Adathalász e-mail felismerése

Kivonat Paul Arnote (parnote) – „Teltale Singns Of A Pishing E-mail” című cikkéből

PCLinuxOS Magazine – 2015. november

Írta: Paul Arnot (parnote)

Az adathalászat örökké jelen van, de különösen az év vége felé válik ismét aktuálissá, amikor az ünnepek közeledtével az ajándékvásárlási láz fokozódik.

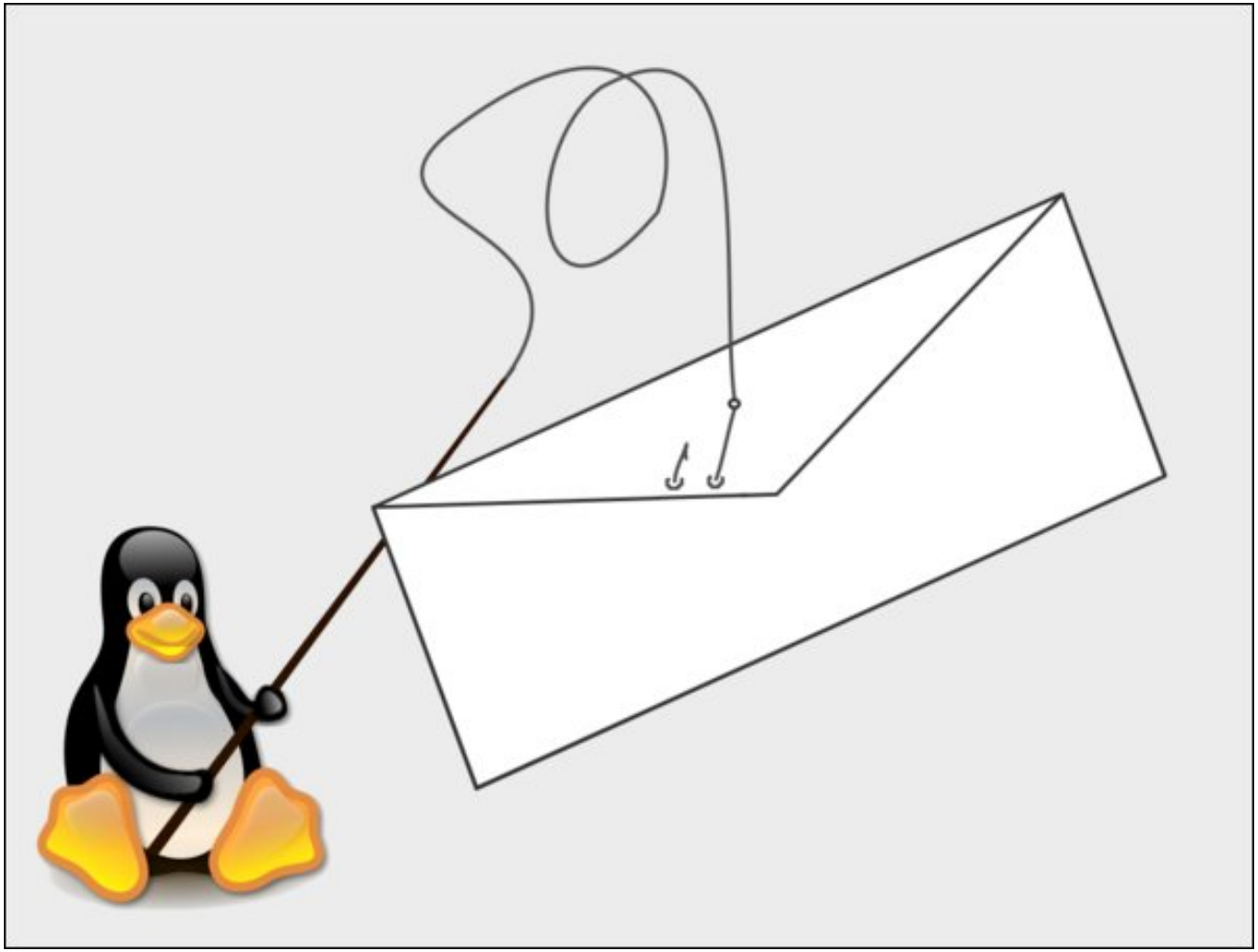
Az adathalászatnak *(eredetileg angolul phishing, kiejtése: fising, a fishing=halászat szóra hasonlít) azt az eljárást nevezzük, amikor egy internetes csaló oldal egy jól ismert cég hivatalos oldalának láttatja magát, és megpróbál bizonyos személyes adatokat, például azonosítót, jelszót, bankkártyaszámot stb. illetéktelenül megszerezni. A csaló általában e-mailt vagy azonnali üzenetet küld a címzettnek, amiben megpróbálja rávenni az üzenetben szereplő hivatkozás követésére egy átalakított weblapra, ami külsőleg szinte teljesen megegyezik az eredetivel. - forrás: http://hu.spam.wikia.com/wiki/Phishing*.

