Victory over Viruses!
Marshall District Library
March 19, 2013

Definitions

If you're not sure what the difference is between a bot and a worm, take a look at these definitions of Malware from Norton Antivirus Center. Minus the obvious plugs for their product, it is a good overview of the different types of threats that are out there. We talked about Spyware, Adware, Keyloggers, Bots, Viruses, Worms, Trojans and Rootkits.

Malware Prevention

During the class, we talked about different types of tools to prevent malware, and some healthy habits to get into to avoid attacks.

- Antivirus Software – Please, please use antivirus software of some kind. There many options, including free and paid services that can prevent, detect and remove malware of all kinds.
- Internet Security Software – Usually part of an anti-virus suite, this kind of software protects your personal information when you are using the web for things like banking or purchasing products online.
- Firewalls – Every Operating System has some kind of firewall system. Make sure yours is turned on. Firewalls let the good stuff in, and keep the bad stuff out.
- Updates and Patches – Keep your software up to date, including Operating System updates (Windows or Mac OSX). Also keep browser patches up to date, including flash and java.
- Beware of Hoaxes – If something seems too good to be true, don't click on it. (e.g. "Click here for a free iPad!!!")

Browse Safer

Safe Internet Browsing Tips (adapted from Norton AntiVirus Software Center):

- Keep software and security patches up to date.
    - Patches are often put out *after* threats have attacked their programs, and the companies are making sure other users aren't affected.
        - Adobe Reader – In 2009, attacks using malicious PDFs made up 49 percent of Web-based attacks, according to security firm Symantec.
        - Adobe-Flash
        - Oracle-Java
- Only visit reputable or trustworthy sites
    - When people visit untrustworthy sites, they may accidentally:
        - share their personal information

        - allow spyware and adware to be implanted into their computer
- If you are banking or making a transaction, look for the https://
    - A plain http connection may not be secure when banking or making purchases online, meaning your information could be intercepted by a hacker.
- Never give a password or Social Security # to anyone (even if the email/site looks official).
    - A reputable company would never ask for this information. Exceptions may apply ex: filing taxes online or filing for unemployment online.
- Talk to kids/grandkids about the danger of revealing information online
    - Identity theft
    - Endangerment
- Only use reputable software
    - Some companies may make software that acts as a front for **malware**.
        - Many games from knock-off companies
        - Track computer usage (intrusion of privacy)
- Configure Computer Security Settings
    - Make sure security settings are in place for your Operating System, Internet browser(s) and Security Software.
    - If you're not sure, you may want to have more restrictive permissions in place.

Make Stronger Passwords (adapted from MacWorld March 2012)

Make sure passwords are difficult and do not repeat passwords different sites.

- In June 2012, 6 Million LinkedIn passwords were stolen and posted online
- In July 2013, 450,000 Yahoo passwords were leaked.
- If you use the same password across multiple sites, you are making it easy for a hacker to gain access to valuable information, including your email.
    - By clicking "I forgot password," they could use your email to gain access to other sites, such as your Amazon account, etc.

Tips for a stronger password

- Don't reuse passwords
- Avoid: *123456, password, baseball, password1,* or patterns of keys like *qwerty*
- Use a longer password; Experts recommend 12-14 characters

- If possible use a password randomly created by the computer
- Use Password Management Software
- Use entropy – the example below uses two words that would normally never go together:
    - *blanketsensory*
- Mnemonic cues – You could create a phrase and use the first letter of each word, while throwing in a number or capitalization (easier to remember).
    - "I once drank three cups of coffee before realizing it was decaf" = *Iod3cocbriwd*

The Most Dangerous Places on the Web

For a comical yet informative list of the most dangerous places on the web (color coded by threat level – *Blue* being perfectly Safe, *Red* meaning "Danger Will Robinson") please check out this article by PCWorld from September 2010.

Which Antivirus should I use?

There are a range of excellent paid and free tools you can use to prevent, detect and delete malware from your computer system.

Paid or Free Antivirus?

Free Antivirus Software

- Free antivirus software usually provides a bare minimum level of protection.
- It will scan for malware, and often can perform automatic scans, too.
- Features are usually limited.
- Usually no technical support.
- Advertising built in the product for you to upgrade the product to the paid version.
- Most of the free products tested put up identical or nearly identical malware detection scores to the paid varietals put out by the same company.
- Tradeoff of not scoring as high is computer tends to run faster with free anti-virus

Some free antivirus are:

- **AVG**
- **Avira**
- **Avast**
- **Ad-Aware**
- **Microsoft Security Essentials**

Paid Antivirus Software

- Paid antivirus straddles a middle ground between the basic freebies and the feature-packed security suites.
- They typically offer more comprehensive security tools such as parental controls and identity theft protection
- Technical Support
- On the whole, paid antivirus products did a slightly better job at detecting malware than their freebie counterparts. 96.2 percent of the malware samples overall. By comparison, free products' scores were ever-so-slightly worse, detecting 95.7 percent of samples (PC WORLD).
- Slightly better job at removing malware.

Some paid antivirus are:

- **Kaspersky**
- **Norton**
- **Zone Alarm**
- **Trend Micro**

Malware Removal Tools

PC

- Malwarebytes
- Spybot

MAC

- Clamxav