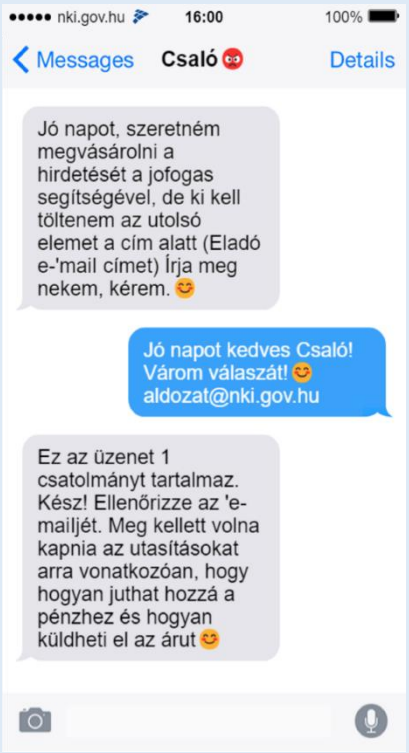
ELBIR

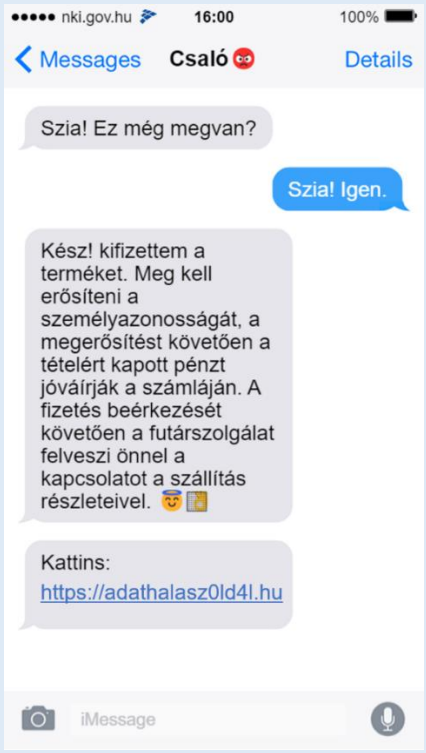
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Célpontban az eladók

Az utóbbi időben elszaporodtak azok az adathalász támadások, amik a hirdetőket veszik célba. A korábbi években elsősorban a Jófogáson voltak jellemzők az ilyen típusú a csalások, azonban manapság az összes népszerű piactéren (Vatera, Facebook Marketplace, Vinted illetve a Fox-post csomagküldő szolgáltatáson) előfordulnak.

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).

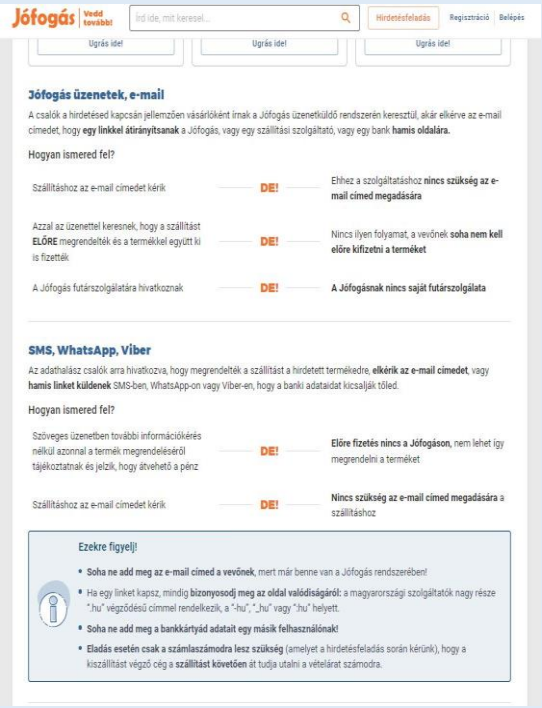
Ezekre az adatokra utaznak

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 1, a bankkártyaszám 2, a lejárati dátum 3, a kibocsátó bank neve 4, a bankkártya típusa 5 (Visa, Mastercard), illetve az internetes vásárláshoz szükséges CVC2/CVV2 kód 6.

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.

Tudtad?



- A Jófogáson a szállításhoz nincs szükség e-mail cím újbóli megadására, mert azt már regisztrációkor megadtad.
- Soha ne válaszolj kapásból, mindig hagyj egy kis időt magadnak, hogy értelmezni tudd a kapott üzenetet!
- Sose add meg a bankkártya adataidat! (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! (A Jófogás Háztól-Házig szolgáltatásának igénybevételekor, a megrendelésekhez kapcsolódó rendszerüzeneteket a regisztrált e-mail címedre küldik meg, illetve ebben az esetben a vásárló közvetlenül a futárnál fizet a termékért.)

Amennyiben csalást észlelsz, szakítsd meg az álvásárlóval a kapcsolatot és jelezd az esetet a platform kapcsolati oldalán (pl.: ugyfelszolgalat@jofogas.hu e-mail címen)! Amennyiben csalás áldozata lettél tegyél feljelentést a rendőrségen!

BÁCS-KISKUN VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes