



# Antivirus Software Defrag & File Cleanup Computer Safety

October 17, 2006

Dodge County

4-H Tech Team

# Viruses and Worms

- The Internet is an invaluable resource. Unfortunately there are fools out there who use it to cause harm to your software and to your data. There are tens of thousands of [viruses](#), [Trojans](#) and [worms](#): the spawn of squandered talent. You need protection.
- If you haven't already, install antivirus software today!
- I recommend:
- for non-commercial use;
  - [AVG v7.0 Free Edition](#), or
  - [avast! Home Edition](#).
- The AVG programs are available at [www.grisoft.com](http://www.grisoft.com) or often on the free CDs which come with PC and Internet magazines.
- Commercial programs may be purchased via the Internet or at your local computer software dealer.

<http://www.mistywindow.com/security/virus-protection.htm>

# Effects of Computer Viruses

- Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk.
- Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user.
- They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

# Computer Trojan

- The Trojan horse is basically a malicious program accompanied by spyware which you get through email attachment, a messenger program, or from an internet download. Trojans sometimes masquerade as a free program you would like. Once you accept the Trojan into your computer, it will perform a basic installation of itself. Typically, trojans tend to do the following:
- Aid in hijacking your web-browser. This means that when you want to go to a particular homepage such as Google or MSN, you end up somewhere else.
- Record your keystrokes and transmit it to the attacker. This gives them access to any password protected accounts you have set up, including banking and other sensitive data.
- Do malicious functions such as rebooting your PC or deleting something.
- Allow the attacker access to your PC to run other code.
- Become a spam relay - sending vast amounts of spam to everyone else.
- The main difference between a computer virus and a computer trojan is that a Trojan does not try to replicate itself.

# Computer Worms

- A **computer worm** is a self-replicating computer program.
- It uses a network to send copies of itself to other systems and it may do so without any user intervention.
- Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

# Types of Computer Worms

- **Email Worms** Spread via email messages. Typically the worm will arrive as email, where the message body or attachment contains the worm code, but it may also link to code on an external website. Poor design[3] aside, most email systems requires the user to explicitly open an attachment to activate the worm, but "[social engineering](#)" can often successfully be used to encourage this; as the author of the "Anna Kournikova" worm set out to prove[4]. Once activated the worm will send itself out using either local email systems (e.g. MS Outlook services, Windows MAPI functions), or directly using [SMTP](#). The addresses it sends to are often harvested from the infected computers email system or files. Since Klez.E in 2002[5], worms using SMTP typically fake the sender's address, so recipients of email worms should assume that they are *not* sent by the person listed in the 'From' field of e-mail message (sender's address).
- **Instant Messaging Worms** The spreading used is via instant messaging applications by sending links to infected websites to everyone on the local contact list. The only difference between these and email worms is the way chosen to send the links.

# Types of Computer Worms

- **IRC Worms** Chat channels are the main target and the same infection/spreading method is used as above - sending infected files or links to infected websites. Infected file sending is less effective as the recipient needs to confirm receipt, save the file and open it before infection will take place.
- **File-sharing Networks Worms** Copies itself into a shared folder, most likely located on the local machine. The worm will place a copy of itself in a shared folder under a harmless name. Now the worm is ready for download via the P2P network and spreading of the infected file will continue.
- **Internet Worms** Those which target low level TCP/IP ports directly, rather than going via higher level protocols such as email or IRC. A classic example is "[Blaster](#)" which exploited a vulnerability in Microsoft's [RPC](#). An infected machine aggressively scans random [\[6\]](#) computers on both its local network [\[7\]](#) and the public internet attempting an exploit against port 135 which, if successful, spreads the worm to that machine.

# Phishing

- (fish´ing) (n.) The act of sending an [e-mail](#) to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for [identity theft](#). The e-mail directs the user to visit a [Web site](#) where they are asked to update personal information, such as passwords and credit card, social security, and [bank account](#) numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided [link](#) and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the [HTML code](#), the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to [update](#) their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately. Phishing, also referred to as *brand spoofing* or *carding*, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting

<http://www.webopedia.com/TERM/p/phishing.html>

# Ways to Avoid Phishing

- If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.
- Area codes can mislead. Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

# Avoid Phishing (cont.)

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

# Avoid Phishing (cont.)

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm>

# Spybot

- Spybot - Search & Destroy detects and removes spyware, a relatively new kind of threat not yet covered by common anti-virus applications. Spyware silently tracks your surfing behaviour to create a marketing profile for you that is transmitted without your knowledge to the compilers and sold to advertising companies. If you see new toolbars in your Internet Explorer that you haven't intentionally installed, if your browser crashes inexplicably, or if your home page has been "hijacked" (or changed without your knowledge), your computer is most probably infected with spyware. Even if you don't see the symptoms, your computer may be infected, because more and more spyware is emerging. Spybot-S&D is free, so there's no harm giving it a try to see if something has invaded your computer.

