TECHNICAL GUIDE No. 4

Email Address Spoofing

FAQ

People say they are receiving mail from my organisation, I know we are not sending this mail intentionally so what is happening?

When you send e-mail from your computer your mail software is programmed to tell the receiver that it is from you. Your address is known as the **reply-to address**, so when you send mail the receiver knows it is from you because of this and their computer knows that when they press the reply button, mail will be sent back to this address. However, your **reply-to address** is simply a setting on your computer which was input when your e-mail was configured, and there is no mechanism for validating that you are actually using a real, or even your own, e-mail in the reply-to address. Therefore, it is technically possible (and relatively simple) for people to send mail out using someone else's e-mail address, making it appear to the recipient as if the mail was not from the actual sender, but from someone else entirely. If someone chooses to send e-mail using someone else's address, when anyone replies to this e-mail the replies will not go to the person who has sent the mail, but instead they will go back to the person who's address has been used.

How do I know if someone else is sending mail, using my address as the reply address?

- If you receive replies to e-mail you know you haven't sent, you can be fairly sure that someone else is sending e-mail using your address as the reply-to address.
- If you receive bounced mail notifications (or delayed delivery notifications) telling you that messages you sent have not been successfully delivered, yet you know you did not send any e-mails in the first place, you can be fairly certain someone else is "spoofing" your address.
- If someone tells you that you have sent them a computer virus (but you have checked all of your systems and found that you are not infected), the likelihood is that they have received the virus from someone else who is using your address.

Why would other people want to use my email address?

On the majority of occasions with email spoofing, it's not an individual person that has maliciously decided to send mail out using your address. Many computer viruses (after infecting a computer) will find any email addresses stored on that machine and pick one at random. It will then mail the virus to all the other addresses, using that one randomly picked email (as the reply-to address). This means that anyone who has had your email address on their computer at some stage, and has subsequently contracted a computer virus, could without knowing it be sending mail out claiming to be coming from you.

Why I am receiving lots of messages from different internet providers telling me that my mail cannot be delivered to it's intended recipient?

Another common reason for email address spoofing can have more serious consequences for the person whose identity has been stolen. Junk email is the cause of much frustration among email users and for this reason, senders of junk email often "steal" someone else's identity when sending mass e-mailings. This ensures that all of the angry replies from people who did not wish to receive their junk mail go to someone else, so they never have to deal with them. In addition to this, many of the e-mail addresses to which they send to are inaccurate or invalid and for each one of these (using your email address as the reply-to address) you could receive a bounce message to say that the email has not been delivered properly. This can be significant, as sometimes these junk mailing lists can contain thousands of invalid addresses, meaning you could potentially receive thousands of unwanted emails.

What can I do to stop people using my email address when they send mail?

Unfortunately if someone is using your address, it can be difficult to track them down and stop it, but it is not always impossible. A better approach is to minimise the likelihood of someone stealing your identity in the first place, and there are many ways in which you can do this.

- Junk email senders often rely on finding poorly configured or insecure mail servers to send their mail. Make sure your companies email server is secure and properly configured. If you are uncertain – contact us to check the configuration for you, we offer this service free of charge. If they cant send the mail in the first place – there is little point in stealing someone else's address!
- Try and avoid getting your email address onto junk mail lists, see our Technical Guide "Managing Junk Mail" for information about how you can avoid this from happening.
- Take precautions to protect your systems from viruses, once a virus gets into a system and starts sending your address book information out onto the internet, it very quickly spreads your email addresses around the net. Even once you have removed the virus, the damage is already done, and all of your email details have been exposed on the internet.

For more information about solutions for combating junk email and protecting your IT system from hackers and virus's, please contact us on (01234) 301133.