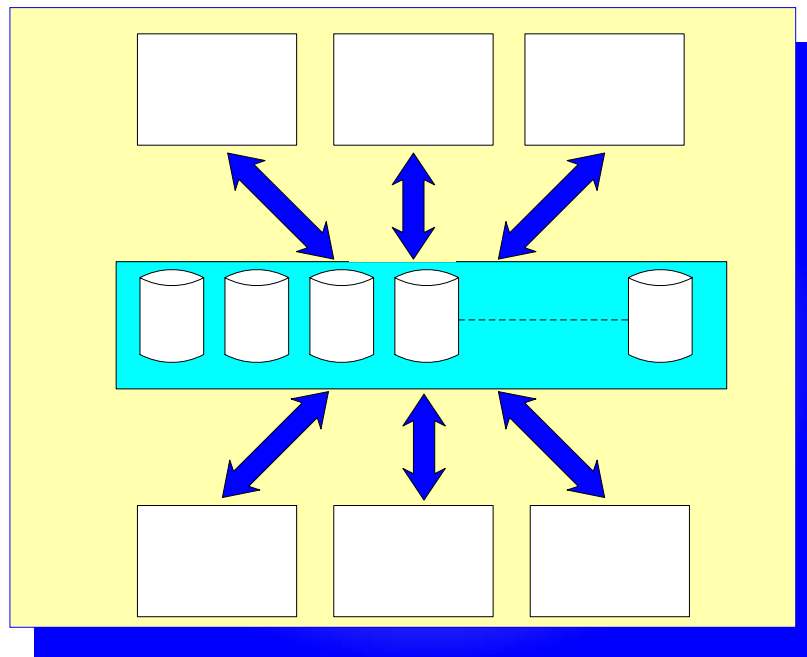


Web Strategy Update

Approximately three years ago we launched our Web Strategy initiative to completely redesign Sinclair's presence on the Internet. Below is the original graphic used to depict the vision.



I am very proud to report that we are almost there. To date most of the major components of this initiative have been completed, and several others, which were not even defined at that time, are well on their way. The one remaining major component is “Common Authentication and Access Control”. We have also made significant progress with respect to this component and should have it completed by the end of this year.

Many people, in the Information Technology Division and in other divisions, played important roles in this achievement—thanks to all of them for their perseverance and dedication!

Ken Moore

Computer Virus activity is rampant Is your computer protected?

Computer virus/worm activity is currently at unprecedented levels. Information security professionals are warning of what appears to be an escalating virus writer community "turf war" on the Internet. Since January 18, 2004, Antivirus vendors have discovered a new or new variant of rapidly spreading virus/worm an average of every other day, and this frequency is increasing rapidly.

ITS is doing all technically possible in our academic environment to prevent infections to Sinclair's systems, minimize damage when prevention fails, and clean/repair/restore infected systems. However, technology alone cannot prevent these attacks. **If every Sinclair systems user takes some basic protective action, we can minimize disruption to all.**

All users should:

1. Shut-down all PCs at the end of the day or when no longer needed for use. When a network-connected PC is re-booted, ITS automatically "pushes" the latest security patches and updates to the PC operating system during the start-up process.

2. Never open e-mail message attachments unless you are certain the attachment is valid and virus free. Most of the current virus threats rely on unsuspecting or curious users who open the e-mail the virus attachment travels in, then click on the attachment to see what it is, thereby launching the malicious program. It is no longer safe to assume that because you know an individual, the message is from the individual. Viruses scour address books and mailboxes for addresses, then "spoof" these addresses so it appears the message is coming from someone you know. They also disguise themselves using reasonable subject lines (such as, please review this document, or please update your address) and names for the attachment. **If you are sending an email attachment, personalize it!** Be specific in the subject line and message body so the recipient can be reasonably sure the message is valid. For example, the subject "Updating the

Sinclair Telephone Directory" is specific to a Sinclair process and likely safe; when the message body also refers to incidents specifically related to the College, and also contain the signature block of the sender, it further validates the message.

A new (and dangerous) variant was released March 3, 2004...