<http://www.safer-networking.org/en/spybotsd/index.html>

# Spyware

- In the field of computing, the term **spyware** refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

<http://en.wikipedia.org/wiki/Spyware>

# Adware

- **Adware** or **advertising-supported software** is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

<http://en.wikipedia.org/wiki/Adware>

# Adaware

- Ad-Aware Personal remains the most popular anti-spyware product for computer users around the world, with nearly one million downloads every week. Free anti-spyware version provides you with advanced protection against spyware that secretly attaches and takes control of your computer, resulting in aggressive advertising pop-ups, sluggish computer activity, even identify theft through stolen bank details, passwords, and credit card account numbers.

[http://www.lavasoftusa.com/products/ad-aware\\_se\\_personal.php](http://www.lavasoftusa.com/products/ad-aware_se_personal.php)

# Defrag

- Double-click My Computer
- Highlight a local hard disk drive by clicking on it once.
- Right click the highlighted local drive
- Click properties
- Click the tools tab and click the defragment now button.

<http://www.computerhope.com/software/defrag.htm#07>

# Disk Cleanup

- The Disk Cleanup tool helps you free up space on your hard disk by searching your disk for files that you can safely delete. You can choose to delete some or all of the files. Use Disk Cleanup to perform any of the following tasks to free up space on your hard disk:
  - Remove temporary Internet files.
  - Remove downloaded program files. For example, ActiveX controls and Java applets that are downloaded from the Internet.
  - Empty the Recycle Bin.
  - Remove Windows temporary files.
  - Remove optional Windows components that you are not using.
  - Remove installed programs that you no longer use.

# Start Disk Cleanup

- Click **Start**, and then click **Run**. In the **Open** box, type cleanmgr, and then click **OK**.  
  
-or-
- Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Cleanup**.  
  
-or-
- In Windows Explorer or My Computer, right-click the disk in which you want to free up space, click **Properties**, click the **General** tab, and then click **Disk Cleanup**.

<http://support.microsoft.com/kb/310312>

# Enforcing Household Internet Rules

- Kids who use MySpace, or the Internet in general, should be restricted to a few household rules regarding Internet usage. Putting these rules in place can be very helpful in reducing the potential for danger. Some of the general Internet rules parents might consider are:
- Do not post full name and address online or even school location. This will help to prevent stalking which could become a problem if online predators know where your child lives or go to school.
- Restrict Internet usage to specific hours during the day. This can prevent overuse of the Internet.
- Do not agree to meet online friends in person without consent. Ideally the parents should also accompany their children on these meetings and should ensure the meetings take place in a well lit, public location such as a coffee shop as opposed to a secluded spot such as an individual's home.

# More Internet Safety

- Do not respond to threats or harassment. Kids should be taught to ignore this type of behavior and report these instances to parents or the Internet service provider instead of responding to the threats. Responding to threats or harassing messages can exacerbate a potentially harmful situation.
- Internet usage should be restricted to high traffic locations in the house. For example kids should only be allowed to use the Internet in computers which are in locations such as the family room or kitchen as opposed to allowing kids Internet access in their bedrooms.

<http://ezinearticles.com/?Keeping-Kids-Safe-on-MySpace&id=316693>

# Choose a Good Password

- Choose a short, simple phrase, six to eight words, that will be easy for you to remember.  
I like to eat green peas.
- If any of the words are homonyms for other letters or symbols, write them with those symbols (e.g. are =r, you = u, two = 2)  
I like 2 eat green peas.
- Now, make an acronym. Drop all but the first letter of each word.  
Il2egp
- Capitalize arbitrarily, but with restraint, try to keep the password easy to remember.  
iL2eGp
- Add a punctuation mark or two to bring your password's length to seven or eight characters.  
iL2eGp!

<http://www.cae.wisc.edu/site/public/?title=passwrhlp>



# Computer Safety Quiz

- Q: Do you have anti-virus software installed on your computer to block email virus and worms?
- Q: Does your anti-virus software automatically update itself with current virus definitions?
- Q: Do you have a policy of never opening an email attachment even if it is from someone you know?



# Computer Safety Quiz (cont.)

Q: Do you use strong passwords -- those which contain a combination of at least eight alpha and numeric characters?

Q: Do you regularly back up your important files on a removable disk or other removable media?

Q: Do you have a software program installed that can detect and remove spyware?



# Computer Safety Quiz (cont.)

Q: Are you using the full capability of your browser's security and privacy features?

Q: Do you regularly delete cookies and remove temporary Internet files from your computer?

Q: Do you turn off software features that you do not use, such as instant messenger type services and file-sharing?

[http://crime.about.com/od/quiz/a/quiz\\_computer.htm](http://crime.about.com/od/quiz/a/quiz_computer.htm)



# Next Workshop

- Basics of MS Word  
and Keyboard Shortcuts

- October 24, 2006  
6:30-8:20 PM