

Spam emails

Tuesday, 30 August 2016

Last Updated Tuesday, 30 August 2016

A number of members have reported that their email has been used by supposed 'hackers' and that people in their contact list have received an email from them with malicious content.

Here are a couple of explanations for what may have gone on..

The first explanation relates to "Spoofing" where spammers harvest emails from a variety of sources and 'forge' an email from them that looks like one from your email. i.e. Email spoofing is the creation of email messages with a forged sender (your) address.

When an SMTP email is sent, the initial connection provides two pieces of address information:

- MAIL FROM: - generally presented to the recipient as the Return-path: header but not normally visible to the end user, and by default no checks are done that the sending system is authorized to send on behalf of that address.

- RCPT TO: - specifies which email address the email is delivered to, is not normally visible to the end user but may be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope and unless the receiving mail server signals that it has problems with either of these items, the sending system sends the "DATA" command, and typically sends several header items, including:

- From: Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address., and

- Reply-to: Jane Roe <Jane.Roe@example.mil> - similarly not checked

There is not much one can do about this. When you have your email out there on a website it is commonly harvested for various (mostly bad) reasons by others. It does not necessarily mean that your email account has been hacked, but it is probably useful to change your password to re-assure yourself.

<http://www.netregistry.com.au/support/my-email-address-appears-to-be-sending-spam-what-do-i-do/>

The second explanation is that you have a virus that looks through your contacts list and sends out real emails from you. Not spoofing. You need to check your computers for viruses and eliminate.

See also this link

https://en.wikipedia.org/wiki/Email_spoofing