Practicing Safe Computing
Hal Bookbinder

Malware

Viruses, Worms, Spy-ware, Ad-ware and Trojan Horses are types of “malware” (malicious software) and all can create havoc with your computer.

- The primary difference between viruses and worms is how they travel. Viruses travel as passengers on a host, like an email. Worms are self-replicating and search you out, forwarding themselves to your computer without any action on your part.
- Once a virus or worm gets inside your computer, it can do a range of things, from simply annoying to highly destructive. This could include
  - Impacting your system’s performance by constantly running in the background and chewing up both computer cycles and memory.
  - Implanting ad-ware or spy-ware into your computer – more about these later.
  - Changing or replacing programs in your computer so that they don’t work the way intended or even don’t work at all. In extreme cases this may so impact your computer that it ceases to function.
  - Causing your computer to restart itself, over and over again. This might be triggered by something you do, by a timer, or at random intervals.
  - Corrupting or erasing the information on your disk.
  - Making your computer into a “zombie”, just waiting for instructions to participate in massive computer attacks.
  - Setting up your computer to forward email, and so becoming a spamming station.
- Spy-ware captures your keystrokes, your email contact list, your personal information or any other information on your disk and forwards this to an outside location, often in a foreign country. The recipient can then use the information to steal your money or even your identity.
- Ad-ware constantly runs and can slow down your computer. Its purpose is to display pop-up advertisements. When running on your computer, this is typically triggered by visiting certain web sites. Turning on your computer’s “pop-up blocker” will not stop the ad-ware from slowing down your computer, but will block the displays.
- Trojan horses appear to be harmless. But, while playing a tune or doing something else which appears to be harmless; they install other malware on your computer.
- So, what can you do to reduce your chances of being infected?
  - Have a current anti-virus and anti-spy-ware program on your computer.
  - Renew your subscriptions to continue getting the latest pattern files.
  - Don’t open suspicious emails. Turn off automatic previewing.
  - Set your computer to download the latest security patches from Microsoft.
  - Turn on your system’s internal firewall, or install another software or hardware firewall.
  - If you have wireless access at home password-protect your access and set it up with an ID that is not broadcast (and so visible by anyone).
  - Use passwords that are not easy to guess (like a month, weekday or a pet’s name), and don’t write them down. Periodically, change them – just in case they were compromised.
  - Regularly back up your data to media that you keep separate from your computer (over the Internet or on a portable disk).
  - Get a Macintosh (only half-joking…they are designed better to avoid viruses and spy-ware)

Cookies

Cookies are small files containing information about the sites that you visit on the Internet, what you do on these sites and data that you might enter, including IDs and passwords.

- ✓ Cookies are not inherently "bad," but can be used to personalize your Internet experience.
  - They can record the websites you visit and when you visit them.
  - They can record your ID and password and so automatically log you into websites.
  - They can record your choices within websites so as to personalize later visits.
  - They are intended to be written and read only by one website.
  - Many websites require that cookies be permitted.
- ✓ But, cookies can be used to spy on you.
  - They can be read by spy-ware that has been implanted on your computer and their contents automatically sent to an outside location.
  - They can be read by viruses and worms and the contents used to trigger annoying or even destructive activities on your computer.
- ✓ You can control cookies by not allowing them at all, removing them or ignoring them.
  - To block all cookies, do the following from within Internet Explorer: Click on "Tools," "Internet Options," and "Privacy." Move the sliding bar up all the way to "Block All Cookies." Click on "Apply."
    - Be aware that many websites will only permit you to visit or perform some functions if writing and reading cookies are permitted.
  - To remove the cookies on your machine, do the following from within Internet Explorer: Click on "Tools," "Delete Browsing History" and "Delete Cookies." Click on "Yes" when asked to confirm. Finally, click on "Close" to close the "Delete Browsing History" window. (These instructions are for IE 7.0. Other versions may work differently.)
    - Be aware that functions that were "automatic" when you revisit web sites may no longer be. Personalization might be lost and you may again have to enter your password on sites that did not previously require this.
    - Removing cookies will cause no harm. You can do it as frequently as you like.
  - Recommend you set your privacy options to "High" or "Medium High" to block many, potentially malicious, cookies.

