Sütő Ágnes
Társ-projektgazda

Freisleben Vilmos
Társ-projektgazda

KiberPajzs
Védelem a pénzügyekben

Légy résen, és ne te légy rés a pajzson!

...a cégeknél is...

CyberSec 2026. október 5.

JELENLEG ÍGY NÉZÜNK KI

médiaunió
rajtad is múlik!

PÉNZÜGYI BÉKÉLTETŐ TESTÜLET

SZERENCSEJÁTÉK ZRT.

one

VISA

NBT
NEMZETI BŰNMEGELŐZÉSI TANÁCS

IVSZ
DIGITÁLIS VÁLLALKOZÁSOK SZÖVETSÉGE

Befektető-védelmi Alap

Magyar Posta

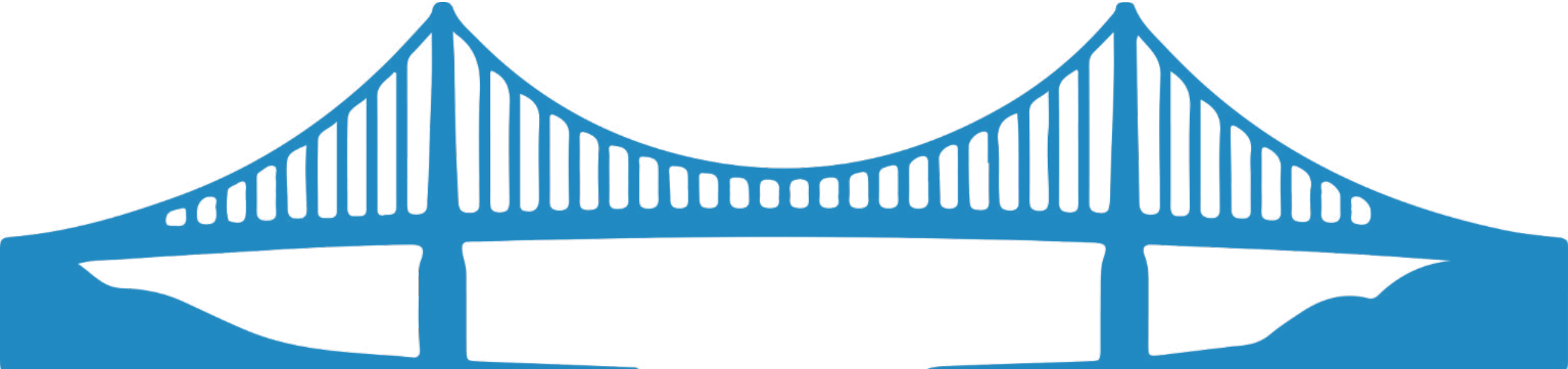


A KIBERPAJZS FŐ PILLÉREI

KiberPajzs

OKTATÁS ÉS TUDATOSSÁG

SZAKMAI EGYÜTTMŰKÖDÉS



KOMMUNIKÁCIÓ – MÉDIAJELENLÉT - SAJTÓTÁJÉKOZTATÓK





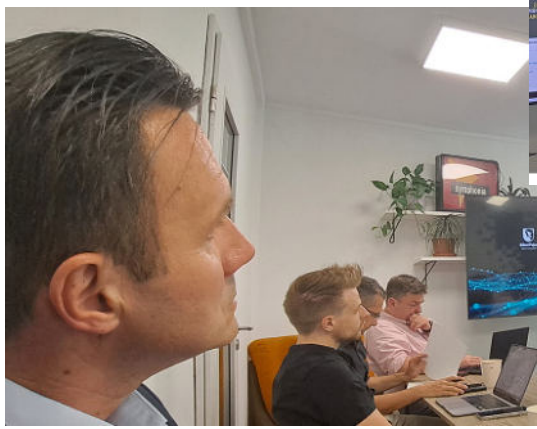


















Fesztiválok

KiberPajzs a nyári eseményeken..







Olympic Day,
CyberTrident Challenge verseny,
Művészetek Völgye,
SZIGET fesztivál
Bálványos….











