információbiztonsági tudnivalók - célzott adathalászat

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 az a célzott adathalászat?

A célzott adathalászat (spear phishing) az adathalászat egy sokkal veszélyesebb fajtája, melyek jellemzően inkább a vállalkozások, vállalatok közép- és felsővezetőit célozzák, ahol nagyobb a megtérülés lehetősége, mint a magánszemélyek esetében. A célzott adathalász támadásokat általában – időnként hetekig, hónapokig tartó – kutatómunka előzi meg annak érdekében, hogy a megtámadott személy nagy eséllyel kattintson linkre, nyisson meg csatolmányt.
A célzott támadások **testre szabottak: jellemzően szervesen kapcsolódnak a célszemély üzleti tevékenységéhez, esetleg magánéleti hobbijához** (pl. utazás) stb. A feladójuk első ránézésre valódinak tűnik, nem egyszer a megtámadott személy ismeretségi, üzleti köréből kikerülőnek látszik, vagy magas reputációval rendelkező szervezetet (pl. sajtó, felügyeleti szerv, stb.) imitálva történik. A célzott adathalász támadások nyelvezete nem árulkodó, tökéletes, választékos magyarsággal készülnek, a bennük szereplő link – ha van bennük link – általában rejtett (pl. bit.ly). Gyakoriak a csatolmányok, melyeket megnyitva kártékony kód, vagy akár billentyűzet leütést naplózó alkalmazás (keylogger) települ.

hol találkozhatunk vele?

Az elmúlt időszak leggyakoribb adathalász csalásai:

- Számlákkal kapcsolatos egyeztetésre kér az MNB? Légy óvatos!

hogyan lehet védekezni ellene?

A célzott adathalász támadások ellen a nagyfokú figyelem és fegyelem nyújthat némi védelmet.

azonosítsa a feladót

Gondosan ellenőrizzük a levél tartalmát, stílusát, helyesírását és a küldőjét is. Ne bízzunk meg abban, hogy látszólag ismerőstől, vagy partnertől kaptunk megkeresést. A legkisebb gyanú esetén is ellenőrizzük vissza a megkeresést egy másik csatornán. Ha tehát egy partner vállalkozástól kapunk e-mailt, akkor az általunk már ismert telefonszámon hívjuk fel a kapcsolattartót és ellenőrizzük, hogy valóban ők küldték-e a levelet.

ellenőrizze a linket

A rejtett linkek ellenőrzésére az Interneten találunk olyan weboldalakat, amelyek segítségével meg tudjuk nézni, hogy valójában hova mutat a link. Ha mégsem tudjuk ellenőrizni, inkább ne nyissuk meg, a csatolmányokon pedig megnyitás előtt futtassunk jogtiszta vírusirtót. Amennyiben a vállalatnál vannak erre szakosodott – kiberbiztonsági – szakemberek, akkor kérjük meg őket, hogy megnyitás előtt vizsgálják meg az e-mailt.

átgondolt megjelenések

A célzott támadások esetén különösen igaz, hogy a megelőzés a legjobb védekezés. Ne osszuk meg a magánéleti történéseinket, fényképeinket a különféle közösségi médiafelületeken, vagy ha mégis megtesszük, akkor figyeljünk a láthatósági beállításokra. Ne állítsuk publikusra ismerőseink listáját és ne engedélyezzük, hogy „tageljenek” minket előzetes hozzájárulásunk nélkül.

Törekedjünk a magánélet és a vállalati életünk teljes szétválasztására, ami azt is jelenti, hogy magáneszközeinken ne kezeljünk vállalati adatokat.

banki támogatás a védekezéshez

A biztonság érdekében fontos, hogy az elektronikus bankoláshoz minden vállalati felhasználó külön azonosító eszközzel rendelkezzen és azokhoz ne biztosítson más számára hozzáférést. A szoftveres azonosító eszközök pl. ViCA alkalmazás biztonságos és egyben kényelmes alternatívát nyújt a fizikai tokenekkel szemben, hiszen további eszköz csatlakoztatása nélkül közvetlenül desktopról elérhető, rendszeres frissítése is egyszerűbb. K&H web Electra rendszerbe már a ViCA okostelefonra fejlesztett alkalmazásával is beléphet, így jelszó alkalmazása helyett akár biometrikus azonosítást (ujjlenyomat vagy arcfelismerés) is választhat.

