

## Email Phishing and Social Engineering

Source: OSX List by Dennis Fazio dfz@mac.com

On Apr 13, 2006, at 3:37 PM, Gisela Drayton wrote:

Twice today I received a message from Apple responding to "my inquiry" as to "How to reset my Apple password." I did not request to reset my password. What can I do about that? This happened about a month ago also. It seems like someone is trying to get into my .mac.com account.

That's right, someone is trying to get into your account and they are using social engineering, not hacking.

The message is not from Apple and if you examine the full headers, you will see that.

This is a phishing attack; they are sending messages to multiple account holders hoping someone will take the bait and type a password into their forged web page so they can capture it. As long as you don't respond or click on any links they give you, you are safe. This is done quite frequently using ebay or paypal accounts to get passwords and using forged bank web sites to get credit card numbers; I get a couple of them each week. Haven't seen one for .mac yet though, so this is a first.

====

On Apr 14, 2006, at 2:54 AM, kathryn mcgee wrote:

Can you explain what the full header will show that makes it clear to us regular folks that we are not hearing from the actual Site claimed in these types of emails?

If you have a "long headers" button on your main window toolbar (you can put it there by customizing your toolbar if it isn't present), click on that and it will show you all the message headers.

Below are the "long headers" from an ebay phishing message I got recently.

The key header lines to watch are the "Received" headers. These are placed in the message by each mail machine it passes through, oldest at the bottom, newest at the top. These are impossible to forge by a spammer or phisher unless they have control of the mail server.

They usually don't, but the better ones can forge these also. The "From" "Subject" "Date" "CC" headers are placed in the message by the users mail program and can all be easily forged, so don't ever trust the "From" address.

You will note in the headers that it started at mail server smtp.ires.pl at address 195.149.226.251. This server is in the Poland (PL) domain, so it is likely (though not necessarily) in Poland. If you see a domain name with a .nn as the last part, the .nn is the 2- letter ISO country code. Messages in these domains are usually from overseas. Ebay would not be sending me messages from a server in the Poland or any other country domain. Neither would Paypal, your bank, your credit card company or Apple.

If it's a .com domain, check what it is carefully. You'll usually see it is not from the organization domain in claims it is (ebay, paypal, apple, etc.)

From: aw-confirm@ebay.com  
Subject: eBay Account - Suspicious Activity  
Date: April 3, 2006 4:36:19 AM CDT  
Cc: recipient list not shown: ;  
Return-Path: <anonymous@smtp.ires.pl>  
**Received: from mac.com (smtpin36-en2 [10.13.9.179]) by ms13.mac.com (iPlanet Messaging Server 5.2 HotFix 2.08 (built Sep 22 2005)) with ESMTP id <0IX500IMKUXU1@ms13.mac.com> for dfz@mac.com; Mon, 03 Apr 2006 12:17:57 -0700 (PDT)**  
**Received: from smtp.ires.pl (25.226.149.195.tld.pl [195.149.226.25]) by mac.com (Xserve/smtpin36/MantshX 4.0) with SMTP id k33JHq4L013593**

for <dfz@mac.com>; Mon, 03 Apr 2006 12:17:56 -0700 (PDT)  
**Received: (gmail 11778 invoked by uid 7063); Mon, 03 Apr 2006 09:36:19 +0000**  
Message-Id: <20060403093619.11775.gmail@smtp.ires.pl>  
Mime-Version: 1.0  
Content-Type: text/html  
Content-Transfer-Encoding: 8BIT  
Original-Recipient: rfc822;dfz@mac.com

Here's another set of headers from a message telling me my National City login and password were out of date.

