



KiberPajzs
Védelem a pénzügyekben

CYBER-SHERIFF WANTED! KIBERSHERIFF KELL!

A kibertér feketelyukai és biztonsági őrei



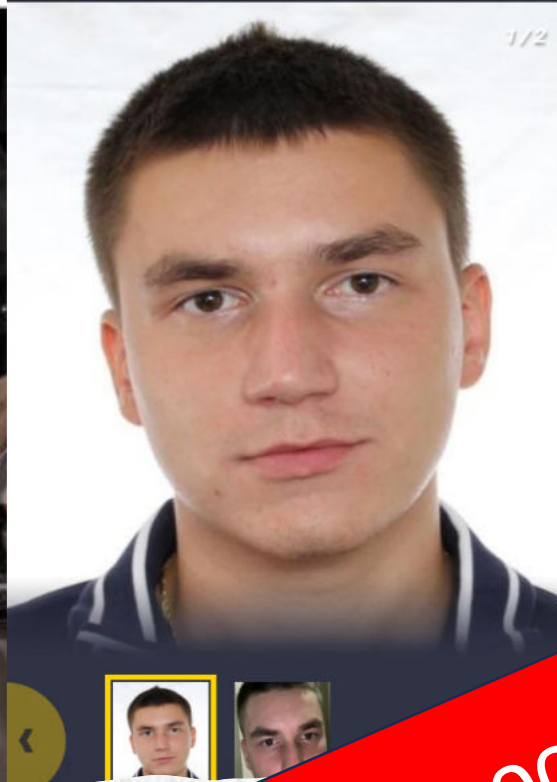
2025. 10. 06.

Have you seen him?

- GLOBÁLIS bűnözés...
- LOKÁLIS védekezés...
- ÖSSZEFOGÁS







1/2

TYMOS
Volodymyr
Віктор

DANGEROUS Wanted

ALIAS:

CRIME:

Computer-related crime

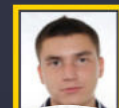
SEX:

APPROXIMATE HEIGHT:

EYE COLOUR:

DATE OF BIRTH:

NATIONALITY:



4.000.000.000.- HUF



INTERNATIONAL REWARD
on ransomware suspect

KiberPajzs

Védekezés a valóságban
Elérni mindenkit... mindenhol..

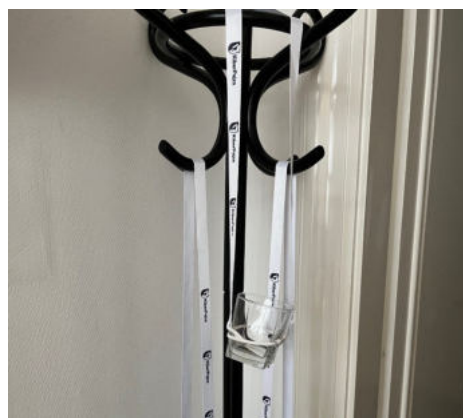




Fesztiválnaptár –

hogyan jelent meg a KiberPajzs a nyári eseményeken?

	Fesztivál	dátum	helyszín
1.	Fishing on Orfű	június 26-28.	Orfű
2.	Sárvári Sörexpressz és XXV. Fúvószenei Várfesztivál	július 4-5.	Sárvár
3.	Veszprémfest	július 8-12.	Veszprém
4.	EFOTT	július 9-13.	Velence
5.	Campus Fesztivál	július 16-20.	Debrecen
6.	Művészetek Völgye	július 19-25.	Kapolcs
7.	FEZEN	július 30.	Székesfehérvár
8.	Sziget Fesztivál	augusztus 6-11.	Budapest, Óbudai Sziget
9.	Mesterségek Ünnepe	augusztus 20.	Budapest
10.	Strand Fesztivál	augusztus 21-23.	Zamárdi
11.	Savaria Fesztivál	augusztus 22-24.	Szombathely
12.	Szegedi Ifjúsági Napok	augusztus 26-29.	Szeged
13.	Családi Mozaikfesztivál	szeptember 7.	Budapest, Puskás Aréna
14.	Rippl-Rónai Fesztivál	?	Kaposvár





