



The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

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

September 2008



What is denial of service?

Denial of service is a type of attack against a system that prevents authorized users from being able to access the system when they need to. For example an attacker may flood a web site with illegitimate traffic so that others can't access the resource.



Current Threat

We continue to receive the spearphishing messages asking for University user names and passwords. **Remember that IITS will never ask you for your password and you should never give it to us.** See the Information Security web site for more information.

Don't Click that Link, Even If:

You should never click links in e-mail messages from people you don't know or in messages you weren't expecting. However, sometimes those links seem tempting. Consider whether you have clicked links in any of the following scenarios and then read why clicking that link was a bad idea.

The message had the bank's logo and tagline so it must be real.

Creators of phishing messages who are seeking your account information often copy logos and taglines of the businesses they are spoofing to make their messages look real. Don't click a link in an e-mail just because the logos look real. Most companies now include their web address on official correspondence and you should go to your past statements or bills to find the real web address.

The site was collecting donations for disaster relief.

Unfortunately anytime a disaster strikes, such as a hurricane, some individuals attempt to profit by setting up fake web sites for disaster relief. The sites may be phishing sites, may install malware (viruses, spyware, etc.) on computers or may collect donations that never make it to the victims. Refer to the Better Business Bureau or the sites advertised from major media sources.

The message promised news about the election.

Sending fake headlines with a link for more information has been a very successful strategy in spreading malware over the last few years. The messages usually contain an outrageous headline and a link for an article, video or picture. To stay informed get your news directly from your favorite news web site, newspaper, television network, etc.

With faculty and staff no longer checking their e-mail from an account with administrative rights from University computers our exposure to malware in these instances is lessened. However, all users should practice safe computing on campus, at home and anywhere they use a computer.

To prevent installing malware...

To prevent being phished...

To prevent being scammed...

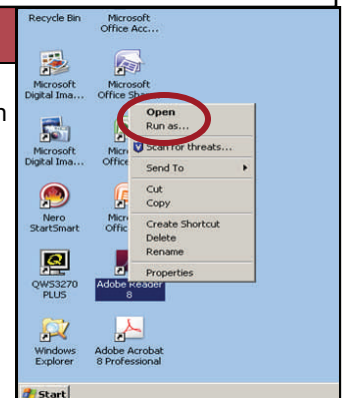
Remember: It's always best to type a web address in yourself or use a bookmark/favorites list rather than clicking links sent to you in e-mail messages.

Attention Administrative Account Users

If you have an administrative account instead of logging in and out of your regular user account to use your administrative account, you can save time by using "Run as." This allows you to run programs as an administrator while logged into your regular user account.

To "Run as" an Administrator:

1. From the Desktop or the Start Menu hold down the Shift key and right click the program you need to use your administrative account with.
2. A gray box appears with the option to "Run as."
3. When asked which account you want to use to run the program choose your administrative account.



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.