TAYLOR UNIVERSITY Client Services Located in the T&LC 4040

http://4040.taylor.edu

Intro to Malware & SPAM

Definitions

- **Virus**: A malicious program that searches out other programs and ‘infects’ them by embedding a copy of itself in them. When these newly infected programs are executed, the embedded virus is executed too, thus propagating the ‘infection’. This normally happens invisibly to the user. Unlike a worm, a virus cannot infect other computers without assistance.
- **Trojan Horse**: A Trojan Horse is a seemingly-innocent program that contains and conceals harmful code. When a Trojan Horse is opened, the malicious code performs its damage on the unsuspecting computer.
- **Worm:** A computer program which replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. Worms are usually designed to slow down a network or to crash it.
- **Spyware:** A technology that assists in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is loaded onto a computer to secretly gather information about the user and relay it to advertisers or other interested parties. It is a hidden software program that transmits user information via the Internet to advertisers; often, this is in exchange for free software.
- **Phishing**: Comes from the analogy that internet scammers are using email bait to fish for passwords and financial data from the sea of internet users. Since hackers have a tendency of replacing "f" with "ph", the term phishing was derived. The term has evolved over the years to include not only obtaining user account details but also access to all kinds of personal and financial data.
- **SPAM**: Unsolicited bulk email, usually advertising or phishing attempts, sent to large numbers of people.

Methods of Infection

- **Viruses, Worms, Trojans:** E-mail, USB drive, website, network share
- **SPAM:** Posting/Registering your e-mail address on websites, forums, lists
- **Spyware:** Website, freeware and other programs, e-mail

Fighting Viruses, SPAM, and Spyware

There are two aspects to fighting viruses, SPAM, and Spyware: *Prevention* and *Detection*. Detection involves two aspects – installing software and keeping that software up-to-date.

Viruses:

Prevention involves using safe computing habits to avoid infection, such as:

- Saving attachments to the Desktop and scanning prior to opening
- Shutting down all unnecessary network shares
- Using read-only shares when possible

Detection involves running anti-malware software and keeping that software up-to-date. Taylor licenses Microsoft Endpoint Protection for Taylor-owned, Windows-based computers. Updates are provided automatically while PCs are physically connected to the internet. Updates include information about new viruses, worms, and Trojan horses.

Learn more: Malware Removal (Win) Malware Removal (Mac)

Spyware:
Prevention involves being careful and informed when installing software. Many free software programs include spyware. Many websites install Cookies and other tracking mechanisms without your knowledge.

Detection involves running anti-malware software and keeping it up-to-date. Many anti-malware programs are free for personal use only. Malwarebytes and Super Antispyware are recommended anti-malware programs for non-Taylor computers. These programs scan every file on your hard disk looking for programs defined as spyware. Once spyware is identified, you're given the option to remove the offending files.

SPAM:
Prevention involves being careful when giving out your email address. You should consider signing up for a Gmail, Yahoo, or other free mailbox and use this alternate address, instead of your Taylor address, when registering online.

Detection involves running anti-SPAM software. Taylor has a SPAM server-side solution (Barracuda) in place to intercept the majority of SPAM related email. SPAM intercepted by Barracuda is held in Quarantine until it is deleted by the user.

SPAM filters work by 'scoring' each piece of mail and routing the mail based on its score. The more 'SPAM-like' the mail is, the higher it scores. High scoring mail is deleted or quarantined. Low scoring mail is delivered to your Taylor mailbox. Barracuda allows each user to adjust their level of SPAM protection. See our SPAM Tutorial for more info.