Olimpic Day –
MBH+ NVSZ
együttműködés

EFOTT – Velence Pont Ott Parti – Budapest Park



Tiszavirág fesztivál – Szolnok
Múzeumok éjszakája – Budapest
Campus fesztivál – Debrecen
MÁV Juliális családi nap
Szegedi Ifjúsági Napok
Sziget fesztivál – Budapest
Nemzeti Sörfesztivál – Környe



KiberPajzs
Védelem a pénzügyekben



ORFK Bűnmegelőzési Osztály, BRFK, Csongrád-Csanád, Fejér, Vas Vármegyei Rendőr-főkapitányságok bűnmegelőzési egységei

- FEZEN (2025. július 30. – augusztus 2.)
- Sziget Fesztivál (2025. augusztus 6-11.)
- XXIV. Savaria Történelmi Karnevál (2025. aug. 22-24.)
- SZIN: Szegedi Ifjúsági Napok (2025. augusztus 27-30.)



ORFK Bűnmegelőzési Osztály, BRFK, Csongrád-Csanád, Fejér, Vas Vármegyei Rendőr-főkapitányságok bűnmegelőzési egységei



KiberPajzs
Védelem a pénzügyekben



Szakmai KONFERENCIA(sorozat)

A konferencia-
sorozat dátumai:

I. 2025. június 24. kedd

II. 2025. október?

III. 2026. január?



KiberPajzs

'A SZAKMAI ÖSSZEFOGÁS LEHETŐSÉGEI A PÉNZÜGYI KIBERBÜNÖZŐK ELLEN'

Online pénzügyi bűncselekmények – ágazatok közötti szakmai együttműködés eredményei és lehetőségei a kiberbűnözők elleni küzdelemben

MEGHÍVÓ

a KiberPajzs Program, az Igazságügyi Minisztérium, az Országos Rendőr-főkapitányság és a Magyar Bankszövetség közös szakmai konferenciájára

A KiberPajzs program 2022. évi indulása óta a 13 szervezet, köztük az alapító Magyar Nemzeti Bank és Magyar Bankszövetség, valamint minisztériumok, egyéb szakmai szervezetek és bankok (https://kiberpajzs.hu/a-kezdemenyvezessel) vizsgálják a fogyasztói szokásokat, azok változásait, valamint a pénzügyi kiberbűnözés, illetve a pénzügyi kiberbűnözés kapcsán megfigyelhető visszatérő kiberbűnözési kockázatokat. A projekt egyik legfontosabb célja a tájékoztatás, az edukáció, az ügyfelek és felhasználók figyelmének felhívása a pénzügyi kiberbűnözés veszélyeztető kockázataira, hogy az elsajátított ismeretek segítségével a tudatosság alakuljon ki a digitális pénzügyi szolgáltatásokat használó lakosság körében. Ezen konferencián a pénzügyi kiberbűnözésben részt vevő intézmények, valamint a bűnüldöző szervek, a bíróságok és a hatóságok információit és tapasztalatot tudjanak cserélni egymással, ezáltal hatékonyabbá válik a kiberbűnözés elleni küzdelem.

A szervezők ezúton tisztelettel meghívják Önt a KiberPajzs szakmai konferenciájára.

Időpont: 2025. június 24. kedd, 9:00 órai kezdettel

Helyszín: Készenléti Rendőrség, 1101 Budapest, Kerepesi út 47-49., 11. emeleti terem
(A regisztráció 8.30 órakor kezdődik - kérjük, legkésőbb 8.45-órakor szíveskedjen megérkezni a rendezvény helyszínre.)

A konferencián beszámolunk Önöknek a kiberbűnözők elleni harc helyzetéről és gyakorlati lehetőségeiről a bűnüldözés és az igazságszolgáltatás eszközeinek segítségével.

A konferencia célja a vonatkozó területen dolgozó szakemberek számára magas szakmai színvonalú, kifejezetten gyakorlatias megközelítésű, hatékony eszközökre, jó gyakorlatokra koncentráló, új ágazati szakismereteket biztosító képzés nyújtása, az eredményes büntetőeljárást támogató, gyakorlati ismeretek bemutatása.

