

What is That Email "Really" Telling Me

Understanding Email Header Spoofing

Keith Turpin

Chief Information Security Officer

Universal Weather and Aviation

March 2017

Introduction

Email is a business critical tool that isn't going away

It is also an open door to an organization's network and people

Criminals like open doors



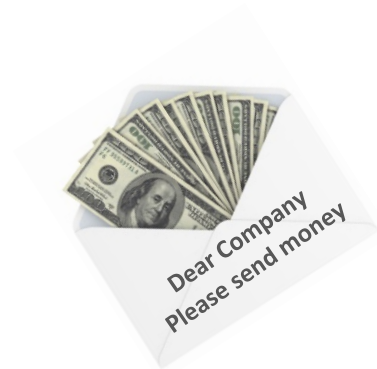
Getting the Message

Email Spoofing: Altering email headers to make a message appear to come from somewhere other than the actual source

Fraudulent emails can impact an organization in two ways:

1. It can be the recipient of spoofed email
2. It can be the impersonated sender in email sent to other organizations

Impact:



1 billion dollars in e-mail business fraud losses reported over an 18-month period



1,300% increase

Objectives

This presentation is intended to help IT and security teams:

- Better understand the mind of the attacker
- Identify meaningful email header information
- Determine an email's lifecycle
- Quickly identify spoofed email
- Help business partners understand when you are the spoofed sender
- Identify services and accounts used for reporting abuse and compromises
- Build a story around a spoofing event, which can be used for end user education
- Understand some defensive strategies

Email Attack Roundup

1. Marketing and other generic spam
2. Email address validation
3. Dragnet phishing
4. Spear Phishing
5. Fake news or social engineering
6. Malicious payloads
7. Links to malicious payload websites
8. Attachments with embedded links to malicious payload sites
9. Links to impersonated login sites

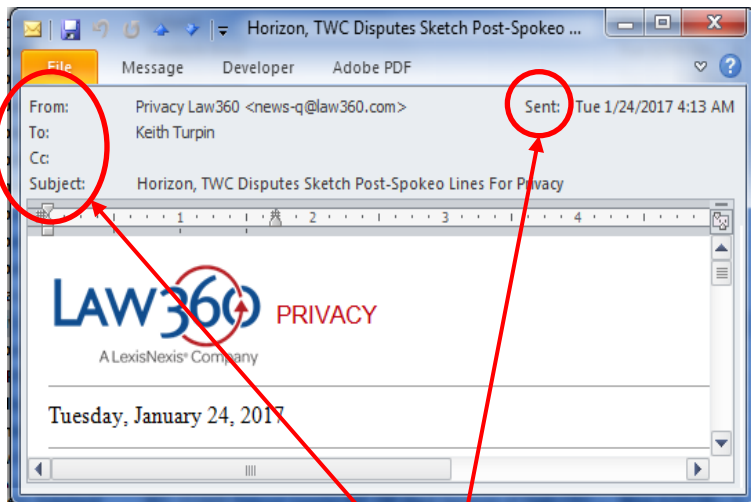
Message vs Envelope Headers

Message headers are used by people

Envelope headers are used by the SMTP server

Message Headers are visible in the email

Envelope Headers contain routing details



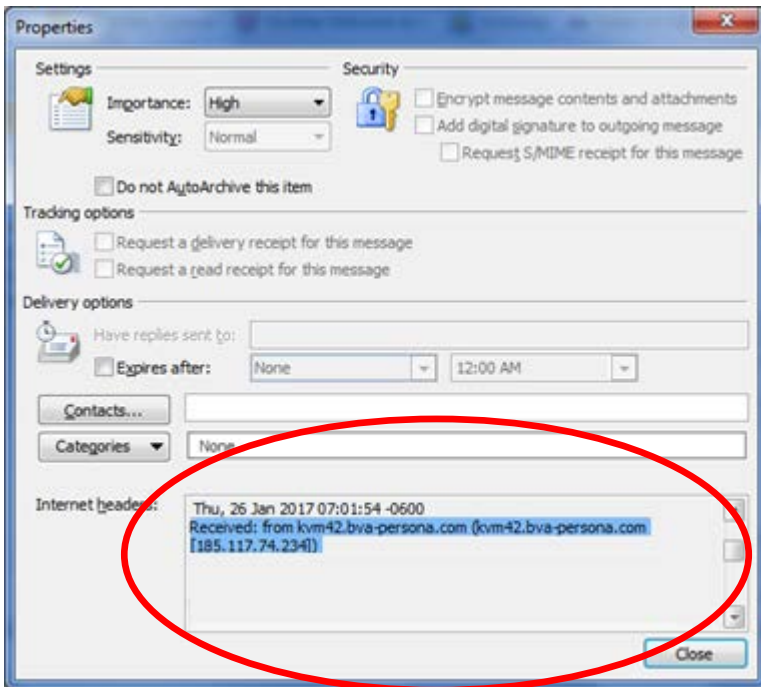
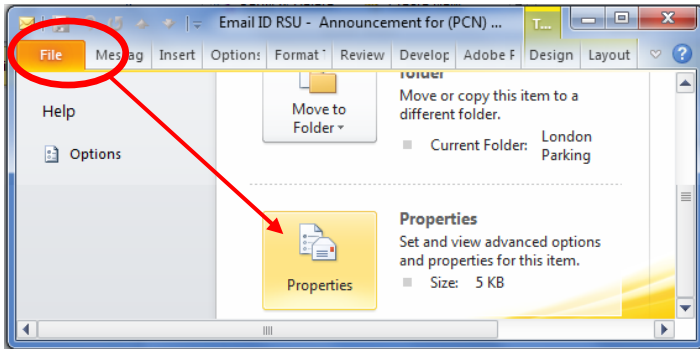
The email Message Headers are contained in the Envelope Header

