Avoiding the threat of computer viruses

Brendon Neal
Section Editor

Computer viruses can destroy months of student work and cost thousands of tax-payer dollars in software and hardware.

According to "Computer Viruses: An Introduction," a handout being given out by the Computer Lab to people with a virus on their home computers, there are a couple of misconceptions about viruses. A virus can't move from one type of computer to another, such as from an IBM-compatible to a Macintosh computer.

Viruses don't generate themselves; they are programs made by a person. However, they appear to come out of nowhere because they aren't intentionally copied to a disk.

The other wrong belief is that all viruses are harmful. Sometimes, although rarely, they just cause minor damage as a side effect of some other larger activity.

Viruses occur in open systems such as the ones at the college. Home users can also get viruses, especially if they use open systems as well.

There are, however, ways to lessen the chances of "catching" a virus and ways of minimizing damage if you do get one.

No one anti-virus program can find all viruses because they vary so greatly in design that there is no exact pattern that can be detected. However, many are variations of standard ones. Because thousands of new viruses come out every month, computer owners need to keep their anti-virus programs updated. Usually, companies or designers will have bulletin boards or phone numbers where updates can be downloaded or ordered for free or for a small fee.

Viruses are usually caught from pirated or non-copyrighted materials. A way to avoid viruses is to not download programs from bulletin boards. Either intentionally or not, customers of these boards can upload infected programs to the board. With the thousands of programs on the boards, it is nearly impossible for the people running them to keep track of all programs and check them for viruses. Often programs seem to accomplish what they are supposed to, and even well-known programs can be infected by the person that puts the program on the Bulletin Boards. Then when you put the program on your computer, your computer receives the virus along with the main program. Instead of getting them from boards, get software from the original author whenever possible. This way you can verify to some degree that the program doesn't have a virus and can know who put the virus on if there is one.

Making backups of your hard drive and diskettes is very important. Getting a tape drive for your computer allows you to back-up your drive whenever you wish without having to store dozens of diskettes. If you get a virus that damages all or part of your hard drive you can use the backups to retrieve the information that was on it as of the last backup. How often you should backup your computer depends upon how often you change/use your computer. Once a month is considered a good idea. This also protects against hardware failures that do occur.

Avoid using boot disks unless you have no hard drive. The common way viruses get put on a computer is from bootup disks.

Keep your disks write-protected (tab on back of disk in the upright position) except when you are copying information onto the disk. This way viruses can't be spread onto your disk from other disks or hard drives.

Another way to find out if your computer has a virus is to look for "strange behavior." If any of the following occurs, you should get your computer checked: take longer than normal to load programs, showing unusual error messages, memory size increasing or decreasing, disk lights staying on longer than they used to and files that disappear for no reason. Any of these can be signs of viruses.

continued from page 2

Questioning the government

Has the confusion in the Capitol clouded the minds of the people representing us, representing our country?

Our Federal government only shut down for a short period of time, but can we be sure that it won't happen again? The shutdown happened because the government fiscal year had ended and Congress hadn't yet approved spending plans for next year. In the past, Congress has passed a continuing resolution to pay the bills for a few weeks until the real budget had been worked out. But Congress and Clinton couldn't agree on even that because each saw the vote as a preview of the battle over the seven-year plan.

Why can't they make up their minds? We have voted people into position to represent us in decisions concerning our country, but Congress has been overwhelmed with making more money and has forgotten what they are there for in the first place.

The threat that our country can be shut down because Congress can't quit arguing, shows us that they have either taken upon themselves too many appropriations bills that need to be passed, or they don't have the most important thing on their minds - our country.

Mail-in ballots are due Dec. 1, for the primary elections to fill Packwood's seat. We must take it upon ourselves to keep our Congress in check. We should contact them and let them know what we think. Let's make it loud and clear what we want.

Drafting an Electronic Information Resource Policy

The following document is the college's Electronic Information Resource Policy draft as of Nov. 13 1995.

This isn't the final draft. The document has been going through a review process since April 1995. ASG, faculty, Classified Associaton, Instructional Council, Information Resource Committee and the President's Council are some of the groups that have been invited to participate in the review of the plan.

