Why is this training necessary?

Basic cybersecurity awareness training is mandated by the State of Texas Administrative Code (TAC). Your participation in this training fulfills that state requirement. Throughout the brief training, we hope to provide questions and answers for you to gauge your own cybersecurity awareness.

Cybersecurity Awareness Training

We Are *All* Responsible. . .

Every employee has a responsibility to protect Springtown ISD's confidential data and information resources. Your partnership is critical to our Instructional Technology (IT) and network security goals and strategies.

Board Policies related to technology resources can be found here: https://pol.tasb.org/Home/Index/983

Our Employee Handbook addresses general technology expectations/requirements here (see p. 43): https://www.springtownisd.net/cms/lib3/TX21000442/Centricity/Domain/35/2019-2020%20Employee%20Handbook.pdf

Confidential Information—Personally Identifiable Information

- Information identifying personally owned property, such as vehicle registration number or title number and related information

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Sensitive Information

- Information that could lead to breach of data systems/protections/controls
  - Account credentials
  - Information regarding the structure/configuration of security controls
  - Some policies/procedures needed to gain access to resources
- Information that is considered the trade secrets of an organization
- Intellectual Property
- Any other information an organization considers private and/or does not wish to make publicly available

Acceptable Use

Information Resources are State of Texas strategic assets that must be managed as valuable resources:

- To ***ensure compliance*** with applicable statutes, regulations, and mandates regarding the management of information resources
- To ***establish*** prudent and acceptable ***practices*** regarding the use of information resources
- To ***educate individuals*** who may use information resources associated with SISD job responsibilities

Protect your personal information

Local policy does not prohibit staff members from using district-owned computers and access points for legitimate and appropriate personal business.

Each employee is responsible for protecting their personal information while using district resources. The Federal Trade Commission offers guidance through "Onguard Online," available through this link:

https://www.consumer.ftc.gov/media/video-0023-five-ways-help-protect-your-identity

Authorized Software

Information Resources are State of Texas strategic assets that must be managed as valuable resources:

- Any software installed or copied on any district-owned technology resource (TR) must be legally licensed and managed
- The following general categories of software are prohibited on all Springtown ISD technology resources, unless authorized by the District's Chief Technology Officer (CTO) or Superintendent:

  a. Hacking tools, password descramblers, network sniffers, and port scanners.
  b. Software that proxies the authority of one user for another, for the purpose of gaining access to systems, applications, or data illegally.
  c. Software that instructs or enables the user to participate in any activity considered a threat to local, state or national security.

- The CTO and/or campus-level TAG staff may provide a list of prohibited software and may add to the list as new threats are discovered

Cybersecurity Awareness Training

Email

Phishing emails are designed to trick you into giving away your springtownisd.net username and password to computer hackers on the Internet. Springtown ISD will **NEVER** email to ask you for your username and password.

If you have responded to one of these emails and **provided your springtownisd.net username and password**, please contact our Technology Department immediately via 817-220-2565

If you receive phishing emails but did not click on any links, then simply delete the email - no further action is needed.