The latest virus "spoofs" the "from" address so it appears to come from IT management within the organization (i.e. administrator@sinclair.edu or similar), and the message instructs the user to click an attachment to clean their PC of viruses, block SPAM, or other seemingly plausible request. When the user clicks the attachment the virus is launched. **At Sinclair, all messages or alerts warning of malicious code that require user action will originate from an individual, (i.e. Krasofsky, David; McCollum, Scott; O'Callaghan, Daniel; Moore, Kenneth) or from an account with Sinclair in the generic address (Sinclair ITS@sinclair.edu), in which case the message will include the originator's signature block.**

3. Do you have a home computer? Do you use it to check email or connect to the Internet?

If you do NOT use antivirus software, or if it is NOT regularly updated, you are virtually guaranteed to be infected with malicious code such as viruses and worms. If you use your unprotected PC to check your work email, access your network directory, or simply email other Sinclair employees, you risk infecting the SCC network. As a Sinclair employee, you can get this antivirus software FREE from the LRC.

http://intranet.sinclair.edu/its/itswebsite/it_policies/policyindex.htm For additional information on protecting your home PC, <http://www.sinclair.edu/departments/infosec/SecurityAwareness/index.cfm>.

To try to put the number and type of the most prolific threats into perspective:

Continued on Page 3

Computer Virus activity is rampant Is your computer protected?

Continued from Page 2

As of March 2, 2004 Netsky.D was most prolific "in the wild" and causing the most traffic; Netsky is a virus/worm originally detected February 16; by March 2nd there were 6 known variants. The Bagle (also called Beagle) worm was discovered January 18, 2004; by March 2nd there were 7 known variants. MyDoom (also called Novarg) was discovered January 26, 2004 by March 2nd there were 5 known variants.

In addition to the above, new variants of Netsky and Bagle were discovered March 3, 2004.

For continually updated virus information:
<http://us.mcafee.com/virusInfo/default.asp?cid=9043>
<http://www.sophos.com/>

Dan O'Callaghan



Technology Services Update



ITS technicians have been busy installing LCD monitors, HP laser jet printers, lab PCs, Administrative PCs, and laptops. The printers were ordered and delivered in January as well as the 400 LCD monitors IBM had been holding for us.

ITS technicians worked overtime on weekends and evenings to install the new equipment and clear the hallway. As you can see from the

pictures, they succeeded in installing the new LCD monitors and printers and have created the need for another Sinclair surplus sale.



Pictures by Pat Bernard

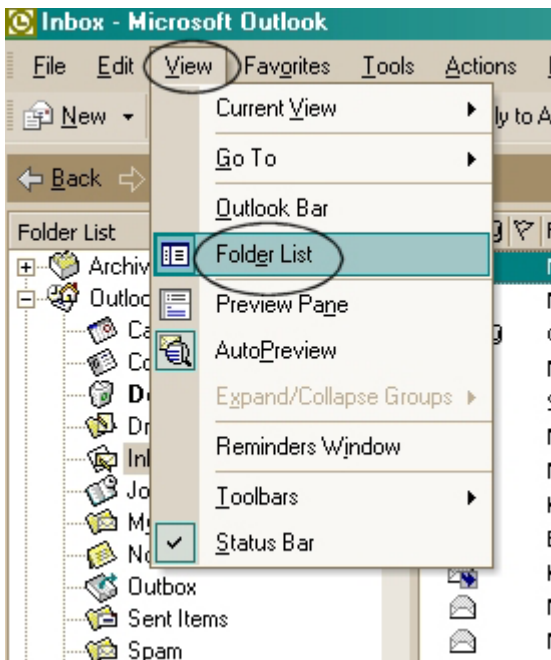
ITS technicians have installed 23 lab printers, 334 lab monitors, 334 lab PCs, 23 Administrative printers, 120 Administrative LCD monitors and 120 Administrative PCs for the Replacement and Renewal process this fiscal year on campus. They have also imaged and distributed 36 laptops for Replacement and Renewal this fiscal year.

Donna Blankenship

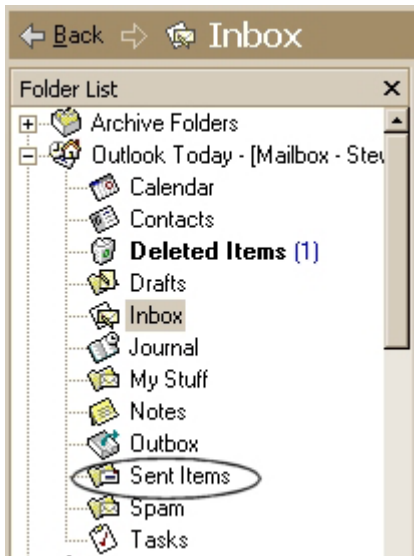
Recall or Replace a Message You've Already Sent in Outlook

