

Security! Security! Security!

Why do we keep badgering you about security? Because we cannot over-emphasize the importance of computer security. Spam, spyware, phishing, bots, are everywhere (see Information Security Corner by Dan O'Callaghan on Page 4). Computer hacking is no longer just a game; it has become a multi-billion dollar industry - and it's costing most organizations large amounts of dollars and time to secure their technology resources. But, these expenditures are not enough. Every user must participate. Every user must learn and practice the "Dos and Don'ts" of secure computer and network utilization. We all must work together to provide a satisfactory experience while maintaining a secure environment.

Ken Moore

.....

Exchange/Office 2003 Upgrade Survey Now Being Conducted by Information Technology Services



Information Technology Services is seeking feedback from Sinclair users on the recent Exchange/Office 2003 upgrade. Please help ITS serve campus users better by completing the attached Exchange/Office 2003 survey.

Answering the survey questions will only take a few minutes and will assist ITS in planning and implementing future projects.

To complete the survey, click on the link below:

http://our.sinclair.edu/sites/its/survey/off2003_survey.cfm

Cheryl Stewart

Colleague Web Reports

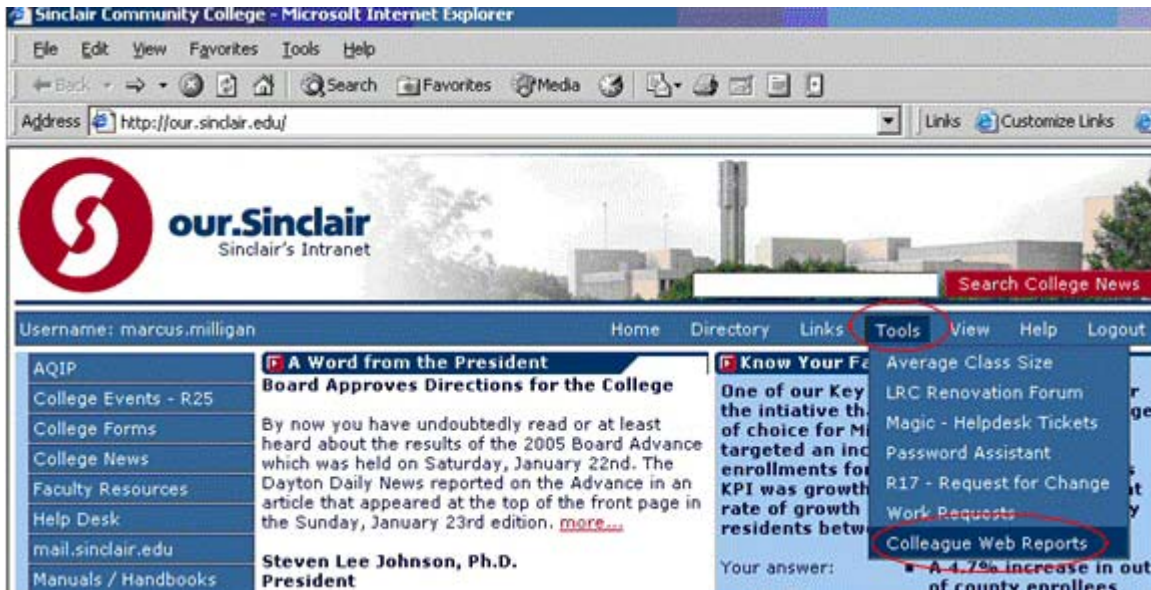
Administrative Systems in cooperation with Web Systems has developed **Colleague Web Reports** to allow faculty and staff to execute live reports from the Colleague system.

you are also encouraged to send report suggestions to marcus.milligan@sinclair.edu.

