ADATHALÁSZAT

Személyes és pénzügyi adataink komoly értéket képviselnek. Ha ezek illetéktelen személyek részére hozzáférhetővé válnak, az komoly anyagi károkat is okozhat. A bűnözők megtévesztő e-mailek és közösségi oldalakon keresztül küldött üzenetek segítségével próbálnak meg hozzájutni a felhasználók adataihoz. Az e-maileket és üzeneteket nagyon sok embernek elküldik, bízva abban, hogy néhányan bedőlnek és megadják az adataikat.

#Adatahalászat #https #Spam #Phishing #SzemélyesAdatok #PénzügyiAdatok

Az adathalászok jellemzően egy **hamisított weboldalon** keresztül próbálnak személyes és pénzügyi adatokhoz (tipikusan felhasználói név, jelszó, bankkártya adatok) jutni. Megbízható szervezetek, bankok, elektronikus kereskedelemmel foglalkozó weboldalak, online fizetési szolgáltatók ismertségét kihasználva, azok weboldalait **lemásolva** igyekeznek a felhasználók bizalmába férkőzni.

A csalók **e-mailt** vagy közösségi oldalon, illetve egyéb üzenetküldő szolgálatáson keresztül **üzenetet küldenek** a címzettnek, amiben rávesznek az e-mailben vagy üzenetben szereplő **hivatkozás** követésére. Arra kérik a felhasználót, hogy **jelentkezzen be** valamilyen megbízható szervezet (levelezési szolgáltató, PayPal, eBay, bank stb.) honlapjához nagyon hasonlító weboldalra, amit azonban a csalók üzemeltetnek, és itt a megadott személyes és pénzügyi adatok a csalókhoz kerülnek.

TIPIKUS ÜZENETEK

- **Frissítse jelszavát** az alábbi linken!
- **Lépjen be a fiókjába,** ellenkező esetben 24 órán belüli törlődik!
- A mellékelt számla befizetéséhez a linken **adja meg a bankkártya adatait**!

BIZTONSÁGI TANÁCSOK

- Mindig ellenőrizzük, hogy valóban a feladónak tűnő személy, szervezet küldte az e-mailt!
- A bankok nem kérnek e-mailben bankkártya adatokat, más szervezeteknek pedig ne adjuk meg azokat!
- Online történő bankkártyás fizetésnél mindig győződjünk meg arról, hogy valódi bank oldalon adjuk meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adjuk meg azokat!
- Amikor belépünk egy banki vagy bármilyen más oldalra, győződjünk meg arról, hogy az valóban ahhoz szervezethez tartozik. Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (https előtag) oldalon adjunk meg!

ÁRULKODÓ JELEK – E-MAILEK, ÜZENETEK

Bár az adathalász e-mailek és üzenetek egyre kifinomultabbak, azért viszonylag könnyű felismerni, hogy az e-mailt vagy üzenetet csalók küldték:

- a küldő e-mail címe bár **hasonlít** valamelyik megbízható szervezetéhez, attól **eltér**:
- a második szintű tartomány névben: google helyett gooogle vagy g00gle vagy,
- legfelső szintű tartomány nevében (.hu, .com, stb.) google.com helyett google.xyz,
- szervezet **hivatalos** e-mail címe **helyett privát** emailről érkezik: pl. support@paypal.com helyett paypal@gmail.com,

- olyan szolgáltató nevében küldték ki, akivel **NEM ÁLLUNK KAPCSOLATBAN**,
- a levélben használt **MEGSZÓLÍTÁS ÁLTALÁNOS**, nem szerepel benne a címzett neve,
- a szöveg **HELYESÍRÁSI, NYELVHELYESSÉGI HIBÁKAT** tartalmaz, magyartalan, valószínűsíthető, hogy fordítóprogrammal készült,
- bár a megadott link látszólag hasonlít az eredeti oldal címére, a kattintás után a **CÍMSORBAN** teljesen más jelenik meg.

ÁRULKODÓ JELEK – ADATHÁLASZ WEBOLDALAK

Az áloldalak sok esetben kinézetükben, szerkezetükben nagyon **HASONLÍTANAK** az eredeti oldalhoz, más esetben csak szervezet arculati elemeit (színek, logók) alkalmazzák egyszerűsített formában. Vannak az olyan egyértelmű jelek, amelyek jelzik, hogy áloldalról van szó.

- A böngésző címsorában nem a szervezet **HIVATALOS HONLAPJÁNAK** internetes (URL) címe szerepel, hanem teljesen ismeretlen, a hivatalos oldal címére esetleg hasonlító más szöveg.
- A URL címben **HTTPS HELYETT CSAK A HTTP** szerepel, vagyis az oldal nem rendelkezik tanúsítvánnyal és a felhasználó számítógépe és az oldal közötti kommunikáció sem titkosított.
- A megbízható tanúsítvánnyal rendelkező oldalakat a böngészők általában jelzik (általában **KIS LAKATTAL**) illetve **ZÖLD JELZÉSSEL** a böngésző címsorában.