… AMI MÁR EDDIG MEG IS VALÓSULT

KiberPajzs
Védelem a pénzügyekben



Bankszövetségi ajánlás:
bankszakmai oktatóanyag és áldozatokkal történő kommunikáció



Konferenciák

Nyomozók, ügyészek, bírók számára

KiberPajzs brand mélyülése

jogalkotói és kormányzati szinteken is



IM Online csalás elleni munkacsoport:

2024. évi XVIII. tv
2024. évi LXIV. tv:
2025. évi XLIX. tv.: 28 tv.



Kereszthitelesítés:

Javasolt kereszthitelesítési módszer(ek), megoldás(ok) kidolgozása



Hívószám hamisítás szűrése, blokkolása

magyarországi nem mobil számok esetében 2025. október 15-től, mobilszámok esetében 2026. június 1-jétől kell alkalmazni

KiberPajzs
Védelem a pénzügyekben

MIN DOLGOZUNK MOST?

Főbb témáink, projektjeink, eredmények

AMIKKEL FOGLALKOZUNK…

KiberPajzs
Védelem a pénzügyekben



Csalárd SMS szűrés



Befektetési csalások megelőzése

Lakossági adathalász bejelentések kezelése (PIHE)



Segédlet a Rendőrség ügyfélszolgálata számára *a pénzügyi biztonságot érintő kérdések tárgyában*





Napi híradások, lakossági warningok



Business fraud, AI kihívásai

CSALÁSRADAR SZAKMAI CSOPORT

KiberPajzs
Védelem a pénzügyekben



Projekt célja:

- ✓ Havi rendszerességgel a csalási trendek figyelése, a TOP csalási formák azonosítása, kiugróan emelkedő, vagy új csalástípusok azonosítása.
- ✓ Az eredmények felhasználása a KiberPajzs munkacsoportokban pl: kommunikációs munkacsoportban a lakossági értesítések és warningok készítéséhez, stb…
- ✓ A csalástípusok megnevezésének, tartalmi meghatározásának egységesítése a tagok között.

