Community College of Philadelphia

Minutes

Technology Coordinating Committee
05.21.2014 2:30 p.m.
B2-26

2013-14 Committee Members Present:

Federation Delegates & Alternates	
Eva Agbada	**A**
Ed Baker (A)	**A**
Frank Bartell (A)	**A**
Heidi Braunschweig	**A**
Steven Davis	**P**
Steve Jones (A)	**A**
Fran Lukacik	**P**
Craig Nelson	**P**
Noelia Rivera-Matos	**A**
Jessica Rossi	**A**
Sean Sauer	**A**
Karen Schermerhorn	**P**
Ted Wong	**A**
Administrative Appointees & Alternates:	
Rikki Bardzik (A)	**A**
Jody Bauer	**P**
Gary Bixby	**P**
Bill Bromley	**P**
S.K. Calkins	**A**
Arnold DiBlasi	**A**
Ellen Fernberger	**P**
Susan Hauck	**A**
Sam Hirsch	**A**
Allan Kobernick (A)	**A**
Gim Lim (A)	**P**
Peter Margolis	**A**
Aileen Rollins (A)	**P**
Jocelyn Sirkis (A)	**P**
Jim Spiewak (A)	**A**
David Watters	**A**

Community College *of* Philadelphia

Minutes - DRAFT

Technology Coordinating Committee
05.21.2014 2:30 p.m.
B2-26

I. **Call to Order**

Meeting called to order at 2:35PM.

II. **Attendance**

Attendance as noted on Page 1 of this document.

III. **Approval of minutes (Action)**

a. **April 16, 2014 Minutes – Approved**

IV. **Old Business (Informational)**

a. **Updates from Workgroups**

i. **Responsible Printing Workgroup**
The committee met on April 22, 2014. See the minutes – "Meeting Minutes -Responsible Printing Workgroup 4-22-2014.pdf"

ii. **No other workgroups have met**

V. **New Business**

a. **Update from Jody on an Information Security PowerPoint for sharing with the college community.**

i. See attached – "IT Security Awareness.pdf"

ii. Suggested that it contain more "personal" information related to home users to draw them to the sessions.

b. **Question concerning June meeting**

i. **Determined by the quorum present no June meeting will be held**

c. **Congratulation to Dr. Schermerhorn for her years of service. She will be missed at the TCC.**

VI. **Adjournment @ 3:15PM**

TCC Workgroup for the Responsible Printing Policy

Meeting Minutes
April 22, 2014, 1:00pm - 2:00pm

In attendance

J. Bauer (ITS), J. Spiewak (Planning & Finance), M. Myers (SACC & Learning Labs), J. Rossi (Library), F. Lukacik (Allied Health), C. Nelson (Computer Technologies), E. Adolphus (SACC), J. Thomas (SACC), E. Agbada (Library)

Background information & current printing conditions

J. Bauer and J. Spiewak provided some background information on the GoPrint system. The College has a pay-to-print system (GoPrint) but is currently only running this as a pilot program in the Library at Main Campus. The full implementation of this system was frozen because the sub-committee tasked with deciding on a reasonable allotment for our students was unable to make a final determination on the print quota.

Discussion ensued regarding various printing issues around the College. Examples:

1. Differing page printout limits:
    a. SACC labs only allow students to print 30 pages per day
    b. Library allows for unlimited printouts per day (30 pages maximum per print job).
    c. Printers in computer classrooms offer unlimited printing
2. Free-standing PCs with attached printers and printers in computer classrooms are difficult to effectively monitor and maintain.

Scope & Tasks

This Responsible Printing Workgroup is not responsible for implementing the GoPrint system. We will focus on creating a policy (or set of guidelines) to assist the College community use our printing resources in a more environmentally-friendly and cost-efficient manner.