From: hostmaster@selectcomfort.com  
Subject: Urgent Member Alert  
Date: March 15, 2006 9:01:35 PM CST  
To: [deleted]  
Reply-To: hostmaster@selectcomfort.com  
Return-Path: <hostmaster@selectcomfort.com>  
Received: from psmtplib.com (exprod6mx137.postini.com [64.18.1.44]) by bodb.mc.mpls.visi.com (Postfix) with SMTP id 51D8D4A12 for <dfazio@visi.com>; Wed, 15 Mar 2006 21:06:33 -0600 (CST)  
**Received: from source ([208.42.156.101]) by exprod6mx137.postini.com ([64.18.5.10]) with SMTP; Wed, 15 Mar 2006 22:06:33 EST**  
**Received: from 209.98.94.88 (unknown [24.244.178.240]) by breg.mc.mpls.visi.com (Postfix) with SMTP id 850CC6506 for <dfazio@breviis.net>; Wed, 15 Mar 2006 21:06:31 -0600 (CST)**  
**Received: from 196.191.255.45 by 24.244.178.240; Thu, 16 Mar 2006 03:59:35 +0100**  
Message-Id: <AFUHRVLOCTNWAYYTBTAOYYK@aol.com>

There are several clues of forgery here:

1. the sender's address is from the selectcomfort.com domain, not National City (notice that the "Reply-to" header is also forged)
2. The 1st mail server in the line is 196.191.255.45. Notice there is no domain name - an immediate cause for suspicion. If I do a whois lookup on that address, nothing is found in the database indicating it is probably forged. (Don't worry about that for now if you don't know what whois is).
3. the Message-Id is from aol.com. The message ID is placed in the message header by the originating mail server. National City would not send me a message from an AOL account.

As you can see, if you know what you're looking for, there are clues in the extended headers to help you determine if a message is legitimate. The bit of info given above can help with obvious ones. The best thing to do is to observe safe practices when you receive messages like this having to do with your accounts someplace.

Several others in this thread gave excellent advice on practices to use or avoid to protect yourself from a phishing scam. Reputable businesses don't send messages asking you to verify your account or password nor do they say your account will be terminated unless you log in and do something. Always be suspicious of these.

====

Internet mail is defined in RFC 2821 (Simple Mail Transport Protocol or SMTP) and RFC 2822 (Internet Message Format). These standards set the exact format and syntax of Internet mail messages for interoperability.

Mail, on the Internet is handled by two separate agents: the Mail User Agent (MUA) and the Mail Transport Agent (MTA). The User Agents are the mail programs like Apple Mail, Eudora, Outlook, that we run on our computers to transmit, receive and store messages. The Transport Agents are the programs like Sendmail, Postfix, Microsoft Exchange, that run on the mail servers at our ISP that move the message generated by the User Agent to the final destination server where the recipient has an email account and can fetch the message.

Some of the headers are placed in the message by the User Agent and some by the Transport Agent. I've rearranged the headers into groups that are related.

**From:** josh@bigbend.us  
**Subject:** RE: Our stunning items are to express your good taste.  
**Date:** January 5, 2006 11:50:10 PM PST  
**To:** jerrywilsons@mac.com  
**Cc:** anniesykes@mac.com, ciccibaba@mac.com, boy231@mac.com, cubilloss@mac.com  
**Reply-To:** josh@bigbend.us

This first set of headers are created by the User Agent (Outlook Express, in this case), or generated by the Transport agent from information supplied by the User Agent. They are self explanatory and you've seen them on all messages. These are the basic 4 header lines of a message (From, To, Subject, Date). Often Cc and Bcc are added if copies are to go to others. Reply-To can sometimes be inserted to force the recipient's User Agent to send a reply to a specified address rather than the "From:" address.

Message-Id: <9aa601c6129e\$337a1790\$fd309af9@josh>  
Content-Type: text/plain; charset=us-ascii  
Content-Transfer-Encoding: 7bit  
Original-Recipient: rfc822;jerrywilsons@mac.com  
Mime-Version: 1.0

This next set describes the message information. All messages have a unique ID generated by the first MTA. The Content-Type and Content-Transfer-Encoding describe the format of the message body; in this case, plain ASCII text. All messages must be transmitted in 7-bit ASCII, though there is now a provision for 8-bit MIME to an other kinds of character set encoding to accommodate non-english languages. The Original-Recipient header is usually put on when a message is "bounced" or "redirected" to another. Mime-Version is always put in for all MIME capable mailers.