A konferencia várható programja:

- Dr. Tuzson Bence, Magyarország igazságügyi minisztere megnyitja a rendezvényt
- Üdvözlő beszédet mond:
 - Dr. Tórecsik Sándor r. vezérőrnagy, az ORFK bűnügyi országos rendőrfőkapitány-helyettese
 - A KiberPajzs program társ-projektgazda vezetője
- Gyakorlati szakmai előadásokat hallhatnak az IM, MBSZ, ORFK szakmai egységei (BJFH ÁT, ISZFO, NAV PEI, NNI, LÜ) részéről

A csatolt programban részletes információkat talál, ezért kérjük, olvassa el végig levélünket!

Kérjük, hogy részvételi szándékát legkésőbb 2025. június 12-én 12.00 óráig jelezze a titkarsag@bankszovetsag.hu címen.



KiberPajzs

'A SZAKMAI ÖSSZEFOGÁS LEHETŐSÉGEI A PÉNZÜGYI KIBERBÜNÖZŐK ELLEN'

a KiberPajzs Program, az Igazságügyi Minisztérium, az Országos Rendőr-főkapitányság és a Magyar Bankszövetség közös szakmai konferenciája
2025. június 24. – Készenléti Rendőrség
TERVEZETT TEMATIKA

(Az előadói egyeztetések még zajlanak, ezért a programváltoztatás jogát fenntartjuk.)

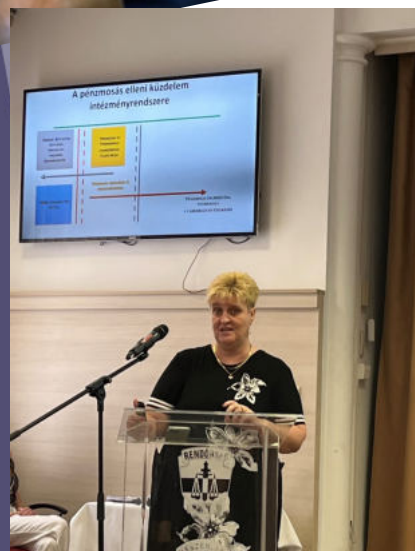
Időpont	Esemény	Előadó
8.30-9.00	Regisztráció	
9.00-9.10	Üdvözlő beszéd	Dr. Tuzson Bence, Magyarország igazságügyi minisztere
9.10-9.20	Programnyitó	KiberPajzs program társ-projektgazda vezetője
9.20-9.25	Attekintés	Dr. Tórecsik Sándor r. vezérőrnagy, az ORFK bűnügyi országos rendőrfőkapitány-helyettese
9.25-9.55	Online bűncselekményeket érintő új büntetőjogi szabályok összefoglalása	Jancsó Gábor IM BJFHAT
	Aldozatokat kapcsolatos optimális eljárások - sértettek számára nyújtható segítség	IM ISZFO és Magyar Bankszövetség
	Eljárások - büntetőeljárások lehetőségei, kihívásai	Földes Hajnalka alezredes, főosztályvezető-helyettes, NAV
	Eljárások - büntetőeljárások lehetőségei, kihívásai	Dr. Kovács Levente főtitkár, Magyar Bankszövetség
	Eljárások - büntetőeljárások lehetőségei, kihívásai	Magyar Bankszövetség által felkért pénzügyi vezetők (Bucsek Gábor - OTP, Ragó István - Raiffeisen)
12.15-12.30	Visszaélésszűrő Rendszer - Eljárások támogatásának lehetőségei, kihívásai	Oláh Gábor vezérigazgató, GIRO
12.30-13.00	Az online bűncselekmények bünygyi nyomozásának kihívásai, tapasztalatai - megoldások, jó és rossz gyakorlatok (I. rész)	ORFK
13.00-14.00	Ebed	
14.00-14.30	Az online bűncselekmények bünygyi nyomozásának kihívásai, tapasztalatai - megoldások, jó és rossz gyakorlatok (II. rész)	ORFK
14.30-15.00	Pénzügyi nyomozás, vagyonvisszaszerzés a kibertérben	NNI VVH és NNI Kiberbűnözés Elleni Osztály (ORFK)
15.00-15.20	Kihívások, tapasztalatok, megoldások - online bűncselekmények elleni nyomozás ügyész szemmel	Losonczi-Molnár Melinda, LÜ Általános és Kiberbűnözés Elleni Osztály vezetője, Legfőbb Ügyészség
15.20-15.25	Zárszó	