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

Üdvözlettel:
K&H Bank

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

Ezt a levelünket a(z) imre.fonai1@gmail.com címre küldtük.

Leveleinket minden esetben a K&H Bank hivatalos domain-jéről küldjük, tehát a feladó e-mail címében **a @ utáni rész utolsó két tagja minden esetben kh.hu**. Leveleink csak kh.hu aloldalaira mutató linket tartalmaznak, azaz, ha a link fölé húzza az egérkurzort, az ablakban megjelenő link címének első része minden esetben kh.hu, vagy cdn-exponea.kh.hu.

Az adathalászat komoly fenyegetést jelent mindenki számára. A támadó bármilyen online csatornán, de SMS-ben, vagy épp telefonon is megkeresheti. A K&H Bank soha nem kezdeményez telefonhívást a +36 1/20/30/70 335-3355 telefonszámok bármelyikéről**, ezeket a számokat kizárólag ügyfelek telefonhívásainak fogadására tartja fenn**. Amennyiben az előbbi számok bármelyikét látja a kijelzőn, telefonszám hamisításos csalás áldozatává válhat, ezért ilyen esetekben kérjük, hogy haladéktalanul szakítsa meg a vonalat. Kérjük, hogy mielőtt az adatait kiadná, győződjön meg arról, hogy a kapcsolatot felvenni szándékozó személy vagy szervezet az, akinek mondja magát és soha ne kattintson gyanús üzenetben érkező linkre, vagy csatolmányra.

KiberPajzs
Védelem a pénzügyekben

Vértezze fel magát a kibercsalásokkal szemben, látogasson el a KiberPajzs honlapra! (https://kiberpajzs.hu)
További információkat a https://www.kh.hu/biztonsag-a-penzugyekben oldalon talál.
Ügyeljen adatai biztonságára!

Jelen üzenetet a K&H Bank Zrt. (1095 Budapest, Lechner Ödön fasor 9., a továbbiakban: Bank), mint adatkezelő korábban adott hozzájárulása alapján küldte meg Önnek a részére megadott elektronikus levelezési címére.

Hozzájárulását kifejezetten erre a programra vonatkozóan bármikor, korlátozás és indokolás nélkül, ingyenesen visszavonhatja a bubadigi@kh.hu elérhetősége felé intézett nyilatkozattal. Hozzájárulás visszavonása hiányában a Bank a regisztráció során megadott adatait a program végét követően, legkésőbb 2025. év végén törli.

Az adatkezeléssel kapcsolatos bővebb tájékoztatást a https://www.kh.hu/adatvedelem internetes oldalon található Adatkezelési tájékoztatóban, valamint a Bank Üzletszabályzatában talál, továbbá személyes adatai kezeléséről tájékoztatást kérhet a Bank Vállalati Ügyfélszolgálatán (+36 1 468 7777, vallalatiugyfelszolgalat@kh.hu).

Jelen üzenet nem minősül ajánlattételnek. A kondíciók módosításának jogát a Bank fenntartja. A mobilinfo termék részletes leírását, illetve feltételeit az ügyfélszerződés, a Vállalati ügyfelek részére nyújtott pénzforgalmi és betéti szolgáltatások Általános Szerződési Feltételei, a K&H Mobilinfo szolgáltatás Általános Szerződési Feltételei, az Elektronikus azonosítású banki szolgáltatások Általános Szerződési Feltételei, az Üzletszabályzat, valamint az aktuális Hirdetmény vállalati ügyfelek részére tartalmazza.