DE IBK

Divatos adathalász csalás – csomagod érkezett

A mobilos adathalász csalások egyre népszerűbbek a kiberbűnözők körében. A felhasználók egy részét viszonylag könnyű megtéveszteni, hiszen a sürgető hangnem, esetleg egy-egy csábító ajánlat, csomag érkezéséről szóló SMS könnyen megtéveztheti az embert.

A támadók egy olyan üzenetet jelenítenek meg a készüléken, amely valamilyen cselekvésre akarja rávenni a leendő áldozatot. Ilyen esetekben (is) a megszemélyesítést használják módszerként, tehát valamilyen ismert szolgáltató, szervezet – ebben az esetben csomagküldő szolgálat – nevében küldik az üzenetet.

A csalók a megtévesztő üzenetekben egy csomaggal kapcsolatos eseményre hívják fel a figyelmet, amihez egy linket is párosítanak. A link egy olyan oldalra mutat, amely – a legtöbb esetben – egy csomagküldő szolgálatnak adja ki magát, és kéri a "saját" applikáció letöltését, és / vagy érzékeny személyes adatok (név, e-mail cím, felhasználónév, jelszó, bankkártya adatok) megadását.

Az SMS szövege lehet például a következő:

- „Megérkezett a csomagja, kövesse nyomon itt [URL]"
- „Jelentkezzen be, hogy megerősítse a kézbesítést. [URL]"
- „A csomag kézbesítése meghiúsult. Csomagja vissza lesz küldve, ha nem erősíti meg: [URL]"

Hogyan védekezhetünk? Mutatjuk!

- Ha kétségek merülnek fel az üzenet valódiságát illetően, akkor mindig javasolt kapcsolatba lépni egy másik csatornán azzal, akinek a nevében érkezett az SMS.
- Az SMS-ben érkezett linkekre semmiképp sem javasolt a kattintás, és a megadott telefonszámokat sem érdemes felvenni egyetlen csevegő alkalmazásba se.
- Amennyiben mégis rákattintottunk a linkre, utána semmiképp se töltsük le azt az applikációt, programot, amit felajánl a rendszer, inkább lehetőség szerint mielőbb töröljük az üzenetet.
- A kapkodás sosem jó. Szánjunk időt arra, hogy átgondoljuk az üzenet tartalmát, és adott esetben nézzünk utána a feladónak, vagy a megszemélyesített szervezetnek más fórumokon. Például az adott cég hivatalos elérhetőségein.
- Soha ne válaszoljunk olyan szöveges üzenetekre, amiben PIN kódot, online banki jelszót vagy más bizalmas adatot kérnek! Ha ez mégis megtörtént, akkor azonnal értesítsük a releváns pénzintézetet!
- Amennyiben ismerős számról érkezik az SMS, az sem garancia arra, hogy megbízható. Lehetséges, hogy az adott ismerősünk már áldozatul esett a csalóknak, így fel tudják használni az ő telefonszámát és adatait is.
- Soha ne telepítsünk mások kérésére olyan programot a telefonunkra (se), amit nem ismerünk, és / vagy harmadik, nem ellenőrzött féltől érkezik.

- Fontos megjegyezni, hogy egyetlen szolgáltató sem kér SMS-ben jelszavakat vagy PIN-kódokat, sem más bizalmas adatokat!
- Ha mégis megadtuk pénzügyi adatainkat, akkor javasolt minél gyorsabban felvenni a kapcsolatot a bankunkkal.