Note: this example shows content from two different email

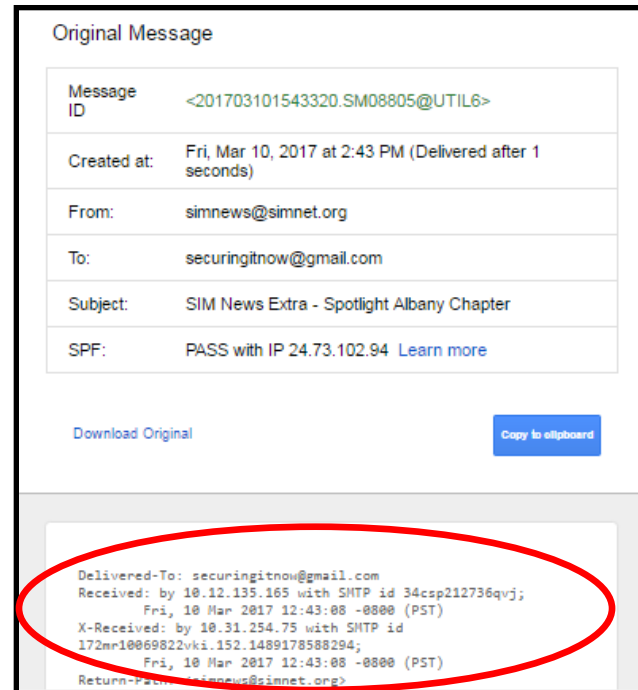
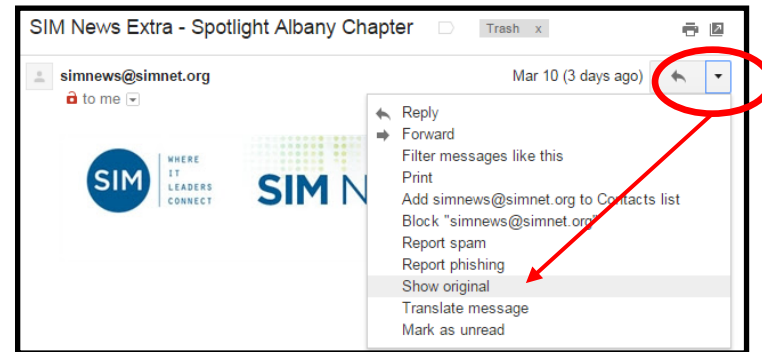
```
Delivered-To: *****@gmail.com
Received: by 10.64.233.6 with SMTP id s6csp69463iec;
  Wed, 8 Mar 2017 14:09:03 -0800 (PST)
X-Received: by 10.107.53.91 with SMTP id c88mr101001651oa.24.1489010943782;
  Wed, 08 Mar 2017 14:09:03 -0800 (PST)
Return-Path: <bounce-866153_HTML-1290912643-4924861-10359607-1636@bounce.e-
mail.microsoft.com>
Received: from mta22.microsoftstore.email.com (mta22.microsoftstore.email.com. [64.132.89.196])
  by mx.google.com with ESMTPS id q187si1312902itc.66.2017.03.08.14.09.03
  for <*****@gmail.com>
  (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
  Wed, 08 Mar 2017 14:09:03 -0800 (PST)
Received-SPF: pass (google.com: domain of bounce-866153_html-1290912643-4924861-10359607-
1636@bounce.e-mail.microsoft.com designates 64.132.89.196 as permitted sender) client-
ip=64.132.89.196;
Authentication-Results: mx.google.com;
  dkim=pass header.i=@email.microsoft.com;
  spf=pass (google.com: domain of bounce-866153_html-1290912643-4924861-10359607-
1636@bounce.e-mail.microsoft.com designates 64.132.89.196 as permitted sender)
  smtp.mailfrom=bounce-866153_HTML-1290912643-4924861-10359607-1636@bounce.e-
mail.microsoft.com
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=102420140131; d=email.microsoft.com;
h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:List-ID:Message-ID:Content-Type;
bh=9TPxqyq0S0S0eRzIdsshJUWadw=;
b=nhppTDrpCbDvTcGP55qJgztVgtDvW0Hvbg0WR39gr5agcvksrPZe49vb6+yMVG450aBR0/ncF5/
ee#7NXOU34Pp9bLcPMDZsrFDn64Mvv7yDbJ5Vx5E5+6R04NocHvR/e75XAY8JZxGcaycVWV3L
kr9yhYCohYExEManE04=
DomainKey-Signature: a=rsa-sha1; c=no; q=dns; s=200608; d=microsoftstore.email.com;
b=Hoq2+8xpDhjq6dwoBwq15JChJg5HIPC/n8a#9Jhd9gcKF2i72xmWxskTCg9CT/yUlwJsdN/3WK
SRIF5dz16A3f+ii+FW96i7e25PQbqWdUx8509kd/ZiF985rCndVBpeyPhJUud90+Htj5kYIRn
En8k5yf9xZjaoPyAyPI=;
Received: by mta22.microsoftstore.email.com id ho20fu163hsj for <*****@gmail.com>; Wed, 8 Mar
2017 16:04:40 -0600 (envelope-from <bounce-866153_HTML-1290912643-4924861-10359607-
1636@bounce.e-mail.microsoft.com>)
From: Microsoft Store <microsoftstore@microsoftstore.email.com>
To: <*****@gmail.com>
Subject: For artists, for scientists, for everyone.
Date: Wed, 08 Mar 2017 16:04:40 -0600
List-Unsubscribe: <mailto:leave-*****-fdfa15727c640d7c77127476-
fe8d107977600c7b74-fe60157076610d7b7513-f2f15767662@leave.email.microsoft.com>
MIME-Version: 1.0
```