Suggested Action Items

1. Create Printing Guidelines for Students. Examples:
    ○ How to print double-sided handouts
    ○ How to print multiple powerpoint slides on one page
2. Create Printing Guidelines for Faculty. Examples:
    ○ How to create printer-friendly powerpoint presentations
    ○ How to limit printing for PDF files
    ○ How to use fonts that use less printer toner

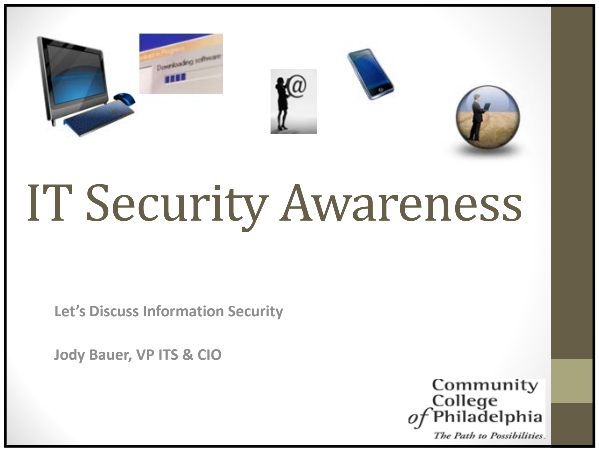
Other considerations

J. Bauer announced that with the Fall 2014 semester, all students will be transitioned fully to AD and OWA. This will mean that they will use their AD credentials to login to all College PC's. Since they are logging in with their individual credentials, we will be able to start tracking statistics for printouts. Once we have a clearer picture of the actual printing patterns and usage numbers for our Students, we can make recommendations on a reasonable print allotment. Hopefully, this data will allow the College to move forward with the full implementation of GoPrint.

For next meeting (date and location TBA)

1. Draft responsible printing guidelines for students and faculty

Submitted by: E. Agbada



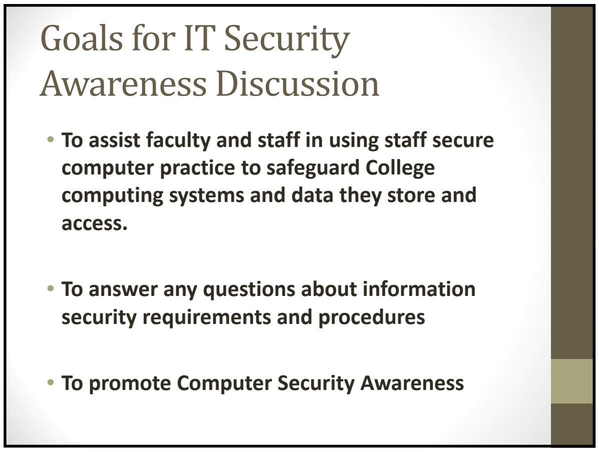
IT Security Awareness

Let's Discuss Information Security

Jody Bauer, VP ITS & CIO

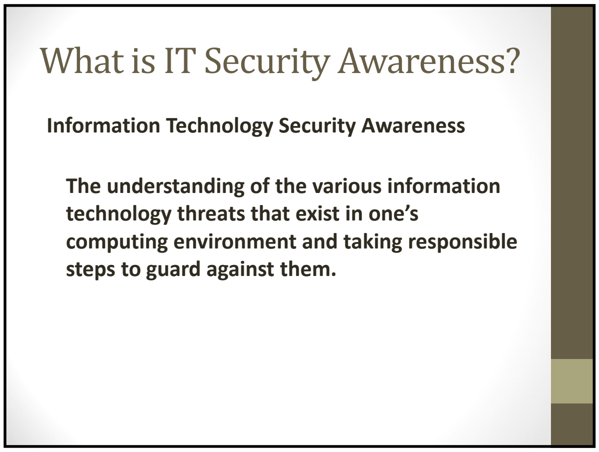
Community College of Philadelphia

The Path to Possibilities.



Goals for IT Security Awareness Discussion

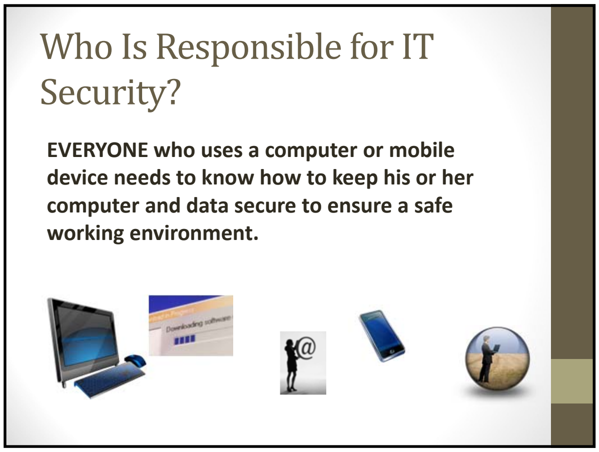
- To assist faculty and staff in using staff secure computer practice to safeguard College computing systems and data they store and access.
- To answer any questions about information security requirements and procedures
- To promote Computer Security Awareness



What is IT Security Awareness?

