

Winter 2002

The OLRC News

Tech Talk

Viruses, Viruses, and More Viruses

Kimberly S. McCoy & Marty Ropog



In recent years viruses such as Melissa, Code Red, SirCam and the "I Love You" virus, just to name a few, have been in the news because of their ability to spread at a rapid pace and affect

so many users in a short period of time. For example in March of 1999, the Melissa virus forced Microsoft and other major businesses to shut down their e-mail systems until the situation was handled. Also, in May of 2000, the "I Love You" virus reached at least 45 million users in one day and caused major corporations including Ford Motor Company to close down their e-mail systems for a period of time. Unfortunately, viruses will continue to be a part of our daily lives as society continues to utilize the many tools and resources available through computers. Hopefully, this guide will assist you in not becoming a virus victim and eliminating the possibility of giving or spreading one to your colleagues, friends, and family members.

What is a virus?

Whatis.com sited at <http://whatis.techtarget.com/> defines a virus as a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. Viruses can be transmitted as attachments to e-mail note, as downloads, or be present on a diskette or CD. The source of the e-mail note, downloaded file, or diskette you've received is often unaware of the virus." Viruses have the capabilities of corrupting and deleting files, causing a real nightmare for you and your computer system.

What is a worm? Webopedia available at <http://www.pcwebopaedia.com/TERM/v/virus.html> states "A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs." Unfortunately,

worms are usually intended to attach themselves to the e-mail addresses in your address book and may be programmed to go through a computer network. Melissa, "I Love You", Code Red and SirCam are all considered worms.

How do I protect my computer from viruses and worms?

There are a number of genuine computer viruses out there that have a range of different affects - from wiping out key files on your hard drive to doing absolutely nothing. Your best defense against these viruses and worms is a *regularly updated* virus scanner also referred to as an anti-virus program. Anti-virus programs allow users to search their computer for viruses and remove the infected file(s). A user can schedule these programs to scan/search on a daily, weekly or monthly basis. A user also has the option of setting up these programs to scan items downloaded from the Internet or attachments received via email and floppy diskette from others. If you regularly download items from the Internet and don't already have a download folder, create one. Then make a habit of saving all items downloaded from the Internet into the download folder and scan the folder prior to opening or executing the item you just downloaded. McAfee, accessible at <http://www.mcafee.com> and Norton Antivirus protection located at <http://www.symantec.com/>, are two of the most popular virus programs used. In addition to having one of these applications on your system, it's essential that the program and its virus definitions are current. Information on updating is available in the program's help files or on their Website. Both sites provide a comprehensive list of recent viruses, the date they were discovered, protection information, risk rating, how they may infect your system and removal instructions. Symantec Norton Antivirus page is available at <http://securityresponse.symantec.com/avcenter/vinfodb.html> and McAfee's resource is obtainable at <http://vil.nai.com/VIL/newly-discovered-viruses.asp>.

The second-best defense is to be wary of e-mail attachments, even if the attachments are from someone you

know and trust. Check a few things before you open any attachment:

- 1.) Does the language sound strange - grammar, spelling, and word choice inconsistent with the sender's usual messages?
- 2.) Is the message personalized or does it just start with "Hi!" or simply start a message (W32/Goner is the most recent example of this)?
- 3.) Is the attachment titled strangely, particularly from that person (For example, the I LOVE YOU virus)?
- 4.) Are you expecting an attachment from the sender? If not, contact the sender prior to opening the attachment.
- 5.) Is the extension (the last 3 letters of the filename) one of the following: .exe, .vbs, .bat, .scr? If you're not sure, check one of the sites referenced below for the filename.

Don't just use the subject of the e-mail to confirm validity. Several viruses sent out through email have genuine sounding subjects that may have come from messages in your own inbox.

Finally, get in the habit of backing up your files on a regular basis. In the event you do become a virus victim and your files are corrupted or erased at least you will have a clean and virus free backup. We recommend backing up your entire system once a week to a zip disk, a cd, or on your local network.

What is a Virus hoax?

A virus hoax is an e-mail about a virus that doesn't exist, unfortunately it only takes a minute to send out hoaxes to everyone in your e-mail address book. Always assume that virus "warnings" are hoaxes (most are) even if the message is from someone you know and trust. About.com has an excellent article about how to spot an email hoax available at http://www.urbanlegends.about.com/c/ht/00/07/How_Spot_Email_Hoax0962932962.htm. According to the article, a few things you should watch out for are wording such as "Forward to everyone you know," "This is not a hoax/urban legend," and the mentioning of a person or company in authority for instance, "AOL has confirmed that this is a real virus!"

Before forwarding or acting on any type of warning, please visit one of the following sites to confirm its validity:

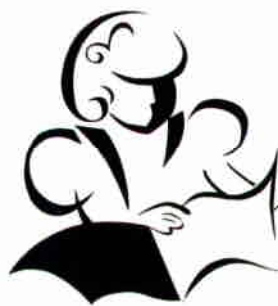
- a) Symantec Security Response <http://www.symantec.com/avcenter/>
- b) McAfee Avert Virus Alerts <http://www.mcafee2b.com/avert/virus-alerts/default.asp>
- c) Vmyths.com-Truth About Computer Virus Myths & Hoaxes <http://www.vmyths.com>
- d) Urban Legends Reference Pages: <http://www.snopes2.com/inboxer>
- e) HoaxBusters from CIAC through the U.S. Department of Energy <http://hoaxbusters.ciac.org/HBHoaxInfo.html>
- f) Virus Bulletin <http://www.virusbtn.com/index.html>
- g) Urban Legends and Folklore <http://urbanlegends.about.com/>

Lastly, "When in Doubt, Don't Send It Out"

Hoaxbusters <http://hoaxbusters.ciac.org/HBHoaxInfo.html>



Focus on Women and Literacy



The OLRC, with the help of Dr. Joanne Dowdy of Kent State University, is developing a webliography of women and literacy resources that contain useful information for instructors and students. This information includes websites, books, movies, and ERIC documents.

Daphne Greenberg of the University of Georgia will be overseeing a Women and Literacy Special Collection. The Special Collections are collections of high quality internet resources. If you haven't visited the Special Collections you can do so by going to <http://literacy.kent.edu> and clicking on the Collections button toward the top of the page.

New Showcase Items

*Integrating Technology into ESOL Curriculum:

<http://easternlincs.world.org/docs/cia/index.htm>

This site was developed for teachers who are interested in integrating technology into ESOL/EFL classrooms and promotes the use of technology in the field to bring more equitable access to knowledge, skills, and technology to learners.

*Charting a Course: Preliminary Needs Assessment Using Equipped for the Future:

<http://www.vcu.edu/aelweb/charting.PDF>

A collection of handouts and forms produced during an Equipped for the Future project for the Virginia Adult Learning Resource Center. Team members focused on orientation activities that require thought and input from the student. (Adobe Acrobat needed to view this document)

LINCS Tutorial

If you are new to the LINCS system, you may find this online introduction and tutorial of interest. <http://www.nwlincs.org/nwlincsweb/tut123.htm>