OAKLAND UNIVERSITY™

Thursday, September 4, 2003

Take steps to ensure desktop security

*By **Jeff Samoray**, OU Web Writer*

When it comes to keeping Oakland University's computer network and your own personal computer secure from viruses and other malicious attacks, there are a number of things individual users can do, many of which are quick and simple to perform.

"Users should focus on three areas: physical protection of your computer, network protection and operating system protection," said OU Security Systems Analyst Christopher Condie. "There are measures individual users can take to protect themselves as much as possible from viruses and other problems."

Physical Protection

Physical protection, or keeping your computer secure after you've logged on, is a seriously overlooked issue, perhaps because of the amount of media attention computer viruses have received of late.

"It's good to always ask yourself, 'What could happen if someone were able to access the data on my computer without my knowledge?'" Condie said. "The biggest threat is that someone else could use your machine while you're already logged on and begin accessing data or committing changes – all those functions will then be performed under your user name and ID. Remember that whatever access rights you have, others can also have them if they sit down at your computer while you're away."

Condie suggested that users perform two physical protective functions:

- Use an activated, locking screen saver to prevent casual access to your machine while you're away. Windows 2000 and XP and Mac OS X offer such screen savers in their operating systems.
- Don't share your machine with others not entitled to see the data on your computer. If more than one person must have access to your machine, set it up for multiple users and log out when you finish your work.

"The number one physical protection is the locking screen saver," Condie said. "It's also important to use common sense and be aware of those who use your machine."

Network Protection

Network protection involves installing anti-virus software on your computer and ensuring that the virus definitions are kept up-to-date.

"Anti-virus software, when properly used and installed, is the first line of defense against malicious activity that might be aimed at normal desktop machines," Condie said. "The Helpdesk can download Norton anti-virus software to your computer. After it's installed, we have a server on the network that can communicate with your computer and perform needed updates when you log on to the network domain. This software is meant to catch any type of virus known to Symantec (the manufacturer of Norton software)."

Some signs that may indicate your computer has been infected by a virus include:

- Your machine, though relatively new, is running very slow.
- Unusual activity such as programs closing without prompting.
- Unknown files become deposited on your computer.

"Those who don't keep their anti-virus definitions current are susceptible to bringing in viruses that the university is trying to protect the servers from," Condie said. "If you think you've been hit by a virus, contact the Helpdesk immediately because your computer may be in danger of infecting others. It's better to call us and be sure your computer is not infected than to not call at

all and be continuously infecting other machines."

Condie also suggests that users follow these guidelines to keep the network protected:

- Don't download shareware programs, MP3 sound or music files, video files, or anything whose source is unknown to you. Ask yourself, "Do I know where the attachment came from?" And, "Was I expecting it?" before opening a file that's been sent to you.

- Turn off your machine when you're not in the office or away from your desk for extended periods of time.

Operating System and Software Packages

Users also can defend themselves against viruses and other attacks by keeping their operating systems and software packages up-to-date.

"Most hackers take advantage of well-known operating system problems," Condie said. "The best thing to do is to check the Web site of your operating system, whether it be Windows, Mac or Linux, on a weekly basis for patches and updates for known vulnerabilities. Your computer is susceptible to any new vulnerability that has been exposed since you've last updated your operating system. If there are applications you use often, you should make sure to keep them up-to-date."

Condie also added that, though PC users have been more frequently attacked by hackers, Mac users should take the same precautions to ensure their computers remain secure.

For more information on desktop security and updates on anti-virus measures and the current state of the university computer system, visit the **University Technology Services** Web site. The UTS Web site also has a page devoted to **virus information**.

If you have questions on how to install a locking screen saver, whether your computer has up-to-date anti-virus software, or if you are experiencing a computer problem, contact the UTS Helpdesk at (248) 370-HELP (4357), e-mail **helpdesk@oakland.edu** or fax a detailed description of your request or problem marked "ATTENTION: HELPDESK" to (248) 370-4209.

SUMMARY
When it comes to keeping Oakland University's computer network and your own personal computer secure from viruses and other malicious attacks, there are a number of things individual users can do, many of which are quick and simple to perform. And while PC users have been more frequently attacked by hackers, Mac users should take the same precautions to ensure their computers remain secure.

Created by CareTech Administrator (webservices@caretechsolutions.com) on Thursday, September 4, 2003
Modified by CareTech Administrator (webservices@caretechsolutions.com) on Thursday, September 4, 2003
Article Start Date: Wednesday, November 19, 2003