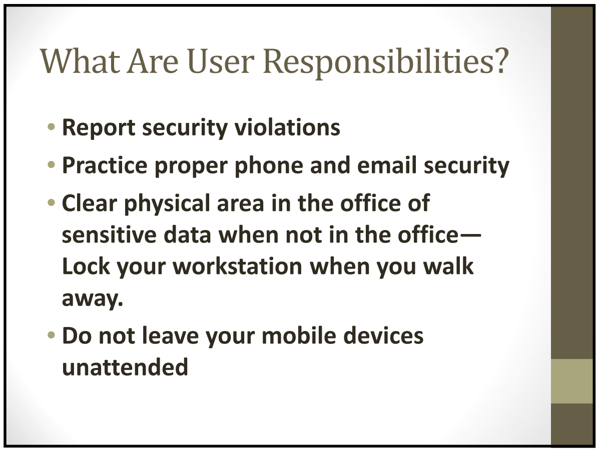
Information Technology Security Awareness

The understanding of the various information technology threats that exist in one's computing environment and taking responsible steps to guard against them.



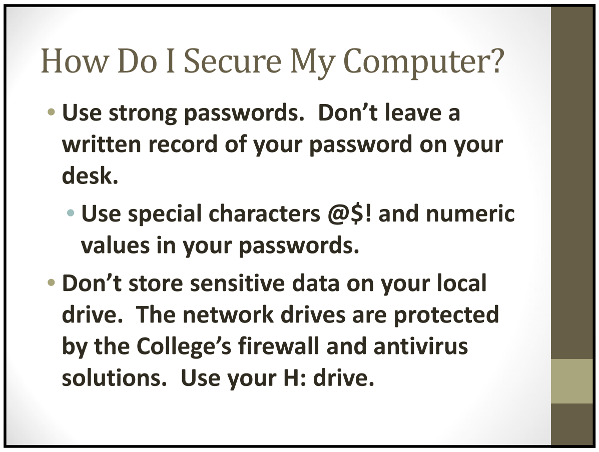
Who Is Responsible for IT Security?

EVERYONE who uses a computer or mobile device needs to know how to keep his or her computer and data secure to ensure a safe working environment.



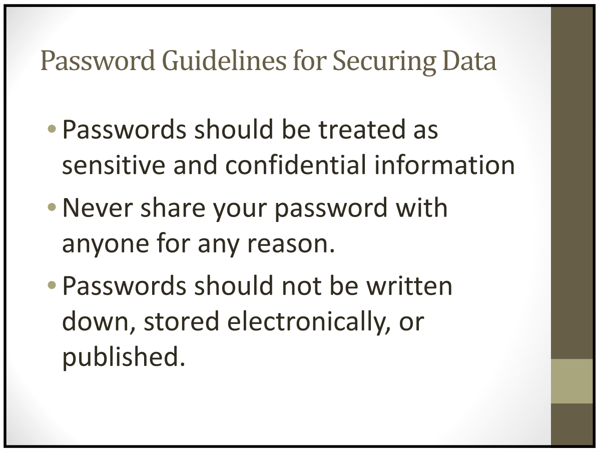
What Are User Responsibilities?

- Report security violations
- Practice proper phone and email security
- Clear physical area in the office of sensitive data when not in the office—Lock your workstation when you walk away.
- Do not leave your mobile devices unattended



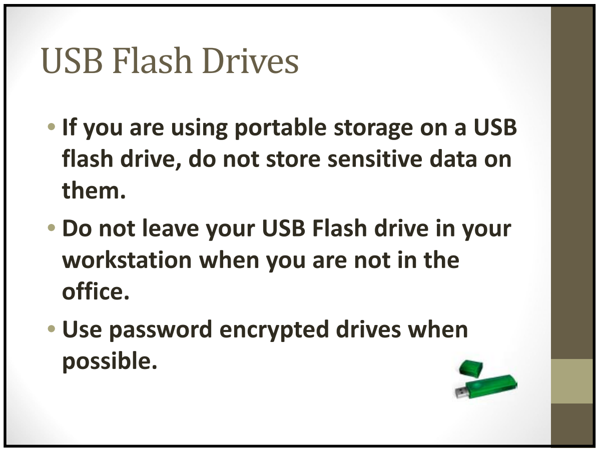
How Do I Secure My Computer?

