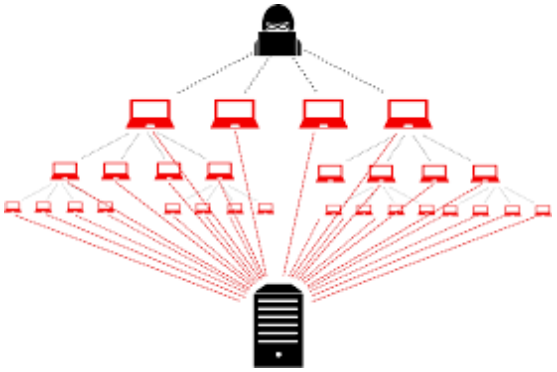
- bűnözői csoportok specializálódása az online csalások elkövetésére

- kockázatkerülés és kockázatcsökkentés



Kibertámadások általi fenyegetések

Főbb fenyegetések a kibertérben:



-Elosztott szolgáltatásmegtagadási (DDoS) támadások: Ezek a támadások túlterhelik a célzott rendszereket, szolgáltatásokat, weboldalakat, így azok elérhetetlenné válnak a felhasználók számára.

- Adatszivárgások és adatlopások: A támadók érzékeny információkat szereznek meg, például felhasználói adatokat, pénzügyi információkat vagy szellemi tulajdont.

- Zsarolóvírus (ransomware) támadások: A kiberbűnözők titkosítják az áldozat adatait, és váltságdíjat követelnek a visszaállításért. Bár konkrét októberi esetekről nincs információ, a zsarolóvírusok továbbra is jelentős fenyegetést jelentenek.

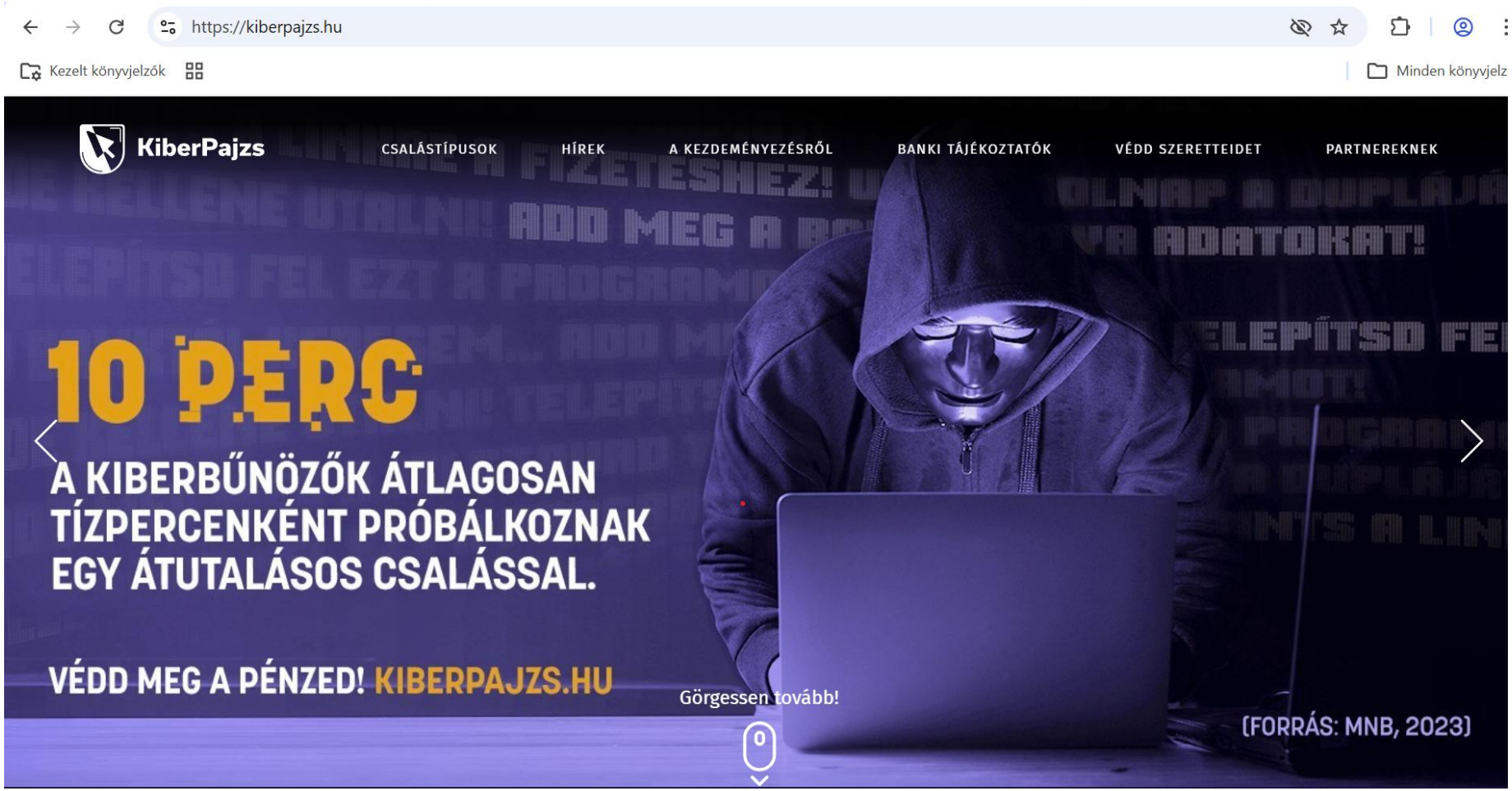
- Adathalász (phishing) támadások: A támadók megtévesztő e-mailekkel vagy weboldalakkal próbálják megszerezni a felhasználók bizalmas adatait, például jelszavakat vagy banki információkat. Ezek a támadások gyakran kihasználják az aktuális eseményeket vagy híreket a hitelesség növelése érdekében.

Pénzintézeti oldal, megelőzési tevékenység:

A csalások kezelése, megelőzési tevékenysége és az operatív intézkedések során a monitoring tevékenység, az egycsatornás információáramlás, az események azonnali, valós időben történő kezelése és a bevezetett intézkedések meghozatala egységes koordináció keretében történik. Az észlelést követően, vagy a jelzést követően az esetek kezelése és lezárása az elejétől a végéig egy kézben van.

Kommunikáció, edukáció és biztonságtudatosság: Az online csalások elleni küzdelem, az írott és az elektronikus, valamint a közösségi média felületein nagyobb intenzitással és bővebb tartalommal jelent meg, beleértve a banki felületeken kialakított figyelemfelhívó és edukációs tartalmakat.

Kiberpajzs


https://kiberpajzs.hu
Kezelt könyvjelzők
Minden könyvjelz
KiberPajzs
CSALÁSTÍPUSOK
HÍREK
A KEZDEMÉNYEZÉSRŐL
BANKI TÁJÉKOZTATÓK
VÉDD SZERETTEIDET
PARTNEREKNEK
10 PERC
A KIBERBŰNÖZŐK ÁTLAGOSAN TÍZPERCENKÉNT PRÓBÁLKOZNAK EGY ÁTUTALÁSOS CSALÁSSAL.
VÉDD MEG A PÉNZED! KIBERPAJZS.HU
Görgessen tovább!
(FORRÁS: MNB, 2023)

Társadalmi szerepvállalás - Kiberpajzs:

A digitalizáció ugrásszerű térnyerése a bővülő pénzügyi szolgáltatási kör mellett az ügyfelek oldalán is egyre nagyobb nyitottságot eredményezett.

Mindezzel párhuzamosan fokozatosan növekszik a digitális térben elkövetett pénzügyi visszaélések száma is.
A pénzügyi rendszer biztonságosan működik, főként az ügyfeleket célozzák, nem pedig az informatikai rendszereket.

Emiatt a piaci szolgáltatók technikai védelme mellett kiemelten fontos az ügyfelek pénzügyi tudatosságának erősítése is.

A pénzügyi szolgáltatók is felelősek az ügyfeleik és azok pénzügyi eszközeinek biztonságáért.

Kiemelt jelentősége van, hogy maguk az ügyfelek is felkészültek legyenek az online térben megjelenő veszélyekkel kapcsolatban: a megfelelő ismeretek birtokában pénzügyeiket kellő óvatossággal kezeljék a különböző digitális eszközökön és csatornákon, valamint tudatában legyenek a digitális eszközök használatából eredő kockázatoknak, és a veszélyt a lehető leggyorsabban felismerve képesek legyenek ellenállni a támadásoknak.