Viewing Headers

Headers in Outlook



Headers in Gmail



Envelope Header Breakdown

Envelope Headers contain many fields, but these are most important

Return-Path:

- Delivery issue notices are sent to this address
- Validated by SPF

Reply-To:

- Email address used in message replies
- Overrides the "From" address in replies

Received:

- A single email will often have several "Received" entries
- The bottom "Received" entry will show the first server to handle the message

Lines beginning with X-:

- Extra data that is not contained in any standard
- Added by email servers and security tools

NOTE: *Received and X- fields created by your own email services are the only completely trustworthy entries*

Example 1: Header Walk Through

From: CFO [mailto:CFO@universalweather.com]
Sent: Monday, January 23, 2017 11:51 AM
To: Melody *****
Subject: Melody

Hi Melody,

I want you to send me the list of W-2 copy of employees wages and tax statement for 2016, I need them in PDF file type. Kindly prepare the lists and email them to me asap.

Regards,
CFO

GoDaddy email service

=====
Internal routing above top line removed for example
=====

Received: from p3plwbeout24-04.prod.phx3.secureserver.net ([68.178.252.188] verified) by *****.univ-wea.com (#.#.#.59/#.#.#.59) with ESMTPS id v0QD1jq4014164 for melody.*****@universalweather.com; Mon, 23 Jan 2017 11:51:12 -0600

GoDaddy IP

Received: from localhost ([68.178.252.152]) By p3plwbeout24-04.prod.phx3.secureserver.net with bizsmtp id btrBlu0013J2rYL01trBCG; Mon, 23 Jan 2017 10:51:11 -0700

GoDaddy IP

Internal handoff

Received: (qmail 16608 invoked by uid 99); 23 Jan 2017 17:51:11 -0000
Content-Type: text/html; charset="utf-8"

User-Agent: Workspace Webmail 6.6.1

GoDaddy Webmail Service

X-Originating-IP: 154.118.68.169

Message-ID: <20170123105110.813345af76f4fb74a86befd72a8b63d9.1d3ff0a611.wbe@email24.godaddy.com>