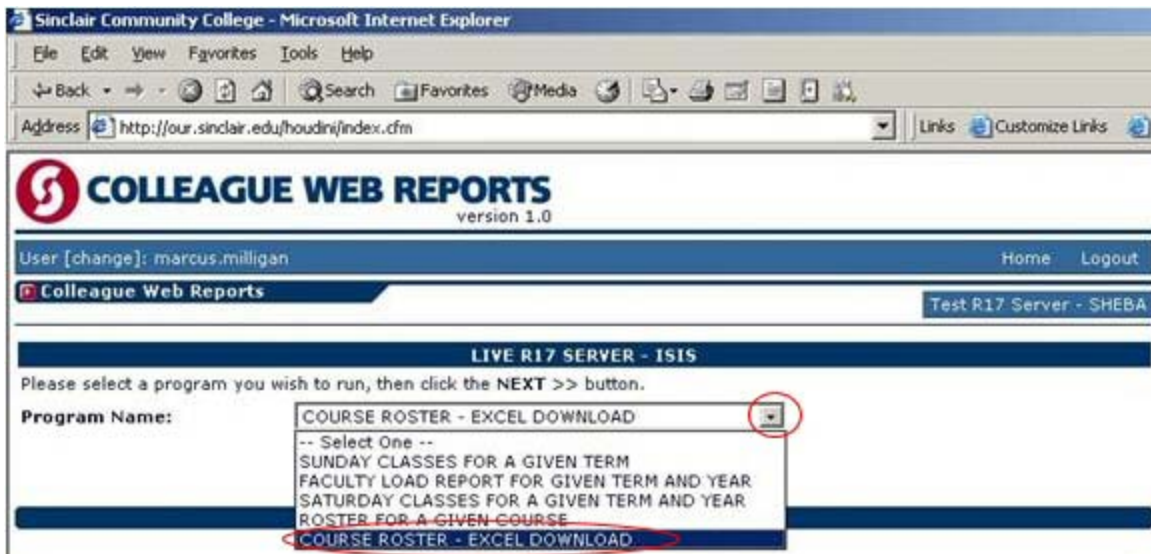
NOTE: Only those users with a Colleague account will have access to Colleague Web Reports.

Over time more reports will be added to the menu,

To access Colleague Web Reports, go to <http://our.sinclair.edu>, click on **Tools** and select **Colleague Web Reports**.



Click on the **drop-down arrow** and select one of the available reports.



Continued from Page 2

Enter the information required for the selected report and click on **Submit**.

The screenshot shows the 'COLLEAGUE WEB REPORTS' interface in a Microsoft Internet Explorer browser. The address bar shows 'http://our.sinclair.edu/houdini/dspInput.cfm'. The user is logged in as 'marcus.milligan'. The page title is 'LIVE R17 SERVER - ISIS'. The program name is 'COURSE ROSTER - EXCEL DOWNLOAD' and the description is 'Course Roster with Excel download'. Below this is a table with three columns: 'Parameters Required', 'Sample Parameters', and 'Input Parameters'. The 'Input Parameters' column contains four text input fields with the values '04/SP', 'AVT', '297', and '50'. Below the table are 'Reset' and 'Submit' buttons. The 'Submit' button is circled in red.

Parameters Required	Sample Parameters	Input Parameters
Enter Term	03/FA	04/SP
Enter Subject	ENG	AVT
Enter Course Number	111	297
Enter Section Number	01	50

The report is displayed as seen below. You can print it by clicking on the **Print Report** button or download it by clicking on the **Download** button at the top right to get the Microsoft Excel version.

The screenshot shows the 'COLLEAGUE WEB REPORTS' interface displaying the 'Course Roster Report'. The address bar shows 'http://our.sinclair.edu/houdini/actObject.cfm'. The user is logged in as 'marcus.milligan'. The page title is 'LIVE R17 SERVER - ISIS'. At the top right, there are 'Print Report' and 'Download Excel Report' buttons, both circled in red. The report content is as follows:

Course Roster Report

Student:	██████████
Tartan ID:	██████████
Home Phone Number:	██████████-██████████
Business Phone Number:	██████████
Grade:	██████████



Information Security Corner

Spyware – What it is, Why it’s a threat, and How to protect yourself from it.

Does your PC seem to be getting sluggish? Are you seeing an increase in pop-up ads, maybe even when you aren’t using the Internet? Has your home page been changed, and does it resist letting you reset it? Do you have toolbars in your browser that you didn’t install? Are they difficult to turn off or hide? Are you getting strange or unexpected results when searching the Internet? If any of this is happening to you, your computer is very likely infected with spyware!

What is spyware?

