Az adathalászat reneszánsza

Világszerte 540 millió online bankoló, Nyugat-Európában például az internethasználók 50-60%-a jelent állandó célpontot az adathalászoknak. A comScore mérései szerint például Hollandiában az internetezők kétharmada használ netbank szolgáltatásokat, ami a legmagasabb arány Európában - de a többi ország sincs nagyon lemaradva. Ennyi potenciális célponttal nem csodálkozhatunk rajta, ha az adathalászat reneszánszát éli.

2009. őszén számoltak be a különböző médiumok a hazai bankokat és felhasználókat érintő igazán profi adathalász támadásokról, amelyek az OTP, Erste és Raiffeisen bankokat vették célba. Utána pár év nyugalom következett, de az adathalászok most már okosabbak és kreatívabbak mint valaha, és új átverésekkel próbálnak ismételten hozzáférést szerezni bankszámláinkhoz.

Most bemutatjuk a legújabb banki átveréseket, amelyek úgy tűnik 2012-ben is meghatározó szerepet töltenek be és messze a legnagyobb anyagi kárt tudják okozni az otthoni internetezés közben.

Trükkös bankkártya csalások

Újfajta bankkártya csalási trükköknek köszönhetően akár már a PIN-kód ismerete nélkül is kifoszthatják számlánkat a leleményes bűnözők, miközben bankkártyánk ott lapul a pénztárcánkban és mi mit sem sejtünk az egészről.

Vásárlás és licitálás 'készpénznyereménnyel'

Egy eddig nem túl elterjedt, de annál eredményesebb csalási módszer látott napvilágot a napokban Magyarországon: a csalók egy újfajta telefonos-internetes trükk segítségével szereznek több tízezer forintot gyanútlan áldozataik bankszámlájáról. Találomra felhívnak embereket és közlik velük, hogy nagy összegű pénznyereményt nyertek, majd ahhoz, hogy ezt minél gyorsabban megkapják, megkérik őket, hogy adják meg bankkártya adataikat.

Miután megszerezték a szükséges információkat, egy internetes aukciós oldalon megvásárolnak egy előre kinézett terméket. Az online vásárlásnál ugyanis nem kell megadni PIN-kódot; a név, a bankkártya száma és a lejárati dátum megadása elegendő a vásárláshoz. A fizetésnél azonban a csalók nem a termék árának megfelelő összeget utalnak át az eladónak, hanem a kért összeg többszörösét. Majd ezután felhívják az eladót, hogy véletlenül nagyobb összeget utaltak át, és megkérik, hogy a vásárolt termék átvételekor a többlet összeget készpénzben adja vissza nekik.

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, e-mail: elbir@bacs.police.hu

A csalóknak így bankkártya nélkül is sikerül készpénzhez jutniuk úgy, hogy az eladó nem is tudja, hogy éppen egy bűncselekményhez nyújt segítséget, az áldozat pedig csak akkor szerez tudomást az átverésről, amikor a remélt nagy összeg helyett inkább még kevesebb pénzt talál a számláján.

Adathalász emailek

Tárgy **Figyelem! Ön MKB fiók korlátozott volt!**
Feladó MKB Bank
Címzett [redacted]
Dátum Szer 08:09

Tisztelt MKB Bank tag:

Figyelem! Ön MKB fiók korlátozott volt!

Mint a mi biztonsági intézkedések, rendszeresen képernyo tevékenység az MKB rendszerben.
Nemrégiben a kapcsolatot veled észlel, egy kérdés a fiókjában.

Ha bejelentkezik, akkor látni helyreállítása érdekében fiókja hozzáférést.
Köszönjük megértését, mint mi a munka annak érdekében vegyék a biztonságot.

Kattintson ide, hogy aktiválja fiókját

Köszönjük a gyors választ erre a kérdésre.
Kérjük, értse meg, hogy ez egy biztonsági intézkedés, amelynek célja, hogy segítsen megvédeni Önt és számla.
Elnézést kérünk az esetleges kellemetlenségekért.

MKB Bank Zrt.
Székhely: 1056 Budapest, Váci u.38.
Cégjegyzék helye és száma:
Fovárosi Bíróság, mint Cégbíróság,
Cg. 01-10-040952

MKB TeleBANKár
Lakossági ügyfélszolgálat: 06-40-333-666
Vállalati ügyfélszolgálat: 06-40-333-777
Külföldrol: +36-1-373-3333

A bankkártyás csalások másik alapvető eszköze az e-mailes adathalászat. A telefonos megkeresés helyett sokszor e-mailen keresztül próbálnak meg a csalók személyes adatokhoz hozzájutni. A bank nevében küldenek egy levelet, amelyben azt kérik, hogy a levélben található linkre kattintva jelentkezzünk be az internetbank oldalára. A link azonban nem a megnyitni kívánt oldalra mutat, hanem csupán egy ahhoz nagyon hasonló weboldalra, ahol felhasználó nevünket és jelszavunkat begépelve már ki is szolgáltattuk személyes adatainkat a csalóknak. (Ilyen esetekre rendkívül értékessé válik a vírusvédelem, vagy a böngésző káros honlap szűrője!)