From: CFO <CFO@universalweather.com>

X-Sender: andy.farrell@henleyfineart.com

GoDaddy uses the X-Originating-IP header which is the IP of the client accessing the service

Reply-To: CFO <CFO@highmail.net>

To: <melody.*****@universalweather.com>

Subject: Melody

Date: Mon, 23 Jan 2017 10:51:10 -0700

MIME-Version: 1.0

Return-Path: andy.farrell@henleyfineart.com

Does not match "From" address

Reply-To Domain does not match "From" domain. This is where attacker is waiting for response

Example 1: Where is Highmail.net

We know the email was forged, but we can learn a lot looking into:

- Reply-To: CFO@highmail.net
- X-Originating-IP: 154.118.68.169
- Return-Path: andy.farrell@henleyfineart.com

```
Pinging highmail.net [93.115.38.30] with 32 bytes of data:  
Reply from 93.115.38.30: bytes=32 time=141ms TTL=60  
Reply from 93.115.38.30: bytes=32 time=140ms TTL=60  
Reply from 93.115.38.30: bytes=32 time=144ms TTL=60  
Reply from 93.115.38.30: bytes=32 time=142ms TTL=60
```

Whois Lookup related to '93.115.38.0 - 93.115.38.255'

% Abuse contact for '93.115.38.0 - 93.115.38.255' is 'email@QHoster.com'

Maintained by
QHoster.com

```
inetnum:      93.115.38.0 - 93.115.38.255  
netname:      BZ-FASTSERV-20071221  
country:      BG  
org:          ORG-FSI1-RIPE  
admin-c:      QL56-RIPE  
tech-c:       QL56-RIPE  
status:       ALLOCATED PA  
mnt-by:       RIPE-NCC-HM-MNT  
mnt-domains:  QHoster  
mnt-routes:   belcloud  
created:      2015-02-09T15:53:47Z  
last-modified: 2016-07-25T15:26:52Z  
source:       RIPE
```

Where the server hosting
highmail.net is located
BG = Bulgaria
(ISO 3166 Country Code)

Regional Internet Registry for
Europe, Middle East and
Central Asia

```
organisation: ORG-FSI1-RIPE  
org-name:     Fast Serv Inc.  
org-type:     LIR  
address:      1 Mapp Street  
address:      Belize City  
address:      BELIZE
```

Where Fast Serv Inc.
is registered

Example 1: Who is highmail.net

Spammer and email fraudsters often setup throw away domains

- Reply-To: CFO CFO@**highmail.net**
- X-Originating-IP: 154.118.68.169
- Return-Path: andy.farrell@henleyfineart.com

Whois Lookup related to highmail.net

```
DOMAIN INFORMATION
Domain:highmail.net
Registrar:NAME_SILO, LLC
Registration Date:2016-12-26
Expiration Date:2017-12-26
Updated Date:2016-12-26
Status:clientDeleteProhibited
clientRenewProhibited
clientTransferProhibited
clientUpdateProhibited
Name Servers:ns1.ghoster.net

REGISTRANT CONTACT
Name:Domain Administrator
Organization:See PrivacyGuardian.org
Street:1928 E. Highland Ave. Ste F104 PMB# 255
City:Phoenix
State:AZ
Postal Code:85016
Country:US
Phone:+1.3478717726
Email:email@privacyguardian.org
```

The highmail.net domain was just created in Dec 2016

Actual Registrar hidden through use of PrivacyGuardian

Privacy Guardian has an abuse reporting form, but my report went unanswered

Example 1: Who is highmail.net

If the information is valid, the culprit was far away

- Reply-To: CFO CFO@**highmail.net**
- X-Originating-IP: **154.118.68.169**
- Return-Path: andy.farrell@henleyfineart.com

Whois Lookup related to originating Client Device IP

```
inetnum:      154.118.64.0 - 154.118.95.255
netname:      Spectranet-INET-LTE_DYN_ALLOC
descr:        Dynamic allocation for LTE customers
country:      NG
admin-c:      TCS1-AFRINIC
tech-c:       TCS1-AFRINIC
status:       ASSIGNED PA
mnt-by:       SNL-MNT
source:       AFRINIC # Filtered
parent:       154.118.0.0 - 154.118.127.255
```

```
person:       Technical Contact SN
address:      PLOT NO-36B MOBOLAJI JOHNSON AVENUE OREGUN INDUSTRIAL ESTATE ALAUSA-IKEJA,
address:      IKEJA
address:      Nigeria
phone:        +234-15012345
nic-hdl:      TCS1-AFRINIC
source:       AFRINIC # Filtered
```



Spectranet is the first Internet Service Provider to launch 4G LTE internet service in Nigeria. As the market leader, we are committed to giving our esteemed customers a world class internet experience.