A közös felelősség közös fellépés a kiberbűnözés és az online bűncselekményekkel szemben,

2022 őszén KiberPajzs néven közös kommunikációs és edukációs kampány

A szervezetek az együttműködés során folyamatosan vizsgálják a fogyasztói szokásokat, azok változásait, valamint a pénzügyek, illetve a pénzforgalom lebonyolítása kapcsán megfigyelhető visszaélési mintázatokat és kiberbiztonsági kockázatokat.

Figyelembe veszik a nemzetközi trendeket, szakmai munkájukba beépítik ezeket a tapasztalatokat, amelyeket végső soron a pénzügyi rendszer biztonságának, valamint az ügyfelek pénzügyi tudatosságának növelésére fordítanak.

A KiberPajzs projekt egyik legfontosabb célja a tájékoztatás, az edukáció, az ügyfelek és felhasználók figyelmének felhívása az online tér pénzügyi biztonságot veszélyeztető kockázataira, hogy az elsajátított ismeretek segítségével a lehető legteljesebb pénzügyi tudatosság alakuljon ki a digitális pénzügyi szolgáltatásokat használó lakosság körében.

KiberPajzs
Védelem a pénzügyekben

Emellett fontos cél az is, hogy a pénzügyek lebonyolításában részt vevő intézmények, valamint a bűnüldöző szervek és egyéb hatóságok információt és tapasztalatot tudjanak cserélni egymással, ezáltal hatékonyabbá téve a visszaélések elleni harcot.

Kik vesznek részt a KiberPajzs projektben?

Magyar Nemzeti Bank

A pénzügyi szolgáltatások igénybevételének előfeltétele a biztonságos és fejlett digitális pénzügyi infrastruktúra. Ennek felügyelete és a működéshez szükséges szabályozás kialakítása a Magyar Nemzeti Bank feladata. A KiberPajzs program alapítójaként az MNB célja, hogy segítse a felhasználóknak felismerni a digitális eszközökben és az online térben rejlő kiberkockázatokat, és tanácsokkal szolgáljon azok felismeréséhez és kezeléséhez.

Rendőrség

A rendőrség alapvető feladata a bűncselekmények megakadályozása, felderítése, a közrend és a közbiztonság, az államhatár rendjének védelme. Nagy hangsúlyt fektetünk a közösségi és virtuális terek rendjének védelmére. Azért csatlakoztunk a KiberPajzs programhoz, mert meggyőződésünk, hogy együttes erővel hatékonyabban lehet fellépni a bűnözőkkel szemben, eredményesebbek lehetünk az áldozattá válás megelőzésében.

Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet

Cél a magas színvonalú kiberbiztonság megvalósítása, különös tekintettel a közigazgatási szervek és a létfontosságú rendszerelemek terén. Emellett fő küldetésünk segíteni az emberek védekezését a kibertérben zajló visszaélésékkel szemben és felkészülését a jövő kiberbiztonsági kihívásaira.

Nemzeti Média- és Hírközlési Hatóság

Az NMHH kiemelt célja a biztonságos internethasználat elősegítése. A Hatóság a médiaigazgatási feladatok mellett ellátja, az elektronikus hírközlési, a postai, valamint a bizalmi szolgáltatások felügyeletét, e területeken közreműködik a tudatos fogyasztói döntéshozatal kultúrájának fejlesztésében.

Magyar Bankszövetség

A Magyar Bankszövetség a KiberPajzs program egyik kezdeményezője és társ-projektgazdája. Az MBSZ több mint 50 tagintézménye a teljes magyar bankszektort lefedi. Az összes hazai pénzintézet összefogásával, kiemelt figyelemmel munkálkodunk a korszerű digitális pénzügyi megoldásokért és a digitális térben is az ügyfelek pénzügyi biztonságáért. KiberPajzsot kovácsolunk piaci, hatósági és kormányzati intézmények összefogásában – a védekezés tudatosságát, kulcsát adva az Ügyfél kezébe.

IgazságügyiMinisztériumAz Igazságügyi

Minisztérium két területe, a fogyasztóvédelem és az áldozatsegítés is érdemben foglalkozik az online térben bekövetkezett jogsértések kezelésével. A szakterületek kiemelt feladata a prevenció és az edukáció, valamint a bűncselekmények áldozatainak történő segítségnyújtás.

Csalások kezelése, megelőzési tevékenység

Pénzügyi Békéltető TestületA Pénzügyi Békéltető Testület a Magyar Nemzeti Bank által működtetett, bíróságon kívüli, alternatív vitarendezési fórum, amely 2011. július 1-je óta nyújt lehetőséget a fogyasztók és az MNB által felügyelt pénzügyi szolgáltatók közötti pénzügyi tárgyú fogyasztói jogviták békés rendezéséhez.

Szabályozott Tevékenységek Felügyeleti HatóságaA Szabályozott Tevékenységek Felügyeleti Hatósága nemzeti kiberbiztonsági tanúsítási hatóságként és általános kiberbiztonsági felügyeletként a kiemelt ágazatokban működő vállalkozások és az állampolgárok magas biztonsági szintjének elérését segíti.

PÉNZÜGYI BÉKÉLTETŐ TESTÜLET

SZTFH

Szabályozott Tevékenységek Felügyeleti Hatósága

Nemzetgazdasági MinisztériumA Nemzetgazdasági

Minisztérium, mint a nemzeti pénzügyi szolgáltatásokért, valamint a pénz-, tőke- és biztosítási piac szabályozásáért felelős intézmény, elkötelezett a háztartások, családok és diákok pénzügyi edukációja és védelme mellett, miközben prioritásként kezeli a pénzügyi tudatosság és a digitális biztonság megerősítését.

NEMZETGAZDASÁGI MINISZTÉRIUM

Magyar Államkincstár

A Magyar Államkincstár országos hatáskörű központi költségvetési szerv. Feladatai közé tartozik a társadalombiztosítási és családtámogatási ellátórendszerek működtetése, a közpénzek ellenőrzött kifizetése. Piacvezetőként a lakossági állampapír piacon célja, hogy ügyfelei kiberbiztonsági tudatosságát támogassa, és az értékpapírszámlák védelmét biztosítsa.

Magyar Államkincstár

Csalások kezelése, megelőzési tevékenység

Nemzeti Védelmi Szolgálat

A Nemzeti Védelmi Szolgálat a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, amelynek speciális kiberfelderítési egysége a nyomozóhatóságokkal szorosan együttműködve veszi fel a harcot a bűnözőkkel. Az online térben elkövetett bűncselekmények felderítéséhez és visszaszorításához elengedhetetlen a szoros együttműködés, amelyhez jelentős támogatást biztosít a Kiberpajzs.

Mastercard

A Mastercard globális technológiai vállalatként vezető szerepet játszik a biztonságos digitális fizetési rendszerek és kiberbiztonsági megoldások fejlesztésében. Piacvezetőként egyaránt elkötelezett a hazai elektronikus fizetési ökoszisztéma fejlődése és védelme iránt. A KiberPajzs programmal való együttműködés célja, hogy növelje a felhasználói tudatosságot, támogassa a digitális tér kockázatainak kezelését, és elősegítse a fenntartható, biztonságos online pénzügyi környezet kialakítását.

Csalások kezelése, megelőzési tevékenység

Szerencsejáték Zrt.A Szerencsejáték Zrt.
100 százalékos állami tulajdonban lévő szerencsejáték-szervező gazdasági társaság. Felelős játékszervezőként a vállalat fő célja, hogy a játék valóban játék maradjon, ezért számos szemléletformáló területen, köztük a kiberbiztonsági tudatosság elmélyítésében is kiemelt szerepet vállal.

VISA
A Visa a világ egyik vezető digitális fizetési szolgáltatója, több mint 200 országban segíti a tranzakciókat a fogyasztók, kereskedők, pénzügyi intézmények és kormányzati szervezetek között. A Visa folyamatosan fektet a legújabb technológiákba a csalások észlelésére és megelőzésére, és már 30 éve alkalmaz mesterséges intelligenciát használó megoldásokat a csalásfelderítésben. A Visa nemzetközi tapasztalatával is képes segítini a helyi fogyasztók védelmét, globális tudását és nemzetközi legjobb gyakorlatait hozva a Kiberpajzs együttműködésbe.

