Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

Adathalászat (phishing)

2012. május

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető....3
Adathalászat (phishing)....3
Banki és pénzügyi szektor ellen irányuló támadások....3
A biztonságos banki weboldal ismertető jegyei....4
Adathalász weboldalak....4
Adathalász e-mailek....6
Javaslatok....8
Egyéb adathalász támadások....9
Javaslatok....9
Elérhetőségeink....10

Bevezető

Napjaink egyik komoly informatikai fenyegetései közé tartozik az adathalász (phishing) tevékenység. Az adathalászat leginkább a banki és pénzügyi szektort érinti, de nem elhanyagolható a speciálisan egy-egy szervezet vagy cég ellen indított adathalász támadás sem.

Adathalászat (phishing)

Maga a phishing szó a „password” és a „fishing” szavakból tevődik össze, kb. annyit jelent, mint jelszavakra halászni. Az adathalászathoz a támadó változatos módszereket használnak, így egyre gyakrabban hamisítanak e-maileket vagy weboldalakat, és ezzel próbálva a felhasználókat rávenni bizalmas adatok (jelszavak, hozzáférési adatok, bankkártyaszámok, speciális céges adatok) kiszivárogtatására, amelyet a későbbiekben a támadó felhasznál.

Banki és pénzügyi szektor ellen irányuló támadások

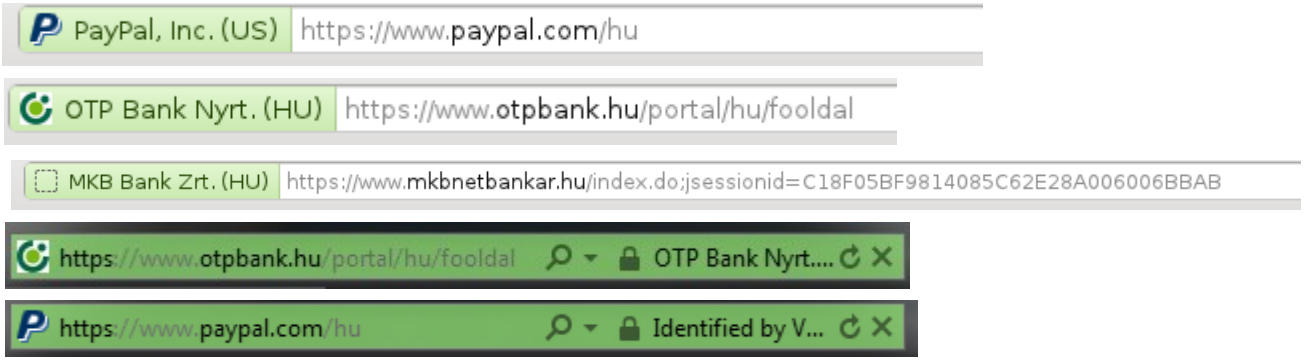
Az adathalászat leginkább a banki és a pénzügyi szektort érinti, hiszen egy, a támadó által megszerzett bankkártya adat, online bankfiók hozzáférési adata az esetek nagy többségében mindig az áldozat megkárosításával jár. Napjaink informatikai technikáinak felhasználásával a banki és pénzügyi szektort nem csak adathalász támadások érhetik, hanem egyre gyakrabban fordul elő szolgáltatás megtagadás (DoS - Denial of Service) vagy elosztott szolgáltatás megtagadás (DDoS - Distributed Denial of Service) támadások. Az ilyen jellegű támadások célja a banki vagy a pénzügyi tranzakciókat bonyolító weboldal lebénítása. A támadók így jelentős fennakadásokat tudnak okozni a weboldal normál üzemeltetéséhez képest. Ilyen DDoS támadás zajlott Észország elektronikus kormányzata ellen 2007. április és májusában, amely a bank szektort is érintette, és komoly anyagi károkat okozott mind az állampolgárok, mind a bank szektor számára - a támadás következtében a banki rendszer megbénult, sem az átutalás, sem a készpénz felvétel nem volt lehetséges. A bankok és a pénzügyi tranzakciókat lebonyolító weboldalak üzemeltetői nagy figyelmet fordítanak arra, hogy weboldaluk a lehető legjobban legyen védve a külső (esetleg belső) forrásból érkező támadások ellen, ezért nagyon ritkán fordul elő az, hogy kompromittálnak egy ilyen weboldalt.

