

Special Report
of the
University Computer and Electronic Communications Committee

Avoiding Dangerous Software

March 22, 2005

Computer infections by viruses, trojans, and other malware have been a persistent problem on campus. Such infections can and do destroy valuable data and provide “backdoors” that permit unauthorized access to data on the local computer and on other computers with which it connects. They also needlessly consume scarce computer staff resources and waste end-user time needed to eradicate the infections and mitigate their effects.

Such computer infections are too often spread by means of application software that is inherently insecure and/or is a popular target. Among such applications are Internet Explorer, which can allow malicious programs to be downloaded and executed on the user’s computer, and Outlook Express, which may open attachments without explicit user intervention.

Safer alternatives to such especially vulnerable software are readily available, including the Firefox and Opera web browsers and the Thunderbird e-mail client.

Therefore the Committee recommends that:

1. All computer end-users should refrain from using such especially vulnerable software whenever possible, and should use safer alternatives instead.
2. All providers of computers on campus should install such safer alternatives on computers they manage, make access to that software easily visible, and inform and educate end-users as to these alternatives. Settings for each package should be defined to minimize the security risk (e.g., not using the Microsoft Viewer for e-mail in Eudora).
3. Directions and documentation for computer users to access campus resources should not require, and should discourage the use of, dangerous software and should suggest alternatives.
4. Computer administrators and users should be reminded to keep *all* software packages up-to-date.
5. Documents prepared for wide distribution, including web pages and e-mail messages, should be as platform-independent and standards-compliant as possible so that users will be able to make security-conscious choices about the software used for viewing them. For example, e-mail messages intended for a large number of recipients should be sent as plain text, rather than HTML.
6. The Office of Information Technology should promulgate this policy.