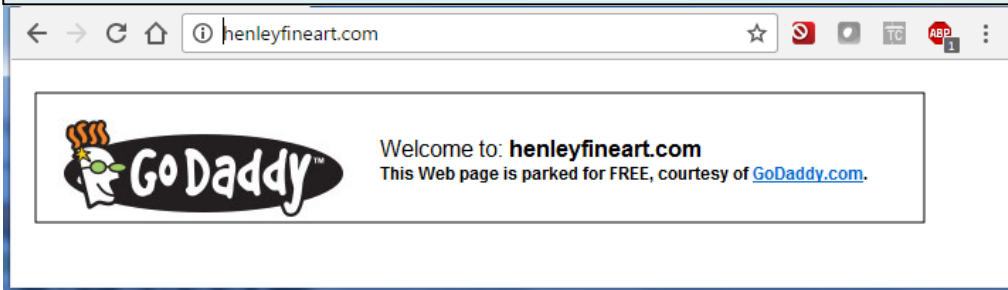
Client location based on IP registration.

Example 1: Looking into henleyfineart.com

Contacting providers and other parties associated with a fraud email may break the attack chain and provide notification to other victims

- Reply-To: CFO CFO@**highmail.net**
- X-Originating-IP: **154.118.68.169**
- Return-Path: andy.farrell@**henleyfineart.com**

Checking henleyfineart.com when incident first occurred



Follow-up after reporting issue to GoDaddy



Regarding henleyfineart.com

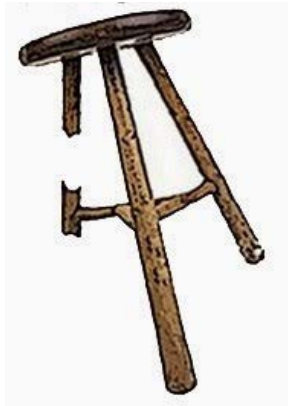
1. Email fraudsters will often alter the Return-Path to show a different domain located on the same hosting provider. This gives them the same IP range for source verification, while pointing the finger at someone else.
2. henleyfineart.com could have been legitimately compromised and been the true source of the email.

Mounting a Defense

Email Fraud is a like a three legged stool that relies on multiple exploit paths to succeed:

1. People..... *Trained, tested and informed*
2. Business Process.....*Out of band verifications and incident reporting*
3. Technology.....*Email security gateways*
Web security gateway
SPF, DKIM and DMARC
Suspicious email tagging

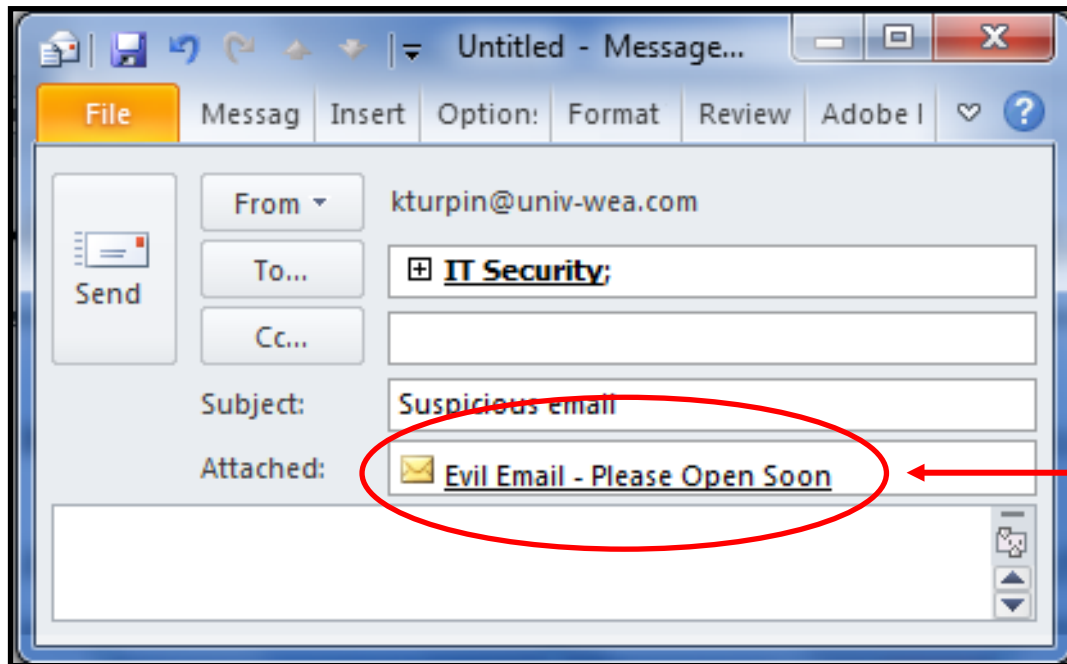
Break any one leg, and the whole scam comes tumbling down



Headers and Incident Response

Important: Envelope Headers are lost when messages are forwarded!

