Welcome to the FSU Basic Cybersecurity Training. A cybersecurity tutorial for Florida State University students, faculty, and staff

Overview - Today we will talk about cyber threats, consequences, actions, cybersecurity at work and home, and university cybersecurity resources

Cyberthreats - First, let's talk about some common cyber safety threats and the problems they can cause.

Cyberthreats:
  - **Identity Thieves**
    People who obtain unauthorized access to your personal information—such as your FSUID, SSN, bank accounts and passwords. They use this to commit crimes such as fraud or theft.
  - **Hackers**
    Hackers are people who secretly get access to a computer system in order to steal information or cause damage.
  - **Malware**
    Malware (short for "malicious software") is any program or file that is harmful to a computer user, including computer viruses, worms, Trojans and spyware.
  - **Phishing**
    Phishing steals personal information by tricking you into clicking a link or entering your username & password. Phishing comes in many forms: emails, phone calls, website downloads.

Consequences - Defense against cybersecurity threats requires your action. If you do nothing, the results could be grave.

Consequences:
  - **Job Hindrances** - Loss of access to campus computing network, Inability to access files and do work
  - **Data Loss** - Loss of confidentiality and integrity, Loss of valuable university info or research, and Compromised personal data
  - **Disciplinary Actions** – Lawsuits, Loss of public trust, Loss of grant opportunities, Prosecution, Internal disciplinary action, Termination of employment
Actions – Follow these tips to protect yourself, others, and the university from common cybersecurity threats.

Actions – Top Eight Cybersafety Actions
- Protect Passwords
- Prevent Identity Theft
- Beware of Phishing
- Avoid Malware
- Run Antivirus Software
- Install Updates
- Back up Important Files
- Turn on Firewalls

According to the Pew Research Center, 64% of Americans have had personal information exposed by a data breach.

Protect Passwords
- NEVER share your passwords with anyone
- Avoid dictionary words
- Do not use common passwords, such as password1, abc123, qwerty1, letmein, yourname1
- Change your passwords periodically and when creating a password
  - Use at least eight characters
  - Mix uppercase and lowercase letters, numbers and symbols
  - Use mnemonics to help you remember a difficult password
  - Example: $e^^iNo1e = Seminole
  - Example: W00H!TCwontW$ = Woohoo! The Cubs won the World Series
- Use different passwords for different sites
- Store passwords in a safe place
  - Never keep passwords on a sticky note near your computer
  - Consider using a password vault such as LastPass or KeePass

Prevent Identity Theft
- Don’t give out Social Security numbers, driver license numbers, bank account numbers or other personal information unless you know exactly who’s receiving it
- Protect other people’s information as you would your own
- Never send personal or confidential information via email or instant message
- Every year, order a copy of your credit report from each of the three major credit bureaus—Equifax, Experian and Trans Union
  - www.equifax.com
  - www.transunion.com
  - www.experian.com

**Slide 12**

**Beware of Phishing**

- Phishing attacks steal personal information by tricking you into doing something, like clicking a link or entering your username and password. Phishing comes in many forms: emails, phone calls, website downloads. These phishing attempts may look like they are from Florida State University—often IT Services or the Service Desk—but don’t fall for the tricks! Follow these tips to help protect yourself from phishing attacks.
- **REMEMBER! FSU WILL NEVER ASK YOU FOR YOUR FSUID USERNAME AND PASSWORD IN AN EMAIL OR PHONE CALL.**

**Slide 13**

**Tips to Avoid Phishing Scams**

- **Be skeptical** of messages that require “immediate action” or threaten that you will lose something.
- Instead of clicking, **type website addresses** in your browser to access sites directly.
- Before clicking, **hover over or long tap a link** to display the true URL and see if it is linking to a reputable website.
- **Think before clicking** email and website links and never click a link that looks suspicious.
- **Do not open attachments** you aren’t expecting—especially ZIP files—and NEVER run .exe files.
- **Avoid providing personal information** over the phone, especially from an unsolicited call.
- **Never send credit card** or other sensitive information via email.
- **Use common sense.** If it looks like spam, then it probably is spam.

