



The Security Minute

A communication of the Longwood University Information Security Office

Take a second to be secure.

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

Security: Myths Versus Reality

Myth #1: Security isn't my responsibility.

Security is everyone's responsibility. Technological controls offer a layer of security, but decisions we make as users are essential to protecting information and systems. For example, for authentication processes (which verify users are who they say they are) to be effective passwords should never be shared with anyone. This is just one example of a way we must personally take responsibility for security everyday.

Myth #2: I don't have anything that a hacker would want.

All computers and their users are vulnerable to security threats such as malware installation and unauthorized access, which can lead to outcomes such as theft of information or unavailability of resources.

Computers and users are not targeted only for the information they hold, but their potential to be used for harm. Computers compromised by malware can be used to attack other computers, to send spam or to spread malware. Compromising just one account on an organization's network can give hackers the access they need to carry out more malicious attacks on an organization as a whole.

Myth #3: My antivirus software protects me.

Antivirus software does protect computers from malware such as viruses, worms and Trojans. However, other malware such as spyware and adware may not be detected by traditional antivirus software. As new strains of malware are created antivirus software must be updated to detect the new threat. Antivirus software that is not regularly updated offers limited protection. In addition, by observing safe computing practices, such as deleting suspicious e-mails, you can join your antivirus software in the fight against malware.

Time for Security Awareness Training

MOAT Recertification Deadlines Approach for Many

Annual security awareness training provided through the online program MOAT uses up-to-date examples and avoids technical jargon to provide information about security that will benefit you in your professional and personal life.

If you completed MOAT training last spring you have already or will soon receive an e-mail from Awareness.com notifying you that you must renew your certification. In general, faculty were enrolled in MOAT last spring; staff were enrolled in MOAT last summer. All new faculty and staff are enrolled in MOAT when their LancerNet ID is created.

To receive your MOAT recertification you will review information on security through the MOAT modules, take quizzes testing your security knowledge and agree to Longwood University policies in the "Vault." Information on completing the training is available from the Information Security website www.longwood.edu/infosec. Please note that only a Windows PC using the Internet Explorer browser can be used to complete the MOAT training. In addition, you must allow pop-ups from the site to complete the training.

University Policy #6131: Security Awareness and Training requires you to complete the training to retain access to University IT resources and systems.

March 2008



What is ... a patch?

Patches are small pieces of software that are distributed to fix problems with a computer program. Patches are necessary because imperfections in the way programs work may be exploited by hackers if not repaired.



Security Spotlight

Who are you sharing your Outlook calendar with?

In your Outlook calendar, the permissions for the "Default" account should be set to "none" to prevent all users (faculty, staff, vendors, etc.) from being able to read, change or delete your calendar entries.

For steps on setting your Outlook permissions visit: http://www.longwood.edu/helpdesk/outlook_calendar.htm.



The Security Minute will be a monthly publication designed to raise awareness of information security related issues and concerns. Look for upcoming issues of *The Security Minute* and other security awareness initiatives.