Always have users create a new email, then attach the suspicious email to the new message. Sending the original message as an attachment, preserves the headers.



Fraudulent email attached to a new email to preserve headers

Technology - SPF, DKIM and DMARC

(SPF) Sender Policy Framework:

Looks up the domain in the "Return-Path" (the SMTP envelop sender) and verifies that the corresponding IP is authorized to send email for that domain

- Does not prevent attackers from spoofing the "From" address

(DKIM) DomainKeys Identified Mail:

Digitally signs emails and the receiver runs a DNS query to get the public key from the sender domain

- Does not prevent attackers from spoofing the "From" address
- Can validate message integrity

(DMARC) Domain-based Message Authentication, Reporting and Conformance :

Builds upon both the DKIM and SPF specifications

- Verifies the "From" domain matches the "Return-Path" domain checked by SPF
- Verifies the "From" domain matches the "d= domain name" in the DKIM signature

Questions



Example 2: London Traffic Ticket

From: London Borough of Barking and Dagenham Council <support@lbbdwork.com>
To: Sean Sent: Thu 1/26/2017 7:02 AM
Cc:
Subject: Email ID RSU - Announcement for (PCN) Owner

NOTE: Actual London Borough of Barking and Dagenham website: www.lbbd.gov.uk



Reminder for (PCN) Holder

Alerting You that according to civil enforcement officers (CEOs) Cllr Daniel Young records next parking contravention took place.

Reference Number	85912
Location	Harrow Road
Time of Issue	13:27
Penalty Cause	Using a vehicle with defective breaks/tyres/steering (CU10/30/40)
Date of Issue	16/01/2017
Notice Number	BZ876595

Please find enclosed evidence to this effect.

[VIEW RECORDS AND CHALLENGE THE TICKET OPTIONS](#)

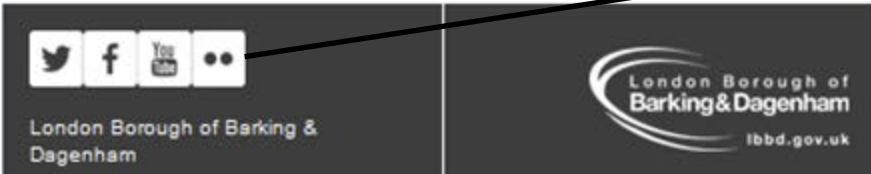
Do not ignore the PCN. Please, be noted If you do not pay or challenge a parking ticket, the penalty charge will increase. You have 28 days to make a formal challenge after you get a notice to owner.

thebridgewatertriangledocumentary.com/wp-content/plugins/woocommerce/np613ysi/pdgdK0ft.php

Redirects to:

hw4t.cpsnorthernonline.com/local/CPS_Enforcement/options/parking_ticket.php

Social media links go to authentic Borough sites



Example 2: More Domains in the Header

===== *Internal routing above top line removed for example* =====

Received: **from kvm42.bva-persona.com (kvm42.bva-persona.com [185.117.74.234])** ← Sending email server
by xxxxxxxx.univ-wea.com (#.#.#.0.59/#.#.#.0.59) with ESMTPS id

v0QD1jq4014164

verify=NOT) for <sean.*****@univ-wea.com>; Thu, 26 Jan 2017 07:01:52 -0500

Message-ID: <A8521AE41BCFE3F02C2960DFDB0E56DB@lbbdwork.com>

Return-Path: support@lbbdwork.com ← Different domain set for Return-Path

From: London Borough of Barking and Dagenham Council <support@lbbdwork.com>

To: <sean.*****@univ-wea.com>

Subject: Email ID RSU - Announcement for (PCN) Owner

Date: Thu, 26 Jan 2017 14:01:50 +0100

Organization: London Borough of Barking and Dagenham Council

Example 2: Disposable Domains for Scam

Addresses of Interest:

Email Server:	cpsnorthernonline.com
Return-Path:	lbbdwork.com
Link Path:	thebridgewatertriangledocumentary.com
Redirect:	bva-persona.com [185.117.74.234]

lbbdwork.com

DOMAIN INFORMATION

Domain:
lbbdwork.com
Registrar:
NAMESILO, LLC
Registration Date:
2017-01-25
Expiration Date:
2018-01-25
Updated Date:
2017-01-25