KiberPajzs

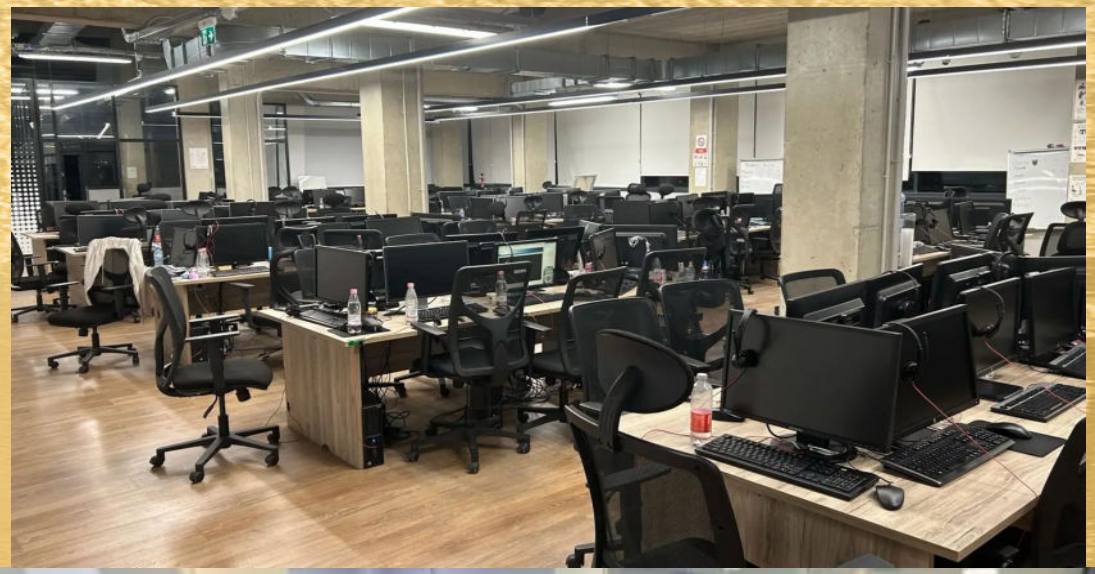
Védelem a pénzügyekben

FÓKUSZBAN A BUSINESS FRAUD

A CSALÓK PROFESSZIONÁLIS HÁTTÉRREL DOLGOZNAK

KiberPajzs
Védelem a pénzügyekben

- Vállalati környezet, szervezet
  - vezetőség, pénzügy, informatika, humánerőforrás, egyén alegységek
- Call center működtetése
- Fix fizetés és jutalék
- A megtévesztés és befolyásolás gátlástalan mestere





Forrás: www.europol.europa.eu

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,
Semmelweis Egyetem

„A védekezői oldalon nagy probléma az emberi erőforrás és a szakértelem hiánya."

Anonim szakértő

A KIBERBŰNÖZÉS MINDENKIT ÉRINT

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

KIFEJEZETTEN VÁLLALKOZÁS SPECIFIKUS CSALÁSI METÓDUSOK

KiberPajzs
Védelem a pénzügyekben



- KETTŐS CEO CSALÁS
- VÁLTSÁGDÍJ CSALÁS
- LEVELEZŐFIÓK FELTÖRÉS, HAMIS SZÁMLASZÁMVÁLTOZÁSRÓL ÉRTESÍTÉS
- SZÁMLACSALÁS
- VISSZAIGÉNYLÉSI CSALÁS

TOVÁBBI CSALÁSTÍPUSOK IS VESZÉLYEZTETIK A VÁLLALKOZÁSOKAT

KiberPajzs
Védelem a pénzügyekben



- ÁLDOZATOK ISMÉTELT MEGKÁROSÍTÁSA A KORÁBBI CSALÁSI ESETRE HIVATKOZÁSSAL
- HAMIS BANKI TELEFONHÍVÁS
- ADATHALÁSZ EMAILEK, SMS-EK
- HAMIS HATÓSÁGI MEGKERESÉS (pl: büntetés, közteher befizetés, pénz visszautalás)

Hallott már az alábbi csalástípusokról?

Váltságdíj 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 'váltságdíjat' követelhetnek, azzal fenyegetve, hogy nyilvánosságra hozzák az ügyféladatokat.

Számlacsalás

Cégéhez ismeretlen ügyféltől érkezik számla, amely teljesen eredetinek kinéző, 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 csaló ügyfelek vitatják a tranzakció, vagy kézbesítés megtörténtét, ami azt eredményezi, hogy cégének vissza kell fizetnie a termék árát. A csalók 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 óvatosnak lenni és konzultálni egy szakértő kollégával!

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

7 TIPP a csalás elleni küzdelemhez, 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 mobiletelefonról, 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 leellenőrizheti, 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 csalónak 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 észben tartanunk, és ezzel hozzáférünk az összes többi jelszóhoz.

3. A számlafizetéseket mindig duplán ellenőrizze!

Jogtalan kifizetés, vagy csaló 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, vigyázzunk 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 középvállalatok 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 KIBERCSALÁS ÁLDOZATÁVÁ VÁLIK, A LEGFONTOSABB AZONNALI TEENDŐK: ÉRTESÍTSE BANKJÁT ÉS TEGYEN FELJELENTÉST A RENDŐRSÉGEN!



Üzleti kibervédelmi KISOKOS

- *Életszerű példák*
- *7 + 1 TIPP*

KKV KIBERBIZTONSÁGI (AWARENESS) EDUKÁCIÓS KVÍZ

KiberPajzs
Védelem a pénzügyekben

Kóddal védett tartalom
A www.kiberpajzs.hu/Partnereknek fülön

Nézd meg a linket Ági: Kiberbiztonsági edukációs kvíz kis- és középvállalatok számára | KiberPajzs
kód: 123456789 **most tesztre**.