Az ügyfeleknek és a felhasználóknak tisztában kell lennie arról, hogy hogyan lehet felismerni az eredeti banki vagy pénzügyi tranzakciókat lebonyolító weboldalt, illetve arról, hogy hogyan lehet felismerni egy hamisított weboldalt. Ennek köszönhetően, amikor a felhasználó találkozik egy ilyen szituációval, akkor tudni fogja, hogy mi a teendője.

A biztonságos banki weboldal ismertető jegyei

Az első és legfontosabb, hogy **a bankok soha nem kérik el a felhasználóneveket és a jelszavakat**. Az eredeti banki vagy pénzügyi tranzakciókat lebonyolító weboldalak megnyitásakor a felhasználó több dolgot is megfigyelhet, hogy meggyőződjön arról, hogy a weboldal valóban eredeti e.

Az első ilyen a címsáv



A képeken látható címsávokból megállapítható, hogy ez eredeti weboldal megnyitásakor a címsáv egy része vagy egésze zöld színben látszódik, ami a biztonságos HTTPS kapcsolatot jelenti. A HTTPS kapcsolat azt jelenti, hogy az adatok titkosításra kerülnek a weboldal és a felhasználó között, valamint az oldal egy olya tanúsítvánnyal rendelkezik, amely bizonyítja a weboldal eredetiségét. Továbbá az is látszódik, hogy a weboldal neve semmilyen módon nincs módosítva (lsd. későbbi fejezetek).

Amennyiben a weboldalon hírek olvashatók, úgy a felhasználó arról is meggyőződhet, hogy azok mennyire aktuálisak, ugyanis a bankok rendszeresen frissítik híreket.