Befektető-védelmi Alap

A Befektető-védelmi Alap (BEVA) törvény alapján működő, önálló jogi személy, amely a tagjai befizetéseiből finanszírozott kártalanítási rendszert működtet. Feladata, hogy meghatározott összeghatárig kártalanítást nyújtson abban az esetben, ha valamely tagja fizetésképtelenné válik, és az ügyfelek jogszabályban meghatározott követeléseit fedezet hiányában nem képes teljesíteni. Az online pénzügyi csalások egyik gyakori formája a megtévesztésen alapuló befektetési csalás. Ilyen esetben intézményesített védelem nem áll rendelkezésre, ezért különösen fontos a körültekintő befektetői magatartás. A KiberPajzs támogató partnereként a BEVA a pénzügyi tudatosság erősítésével és – kiemelten a befektetési csalásos - visszaélések elleni fellépés támogatásával járul hozzá a pénzügyi rendszer stabilitásához és a befektetői bizalom fenntartásához.

honlapját és főbb elérhetőségeit.

Csalások kezelése, megelőzési tevékenység

Banki tájékoztatók

- a károk mérséklése érdekében első lépésként

- a bankot kell tájékoztatni.

- a lehető leghamarabb kell cselekedni.

Bank neve	Honlap	Telefonszám	E-mail cím
CIB Bank Zrt.	Honlap	+36 1 4 242 242 9-es gomb	cib@cib.hu
DUNA TAKARÉK BANK Zrt.	Honlap	+36 80 900 900	visszaeles@mbhdunabank.hu
ERSTE BANK HUNGARY Zrt.	Honlap	+36 1 302 5885	erste@erstebank.hu
GRÁNIT Bank Zrt.	Honlap	+36 1 510 0527 vagy +36 70 960 9871 11-es menüpont	info@granitbank.hu
KDB Bank Európa Zrt.	Honlap	+36 1 473 4440 vagy +36 1 374 9990	info@kdbbank.eu
Kereskedelmi és Hitelbank Zrt.	Honlap	+36 1/20/30/70 335 3355	bank@kh.hu
MagNet Magyar Közösségi Bank Zrt.	Honlap	+36 1 766 4544	info@magnetbank.hu
Magyar Cetelem Bank Zrt.	Honlap	+36 1 458 6070	cetelem@cetelem.hu
MBH Bank Nyrt.	Honlap	+36 80 350 350	ugyfelszolgalat@mbhbank.hu

Csalások kezelése, megelőzési tevékenység

KDB Bank Európa Zrt.	Honlap	+36 1 473 4440 vagy +36 1 374 9990	info@kdbbank.eu
Kereskedelmi és Hitelbank Zrt.	Honlap	+36 1/20/30/70 335 3355	bank@kh.hu
MagNet Magyar Közösségi Bank Zrt.	Honlap	+36 1 766 4544	info@magnetbank.hu
Magyar Cetelem Bank Zrt.	Honlap	+36 1 458 6070	cetelem@cetelem.hu
MBH Bank Nyrt.	Honlap	+36 80 350 350	ugyfelszolgalat@mbhbank.hu
Oberbank AG Magyarországi Fióktelep	Honlap	+36 1 211 0202 vagy +36 1 373 3399	EBSupport_HU@oberbank.hu
OTP Bank Nyrt.	Honlap	+36 1 366 6800	informacio@otpbank.hu
Polgári Bank Zrt.	Honlap	+36 1 373 3399	csalasmegelozes@polgaribank.hu
Raiffeisen Bank Zrt.	Honlap	+36 80 488 588	adathalasz@raiffeisen.hu
UniCredit Bank Hungary Zrt.	Honlap	+36 1/20/30/70 325 3200	info@unicreditgroup.hu

Hírek, figyelmeztetések

FIGYELMEZTETÉSEK

HÍREK

SZŰRŐK

Ez a hat leggyakoribb Apple Pay-csalás: így lehet kivédeni

2026. ÁPRILIS 9. CSÜTÖRTÖK

A rendőrség soha nem kér pénzt vagy banki adatokat

2026. ÁPRILIS 8. SZERDA

Elkövetési módszerek ismertetése

Telefonos

- Hamis banki telefonhívás (vishing)
- Nem banki szolgáltatók nevével történő visszaélés
- Visszahívásos telefonos csalás (wangiri)
- Hívószám-hamisítás (spoofing)
- Munkahelyi csalás: hamis vezetői utasítás e-mailben vagy telefonon
- Munkahelyi csalás: hamis ügyfél vagy beszállító

Számítógépes

- Lándzsás adathalászat (spear phishing)
- Hamis befektetési lehetőségek
- Hamis online webáruházak, ajánlatok
- Eladók átverése az online piactereken
- Személyesadat-lopás a közösségi médiában
- Hamis szolgáltatói ügyintézés a közösségi médiában (Angler phishing)
- Hamis tranzakciók jóváhagyása

SMS-es

- Hamis banki SMS (smishing)
- Nem banki szolgáltatók nevével történő visszaélés

E-mailes

- Adathalász banki e-mail (phishing)
- Nem banki szolgáltatók nevével történő visszaélés
- "Nigériai típusú" csalások
- Hamis befektetési lehetőségek
- Munkahelyi csalás: hamis vezetői utasítás e-mailben vagy telefonon
- Munkahelyi csalás: hamis ügyfél vagy beszállító

Az egyik legfontosabb cél:
- a tájékoztatás, az edukáció, az ügyfelek és felhasználók figyelmének felhívása az online tér pénzügyi biztonságot veszélyeztető kockázataira,
- a lehető legteljesebb pénzügyi tudatosság alakuljon ki a digitális pénzügyi szolgáltatásokat használó lakosság körében.
- a digitális biztonsági alapismeretek fontossága
- körültekintés és a megszerzett alapismeretek védelmet nyújthatnak a pénzügyekben.

Csalások kezelése, megelőzési tevékenység

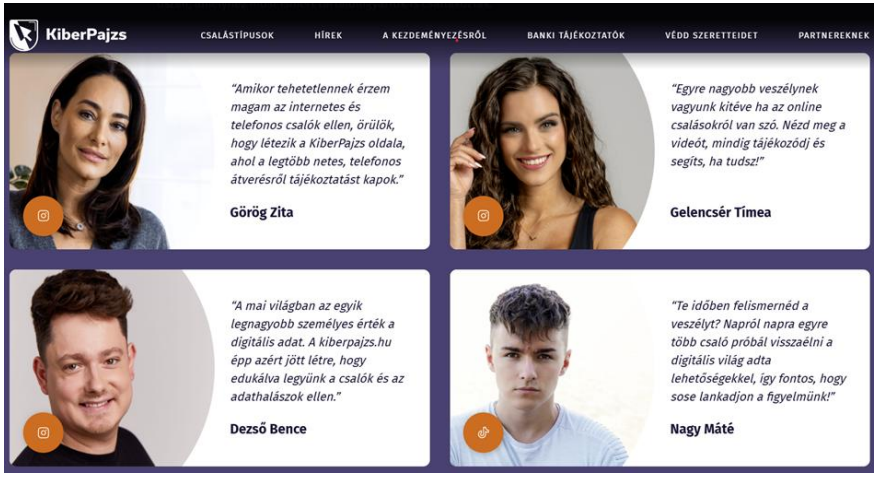
Hogyan védhetjük meg magunkat és egymást?
Ismered a módszereiket?

A KiberPajzs weboldala folyamatosan új információkkal frissül a legújabb csalási módokról.

Hívjuk fel a figyelmet: Hallottál egy új csalási formáról? Fura SMS-t kaptál? Levágós sztorival hívtak telefonon? Meséld el családtagjaidnak, barátaidnak is.

Ha már megtörtént a baj: Jelenteni a számlavezető bankjánál az esetet, bejelenteni a rendőrségen.

Nem ciki megosztani: A csalások áldozatai rendszerint magukat hibáztatják, tabuként kezelik a témát, nem beszélnek az élményeikről.



