A phishing és a szolgáltatók felelőssége

2021. november 17.

Dravecz Tibor
ügyvezető
INTEGRITY Kft.

Marczisovszky Dániel
CTO
INTEGRITY Kft.

"Phishing is a type of social engineering where an attacker sends a fraudulent ("spoofed") message[1] designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware." – Wikipedia

Phishing

Erste Bank Zrt. <no-reply@erstebank.hu> Érvényesítse most ! <https://direktnet.raiffeisen.hu/direktnet/img/head_logo.png> Tisztelt Ügyfelünk, DirektNet-profilját zároltuk 04-11-2020 07:11:01 Fiókjának feloldásához kattintson ide <http://36.89.140.122/aspx.php> Üdvözlettel, Raiffeisen Bank Zrt. --- Dear Customer, Your DirektNet profile has been locked on 04-11-2020 07:11:01 To unlock your account, please click here <http://36.89.140.122/aspx.php> Regards, Raiffeisen Bank Zrt.	Totál Bank Zrt. <info=totalbank.hu@bnc.protopmail.com>; on behalf of; Totál Bank Zrt. info@totalbank.hu [Norton AntiSpam] ***SPAM*** Energiahatékonysági hitel 0%-os kamattal! <https://esputnik.com/repository/applications/images/blnk.gif> <https://img.automizy.com/28a7~~~c6a380097~~~a7492045e9940778/emaileditor/c81821118a~~~eada7a858c4a8e4d81e21dd6431.jpg> Tisztelt Ügyfelünk! Növelje lakásának, házának energiahatékonyságát, csökkentse rezsiköltségeit és telepítsen megújuló energiaforrásokat az akár 10 millió Ft-ig is felvehető, fix 0%-os kamatozású kölcsönnel! … Üdvözlettel: Totál Bank Zrt. … ADATKEZELÉSSEL KAPCSOLATOS TUDNIVALÓK Jelen levelünket a 2020.06.11-én hatályban lévő … juttattuk el Önnek. Ön bármikor, indoklás nélkül kérheti adatainak … kezelésének megszüntetését. Az adatkezelés megszüntetésére vonatkozó kérelmet postai úton vagy e-mailben lehet a Bankhoz eljuttatni számlaszáma(i) feltüntetésével (Totál Bank Zrt., 9999 Budapest, e-mail: info@totalbank.hu). <https://opn.automizy.com/5/dS6LpImttCf5FrP~~~CuV76WRl0f2voK4dnP8mfvRxfCyqnqHO30dj47Qxx8-8.gif>

[1] például e-mail üzenet

Honnan ered a probléma?

A(z e-mail) phishing probléma alapja:

- hamis címet (forrást, szerzőt, feladót stb.) adhat meg a feladó,
- költséghatékonyan, könnyen és büntetlenül teheti ezt (spammelhet, megtéveszthet).

Hagyományos levelekkel is követnek el hasonló csalásokat, csak éppen relatíve költséges volta miatt ez kevésbé hatékony visszaélési mód.

Hagyományos postai levél

Boríték

Feladó neve és címe

Címzett neve és címe

Levél

Gipsz Jakab és társai Kft.
Kukutyin, Lenin út 33.
+41 99 999-999

Piros Arany részére

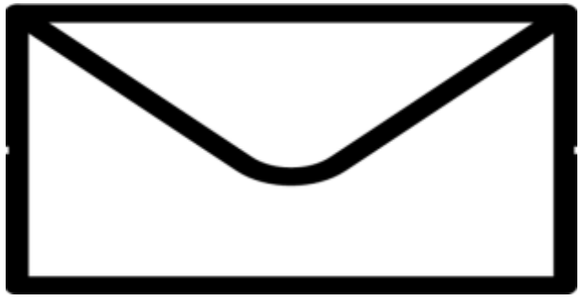
Tárgy: minta

Tisztelt Piros Arany!