Spyware is a generic—and controversial—term for software that collects information about you and transmits this information to its “home” vendor—often covertly. Some of this software (called *adware*) may be relatively harmless or even marginally beneficial as it simply tracks your Internet use habits to deliver targeted advertising; this allows some Web sites to remain free of charge. However, much of this software is more invasive and borders on illegal, capable of capturing personal, financial, and security (PINs & passwords) information, and transmitting this ‘home’ without the user’s knowledge or consent (this is truly *spyware*). Some spyware actually redirects all of the user’s Internet traffic through their ‘proxy’ server and captures every site visited and every action taken. The vast majority of these software applications fall in the middle-ground between adware and spyware, but a growing threat is illicit spyware applications that capture every keystroke, cause damage, abet identity theft, and/or hijack systems to turn them into spam ‘bots’ (robots). Regardless of what the vendor calls it, the technology that powers adware and spyware is the same, and the end-user has little or

no knowledge or control over specifically what information is being collected. From an information security perspective, this technology is all considered spyware.

How does a computer get infected with spyware?

Most spyware applications are ‘bundled’ with free software programs downloaded from the Internet. The ‘free’ weather alert, screensaver, clock synchronizer, game, or toolbar downloaded and installed also installs software that gathers information and reports to the sponsor. This is generally disclosed in the End User License Agreement (EULA)—the window with the ‘I Agree’ button that appears during installation—but is often buried in the fine print or is full of technical jargon the average user doesn’t understand. Specific details of what information is collected and how it is used are seldom found in the EULA.

Some of the illicit, most invasive, and dangerous spyware applications are installed via worms, viruses, and/or other exploits, but many are also increasingly installed when a user simply visits a Web site or clicks a pop-up advertisement (called ‘drive-by’ installation). Some unscrupulous individuals register Web addresses with names of popular products or legitimate sites; when a user lands on one of these pages, spyware is automatically installed. Pop-up windows are also used to install spyware *Surf faster, accelerate your Internet connection!* is a common one. Ironically, many have enticing security related messages such as *Free email virus scanning software*, and even

Continued on Page 5

Continued from Page 4

Your computer may be infected with spyware-Scan Now! Users who click the pop-up or install the software advertised are then infected with spyware.

Why is spyware a threat?

By design, spyware unobtrusively collects information from the user's computer and transmits it to another computer. Even if the user has consciously accepted the EULA and understands that information is collected, the user has little or no ability to see or control exactly what information is being collected and sent, who is receiving it, and how it is being used. If data such as credit card numbers, bank account information, or passwords is harvested, even unintentionally, it is transmitted to the collecting computer.

Spyware technology can also do much more than simply harvest information. Because they are executable programs, spyware applications can be written to perform the same tasks as any other software programs. They may be written to create, modify, and access information stored on the hard drive, can snoop on other applications (such as email, word processing, financial management, messaging, and chat), can change what programs launch when your computer is turned on, hijack your Internet homepage (and resist changing it back!), and can even collect and transmit every keystroke. Even if the application does not initially do anything 'harmful' when installed, it is susceptible to hacking and other attacks that can provide an intruder full control of the infected system. Because of the powerful abilities of spyware technology, it is rapidly becoming the tool of choice for criminals and other malicious individuals. Fraudsters such as 'phishers' are abandoning direct requests for personal information via email, and are instead using apparently benign messages to install spyware such as key-loggers, Trojan horses, and other malicious spyware applications.

What can I do to reduce the likelihood of being infected with spyware?

One of the easiest and most effective ways to reduce the likelihood and severity of spyware

infestations is to follow good basic security practices.

- Carefully read the EULA before installing any software, and particularly 'free' software downloaded from the Internet. Look closely for 'additional' (bundled) software that installs with the main program.
- Don't click in/on advertising pop-up windows or boxes that appear when browsing.
 - to close them, right-click its button on the task bar and left-click 'Close'
 - persistent windows can be closed by pressing the Alt and F4 keys simultaneously
- Don't click 'Yes' when unexpectedly prompted to run or install software or plug-ins.
- Don't click on any link in, or reply to any spam (unsolicited email) message—particularly those that claim to scan your PC for viruses or spyware.
- Adjust Internet Explorer security settings. Microsoft recommends security settings for the Internet zone of 'Medium' or higher. See Working with Internet Explorer Security Settings (<http://www.microsoft.com/windows/ie/using/howto/security/settings.msp>)
- Use antivirus software, and update the virus definitions frequently (preferably daily)
- Use an Internet Firewall
- Keep your PC updated with the latest patches (Windows Update)
- Use an Anti-Spyware tool to regularly scan and clean your computer.