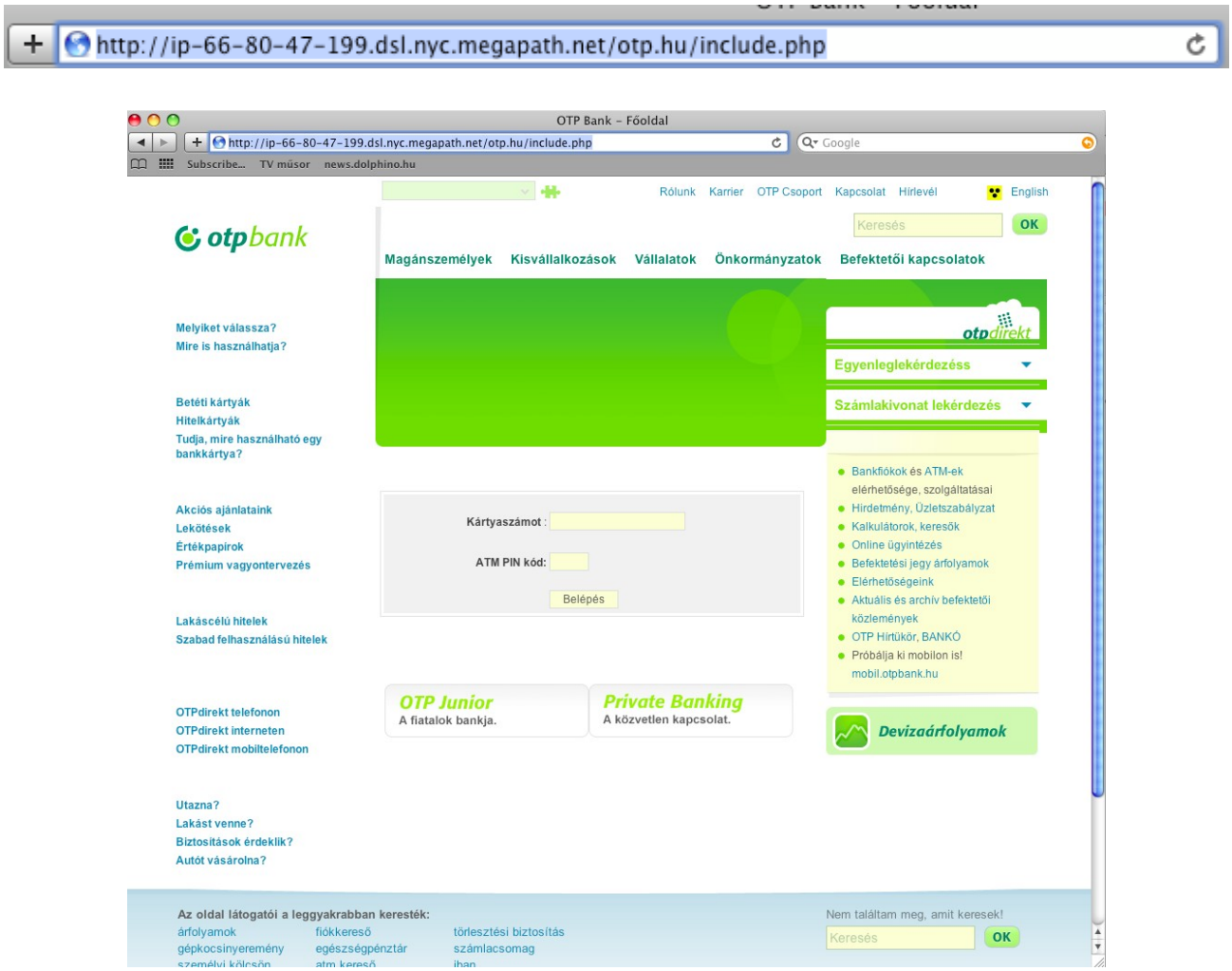
Adathalász weboldalak

A banki és a pénzügyi szektort érintő adathalász tevékenység kapcsán a támadók minden esetben igyekeznek az adott banki vagy a pénzügyi tranzakciókat bonyolító weboldalt a megszólalásig lemásolni, hogy a gyanútlan felhasználó ne sejtsen semmit, és „önként” megadja belépési és/vagy bankkártya adatait. A csalók vagy olyan internet címeket használnak, amelyek csak csekély mértékben térnek el a komoly cégekétől, vagy meghamisítják különböző módszerekkel a böngésző cím mezőjét, esetleg módosítják az operációs rendszer hosts fájlját - így a hamisított weboldal, bármilyen weboldal címének megfeleltethető, így ez a módszer nehezen felismerhető. Viszont attól, hogy egy weboldalt lemásolnak, attól még a felhasználók ezeket az oldalakat nem találják meg. Ahhoz, hogy egy adathalász weboldal üzemeltetése a támadók számára megtérüljön a felhasználókat erre a hamisított weboldalra kell irányítania.

Ilyen weboldalakra példa a következő képek:

Az első kép a böngésző címsávját mutatja. A címsávból látható, hogy a weboldal nem az eredeti PayPal weboldalra mutat, hanem annak egy kitűnő másolatára. Amennyiben a felhasználó itt adja meg belépési adatait, úgy azok a támadó kezére jutnak, és a későbbiekben komoly esélye van a megkárosításnak.

Az adathalász támadások nem csak a nagy külföldi bankokat és pénzügyi tranzakciókat lebonyolító weboldalakat érik. A magyarországi bankok ellen irányuló adathalász támadást is meg kell említeni. A lentebb található képeken is jól látható a böngésző címsávja, amely egyértelműen árulkodik arról, hogy a weboldal nem az eredeti banki oldal.

