INFORMATION TECHNOLOGY SERVICES

FSU BASIC CYBERSECURITY TRAINING

A cybersecurity tutorial for Florida State University students, faculty and staff

OVERVIEW

- Cyberthreats
- Consequences
- Actions
- Cybersecurity at Work and Home
- 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
- 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

64% of Americans have had personal info exposed by a data breach

Pew Research Center

PROTECT PASSWORDS

- NEVER share your passwords with anyone!

- Create strong passwords that are difficult to guess
  - 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, text message, 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

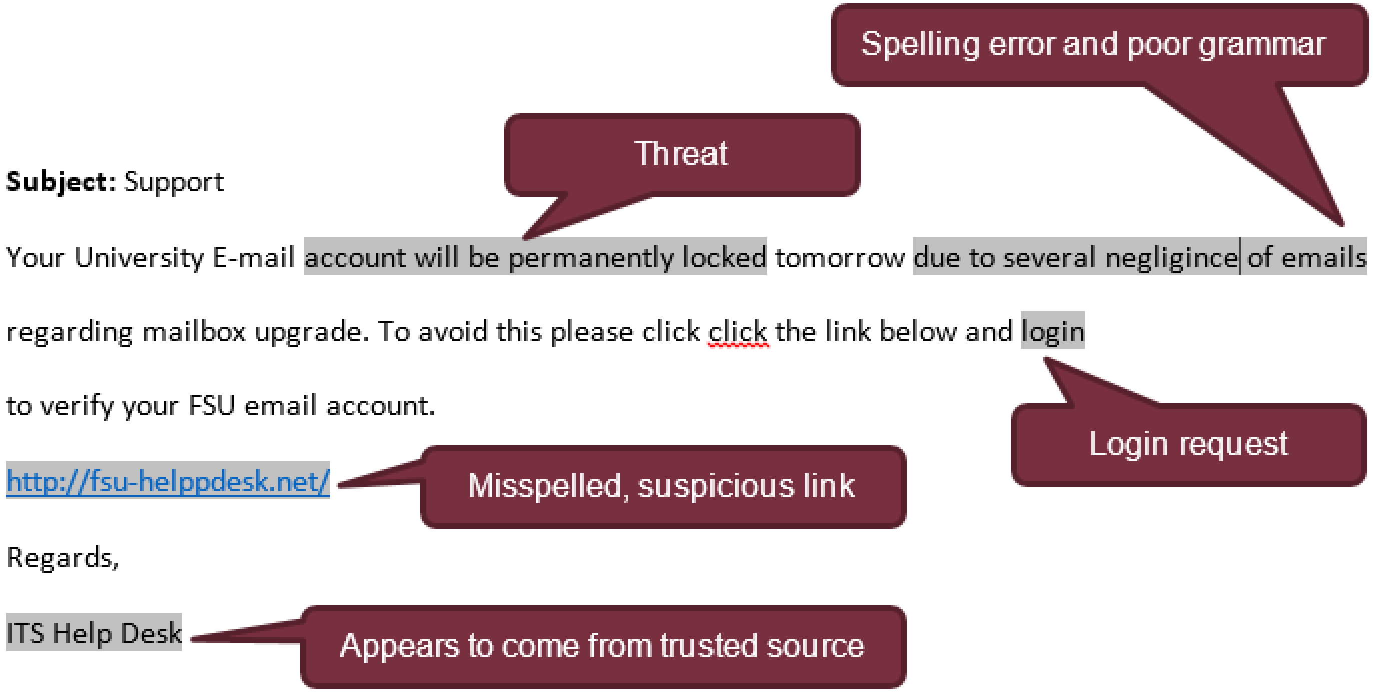
  - www.equifax.com
  - www.transunion.com
  - www.experian.com

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.**

PHISHING EXAMPLES



Subject: Support

Your University E-mail account will be permanently locked tomorrow due to several negligince of emails regarding mailbox upgrade. To avoid this please click click the link below and login to verify your FSU email account.