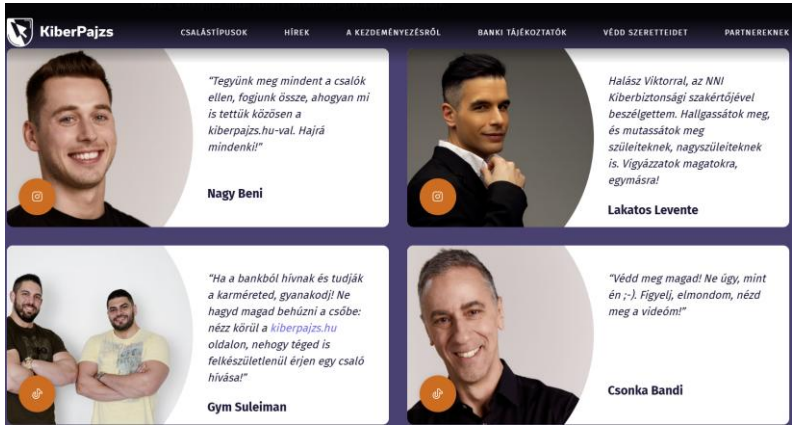
Csalások kezelése, megelőzési tevékenység

Miért fontos a beszélgetés?
Sokan, főleg az idősebbek még nincsenek tudatában a veszélyeknek, vagy nem tudják pontosan hogyan védekezhetnek a csalókkal szemben.

Védjük meg magunkat és szeretteinket a csalóktól:

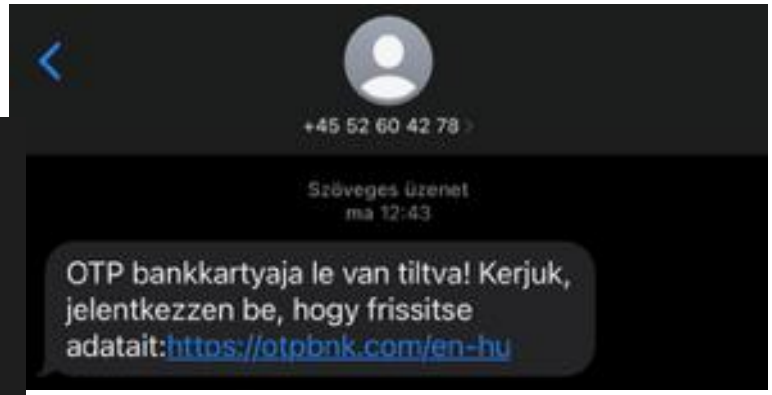
-ismerjük meg a módszereiket
- vértezzük fel szeretteinket az átverésekkel szemben

Együtt erősebbek vagyunk a csalóknál!



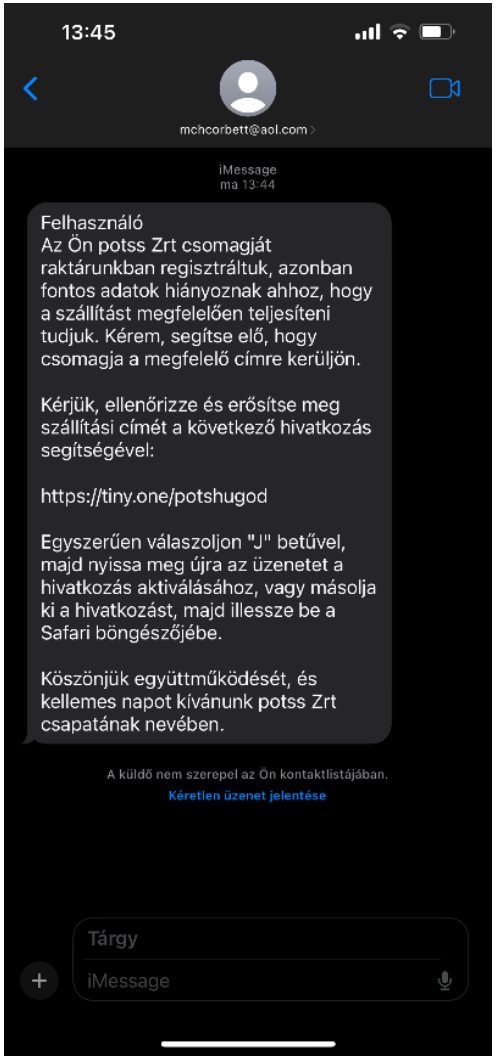
Elkövetési módszerek

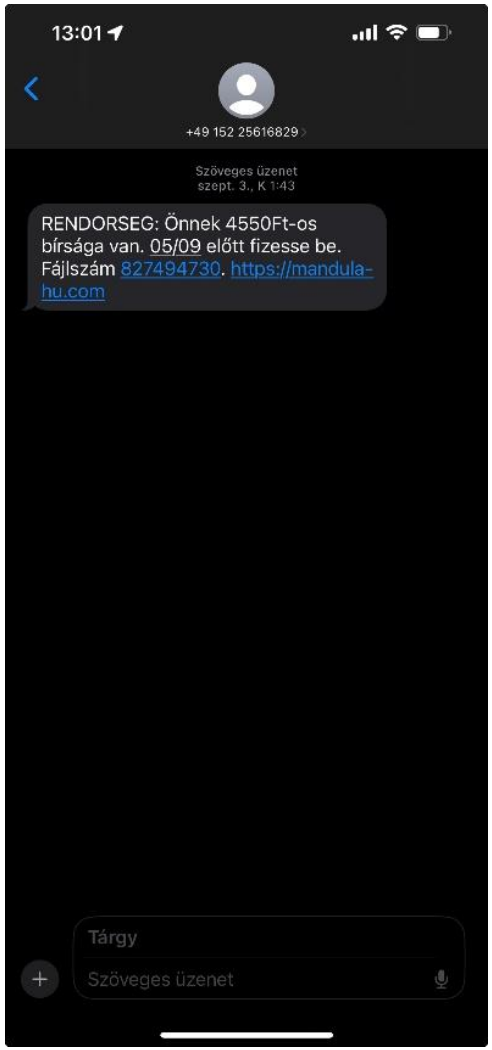
Banki sms, más szolgáltatótól vagy rendőrségtől e-mail üzenet: bankkártyája tiltva, hamis linken keresztül megadják fizetési adataikat és a megerősítő kódot vagy a megerősítő kódot banki alkalmazottként csalják ki tőle, úgy hogy a kapott üzenetre hivatkoznak



Elkövetési módszerek

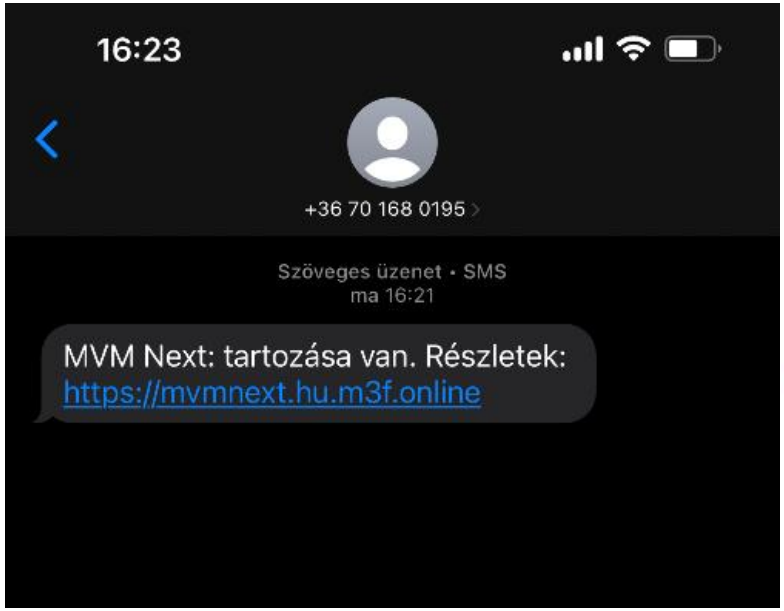
Hamis weboldalra navigáló linket tartalmazó üzenet és adathalász weboldalakra irányító üzenetek: csomagja érkezett…

