Spoofed/Forged Email

I. Description

Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Examples of spoofed email that could affect the security of your site include:

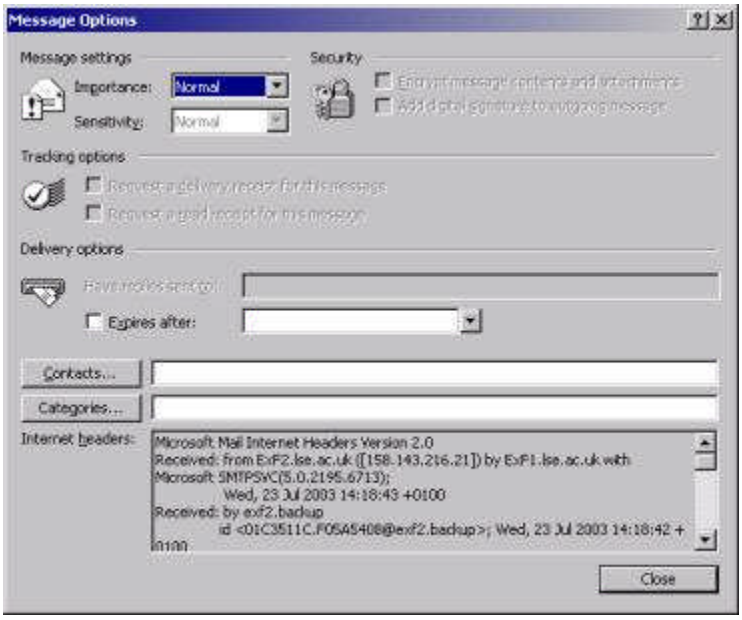
- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

If, after investigating the activity, you find that there is more to the incident than spoofed email (such as a compromise at your site or another site),

Displaying 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**.

1. With the Outlook **Inbox** displayed, right-click on the message and click on the **Options** command to display the **Message Options** dialog box.



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

2. Scroll to the bottom of the information in the **Internet Headers** box, then scroll slowly upwards to read the information about the email's origin. The most important information follows the "Return-path:" and the "Reply-to:" fields. If these are different, the email is not who it says it's from.

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.

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.

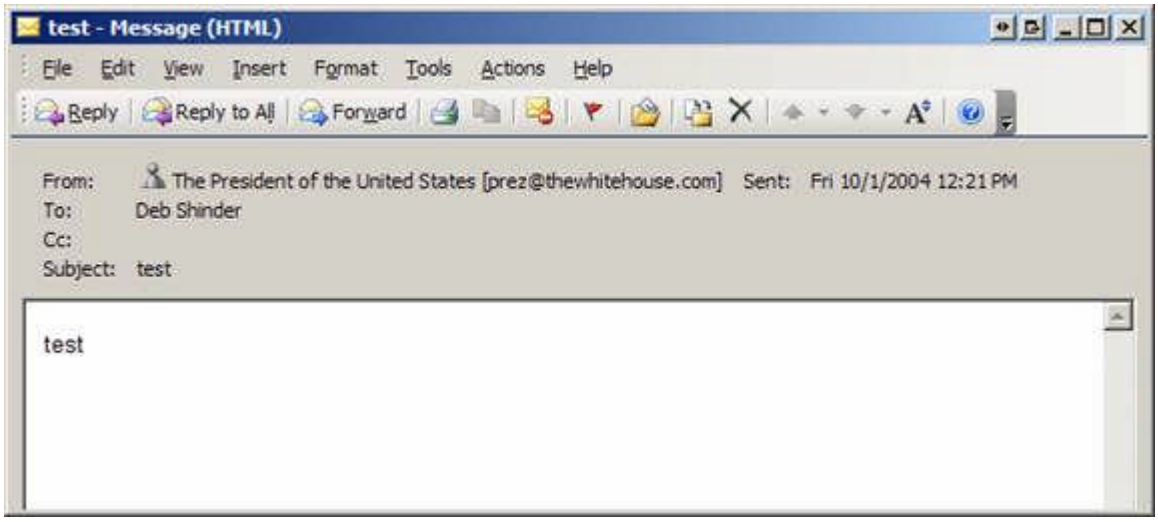


Fig 2: The recipient sees whatever information you entered

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.