http://fsu-helppdesk.net/

Regards,

ITS Help Desk

Spelling error and poor grammar

Threat

Login request

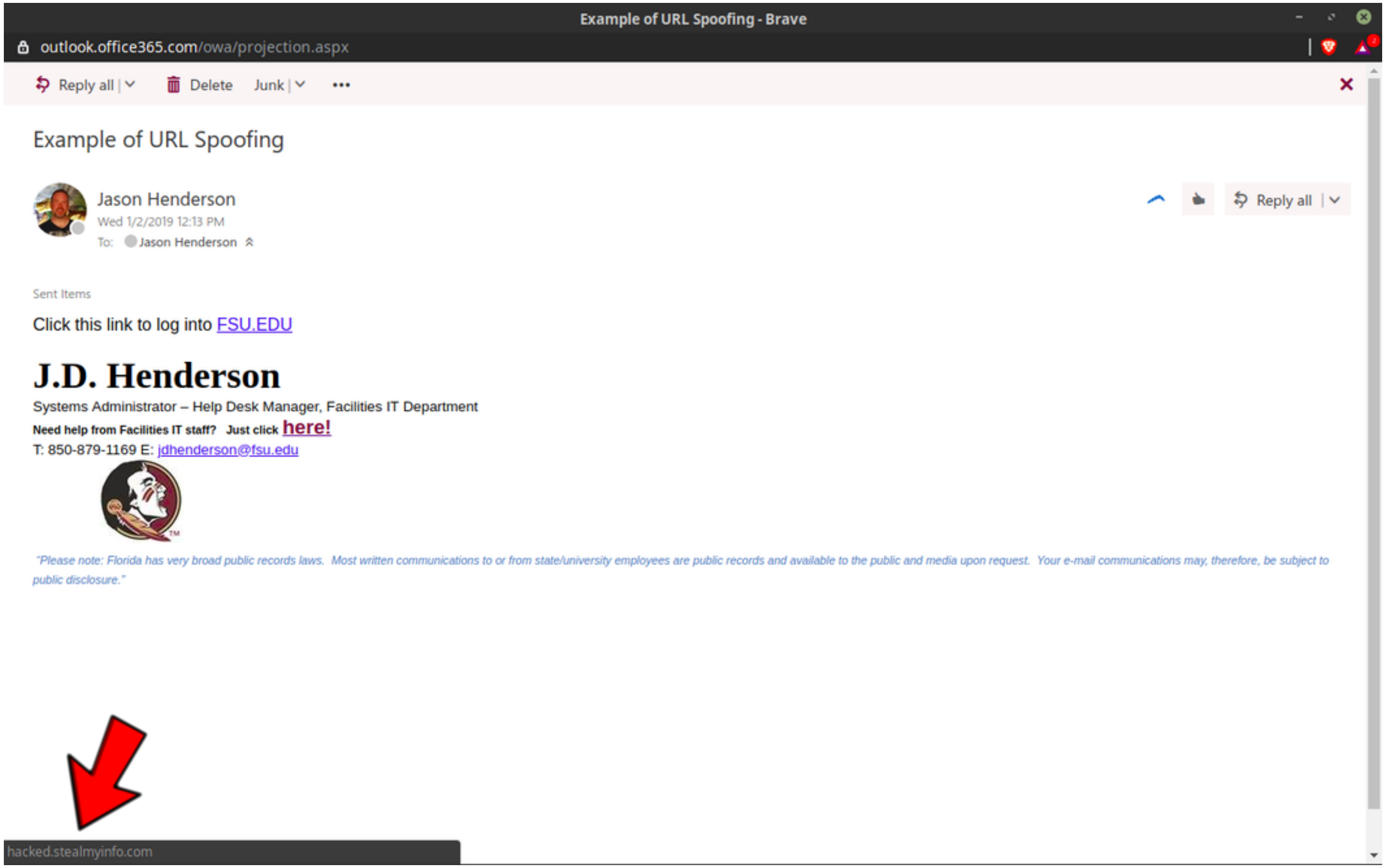
Misspelled, suspicious link

Appears to come from trusted source

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 you don’t trust.
- **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.

EXAMPLE OF PHISHING SCAM


Example of URL Spoofing - Brave
outlook.office365.com/owa/projection.aspx
Reply all
Delete
Junk
Reply all

Example of URL Spoofing

Jason Henderson
Wed 1/2/2019 12:13 PM
To: Jason Henderson

Sent Items

Click this link to log into FSU.EDU

J.D. Henderson
Systems Administrator – Help Desk Manager, Facilities IT Department
Need help from Facilities IT staff? Just click here!
T: 850-879-1169 E: jdhenderson@fsu.edu

"Please note: Florida has very broad public records laws. Most written communications to or from state/university employees are public records and available to the public and media upon request. Your e-mail communications may, therefore, be subject to public disclosure."

hacked.stealmyinfo.com

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, credit card numbers, and other confidential information

- Adware not only slows your computer, but can track the sites you visit

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

INSTALL SOFTWARE AND SECURITY 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.

BACK UP IMPORTANT FILES

- Create offline 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

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
  - Mac Firewall
  - Microsoft Firewall

CYBERSECURITY AT WORK AND HOME

Find out how to keep your information, computer, and other devices secure wherever you are.

