Practicing Safe Computing
Hal Bookbinder

Definitions

Malware – executable software that is intended to simply annoy, steal information, delete data or even damage or disable computers and computer systems.

Classes of Malware

- Based on how they travel
  - Viruses –arrive as passengers on email or from websites you visit.
  - Worms – spread themselves by finding other computers.

- Based on how they appear
  - Trojan Horses – appear to be something innocent.

- Based on what they do
  - Spy-ware – captures information from your computer and forwards it.
  - Ad-ware – triggers pop-up advertisements.
  - Hijacker – turns your computer into a slave or "zombie".

Other terminology

- Bot (short for Robot) – Software that can execute commands, reply to messages, or perform routine tasks, either automatically or with minimal human intervention.

- Cookies – Small, non-executable files containing information to customize or maintain your session with a specific website. Must be allowed to access many web sites.

- Dark Web – The "hidden" web, accessed only through special browsers and passwords. Private information is bought and sold on the dark web.

- Firewall – Software or hardware that hides the presence of a computer or network from others on the Internet until you choose to be seen.

- Human Engineering – Using psychology to trick a person into sharing things or doing things. Often this is behind both human and automated phishing.

- Phishing - Tricking or scaring you into taking action including sharing personal information. Could be interactive with a person or fully automated.

- Zombie – Computer which has been compromised and is now the slave of a remote computer and will do what it is told to do, when it is told to do it.

Practicing Safe Computing
Hal Bookbinder

Safe Computing Checklist

Anti-malware Management

- ✓ Maintain current commercial anti-malware software on your computer.
- ✓ If you must temporarily turn it off, turn it back on as soon as you are able to do so.
- ✓ Do not rune more than one anti-malware program on you system concurrently.
- ✓ Maintain a software or hardware firewall between your computer and the Internet.
- ✓ Set system to automatically download and install all security patches.

Back-ups

- ✓ Back up you operating system as a recovery disk.
- ✓ Regularly back up your data.
- ✓ Store your backup geographically separately from your computer.
- ✓ Protect your sensitive backed up data.

Cookie Management

- ✓ Routinely delete unneeded cookies.
- ✓ Set security at “medium” level. Then adjust as necessary.

Passwords

- ✓ Password protect your system, your router and sensitive files.
- ✓ Do not use the same password for your web access.
- ✓ Do not use passwords that can be easily guessed.
- ✓ Do not share your password with anyone, including technical support.
- ✓ Use complex passwords with a combination of letters, numbers and special characters.
- ✓ Periodically change your passwords.
- ✓ Obtain and use a password management tool.

Session Management

- ✓ Log off each application when you are finished. Don’t just close the window.
- ✓ Lock your computer when you are leaving the area.

Be Careful

- ✓ Don’t open suspicious emails or click on unknown links.
- ✓ Avoid questionable websites.
- ✓ Don’t respond to requests for personal information.
- ✓ Don’t insert unknown USB storage drives into your computer.
- ✓ Stay informed and promptly take appropriate action when issues arise.

Practicing Safe Computing
Hal Bookbinder

Be Proactive

Pay attention to alerts

- Pay attention to alerts about computer breaches and safe computing practices that appear in newspapers, in magazines and on broadcast media.
- Read my monthly articles at http://www.tinyurl.com/ComputingArticles. Following is a listing of all articles published to date:

2019 (through March)

- "Google Chrome Critical Error!"
- "5G, Fifth Generation Cellular
- "Ten Tips" (for safe computing)

2018 (through November)

- "Practicing Safe Tsedakah"
- "Facebook Tokens"
- "iPhone Tips"
- "Google Search Tips and Techniques"
- "Urgent Demand for Payment"
- "Best Anti-virus Protection of 2018"
- "Microsoft Word Tips & Tricks"
- "What is GEDCOM?"
- "Precautions while Traveling"
- "Meltdown and Spectre"
- "Password Managers, Again"

2017

- "Take care when you use Google"
- "What is the 'Dark Web'?"
- "Top 10 Tips for Detecting Phishing"
- "The Internet is forever"
- "Phishing email from your Bank"
- "Modems and Routers"
- "Verizon 2017 Data Breach Report"
- "Protection from WannaCry Ransomware"
- "Malware Protection"
- "Viruses, Worms, Trojan Horses, Spyware"
- "Searchable Government Databases"
- "Wireless Access"
- "Yahoo again, Biggest Hack Ever!!!"

2016

- "Verifying What You See"
- "Yahoo Email Services"
- "Password Managers"
- "Sharing Your Family Tree & Identity Theft"
- "Passwords"
- "Social Engineering"
- "Avoiding becoming victim of Ransomware"
- "Backing up your System"
- "Is it true that Apples are safer than PCs?"
- "What are 'cookies' and should they concern you?"
- "Is Your Virus Protection Actually Working?"

2015

- "A Free Scan of Your Computer"
- "Credit reporting agencies"
- "Don't help them steal your identity"