Fogyasztóvédelmi figyelemfelhívás, az Online adathalász "támadások" hatékonyabb megelőzése érdekében!

Az online vásárlások jelentős mértékű növekedésével párhuzamosan az adathalászok is egyre kifinomultabb módszerekkel és egyre gyakrabban próbálják megszerezni az online vásárlók adatait, beleértve bankkártyaadataikat is.

Adatainak védelme érdekében ezért kérjük, hogy fokozottan ügyeljen a biztonságos bankkártya-használatra, valamint figyelmesen olvassa el az alábbi tájékoztatást!

Felhívjuk szíves figyelmét arra, hogy az ügyfelek bankkártyájukat saját kockázatukra használhatják, így a kártyabirtokos saját kockázata körébe tartozik, hogy kinek, mikor, hol, milyen módon adja meg a kártyaadatait.

Az interneten terjedő csalások legtipikusabb formája az adathalászat (angolul: phishing). A csalók adathalászat esetén egy internetes csaló oldalt készítenek, amely egy jól ismert cég hivatalos oldalának látszatát kelti, melynek segítségével különböző, aprólékosan kidolgozott megtévesztő módszerekkel megpróbálnak személyes adatokat, valamint a banki műveletekhez szükséges bizalmas, titkos adatokat (például: azonosító kódot, jelszót, bankkártyaszámot, cvv kódot stb.) megszerezni. Ezekkel aztán belépnek az ügyfél internetbankjába, és onnan előre megszervezett számlákra utalják az ügyfél pénzét.

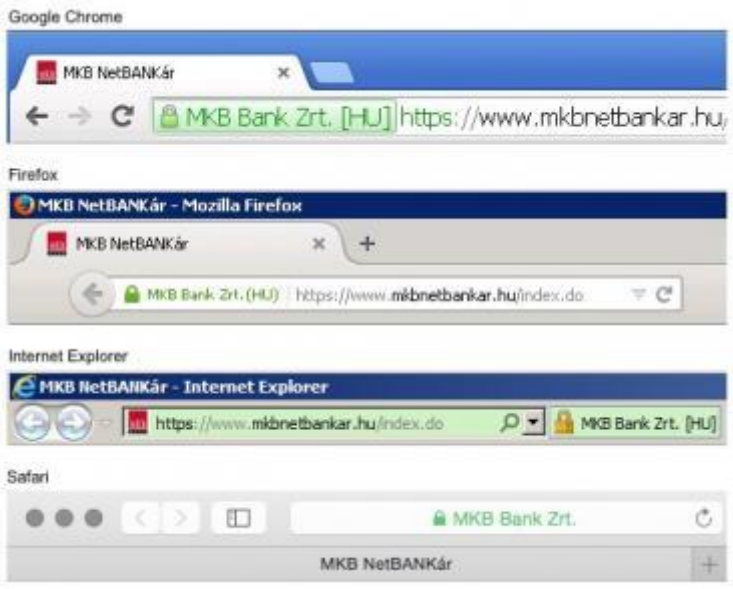
Honnan ismerhető fel a csaló e-mail?
Egyik ismert módszer, hogy a csalók online szolgáltatók (pl. Paypal, Apple) nevében email-t küldenek, melyben tájékoztatják, hogy biztonsági okokból zárolták a hozzáférést az érintett fiókjához, amit úgy tud feloldani a kártyabirtokos, ha az email-ben küldött linkre lépve frissíti az adatait. A csalók által küldött link minden esetben hamis, bár látszólag az online szolgáltató felületére visz, amely egy űrlapot tölt be a személyes és a kártyaadatok megadásához. Fontos, hogy ezek az e-mailek megjelenésüket tekintve nagyon hasonlítanak a szolgáltató által alkalmazott megjelenítési formára (fejléc, grafika stb.), de ha magyar nyelven íródnak, akkor általában rossz magyarsággal.

Tudnia kell, hogy a számlavezető hitelintézetek, illetve a megbízható online kereskedők sosem kérnek e-mailben, a weboldalukra beírással, vagy SMS-ben személyes adatot, továbbá más "érzékeny" adatokat, mint pl. PIN kódot, jelszavakat, kártyaszámokat. Különösen érvényes ez az "adatfrissítés", vagy ehhez hasonló címen kért adatátadásra. A kártyaszámot is csak az a bank kéri el a kiválasztott fizetés teljesítése során, amely kibocsátotta a bankkártyát, és amelynek elektronikus banki rendszeréhez az online vásárlás során kapcsolódik a vásárló. Az ilyen e-mail adatkérések minden esetben rosszhiszeműek, mindig csalók (valamint az ő megbízottaik) küldik.