"This is an Electronic Information Resource Policy, not a policy to restrict the use of E-mail. E-mail is only one of many electronic information resources on campus" explained Paul Rothi, chief information officer.

"These groups are being invited to review this draft. The goal is to reach consensus that these are rules we as a college community agree to live by," Rothi said. When consensus is reached, and a final draft developed, it will be sent to the Board of Education for formal adoption.

TITLE: DRAFT ELECTRONIC INFORMATION RESOURCE POLICY Policy ~ (Draft #5, 11/13/95)

PURPOSE: This policy statement establishes measures for the protection, access, responsibility and acceptable use of Clackamas Community College's electronic information resources. The electronic information resources at CCC are to be used in a manner that supports the educational mission of the college. CCC by mission and policy encourages learning, research, creativity, teaching, and the free exchange of ideas in a climate of openness and sharing. Electronic information technologies are an important set of tools in this effort.

DEFINITIONS:
Electronic Information Resources (EIRs): all electronic hardware, software and associated data that support the following: administrative information systems, desktop computing, library automation, multi-media, data, video and voice networks, electronic mail (Email), Internet access, modems, scanners, telephone systems, voice mail, copy machines, fax machines, electronic publications including video, or any similar electronic based functionality.
User: any person authorized to use the college's electronic information resources
Authorized Accounts: Username/password pairs or similar codes or code devices such as copy cards that allow a person access to an EIR.

ACCEPTABLE USAGE:
In order to make possible the widest use of these important technologies a set of shared understandings and rules is necessary. In general the same ethical conduct that applies to the use of all college facilities applies to the use of electronic media. Users should show respect for college property, consideration of others, responsibility for actions, and authorized and efficient use of college resources. In addition, users of EIRs should have a basic understanding of the role of the law as regards copyright and other legal issues.

> ***"This is an Electronic Information Resource Policy, not a policy to restrict the use of E-mail"***

College EIRs must always be used in compliance with all international, federal, state, and local laws. EIRs are to be used through authorized accounts. Users must not share their authorized accounts with others in a manner that jeopardizes the security or integrity of the EIR. Users must not use college EIRs to make unauthorized entry to other EIRs inside or outside of the college. Users must respect the privacy of others by not inspecting, broadcasting, or modifying EIRs assigned to individuals without permission. CCC EIRs must be used for college related purposes and activities as defined by custom, contract and board policy, although occasional personal use is permitted. For example, an employee may do homework on personal time. The college cannot guarantee that messages or files are private or secure.
Mass electronic mailings and audix messages to the entire campus must have Dean approval. System management techniques should be used by all levels of college staff to ensure that: a) the integrity of information is preserved through access controls and data custodianship assignments; b) system capabilities can be reestablished within an appropriate time frame upon loss or damage by accident, malfunction, breach of security, or natural disaster; and c) actual or attempted breaches of security can be detected promptly. Network and system utilization activity will be monitored for purposes of maintaining system performance and security. All data should be treated as confidential unless designated or authorized for public release. Data will generally be shared among those users whose work can be done more effectively by knowledge of such information unless prohibited. Access to data is not approval for its use outside an individual's official college responsibility. No one shall deliberately attempt to degrade the performance of any EIR or block access to others. No one shall knowingly introduce invasive computer software such as viruses on media that is brought to the college from outside of the college. All data and software housed on college EIRs must be owned by or licensed to the college, comply with contract agreements between CCC and its employee associations, and comply with federal and international copyright law. Users shall be responsible for messages they transmit through the college s EIRs and shall obey the acceptable use policies of the Internet and any rules of discussion forums in which they participate. Fraudulent, harassing or obscene messages and/or materials as defined by contemporary court decisions are not to be sent or stored. Information that is published electronically using World Wide Web, Kiosks, Bulletin Board Systems, or similar electronic applications for broad general consumption outside of the college shall be subject to the same standards as conventional publications with respect to the representation of the college.

Failure to abide by this policy may result in temporary or permanent denial of access to CCC's EIRs. Punitive or legal action may also be taken by the appropriate administrative or judicial body in accordance with college policies and bargained agreements