- Use strong passwords. Don't leave a written record of your password on your desk.
  - Use special characters @$! and numeric values in your passwords.
- Don't store sensitive data on your local drive. The network drives are protected by the College's firewall and antivirus solutions. Use your H: drive.



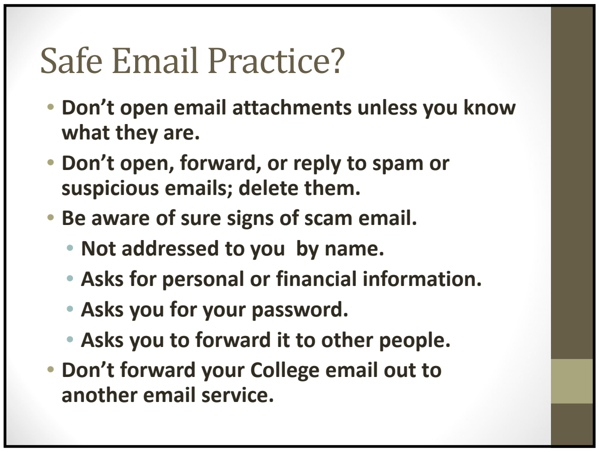
Password Guidelines for Securing Data

- Passwords should be treated as sensitive and confidential information
- Never share your password with anyone for any reason.
- Passwords should not be written down, stored electronically, or published.



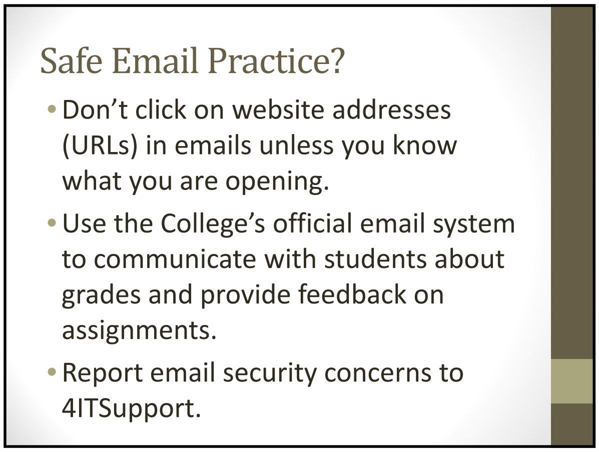
USB Flash Drives

- **If you are using portable storage on a USB flash drive, do not store sensitive data on them.**
- **Do not leave your USB Flash drive in your workstation when you are not in the office.**
- **Use password encrypted drives when possible.**



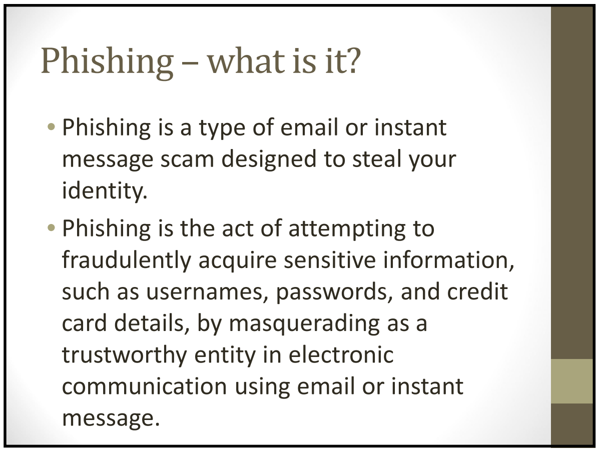
Safe Email Practice?

- **Don't open email attachments unless you know what they are.**
- **Don't open, forward, or reply to spam or suspicious emails; delete them.**
- **Be aware of sure signs of scam email.**
  - **Not addressed to you by name.**
  - **Asks for personal or financial information.**
  - **Asks you for your password.**
  - **Asks you to forward it to other people.**
- **Don't forward your College email out to another email service.**



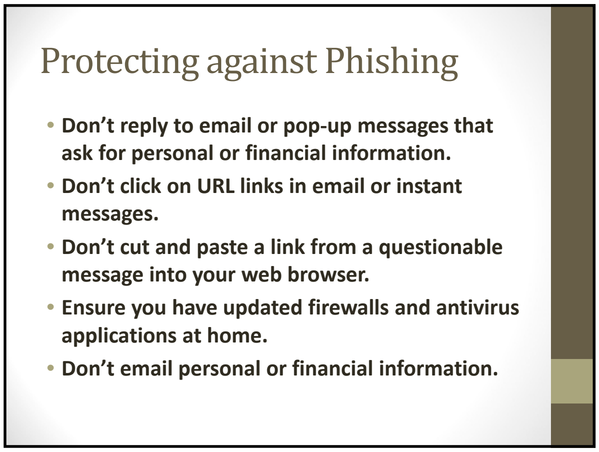
Safe Email Practice?

