Understanding E-mail Spoofing

Date Launched: Oct 20, 2004
Last Updated: Oct 29, 2004
Section: Articles :: Content Security (Email & FTP)
Author: Deb Shinder
Printable Version
Rating: 4.1 / 5 - 38 Votes

1 2 3 4 5

Spam and e-mail-laden viruses can take a lot of the fun and utility out of electronic communications, but at least you can trust e-mail that comes from people you know – except when you can't. A favorite technique of spammers and other "bad guys" is to "spoof" their return e-mail addresses, making it look as if the mail came from someone else. In effect, this is a form of identity theft, as the sender pretends to be someone else in order to persuade the recipient to do something (from simply opening the message to sending money or revealing personal information). In this article, we look at how e-mail spoofing works and what can be done about it, examining such solutions as the Sender Policy Framework (SPF) and Microsoft's Sender ID, which is based on it.

The Problem

If you receive a snail mail letter, you look to the return address in the top left corner as an indicator of where it originated. However, the sender could write any name and address there; you have no assurance that the letter really is from that person and address. E-mail messages contain return addresses, too – but they can likewise be deliberately misleading, or "spoofed." Senders do this for various reasons, including:

- The e-mail is spam and the sender doesn't want to be subjected to anti-spam laws
- The e-mail constitutes a violation of some other law (for example, it is threatening or harassing)
- The e-mail contains a virus or Trojan and the sender believes you are more likely to open it if it appears to be from someone you know
- The e-mail requests information that you might be willing to give to the person the sender is pretending to be (for example, a sender might pose as your company's system administrator and ask for your network password), as part of a "social engineering" attack
- The sender is attempting to cause trouble for someone by pretending to be that person (for example, to make it look as though a political rival or personal enemy said something he/she didn't in an e-mail message)

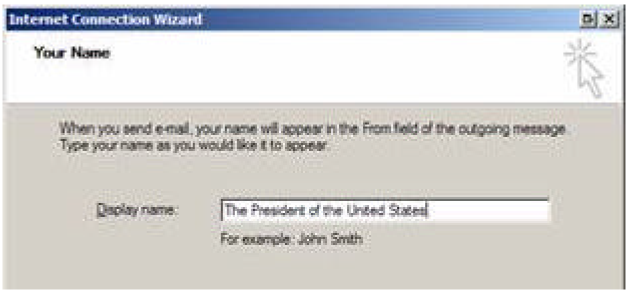
Note:
"Phishing" – the practice of attempting to obtain users' credit card or online banking information, often incorporates e-mail spoofing. For example, a "phisher" may send e-mail that looks as if it comes from the bank's or credit card's administrative department, asking the user to log onto a Web page (which purports to be the bank's or credit card company's site but really is set up by the "phisher") and enter passwords, account numbers, and other personal information.

Whatever the motivation, the objective of spoofed mail is to hide the real identity of the sender. This can be done because the Simple Mail Transfer Protocol (SMTP) does not require authentication (unlike some other, more secure protocols). A sender can use a fictitious return address or a valid address that belongs to someone else.

Receiving mail from spoofed addresses ranges from annoying to dangerous (if you're taken in by a "phisher"). Having your own address spoofed can be even worse. If a spammer uses your address as the return address, you may suddenly find yourself inundated with angry complaints from recipients or even have your address added to "spammer" lists that results in your mail being banned from many servers.

How Spoofing Works

In its simplest (and most easily detected) form, e-mail spoofing involves simply setting the display name or "from" field of outgoing messages to show a name or address other than the actual one from which the message is sent. Most POP e-mail clients allow you to change the text displayed in this field to whatever you want. For example, when you set up a mail account in Outlook Express, you are asked to enter a display name, which can be anything you want, as shown in Figure 1.



