



Computer viruses originated along the same timeline as personal computers, both PC and Mac,* during the 1980s. Some viruses are relatively benign, though they may still waste your time; some wreak havoc on network bandwidth and storage capacity; and some of them are intentionally destructive. There are many actions you can take to protect your computer and files from what is referred to as malware: viruses, worms, and Trojan horses. Read on...

Viruses, Worms, & Trojan Horses

- **Viruses** - computer programs designed to replicate themselves and create problems. Some viruses may simply open a message window onscreen; others may corrupt or erase files, re-format hard drives, alter computer boot-up records, or load themselves into memory to continue their destructive behavior. Transported through e-mail and file-sharing.
- **Worms** - viruses that “live” in hard drives, replicate themselves, and have “payloads” that include deleting files, overloading networks, or rewriting source code which allows unauthorized access and often subsequent spamming. Transported through e-mail and file sharing.
- **Trojan horses** - malicious code or programs that do not replicate themselves, but can wipe out programs, erase hard drives, send e-mails to entire address books, or lie in wait until some pre-set time when thousands of computers then begin to run the program simultaneously, potentially having a negative affect on worldwide productivity. Disguise themselves as a valid program or file.
- **Virus hoaxes** - false warnings of viruses. Virus hoaxes, in addition to wasting time, diminish vigilance against real viruses.

Note: Spyware, tracking software designed to increase ad traffic on Web sites, is yet another form of computer “malware.” It is not illegal but can be extremely disruptive, hijacking browsers and slowing down computer operations. Ad-aware at www.lavasoftusa.com can help.

How “Malware” Spreads

- ◆ E-mail attachments (*even from people you know*)
- ◆ Software that has not been updated or “patched”
- ◆ Diskettes, CDs and other storage devices
- ◆ Games in disguise
- ◆ Downloaded software
- ◆ Internet Relay Chat
- ◆ Peer-to-peer networks

*Although viruses occur less frequently on Mac OS, it is advisable to take precautions to keep your system safe.

www.csus.edu/uccs/documents/quikrefsite



SACRAMENTO STATE

VIRUSES

Three levels of prevention

1. University:

- Provides a Sac State firewall that scans inbound e-mail servers for viruses, Trojan horses and worms.
- Installs anti-virus software on all University-owned computers, including those in the computer labs.

2. Individual computers:

McAfee VirusScan is licensed for use by all Sac State faculty, staff, and students for home and work computers. Download the software at <http://software.csus.edu/welcome.aspx>

3. Individual choices:

- Install anti-virus software on your personal computer.
- Update your anti-virus software regularly—configure it to automatically update, if possible. As new viruses spread, anti-virus software must be updated to defend against the new viruses.
- Update computer system weekly. Install critical updates and service packs as they become available. Restart computer after installing.
- DELETE E-MAIL ATTACHMENTS from senders you don’t know. SCAN ALL other e-mail attachments prior to opening them. Even a sender you know can have a virus.
- Be alert to unusual misspellings or use of terminology like “my friend” in e-mail subject lines and attachment names. If in doubt, delete the e-mail.

What to do

- Delete e-mail attachments from unknown sources.
- Save other attachments in a C:\Temp file. Right mouse click on file and select “Scan for Virus.” If no infected items are found, then the attachment can be safely opened.
- If you think you have a virus, worm or Trojan horse, turn off your computer and contact your department or college ITC listed at www.csus.edu/uccs/helpdesk/itc.htm or the University Help Desk at <http://www.csus.edu/uccs/helpdesk/> or telephone 278-7337.

Additional Protections

- Consider installing a firewall on your personal computer to scan for viruses, worms and Trojan horses.
- Enable Macro Virus Protection in Microsoft applications: Tools > Options > check Macro Virus Protection if your operating system is older than 2002. Newer systems default to this protection.
- Make back-up copies of your files regularly in the event your computer becomes infected, so you will not lose all of your materials if your hard drive is erased.

Learn more

- Sac State Campus-Wide Virus Alerts: <http://www.csus.edu/uccs/services/antivirus/virusalerts.stm>
- Sac State Virus Tools/Utilities: <http://www.csus.edu/uccs/services/antivirus/quickremove.stm>
- McAfee has a FreeScan service that will search for viruses on your system -- available at: <http://us.mcafee.com/root/mfs/default.asp>
- *Antivirus Research*: IBM Digital Immune System for Cyberspace at: www.research.ibm.com/antivirus