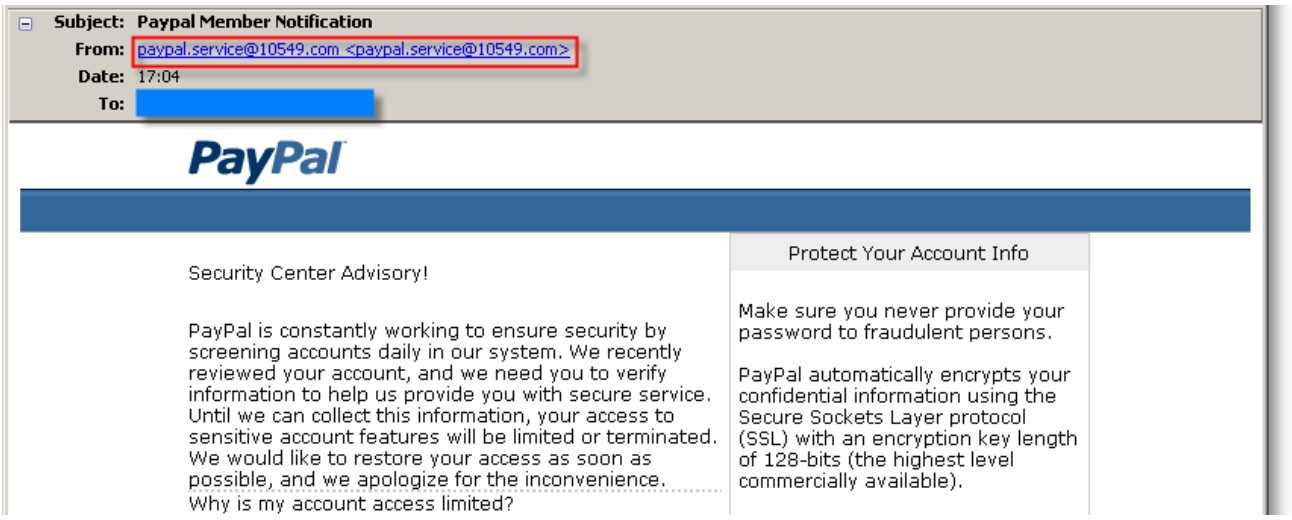


Adathalász e-mailek

A támadók az ügyfelek és a felhasználók az adathalász weboldalra irányítását legegyszerűbben e-mailen keresztül tehetik meg úgy, hogy komoly bankot, vagy egyéb céget imitálva a csalók a címzetteket az e-mailben arra szólítják fel, hogy aktualizálják adataikat, olyan ürüggyel, hogy pl. lejár a hitelkártya, meg kell újítani a jelszót, a hozzáférési adatok elvesztek, stb. Az ilyen tartalmú levelek hitelesnek látszanak. Ezek a HTML formátumú e-mailek tartalmaznak egy hivatalosnak tűnő linket, amely mögött azonban maga az adathalász oldal található.

A támadók igyekeznek olyan e-mail üzeneteket küldeni a felhasználók és az ügyfelek részére, amely eléggé hiteles ahhoz, hogy a felhasználó meglátogassa az adathalász weboldalt. Egy ilyen e-mail üzenetet a figyelmes felhasználó a feladóból (lsd. képek) és a e-mail törzsének szövegezéséből meg tudja állapítani a csaló szándékot.

Az e-mailek szövegezése nagyon eltérő lehet. Külföldi bankok és pénzintézetek általában angol nyelven kommunikálnak ügyfeleikkel, így ezen e-mailek megírása egyszerűbb, de több esetben is észrevehető, hogy az e-mail szövegezése hibás. A magyar bankok ellen irányuló adathalász támadásokhoz tartozó e-mail üzenetek jelentős része könnyen felismerhető, ugyanis az e-mailt elolvasva az ügyfelek és a felhasználók számára szembetűnő lehet az elektronikus levél „magyartalansága” és helyesírási hibái. A következő képek ezeket szemléltetik.