You can recall or replace a message **only if its recipient is logged on and using Microsoft Outlook and has not read the message or moved it from their Inbox.**

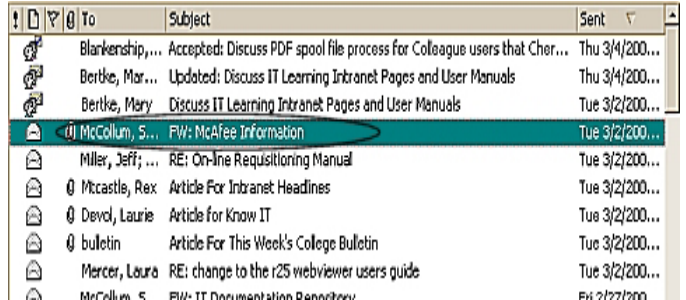
1. If the **Folder List** (Displays folders available in your mailbox) is not visible, click the **View** menu, and then click **Folder List**.



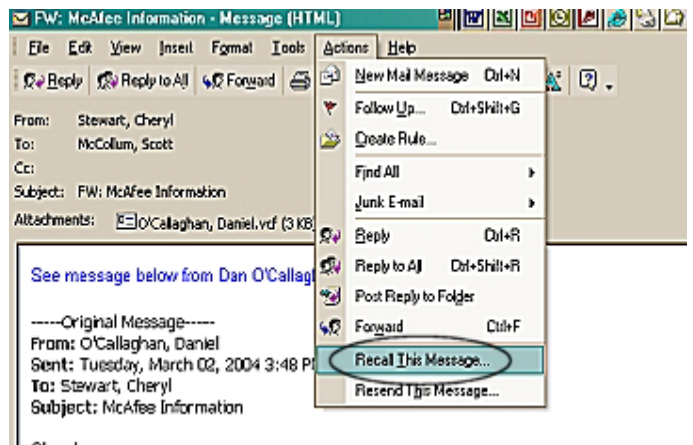
2. Click Sent Items.



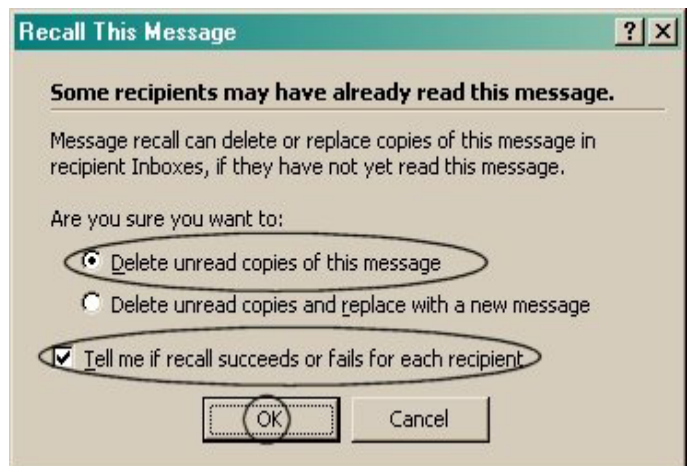
3. Open the message you want to recall or replace.



4. On the Actions menu, click Recall This Message.



5. If you wish to recall the message, click **Delete unread copies of this message**.



Continued on Page 5

Recall or Replace a Message You've Already Sent in Outlook

Continued from Page 4

To be notified about the success of the recall or replacement for each recipient, select the **Tell me if recall succeeds or fails for each recipient check box**. **Replace the message**. Click **OK**.

- To recall and replace the message with a new one, click **Delete unread copies and replace with a new message**. Click **OK**, and then **type a new message**. To be notified about the success of the recall or replacement for each recipient, select the **Tell me if recall succeeds or fails for each recipient check box**. Click **OK**.



NOTE: To replace a message, you must send a new one. If you do not send the new item, the original message is still recalled.

Cheryl Stewart

Guidelines for Use of the “All Sinclair Users” Option in Microsoft Outlook

The use of the “All Sinclair Mail Users” option is limited to email messages for academic and administrative uses. This option gives users the ability to send email to all Sinclair mail users. Good judgment should be exercised in the use of this option. The message should be campus-wide in nature. It should also contain material that is time-sensitive and would not more appropriately be published in another format such as the President’s Bulletin. **“All Sinclair Mail Users” messages should be a maximum of one (1) MB in size (including file attachments).**

Examples of appropriate use include:

- Timely announcement of College-sponsored speakers.
- Timely announcements of College-sponsored events or meetings.