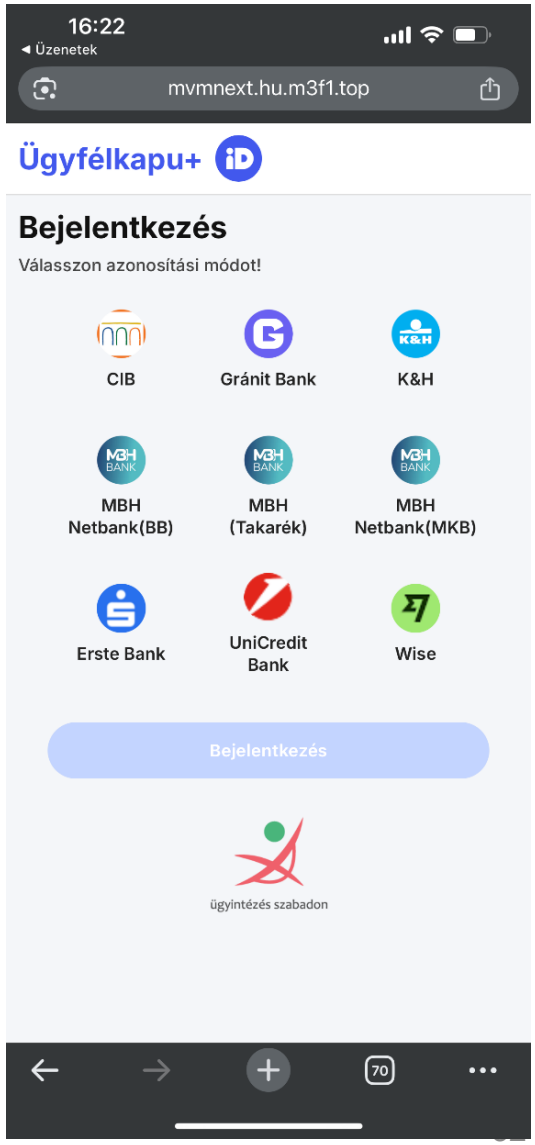




Elkövetési módszerek

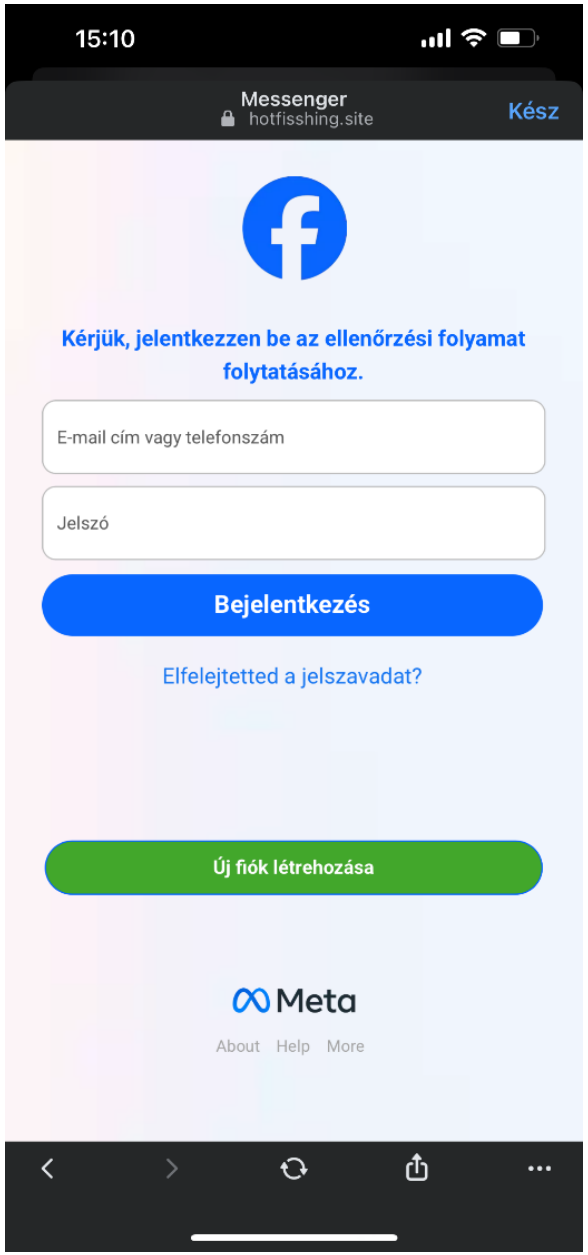
Hamis weboldalak: közműszolgáltatók belépési felületei

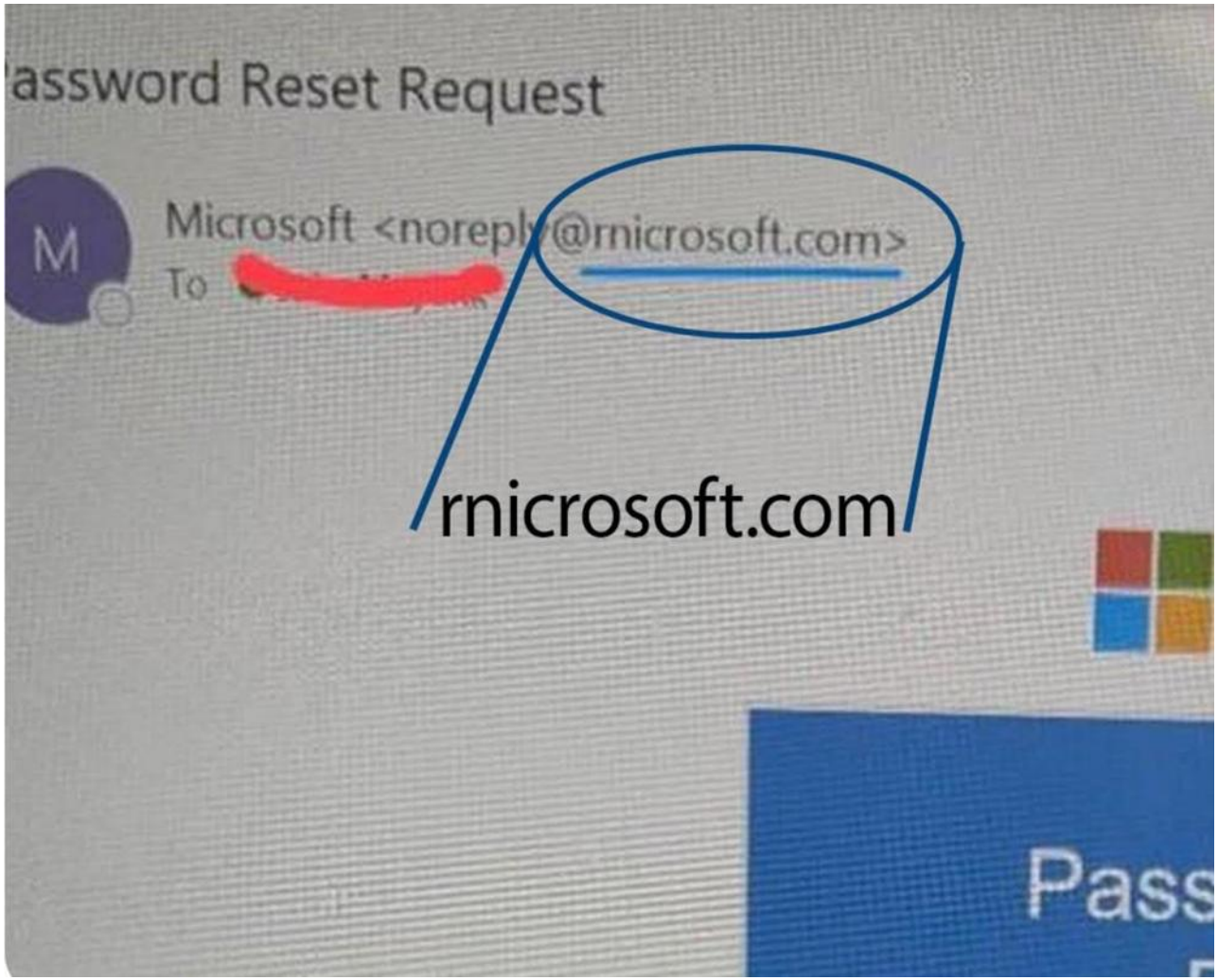




Elkövetési módszerek

Hamis weboldalak: közösségi média belépési felületei




assword Reset Request
M
Microsoft <noreply@rnicrosoft.com>
To
rnicrosoft.com
Pass

rn = m?

