DE IBK

Online piacteres csalások – készülj fel!

Az online piacteres csalások évek óta jelen vannak, ám a pandémia óta új módszerek is megjelentek. Már nem csak a hibás, hamisított termékek ─ vagy egy másik tipikus példát említve, hogy előreutalás után egyáltalán nem kapunk árut ─ jelentenek kockázatot, hanem az érzékeny adatokra utazó adathalászatra is fel kell készülnünk. Mint mindig, ha tájékozottak vagyunk, könnyebben kikerülhetjük a csapdákat, e heti tippünkben ehhez szeretnénk segítséget nyújtani.

Célpontban az eladók

Az utóbbi időben elszaporodtak azok az adathalász támadások, amik a hirdetőket veszik célba.

2020 és 2022 között elsősorban a Jófogáson voltak jellemzők az ilyen típusú a csalások, azonban manapság az összes népszerű piactéren (Vatera, Facebook Marketplace, Vinted, illetve a Foxpost csomagküldő szolgáltatáson) előfordulnak.

2023-ban már közel 400 online piacteres csalásról érkezett bejelentés az NBSZ NKI-hoz. A tapasztalatok szerint sajnos továbbra is sokan áldozatul esnek.

Az átverés első lépéseként a csalótól egy vásárlási szándékot jelző üzenet érkezik, amiben valamilyen kifogással elkérik az **e-mail címünket** vagy egyből egy **webes hivatkozást** küldenek nekünk. Az indok a legtöbbször az, hogy a csaló azt állítja, hogy a kézbesítéshez vagy a vásárlás lebonyolításához szeretne kontaktot egyeztetni.

Másik, gyakori típus, hogy a csaló azt állítja, hogy már előre kifizette a terméket, de a vételár mellett a szállítási díjat is átutalta, amit most szeretné visszakérni. (Ilyenkor a csaló sokszor egy hamis képet is mellékel, amin úgy tűnik, mintha elutalta volna az összeget).

Szintén gyakori, hogy a csaló a szállítás miatt egy **állítólagos** „plusz biztosítási díjra” hivatkozik, ami miatt „zárolva lett” az átutalása. Ilyenkor azt kéri, hogy az eladó ezt fizesse ki számára, és majd ő azt utóbb hozzácsapja vételárhoz. Ez általában nem kiugróan nagy összeg (30-60 000 forint).

Ezekre az adatokra utaznak

Amennyiben az e-mail címünk megadására kérnek minket, a levelezőfiókunkba érkezni fog egy e-mail, egy káros tartalmú webes hivatkozással.

A csaló által küldött hivatkozás az eredeti online piacteres vagy banki oldalhoz hasonlító weboldalra fog irányítani, ahol a leggyakrabban a bankkártyánk legfontosabb adatainak a megadására fognak kérni minket. Ilyen adatok például a kártyabirtokos neve, a bankkártyaszám, a lejárati dátum, a kibocsátó

bank neve, a bankkártya típusa (Visa, Mastercard), illetve az internetes vásárláshoz szükséges CVC2/CVV2 kód

Mire figyeljünk?

- Az üzenetek nyelvezete **gyakran nehezen értelmezhető** és rossz magyarsággal íródik, ezeket könnyű észrevenni. Azonban a fordítóprogramok és a Mesterséges Intelligencia-alapú technológiákat alkalmazó szövegalkotó szoftverek (pl.: **chatGPT**) előretörésével erre egyre kevésbé támaszkodhatunk.
- Ami minden esetben jellemző: **gyors cselekvésre szeretnének rávenni** minket, **személyes átvételtől pedig elzárkóznak**.
- Az üzenetek mindig **tartalmaznak valamilyen gyanús hivatkozást**, amely az eredeti oldalhoz hasonló felületre irányít át minket.

Hogyan védekezhetünk?

- Már a hirdetés feladása előtt fontos lépés, hogy **tájékozódjunk** a felhasználási feltételekről. Az adott piactér weboldalán az impresszum adatokhoz legörgetve találod az Általános Szerződési Feltételeket (ÁFT)
- Soha ne válaszolj kapásból, mindig hagyj egy kis időt magadnak, hogy értelmezni tudd a kapott üzenetet!
- Sose add meg a bankkártya adataidat! [Gondold végig, ahhoz, hogy valaki utalhasson neked, elég a **bankszámlaszámodat** tudnia.]
- Ne kommunikálj a vevővel a platformon kívül (Viberen, WhatsAppon, stb)! Ha mégis egyeztetni kellene, azt telefonon intézd!
- Részesítsd előnyben a személyes átadás-átvételt! Ha erre nincs mód, **tájékozódj** a csomagküldési lehetőségekről!

Amennyiben csalást észlelsz, szakítsd meg a hamis vásárlóval a kapcsolatot és kérjük jelezd az esetet a platform kapcsolati oldalán!