

LRC Temporary Move

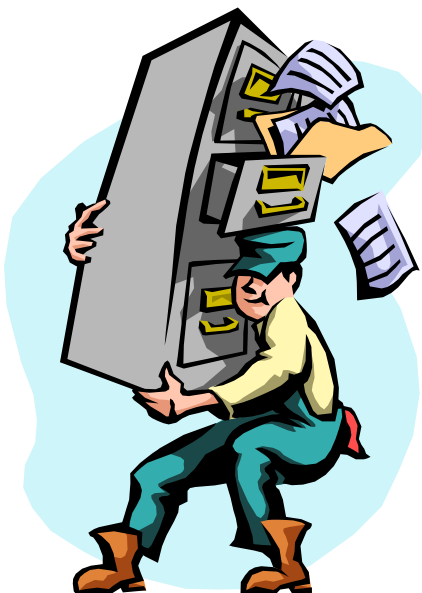
The existing library has reached the end of its first life cycle - it needs major renovation. The electrical, heating, ventilating, air conditioning, and lighting systems need attention. Simultaneously, the accelerating pace of technological change is mandating reconfiguration of the library resources. Likewise, the changing attitudes and lifestyles of our students demand a more socially engaging environment.

The library renovation project has started. One of the first steps will be to move the library to a temporary location, Building 7, 2nd floor. We realize this will be cramped quarters, but the move is necessary because of the large amount of dirt and dust expected during the reconstruction phase. Movement of some of the collection will commence during February as preparation for the relocation. The actual relocation will occur during Spring Break (March 21-25, 2005).

If all goes well, the renovated LRC should be operational in April, 2006. Additional communiqués will be provided in the College Bulletin and Know IT as progress is made.

If you have any questions, please contact Doug Kaylor, Director, Learning Resources Center, or myself.

Ken Moore



Exchange 2003 Implemented on January 22 and Office 2003 Being Implemented on January 31



Information Technology Services upgraded the Microsoft Exchange 2000 servers to Exchange 2003 on January 22.

The most immediate change as a result of this upgrade is to Outlook Web Access. It now has a similar look to the campus version of Outlook as well as some additional functions. **New instructions for using Outlook Web Access are found at:**
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/otlk/owa/owa.htm

In addition to the changes to Outlook Web Access, the Shared Secret has been eliminated and the Password Assistant has been replaced by other updated procedures. Links to the updated procedures and information are below:

Password Changes – instructions to show you how to change your password on and off campus
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/psswrld.htm

Getting Started with Your Network Account at Sinclair Community College – document to be given to all new employees to help them get started with their network accounts
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/gettingstarted.htm

Welcome to Your Network Account at Sinclair Community College – information about user accounts and their services associated with them.
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/welnetaccts.htm

ITS will automatically install Office 2003 campus-wide on January 31. ITS is upgrading to Office 2003 which includes the latest version of Outlook, the client for Exchange, to enhance the

stability and functionality of email and calendar services. This upgrade will allow users to take the best advantage of the enhancements associated with the upgrade to Exchange 2003.

Office 2003 is now a part of the administrative workstation image so all new or re-imaged computers will receive this version of Office. Office 2003 is also available now for individual installation on all existing imaged computers. Installation instructions are included below. If you choose not to install the software now yourself, **it will be installed automatically by ITS on January 31. It is strongly recommended that users install the software themselves now so that they can control when it is installed.**

Office 2003 installation instructions are found at:
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/its/instoff2003.pdf.

NOTE: Office 2003 will be installed in campus labs at the request of each lab's manager.

NOTE that installing Office 2003 yourself or through the automatic process will remove ALL previous versions of Office software from your PC. If you have compatibility concerns with data created with older versions of Office software, please contact the IT Help Desk at 512-HELP (4357) or at helpdesk@sinclair.edu before the mandatory installation of Office 2003 Winter Quarter.

Additional information about the Exchange 2003 and Office 2003 upgrades can be found at:
http://our.sinclair.edu/sites/its/itswebsite/it_policies/nessie/nessie.htm.