Cybersecurity Awareness Training

Email

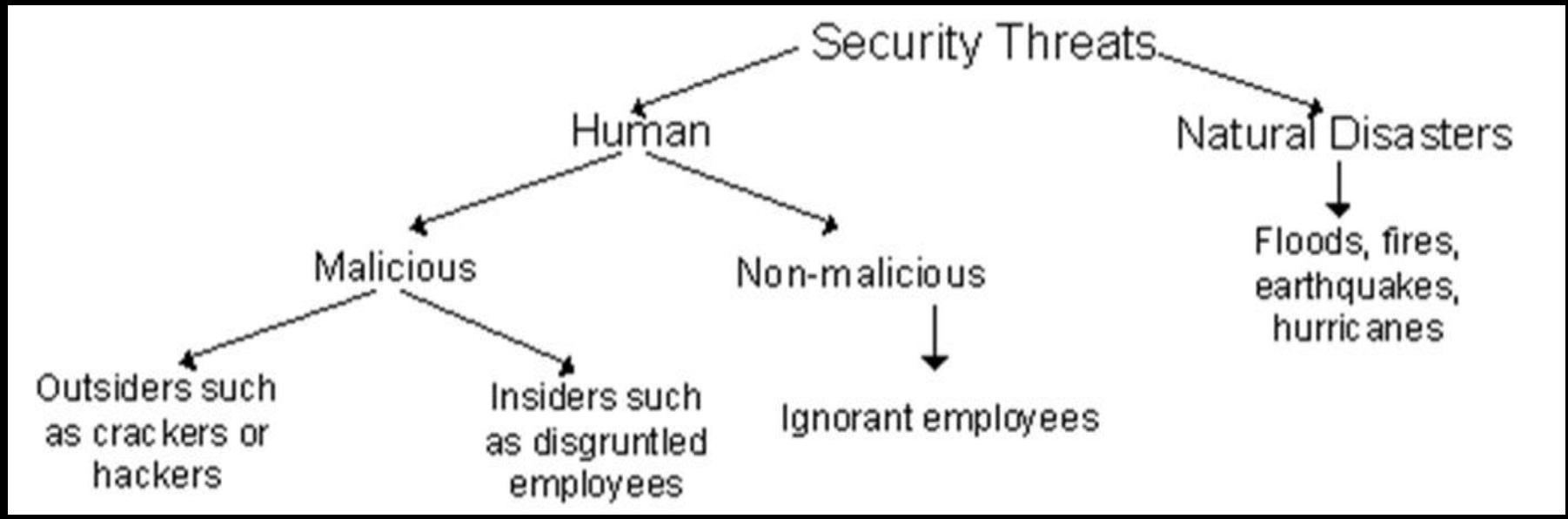
Springtown ISD's Technology Department recommends the following cybersecurity practices to protect yourself and SISD resources from this and other email scams:

- Do not click on links contained within an email unless you are certain of the sender's identity and expecting the information;
- Do not open attachments unless you are certain of the sender's identity and expecting the information;
- Delete and do not reply to any suspicious or suspect emails;
- Update your desktop, laptop, and/or mobile device anti-virus software; and

Which of the following is a suspicious email?

a) An unexpected message from an International Prince indicating that he would like to share his inheritance with me.
b) An email from a bank that I haven't used in years, but they claim they need my account information to process a transaction.
c) An email from a Russian beauty queen, who is looking for my assistance in finding an American husband.
d) A threatening communication from the IRS indicating that my taxes are overdue, and will be pressing charges if I don't log in a provide my Information.
e) All of the above.

Where Do Technology Security Threats Come From?



Criminals and Intentions

Data and information resource theft can be motivated by:

- Money/profit
- Revenge/retaliation
- Political gain
- Special cause activism (Hacktivism)
- Hate
- National security (domestic and international)
- Fun/excitement/self-aggrandizement

Understanding Risk

Risk = Threat x **Vulnerability**

Bottom Line:

The security posture of the District's information systems is directly relatable to the **risk**

Risks and Threats

Extortion	• Email scams (phishing)
Loss of intellectual property/data	• Email scams • Malware • Malicious Websites
Disruption of Services	• Advanced techniques typically aimed at institutional resources

Risks and Threats

Distort accountability	• Reputational hits • Legal accountability
Data corruption	• Impact operations or customers through data
Terrorism	• Focused attacks coordinated with physical attacks

Incident Management - Procedures

Should you become aware of a data security issue, immediately report the incident:

- For virus and/or worm infections, compromised systems, or improper use complaints, contact the District's Technology Department at 817-220-2565 or CTO Robert McHenry via rmchenry@springtownisd.net

- For potential criminal acts (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact either
  1) the Technology Department or
  2) Superintendent Mike Kelley at 817-220-1700

Internet Use

- Springtown ISD internet or intranet access may not be used for personal gain, political gain, nor for personal solicitations.
- No data considered confidential or sensitive will be made public.
- Confidential material transmitted over an external network must be encrypted.
- Electronic files must be retained and destroyed in accordance with State records retention schedules.
- Incidental use must not result in direct costs to Springtown ISD or interfere with the normal performance of an employee's work duties.

Internet Use Policy

- Files downloaded from the Internet must be scanned for viruses using District-approved virus detection software with up-to-date virus definition files.
- Software that uses the Internet must incorporate vendor-supplied security patches.
- Websites and applications must comply with SISD's *Acceptable Use Policy*.
- **All** user activity on the District's network and/or technology resources are subject to logging and review.

Cybersecurity Awareness Training

Multi-Functional Device Hardening

The advancement and innovation of copier/printer/scanner/fax technology has created a breed of devices commonly called "**Multifunctional Devices** (MFD)." Certain features associated with these devices can pose a serious infrastructure and information security risk.