Examples of inappropriate use include:

- Garage sale and other personal for sale announcements.
- Non-Sinclair sporting event tickets for sale.
- Messages including attachments larger than 1 MB.

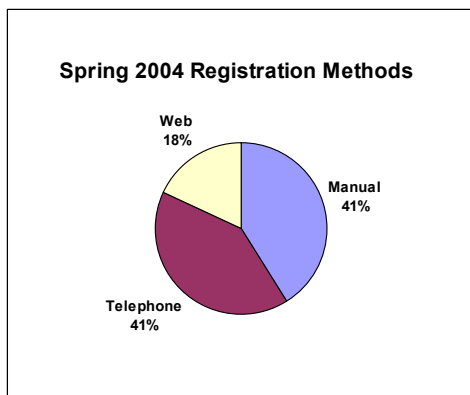
If users are unsure if a message should be distributed to all users, they should obtain approval from their supervisors. Supervisors should obtain approval from the appropriate manager, dean, or director. Final approval for an “All Sinclair Mail Users” message rests with the respective Vice President.

Cheryl Stewart

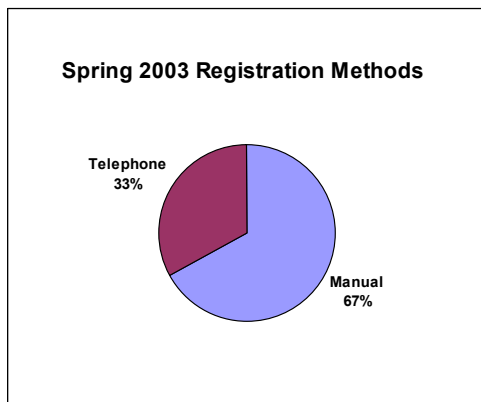
On-Line Services

Spring term, 2004 marked the first term where registration and payments through the Web were available for the entire registration period. We'd like to share some statistics on how the new processes are being used.

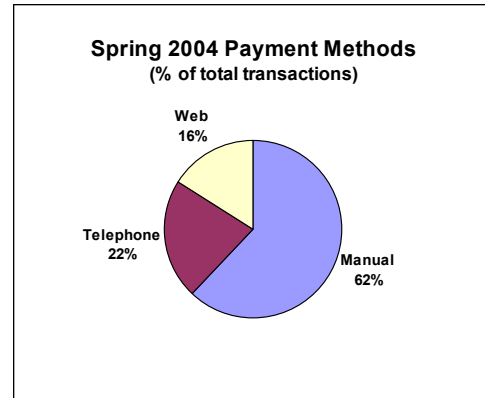
Through the first three weeks of registration for Spring, manual and telephone registration transactions are equal at approximately 41% of the total volume. Web registration has handled around 18% of the total volume.



By comparison, in Spring 2003 two-thirds of all transactions were handled manually and telephone registration was the only option, handling the remaining third.



The other new capability on the Web is the ability to pay online using Visa or Mastercard. Data from the Bursar's office indicates that students are taking advantage of alternative methods of payment available through both the telephone and the Web.

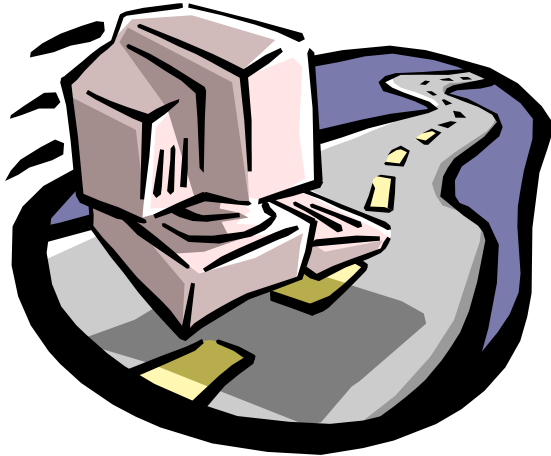


You may be aware that the first day of registration presented some real challenges for the system. Elimination of mail-in registration and a rush to get into classes before they closed pushed the volume of transactions on the first day to twice what it had been a year earlier. Since that time, both the Web registration and telephone registration systems have been handling transactions without major issues. In order to avoid such issues in future terms we are working to implement a number of solutions. The Enrollment and Registration Committee will be looking at ways of staggering the registration process so that students are not all eligible to begin registering on the same day. Systems Development and Maintenance and Information Technology Services are working on upgrades to the servers including additional processing power, upgrades to the database and operating systems, separating some services onto other systems, and complete replacement of the servers which is scheduled as part of the 2004/2005 renewal and replacement cycle.