Az elmúlt napokban pont egy ilyen adatlopási kísérletre figyelmeztette ügyfeleit az OTP Bank. A csalók a pénzintézet arculatának megújulását kihasználva küldtek ki számtalan levelet, amelyben arra kérik a számlatulajdonosokat, hogy a levélben található linkre kattintva frissítsék személyes adataikat a bank weboldalán. Mivel épp most változott a hivatalos honlap is, ezért a bankolók jó eséllyel keverik össze a hamis oldallal, hiszen ki tudná eldönteni, hogy ez éppen az új dizájn, vagy egy átverés?

Aki pórul jár, neki a link egy hamis oldalra vezet, ahol egy űrlapot kitöltve személyes adatokat kérnek a felhasználóktól. Bár a hamis oldal rendelkezik néhány hibával: a böngésző címmezejében például otpbank.hu helyett a mozambiquematters.com (vagy más) oldalcím olvasható, a kitöltendő adatlapon pedig a CVV kódot az (automatikus) fordítás során "spórás növény" feliratra cserélték, ami szerencsére feltűnő és meglehetősen vicces hiba. Viszont ha valaki nem nézi meg figyelmesen a betöltött oldalt, akkor és a hibák is elkerülhetik a figyelmét, akkor máris a csalók áldozatául eshet. A nagy számok törvénye alapján pedig az is bőven megéri a csalóknak, ha ezerből csak egy netbank felhasználó belépési adatait sikerül megszerezni.

6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, e-mail: elbir@bacs.police.hu

Adathalászat a Facebookon

Ha adathalászatról, csalásról van szó, akkor természetesen a Facebook sem maradhat ki a sorból, ahogy azt már korábbi cikkeinkben is bemutattuk. Szívesen próbálunk ki különböző alkalmazásokat, vagy töltünk ki kvízeket a Facebookon, amit a csalók előszeretettel ki is használnak.

Manapság több, a Facebook stílusához hasonlóan kinéző kérdőív terjed, amely elsősorban bankkártya adatainkra kíváncsi. A gyanútlan felhasználóktól a szokásos, interneten megadni tilos adatokat: a kártyatulajdonos nevét, a bankkártya számát, lejárati dátumát, a kártyaazonosítót és a számlatulajdonos címét kérik el, hogy az átverés szerint így ellenőrizzék a személyazonosságát, és hogy biztonságosabbá tegyék Facebook-fiókját. Aki azonban gondolkodás nélkül kitölti az űrlapot, annak adatai rögtön a csalók kezére jutnak, és így bármikor hozzáférhetnek az áldozat bankszámlájához annak tudta nélkül.

Pedig a bankkártya alapú azonosítás nem ördögtől való. Európában több országban használnak bankkártyát például a cigaretta-árusító automatáknál, még készpénzes fizetés esetén is, hiszen a bankkártya nagyszerűen alkalmas például a tulajdonos korának ellenőrzésére. Így a kiskorúak hiába dobálják be a cigivásárláshoz elegendő készpénzt, egy "felnőtt korú" bankkártya nélkül mégsem vásárolhatnak. Az analógiával élve a Facebookon is ideális megoldásnak tűnik személyazonosságunk bankkártyával történő igazolása, pedig a valóságban ez komoly átveréshez fog vezetni.

Hogyan tudunk védekezni?

Az online adathalász csalások egyre inkább szaporodnak és mindig valamilyen új módszerrel próbálnak meg a bűnözők személyes információkat megtudni áldozataikról. Fontos tehát, hogy vigyázzunk adatainkra, és ne adjuk meg őket ismeretlen online oldalakon, kérdőívekben. Még azokat az adatainkat sem, amik ártalmatlannak tűnnek.

Ugyanígy óvatosan bánjunk a bankoktól érkező levelekkel és telefonokkal is. A bankok se telefonon, se e-mailben nem kérik el bankkártya adatainkat, hiszen ha valakik, akkor ők ezeket pontosan tudják. Ha bárki banki alkalmazottnak mondva magát mégis ezt kéri tőlünk, akkor kezdjünk el gyanakodni és semmiféleképpen ne adjuk meg neki adatainkat, inkább hívjuk a bank központi számát. Internetbankunk honlapcímét is mindig magunk gépeljük be a böngészőbe, ne egy linkre kattintva nyissuk meg az oldalt. Ha pedig bármilyen gyanús pénzmozgást fedezünk fel bankszámlánkon, ne habozzunk, és azonnal hívjuk bankunk ügyfélszolgálatát és jó eséllyel visszajuthatunk pénzünkhöz!

Forrás: www.vipre.hu

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, e-mail: elbir@bacs.police.hu