Itt az a nagy kérdés, ha itt toborzni is akarsz, akkor kit keressenek elérési kódokért. Lehet, hogy nem kellene mégsem hirdetni, vagy kitalálni akkor, hogy csak annyit mondunk, h keresse a projekt gazdák, vagy Kardos Ferit… bárkit (email címet meg passz, hogy jelezzünk-e)

1 2 3 4 5 6 7 8 9 10

1. Egy régóta ismert beszállító e-mailben jelzi, hogy megváltozott a bankszámlaszáma. A levél stílusa, az aláírás és a kapcsolattartó neve is megegyezik a korábbiakkal. Az új számlaszámot a következő fizetéstől kérik használni.

Mit tesz?

- ○ Megvizsgálom, hogy a kérés ugyanattól a kapcsolattartótól érkezett-e, akivel korábban is dolgoztunk és ha minden megegyezik, rögzítem az új számlaszámot
- ○ Válaszolok az e-mailre, és kérem, hogy egy hivatalos, cégszerűen aláírt nyilatkozatban erősítsék meg a bankszámlaszám-változást.
- ○ A változást csak egy korábban ismert és független csatornán történő visszaigazolás után fogadom el (pl. ismert telefonszám, szerződésben szereplő kapcsolattartó, korábbi hivatalos elérhetőség).



KÖVETKEZŐ

Adatvédelmi tájékoztató

Pontosan!

A beszállítói bankszámlacsalások egyik legfontosabb jellemzője, hogy a támadó gyakran hozzáfér a levelezéshez, vagy nagyon pontosan ismeri a kommunikációs mintákat, amiatt a levél valós kapcsolattartó nevében érkezhet, tartalmazhat helyes aláírást..stb.
Itt tehát nem az a kérdés, hogy az e-mail hitelesnek tűnik-e, hanem h**ogy a változás függetlenül ellenőrzött-e**.

A bankszámlaszám-változás esetén a legerősebb kontroll a független csatornán történő visszaigazolás!

TOVÁBB

Belépési kódért és elérésért keressen bennünket!

