

Egy gyenge minőségű papucs volt a csomagban

Internetes böngészés közben talált rá egy pápai nő egy hirdetésre, amelyben márkás papucsot kínáltak eladásra. Leadta a megrendelést, és utánvétes fizetési módot választott. Pár nap múlva meg is érkezett a csomaggal a futár, amiért még a kibontás előtt kifizetett 15.500 forintot, anélkül, hogy a tartalmát előtte ellenőrizte volna. Csak később, a csomag kibontása után szembesült azzal, hogy a márkás lábbeli helyett egy jóval kisebb értékű, gyenge minőségű terméket kapott.

A Veszprém Vármegyei Rendőr-főkapitányság Bűnmegelőzési Osztályának ajánlása:

Ha ismeretlen helyről rendelünk, az sem garantálja anyagi biztonságunkat ha utánvétes fizetési módot választunk, hiszen gyakran csak a csomag kifizetését követően ellenőrizhetjük annak tartalmát. Ennek elkerülésére érdemes a már kipróbált, megbízható webáruházakat választani. Ezek többsége már kínál olyan lehetőséget, hogy a csomag tartalmát a kifizetés előtt is lehet ellenőrizni. Kérjük éljen ezzel a lehetőséggel.

Bővebb információk a kiberpajzs.hu oldalon.

A gyermekülés eladása közel 5 millió forintjába került – A családok becsapták

Egy veszprémi férfi gyermekülést hirdetett meg eladásra egy népszerű, használt cikkek kereskedelmére szakosodott weboldalon. A hirdetésre hamarosan jelentkezett egy vevő, aki jelezte vételi szándékát és kérte az eladót, hogy a terméket „háztól-házig” szolgáltatással vásárolhassa meg. Miután az eladó ebbe beleegyezett, kapott egy hivatalosnak látszó e-mailt, ami látszólag a csomagfeladás menetéről és a vételárhoz való hozzájárulásról szólt. Itt elkérték bankkártya és bankszámla adatait, amit meg is adott, beleértve a bankkártyáján található CVC kódot is. Ezután a vételár beérkezése helyett azt tapasztalta, hogy számlájáról közel 4.700.000 forintot leemeltek.

Az ügyben csalás miatt nyomoz a rendőrség.

A következő néhány egyszerű szabály betartásával elkerülhető, hogy Ön is sértetté váljon:

- Nem megbízható forrásból származó linke kattintva vagy ismeretlen webhelyeken soha ne adják meg banki adataikat, beleértve a háromjegyű biztonsági CVC kódot, PIN kódját, illetve netbankjuk belépési adatait!
- Online banki tranzakciókat csak a bank saját online, megbízható felületén keresztül, illetve az előre telepített banki alkalmazásokban végezzenek.
- Ismeretlen eredetű programot soha ne telepítsen fel vagy töltsön le a számítógépére, illetve a telefonjára, bárki is javasolja azt Önnek! Ilyet a bankok soha nem kérnek az ügyfelektől és még arra sem kötelezik őket, hogy a netbankot használják.
- Kétség esetén pedig még az adatok megadását megelőzően vegyék fel a kapcsolatot a pénzügyi intézettel.
- További hasznos tanácsokat az alábbi linken olvashatnak az online csalásokkal kapcsolatban: <https://kiberpajzs.hu/>

VIGYÁZZON AZ ISMERETLEN TELEFONHÍVÁSOKKAL!

Ha bankja nevében keresik telefonon bármilyen gyanús tranzakcióval kapcsolatban, szakítsa meg a hívást és a pénzügyintézet hivatalosan közzétett telefonszámán, illetve a bankkártyája hátoldalán megadott telefonszámon visszahívással győződjön meg annak valóságtartalmáról.

Nem így tett a napokban az a balatonalmádi sértett, aki fogadott egy ilyen hívást, majd a csalók kérésére egy telefonjához távoli hozzáférést is biztosító alkalmazást is telepített telefonjára. Ezt követően valamennyi telefonján végzett művelet, illetve banktól kapott visszaigazoló SMS megismerhetővé vált a bűnelkövetők számára, akik ezt kihasználva közel 7.500.000 forintot utaltak el számlájáról.

A Veszprém Vármegyei Rendőr-főkapitányság Bűnmegelőzési Osztályának ajánlásai:

Különösen fontos, hogy idegenek kérésére semmilyen alkalmazást ne telepítsünk eszközeinkre, illetve idegenek kérésére semmilyen banki adatunkat ne adjuk meg. A hivatalos banki azonosításhoz soha nem kéri internetbankos belépési kódunkat, vagy a bankkártyánk hátoldalán található CVC kódot.

További hasznos információk: www.kiberpajzs.hu