For additional questions, contact the IT Help Desk at 512-HELP (4357) or at helpdesk@sinclair.edu.

Cheryl Stewart

Sinclair Network Security

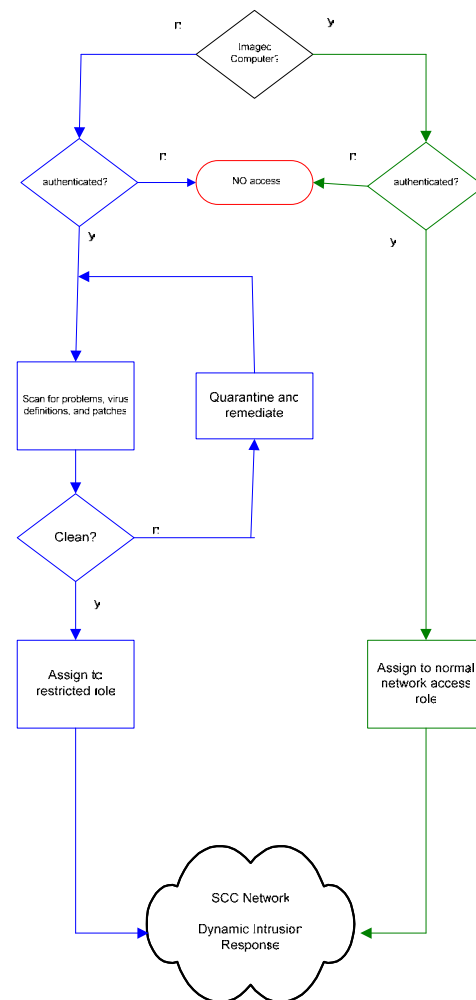
The Information Technology Services (ITS) team is responsible for maintaining a high-performance, manageable, and scalable IT system that facilitates a balance between a secure and collaborative environment for the college’s students, faculty, and staff. ITS has worked hard researching, testing, and implementing technologies that address specific issues for the college network. Examples of these technologies include virus protection, firewalls, spam filtering, intrusion detection/prevention systems, and software updating/patching systems. However, the College faces some complex challenges in achieving a truly secure network.

These challenges are due to the fact that a network connection is typically a wide-open “pipe” that connects all computers together. While access to server-based resources can be limited based on a user ID/password authentication, there is nothing to prevent an unauthorized user from connecting a device to the network without authenticating to a server. The growth in wireless networking and the need to provide protection from the introduction of unauthorized wired and wireless computing devices as well as the need to protect the network from the proliferation of network-borne viruses and worms caused the ITS team to undergo the development of a comprehensive plan for a Secure network.

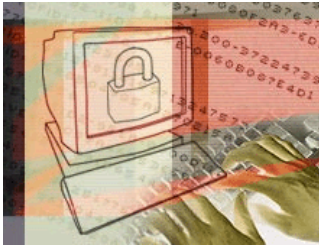
This plan, which was completed in October 2004, provides a roadmap for the implementation of network authentication for all computers that connect to the Sinclair network; controlled access for unknown devices; and the isolation and remediation of problems with un-patched or virus-infected PCs. The plan defines a clear path towards the vision of a network where access to network resources is based on the role of the user, the configuration of the computing device they are using, and the verifiability that the device is problem free.

The plan’s implementation began in December 2004 with the definition of the various roles that users and devices can be authenticated into. The

second phase, Dynamic Intrusion Response, will start in February and will deal with the constant monitoring of network traffic for abnormalities and the isolation of the offending computer. Additional phases will be completed during the next 6 to 9 months. When the plan has been fully implemented, there will be no ability for a computer to communicate on the Sinclair network without the user of the device passing an authentication process. Also, the plan will provide for different levels of access based on whether the device is a Sinclair-imaged computer or a device with an unknown configuration. Further information on this project will be provided as we implement the remaining phases.



Scott McCollum



Information Security Corner

Email 'Chain Letters' Identifying Hoaxes and Urban Legends

Do you know anyone who is waiting for a \$1000 check from Bill Gates or Microsoft, as a reward for 'beta-testing' email tracking software by forwarding an email to everyone in their address book?