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 and other private information
- 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

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 on your home network and PC
- 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.

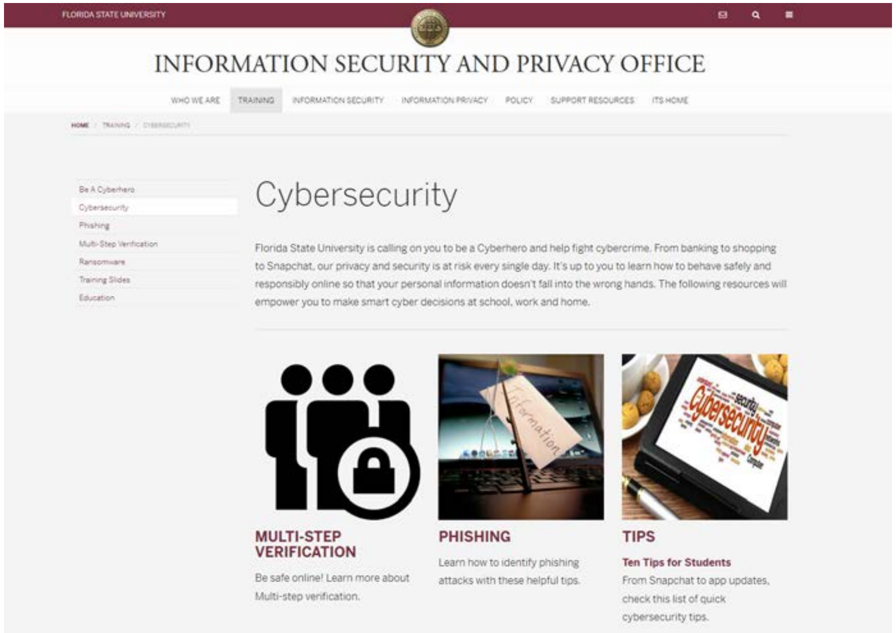
UNIVERSITY CYBERSECURITY RESOURCES

Find out more about cybersecurity at Florida State University

UNIVERSITY CYBERSECURITY RESOURCES

- For more info about cybersecurity at Florida State University, visit its.fsu.edu/ispo

- Follow us on Twitter @floridastateITS



INFORMATION SECURITY AND PRIVACY OFFICE

Cybersecurity

Florida State University is calling on you to be a Cyberhero and help fight cybercrime. From banking to shopping to Snapchat, our privacy and security is at risk every single day. It's up to you to learn how to behave safely and responsibly online so that your personal information doesn't fall into the wrong hands. The following resources will empower you to make smart cyber decisions at school, work and home.

MULTI-STEP VERIFICATION

Be safe online! Learn more about Multi-step verification.

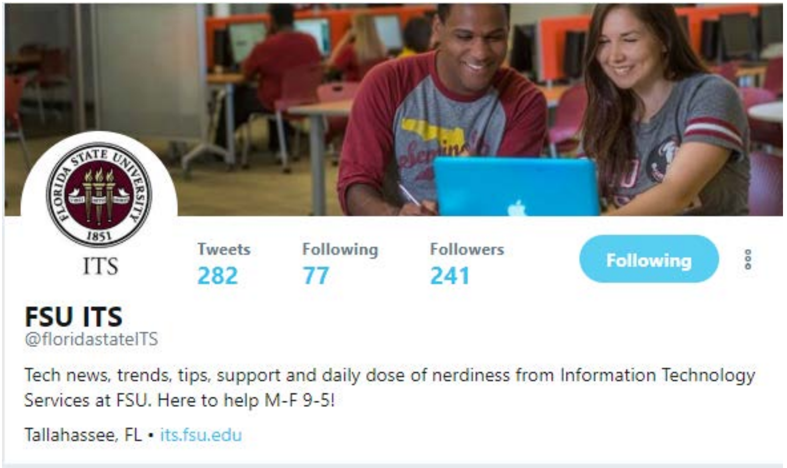
PHISHING

Learn how to identify phishing attacks with these helpful tips.

TIPS

Ten Tips for Students

From Snapchat to app updates, check this list of quick cybersecurity tips.



Tweets 282 Following 77 Followers 241

FSU ITS
@floridastateITS

Tech news, trends, tips, support and daily dose of nerdiness from Information Technology Services at FSU. Here to help M-F 9-5!

Tallahassee, FL • its.fsu.edu

CONTACT

Information Technology Services

Information Security & Privacy Office
Florida State University
cybersecuritytraining@fsu.edu
its.fsu.edu/ispo

Philip Kraemer, Training Coordinator
pkraemer@fsu.edu

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