Home users, see 'Protect Your Home PC - for Free' for basic information security tips and tools. (http://www.sinclair.edu/departments/infosec/pub/SATE_brochure_Protect_your_home_PC_Feb05.pdf)

How can I detect and remove spyware?

As a minimum, users should occasionally scan their systems to ensure they know if any spyware programs are running, and should also eliminate any unwanted spyware. An effective, proven free anti-spyware tool is Ad-Aware SE, available from: <http://www.lavasoftusa.com/>. Another good

Continued on Page 6

Continued from Page 5

spyware detector is **SpyBot S&D** (Search & Destroy) available from: <http://www.safer-networking.org>. Be very careful to type the URL (Web Address) exactly as listed above because some unscrupulous companies actually use very similar addresses to trick the unsuspecting into *installing* spyware instead of the spyware removers!

Microsoft is also developing a free antispyware tool. As of this publication date, this software is 'beta' (test mode). If you are comfortable testing software, the URL is: <http://www.microsoft.com/athome/security/spyware/default.mspix>

Dan O'Callaghan
Chief Information Security Officer

Accurate as of March 2005

.....

Updated McAfee VirusScan Software Now Available at the LRC

To assist users with protection against viruses, Information Technology Services makes McAfee virus detection and disinfection software available to Sinclair users for home use. **An updated version of the McAfee software, version 8.0i, for Windows systems NT, 2000, and XP is now available at the LRC.**

McAfee VirusScan software CDs are available for checkout in the LRC.

NOTE: Two versions of the software are included on the CDs. Windows 95, 98, and ME users should install version 4.5.1. Windows NT, 2000, and XP users should install version 8.0i. Documentation and installation instructions are also included on the CDs. Installation instructions are also available at:
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/mcafee/mcafee.htm

A Tartan card is needed to check out the CDs. The CDs may then be taken home and installed on a home PC. The CDs must be returned to the LRC. The intended user can check out the CDs (i.e., secretaries can't be sent in someone else's place). The software can be checked out for a total of three business days.

Additional information about the McAfee

VirusScan software can be found at:

<http://www.networkassociates.com/us/products/home.htm>
<http://www.nai.com/us/downloads/>
<http://www.networkassociates.com/us/support/>

It is especially important that Sinclair users who share files between work and home scan those files for viruses in both locations. A virus picked up at home could be brought to work and vice versa.

It is equally important to keep the McAfee virus scan software installed on your home PC up-to-date. AutoUpdate instructions are enclosed with the installation instructions. **NOTE: AutoUpdate requires Internet access.** ITS recommends that PC users update the McAfee VirusScan software on their home PCs at least once daily.

Comments and suggestions are welcome and should be sent to the **IT Help Desk, via e-mail to helpdesk@Sinclair.edu or by voice at 512-HELP (4357).**



Cheryl Stewart

Media Services Gets New Home



By now I am sure that all of you know that a major renovation of the LRC has started. This project will take about a year to complete. You may or may not know, the LRC has moved to the Ballroom on the second floor of Building

7 and Media Services is now located on the second and third floor of Building 14. Unlike the LRC which will be moving back to the lower level of Building 7 when this project is completed, Media Services will be staying in Building 14. This is a permanent move for the department.

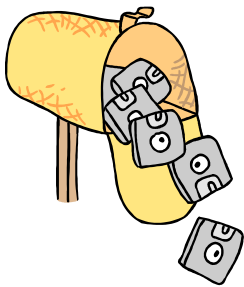
With this in mind, there are some changes in how Media Services will provide some services. One of the biggest changes is regarding the videos which our clients use for classrooms and meetings. Since the video collection has always been the property of the LRC, it will remain so. However, Media Services will still provide delivery of these items as we have done in the past.

Because of space issues, the entire video collection will **NOT** be moved to the Ballroom with the LRC staff. Media Services has two lists of videos from the inventory of almost 3,500 videos in the collection that **WILL** be moved with the LRC to the Ballroom. Media Services has gone through records from the past year to create an accurate list of the most used titles for the first list. For example, if you have requested a specific title during the past year, it will go into the group of titles to be moved. In addition to the most used titles, all of the titles that are currently on **RESERVE** will go with the LRC staff. The remainder will be put into storage and **NOT** be available for use during this time period.