Have you been solicited to provide a complete stranger (often from Nigeria) "ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THESE TRAPPED FUNDS, US\$21,320,000.00 (TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS)"?

Ever received a warning like "This information arrived this morning, from Microsoft and Norton. Please send it to everybody you know who accesses the Internet" or been urged "WE NEED TO DO EVERYTHING POSSIBLE TO STOP THIS VIRUS"?

Email messages with contents such as these are familiar to nearly everyone who has an email account. Some are sent by strangers, others by (usually) well-intentioned friends or family members. Regardless of content or source, email 'chain letters' are potential problems. These problems range from being a potential annoyance, through being the vector for malicious virus or worm attacks, to resulting in significant damage due to fraud or criminal activity.

When you receive a chain-letter message, and 'pass it on', you should be aware of and consider the implications of doing so. Even the most harmless, funny, cute, or inspirational chain messages:

- use network/Internet bandwidth during transport.
- consume storage space on mail servers and inboxes (picture and music files in particular can be very large).
- require the recipient to take the time to open and at least screen the content for value.
- may offend and/or annoy some recipients

This doesn't mean you shouldn't share these type messages to people you know would enjoy/benefit from them, but you should definitely consider to

whom (and to where) you are sending the messages; it is highly unlikely everyone in your address book needs or wants to receive them.

Some messages should *not* be forwarded—hoaxes and 'urban legends.'

Hoaxes and 'urban legends' both attempt to trick or defraud users. The three previous examples are examples of common ones. A hoax message is often intentionally malicious, such as instructing the recipient to delete a file necessary to the operating system by claiming it is a virus. Intentionally malicious hoaxes also include scams attempting to convince recipients to send money or personal information - [phishing](#) messages are malicious hoaxes.

'Urban legends' are hoaxes that are not overtly malicious but try to convince the recipient of an unlikely event or to take some unnecessary action, nearly always instructing the recipient to 'send to as many others as possible'. Common topics of urban legends include dire warnings about new and devastating viruses (and the A-V vendors don't know about them!), free money offers, reports of

Continued on Page 5

Continued from Page 4

children in trouble, and requests for boycott of a product or company due to a rumored policy or action. Urban legends generally have few tangible negative effects (other than the resource issues above), but do result in significant lost time as people sift through and attempt to verify information, and they result in the spreading of hype, fear, and paranoia.

How can you recognize a hoax or urban legend message?

Some messages are more suspicious than others, but ‘warning flags’ should activate if a message has many of these characteristics:

- there is a statement urging you to forward the message.
- it has already been forwarded multiple times (evident from the trail of email headers or multiple <FW>).
- it claims it's not a hoax.
- it suggests tragic consequences for not performing some action (including sending it on!).
- it promises money, gift certificates, or other reward for performing some action (especially passing it on!).
- there are multiple spelling or grammatical errors, or the logic is suspect or contradictory.
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software (NEVER follow the instructions or open the attachment...you will likely be infecting yourself!).

It looks like it might be legitimate...how do I know if it's not?

If you want to check the validity of an email, there are many web sites that provide information about hoaxes and urban legends. Some of the most popular are:

- Urban Legends and Folklore - <http://urbanlegends.about.com/>

- Urban Legends Reference Pages - <http://www.snopes.com/>
- Hoaxbusters - <http://hoaxbusters.ciac.org/>
- TruthOrFiction.com - <http://www.truthorfiction.com/>

What should I do when I receive a hoax or urban legend message?

The most important thing you can do is actually a ‘not do’ - **do not** forward the message or follow its instructions!