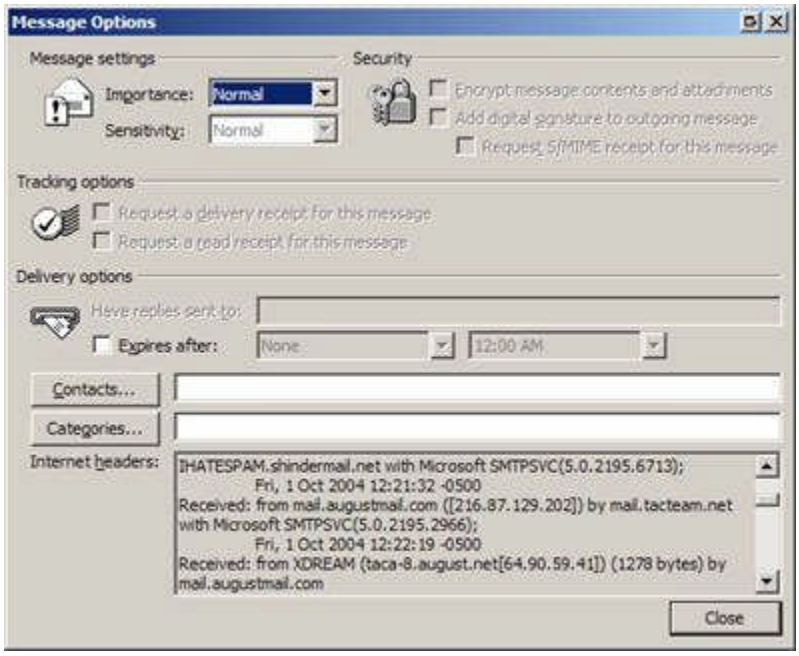
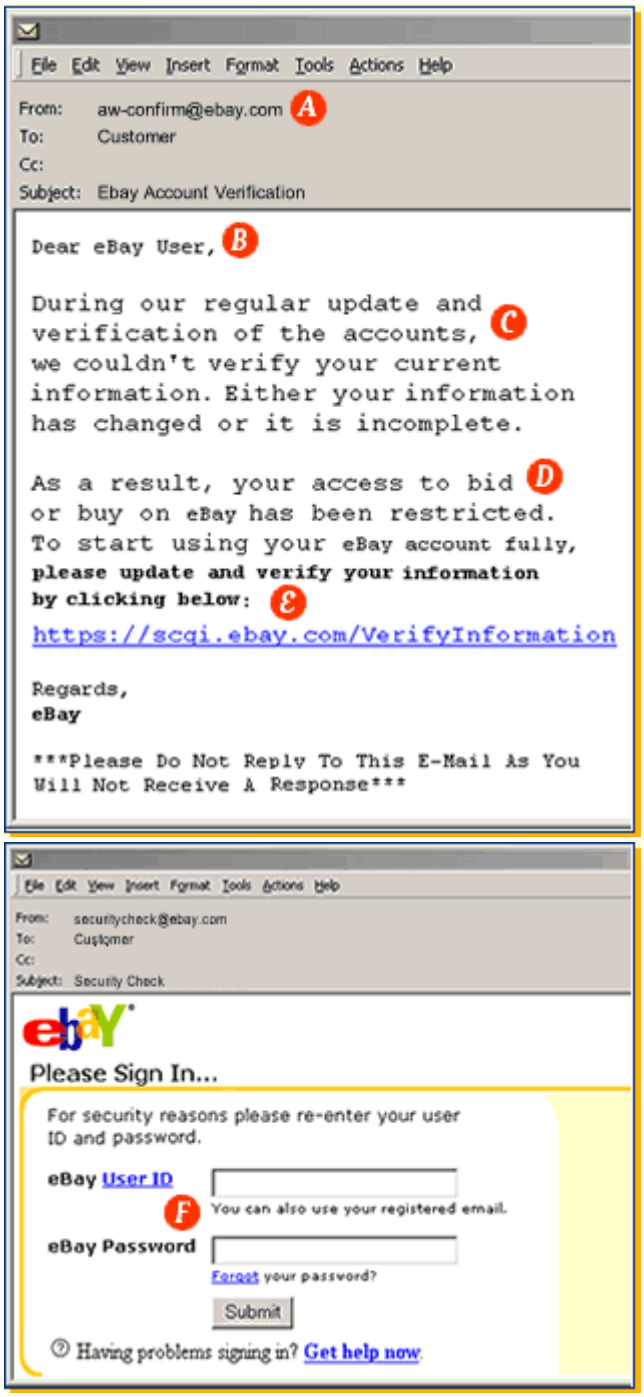


Fig 3: Viewing the e-mail headers

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

Warning Signs of a Spoof Email



A. Sender's Email Address

Spoof email may include a forged email address in the "From" line - Some may actually be real email addresses that have been forged. (From: billing@ebay.com; From: eBayAcctMaintenance@eBay.com; From: support@ebay.com).