- Don’t click on website addresses (URLs) in emails unless you know what you are opening.
- Use the College’s official email system to communicate with students about grades and provide feedback on assignments.
- Report email security concerns to 4ITSupport.



Phishing – what is it?

- Phishing is a type of email or instant message scam designed to steal your identity.
- Phishing is the act of attempting to fraudulently acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in electronic communication using email or instant message.

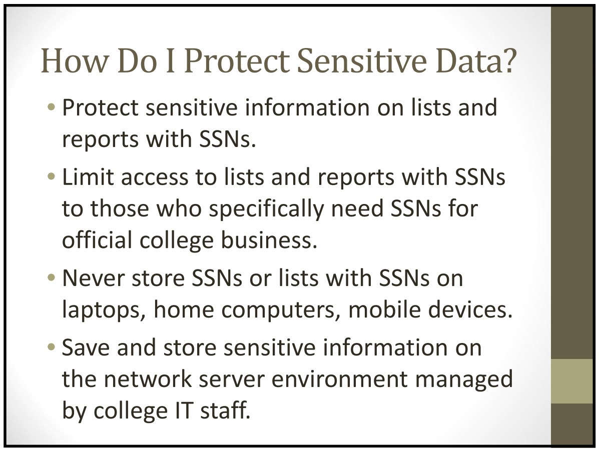


Protecting against Phishing

- **Don’t reply to email or pop-up messages that ask for personal or financial information.**
- **Don’t click on URL links in email or instant messages.**
- **Don’t cut and paste a link from a questionable message into your web browser.**
- **Ensure you have updated firewalls and antivirus applications at home.**
- **Don’t email personal or financial information.**

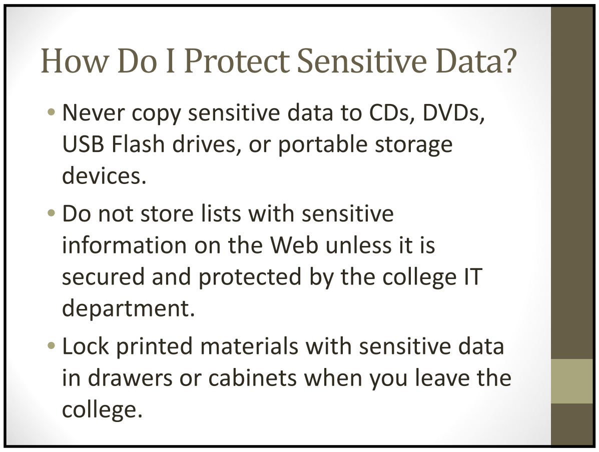
Report Phishing

If you are scammed, visit Federal Trade Commission's Identity Theft website – www.consumer.gov/idtheft



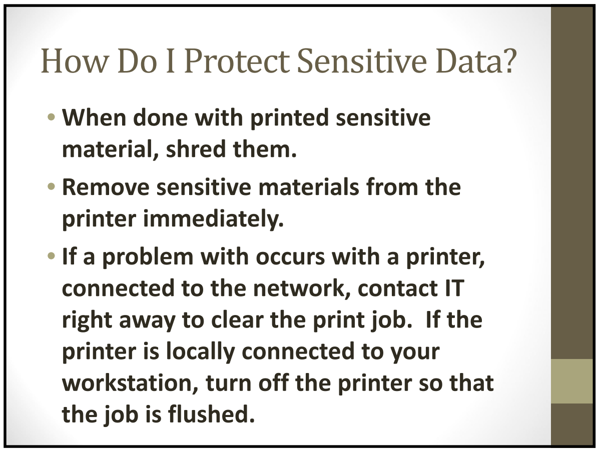
How Do I Protect Sensitive Data?

- Protect sensitive information on lists and reports with SSNs.
- Limit access to lists and reports with SSNs to those who specifically need SSNs for official college business.
- Never store SSNs or lists with SSNs on laptops, home computers, mobile devices.
- Save and store sensitive information on the network server environment managed by college IT staff.