Practicing Safe Computing
Hal Bookbinder

Phishing

Phishing is any activity that seeks to trick you into revealing personal information, over the Internet, on the phone, by mail, or in person.

- ✓ Most of us have received one or more of the following
  - A scary email ("There has been unusual activity on your Paypal account. Please click here immediately to verify activity or your account may be closed."),
  - One that promises instant riches ("You have been selected as a winner in the Spanish National Lottery. To claim your 7 million Euro winnings, please click here."), or
  - One that simply asks for your help ("We are doing a periodic verification of accounts at your branch of Bank of America. Please click here and answer a few simple questions to help us complete this audit.").
- ✓ Invariably, these are attempts to phish for your personal information which can then be used to steal your money or even your identity.

- ✓ When you do click on the link, you will typically be taken to an official-looking page which will ask you to log in to your account with your ID and password. When you comply you will receive a message like,
  - "We are sorry but the system is currently down for maintenance. Please try again later.", or
  - "Thank you, we have checked your account and everything is correct.", or simply
  - "Thank you for your assistance."
- ✓ Occasionally, you will now be asked for even more personal information ("It appears that your account has been compromised. You must immediately provide the information below or your account will be closed!")
- ✓ Be assured, however, that whatever information you provide is now in the hands of criminals in Russia, Nigeria, China or somewhere else far away.
- ✓ You have been phished!

- ✓ To avoid being phished online
  - Never respond to emails that request personal financial information.
  - Visit websites by typing the URL into the address bar and not by clicking on the email link.
  - Set your browser security settings or email settings to monitor for phishing.
  - Keep a regular check on your accounts.
  - Never click on a link offered in an email or pop-up unless you are sure of the desitination.

- ✓ If you forget and fall for the bait, do not ignore this an hope nothing bad will happen. Rather
  - Immediately contact your financial institution.
  - Contact the three major credit bureaus. Request a fraud alert be placed on your credit report.
    - Equifax, (800) 525-6285
    - Experian, (999) 397-3742
    - TransUnion, (800) 680-7289
  - File a complaint with the FTC at www.ftc.gov or (877) 382-4357.

- ✓ Banks will never ask you to verify your online banking username and password…and the likelihood of your winning the Spanish National Lottery is pretty much nil.

Practicing Safe Computing
Hal Bookbinder

Backing up your Computer

We all know that we should regularly back our computer. But, many of us do not do so until after the crisis hits and we have lost years of information, including results of our genealogical research. Set a goal of backing up your computer's hard disk(s) monthly and backing up critical or changing files (like your financial files or genealogical database) weekly. This can be done manually or automatically.

- ✓ Consider purchasing an external hard disk and copying your data files to it periodically. Then, store the hard disk separately from your computer so a disaster does not destroy them both.
- ✓ Also, consider separating the data files in your computer from the program files by putting them into a separate logical drive or directory. You can then just back up this drive or directory and not the program files.
- ✓ A convenient way to back up your critical files might be to copy them to a USB flash drive, or write them to a CD/ROM or to a DVD. Store the backups away from your computer.
- ✓ If you do not want to fuss with media, you could consider emailing critical files to a web mailbox, or "FTP'ing" them to a server on which you have space.
- ✓ If your computer has two internal physical (not logical) hard drives, you could periodically copy your date from one to the other. This will help if one of the disks "crashes," but won't do you much good if the entire computer is destroyed.
- ✓ Remember that aside from backups for dealing with disasters, they can be helpful if you simply need to restore a file you mistakenly deleted or changed.

This paper combines and expands upon several articles written by Hal Bookbinder and published between 2006 and 2008 in *Dates and Updates*, the newsletter of the JGS Los Angeles.