BRUCE MEYER & ASSOCIATES

Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

UCE (Unsolicited Commercial Email)

a.k.a. Junk Mail or "spam"

Part 2

In our original article about spam, we discussed some ways to protect yourself from receiving spam. If you have not read this article, please take a few moments and visit our website (http://www.bm-a.biz/Articles/BMA_spam.pdf). In addition to using anti-spam programs, not using "unsubscribe" links, and having a separate email address for website and newsletter registrations, we want you to have some tools to help fight spam.

One of the first steps to recognizing spam is to take a look at the sender of the message. Unless your friends and relatives did not set up their email programs correctly, it is rare to receive a "real" email with no sender noted. Look for unlikely email addresses, also. I'd bet that %%47212jt389^&@hotmail.com is a phony. Likewise, it is quite unusual for very famous folk to take the time to send you an email – especially one selling something. I was pleasantly surprised that George W. Bush had taken the time to send me an email. I was even more surprised that he wanted to sell me a "legal" copy of "Microsoft Office" for just $16.95 plus shipping. Now I'm wondering if Tom Cruise was really selling Cialis ☺

Remember that *anyone* can program any return address (including yours) into their email program. To find out who really sent that message (and to report them to their ISP) takes a little detective work. If you are armed with the right tools, you could make Sherlock Holmes proud.

STEP 1 – LOOK AT THE MESSAGE HEADERS

The key to the origin of an email message is the sender's IP address. An IP address is a unique identifier for each computer on the internet, at any given time. IP addresses may change from computer to computer, but each Internet Service Provider is assigned a range of IP Addresses to use. With the IP address and the time, they can track which user was on the internet at any given time.

In Microsoft programs (Outlook and Outlook Express) right-mouse click on the subject of a message and select properties. When the properties open, click on the tab that says "details". The information that appears in this window is the message header. For other programs (Netscape, Eudora, Thunderbird, and most webmail programs, select "View all message headers"). Once you have the message headers, you may want to copy them into notepad or another program. They will look something like this:

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz

```
Return-Path:<alert@citibank.com>
Delivered-To:you@yourdomain.com

Received: (qmail 21953 invoked by uid 512); 7 Nov 2004 07:58:05 -0500
Received: from alert@citibank.com by bronze by uid 504 with qmail-
scanner-1.20(clamuko: 0.73. Clear:RC:0(81.111.174.155):.
     Processed in 0.525603 secs); 07 Nov 2004 12:58:05 -0000
Received: from unknown (HELO cpc2-bexl2-3-0-cust155.brom.cable.ntl.com)
([81.111.174.155])
     (envelope-sender <alert@citibank.com>)
     by bronze.nb.net (qmail-ldap-1.03) with SMTP
     for <you@yourdomain.com>; 7 Nov 2004 07:58:05 -0500
X-Message-Info: 5N8nsSMZobc254bxxH22ELTz749Xq10l6OxOYKu90
Received: from dns4bbtec.net ([16.24.180.200]) by jjp2-PR4.bbtec.net
with Microsoft SMTPSVC(5.0.2195.6824);
     Sun, 07 Nov 2004 06:01:35 -0700
Received: from bbtec.net [127.0.0.1] by dnsbbtec.net
     (SMTPD32-7.12 ) id VI468VEX5; Sun, 07 Nov 2004 08:53:35 -0400
Subject: Citibank Alerting Service
From: Citibank
To: you@yourdomain.com
Message-Id: <5210099464.yrv642@bbtec.net>
Content-Type: multipart/alternative;
     boundary="--578786450266688553"
```

You want to look at the "Received" sections of the email headers for the farthest-down IP address – in this case, 16.24.180.200. This identifies who sent the email, on `Sun, 07 Nov 2004 06:01:35 -0700`. This is the information the ISP will need to have.

Now we need to know the ISP. One of the best free tools to find this information is from an Australian company, called Eye-Net Consulting. Go to their free IP address lookup at: http://www.enc.com.au/itools/inetnum.php

We now get the following information back, confirming the brom.cable.ntl.com that preceded the IP address in the "received" section.

Registrant Digital Equipment Corporation 20555 State Highway 249, M020303
CountryUS
Network Address16.0.0.0 - 16.255.255.255 NIC
HandleNET-16-0-0-0-1
StatusDirect Assignment
Tech ContactZC41-ARIN
Abuse (spam) Contact NAR-ARIN

BRUCE MEYER & ASSOCIATES
Computer & Network Support
Accounting & Manufacturing Software
Medical Billing Services & Software

Often there will be a link for an address to report abuse in the results above. Most ISPs have an address called abuse@ (followed by the domain name) to report spammers. A third possibility is to visit the website and look for a contact link to report the spammer. You will need to include the full email headers in the message for the ISP to take any action. Without them, nothing can be done.

Unfortunately, the sending of spam is fairly complex. In this case, the headers tell us that someone using HP.com sent spam to another computer in England, to have that computer deliver it to a list of addresses. The more computers they can go through, the less chance they have of being caught.

It is likely that Hewlett-Packard does not send out spam on a regular basis. They may have had a security breech, and had someone break into their email system. The user in England was most likely a DSL customer who left their computer on, and did not have a security firewall, thus having no idea someone was sending spam though their computer.

When reporting spam to an ISP, **PLEASE** be sure to include all the message headers, as well as a copy of the spam you received. The more information you send, the easier it is for the ISP to catch the spammers and disable their internet access.

Thanks,

Bruce Meyer

809 Highland Avenue, Greensburg, PA 15601-4315
Voice: 724-837-9433 Fax: 724-832-2576
Email: bmeyer@bm-a.biz Website: www.bm-a.biz