OAKLAND UNIVERSITY

Tuesday, April 6, 2004

UTS curbing spam to keep OU computers, data safe

*By **Dawn Pauli**, contributing writer*

Weak Internet security is costing businesses more than lost time and data. An industry study estimates it costs organizations an average of $100,000 for recovery efforts after a negative cyber event, such as a virus.

To take a proactive approach to cyber security, **University Technology Services** (UTS) continues to reevaluate OU's networks and systems and add necessary security measures.

"We need to make sure the Oakland University networks and systems operate effectively and efficiently in support of communications, teaching and research," said Theresa Rowe, assistant vice president of UTS. "Our technology environment requires that desktop systems be well-maintained."

An important aspect of security is ensuring e-mail messages contain positive material that does not contaminate or slow down the environment. UTS is implementing changes to help curb the influx of unsolicited e-mail, also known as spam, from entering OU computers, while still preserving privacy and free speech.

"A flood of spam e-mail can be generated by viruses, and in recent weeks, network traffic has been slowed by such floods," Rowe said. "Spam also can be generated by mass-marketers and sharing material unrelated to university communications, education and research."

OU's e-mail system processes more than 200,000 e-mail messages a day.

"Just two years ago, when we selected our new e-mail system, that is the amount we processed in one week," Rowe said. "This increase has added extra strain on our network and e-mail systems, and it also is a burden to everyone on campus as each person has to deal with the extra unsolicited e-mail in inboxes each day."

This winter semester, UTS implemented new technology and practices to help keep the influx of viruses, unsolicited e-mail and invalid e-mail from entering university networks and systems.

The following is an overview of the actions UTS is taking and how they impact the way OU employees receive e-mail messages:

- **Antivirus Measures** — Messages that contain a virus are removed in most instances. If a message is received with a virus, it will be deleted. Most e-mail that contains a virus is spam or some kind of attack and does not usually contain a legitimate e-mail. UTS will not try to preserve the message.

- **Attachments** — Messages that contain specific file extensions known to be potential viral transport media will have the attachment stripped off and just the text of the message sent. Most viruses attack Windows-based computers and are included in files with the following extensions that will be deleted: .bat; .com; .exe; .inf; .pif; .reg; .wsh; .vbs; .zip; .scr.

  Employees still can share files, however, they need to take additional steps. The preferred method for transferring files is the Secure File Transfer Protocol (SFTP). Information about SFTP can be found on the **UTS** Web site. Click on Help Documentation in the left navigation, and then click on the appropriate document:

  - How Do I Use WinSCP for Secure FTP (Win)?
  - How Do I use Fugu for Secure FTP (Mac)?

  Another way to share files is create a private key and provide it to those who will receive the files:

1. Rename the file extension from .zip to a personal value that you choose, such as myfile. Use an extension value that is not on the delete list. Attach the myfile file in your e-mail.
2. In the e-mail text, let the recipient know the correct file extension.
3. The recipient receives the file and renames the file back to the correct extension.

- **Blocking Invalid Users** — Messages destined for an invalid OU e-mail address are immediately rejected. These messages are refused and an error code sent back to the sending host. This stops a "denial of service" attack on OU systems, where the university is flooded with e-mail sent to "**unknown@oakland.edu**" and the systems are overwhelmed trying to process the errors.

- **Blocking Known Offenders** — Messages sent from a list of known offenders, often called Realtime Blackhole List, are being rejected. This list is compiled and regularly updated by Spamhaus. The rejected sites are known repeat offenders of sending bulk spam, sending an excessive number of messages to e-mail servers, or are open relays of e-mail. By joining other universities using Spamhaus, OU does not have to read or evaluate the message. Decisions are made based on a collective decision.

- **Blocking Bad Servers** — Servers that are mis-configured, send too many connections, or are unresponsive to proper Internet protocols are blocked and the administrator is notified until the corrections can be made to their servers.

“These measures have helped create a more stable environment and control the costs and resources needed in providing the university with quality messaging services,” Rowe said. ”Desktop computers, and in particular those computers running the Windows operating system, are often targeted by virus-infected e-mail. We will do our best to update Windows computers that attach to the university network.”

A notice about the update may appear on a computer connected to the OU network. The system follows general rules that apply to most situations when doing the automatic update.

“We can't guarantee that all updates will occur in a timely way in all situations, on all desktops and laptops,” Rowe said. “It is good system management practice to still visit Windows Update. Also, we only push the critical updates. Microsoft offers additional patches and updates that may be of interest to various individuals.”

Rowe also reminds employees to make sure their home computer systems are updated.

“Visiting the site will verify the currency of your computing environment while protecting your computer and protecting the computing stability of your network neighbors as well,” she said.

SUMMARY
To take a proactive approach to cyber security, University Technology Services (UTS) continues to reevaluate OU’s networks and systems and add necessary security measures. UTS is implementing changes to help curb the influx of unsolicited e-mail, also known as spam, from entering OU computers, while still preserving privacy and free speech.

Created by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, April 6, 2004
Modified by CareTech Administrator (webservices@caretechsolutions.com) on Tuesday, April 6, 2004
Article Start Date: Tuesday, April 6, 2004