MEGVALÓSULT!
1. kör





KiberPajzs
Védelem a pénzügyekben

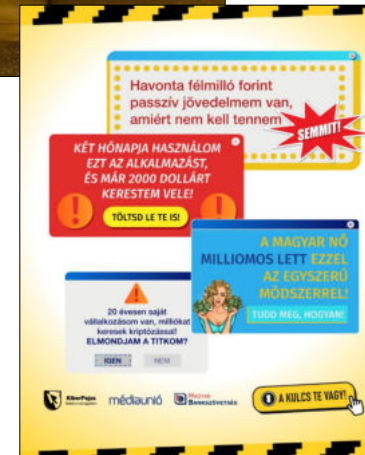
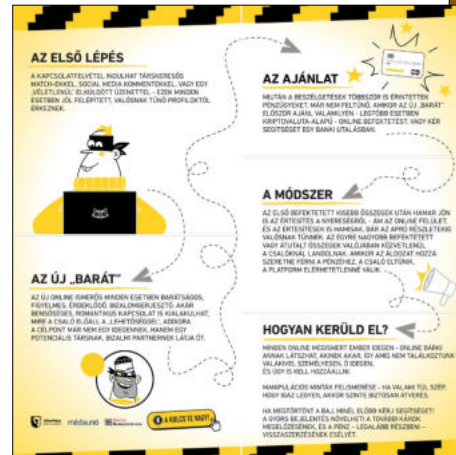


KiberPajzs Bírói, jogi konferencia



Médiaunió, Magyar Bankszövetség – futó kampány

- Július végén új közlemény („Pig butchering”):
 - 30+ megjelenés (pl. Portfólió, Index, Pénzcentrum stb.)
- Augusztusban 280 city light plakát (CLP) országszerte:
 - A megjelenés bruttó értéke 81 millió Ft
- Júliusban és augusztusban havonta 3-4 FB-poszt



Vállalati digitális csalások - Mit tegyünk?



KiberPajzs
Védelem a pénzügyekben

Üzleti kibervédelmi
KISOKOS



KiberPajzs
Védelem a pénzügyekben



KiberPajzs
Védelem a pénzügyekben



KiberPajzs
Védelem a pénzügyekben

KIBERBIZTONSÁGI TANÁCSOKÉRT
ÉS TOVÁBBI CSALÓFOGÓ TIPPEKÉRT
LÁTOGASSON EL OLDALUNKRA



kiberpajzs.hu

Üzleti kibervédelmi **KISOKOS**

*‘Olyan erős a szervezet
védelme, mint
a leggyengébb láncszeme’
– vagyis az ember.*

- ,Olyan erős a szervezet védelme, mint a leggyengébb láncszeme’ – vagyis az ember
- Tulajdonosi szemlélet szükséges a munkatársak részéről



KiberPajzs
Védelem a pénzügyekben

Hallott már az alábbi csalástípusokról?

Váltásdíj csalás

Cége egyik munkatársa emailt kap, melyben egy szakmai szervezet kéri őt a céges adatok megadására, az adatok frissítése miatt. A linkre kattintva viszont letöltődik egy rosszindulatú szoftver, amelynek segítségével a támadók hozzáférhetnek a cég adatbázisához. A támadók ezután akár lezárhatják a cég munkaállomásait is és 'váltásdíjat' követelhetnek, azzal fenyegetve, hogy nyilvánosságra hozzák az ügyfeladatokat.

Számlacsalás

Cégéhez ismeretlen ügyféltől érkezik számla, amely teljesen eredetinek kinéz, aláírt szerződéssel van alátámasztva. A hamis számla kiállítója egy állandó partner arculatát másolja, és sürgős utalást kér, egy megváltozott, új számlaszámra.

Visszaigénylési csalás

Visszaigénylési csalás esetén a csalo ügyfelek vitatják a tranzakció, vagy kézbesítés megtörténtét, ami azt eredményezi, hogy cégének vissza kell fizetnie a termék árát. A csalog gyakran lopott kártyaadatokat használnak. A vállalkozásoknak kihívást jelent a jogszerű tranzakciók bizonyítása, valamint a büntetések, a magasabb díjak vagy akár a kereskedői számlájuk elvesztésének kockázata.