One last item, if there are any **SAME DAY REQUESTS** for videos for your class or meeting, it will be the responsibility of the client **TO PICK UP AND RETURN** them to the LRC's circulation desk at the new location in the Ballroom. **IF YOUR TITLE IS NOT ON THE LIST, IT WILL NOT BE AVAILABLE.**

Barry L. Payne,

Size Limits Placed on Email Attachments to Distribution Lists in Outlook



In order to limit our exposure to denial of service attacks and to reduce the impact of large emails that can be sent through Outlook, Information

Technology Services has set a **one (1) MB size limit on all email attachments sent to the**

following distribution lists in Outlook:

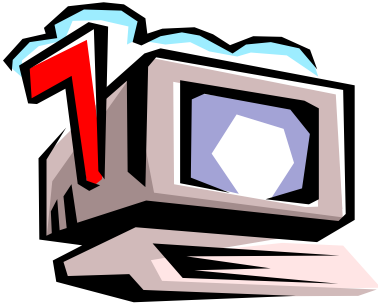
- ZZZ - Support Staff
- ZZZ - Student Employees
- ZZZ - SCC Fulltime Faculty
- ZZZ - Professional Staff
- ZZZ - Part-time staff

- ZZZ - Part-time faculty
- ZZZ - Full-time employees
- ZZZ - All Sinclair Mail Users
- ZZZ - All Faculty

Any email with an attachment larger than 1 MB will not be able to be sent to the above distribution lists.

For additional questions or information, contact Scott McCollum at scott.mccollum@sinclair.edu or at 512-3068.

Cheryl Stewart



Hints from the Help Desk

Your Network Account at Sinclair Community College

Network accounts are created for all active College employees (faculty, staff, etc.).

This account provides you with access to the tools routinely used to conduct Sinclair business, including: Outlook (the email, calendaring, and scheduling software); the Intranet and Internet pages; the portal, my.Sinclair.edu; and other PC applications. Please read the important account information below.

Due to the automatic account creation process, Information Technology does NOT issue individualized network account letters to new employees. Login IDs and initial passwords follow a standard format for all users.

All new employees should receive a document called Getting Started with Your Network Account at Sinclair Community College. This document contains account information and instructions on how to access a network account for the first time. This document can be found at the following link:
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/gettingstarted.htm

It is not necessary for a new employee to contact the Help Desk about network account information unless they experience problems or have questions while accessing their account.

Important additional network account information can be found at the following link:
http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/welnetaccts.htm

NOTE: Network account access does NOT include access to the Colleague system. Colleague accounts are NOT issued automatically. Colleague account access is granted through a different process that can be found at:
<http://our.sinclair.edu/sites/colleague/colleaguewebsite/colleague.htm>

Please contact the Help Desk at helpdesk@sinclair.edu or at 512-HELP (4357) for any questions or additional information about the Network Account process.

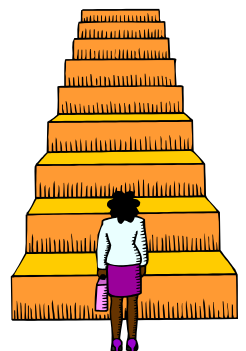
Cheryl Stewart



Food For Thought.....

The pessimist sees the difficulty in every opportunity; the optimist sees the opportunity in every difficulty.

~ L. P. Jacks ~



SpamAssassin Instructions Have Been Updated



The instructions for using the Spam Assassin application have been updated to reflect the changes associated with the update to Outlook 2003.

The revised instructions can be found at the following link:

[http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/otlk/](http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/otlk/spam_assassin/spamassassininstructions.htm)

[spam_assassin/spamassassininstructions.htm](http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/otlk/spam_assassin/spamassassininstructions.htm)

SpamAssassin is a software product that helps users filter unwanted Spam email messages.

SpamAssassin filters run on the incoming mail relay server, and they tag Spam messages with the following line in the header section of an email message:

“SpamAssassin says this is SPAM”

Headers aren't shown in the normal Outlook display but can be viewed by right clicking on a message and selecting Options in the drop down menu.

You use SpamAssassin filters by setting up a rule in Outlook. All messages containing the phrase above will be forwarded to the folder of your choice. You can then go to that folder, review the messages, and delete them, etc. Due to the rules that SpamAssassin uses, false identifications of messages as spam are possible so you should review the folder periodically.