…

Kelt, …

E-mail üzenet



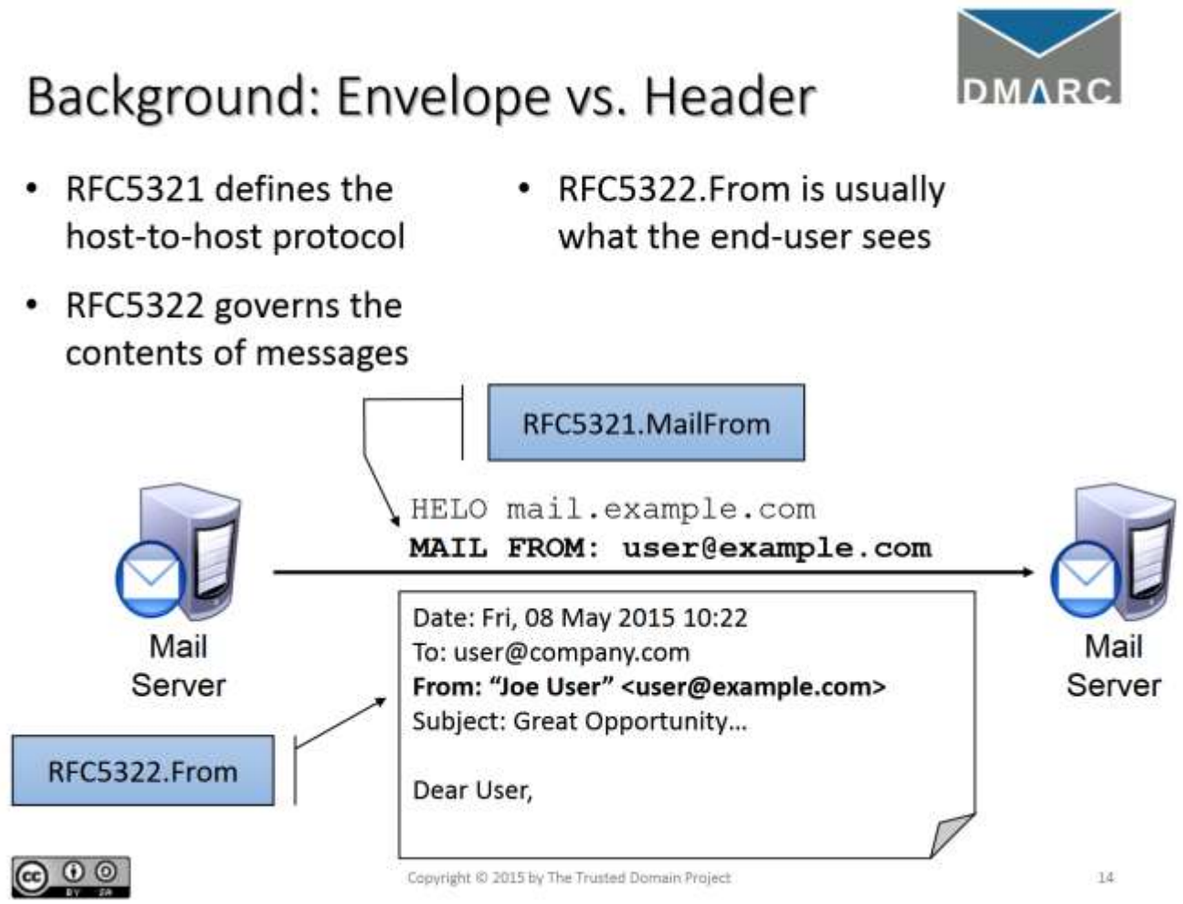
= boríték (envelope) + levél (content)
(RFC 821/5321)

levél (content) (Internet Message Format, RFC 822/2822/5322)