If the message is a confirmed urban legend or other non-malicious hoax, simply **delete** the message. If you know the message sender well (particularly if the sender is an email or Internet novice), you may wish to help teach them about email chain letters - *individually and privately* (feel free to send them this article if you think it will help). In most cases, sending a follow-up ‘this is a hoax’ message to all original recipients is not effective or desirable. If the message is a ‘warning’ about a virus or other malicious code, validate it via a reliable source before taking any action. If you can’t validate the information, it is very likely a hoax - information security organizations and vendors rapidly publish information on known exploits. Reliable sources include your organization’s information security office, anti-virus vendors’ web sites, information security specific sites such as CERT, CIAC, or SANS. Links to some reliable sites are:

- A-V Vendor Symantec (Norton)- <http://www.symantec.com/>
- A-V Vendor McAfee - <http://www.mcafee.com/>
- A-V Vendor Sophos – <http://www.sophos.com>
- Microsoft- <http://www.microsoft.com/security>
- CIAC- <http://www.ciac.org>
- CER- <http://www.cert.org>
- SANS- <http://www.sans.org>

Dan O’Callaghan
Chief Information Security Officer

Duplicating Keys of State College's and Universities

Did you know you would be guilty of breaking the law for duplicating college keys?

The OAC section 3345.13 states that,

“ No person shall knowingly make or cause to be made any key for any building, laboratory, facility, or room of any college or university which is supported wholly or in part by the State of Ohio, contrary to any regulation respecting duplication of keys adopted by the board of trustees of such college or university.”

The OAC section 3345.99 also covers penalties for such activities as follows,

“(A) Whoever violates section 3345.13 of the Revised Code shall be fined not less than fifty nor more than one hundred fifty dollars.”

That is pretty simple to understand. We have been very fortunate here at Sinclair Community College and have experienced very few incidents of this nature. Please ensure this information is distributed throughout your departments. If you have any questions please contact me at extension 4529.



Woody Woodruff



Open Labs Conduct Survey

In an effort to better serve the needs of our students, Information Technology Services (ITS) created a survey targeting the Academic Open Labs. The survey was designed to gather information regarding students' use of technology and support in the Open Computer Lab spaces at Sinclair.

The survey was conducted in the Open Labs by the departmental Lab Coordinators. ITS and the other campus departments will use the results of this survey to make informed decisions regarding Open Lab issues.

The Survey covers a wide variety of issues. The areas of greatest interest to ITS were:

- **Satisfaction:** Student satisfaction with service such as support staff availability and knowledge.
- **Computer Labs:** Student satisfaction with software availability, hardware reliability and environment.
- **Technical Support:** Nature of problems experienced by students, and the quality of help received from lab support staff.
- **Computer Ownership:** Details regarding

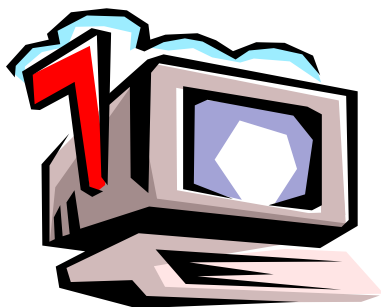
students' home computer ownership and needs in Open Labs.

- **Needs Assessment:** Importance of floppy disk, zip disk, jump drives and other devices needed to transfer files from home to campus computers
- **Printing Needs:** Student printing needs including printer usage and average number of pages printed per quarter.

Each Open Lab constructs its service plan around the function and/or department that it serves. This kind of planning can lead to poor customer experiences. The first step in revising this process is to view the lab from the students' perspectives.

Open Labs are striving to move from good support to great support by ensuring that issues are taken care of before the student ever notices that they exist and by elevating our skills to become experts to support not only the lab environment, but Sinclair Community College as a whole. This will be particularly important as Sinclair continues to grow and additional support is needed both on the main campus as well as off campus sites.

Jeanna Reedy



Hints from the Help Desk

Infolink PC Instructions & Information



The Infolink PCs are computers equipped with a PC, a monitor, a VCR, and a wireless keyboard and mouse. They are located in small rooms in Building 14.

