Email Security: Preventing disclosure at work and at home

Information Security Office

2018 National Cybersecurity Awareness Month

South Texas College

Opening Statement

NCSAM was started in 2004

FACT: 92.4% of malware is delivered via email*

FICTION: if your password is stolen you have time to reset it

* Verizon 2018 Data Breach Investigations Report

The time it takes cybercriminals to compromise a system is often a matter of minutes or even seconds*

NCSAM 2018 Campaign

- Make Your Home a Haven for Online Safety
- Millions of Rewarding Jobs: Educating for a Career in Cybersecurity
- It's Everyone's Job to Ensure Online Safety at Work
- Safeguarding the Nation's Critical Infrastructure

Email Security

RISKS

- Disclosure
- Impersonation (Identity Theft)
- Legal Issues
- Breach By Proxy
- Privacy

Email Security

- DO: Keep separate work and personal email accounts.
- DO: Secure your accounts using multi-factor authentication.
- DO: Know how to classify data that you own or handle.
- DO: Protect your mobile devices with a PIN or password.

- DO NOT: Use the same password for your work and personal email.
- DO NOT: Use public computers to log into your accounts.
- DO NOT: Send confidential information over unsecure email.
- DO NOT: Forward work email to your personal email account.

Data Classification Categories

CLASSIFICATION CATEGORY	EXAMPLES
Confidential	• Student academic records (grades, class schedules and/or GPA) • Personally identifiable information (PII) protected by FERPA or Texas Law (with or without social security numbers) • Federal Tax Information (FTI) • Counseling and health records (HIPAA) • Credit card information (PCI) • Private individual financial information (GLBA) • Aggregate data without disclosure avoidance methods • Departmental data that needs to be kept private • Information that we are bound to protect by a legally-binding agreement • Data protected by CJIS (Criminal Justice Information Services) Security Policy • Data classified as Controlled Unclassified Information by the federal government • Information related to security or infrastructure issues for computers, which is confidential through Section 552.139 of the Texas Government Code
Restricted	• Directory data for students that opted-out from disclosure • Public information requested outside of the official process
Public	• Course listing information • Aggregate data with disclosure avoidance methods • Employee directory • Public information requested through the official process

Acceptable Storage Locations

STORAGE LOCATION	CONFIDENTIAL	RESTRICTED	PUBLIC
College Desktop	Only if the disk is encrypted	Only if the disk is encrypted	Yes
College Laptop	Only if the disk is encrypted	Only if the disk is encrypted	Yes
College Smartphone/Tablet	Only if compliant with mobile device standard	Only if compliant with mobile device standard	Yes
College Email	No	Yes	Yes
Personal Email	No	No	Yes
Portable Storage (USB)	No	No	Yes
IT Network Storage	Yes	Yes	Yes
Secure Share (LiquidFiles)	Yes	Yes	Yes
College Cloud Storage (OneDrive)	Only class grade books	Yes	Yes
Personal Cloud Storage	No	No	Yes
Personal Computer	No	No	Yes
Personal Smartphone/Tablet	Only if compliant with mobile device standard and while employed by STC	Only if compliant with mobile device standard and while employed by STC	Yes
College Website	No	No	Yes

Educating for Cybersecurity

Assoc. of Applied Science - Cybersecurity Specialist

This hands-on degree offers practical experience in a wide array of information security and digital forensics situations that are applicable to the real world. The student will be exposed to everything from how to properly conduct an assessment, and secure and document a network. In addition, the student will learn how to establish a proper chain of custody that is admissible in a court of law when recovering files from intentionally damaged media.

CITP 4346 - Cyber Law and Digital Forensics

This course presents the laws and legal issues that impact law enforcement, businesses, and investigators when preserving, collecting, and analyzing digital data and evidence of computer crimes. Students will examine the tools and techniques required to conduct a successful investigation of illegal activities related to information technology.

CITP 4347 – Principles of Cybersecurity

This course introduces the basic concepts and principles of cybersecurity and the fundamental approaches of securing systems. Its main topics include: security basics, security management, risk assessment, software security, operating systems security, cryptography protocols, network authentication, security network applications, malware, network threats and defenses, web security, mobile security, cloud computing, virtualization, ethical issues and privacy.

Awareness Campaign Links

AxCrypt – File Encryption Software	https://www.axcrypt.net/information/how-to-use/
DUO Security How-To	https://iso.southtexascollege.edu/howto-duo-security/
Gmail Confidential Mode	https://support.google.com/mail/answer/7674059?co=GENIE.Platform%3DDesktop&hl=en
Gmail Multi-Factor Authentication Set Up	https://www.google.com/landing/2step
National Cyber Security Alliance - Stay Safe Online	https://staysafeonline.org/stay-safe-online
O365 - Microsoft Authenticator App	https://docs.microsoft.com/en-us/azure/active-directory/user-help/microsoft-authenticator-app-how-to
SecureShare (LiquidFiles)	https://secureshare.southtexascollege.edu

Questions and Answers

"Cybersecurity is our shared responsibility."

Information Security Office
infosec@southtexascollege.edu
956-872-2335