Deepfake MI csalás

Elkövetési módszerek

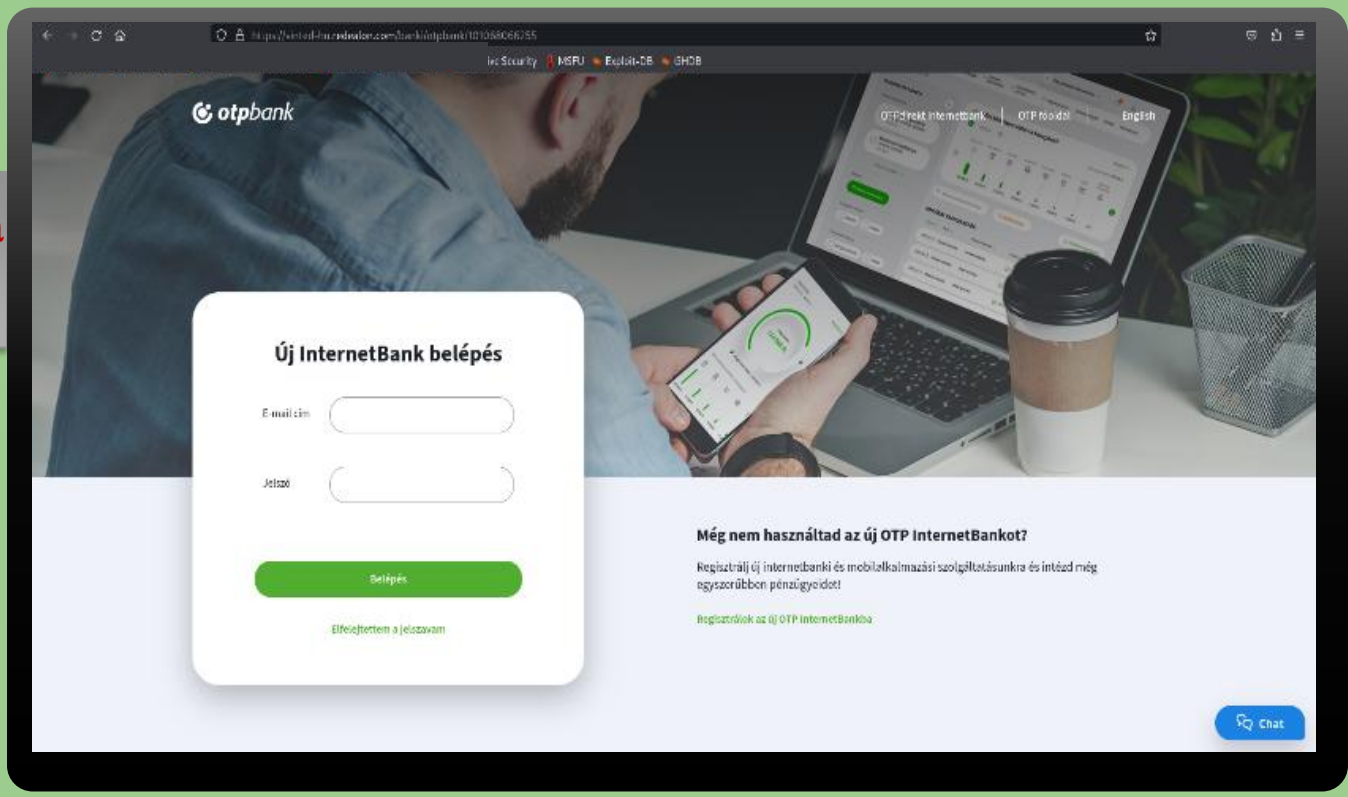
https://internetbank.otpbank.hu/auth/bejelentkezes?url=%2FfooIdal

valódi internetbank

https://vinted-hu.redealon.com/banki/otpbank/101068066255

csaló internetbank

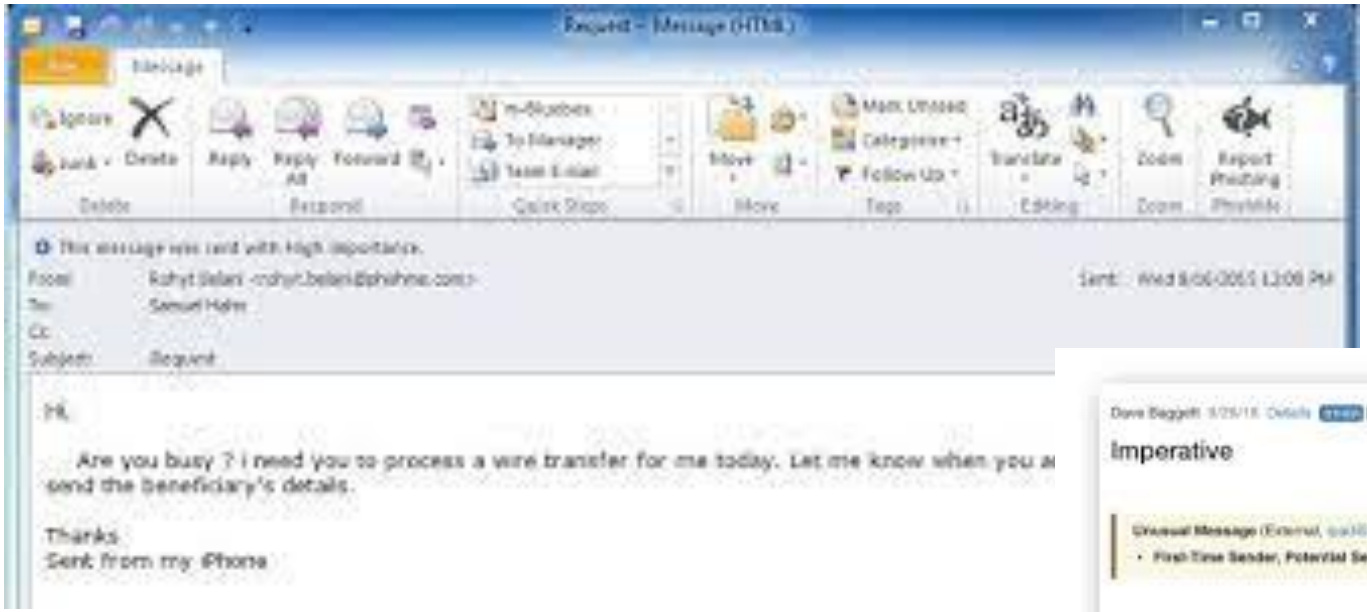
Személyes adatok kiadása az adathalász weboldalon



Elkövetési módszerek

Számlaeltérítés és a CEO Fraud

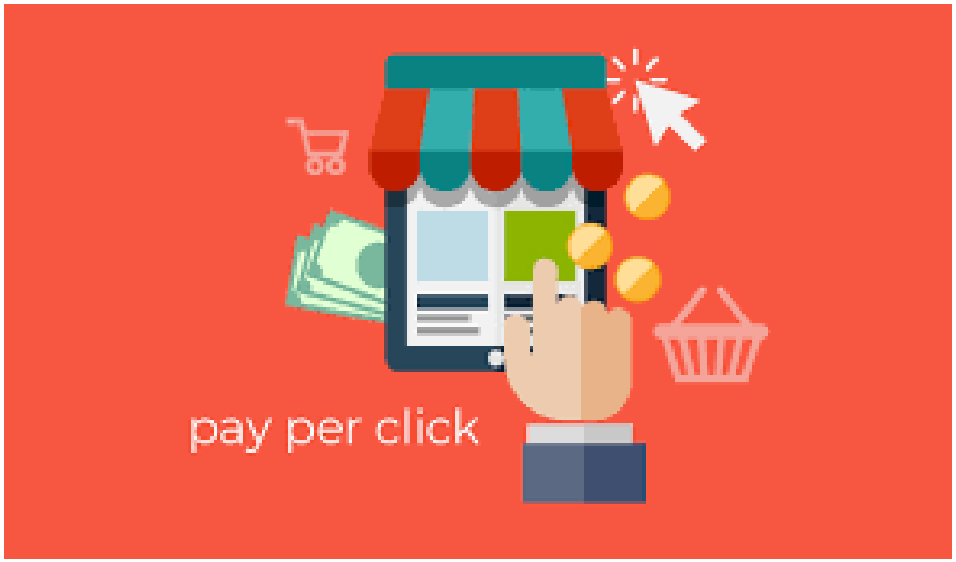
Az elkövetők általában jelentősebb gazdasági társaságok levelező rendszerének feltöréséve, az ott dolgozók megtévesztésével megszerzett adatok birtokában olyan, üzenetet küldenek a sértett, jellemzően külföldi cég üzleti partnere nevében, hogy az éppen esedékes fizetési kötelezettségét már egy új számlaszámra teljesítse. A csalók ezekben az esetekben a számlákra érkező összegeket jellemzően külföldi bankoknál vezetett számlákra utalják tovább.