X-Mimeole: Produced By Microsoft MimeOLE V5.00.2919.6700  
X-Mailer: Microsoft Outlook Express 5.00.2919.6700  
X-Msmail-Priority: Normal

Any header that begins with X- is custom. This provides a way for User or Transport agents to put in custom headers in a standard way. These were inserted by Outlook Express as additional documentation. The X-Mailer header gives a nice way to see which mail program the sender used.

Return-Path: <josh@bigbend.us>  
**Received:** from mac.com (smtpin06-en2 [10.13.10.151]) by ms74.mac.com (iPlanet Messaging Server 5.2 HotFix 2.03 (built Nov 22 2004)) with ESMTP id <0ISP0014RKK1UD@ms74.mac.com> for jerrywilsons@mac.com; Fri, 06 Jan 2006 21:57:37 -0800 (PST)  
**Received:** from bigbend.us ([218.80.113.99]) by mac.com (Xserve/smtpin06/MantshX 4.0) with SMTP id k075vXDF002319; Fri, 06 Jan 2006 21:57:34 -0800 (PST)

These next ones are the trace headers. They're put in by the Transport Agent to trace the path of the message as it is relayed from server to server. They are stacked with the first one on the bottom and the last, or recipient server, at the top of the list. The primary purpose of the Return-path is to designate the address to which messages indicating non-delivery or other mail system failures are to be sent. Usually it is the same as the sender's address, but not always, such as for mail lists. It is inserted by the destination server.

To interpret the Received headers, starting with the bottom, the message was first received by server mac.com from sending PC bigbend.us. Bigbend's actual IP address is given in brackets. The mac.com machine is described in the parentheses and its IP address is given in brackets. SMTP was the transport protocol and it attached an ID number for its internal tracking logs. The message was received by mac.com on Fri Jan 6 at 21:57:34 PST which is 8 hours before UTC (formerly called Greenwich Mean Time or GMT). You need to watch the -0800 part to get the real universal time when tracking messages. the time zone isn't always supplied or supplied accurately.

Next, mac.com sent the message to ms74.mac.com (described in the parentheses) with Extended SMTP. It added its own ID for internal tracking. Since this is the destination host and had the mailbox for Jerrywilsons, the message was stored in the inbox at 21:57:37 PST (3 seconds after getting it from mac.com).

The Trace headers are your best tool for verifying the source of a message, since they are harder to forge; a spammer or phisher doesn't usually have control of mail servers, and definitely doesn't have control over intermediate servers. You can pretty easily tell right away that a message did NOT come from ebay, paypal or your bank.

This is the end of the headers that information was requested on. The 3rd part contains information on internal MIME headers.

Sometimes, you'll get a multipart MIME message (a message with attachments, and you'll see this

header if you display the raw message:

```
Content-Type: multipart/related;  
  boundary="-----_NextPart_000_0011_05C60785.D69395A0"
```

Notice there is a different content type than text/plain. This tags a multipart message. The Boundary= indicates the string that forms the boundary between parts. Within the body of the message, will be MIME headers specifying the part boundaries and the encoding of that particular part. In this message, which was a spam message, there was plain text, an HTMLpart and a picture part. There will be separate MIME headers within the body of the message separating the different MIME parts.

```
-----=_NextPart_000_0011_05C60285.D69395A0  
Content-Transfer-Encoding: 7bit  
Content-Type: text/plain;  
  charset=us-ascii
```

and quietcmd , cremasterial on votaria on gracias on mesela

This is the MIME header for the plain text part with the text right below it. It was Spanish spam.

```
-----=_NextPart_000_0011_05C60285.D69395A0  
Content-Transfer-Encoding: quoted-printable  
Content-Type: text/html;  
  charset=us-ascii
```

```
<html xmlns:v=3D"urn:schemas-microsoft-com:vml"  
xmlns:o=3D"urn:schemas-microsoft-com:office:office" xmlns:w=3D"urn:schemas-microsoft-com:office:word"  
  xmlns=3D"http://www.w3.org/TR/REC-html40">  
--snip--
```