NOTE: Setting up a rule for SpamAssassin is not difficult but you need to follow the instructions carefully in order to correctly set up the rule.

Cheryl Stewart

Changing Your Network Password

Your initial network password is: passXXXX. The word pass (all lower case letters) followed by the last 4 numbers of your Social Security number (represented above as Xs). **All users should change their initial password the first time they log into their network accounts.**

All campus users are required to change their network passwords every ninety (90) days. Users will receive an email reminder in Outlook and a reminder message during the network login process to change their password before it expires.

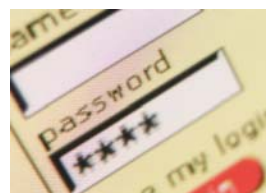
Users should create secure, hard-to-guess passwords. Secure passwords: are at least eight (8) characters in length; contain a combination of upper and lower-case letters, numbers, and symbols; and do NOT consist of common names or words. Your new password cannot be the same as any of your previous 13 passwords.

Users should also exercise good password management by: **always changing an initial**

password assigned by IT staff immediately upon receipt; changing passwords, where possible, at least every ninety days or when required to do so by the system being used; and never writing down a password and posting nearby a computer.

You can change your network password both on-campus and off-campus. **Detailed instructions on changing your password can be found at the following link:** http://our.sinclair.edu/sites/its/itswebsite/it_policies/procedures/netacctpro/psswrld.htm

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



Cheryl Stewart

Cyberservice Word Search

The following terms are used often by the members of Cyberservice in Building 14. Try your hand at finding them. To find them all you must look horizontal, vertical, diagonal and backwards. Descriptions of these terms are on the following page.

- | | | |
|--------------------------|----------------------------------|-------|
| Coder/decoder | ATM | FTP |
| Codec | Asynchronous transfer mode (ATM) | PTEL |
| Videoconferencing | Bandwidth | T-1 |
| MCU | Polycom | DID |
| Direct inward dial (DID) | POTS | H.320 |
| Bridge | Distance Learning | |

X	O	T	M	L	Y	B	P	O	M	Q	R	Q	R	M	L	A	E	O	D	E	I	N	G	O
E	I	D	D	O	R	D	I	S	T	X	A	T	N	N	W	I	D	T	H	M	O	D	E	L
O	T	E	L	I	N	G	I	E	M	P	C	O	D	E	X	E	O	Q	M	P	I	E	G	H
S	M	A	D	Q	S	A	B	S	P	O	L	Y	C	O	M	A	H	3	O	E	D	E	X	P
3	O	G	S	Y	Z	T	C	E	T	T	C	O	D	E	L	X	M	L	P	O	D	L	N	G
2	E	O	R	Y	T	O	A	L	M	X	I	A	J	M	N	O	Y	L	M	R	E	L	N	Q
O	C	U	R	L	C	3	2	N	O	Y	P	O	T	S	A	D	M	R	C	X	L	I	A	E
L	T	L	Q	T	H	X	Y	L	C	L	Q	S	L	T	E	Q	E	L	L	Y	C	O	D	E
Q	R	M	L	S	Q	C	S	W	L	E	C	W	P	A	X	F	X	A	Y	N	L	R	Q	B
3	2	M	T	R	Q	W	D	E	E	R	L	X	R	2	S	L	I	M	E	2	M	E	H	A
M	O	D	E	X	I	N	W	A	R	D	O	E	M	N	E	D	A	R	F	E	N	T	C	N
W	C	X	F	P	O	L	Y	X	V	C	M	E	A	R	D	P	E	R	F	L	D	E	O	D
C	O	M	F	T	P	Q	Q	I	O	O	T	R	P	R	X	F	E	Q	T	I	L	A	D	V
Q	S	T	P	T	R	R	D	D	R	E	T	O	A	X	N	Q	O	Y	W	M	I	P	C	I
R	C	X	M	O	M	E	E	E	R	S	R	W	P	O	U	I	N	D	U	T	C	T	O	D
P	W	L	N	Q	O	M	S	S	U	A	N	E	C	E	A	M	N	X	A	T	M	I	D	E
A	B	E	E	R	B	U	D	O	X	I	U	O	N	Q	Z	A	Q	G	B	B	C	M	E	O
E	A	O	P	X	Q	N	N	M	T	L	E	C	P	R	B	R	A	O	I	O	X	E	C	W
X	L	N	M	H	F	O	T	C	A	D	Y	P	N	Q	L	B	C	D	E	C	I	M	A	I
T	J	Q	W	C	R	N	E	V	I	3	2	P	R	M	A	P	X	L	M	N	R	Q	P	D
M	L	N	W	H	L	R	O	V	Q	6	8	1	1	M	H	3	2	0	1	T	X	O	N	T
Q	T	M	C	L	I	A	X	V	I	D	E	O	B	E	E	R	B	U	D	L	I	T	E	H
S	A	Y	O	D	I	D	P	X	L	M	C	U	P	T	E	L	A	B	C	F	O	X	3	2
Y	S	Q	X	Y	N	D	A	I	J	Q	J	N	E	J	X	Y	B	C	D	M	O	T	O	R
A	X	L	Q	P	E	G	G	C	O	D	E	R	D	E	C	O	D	E	R	C	P	U	3	6

