

Adathalász banki e-mail (phishing)

Ez az adathalász csalási forma olyan, banki ügyfeleket célzó, csaló szándékú e-mail, amely személyes, pénzügyi vagy biztonsági információi megosztására próbálja rávenni a címzettet.

Ezek a levelek azonosnak tűnhetnek azokkal az üzenetekkel, amelyeket a létező bankok küldenek: a csalók lemásolják a valódi e-mailek logóit, kinézetét és stílusát, esetenként korábbi (hamis vagy valós) levélváltások részleteit is tartalmazzák.

Általában sürgető hangvételűek, például büntetéssel fenyegetnek arra az esetre, ha valaki nem válaszol, de arra is kérhetik, hogy töltsön le egy mellékletet, vagy kattintson egy hivatkozásra.

A kiberbűnözők arra építenek, hogy az emberek elfoglaltak: felületes áttekintésre, futó pillantásra a hamis e-mailek igazinak tűnnek. Ennek következtében a címzett nagyobb valószínűséggel veszi komolyan őket, és cselekszik a leírtak szerint.

Mit tegyen, hogy ne váljon ilyen csalás áldozatává?

Kezelje óvatosan, fenntartással a kéretlen banki e-maileket!

Minél sürgetőbb a levél hangvétele, legyen annál gyanúsabb!

Legyen különösen éber, ha egy „banki” e-mail bizalmas információkat kér, például az online banki jelszavát! A bankok kizárólag biztonságos módon, az online banki felületen vagy mobilapplikációban kommunikálnak az ügyfelekkel, sosem kérnek bizalmas adatokat ilyen formában!

Ne kattintson az üzenetben lévő hivatkozásokra, és ne nyissa meg a mellékleteket, a webes bejelentkezések címeit inkább manuálisan gépelje be, vagy használja a hivatalos (esetleg a kedvencek közé elmentett) banki oldalt!

Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvételekkel szemben, amely során nem tud minden kétséget kizáróan megbizonyosodni a másik fél identitásáról! Különösen igaz ez az elektronikus kommunikációra: ne válaszoljon a gyanús e-mailekre!

Vizsgálja meg alaposan az e-mailt! Keressen furcsaságokat, következetlenségeket és értelmetlennek tűnő dolgokat, például a következőket: furcsa nyelvezet, helyesírási hibák, sürgető hangnem, szokatlan formátumú csatolmány (.zip stb.).

Keressen nehezen észrevehető különbségeket a feladó címében: a nulla például nagy „o” betűnek tűnhet: 0 vs. O! Vesse össze a küldő e-mail-címét a bank korábbi üzeneteivel!

Legyen különösen körültekintő a mobil eszközök használatakor! Telefonon vagy táblagépen nehezebb lehet észrevenni az adathalász kísérleteket. Nem lehet a gyanús hivatkozások fölé vinni az egérmutatót, és a kisebb kijelző miatt a nyilvánvaló hibákat is nehezebb beazonosítani.

A gyanús e-maileket jelentse bankjának: minden vállalat szívesen veszi az ilyen típusú támadásokról szóló információkat. Ha kétségei vannak, hívja fel a bankját!

Mindig tartsa naprakész állapotban szoftvereit, beleértve a böngészőt, a vírusirtó programokat és az operációs rendszert!

Úgy érzi, hogy csalás áldozatává vált, illetéktelenekhez kerültek jelszavai, azonosítói? Hívja telefonon a számlavezető bankját, majd a rendőrséget, és jelentse be az eseményt!