Elkövetési módszerek

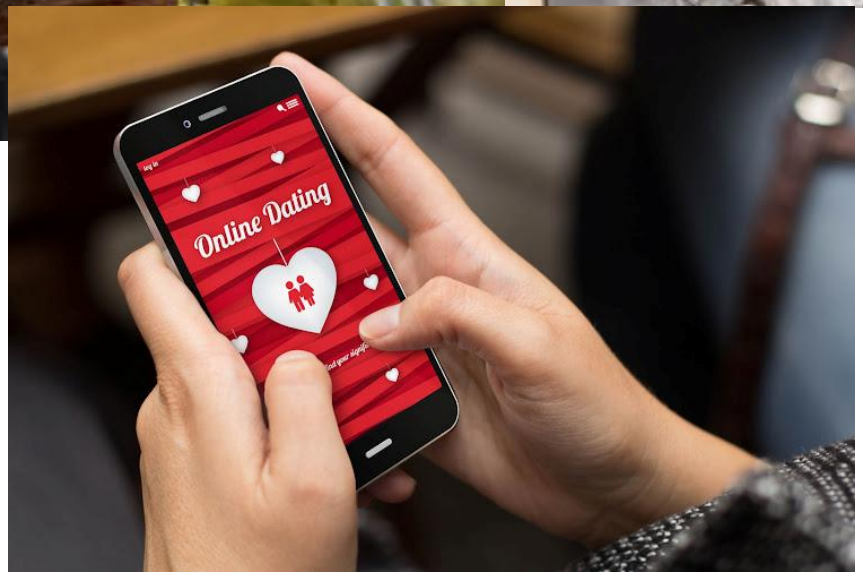
Hirdetési csalások

Az elkövetők különböző termékeket áron alul kínálnak eladásra közösségi oldalakon, internetes hirdetési portálokon. A termékek árát, vagy annak előlegét előre kérik megfizetni az erre a célra általában strómanok által nyitott számlákra (ezt követően a termékeket nem küldik el a sértettnek, akinek hívásait már nem fogadják. Ezen ügyek egész évben jellemzően voltak.



Elkövetési módszerek

romantikus csalás, örökség ígérete



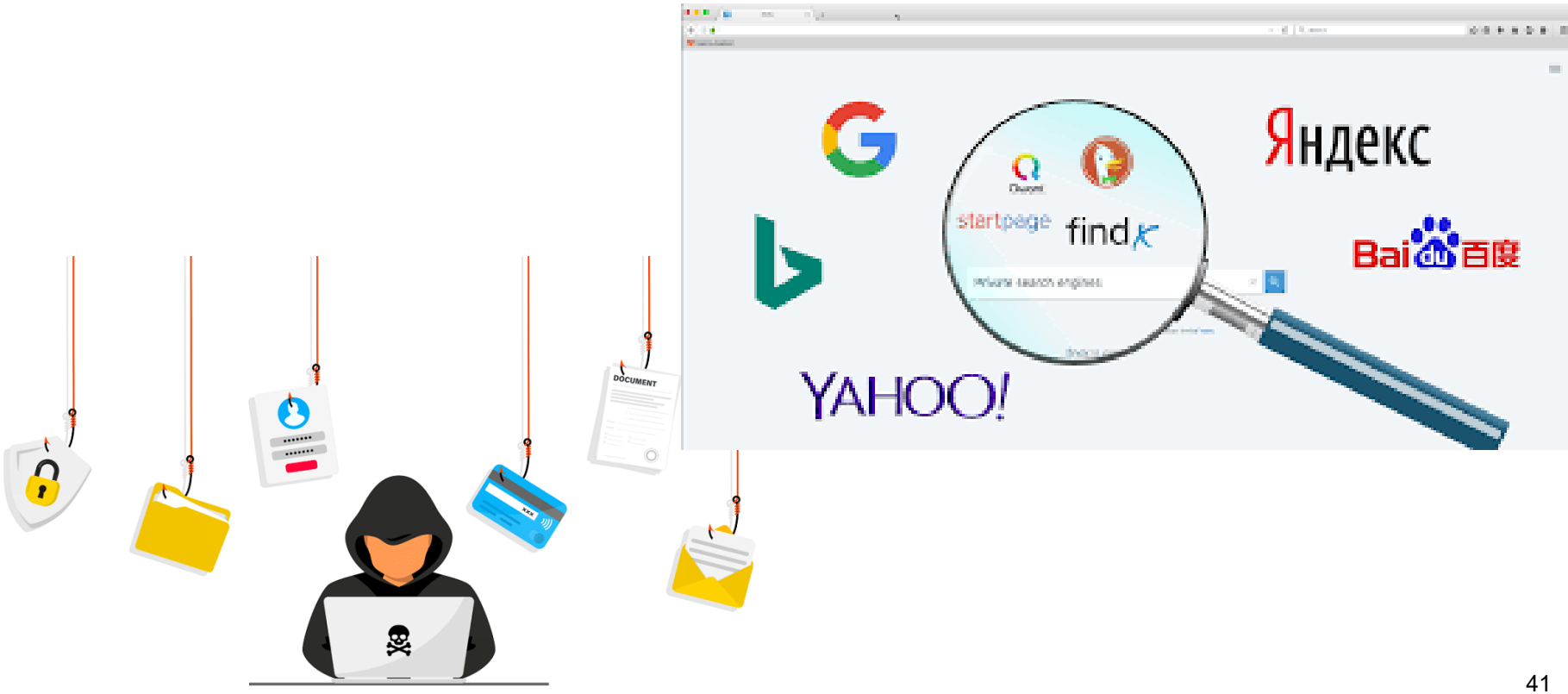
Elkövetési módszerek

Nyereményjáték: a Bank és közüzemi szolgáltatók nevében közzétett, pénznyeremény ígéretével elkövetett csalás

Elkövetési módszerek

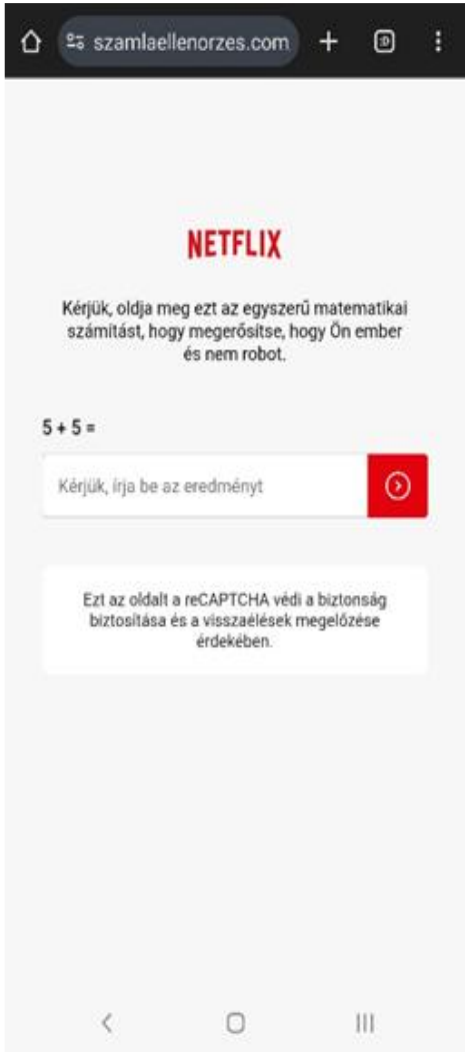
Google phishing

A csalók a Bank internetbanki weboldalát lemásolják, majd a klónozott oldalakat világszerte számos szerverre feltöltik. Annak érdekében, hogy az ügyfelek az álweboldalakra rátaláljanak, az elkövetők fizetett hirdetési kampányokat indítanak, így a klónozott/hamis internetbanki weboldalak a találati listában az első helyen szerepeltek.



Elkövetési módszerek

Hamis weboldalak: Streeming szolgáltatók és pénzintézetek internetbankjának belépési felületei



Megelőzés és biztonsági tudatosság

Mit tegyünk – Mit ne tegyünk

Mit tegyünk, mik azok a dolgok amelyekre oda kell figyelnünk, hogy ne legyünk áldozatok?

Hogyan kell biztonságtudatosan viselkednünk, cselekednünk?

