



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)

December 2008



## What are potentially unwanted programs?

Sometimes the programs you choose to install perform operations that you are unaware of and you do not want. For example, some programs you choose to install may also function as spyware that tracks what you do online.

## Dates to Remember



### December 5-6

Several new and revised IITS policies presented to the Board of Visitors for approval

### December 12

Online review of policies in Blackboard ends for policies to be presented to the BOV for approval in March 2009. See the Information Security web site for details.

## 5 Steps to Safer Online Shopping

If you plan to be one of the millions of Americans who will make purchases online this season we want to provide you several tips for safer online shopping.

- 1. Don't ever send account information in an e-mail.** No legitimate company will ask you to e-mail an account number. Legitimate companies are prepared to handle your transaction in a more secure way.
- 2. Make your purchases at websites that use "https."** While this prefix cannot provide 100% assurance that the site is safe, you should never enter account information into a site that doesn't secure your transaction in this way.
- 3. Be careful about providing your e-mail address.** Realize that providing your e-mail address can lead to spam. Consider using a separate personal account for online purchases. Make sure to indicate that you are not interested in receiving future offers if indeed you are not interested in receiving promotional e-mails from the retailer, or its partners, in the future.
- 4. Shop with trusted companies.** Never rely on the links within e-mail messages, blog postings, Facebook or MySpace postings or message boards to take you to a retailer's site; always type the address in yourself. This will help you avoid potentially unscrupulous vendors and sites that may infect your computer with malware. Also, remember that all reputable online businesses should have a physical address and a phone number.
- 5. Check your statements.** Checking your account statements regularly will help you detect fraudulent charges quickly.

Whether at work or at home the advice is the same, it's always worth taking a little time to be secure. A few seconds to type a web address, to check for https before entering account information or to find a seller you trust can save you time (and a major headache) in the future.



*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).