TOVÁBBI
CSALÁSTÍPUSOKÉRT
KATTINTSON IDE:



Az Ön vállalkozása mit tehet, hogy ne váljon kibercsalások áldozatává?

A digitális világban digitális bűnözők ellen kell harcolni. Ezért vált fontossá az online térben a „Zéró Bizalom Elve”:

- ✓ Senkinek ne adja ki kódjait, jelszavait!
- ✓ Ne telepítsen senki kérésére programokat és ne kattintson ismeretlen, vagy gyanús linkre!
- ✓ Mindig ellenőrizze az emailek feladóját, a weboldalak címét és megbízhatóságát!
- ✓ Szokatlan kérés esetén érdemes óvatossággal lenni és konzultálni egy szakértő kollégával!

Szeretné biztonságban tudni a céget és értékeit az online térben is?

7 a csalás elleni küzdelemhez,
TIPP a Nemzeti Kibervédelmi Intézet
kibervédelmi szakértőjétől:

1. Frissítse szoftvereit rendszeresen és telepítsen vírusirtó szoftvert is!

A tűzfalak, szoftverfrissítések és rendszeres biztonsági mentések sokat segítenek a megelőzésben. A már nem használt szoftvereket távolítsa el a mobiltelefonról, a számítógépről és a vállalati szerverekről is – ezzel csökkenti a támadási felületet.

2. Ne jelszavakat, JELMONDATOKAT használjon!

Egyedi, összetett jelkódokat használjon és rendszeresen cserélje azokat! A Nemzeti Kibervédelmi Intézet felületén ellenőrizheti, hogy jelkódjai megfelelőek-e: <https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszo-ellenorzo/> Nincs más dolga, mint begépelni a jelszavát (vagy egy Önéhez hasonlót), és ez az online program megmondja, mennyi időbe telne egy csalonak feltörni a fiókját, vagy szerverét. Az eredmény függvényében meggyőződhet arról, mennyire biztonságosak online fiókjai. További védelmet nyújt a többfaktoros hitelesítés, és a jelszókezelő szoftver, melynek használatakor csak 1 db 'mesterjelszót' kell ésszben tartanunk, és ezzel hozzáférünk az összes többi jelszóhoz.

3. A számlafizetéseket mindig duplán ellenőrizze!

Jogtalan kifizetés, vagy csalo tevékenység elkerülése érdekében mindig fokozott figyelemmel ellenőrizze a teljesítendő számlákat! Ha például partnere számlaszám változást jelez, akkor azt telefonon, vagy más csatornán is erősíttesse meg a kiállító céggel.

4. Szabályozza a dolgozók hozzáféréseit!

Ki milyen mappákat láthat? Ki engedélyezhet átutalásokat és rögzíthet új partnereket? Az ilyen és hasonló folyamatokra vonatkozóan hozzon létre egyértelmű és egyszerű belső szabályokat. nsági szabályzatot!

5. Képezze alkalmazottait rendszeresen kibertudnivalókkal!

Az alaposan képzett és felkészült munkatárs a kibervédelem legfontosabb láncszeme. Ahogy saját értékeinkre vigyázunk a való világban, vigyázunk úgy a kibertérben is céges és személyes adatainkra, jogosultságainkra! Akár tesztekkel, helyzetgyakorlatokkal is segítheti kollégái felkészülését.

6. Informálódjon, beszélgessen a kibervédelemről!

Ha naprakész a lehetséges csalásformákkal kapcsolatban és folyamatosan figyeli a lehetséges védelmi technikákat, nagyobb eséllyel védheti meg munkatársait és cége értékeit a mindennapok során.

Tippek és ötletek: www.kiberpajzs.hu, www.akulcstevagy.hu

7. 'MESTERFOKOZAT':

Hozzon létre biztonsági szabályzatot!

Rendszerezze a kockázatokat és a veszélyes folyamatokat.