B. Email Greeting

Many Spoof emails will begin with a general greeting .

C. Urgency
Claims that eBay is updating its files or accounts - Don't worry, it is highly unlikely that eBay will lose your account information.

D. Account Status Threat
Most Spoof emails try to deceive you with the threat that your account is in jeopardy and you will not be able to buy or sell on eBay if you do not update it immediately.

E. Links in an Email
While many emails have links included, just remember that these links can be forged too.

F. Requests Personal Information
Requests that you enter sensitive personal information such as a User ID, password or bank account number by clicking on a link or completing a form within the email are a clear indicator of a Spoof email.

II. Technical Issues

- If you provide email services to your user community, your users are vulnerable to spoofed or forged email.
- It is easy to spoof email because SMTP (Simple Mail Transfer Protocol) lacks authentication. If a site has configured the mail server to allow connections to the SMTP port, anyone can connect to the SMTP port of a site and (in accordance with that protocol) issue commands that will send email that appears to be from the address of the individual's choice; this can be a valid email address or a fictitious address that is correctly formatted.
- In addition to connecting to the SMTP port of a site, a user can send spoofed email via other protocols (for instance, by modifying their web browser interface).

III. What You Can Do

A. Reaction

1. You may be alerted to spoofed email attempts by reports from your users or by investigating bounced email error messages.
2. Following relevant policies and procedures of your organization, review all information (such as mail headers and system log files) related to the spoofed email.

   Examine tcp_wrapper, ident, and sendmail logs to obtain information on the origin of the spoofed email.

   The header of the email message often contains a complete history of the "hops" the message has taken to reach its destination. Information in the headers (such as the "Received:" and "Message-ID" information), in

conjunction with your mail delivery logs, should help you to determine how the email reached your system.

If your mail reader does not allow you to review these headers, check the ASCII file that contains the original message.

NOTE: Some of the header information may be spoofed; and if the abuser connected directly to the SMTP port on your system, it may not be possible for you to identify the source of the activity.

3. Follow up with other sites involved in this activity, if you can identify the sites. Contact them to alert them to the activity and help them determine the source of the original email.

   We would appreciate a cc to "cert@cert.org" on your messages; this facilitates our work on incidents and helps us relate ongoing intruder activities.

   If you have a CERT# reference for this incident, please include it in the subject line of all messages related to this incident. (NOTE: This reference number will be assigned by the CERT/CC, so if you do not have a reference number, one will be assigned once we receive the incident report.)

   You may also want to contact the postmaster at sites that may be involved. Send email to

   postmaster@[host.]site.domain (for example, postmaster@cert.org)

   Please include a copy of this document in your message to sites.

4. To provide as much information as possible to help trace this type of activity, you can increase the level of logging for your mailer delivery daemon.
5. Realize that in some cases, you may not be able to identify the origin of the spoofed email.

B. Prevention (Deterrence)

1. Use cryptographic signatures (e.g., PGP "Pretty Good Privacy" or other encryption technologies) to exchange authenticated email messages. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software. Using certificates in this manner increases the amount of authentication performed when sending mail.
2. Configure your mail delivery daemon to prevent someone from directly connecting to your SMTP port to send spoofed email to other sites.
3. Ensure that your mail delivery daemon allows logging and is configured to provide sufficient logging to assist you in tracking the origin of spoofed email.

4. Consider a single point of entry for email to your site. You can implement this by configuring your firewall so that SMTP connections from outside your firewall must go through a central mail hub. This will provide you with centralized logging, which may assist in detecting the origin of mail spoofing attempts to your site.
5. Educate your users about your site's policies and procedures in order to prevent them from being "social engineered," or tricked, into disclosing sensitive information (such as passwords). Have your users report any such activities to the appropriate system administrator(s) as soon as possible.

IV. Additional Security Measures That You Can Take

A. If you have questions concerning legal issues, we encourage you to work with your legal counsel.

U.S. sites interested in an investigation of this activity can contact the Federal Bureau of Investigation (FBI). Information about how the FBI investigates computer crimes can be found here

http://www.cert.org/tech_tips/FBI_investigates_crime.html

For information on finding and contacting your local FBI field office, see

http://www.fbi.gov/contact/fo/fo.htm

Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps for pursuing an investigation.