Subject: Paypal Member Notification
From: paypal.service@10549.com <paypal.service@10549.com>
Date: 17:04
To:

PayPal

Security Center Advisory!

PayPal is constantly working to ensure security by screening accounts daily in our system. We recently reviewed your account, and we need you to verify information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited or terminated. We would like to restore your access as soon as possible, and we apologize for the inconvenience.
Why is my account access limited?

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal

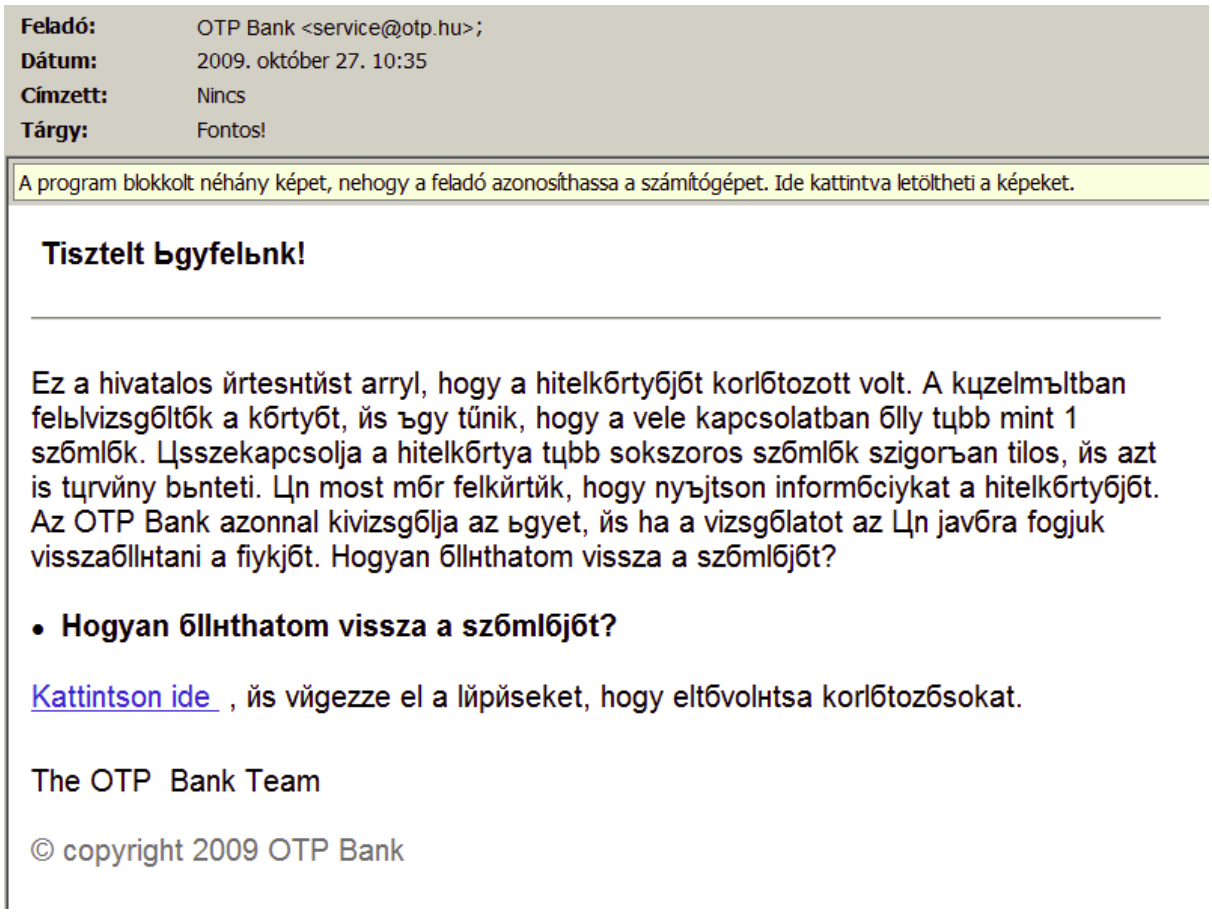
Dear **PayPal** ® customer,

We recently reviewed your account, and we suspect an unauthorized transaction on your account.
Protecting your account is our primary concern. As a preventive measure we have temporary **limited** your access to sensitive information.
Paypal features.To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.