Your Name

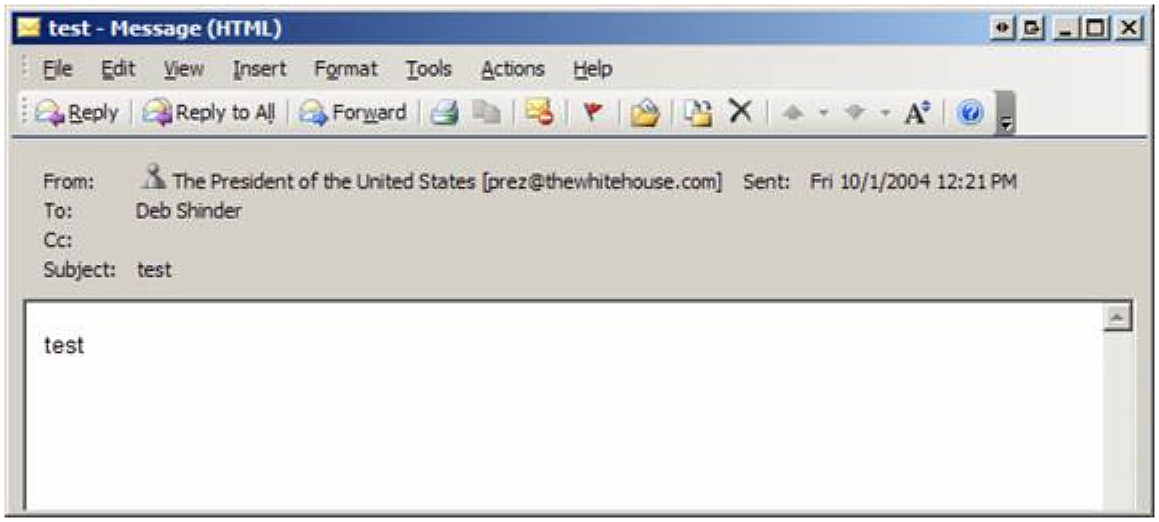
When you send e-mail, your name will appear in the From field of the outgoing message. Type your name as you would like it to appear.

Display name: The President of the United States

For example: John Smith

Fig 1: Setting the display name in your e-mail client

The name you set will be displayed in the recipient's mail program as the person from whom the mail was sent. Likewise, you can type anything you like in the field on the following page that asks for your e-mail address. These fields are separate from the field where you enter your account name assigned to you by your ISP. Figure 2 shows what the recipient sees in the "From" field of an e-mail client such as Outlook.

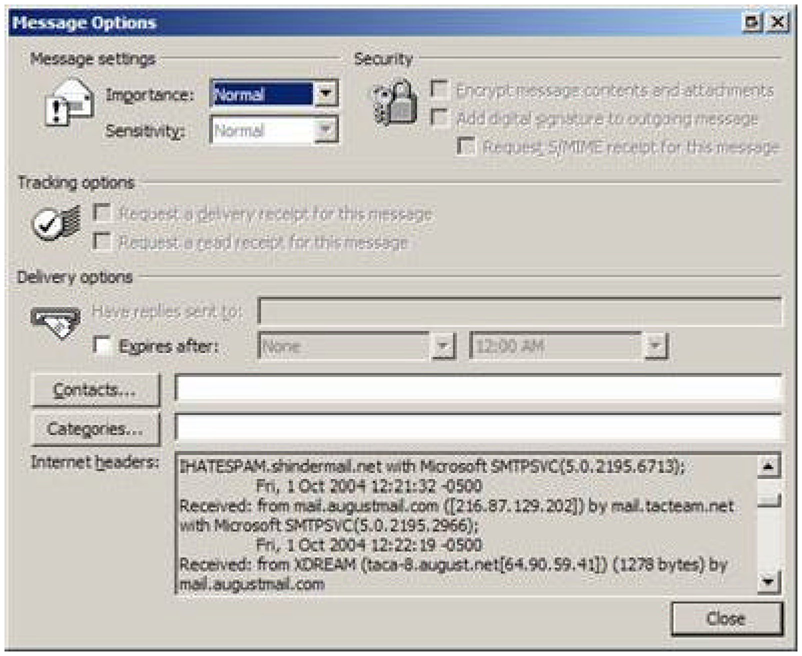


From: The President of the United States [prez@thewhitehouse.com] Sent: Fri 10/1/2004 12:21 PM
To: Deb Shinder
Cc:
Subject: test

test

Fig 2: The recipient sees whatever information you entered

When this simplistic method is used, you can tell where the mail originated (for example, that it did *not* come from thewhitehouse.com) by checking the actual mail headers. Many e-mail clients don't show these by default. In Outlook, open the message and then click **View | Options** to see the headers, as shown in Figure 3.



Importance: Normal
Sensitivity: Normal
□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message
□ Request a delivery receipt for this message
□ Request a read receipt for this message
Have replies sent to:
□ Expires after: None 12:00 AM

Internet headers:

```
IHATESPAM.shindermail.net with Microsoft SMTPSVC(5.0.2195.6713);
          Fri, 1 Oct 2004 12:21:32 -0500
Received: from mail.augustmail.com ([216.87.129.202]) by mail.tacteam.net
with Microsoft SMTPSVC(5.0.2195.2966);
          Fri, 1 Oct 2004 12:22:19 -0500
Received: from XDREAM (taca-8.august.net[64.90.59.41]) (1278 bytes) by
mail.augustmail.com
```

Fig 3: Viewing the e-mail headers

In this example, you can see that the message actually originated from a computer named XDREAM and was sent from the mail.augustmail.com SMTP server.