- Kis- és közép vállalatok számára igénybe vehető képzés („de minimis” keret terhére igényelhető): <https://digitaltechedih.hu/elerheto-kepzeseink/>
- INGYENES szakmai tanácsadás kiberbiztonsághoz kapcsolódóan: <https://digitaltechedih.hu/szolgaltatasok/kiberbiztonsag/>

+1 HA MÉGIS KIBERC SALÁS ÁLDOZATÁVÁ VÁLIK,

A LEGFONTOSABB AZONNALI TEENDŐK:
ÉRTESÍTSE BANKJÁT ÉS TEGYEN
FELJELENTÉST A RENDŐRSÉGEN!



KiberPajzs
Védelem a pénzügyekben

Üzleti kibervédelmi
KISOKOS

• Életszerű
példák

• 7 + 1 TIPP

**Ön és a cége mennyire
kibertudatos jelenleg?
Jelölje az alábbi listában:**

- ☐ Alkalmazottaink rendszeresen járnak kiberképzésekre
- ☐ Az emailjeinket és a dokumentum mappákat csak meghatározott emberek láthatják
- ☐ Számítógépeinket, tabletjeinket csak ellenőrzés után (PIN, ujjlenyomat, stb.) használhatjuk
- ☐ Számláinkat és a kifizetéseinket legalább két ember ellenőrzi és engedélyezi
- ☐ Összetett jelmondatokat használunk
- ☐ Vírusírtót és tűzfalat használunk az informatikai rendszerünkben
- ☐ Sokat beszélgetünk, olvasunk a kibervédelemről
- ☐ Rendszeres a biztonsági mentés a szervereken és a levelezésünkben
- ☐ Rendszeres frissítjük szoftvereinket
- ☐ Rendszeresen egyeztetünk kiberbiztonsági szakértővel

1-4 Biztató kezdő lépéseket tettünk

5-7 Alapvető fejlesztéseink vannak, érezhetően biztonságosabb környezetet alkottunk

8-10 Szervezetünk kibertudatos, jó eséllyel indul a csalókkal szemben

Üzleti kibervédelmi

KISOKOS

- Gyorsteszt a felkészültség teszteléséhez
- Hiányzó eszközök, módszerek tudatosítása



KiberPajzs
Védelem a pénzügyekben



KiberPajzs
Védelem a pénzügyekben

A kiberbűnözés kora

2025

A kiberbűnözés gazdasági hatása
10-szer nagyobb, mint a
kábitószer-kereskedelemé.



A kiberbűnözők már felismerték, hogy az üzleti szereplők is csak emberek; az alkalmazottak vagy a munkáltatók ugyanolyan sebezhetőek, így őket támadva gyakran nagyobb károkat is okozhatnak.

„Általánosságban elmondható, hogy a biztonságtudatosság nem megfelelő, ám az utóbbi időben néhány vezető elkezdte megérezni ennek fontosságát. Ez kulturális szempontból fontos, mert a vezetők példamutatása nélkül nem lesz rendszerszintű változás.”

dr. Palicz Tamás,
Stratégiai igazgatóhelyettes,
Simmelweis Egyetem

„A védekezési oldalon nagy probléma az emberi erőforrás és a szakértelem hiánya.”

Anonim szakértő

A kiberbűnözés mindenkit érint, a felhasználókat és a szolgáltatókat egyaránt, mivel a termékek és szolgáltatások egyre bonyolultabbá válnak. Ha valahol sebezhetőség van, az mindenkit veszélybe sodorhat.

A támadók a szolgáltatókat és más vállalkozásokat is célba veszik, kihasználva a dolgozók sebezhetőségét. A szakértői interjúk alapján a nagyvállalatok rendelkeznek a technológiával, de annak alkalmazása fejlesztésre szorul, míg a legtöbb kkv gyenge védelmi rendszerrel rendelkezik.

A szakértők által kiemelt problémák, amik megnehezítik a védelmet:

- A kiberbiztonságra fordítandó források hiánya
- A kulcsfontosságú üzleti szereplők alacsony biztonságtudatossága
- Az emberi erőforrások és a szakértelem hiánya

KIBERKEDD kampány

Beszélni KELL a
kiberbiztonságról!

KIBERKEDD – DEEPFAKE kampány

Figyelem! Terjednek a Deepfake videók!

A Deepfake (valósághamisító) videók mesterséges intelligenciával készített hamis tartalmak, amelyek összetéveszthetők a valódiakkal. Ezekben gyakran híres emberek arcát, hangját használják fel megtévesztésre.

