



Take a second to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: www.longwood.edu/infosec

April 2008



What is ... e-mail spoofing?

E-mail spoofing occurs when the "From:" lines of e-mail messages are disguised to make e-mail messages appear to be from someone other than the actual sender.

3.8 million

The approximate number of spam messages that were prevented from reaching University inboxes in 2007.

Save Yourself and Your Inbox from Spam

We all know that no foreign royalty needs our help in accessing a large sum of money and that legitimate pharmaceuticals are not advertised through e-mail, but that does not stop spammers from trying to trick us with such messages. Spam uses up IT resources, wastes our time, puts our computers at risk and annoys us, but it is an unfortunate reality for all e-mail users.

Spam is a general term for unsolicited bulk e-mail and the term spam also includes messages phishing for account details and messages spreading malware. While spam filters provide protection from some unwanted messages, some of the messages still make their way to us.

What should I do when I receive spam?

- *Delete all spam messages immediately.*
- *Never click any links in spam messages.* While these messages may contain "unsubscribe" links, clicking the link only verifies that the e-mail account is active and may lead to more spam.
- *Never reply to spam messages.* Do not purchase anything from spammers and do not reply to any message with your personal or account information.

How can I reduce the amount of spam I receive?

Be careful with whom you share your e-mail address.

When you register with online sites and services some companies will ask you if you are interested in receiving messages from other companies they are affiliated with or if they can contact you with offers. The box is generally checked by default to receive such offers. Make sure to uncheck the box to avoid receiving unwanted messages.

Today many organizations (stores, doctor's offices) request your e-mail address. Your e-mail address is rarely required information and you should consider whether you are interested in receiving e-mail solicitation from such companies. In addition, you should make yourself aware of how any organization will use your e-mail address.

Avoid posting your e-mail address on the Internet when it is not necessary. Spammers search the Internet for e-mail addresses and by limiting the number of times your e-mail address appears you may be able to limit the spam you receive.

Messages Go Grey to Prevent Spam

Greylisting is just one way that the University reduces the amount of spam messages you receive by asking for mail from unrecognized sources to be sent again by the sending server. Legitimate mail servers are set up to send the message again, but spammers do not usually retry. A delay you may sometimes notice in receiving messages sent from outside of Longwood is the result of the University's greylisting process which keeps unwanted messages from reaching you.

Less spam means:

- Less messages carrying links to sites spreading malware
- Less messages carrying malicious attachments
- Less phishing messages attempting to steal account information or your identity
- Less messages promoting dangerous scams



Security
Spotlight

Spam scams usually look too good to be true. Find out more about spam scams:

www.LooksTooGoodToBeTrue.com

28%

Percent of messages received at Longwood in 2007 that were spam messages and were stopped before reaching your inbox.



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. If you have any questions regarding the newsletter, please contact Melissa Short at 434-395-2034 or shortmj@longwood.edu.