



The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: <http://www.longwood.edu/infosec/awareness.htm>

February 2008



What is ... phishing?

Phishing is an e-mail based scam that uses e-mail messages appearing to be from well-known organizations, but that are actually from scammers looking for individuals to provide account information (login names, account numbers, passwords, etc.).

Banks and online auctions are often the companies impersonated in phishing messages.

Are You At Risk Of Being Phished?

You receive an e-mail carrying the logo of your bank informing you that your account will be terminated in two days and you should act immediately to protect your account by clicking the provided link. Following the link takes you to a website where you input your login name and password. However, you have not just confirmed your account with a reputable organization. You have provided your information to scammers who are looking for account information to conduct fraudulent transactions or identity theft.

Phishing is a continuously evolving scam that attempts to lure individuals into providing account information such as names, passwords, social security numbers, bank account numbers, etc. The messages may look real, with official-looking logos and well-written requests, but they are actually scams. As a general rule organizations never ask you to provide account information in this way.

The messages are sent to many users hoping at least a few will respond with their account information. Many of the recipients may not be customers of the imitated institution, but the scammers use a well-known organization to increase the chances that at least some of the recipients are customers of the institution imitated in the message.

However, as more individuals and institutions have become aware of phishing, phishers have adapted their scheme. In addition to bulk mailings of phishing messages, phishers have begun to more frequently conduct spear phishing attacks. Spear phishing occurs when the phisher knows something about you prior to sending a phishing message, such as where you work, and uses that information to attempt to gain your trust. Spear phishers may target many users across an organization or they may focus on attempting to scam specific individuals in positions likely to have the most access.

Spear phishers may be looking for access to network resources, such as e-mail accounts for sending spam, or for access to valuable account information. In addition to searching for information such as login names and passwords, spear phishers may also ask you to click a link or open an attachment to install malware onto your computer as a part of their targeted attack.

Tips to protect yourself from phishing:

- Be aware that as a general rule legitimate organizations do not ask for account information in e-mail messages. Know the policies of the organizations with which you do business.
- Never provide your password or other confidential account information in an e-mail.
- Always type in the web address of your bank or any other institution where you have an account and never rely on the links provided in e-mails to access such pages.
- All phishing messages should be deleted immediately and you should never click any links or open any attachments included in the messages because of the risk of malware.



Security Spotlight

Learn more about phishing and see examples of current phishing scams at <http://www.millersmiles.co.uk/>.



Current Threat

Recently several universities, including several in Virginia, reported being the targets of spear phishing attacks. E-mails sent to faculty, staff and students at various universities attempted to trick recipients into providing their passwords. The fake e-mail was made to appear to be from the university's IT office. **Longwood University's Information and Instructional Technology Services will never ask you for your password and you should never provide your password to anyone.**



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.