A csalók ismert személyek nevével élnek vissza, hogy elnyerjék a bizalmadat.

Ezek a videók hamis eseményeket mutatnak be, és a szereplők nem mondták, amit hallasz – sokszor nem is tudnak a videó létezéséről.

Gyakori átverések:

- Kamu befektetési ajánlatok
- Téves infók bankokról, szervezetekről
- Pánikkeltés, bizalomrombolás

Hogyan védekezhetsz?

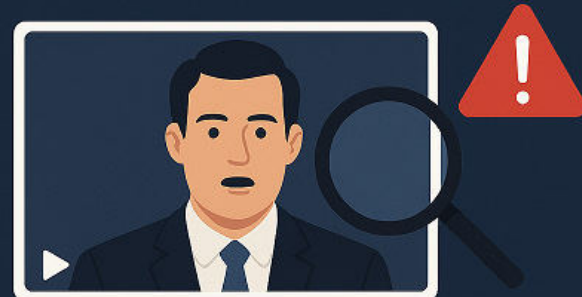
- Figyeld a furcsaságokat: gépi hang, furcsa mimika, homályos részletek
- Ellenőrizz több forrást, mielőtt döntesz
- Ha túl jónak tűnik, hogy igaz legyen... valószínűleg nem az

Találoztál már gyanús videóval?

Írd meg kommentben, hogy tanulhassunk egymástól!



Ne higgy a szemednek!



A cél: a bizalom kihasználása és manipuláció.

Gyakori visszaélések:

- Hamis, „kihagyhatatlan” befektetési ajánlatok
- Pánikkeltés a pénzpiacokon
- Téves információk terjesztése nagyvállalatokról, intézményekről

Mit tehetünk ellene?

- ☒ Légy tudatos – akár szakemberként,

KIBERKEDD – DEEPFAKE kampány



KiberPajzs
Védelem a pénzügyekben



Deepfake: A mély tanulás (deep learning) és a kamu (fake) összevonása. Olyan digitális hamisítási technológia, amellyel a valódihoz a megtévesztésig hasonló multimédiás tartalmakat lehet előállítani.

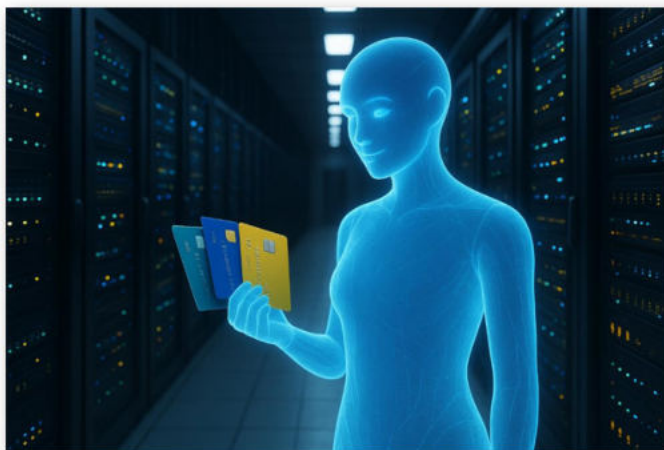


séges Intelligencia a pénzügyekben 3.

10

funkciók a háttérben

kockázatesztelés online vásárlásnál,
nálánál (issuer/hálózati szinten): **valós**
modellek döntenek arról, kell-e plusz
s, vagy blokkolni kell egy tranzakciót.
szabott tippek/értesítések: egyes
a költési mintákból származó **intelligens**
k jelennek meg – ez is többnyire
eli MI.



www.penz7.hu

facebook.com/penz7

penz7.hu

NEMZETI
KIBERVÉDELMI INTÉZET



PÉNZ7
kiberbiztonság
– az AI veszélyei

- 11 éve iskolai tanórák
- Évente 220 ezer diák
- 3. alkalommal KIBER tananyag!
- Digitális Szimat Kihívás

ÖSSZEFOGÁS a kiberbűnözők ellen



NEMZETGAZDASÁGI
MINISZTERIUM



IGAZSÁGÜGYI MINISZTERIUM



médiaunió
rajta is múlik!





