



KiberPajzs
Védelem a pénzügyekben

Üzleti kibervédelmi
KISOKOS

2025. február 20.

Hívószám-hamisítás
Gonosz iker adathalászat
Https adathalászat
Weboldal/domain hamisítás
Telefonos adathalászat
E-mail-es adathalászat
Elosztott szolgáltatás-megtagadásos támadás
Zsarolóvírus
Üzleti e-mail kompromittálás
Sms-es adathalászat
Vezetői csalás/CEO csalás
Közösségi médiás adathalászat
Társadalmi manipuláció
Hamis weboldalak
Lándzsás adathalászat



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

- Alkalmazataink rendszeresen járnak kiberképzésekre
- Az emailjeinket és a dokumentum mappákat csak meghatározott emberek látják
- Számítógépeinket, tableteinket csak ellenőrzés után (PIN, ujjlenyomat, stb.) használhatjuk
- Számláinkat és a kifizéseinket legalább két ember ellenőrzés és engedélyezéssel
- Összetett jelszavakat használunk
- Vírusirtót 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 kibertudatos szakértővel

1-4 Biztató kezdő lépéseket tettünk
5-7 Alapvető fejlesztéseink vannak, érezhetően biztonságosabb környezetet alkotunk kibertudatos, jó gyakorlatokból álló csalókkal szemben

KiberPajzs
Védelem a pénzügyekben

Üzleti kibervédelmi KISOKOS

KIBERTUDATOSÁGI TANÁCSKÖRT ÉS TOVÁBBI CSALÓFOGÓ TIPPEKERT LÁTOGASSON EL OLDALUNKRA

QR code: [kiberpajzs.hu](https://www.kiberpajzs.hu)

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

Hallott már az alábbi csalástípusokról?

Váltógépjelű csalás
Cégre építő mobiltelefonos csalás, amelyben egy csalóval szimulált hívás érkezik a cégre, amelyben a csaló a cégre szólítja fel a vezetőket, hogy beszéljenek vele a csalás megakadályozásáról. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

Számlacsalás
Cégre ismeretlen ügyfélről érkező számlák, amelyek helytelen adatokkal rendelkeznek. A csaló a számla címzettjének partner adatait másolja egy általa elküldött hívással, így a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

Visszajelzéses csalás
Visszajelzéses csalás esetén a csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

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

7 a csalás elleni küzdelemben, a Nemzeti Kibervédelmi Intézet kibertudatos szakértőjétől.

1. Frissítse szoftvereit rendszeresen és telepítse vírusirtó szoftvert is!
A kiberkatasztrófa megelőzése és rendszeres biztonsági frissítések nélkül nem lehet a kiberkatasztrófa megelőzése. A mobiltelefonon is telepítse a vírusirtót, és a mobiltelefonon is telepítse a vírusirtót.

2. Ne jelezzen ki JELMÓNDATOKAT használva!
Győződséggel használja a JELMÓNDATOKAT, hogy megvédje adatait. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

3. A számlafüzeteit mindig duplán ellenőrizze!
A számlafüzeteit mindig duplán ellenőrizze. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

4. Szabályozza a dolgozók hozzáféréseit!
A dolgozók hozzáféréseit szabályozza. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

5. Képezze alkalmazottait rendszeresen kibertudatos allokációk!
A dolgozók kibertudatos allokációk. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

6. Informálódjon, beszélgesse a kibertudatos allokációk!
A kibertudatos allokációk. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

7. MESTERFOKUSZ!
Hozzon létre biztonsági szabályzatot!
A biztonságos allokációk és a veszélyes allokációk. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására. A csaló a csalóval szembe fordított hívást használja fel a csalás megakadályozására.

+1 HA MÉGIS KIBERCASÚS ÁLDOZATÁVÁ VÁLNAK: A LEGFONTOSABB AZONNALI TEENDŐK: ÉRTELTSE BANKJÁT ÉS LEGYEN FELJELENTVE A RENDŐRSÉGEN!

- Figyelemfelkeltés
- Tudatosítás



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
- „Gondos gazda” szemlélet szükséges a munkatársak részéről is
- **ÉRTÉKEK** a kibertérben:
 - ADATOK,
 - HOZZÁFÉRÉS, RENDELKEZÉSI JOG
 - PÉNZESZKÖZÖK

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

Cégehez 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 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 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 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 csalóknak 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 'mesterjelszó' 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 feltesítendő 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, beszélgesen a kibervédelemről!

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

Típek 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-kepzesek/>
- INGYENES szakmai tanácsadás kiberbiztonsághoz kapcsolódóan: <https://digitaltechedih.hu/szolgáltatások/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**



KiberPajzs
Védelem a pénzügyekben

**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 Bízató 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 ellenőrzéséhez
- A hiányzó eszközök, módszerek tudatosítása



KiberPajzs
Védelem a pénzügyekben



KiberPajzs
Védelem a pénzügyekben

Üzleti kibervédelmi
KISOKOS

2025. február 20.