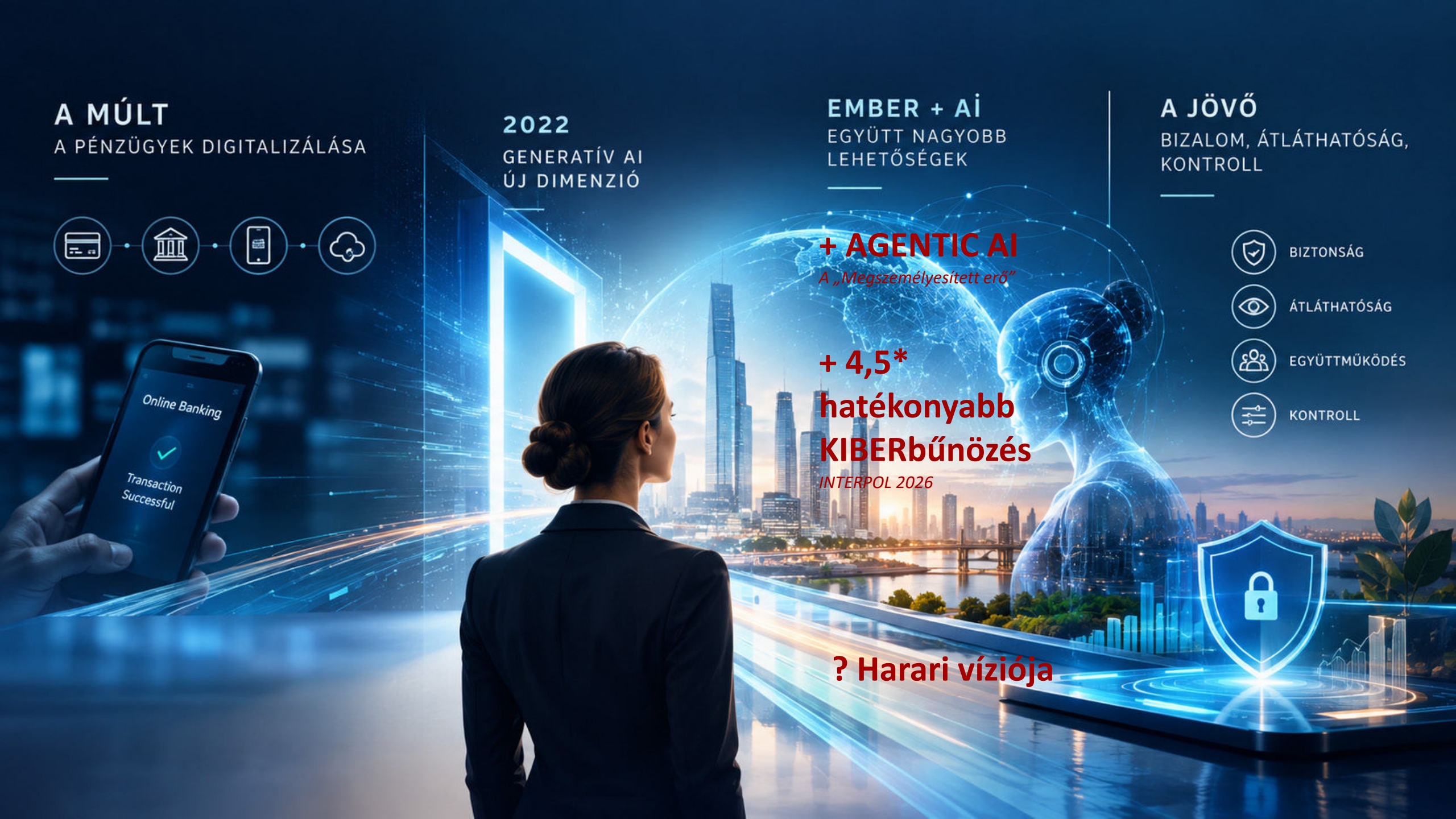


KiberPajzs

Védelem a pénzügyekben

MI és a KIBERpénzügyek

…milyen a jövő?


A MÚLT
A PÉNZÜGYEK DIGITALIZÁLÁSA
Online Banking
Transaction Successful
2022
GENERATÍV AI
ÚJ DIMENZIÓ
EMBER + AI
EGYÜTT NAGYOBB LEHETŐSÉGEK
+ AGENTIC AI
A „Megszemélyesített erő”
+ 4,5*
hatékonyabb
KIBERbűnözés
INTERPOL 2026
? Harari víziója
A JÖVŐ
BIZALOM, ÁTLÁTHATÓSÁG, KONTROLL
BIZTONSÁG
ÁTLÁTHATÓSÁG
EGYÜTTMŰKÖDÉS
KONTROLL

AZ AI ÚJ DIMENZIÓT NYIT

MÁR NEM CSAK FELISMER, HANEM SEGÍT IS –
OTT, AHOL MI TÉVEDÜNK.

- **CSALÓ ÜZENETEK** felismerése
- **SZOKATLAN TRANZAKCIÓK** kiszűrése
- **REJTETT MINTÁZATOK** feltárása
- **TÉVEDÉSEK CSÖKKENTÉSE** támogatása



2022: GENERATÍV AI

ŰJ DIMENZIÓ NYÍLT.

„Az AI akár átveheti a pénzügyi rendszer irányítását – miközben mi már nem is értjük teljesen, mi történik az algoritmusok mögött.”

Yuval Noah Harari
Economist, 2026

A MÚLTBAN
A HOZZÁFÉRÉST VÉDTÜK.

⇒

A KÖVETKEZŐBEN
A FELHATALMAZÁST KELL VÉDENÜNK.

Kié a döntés?
Ki vagy mi cselekszik a nevünkben?



A JÖVŐ KÖZÖS FELELŐSSÉGÜNK
A bizalom új infrastruktúráját kell felépítenünk – biztonsággal, átláthatósággal és felelősséggel.

→

A KONTROLL A KEZÜNKBEN MARADJON –
az AI pedig az éberségünket erősítse a csalókkal szemben.

+

Köszönjük a megtisztelő figyelmet!

Légy résen, és ne te légy rés a pajzson!

www.facebook.com/KiberPajzs

KiberPajzs

Védelem a pénzügyekben