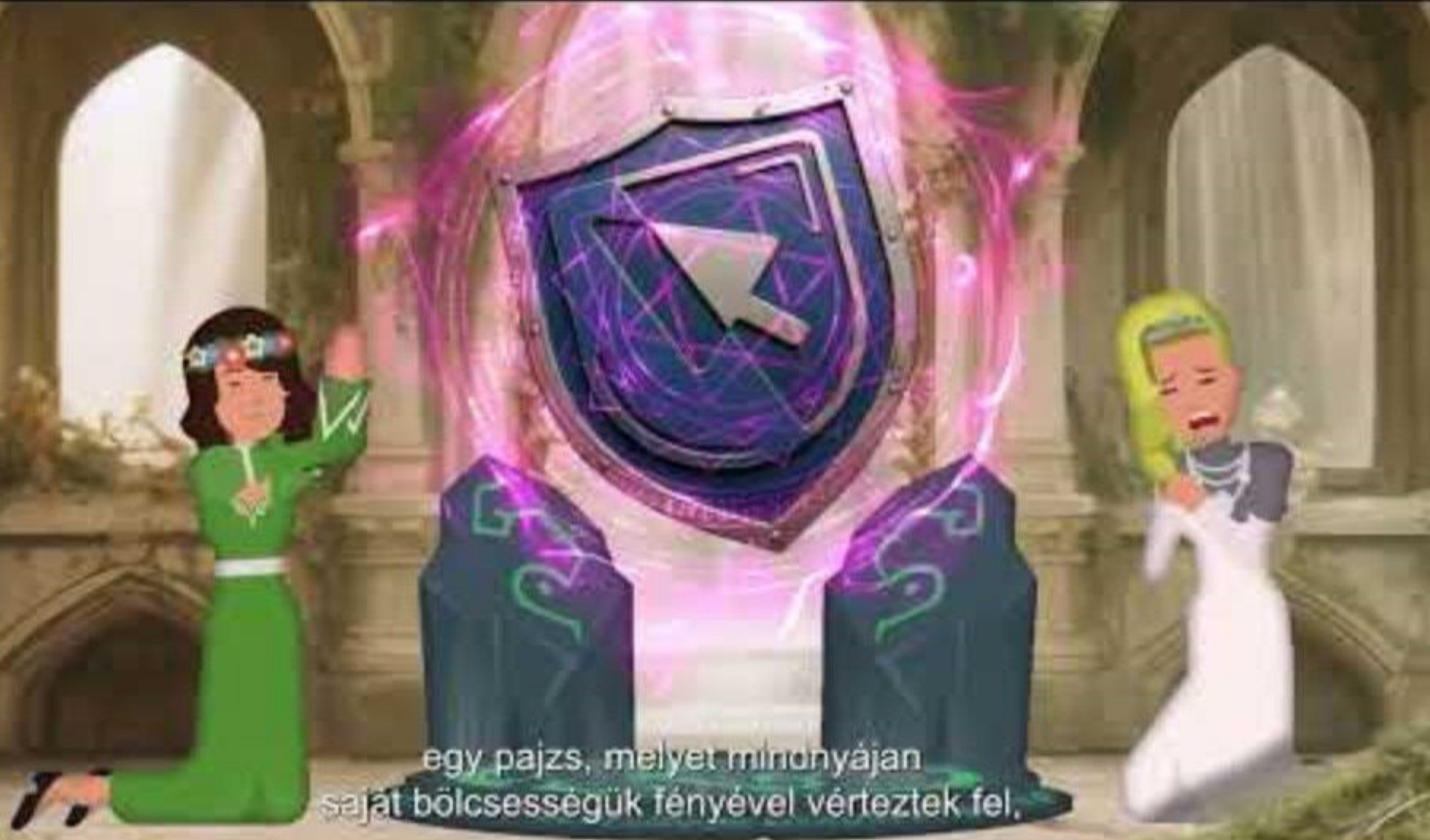
A KiberPajzs születése

*Küzdelem a kiberdémonokkal
téren és időn át*



KiberPajzs

Védelem a pénzügyekben



egy pajzs, melyet minihyájan
saját bölcsességük fényével vértettek fel.



KiberPajzs

Védelem a pénzügyekben



KiberPajzs
Védelem a pénzügyekben