Mik azok a jelek, amik alapján gyanakodhatunk, hogy egy e-mail valószínűleg adathalász átverés?

Túl szép ahhoz, hogy igaz legyen. Felajánl megvételre egy terméket olyan áron, ami túl szép ahhoz, hogy igaz legyen, és nem is igaz.

Nem egyező az URL-címek. Az e-mailben valahol megjelenik egy hivatkozás, de a weblap, amire valójában küld, teljesen más. A modern levelező programok esetén, csakúgy, mint a webböngészők, ha az egérmutató a hivatkozás fölé kerül, megjeleníti a cél URL-jét. Ez lesz az, ami más mint az e-mail szövegében leírt cím.

Félrevezető domain nevek. Ezzel könnyen félrevezethetik a figyelmetlen olvasót. A weblapok névkialakítási struktúrájának ismerete sokat segíthet itt. Például a https://msdn.microsoft.com/en-us/ a miicrosoft.com-hoz tartozó valós domain, mivel a mó-dosító msdn jelölés a microsoft.com domain név-



ől balra jelenik meg. Ugyanakkor a cím: https://msdn.microsoft.com.valamiwebdomai.com nem tartozik a microsoft.com-hoz, hanem a valamiwebdomain.com oldalra irányít.

Nyelvtani és helyesírási hibák. Egy cég magát valamire is tartó marketing szervezete nem engedheti meg, hogy hibás leveleket küldjön ki. A nagyobb cégeknél például külön egység felügyeli a kimenő körleveket. (Szerk.: magyar nyelv esetén ez még kirívóbb, mert a fordítóprogramok nem képesek követni a jelentéstartalom szerint módosuló mondatszerkezeti változásokat, ha a hibás szóhasználatot és ragozást most nem is említjük.)

A költségek fedezésére pénzt kér. Noha ritkán fordul elő, hogy már az első levélben pénzt kérjenek (bár néhány merészebb egyén egyenesen a közepébe vág), de amikor bizonyos költségek fedezeteként (csomagolási, szállítási díjra, adókra, a nagymama bakancsfűzőjére stb.) pénzt kérnek, akkor nagy valószínűséggel elbúcsúzhatsz az ilyen előre küldött összegtől.

Személyes adatokat kér. A bankod sosem kér személyes információkat, amire szükségük van, azt mind tudják. Más cégek pedig nem fognak ilyen banki információkat – hitelkártyaszám, jelszó, vagy biztonsági kérdések – kérni.

Általad nem kezdeményezett ügyletek, lottó és „Ön nyert" típusú üzenetek. Aki nem játszik (pl. lottó), az sosem nyerhet (pl. a lottón). Nem beszélve arról, hogy a lottózóban nem kérik el az e-mail címedet, így nem is értesíthetnek a nyereményedről. Emellett a lottószámokat ismerve úgyis tudom, hogy nyertem-e (vagy sem). Másfajta becsapós üzenetek kérhetik a személyes információidat (közötte a bankkártyaszámodat), a személyi azonosítókártyádról másolatot stb., különben a bankszámládat befagyasztják. Bank nem fagyaszt be számlát azért, mert e-mailre nem válaszoltál.

Régebbi üzenettípus, hogy a **Facebook-fiókod megsérült.** Emiatt kérnek személyes információkat. A Facebook, a számára szükséges információkkal rendelkezik. Ez különösen akkor lehet feltűnő, ha az egyén, mint parnote is, sosem rendelkezett Facebook-fiókkal.

Állami szervként jelöli meg magát. Noha az állami szervek levelezhetnek e-mailben, de sosem, vagy nagyon ritkán indítanak ügyet elektronikusan. (Szerk.: a hivatalos üzenetekben valamilyen hivatkozási szám, kapcsolattartó és hozzá telefonszám stb. mindenképpen megjelenik. Kétség esetén a telefonszámot, ami legritkább esetben mobil szám, érdemes ellenőrizni. Esetleg a hivatkozott szervezet elnevezését nem árt ellenőrizni.)

Egyszerűen csak gyanús az üzenet. Ha úgy érzed, hogy valami nem tiszta, vagy gyanús, **BÍZZ A MEGÉRZÉSEIDBEN!**

Ál-adakozási kérések. Különösen az ünnepek környékén gyakran próbálnak visszaélni az együttérzéseddel. Légy különösen körültekintő, amikor a nehezen megtakarított pénzedet, vagy a személyes adataidat adod ki.

Csomagodat postázták típusú üzenet. Éértesítést kapsz, hogy a megrendelésedet postázták és ha a hivatkozásra kattintasz, akkor valamilyen kém-, vírus-, vagy rosszindulatú programot telepítenek a gépedre … Ez a Windows-felhasználókat fenyegeti igazán. A Linux-felhasználóktól esetleg „nyugtázást" és személyes adatokat kérhetnek. Nem árt, ha tudod, milyen cégekkel kötöttél eddig üzletet, milyen megrendeléseid vannak folyamatban.

Posted by Yankee, on October 25, 2015, running LXDE.