



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](http://www.longwood.edu/infosec)

## Recognizing Fraudulent Web Addresses

You know that you should never click on links that you receive in e-mails that you were not expecting or that come from someone you do not know. The same rule applies to links you encounter on blogs, discussion boards or social networking sites. However, sometimes you may want extra assurance that a link is not legitimate. Understanding the anatomy of a web address can help you spot a fraudulent link.

Imagine the address below is your bank's web address that you see printed on the top of each monthly statement:

<http://www.yourfavoritebank.com/yfb>

Look between the http:// or https:// and the next / to determine the web address

Phishers and scammers may try tricks such as:

- **Misspelling the web address.**

For example, they may create a web site with the address

<http://www.yourfavoritbank.com/> hoping that you won't notice the missing "e" at the end of "favorite."

- **Creating a long address that includes the real web address.**

For example, they may create a web site with the address

<http://www.mnopq.com/yourfavoritebank.com> hoping that you won't notice that you are visiting the site mnopq.com.

- **Using a plausible, but not legitimate web address.**

For example, they may create a web site with the address

<http://www.yourfavoritebank-securitycenter.net/> hoping that you won't verify the actual address of Your Favorite Bank.

When in doubt – don't click that link. When accessing sites that are commonly spoofed in phishing messages, like bank or social networking sites, access the site by typing in the address from memory or from the address you've received on official correspondence (ex. your monthly statement) or use your "Favorites" list.

June 2009



## What is password strength?

Password strength refers to how many attempts it would take for a hacker to crack a password by either guessing or by using an automated program designed to break passwords. A password's strength is determined by the number and variety of characters used and the unusualness of the password (ex. not your user-name).

## Think Security When Setting Your Out of Office Message

Outlook 2007 provides you the ability to set one out of office message for your contacts within Longwood and a separate message for those who contact you from outside of Longwood. While it can be convenient to let your fellow Longwood employees and frequent non-Longwood contacts know about your absence, if you set up auto-replies to be sent to anyone who contacts you from outside the organization, not just those non-Longwood contacts in your contacts list, you could be confirming your e-mail address to spammers. Your auto-reply confirms to spammers that your account exists and is active. Once spammers know that the account is actively being used you are an even bigger target for spam. Weigh your needs versus the risks of spam when setting up your out of office messages.

See the [Help Desk web site](#) for more information on setting up out of office messages in Exchange.



*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](mailto:shortmj@longwood.edu).