



The Security Minute

Take a second to be secure.

A communication of the Longwood University Information Security Office

Protect Yourself: Think Before You Click

The Internet is a useful tool for finding answers quickly; however, taking an extra second to think before clicking a link or installing a program may save you time and frustration as you avoid new and emerging threats.

By now you have likely heard or experienced a horror story resulting from clicking a link in an e-mail or instant message which caused a computer to become infected with malware. You should never click links or open attachments in e-mails or instant messages from individuals you do not know or from whom you were not expecting such a message. As blogs and message boards have emerged as a new form of communication the same rule now applies to these new communication channels. Spammers have moved to blogs and message boards with links to malware-filled websites that can put your computer at risk.

Protect yourself: Avoid following links in blogs or in message board content.

Common spelling mistakes may also put your computer at risk for malware. Typosquatting occurs when a website is created at a web address that is a common misspelling of a popular website address. A typosquatter's goals may include selling the address to the well-known entity with a similar address, presenting pay-per-click advertising, bombarding visitors with pop-up ads or installing spyware that tracks your online activity. During the months preceding the 2008 presidential elections and the 2008 Summer Olympics typosquatters specifically, and malware spreaders in general, may turn to these popular events to lure victims.

Protect yourself: Use antivirus, adware detection and spyware detection programs.

Longwood's Software Library: http://www.longwood.edu/helpdesk/software_library/library051707.htm.

Those spreading malware exploit popular sites and popular searches to infect as many users as possible. Following the assassination of former Pakistani Prime Minister Benazir Bhutto malicious websites promised video of the assassination. When attempting to view the video individuals would be asked to install a component that was actually a Trojan. Popular social networking sites, such as Facebook and Myspace, may also carry malware which may infect visitors who attempt to install add-on applications or view videos.

Protect yourself: Be cautious when prompted to install special components to access multimedia content.

New and Updated Policies

At the December 2007 Board of Visitors Meeting changes were approved for two Information and Instructional Technology Services (IITS) policies and a new IITS policy was also added.

- Policy 6105: Access to Information Technology Resources and Systems received changes most notably affecting termination of access.
- Policy 6128: Malware Protection was updated to reflect the changing environment of threats from which IT resources and systems must be protected.
- Policy 6131: Security Awareness and Training was created to include requirements for annual security awareness training.

View all IITS policies in the Administrative Policies and Procedures Manual: http://www.longwood.edu/vpaf/final_policy_base/Tables/TC6000.htm

January 2008



What is a ...trojan?

A Trojan (sometimes called Trojan horse) is a program that promises to provide a desirable service, such as allowing you to access multimedia files. However, when installed the program has hidden capabilities that are usually malicious, such as monitoring your computer activity for passwords.

A Trojan is a type of malware.



Security Spotlight

What can happen to your computer when you step away for just a second?

Follow the link to view a video demonstrating this risk:

<http://www.researchchannel.org/securityvideo2007/displayevent.aspx?rid=10992>

This video received honorable mention in the 2007 Security Awareness Video Contest sponsored by the EDUCAUSE/Internet2 Computer and Network Security Task Force, the National Cyber Security Alliance and ResearchChannel.



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.