Mi a teendő, ha adathalász gyanús e-mailt kap?
Mindezek alapján, amennyiben banki, államigazgatási, vagy online szolgáltató nevében "biztonsági felkérés"-nek nevezett e-mail érkezik postafiókjába, és az egyedi ügyfél-azonosító, belépési jelszó, PIN-kód, kártyaadatok megadására kéri Önt, kérjük, ne válaszoljon rá, és haladéktalanul értesítse az e-mailben megnevezett bankot (pénzügyi szolgáltatót) vagy online szolgáltatót. Kérjük, hogy ehhez mindig a szolgáltató hivatalos telefonszámát használja, ne pedig azt, amelyet az e-mailben esetlegesen feltüntettek.
Ugyancsak gyakran alkalmazott módszer az, hogy az adathalászok e-mailek segítségével az ügyfeleket hamis – de az eredetire hasonlító – megtévesztő internetbanki oldalra irányítják. Ilyen lehet például valamelyik pénzügyi intézmény internetbankjának kezdőoldala.
Fontos, hogy a megtévesztő szándékkal küldött e-mailek igen gyakran adatmegadásra, aktualizálásra szólítanak fel, vagy valamilyen fenyegetést fogalmaznak meg, pl. olyan mondatok kíséretében, mint ha nem adja meg az adatait, akkor a számla zárolásra kerül.

Honnan ismerhető fel a megtévesztő weboldal?
Kérjük, ügyeljen arra, hogy a bankok/pénzügyi intézmények "valódi" honlapján a böngésző alsó sávján/felső címsorában szerepel a biztonságos kapcsolat meglétét jelző lakat ikon. A böngésző címsorába található **zárt lakat** ikonra kattintva meggyőződhetünk arról, hogy a „https" kapcsolat valóban biztonságos és a megfelelő webhelyen tartózkodunk! Ha ezt nem látja, gyanúra ad okot.
Ugyancsak figyelmeztető jel, ha az online szolgáltató böngészőjében "https" védett kapcsolat helyett csak "http" látható a weblapcím előtt. Ebben az esetben nem a legerősebb elérhető védelem épül fel az ügyfél gépe és az intézmény között.

Biztonságos kapcsolat jelölése a különböző böngészőkben:



Kérjük, figyeljen arra is, hogy a "https" után az elérni kívánt pénzügyi intézmény weblapcíme álljon, mint ahogyan a fenti képeken is látszik.

Az elektronikus banki szolgáltatások biztonságáról és a csalások elleni védekezésről az MNB Pénzügyi Fogyasztóvédelmi Központjának honlapján olvashatók további információk.

Az adathalászok trükkjei a fentiekben ismertetetteken túl lehetnek még olyanok, mikor az ügyfelek adatait nem interneten, hanem telefonon keresztül (telefonhívás/SMS) igyekeznek megszerezni.

A fentiek mellett az is előfordulhat, hogy a csalók trójai programot telepítnek a számítógépre. A telepítést úgy oldják meg, hogy egy látszólag hivatalos e-mailben, ami érkezhet egy banki, államigazgatási, vagy online szolgáltató nevében, egy linket helyeznek el. Ha erre Ön rákattint, akkor látszólag egy "banki alkalmazást" nyit meg, valójában azonban ártó szándékú szoftvereket, vírusokat tölt le a számítógépére, amelyek megpróbálják leállítani a víruskereső- és tűzfalprogramokat.
A trójai program észrevétlenül települ a számítógépre, és megszerzi a fontos információkat (ügyfél-azonosítók és jelszók). A megszerzett adatokat a csalóknak küldi el, akik ezekkel követik el a csalásokat. A trójai programmal szemben megfelelő vírusvédelemmel, tűzfal- és kémelhárító programmal lehet hatékonyan védekezni.

Ezúton is kérjük Önt, hogy biztonsága érdekében SOHA NE VÁLASZOLJON olyan, látszólag a banktól, vagy online szolgáltatótól érkező e-mailekre, SMS-ekre, amelyekben jelszavának, valamint bankkártya biztonsági kódjának, esetleg egyéb érzékeny pénzügyi, illetve személyes adatainak

megadására kérik. Amennyiben ilyen tartalmú e-mailt kap, kérjük, azonnal hívja a Külföldről is hívható ügyfélszolgálati telefonszámunkat: 36 (1) 373-3333.

További fontos kiegészítések az "Önök Biztonságáért" című tájékoztatónkból:

- Az MKB adategyeztetésre felhívó üzenetet SOHA nem jelenít meg honlapján és internet banki rendszerében sem, kivétel ez alól a születési dátum, melyet csak és kizárólag a NetBANKár belépési felületen, többszöri jelszórontást követően kérjük megadni. Minden ettől eltérő kérés bizonyosan csalárd próbálkozás.
- Amennyiben elektronikus banki szolgáltatást vesz igénybe, ellenőrizze a bank weboldalának eredetiségét.
- A lehető legnagyobb körültekintéssel járjon el banki adatainak megadásakor. Tegye fel magának a kérdést, hogy vajon a webhelyen kért információ megadása indokoltnak tűnik-e az Ön által éppen végzett tevékenység során. Nem indokolt például, hogy egy online aukciós webhelyen jogosítványának/útlevelének számát vagy hitelkártyájának PIN-kódját kérjék Öntől. Amennyiben egy webhelyen, vagy email-ben indokolatlanul banki adatokra kérdeznek rá, ne válaszoljon.
- Olyan vállalkozások online szolgáltatásait vegye igénybe, amelyeket ismer és megbízhatónak tart. Amennyiben egy weboldalt gyanúsnak talál, esetleg kétségei merülnek fel adatainak biztonságát illetően, kérjük, ne adja meg adatait és hagyja el a weboldalt.

MKB Bank Zrt.