Ön & biztonságos bankolás

Kedves Imre!

A K&H vállalati biztonságtudatosság program részét képező hírlevelekben megismerheti a leggyakoribb vagy az aktuálisan legnagyobb veszélyt jelentő támadási formákat, valamint ezek kivédési módjait. A vállalatokat érintő támadások sok esetben specifikusabbak, mint azok, amelyeknek elsősorban a magánszemélyek a célpontjai, azonban a vállalatok esetén is elég egyetlen óvatlan kolléga és már meg is történik a baj. Hírlevél sorozatunkban abban próbálunk segíteni, hogy a kollégák megértsék a veszélyt, ami rájuk – és rajtuk keresztül a vállalatra leselkedik.

mi is az adathalászat?

Az adathalász támadások arra irányulnak, hogy **kicsalják az érzékeny információkat** az áldozatoktól, például jelszavakat, bankkártya-adatokat vagy személyes adatokat, esetleg valamiféle kártevőt, kémprogramot telepítsenek. A levelek általános jellemzője, hogy érzelmi nyomást próbálnak gyakorolni. Ilyen lehet egy nagyon kedvező ajánlat, de az ellenkezője, valamilyen hátrány, szankció kilátásba helyezése is. Sok esetben ezek a levelek az emberi kíváncsiságra apellálnak (pl. Nézd csak ki van ezen a képen!) és sürgető hangvételűek. A levelek gyakran magyartalanságokat tartalmaznak (erre azonban nem hagyatkozhatunk, a mesterséges intelligencia segítségével közel tökéletes levelek készíthetőek). A levelek káros, vagy meghamisított oldalra mutató linket, vagy csatolmányt tartalmaznak, feladójuk sok esetben szokatlannak tűnik.

hol találkozhatunk vele?

Ezeket a megkereséseket jellemzően nagy mennyiségben (százezres-milliós nagyságrendben) küldik el a csalók, válogatás nélkül bárkinek, akinek az adatai birtokukban vannak. Emiatt elmondható, hogy adathalász megkeresést bárki és szinte bármilyen csatornán kaphat. A leggyakoribb adathalász csatorna az e-mail és a telefon

(vishing), amely során a hitelesség érdekében a támadók a telefonszámot is meghamisít(hat)ják.

Magánszemélyként a csomagküldő szolgálatok, vagy streaming szolgáltatók nevében küldött támadások gyakoriak, melyek leginkább – de nem kizárólag – sms-ben (smishing) érkeznek. A csalók esetenként az azonnali üzenetküldő alkalmazásokon keresztül küldik el az üzenetet. Feltörekvő támadási forma a hamisított QR-kód beolvastatása az áldozattal (quishing).

Vállalatként jelentős részben - de nem kizárólag - e-mailes támadásokkal találkozhatunk, amik az esetek nagy többségében a vállalat dolgozóihoz érkeznek, rosszabb esetben kulcspozícióban levő kollégákat céloznak. Emiatt érdemes a munkatársakban tudatosítani, hogy a levelek veszélyesek lehetnek abban az esetben is, ha - akár nevesítetten - csupán egy kolléga kapja meg őket magánszemély (és nem vállalati dolgozó) szerepében (pl. konferencia meghívó, sajtómegkeresés).

Az elmúlt időszak leggyakoribb adathalász csalásai:

- Fokozottan ügyelj a biztonságra, ha a NAV nevében érkezik megkeresés!
- & TE ismered a nyárhoz kapcsolódó csalásokat?

hogyan lehet védekezni ellene?

ellenőrizze a linket

Az írásban történt adathalász támadások esetén a legfontosabb a link (QR kód) ellenőrzése: az egeret a link fölé húzva a képernyő bal alsó sarkában, vagy a link felett/alatt/a képernyő sarkában megjelenő ablakban megnézhető, hogy a link valójában milyen weboldalra mutat. Ilyen értelemben a QR-kód is linkként kezelendő és ugyanígy ellenőrizhető. A K&H Bank leveleiben található linkek minden esetben a kh.hu-ra mutatnak (pl. hirlevel.kh.hu, exponea.kh.hu, idopontfoglalas.kh.hu)

figyeljen a megfogalmazásra

Ha egy levél nyelvtani hibákat tartalmaz, túl jó ajánlattal kecsegtet, felkelti a kíváncsiságot, vagy félelmet kelt, esetleg sürget, semmiképp nem szabad a linkre kattintani, vagy megnyitni a csatolmányt!

gyanakodjon szokatlan eljárás esetén

Mindenképp érdemes szem előtt tartani, hogy a bankok semmilyen körülmények közt nem kérik telefonhívásban

- az ügyfelek jelszavát, ePIN, mPIN, vagy 3D Secure megerősítő kódját,
- nem kérik, hogy távoli elérést biztosító alkalmazást telepítsenek az ügyfelek és
- nem kérik, hogy utalják pénzüket egy másik, „szuperbiztonságos” számlára.

Ha ilyen megkereséssel találkozunk, biztosak lehetünk abban, hogy csalók próbálják megszerezni adatainkat és/vagy pénzünket.

További információk a K&H Bank Biztonság a pénzügyekben oldalán találhatóak.

banki támogatás a védekezéshez

Minden ügyfélnek lehetősége van a K&H vállalkozói mobilinfo szolgáltatás segítségével specifikus SMS értesítések igénylésére, ami segít gyorsabban azonosítani az illetéktelen hozzáféréseket és így mérsékelhető az okozott kár is. A szolgáltatás segítségével szabadon meghatározható az értesítési telefonszám, beállítható, hogy milyen típusú vagy milyen összeg feletti tranzakciókról szeretne értesülni. További információkat a szolgáltatásról a mobilinfo oldalán találhat. Igénylés kapcsán keresse a K&H Vállalati ügyfélszolgálatot.

Üdvözlettel:
K&H Bank

Vállalati Ügyfélszolgálat +36 1 468 7777 » kh.hu » bank@kh.hu a KBC Csoport tagja