REGISTRANT CONTACT

Name:
Domain Administrator
Organization:
See PrivacyGuardian.org

cpsnorthernonline.com

DOMAIN INFORMATION

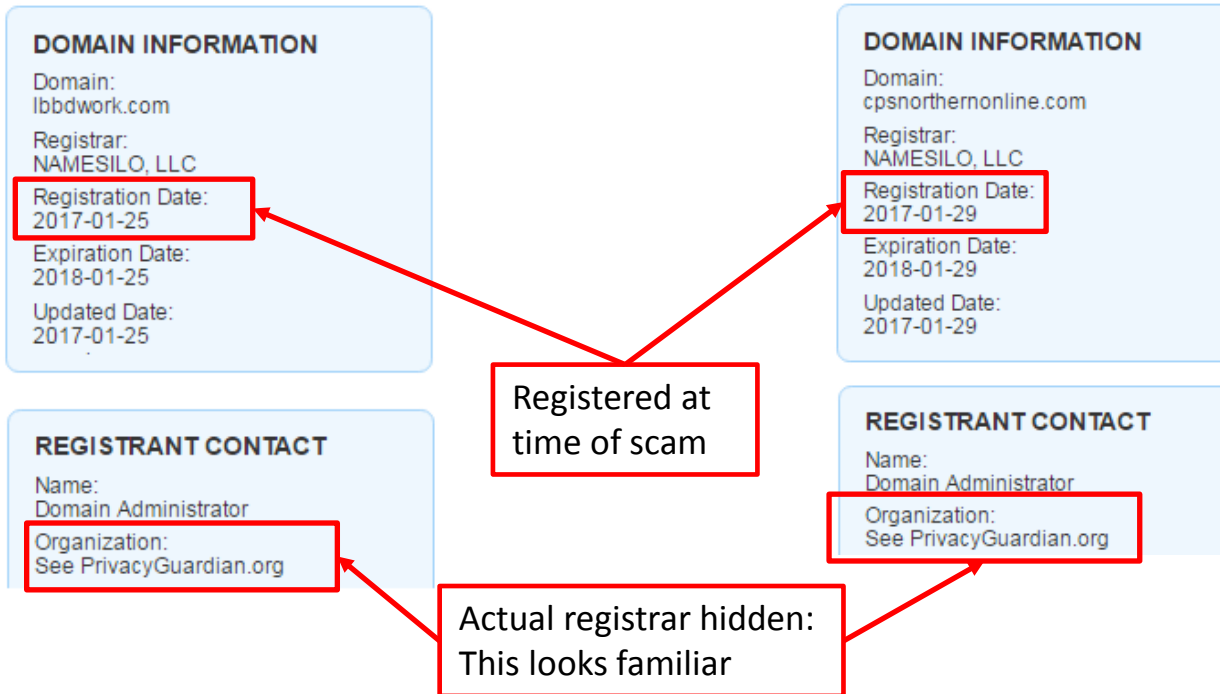
Domain:
cpsnorthernonline.com
Registrar:
NAMESILO, LLC
Registration Date:
2017-01-29
Expiration Date:
2018-01-29
Updated Date:
2017-01-29

REGISTRANT CONTACT

Name:
Domain Administrator
Organization:
See PrivacyGuardian.org

Registered at
time of scam

Actual registrar hidden:
This looks familiar



Example 2: London Traffic Ticket

Addresses of Interest:

Email Server:	cpsnorthernonline.com
Return-Path:	lbbdwork.com
Link Path:	thebridgewatertriangledocumentary.com
Redirect:	bva-persona.com [185.117.74.234]

Although relatively new, this appears to be a legitimate registration. Webserver may have been compromised, but it is off line now.