**Slide 14**

**Avoid Malware**

- Be wary of invitations to download software from unknown sources; even clicking advertisements can result in malware downloads like ransomware, spyware, and adware.
- Ransomware is a type of malware that prevents or limits users from accessing their system—either by locking the screen or encrypting the user’s files—unless a ransom is paid
- Spyware records your actions and keystrokes to steal your passwords and credit card numbers
- Adware not only slows your computer, but can track the sites you visit

**Slide 15**

Run Antivirus Software

- Antivirus software removes viruses and quarantines and repairs infected files and can help prevent future viruses
- Viruses can be transmitted via email, email attachments or IM
- To avoid computer problems caused by viruses, install and run an antivirus program like Norton, McAfee or Windows Defender
- Check to see if your antivirus solution is up to date by periodically opening your antivirus program and checking the last updated date

**Slide 16**

Install Updates

- Updates, also known as patches, fix problems with:
  - Operating systems (e.g., Windows 10, Mac OS X, Android and iOS)
  - Software (e.g., Microsoft Office, Creative Cloud)
  - Apps (e.g., Wells Fargo, The Weather Channel, Facebook)
- Most new operating systems are set to download updates by default.
- Work computers should update automatically. Check with your IT manager to make sure this is the case. Restart your computer after updates are installed so the patches can be applied immediately.

**Slide 17**

Back-Up Important Files

- Create back-up copies of your files to reduce the risk of losing important files to ransomware, a virus, computer crash, theft or disaster
- Save copies of your important documents and files to a flash drive, external hard drive or online back-up service
- Store your back-up files in a secure place away from your computer, in case of fire, theft or ransomware
- Test your back up files periodically to make sure the files are accessible and readable

**Slide 18**

Turn on Firewalls

- Firewalls act as protective barriers between computers and the Internet
- Hackers search the Internet by sending out computer messages to random computers and waiting for responses
- Firewalls prevent your computer from responding to these calls
- Check your computer's security settings for a built-in personal firewall and make sure it is turned on

**Slide 19**

Cybersecurity at work and home - Find out how to keep your information, computer, and other devices secure wherever you are.

**Slide 20**

Cybersecurity at Work

- Work with your IT manager before implementing new cybersecurity measures
- Talk with your IT manager about what cybersecurity measures are in place in your department
- Avoid opening links and attachments embedded in emails if you cannot verify the source.
- Use a cross-cut shredder to destroy documents containing sensitive information, such as non-directory student information, FSU proprietary documents and employee Social Security numbers.
- Report to your IT manager any cybersecurity policy violations, security weaknesses or any suspicious activity by unauthorized individuals in your work area
- Check with your IT manager before installing any programs on your work computer
- Take a moment to read the FSU information policies at its.fsu.edu/ispo/policy
- Avoid opening links and attachments embedded in emails if you cannot verify the source.

**Slide 21**

Cybersecurity at Home

- Never leave your laptop, tablet or phone unsupervised and in plain view
- Password protect all your devices
- Do not install unnecessary programs or apps on your computer or phone
- Install a firewall
- Run a full anti-malware scan regularly
- Watch what you share on social networks. Criminals can befriend you and easily gain access to a shocking amount of information.
- Adhere to copyright restrictions when downloading software, games, movies or music.
- Use a separate account for each family member
  - Set up each account as a standard account
  - Have a separate account with administrator privileges
  - Don't use the administrator account for everyday actions
- Set a screen time-out
- Be careful what info you share on the phone. If someone calls you asking for sensitive information, it's okay to say no. Call the company directly to verify credentials before giving out any info.
- Always be careful when clicking email attachments or links. If it's unexpected or suspicious for any reason, don't click on it.

**Slide 22**

University cybersecurity resources - Find out more about cybersecurity at Florida State University

**Slide 23**

University Cybersecurity Resources

- For more info about cybersecurity at Florida State University, visit [its.fsu.edu/ispo](https://its.fsu.edu/ispo)
- Follow us on Twitter @floridastateITS

**Slide 24**

Contact

- Information Technology Services
  Information Security & Privacy Office
  Florida State University
  [its.fsu.edu/ispo](https://its.fsu.edu/ispo)

- Philip Kraemer, Training Coordinator
  [pkraemer@fsu.edu](mailto:pkraemer@fsu.edu)

- Feel free to contact us with questions or comments on information security or privacy at Florida State University.