

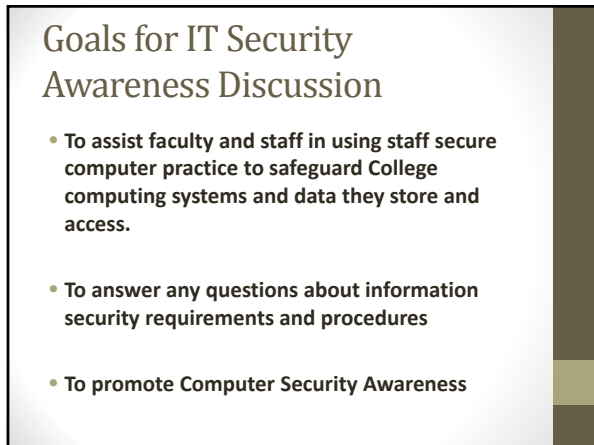
The slide header features a white background with a dark brown vertical bar on the right. At the top, there are five icons: a laptop, a document labeled 'Downloading software', a person with an '@' symbol, a smartphone, and a globe. Below the icons, the title 'IT Security Awareness' is written in a large, dark serif font. Underneath the title, the text 'Let's Discuss Information Security' and 'Jody Bauer, VP ITS & CIO' is displayed in a smaller font. In the bottom right corner, the 'Community College of Philadelphia' logo is present, with the tagline 'The Path to Possibilities.' below it.

IT Security Awareness

Let's Discuss Information Security

Jody Bauer, VP ITS & CIO

Community College of Philadelphia
The Path to Possibilities.



The slide has a white background with a dark brown vertical bar on the right. The title 'Goals for IT Security Awareness Discussion' is at the top in a dark serif font. Below the title is a bulleted list of three items. The first item is 'To assist faculty and staff in using staff secure computer practice to safeguard College computing systems and data they store and access.' The second is 'To answer any questions about information security requirements and procedures' and the third is 'To promote Computer Security Awareness'.

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



The slide has a white background with a dark brown vertical bar on the right. The title 'What is IT Security Awareness?' is at the top in a dark serif font. Below the title is the sub-header 'Information Technology Security Awareness' in a bold font. Underneath is a paragraph defining IT Security Awareness as 'The understanding of the various information technology threats that exist in one's computing environment and taking responsible steps to guard against them.'

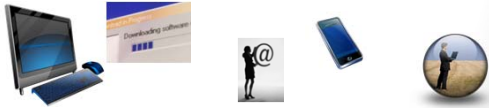
What is IT Security Awareness?

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.