bva-persona.com

DOMAIN INFORMATION

Domain:
bva-persona.com
Registrar:
NEUBOX INTERNET SA DE C
Registration Date:
2016-10-17
Expiration Date:
2017-10-17
Updated Date:
2017-02-14

```
C:>ping bva-persona.com
Pinging bva-persona.com [174.136.30.161]
Request timed out.
Request timed out.
Request timed out.
Request timed out.
C:>ping 185.117.74.234
Pinging 185.117.74.234
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

The appears to be a legitimate domain and site and webserver may have been compromised for redirect.


thebridgewatertriangledocumentary.com

DOMAIN INFORMATION

Domain:
thebridgewatertriangledocumentary.com
Registrar:
GODADDY.COM, LLC
Registration Date:
2012-08-22
Expiration Date:
2017-08-22
Updated Date:
2015-06-18

Example 2: The Borough's Were Notified

After being notified the Boroughs quickly posted notifications to their website and social media



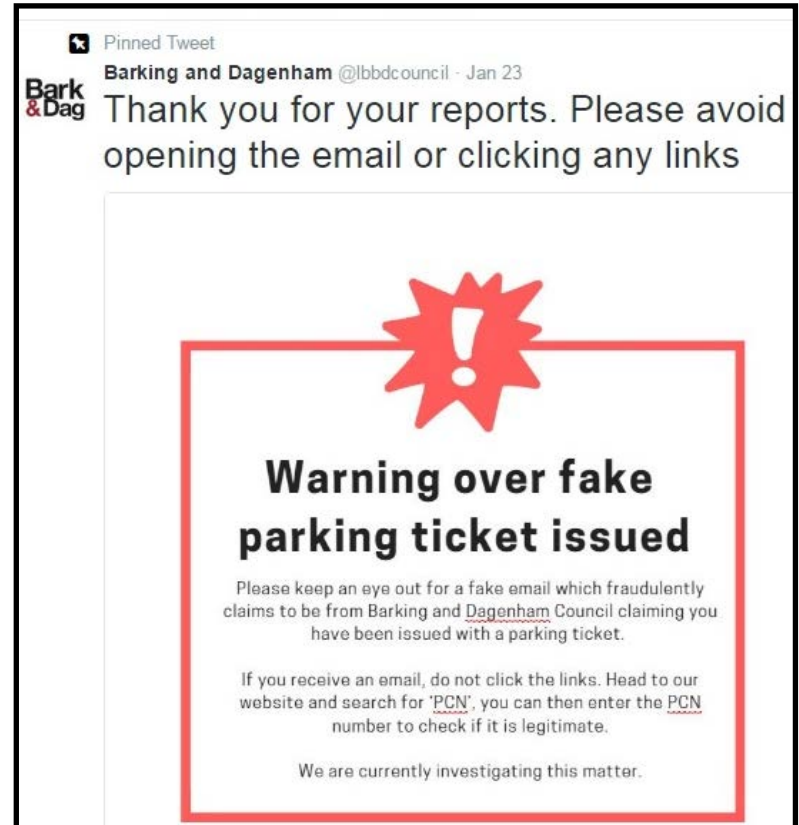
London Borough of
Barking & Dagenham
lbbd.gov.uk

Fake Council Parking Ticket notice

Please be aware that if you have received an email that looks like an official Council parking penalty it is a FAKE.


The Council would never issue a parking fine by email.

Please do NOT click on any link or call or email the Council but delete the email instead.



Pinned Tweet
Barking and Dagenham @lbbdcouncil - Jan 23

Thank you for your reports. Please avoid opening the email or clicking any links



Warning over fake parking ticket issued

Please keep an eye out for a fake email which fraudulently claims to be from Barking and Dagenham Council claiming you have been issued with a parking ticket.

If you receive an email, do not click the links. Head to our website and search for 'PCN', you can then enter the PCN number to check if it is legitimate.

We are currently investigating this matter.

Useful Resources

Checking Risky Attachments

- iGuardian on the InfraGard Portal has a file upload and malware check
- Virus Total (file and website scanning): <https://www.virustotal.com>
- Malwr: <https://malwr.com/>
- Sucuri SiteCheck (website checker): <https://sucuri.net/scanner/>

Email Blacklist Checking Sites:

- Barracuda Reputation Block List (BRBL): <http://barracudacentral.org/rbl>
- SORBS SPAM Blacklist: <http://www.sorbs.net/lookup.shtml>
- Spamhaus blocklist: <https://www.spamhaus.org/>

Open email Relay testing tools:

- Mail Radar: <http://www.mailradar.com/openrelay/>
- MX Toolbox: <http://mxtoolbox.com/diagnostic.aspx>
- DNS Goodies (lots of site analysis tools): <http://dnsgoodies.com/>
- Spam Help Open Relay test: <http://www.spamhelp.org/shopenrelay/>

Anti-Phishing Working Group (APWG)

An international coalition seeking to unify the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership includes more than 1800 institutions worldwide: <http://www.antiphishing.org/>

Best resource for information on SPF, DKIM and DMARC:

<https://blog.returnpath.com/how-to-explain-spf-in-plain-english>

<https://blog.returnpath.com/how-to-explain-dkim-in-plain-english-2>

<https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english>