

Protect Yourself: Viruses and Spyware

This is the third in a series of bulletins for National Cybersecurity Awareness Month. Each bulletin will address a topic in computer security that will help you keep your computer and your personal information safe. This week's topic covers how to help protect yourself from viruses and spyware. The advice in this bulletin is not specific to any one operating system, but rather is advice that every user should heed.

One of the easiest ways for viruses to spread is to trick you into clicking on it. The most famous example of this is the "I Love You" virus from 2000. This virus arrived via email and included an attachment named "Love-letter-for-you.txt.vbs". If a user opened the attachment, the virus infected the computer and then sent out copies of itself to email addresses in the user's address book, pretending to come from the user. It is estimated that this virus, which required users to click on it, affected over 45 million computers worldwide, and is estimated to have caused almost \$10 billion dollars worth of damage.

Most of the people who clicked on the email and were affected were running antivirus software with up to date virus definitions. However, it is important to realize that antivirus software is reactive, and does not work against new viruses. When a new virus is released, antivirus vendors obtain a sample of the virus, and write up virus definitions to allow their software to identify it. Until your computer has updated virus definitions, your antivirus software will not protect you. So you have to be careful about what files you click on.

If you receive an unexpected file or website link from someone over email or an instant messenger, simply send the message back and ask the user if they sent it. This simple step requires little effort, and greatly decreases the odds that you will be tricked by programs that pretend to send messages from your friends that are actually from a virus or spyware program.

The most common way for spyware to spread is to bundle itself with free software that you want. For instance, if you download Kazaa, a popular file-sharing application, it comes bundled with numerous spyware and adware applications. These applications will report back information about your web surfing habits, pop up unwanted advertisement windows, and noticeably slow down the speed of your computer. As a general rule of thumb, there are three types of free software available on the Internet. The first is open source software, which the author has intentionally provided for no charge. The second is shareware software, which the author has provided a limited or trial version for no charge with the hope of getting you to purchase the full version. The third is software bundled with spyware, where the author makes money not from selling software, but from selling information gathered from your computer to advertisers. If you can't clearly identify a piece of software as being open source or shareware, odds are that it is bundled with spyware.

If you have additional questions, you may want to check out Loyola's Information Security website at http://www.luc.edu/is/security/protect_yourself.shtml or send your questions to InfoSecurity@luc.edu. Next week's bulletin will be about protecting yourself from phishing and other online scams.