Unfortunately, even the headers don't always tell you the truth about where the message came from. Spammers and other spoofers often use open relays to send their bogus or malicious messages. An open relay is an SMTP server that is not correctly configured and so allows third-parties to send e-mail through it that is not sent from nor to a local user. In that case, the "Received from" field in the header only points you to the SMTP server that was victimized.

Note:

Note:
For more information about open relays, see http://www.menandmice.com/9000/9221_mail_relay.html.

There Ought to be a Law

In fact, several U.S. states do have laws against e-mail spoofing. Many state anti-spam laws, such as those of Washington, Maryland and Illinois, specifically prohibit using third party mail servers or a third party's domain name without the permission of the third party. The federal CAN SPAM Act also makes it illegal to send unsolicited e-mail with false or misleading headers or deceptive subject lines.

The problem with such legislation is that by its very nature, spoofing conceals the identity of the sender and thus makes it difficult to sue or prosecute. Nonetheless, it's a good idea to report deceptive e-mail to the Federal Trade Commission, which has a special e-mail account set up for that purpose at uce@ftc.gov. You can also go to the Commission's Web site at http://www.ftc.gov/bcp/conline/edcams/spam/ and click the "File a Complaint" link.

Technological Solutions

Although legislation may help to deter some spoofing, most agree that it is a technological problem that requires a technological solution. One way to control spoofing is to use a mechanism that will authenticate or verify the origins of each e-mail message.

The Sender Policy Framework (SPF) is an emerging standard by which the owners of domains identify their outgoing mail servers in DNS, and then SMTP servers can check the addresses in the mail headers against that information to determine whether a message contains a spoofed address.

The downside is that mail system administrators have to take specific action to publish SPF records for their domains. Users need to implement Simple Authentication and Security Layer (SASL) SMTP for sending mail. Once this is accomplished, administrators can set their domains so that unauthenticated mail sent from them will fail, and the domain's name can't be forged.

Note:
For more information about SPF, see http://spf.pobox.com. The specifications for SASL are available in RFC 2222 at http://www.ietf.org/rfc/rfc2222.txt.

Microsoft and others in the industry are working on the Sender ID Framework, which is based on SPF and is under review by the Internet Engineering Task Force (IETF). The technology has been the source of some controversy. AOL recently withdrew its support for Sender ID and went back to SPF, and the Apache Software Foundation announced in September that they were rejecting Sender ID. Most of the controversy is due to patent and licensing issues, but there are some technical differences in the two mechanisms: Sender ID uses RFC 2822 specifications for checking header information in e-mail messages, while SPF uses those of RFC 2821 ("mailfrom" verification).

Note:
You can read more about the Sender ID Framework here: http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx

Other technological solutions, such as digitally signed e-mail, with either desktop or gateway verification, have been proposed by such bodies as the Anti-Phishing Working Group (www.antiphishing.org).

Whichever mechanism becomes the standard, introducing a technological solution is a step in the right direction that will allow you to know who is sending mail to you, just as the telephone company's Caller ID allows you to know who is calling.

Summary

E-mail spoofing is a growing problem and has reached the point where you cannot rely on the information displayed in your e-mail client to tell you who really sent a message. Some jurisdictions have enacted laws against this form of "e-mail identity theft," but the more effective solution is apt to be a technological one that makes it possible to authenticate the senders of e-mail messages. The most popular mechanisms currently in development are SPF and Microsoft's Sender ID. In this article, we took a look at the problem and the proposed solutions.

About Deb Shinder

Debra LittleJohn Shinder(MCSE) is a technology consultant, trainer and writer who has written a number of books on networking, including Computer Networking Essentials, published by Cisco Press and Scene of the Cybercrime, published by Syngress Media. She is co-author, with her husband Dr. Thomas Shinder, of Troubleshooting Windows 2000 TCP/IP and the best-selling Configuring ISA Server 2000, both published by Syngress Media, as well as the new ISA Server and Beyond. Deb tech edited Syngress's Security + Study Guide and was a major contributor to Que's TruSecure ICSA Certified Security Associate exam guide. Deb lives and works in the Dallas-Ft Worth area and can be contacted at deb@shinder.net or via the website at www.shinder.net

Click here for Deb Shinder's section.

Check out these recent articles by Deb Shinder

- **Nov 04, 2004,** Do You Leave Sensitive Data Lying Around?
- **Nov 02, 2004,** Instant Messaging: Does it have a Place in Business Networks?
- **Oct 07, 2004,** Review: Windows XP Security Guide
- **Sep 16, 2004,** Controlling Portable Storage Device Usage (USB/CDs etc) - Software Review: GFI LANguard P.S.C.
- **Aug 12, 2004,** Personal Firewalls for Remote Access Users