- **headers (fejléc)**
- **body (törzs)**

Hagyományos postai levél versus email

Boríték: Feladó neve, címe + Címzett neve, címe Postahivatalok bélyegzői, jelzései	**Boríték (RFC 821/5321, STMP):** Return-Path: <**returnpath email address**> Delivered-To: piros.arany@addresseedomain Received: from MX Received-**SPF**: Pass (sender SPF authorized) … **envelope-from**=… **[RFC5321.From]**; Received: from Providerdomain (Providerdomain [ProviderIPaddress]) Received: from WORKSTATION
Levél: • **Fejléces papír** • **Levél szövege**	**Levél fejléc (RFC 822/5322, Internet Message Format):** Authentication-Results: ...-**DMARC**; dmarc=pass header.from= senderdomain Authentication-Results: ...-**DKIM**; dkim=pass (2048-bit key; secure) header.d=DKIMdomain header.i=@domain ...; dkim-adsp=pass; dkim-atps=neutral **DKIM-Signature: ...** **From: "Gipsz Jakab"** <**gipsz.jakab@senderdomain**> **[RFC5322.FROM]** To: = piros.arany@addresseedomain Subject: test Date: Thu, 8 Nov 2018 19:03:15 +0100 Message-ID: <003d01d4778d$52a276a0$f7e763e0$@domain>



https://dmarc.org/presentations/Email-Authentication-Basics-2015Q2.pdf

Kétféle 'from'

Boríték from - envelope from (RFC 5321 From)[2]

Levél(fejléc) from -Headers from (RFC 5322 From)

Mindkét 'from' könnyen hamisítható! – felhasználókkal ezt tudatosítani kell!

A levelező kliensek tipikusan csak a levélfejléc fromot mutatják

– bár jellemzően megnézhető a boríték from is (több-kevesebb kényelmetlenség árán).

[2] az Envelope From az azt is szabályozza, hogy kit kell értesíteni, ha nem sikerült a levélküldés (ez már inkább csak történelmi ok, abból az időből származik, amikor még gyakran több köztes MTA is részt vett a levél továbbításban)

Hogyan védekezzünk, hogy nevünkben spamet, illetve phishing üzeneteket küldjenek?

Különösen:

- **e-mail atuhentikációs technikák** (különösen **DKIM**, de SPF, DMARC stb.)
- digitális aláírás
- kerüljük a *bugyuta* közléseket, illetve üzeneteket (pl. bankszámlaszámunk változásáról ne hírlevélben értesítsük ügyfeleinket)
- saját üzeneteink megfelelő tartalma
- ügyfeleink, felhasználóink jó tájékoztatása és támogatása
- biztonsági tudat hiányos, illetve biztonságra érzéketlen szervezeti egységek megreformálása
- a teljes szervezetet és működését átfogó és átható stratégia, szabályozás, gyakorlat, ellenőrzés

Digitális aláírás

- DKIM aláírás – lásd a következő diát
- Üzenet, illetve annak valamely részének (pl. egy csatolt dokumentum) **digitális aláírás**a (X.509 SMIME, PGP)
    - **minősített** elektronikus aláírás

- Időbélyegzés
    - minősített szolgáltató általi időbélyegzés

E-mail authentikációs technikák

- SPF
- **DKIM**
- **DMARC**
- és társaik

Ezekkel együtt alkalmazandó (nem e-mail) technikák:

- **DNSSEC**
- stb.

+ Biztonsági tervezés, szabályozás, menedzsment, felügyelet, ellenőrzés, audit

+ mindent (marketinget és üzletet is, a kiszervezett szolgáltatásokat is) átható biztonsági követelmények és kontroll

- Létezik már olyan magyarországi pénzintézet, mely már alkalmazza a DKIM-et
  - állítólag egy ilyen már létezik :-(

- Szintén létezik DNSSEC-et alkalmazó magyarországi pénzintézet,
  - csak nagyon keresni kell, ha ilyenre példát akarunk találni!

Talán léteznek már más jó példák is tárgykörünkben (csak még nem hallottunk felőlük :-(

Ésszerű tartalom

- Ésszerű tartalom
- ésszerű URL-használat

Példák ésszerűtlen tartalomra

- Bankszámlaszám megváltozásának közlése
- …

Elrettentő példák

Mail From:

Totál Bank Zrt. <info=totalbank.hu@bnc.protopmail.com>; on behalf of; Totál Bank Zrt. <info@totalbank.hu>

Bizalmatlanságra okot adó URL:

Totál Bank Zrt. <info=totalbank.hu@bnc.protopmail.com>; on behalf of; Totál Bank Zrt. info@totalbank.hu
[Norton AntiSpam] ***SPAM*** Energiahatékonysági hitel 0%-os kamattal!