Information for Spring indicates that students are increasing their use of technology to interact with the college. The new Web registration and payment functions are helping to make these processes more convenient for students.

Andy Runyan

Are You a “Safe Driver” on the Information Highway?



menacing, or more so, than pot-holes, “trash” on the road, traffic jams, mechanical failures, accidents, “rage drivers,” hijackers, and criminals sharing the road. Unlike on physical roads, the Information Highway driver is traveling the Globe at nearly the speed of light and must increasingly rely on the safety of the vehicle and be aware of anomalies to avoid obstacles and other dangers.

To help Sinclair’s family of Information Highway drivers maintain safe information vehicles and improve awareness of safe “driving” habits, IT has initiated an Information Security Program.

Do you use email? “Surf” the World Wide Web (www.)? Use the Internet for on-line banking or buying? Share or store files over a network? Participate in distance learning? Use mySinclair.edu? Every time you use your computer to engage in one of these activities, you drive your computer, and the information “passengers” within, onto the Information Highway. Are you a *safe* driver?

One of the initial steps in this initiative is the launch of an Information Security Web site where users will be able to find updated and reliable “traffic reports” on dangerous activity, “mechanics and tune-up” information for keeping your PC safe, and “rules of the road.” The site is in the early development stages, you can access it via: <http://www.sinclair.edu/departments/infosec/index.cfm>

Just as on our physical roads, the driver on the Information Highway must contend with a complex mass of freeways, toll roads, side roads, bridges, construction sites, and millions of interchanges. It also has numerous dangers as

Suggestions or topics you’d like to see? Email daniel.ocallaghan@sinclair.edu

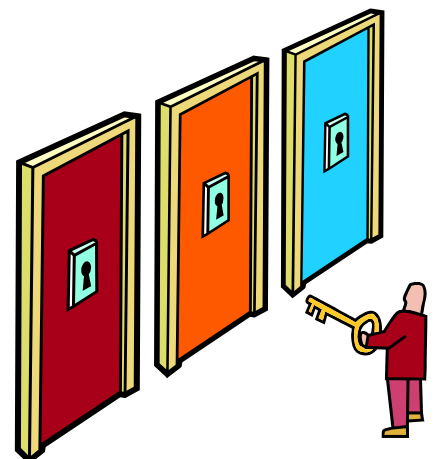
Dan O’Callaghan



Food For Thought.....

I believe that we are solely responsible for our choices, and we have to accept the consequences of every deed, word, and thought throughout our lifetime.

Elisabeth Kübler-Ross



SpamAssassin

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.

To learn how to use SpamAssassin in your Outlook mailbox, go to the SpamAssassin link on the IT Policies and Procedures Intranet page.

http://intranet.sinclair.edu/its/itswebsite/it_policies/procedures/spam_assassin/spamassassininstructions.htm

NOTE: Setting up a rule for SpamAssassin is not difficult but you need to follow the instructions carefully in order to do it correctly. Please contact the Help Desk at helpdesk@sinclair.edu or at 512-HELP (4357) for any questions or additional information about SpamAssassin.



Cheryl Stewart

Automatic Nightly PC Shutdowns Beginning Soon

After our recent problems with viruses on campus, it has become clear that many of our plans for preventing viruses were unsuccessful due to incorrect assumptions.

One of those incorrect assumptions is that all campus computers are turned off at night and rebooted in the morning. **Logging off and rebooting in the morning is necessary to allow updates such Microsoft patches (bug fixes) and updates to virus definitions to take place.**

In addition, the regular rebooting of computers helps to reduce problems by cleaning up the remnants of failed programs and by resetting icons and other characteristics to their normal state. Turning computers off during the night also helps to conserve electricity.

Many colleges and universities have recently suffered 2-5 days outages. We have been extremely lucky, but an increasing amount of the college's resources are wasted each time a major virus is

released to the Internet. We need to take additional steps to keep our network and computers virus-free.