- Login to your Paypal with your Paypal username and password.
- Confirm your identity as a card memeber of Paypal.

Please confirm account information by clicking here Resolution Center and complete the "Steps to Remove Limitations."

•Please do not reply to this message. Mail sent to this address cannot be answered.



Feladó: OTP Bank <service@otp.hu>;
Dátum: 2009. október 27. 10:35
Címzett: Nincs
Tárgy: Fontos!

A program blokkolt néhány képet, nehogy a feladó azonosíthassa a számítógépet. Ide kattintva letöltheti a képeket.

Tisztelt Ьgyfelьnk!

Ez a hivatalos йrtesнtйst arryl, hogy a hitelkбrtyбjбt korlбtozott volt. A kцzelmъltban felьlvizsgбltбk a kбrtyбt, йs ъgy tűnik, hogy a vele kapcsolatban бlly tцbb mint 1 szбmlбk. Цsszekapcsolja a hitelkбrtya tцbb sokszoros szбmlбk szigorъan tilos, йs azt is tцrvйny bьnteti. Цn most mбr felkйrtйk, hogy nyъjtson informбciykat a hitelkбrtyбjбt. Az OTP Bank azonnal kivizsgбlja az ьgyet, йs ha a vizsgбlatot az Цn javбra fogjuk visszaбllнtani a fiykjбt. Hogyan бllнthatom vissza a szбmlбjбt?

- **Hogyan бllнthatom vissza a szбmlбjбt?**

Kattintson ide , йs vйgezze el a lйpйseket, hogy eltбvolнtsa korlбtozбsokat.

The OTP Bank Team

© copyright 2009 OTP Bank

Biztonsági intézkedések Spam | X

feladó **MKB Bank** <info@mkb.hu> részletek elrejtése máj. 14. (7 napja) Válasz
címzett
dátum 2009. május 14. 11:32
tárgy Biztonsági intézkedések

A képek nem kerülnek megjelenítésre.
Az alábbi képek megjelenítése

Kedves MKB ugyfel , Biztonsagi okokbol is felfuggesztettek a fiokjat, egy biztonsagi intezkedes, amelynek celja, hogy megvedjuk Ont es szamla.
Meg kell ujra az adatokat a folyo fizetesi merleg visszaallitja a mukodeset a fiokjat, es megerositi, hogy meg nem volt az aldozatok szamitogepes lopas.
Meg kell ujra adja meg az adatokat a kovetkezo oldalon, hogy az ellenorzesi folyamat soran:

https://www2.mkbnetbankar.hu/login.jsp?lang=HU&start=true

Koszonjuk szives egyuttmukodeset.

© MKB Bank Zrt. Impresszum | Adatvedelmi iranyelvek | Jogi nyilatkozat

A bankoknak és a pénzügyi tranzakciókat lebonyolító weboldalak számára is bosszúságot jelent az adathalász tevékenység, mert gyakran szenvednek el imázs romlást. Szinte minden cég dolgozik olyan módszereken melyekkel ügyfeleiket védik, például több jelszópáros használata, időnként kötelezően változtatandó jelszó, egyszer használatos jelszavak, SMS-ben kapott jelszavak, stb.