Continued from Page

ATM - asynchronous transfer mode, high speed, high bandwidth, low delay, transport technology, integrating multiple data types (voice, video, and data).

Bandwidth - the amount of data that can be transmitted through a connection, generally described in terms of thousand K or million M bits of data per second.

Bridge - device also referred to as a multipoint control unit (MCU), links three or more videoconferencing rooms into a single videoconference. Video switching between rooms may be voice-activated or may involve timed rotation between rooms.

Coder/Decoder (CODEC) - a device that converts analog video and audio signals to digital signals and compresses them for transmission from the origination site. The CODEC at the receiving site converts and decompresses the signal back to analog video and audio signals for video monitors and audio speakers.

Direct Inward Dial (DID) - a service offered by telephone companies which allows the last 3 or 4 digits of a phone number to be transmitted to the destination exchange. <http://www.ct-labs.com/Dr%20C/q47.htm> http://en.wikipedia.org/wiki/Directed_inward_dial

Distance Learning - the incorporation of web, video and audio technologies into the educational process so that students can attend classes and training sessions in a location distant from that where the course is being presented. Distance education systems are usually interactive and are becoming a highly valuable tool in the delivery of training and education to widely dispersed students in remote locations or in instances where the instructor cannot travel to the student's site.

File Transfer Protocol (FTP) - The internet protocol and program used to transfer files between hosts.

H.320 - the ITU international telecommunications union) standard for video and audio transmission between CODECs of different manufacturers.

MCU - multipoint control unit, device frequently referred to as a bridge or digital switch links three or more videoconferencing classrooms (see bridge).

Plain Old Telephone Service (POTS) - conventional analog telephone lines using twisted-pair copper wire.

T-1 - a digital communication line commonly used in the US. It has a maximum capacity of 1.54Mbps and is often used for extremely high-quality videoconferencing or for simultaneous transmission of multiple videoconferences.

Videoconferencing - a system allowing participants at different locations to view and hear each other immediately via video cameras and monitors along with microphones through telephone lines or the internet.

John Szudlarek





LRC Moves to Temporary Location



Photo by Winnie Tseng

The Learning Resources Center moved to its temporary location on the 2nd floor of Building 7 during Spring break, and it was ready for service when students returned to classes on March 28th. This move represents the next step in the LRC Renovation Project. The new library includes 32 public computers, selected reference books, the current year's magazine subscriptions, all reserve materials, any media identified by the faculty for classroom use, a small circulating book collection, and a classroom for library instruction. In preparation for the move, all faculty were invited to identify any books, magazines, or videos to move to the temporary library. This was done to assure that classes were supported and students would find all the materials they need to complete assignments. Since the library could not move its entire book collection, it also added to its base of online, full-text databases with the Opposing Viewpoints Resource Center and Gale Literature Resource Center. Finally, students, faculty, and staff continue to be able to borrow additional books from other college libraries through OhioLINK. At this time, project plans call for the LRC renovation to be completed in April 2006.

Please check the LRC website at <http://www.sinclair.edu/facilities/library/renovation/index.cfm> for updates and photos of the renovation.

If you have any questions concerning the renovation and or library operations, please contact Doug Kaylor, Director, Learning Resources Center at 512-2855.

Doug Kaylor