<https://esputnik.com/repository/applications/images/blnk.gif>

<https://img.automizy.com/28a712bc6a380097~~~a7492045e9940778/emaileditor/c81821118a6bceada7a858c4a~~~d81e21dd6431.jpg>

Tisztelt Ügyfelünk!

Növelje lakásának, házának energiahatékonyságát, csökkentse rezsiköltségeit és telepítsen megújuló energiaforrásokat az akár 10 millió Ft-ig is felvehető, fix 0%-os kamatozású kölcsönnel!

Tudjuk, hogy a mai világban egyre fontosabb a környezettudatosság, ezért szeretnénk figyelmébe ajánlani a Magyar Fejlesztési Bank Zrt. által meghirdetett Lakossági Energiahatékonysági Hitelprogramot.

Képzelje el, hogy:

* korszerűsített fűtési rendszer és megfelelő szigetelés,
* új nyílászárók,
* napelem, napkollektor vagy egyéb megújuló energiaforrás látja el otthona energiaigényét.

Ha elképzelte, most valósítsa meg!

<https://img.automizy.com/28a712bc6a380~~~097a7492045e9940778/emaileditor/91d119a8e84518601e2~~~c581d0697fdba290ed.jpg>
További információért hívja a 1440-es telefonszámot, látogasson el a weboldalra vagy érdeklődjön a Totál Bank Zrt. MFB Pontjain!

KATTINTSON A RÉSZLETEKÉRT! <https://ct.automizy.com/7/JnqugBQSVP-Ejjxv41b9HI8tGsYu7Q3BL~~~3N70-Mg_XAk~~~3fi2RYKtyweac>

A hitelprogram Budapest és Pest megye kivételével Magyarország bármely területén megvalósuló beruházásokhoz igényelhető.

Üdvözlettel:
Totál Bank Zrt.

<https://img.automizy.com/28a712bc6a380097a74~~~92045e9940778/emaileditor/02ca0ba26064e003b0112383424cb~~~9a1eacdf.jpg>

<https://img.automizy.com/28a712bc6a380097a74~~~92045e9940778/emaileditor/60295f7b4728ecd2cd783830ace~~~b7ced71814.jpg>

<https://img.automizy.com/28a712bc6a380097a74~~~92045e9940778/emaileditor/c6caeddc12284f82eda075b441297~~~878403c4.gif>
A Lakossági Energiahatékonysági Hitelprogramból nyújtható kölcsönök igénylése során a Totál Bank Zrt. MFB Pontként a Magyar Fejlesztési Bank Zrt. pénzügyi közvetítőjeként jár el.

Felhívjuk szíves figyelmét, hogy a jelen, kereskedelmi kommunikációban közölt információ nem minősül a 2013. évi V. törvény 6:64.§-a szerinti ajánlattételnek. A jelen kötelező erő nélküli jognyilatkozat kizárólag tájékoztató jellegű, a teljesség igénye nélkül a hivatkozott termék egyes főbb jellemzőit tartalmazza! A Totál Bank Zrt. az MFB kiemelt közvetítő partnereként jár el, kötelezettségvállalása minden esetben egyedi hitelbírálat függvénye. A kölcsön megkötésére a Hitelprogramok keretösszegéig kerülhet sor.

ADATKEZELÉSSEL KAPCSOLATOS TUDNIVALÓK

Jelen levelünket a 2020.06.11-én hatályban lévő marketing célú megkeresésekre vonatkozó felhatalmazása alapján juttattuk el Önnek. Ön bármikor, indoklás nélkül kérheti adatainak közvetlen üzleti megkeresés céljából történő kezelésének megszüntetését. Az adatkezelés megszüntetésére vonatkozó kérelmet postai úton vagy e-mailben lehet a Bankhoz eljuttatni számlaszáma(i) feltüntetésével (Totál Bank Zrt., 9999 Budapest, e-mail: info@totalbank.hu).
<https://opn.automizy.com/5/dS6LpImttCf5FrP~~~CuV76WRl0f2voK4dn~~~mfvRxfCyqnqHO30dj47Qxx8-8.gif>

Tartalom