

Email SPAMMING and Email SPOOFING

Wonder what is going on with all these e-mails that you didn't send yourself? Or those e-mails that look like it was sent by someone but really wasn't?

Within these days of massive communication via e-mail, it comes to be quite important for anyone to be familiar with the following two terms: email “spamming” and email “spoofing”.

- Email spamming refers to sending email to thousands and thousands of users - similar to a chain letter. Spamming is often done deliberately to use network resources. Email spamming may be combined with email spoofing, so that it is very difficult to determine the actual originating email address of the sender. Some email systems, including Microsoft Exchange, have the ability to block incoming mail from a specific address. However, because these individuals change their email addresses frequently, it is difficult to prevent some spam from reaching your email inbox.

- Email spoofing refers to email that appears to have originated from one source when it was actually sent from another source. Individuals, who are sending “junk” email or “spam”, typically want the email to appear to be from an email address that may not exist. This way the email cannot be traced back to the originator.

Malicious Spoofing

There are many possible reasons why people send out emails spoofing the return address: sometimes it is simply to cause confusion, sometimes it is to discredit the person whose email address has been spoofed: using their name to send a vile or insulting message.

Sometimes email spoofing is used for what is known as “phishing”, which aims to trick the recipient into revealing passwords or other information. For example, you get an email from what appears to be the PayPal's account verification department, or from your ISP, asking you to go to a Web page and enter your password, or change it to one of their choosing.

Dealing with a Spoofed Email

There is no way to prevent receiving spoofed emails. If you get a message that is outrageously insulting, asks for something highly confidential, or just plain doesn't make any sense, then you may want to find out if it is really from the person it says it's from. You can look at the Internet Headers information to see where the email actually originated.

Remember that although your email address may have been spoofed this does not mean that the spoofer has gained access to your mailbox.

Internet Headers Information

An email collects information from each of the computers it passes through on the way to the recipient, and this is stored in the email's Internet Headers.

Tip: Internet Headers are best read from the bottom up, as they are added to as the email passes through the system.

Virus spoofing

Email-distributed viruses that use spoofing, such as the Klez or Sobig virus, take a random name from somewhere on the infected person's hard disk and mail themselves out as if they were from that randomly chosen address. Recipients of these viruses are therefore misled as to the address from which they were sent, and may end up complaining to, or alerting the wrong person. As a result, users of uninfected computers may be wrongly informed that they have, and have been distributing a virus.

If you receive an alert that you're sending infected emails, first run a virus scan using a full-featured locally installed anti-virus program (e.g. Norton Anti-Virus, McAfee, Nod32, AVG, BitDefender, etc). If you are not infected, then you may want to reply to the infection alert with this information:

"Your virus may have appeared to have been sent by me, but I have scanned my system and I am not infected. A number of email-distributed viruses fake, or spoof, the 'From' address using a random address taken from the Outlook contacts list or from Web files stored on the hard drive."

But keep in mind that a virus alert message is quite often auto generated and sent via an anti-virus server and so replying to the original email may not elicit a response.

Alternatively, if you receive an email-distributed virus, look at the Internet Headers information to see where the email actually originated from, before firing off a complaint or virus alert to the person you assume sent it.

Source: <http://www.anti-abuse.org/email-spamming-and-email-spoofing/>