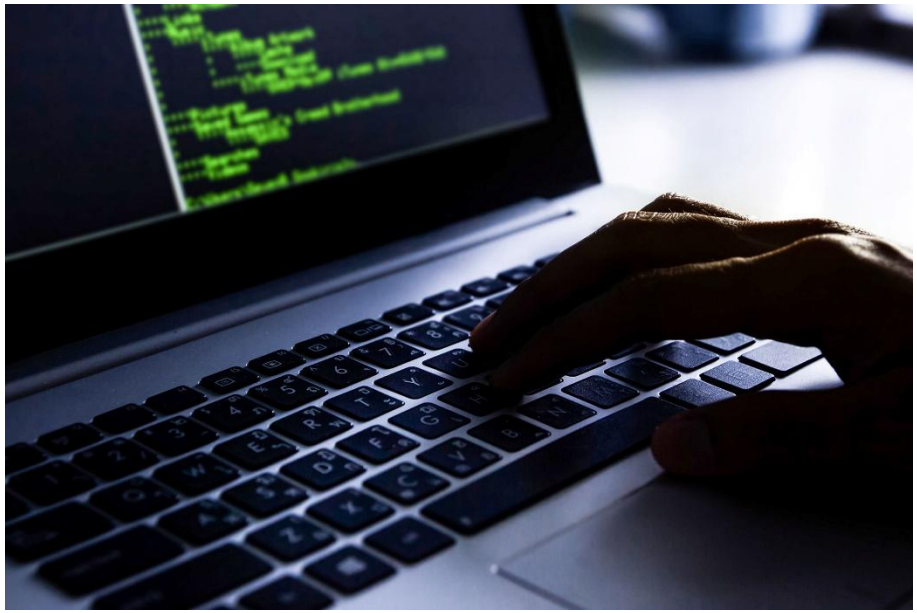
Megelőzés és biztonsági tudatosság

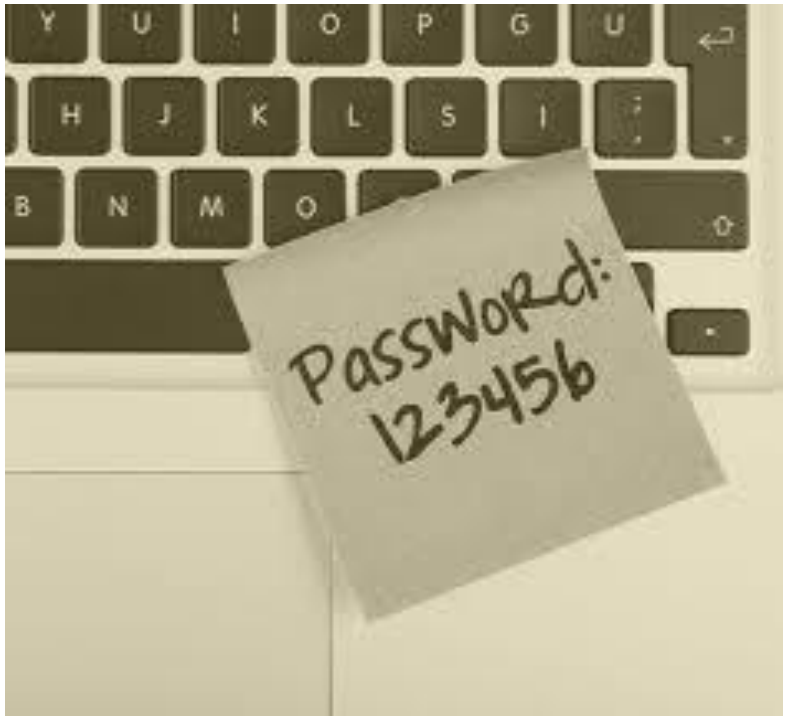
1.Jelszó képzés, kezelés és jelszó használat a kulcs, ha odafigyelünk a helyes és kitalálhatatlan jelszavakra már egy lépéssel beljebb vagyunk

2.a közösségi média felületeken történő felelősségteljes és tudatos biztonság tudatos tevékenység.

3.Online fizetéshez használt jelszó és a közösségi médiában használt jelszó soha nem lehet ugyanaz.

4. Csatolt linkek, hamis weboldalakon, jelszavak megszerzése





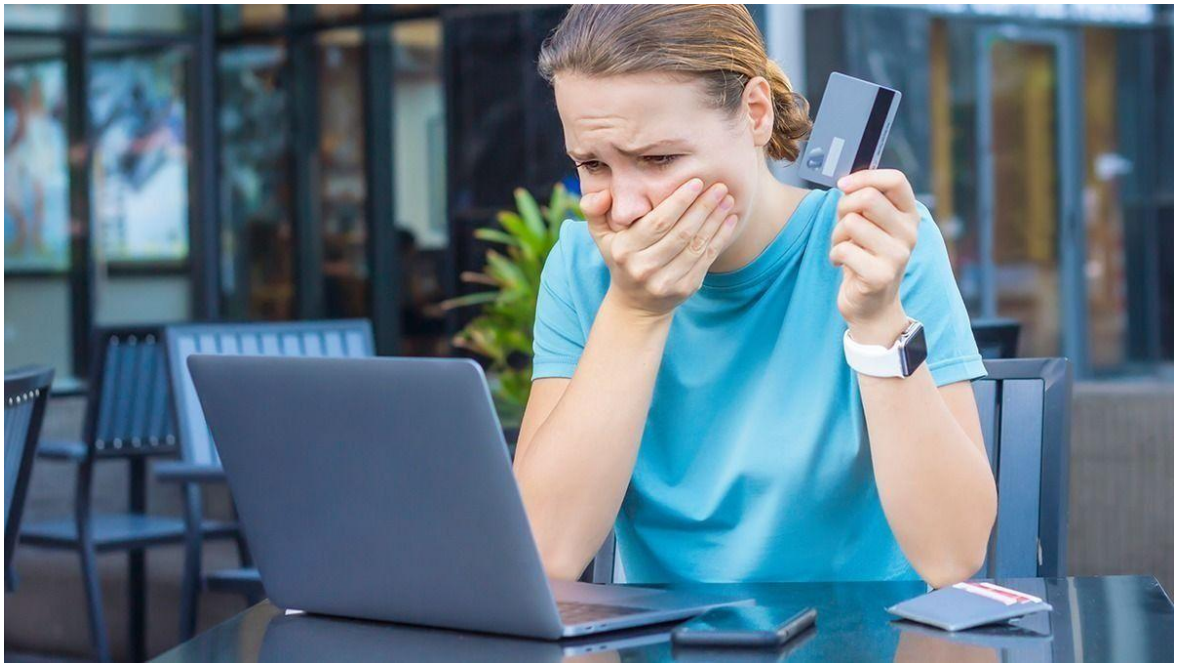
Megelőzés és biztonsági tudatosság

5. Kétlépcsős azonosítás megkerülése és hitelesítő, megerősítő kódok megszerzése

6. Social Engineering

7. Idegen szoftverek telepítése az elkövetési módszerek egyik alapvető része

8. Biztonsági számlára utalás, ilyen van?



Megelőzés és biztonsági tudatosság

9. Üzenetek, figyelmeztetések elolvasása, jóváhagyása, nem olvassuk el.

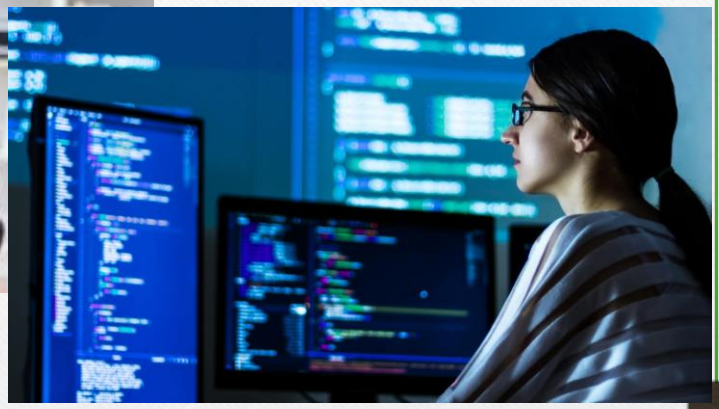
10. A bank nem kér tőlünk soha fizetési adatokat, mégis megadjuk

11. Hamis weboldalak felismerése: gyanús üzenet, sürgető, csatolt link, fizetési adatok megadása

12. Milyen megelőzési, minimalizálási lehetőségeink vannak? Kétlépcsős azonosítás. Limit beállítás, mobilbank: hívás közbeni ellenőrzés, utaláskor funkció, érintéses fizetés, fizetési alkalmazások használata

13. Közösségi média biztonság

13. Ha már megtörtént a baj…mit tegyünk?



KÖSZÖNÖM A FIGYELMET!