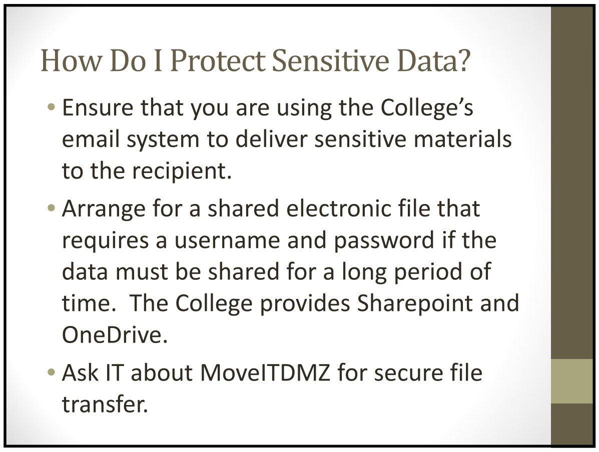
How Do I Protect Sensitive Data?

- Never copy sensitive data to CDs, DVDs, USB Flash drives, or portable storage devices.
- Do not store lists with sensitive information on the Web unless it is secured and protected by the college IT department.
- Lock printed materials with sensitive data in drawers or cabinets when you leave the college.



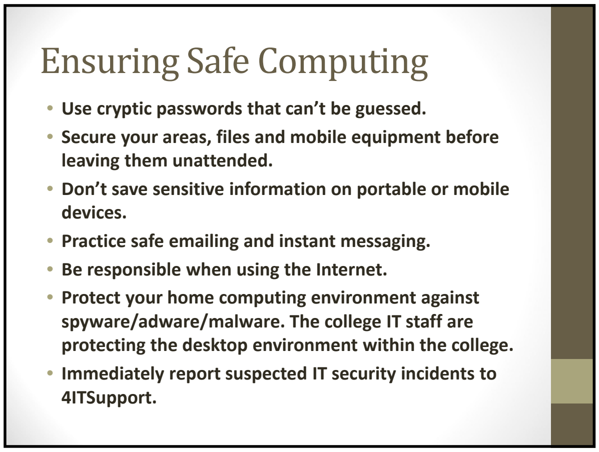
How Do I Protect Sensitive Data?

- **When done with printed sensitive material, shred them.**
- **Remove sensitive materials from the printer immediately.**
- **If a problem with occurs with a printer, connected to the network, contact IT right away to clear the print job. If the printer is locally connected to your workstation, turn off the printer so that the job is flushed.**



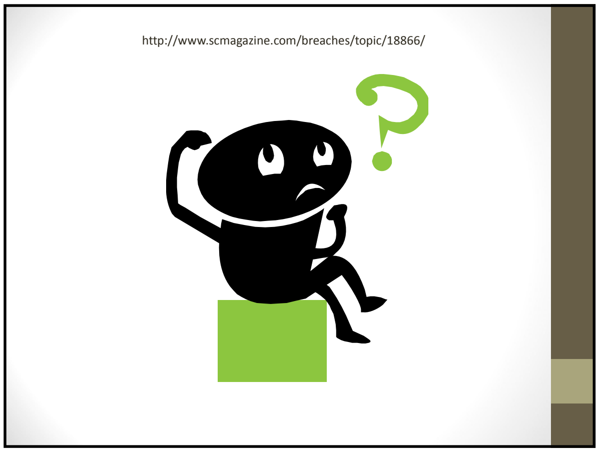
How Do I Protect Sensitive Data?

- Ensure that you are using the College's email system to deliver sensitive materials to the recipient.
- Arrange for a shared electronic file that requires a username and password if the data must be shared for a long period of time. The College provides Sharepoint and OneDrive.
- Ask IT about MoveITDMZ for secure file transfer.



Ensuring Safe Computing

- **Use cryptic passwords that can't be guessed.**
- **Secure your areas, files and mobile equipment before leaving them unattended.**
- **Don't save sensitive information on portable or mobile devices.**
- **Practice safe emailing and instant messaging.**
- **Be responsible when using the Internet.**
- **Protect your home computing environment against spyware/adware/malware. The college IT staff are protecting the desktop environment within the college.**
- **Immediately report suspected IT security incidents to 4ITSupport.**



http://www.scmagazine.com/breaches/topic/18866/