

Email spoofing is a technique frequently used by perpetrators of all manner of email hoaxes to hide their identities and point the blame at somebody else. It is a favourite with spammers and also used by hackers. Spoofing received some media coverage recently when a 12-year-old was able to demonstrate how he apparently sent an email purporting to come from the UK Prime Minister to the Chancellor of the Exchequer.

email spoofing

Background

The sending of spoof email is usually carried out for the purposes of causing embarrassment or the misinterpretation of the individual or organisation whose address has been spoofed.

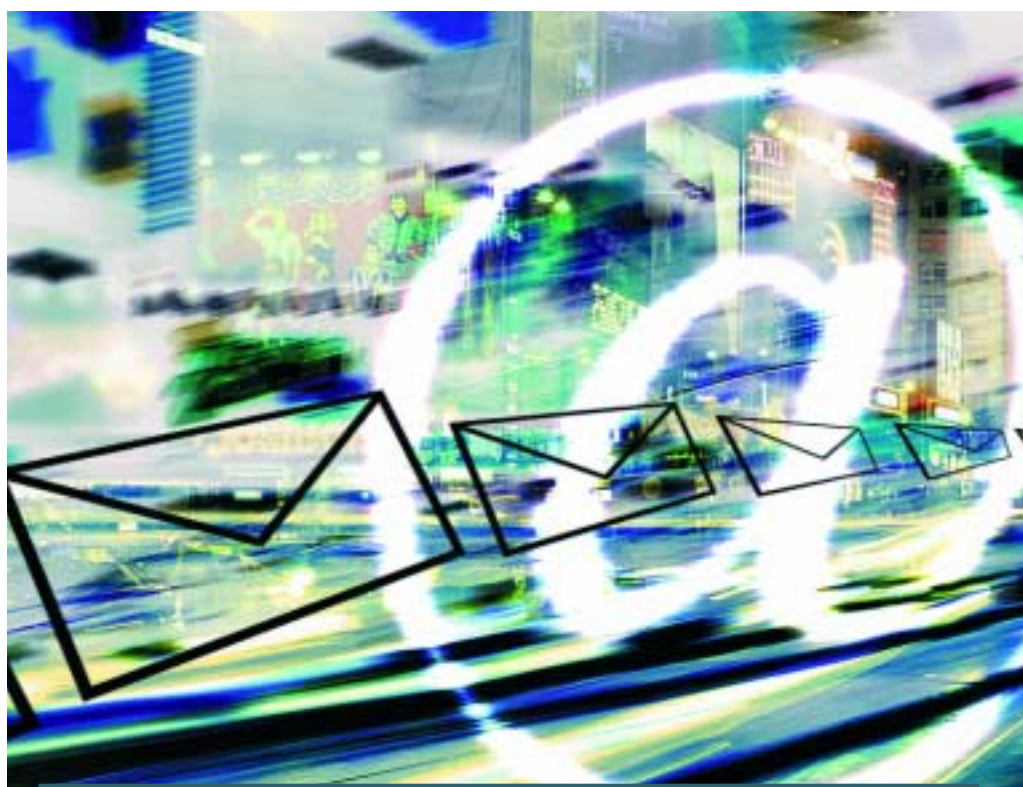
Consequences could include recipients of the email divulging information to those not entitled to have it. The information may then be used in a manner detrimental to the victim of the spoof. For example, interference with customer records, with a resultant impact on the customer. In the UK, the sending of spoof email is, in itself, not illegal although there is scope for legal action where personal information is obtained by deception or the email has threatening content.

Methodology

Sending spoof email is very simple. Most email software displays the "date received", "from" and "subject" fields.

The email header containing address and routing information is generally hidden from view to prevent cluttering the screen and confusing the user.

Consequently a user can be deceived if the sender simply changes the "from" field. The address is not normally checked at any stage in the process of sending an email and does not even have to be a valid address. There is little



Email spoofing - the threat

Any IT literate individual or group could use simple email spoofing. The effects which they can achieve with such attacks are limited only by their imagination and ability to write a convincing bogus content. The following scenarios could be imagined:

- Producing spoof press releases from a company or Government department to cause embarrassment.
- Causing disruption and wasted time by feeding misinformation to critical national infrastructure organisations.
- Encouraging users to switch off IT security features or passwords by spoofing emails from a security department.



that can be done at the server end to stop this, the only available options being:

- to make employees aware of the email spoofing risk;
- to require all email addresses to contain a valid domain name. This is currently being done, but even though the domain names can be checked, the email addresses themselves cannot;
- for internal mail servers to require all source email addresses to contain the organisation's domain, unless the email is coming from an external mail server;
- to provide some form of digital signature, as per Public Key Infrastructure (PKI). This is the only real countermeasure, but even this is not perfect;
- authentication on the mail server (SMTP AUTH), which can provide assistance in tracking down internal staff who create spoofed email, as can the use of the IDENT protocol, which may provide the username of the sender.

Various domain name checks, such as allowing the recipient server to check the existence of the source domain as well as that of the recipient, can be done, but this will depend on the software being used.

Sending spoof email is very simple... Once an email has been received, there is likely to be little about it that immediately identifies it as spoofed.

Identification

Once an email has been received, there is likely to be little about it that immediately identifies it as spoofed. The only technical indicators, to be found in the "internet" or full email header are:

- Instead of being marked as "From:" the email is marked as "Apparently-From:". This usually indicates a hand-built email and as such the address is likely to be false.
- The "Message-ID:" header and the "Received" header immediately above it in the internet headers list contain different domain names. This usually indicates that the headers have been faked.
- The "Message-ID" header contains a domain that differs from the domain in the "From:" address. However, this does not guarantee that the email is spoofed.
- The domain in the first "Received:" header is different from that in the "From:" address. Again, this does not guarantee that the email is spoofed.

Other indicators may include:

- The grammar, language or style of writing is not consistent with the email address the email claims to come from.
- The email may be missing the standard 'signature' the apparent sender may use.
- The email claims to be from an individual who doesn't exist within the organisation in question.
- If email purports to come from a government site, but does not bear a government address.

With all of the above, the common requirement is that users should be both aware of and alert to what indicators they should be looking out for.

If the sender desired further concealment, they could use an open email relay server. These are poorly secured servers that allow anybody on the Internet to connect to them and send email out. In this case, investigators examining the header of the email would only be able to trace back as far as the open mail relay, and not to the true originator.

Conclusion

The effects of email spoofing can be limited by the appropriate configuration of email servers and improved user awareness of the problem. Currently, the only real countermeasure is the use of digitally signed messages that allow a recipient to authenticate the identity of the sender.

N.I.S.C.C. (<http://www.niscc.gov.uk>)