The Infolink PC Room Numbers are listed below:

- 14-105** - Classroom, Booked by Registration through R25
- 14-116** - Classroom, Booked by Registration through R25
- 14-304** - General Conf Room for faculty, staff, and students, Booked through Outlook
- 14-305** - General Conf Room for faculty, staff, and students, Booked through Outlook
- 14-313** - General Conf Room for faculty, staff, and students, Booked through Outlook
- 14-314** - General Conf Room for faculty, staff, and students, Booked through Outlook

Some acceptable uses of the Infolink PCs include:

The rooms, when scheduled through the appropriate person, may be used as a classroom, a meeting room, a breakout room for classes, a student group study room (faculty must book for students), a place for internet access for class, or a place for watching a class-required VHS tape.

An informational page about the Infolink PCs is found at:

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/infolk/infolk.htm.

Instructions on using the Infolink PCs is found at: http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/infolk/infolk.pdf

For general assistance in using the Infolink PCs or to report problems, contact the IT Help Desk at 512-HELP (4357) or at helpdesk@sinclair.edu.

Infolink PC training is available from the Instructional Development Support Department. Training hours are 8:00 AM to 6:00 PM Monday through Friday. To schedule an appointment, call (937)512-4526.

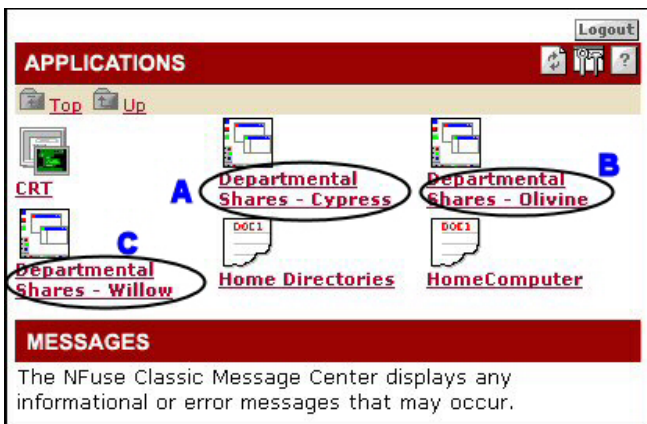


Off-Campus File Access Application (Citrix) Screen is being Changed

Changes are being made to the CRT application screen. Users will no longer have to click on a generic Departmental Shares link and then navigate to the server on which a share resides.



Currently users will see the screen below when accessing the CRT application:



There is a Departmental Shares link for each server on which departmental shares reside:

- A. Cypress
- B. Olivine
- C. Willow

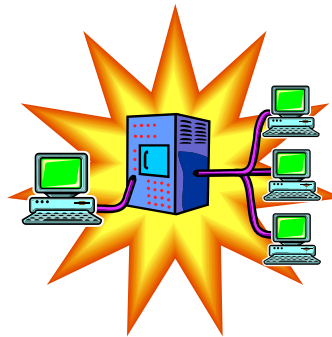
Click on the link for the server on which the departmental share you want to access resides.

Complete instructions on using the CRT application can be found at:

http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/Citrix3/CitrixInstructions.htm

For additional information or questions, contact the IT Help Desk at 512-HELP (4357) or at help-desk@sinclair.edu.

Cheryl Stewart



.....

Food For Thought.....

We are what we repeatedly do, excellence then is not an act, but a habit.

~Aristotle~





Chief Information Security Officer Dan O'Callaghan



As Chief Information Security Officer, Dan O'Callaghan is in charge of providing an efficient and effective information security program to protect the networking, computing and communications infrastructure and to minimize the risks to Sinclair Community College technology investments and the information contained within the college's information technology resources.

In order to accomplish this goal Dan has developed a comprehensive formal security program which includes a documented tactical plan to meet security goals; maintaining, implementing, and evaluating information security policies, practices, standards and procedures; developing and executing effective security awareness programs to educate the user community; defining and documenting levels of violations of security and required responses; and developing a Computer Security Incident Response Team (CSIRT).

Dan is also a regular contributor to the Know IT Newsletter with his *Information Security Corner* in which he addresses current security issues that affect Sinclair employees and students both in the workplace as well as off-campus. Be sure to check out his article in this issue regarding *Email 'Chain Letters' - Identifying Hoaxes and Urban Legends*.