Javaslatok

Egységes, jól bevált és minden helyzetre illő megoldás az adathalász támadások esetében nincs. Csak a felhasználón és az odafigyelésén múlik, hogy kikerülnek e hozzáférési adatai egy esetleges

támadás során. Így elővigyázatossággal és figyelmességgel a kockázatok nagymértékben csökkenthetők az alábbiak figyelembevételével:

- A bankok és pénzügyi intézetek sose kérik el a felhasználónevet és a jelszót az ügyfelektől.
- Egy banki weboldal megnyitásakor, minden esetben meg kell győződni arról, hogy ez az eredeti banki weboldal. Erre több megoldás is lehetséges. A böngészők zöld színnel emelik (lsd. fent) ki a címsávot a biztonságos HTTPS kapcsolatot használó weboldalak esetében, valamint egy lakat jel jelenik meg a címsávban.
- Amennyiben az ügyfél levelet kap a banktól vagy pénzügyi szervezettől, úgy minden esetben érdemes a feladót ellenőrizni, illetve ha a levél linket tartalmaz azt alaposan megnézni, hogy milyen oldalra mutat.
- Amennyiben egy gyanús e-mail üzenetet kap vagy weboldal nyílik meg a böngészőben, minden esetben vegye fel a kapcsolatot a bankkal vagy pénzügyi szervezettel.
- Mindig a legfrissebb adatbázissal rendelkező anti-vírus szoftvert és személyi tűzfalat is érdemes használni, ugyanis elképzelhető, hogy a hamisított weboldal káros szoftvert is megpróbál a felhasználó gépére telepíteni.

Egyéb adathalász támadások

Mivel napjainkban a legtöbb cég és/vagy szervezet rendelkezik valamilyen online felülettel, akár azért, hogy elérhetőek legyenek az Interneten, akár azért, hogy valamilyen szolgáltatást nyújtsanak ügyfeleik számára, ezért ezen felületek és szolgáltatások ellen irányuló adathalász tevékenység mellett sem szabad elmenni. Minden cég kínosan ügyel saját fejlesztéseire, webes felületeinek elérhetőségére és biztonságára, az érzékeny üzleti titkok és/vagy adatok biztonságára stb. Éppen ezért előfordulnak olyan célzott adathalász támadások, amelyek üzleti és/vagy ipari titkokat igyekeznek megszerezni, amelyet aztán más cégeknek tovább lehet értékesíteni, a haszon reményében. Ezen információszerzés egyik támadási formája lehet a social engineering („emberi ráhatás”). Ennél a támadási formánál az emberi gyengeségeket használják ki a támadók, megkerülve ezáltal a hardver- és szoftvereszközök segítségével implementált biztonsági kontrollokat, így a bűnözők hozzáférést szerezhetnek a számítógéphez. Egy sikeres adathalász támadás kivitelezéséhez hozzájárulhat a hiányos informatikai és biztonsági szabályzat hiányossága, vagy az alkalmazott hiányos ismerete ezekkel a szabályozásokkal kapcsolatban. A manipuláció célja többnyire az, hogy a támadók titokban kémprogramot vagy más kártékony programot telepítsenek a számítógépre, vagy rávegyék a felhasználót, hogy kiadja jelszavait vagy más bizalmas pénzügyi- és személyes adatait. Egyesek könnyebbnek találják az emberek gyengeségét kihasználni, mint a szoftverekéit.

Javaslatok

- Ne adjon meg e-mailben vagy interneten (esetleg telefonon) semmilyen személyes adatot, ha nem tudja, ki és miért kéri.
- Ne telepítsen nem megbízható forrásból származó alkalmazást vagy programot.
- Mindig a legfrissebb adatbázissal rendelkező anti-vírus szoftvert továbbá személyi tűzfalat is érdemes használni, így a káros kódot tartalmazó szoftverek feltelepítésének kockázata csökkenthető.
- Informatikai- és adatvédelmi szabályzatok folyamatos felülvizsgálata, és az alkalmazottak részére ezek megfelelő ismertetése.

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937