This is the HTML part, header and content (content clipped for brevity)

```
-----=_NextPart_000_0011_05C60785.D69395A0  
Content-Transfer-Encoding: base64  
Content-Id:  
<8.0.0.22.0.89755194629890.27255883@gpiqueryfonts.fiets.nl.1>  
Content-Type: image/gif;  
  name=3mnipper.gif
```

```
R0lGODlheAH/ANUAAp/////zP/M//MzP+Zmf9mZv8zM/8AAmZ//8z/zMzM/  
8zMzMmcyZzMyZ  
mZnMzJnMmZmZ/5mZzJmZmZmZpLmmZlmZpkzZmaZ/2azmWazZmZm/  
2ZmmWZmZmZmM2YzZmYzM2YA  
MzNm/zNmZjNmMzZmZ/zMzZjMzZmMAMzMAAAAz/wAzMwAA/  
wAAmWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACH5BAAAAAALAAAAAB4Af8AAAb/  
QIBw  
--snip--
```

```
-----=_NextPart_000_0011_05C60785.D69395A0--
```

Finally, comes the encoded GIF image (using base64 encoding) (also greatly clipped) and the final MIME boundary string.

By displaying the raw message, you have the ability to look within the message and see all the attachments and what kind they are: text/ plain, text/html, image/gif, image/jpeg, etc. This may help in diagnosing why you are having trouble with attachments.

Hopefully, the information in these 3 messages will help some understand the details of their mail messages a bit more and perhaps diagnose some routing, decoding, spam or phishing problems on their own a little better. Write if further questions.

====

I refer to the bottom most "Received:" field from your example here:

-----

```
> Received: from bigbend.us ([218.80.113.99]) by mac.com (Xserve/  
> smtpin06/  
> MantshX 4.0) with SMTP id k075vXDF002319; Fri, 06 Jan 2006 21:57:34  
> -0800 (PST)
```

-----

How would I know if "bigbend.us" or "218.80.113.99" are real or cloaked ID's? I'm assuming the "bigbend.us" can be user-set. As for the IP address, do you mean to imply that one should do a whois- lookup to confirm or deny the origin?

The main thing you need to protect from is phishing scams; when the sender uses "social engineering" via email to get you to divulge something like a credit card number or password they can later exploit. Sometimes, it's not an obvious phishing scheme, but you are not sure that the sender is a legitimate business.

Most phishing messages you can spot after a while because they are asking you to give information that is private either via an email response or via a web site. None of the legitimate trading sites or financial houses operate that way.

If you have doubt and want to look deeper into the headers for clues, it can often be obvious there just by the domain names used that don't seem to be right or are inconsistent with each other. If you get a message from a business, the domain name should be consistent with the business name.

### Using Whois:

You should be easily able to do a quick whois lookup to see the owner. You may have to use a couple of different whois servers depending upon the top-level domain. whois.internic.net gets most domains (com, org) or will steer you to the correct whois server.

whois.educause.net is for the .edu domain  
whois.arin.net is best for IP address lookups  
whois.ripe.net is for european domains  
whois.apnic.net is for Asia-Pacific domains  
whois.nic.mil is for military (.mil)  
whois.nic.us is for the .us domain

There is a nice utility called whatroute that will search all at once. You can also do whois searches in various places on the net.

You'll want to see if there is an inconsistency or unusual source for both the domain name and the IP address. Many things in the header can be forged, but usually, the spammer/phisher is not very good and leaves clues in the headers somewhere. You should get a lot of information about the owner of a domain name in the whois lookup and the owner of the IP address where it came from (Note that the IP address may be in within a range that is assigned to a major backbone provider like ATT, UUNET or Wiltel, etc. They don't always subassign them fully.)

It takes some practice and research to learn about domain names and IP address ranges and assignments, but it usually isn't too hard to spot funny things as you check all the headers.

-- Dennis Fazio dfz@mac.com

====

Many thanks to Dennis for sharing his wisdom, knowledge, and experience!  
Tuesday, April 18, 2006 at 7:49 AM Eastern Standard Time

====