In the next few weeks, ITS will begin to automatically shut down all computers at 11pm each night. While we understand that many users are already shutting down computers each night, it isn't being done consistently, and the problems are impacting the entire campus.

ITS will publish the start date for the automatic shutdowns soon in various sources such as the College Bulletin, Intranet Headlines, and Outlook.

Some individuals may need to leave computers running at night for special situations. These situations need to be supported by the appropriate Dean or Director and reported to Steve Linderman at x2538 so they can be evaluated on an exception basis.

Cheryl Stewart

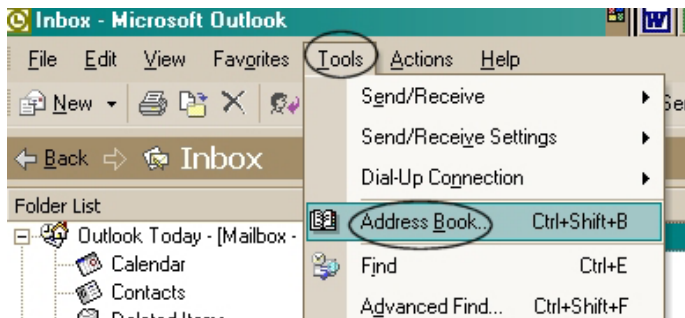
The Wizard Needs Your Help to Update the Magic Database



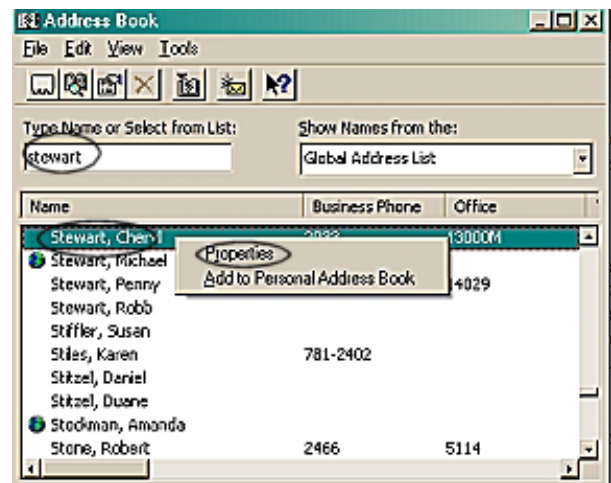
The IT Help Desk is updating client contact information in the Magic database. This information is used to contact clients after they have put a request through to the Help Desk. Accurate contact information helps to ensure prompt responses to client requests. **The Help Desk is asking for your help in updating this information.**

To confirm that your contact information is correct, follow the quick steps below:

1. Open Outlook.
2. Go to Tools.
3. Click on the Address Book.

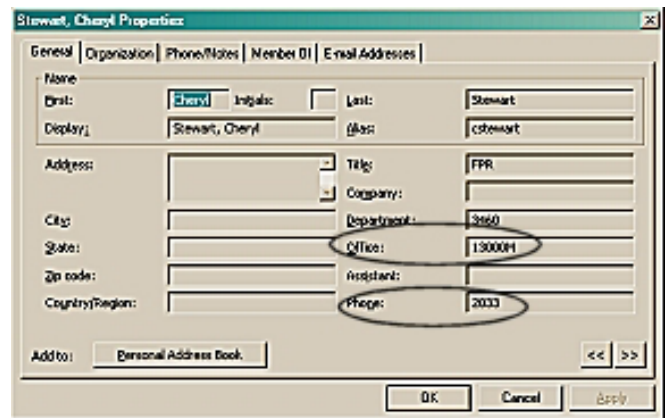


4. Search for your name and highlight it.
5. Right click on your highlighted name.
6. Go to Properties.



7. Check your Office location and Phone information.

If this information is incorrect, click on Internet Explorer and access the school's intranet home page. There are several boxes at the top--click on Campus Directory and open it. When the directory is open, use your gray right scroll bar and scroll all the way down. Select the Request for Information Change box and click on it. Fill in the form and send it.



Questions and comments should be sent to the IT Help Desk at helpdesk@sinclair.edu or at 512-HELP (4357).

Cheryl Stewart



**Vice President for Information Technology
& Chief Information Officer and Executive Secretary**



KEN MOORE

Vice President for Information Technology
& Chief Information Officer
kenneth.moore@sinclair.edu

LAURIE DEVOL

Executive Secretary,
Vice President for Information Technology
Services & Chief Information Officer
laurie.devol@sinclair.edu