Cybersecurity Awareness Training

Multi-Functional Device Hardening

Certain features associated with these Multi-functional devices (MFDs) can pose a serious infrastructure and information security risk. As with all other Information Resource, MFDs must be managed in a secure manner to assure protection against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information.

Which of the following can cybercriminals use to gain access to confidential information?

a) Printer
b) Network-attached copiers
c) Scanners
d) Fax Machines
e) All of the above

Personal laptops, mobile devices, and desktops that connect to the Springtown ISD Network are subject to the District's monitoring, security, and management standards

a) True
b) False

It is acceptable to share passwords with IT staff or other trusted individuals

a) True
b) False

Your account passwords must never be divulged to anyone. Springtown ISD staff members will not ask for user account passwords, and neither should anyone from outside the District. If you experience someone requesting your password to software or hardware owned or managed by the District, please report the incident immediately to **CTO Robert McHenry at 817-220-2565**

Cybersecurity Awareness Training

Mobile Computing

Just as your desktop computer can become infected and overrun by malicious intruders, so can your mobile devices. Awareness of what you are doing and where you're visiting, as well as using safe computing practices, can help protect mobile device activity.

- Enable PIN, passcode, or biometric access to the mobile device;
- Maintain up-to-date software, including operating systems and applications;
- Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi;
- Set Bluetooth-enabled devices to "non-discoverable," so that unauthenticated devices cannot detect them;
- Avoid joining unknown Wi-Fi networks;
- Don't install apps you don't need and delete unused apps;
- Delete all information stored in a device prior to discarding it;
- Do not leave your mobile device unattended.

Public Wi-Fi Networks

Many mobile devices offer services beyond making phone calls, texting, and receiving e-mail. With such a wide variety of mobile devices and options for connectivity, we strongly recommend that you exercise caution and diligence about practicing safe computing.

Cybersecurity Awareness Training

Mobile computing devices are generally not secure and inherently at risk for data loss. As such, information considered _____ should not be stored on a mobile computing device.

a) Confidential or sensitive
b) Syllabus
c) Marketing
d) Course catalog
e) All of the above

Privacy Policy

Privacy Policies are used to establish the limits and expectations for the users of Springtown ISD's technology resources. Internal users should have no expectation of privacy with respect to technology resources.

Privacy Policy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Springtown ISD are not private. The District has stringent policies, procedures, and monitoring for all technology staff members. We adhere to a rigorous check-and-balance system and are subject to periodic internal and external audits.

Integrity and high ethical codes of conduct are cornerstones of our security program.

Privacy Policy

A wide variety of third parties have entrusted their information to Springtown ISD for business purposes, and all our employees must safeguard the privacy and security of this information. Student and employee data is confidential, and access will be strictly limited.

Emails in my inbox and files I have created and stored on TTU-owned/provided information resources are my personal property.

a) True
b) False

Cybersecurity Awareness Training

It is Springtown ISD's responsibility to safeguard and secure each student's personal information, and as an employee of Springtown ISD, I share in this responsibility.

a) True
b) False

Malware Detection

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Cybersecurity Awareness Training

Malware Detection

A **virus** is capable of replicating and spreading to other computers by attaching to messages or programs when a recipient opens the message or launches the program.

A **Trojan Horse** lures you into clicking or downloading the file, they cleverly infect your computer system. In some cases the malicious application makes your system and data available to criminals all over the world, without your knowledge.

Keyloggers covertly record your keystrokes as you type in your various applications, and allow criminals to collect your usernames and passwords.

Adware is malware disguised as advertising or used to generate revenue by an advertiser. Many scam artists use pop-up ads on websites to attract victims.

Ransomware is a form of malware that limits you from accessing your files and information until the “ransom” is paid to remove the restrictions. Frequently, access is not restored even after the “ransom” is paid.

A virus is software/application that securely manages my data.

a) True
b) False

Data and Technology Equipment Disposal

As equipment and resources “age out,” it is extremely important that employees contact the Technology Department for removal and, when appropriate, disposal. ***Environmental and data security concerns must both be addressed by the Technology department*** *before any equipment leaves the District, whether as “surplus property” or through disposal.*

We Are *All* Responsible…

Additional information is available through https://www.stopthinkconnect.org