Health.edu
Texas Tech University Health Sciences Center

Cybersecurity Awareness Training

General Staff Education I 46120

Mandated by State of Texas

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

We Are *All* Responsible. . .

Each of us has the responsibility to protect our workplace's confidential data and information resources. Your partnership is critical to our institutional IT security goals and strategies.

Review all established policies for IT security at your facility.

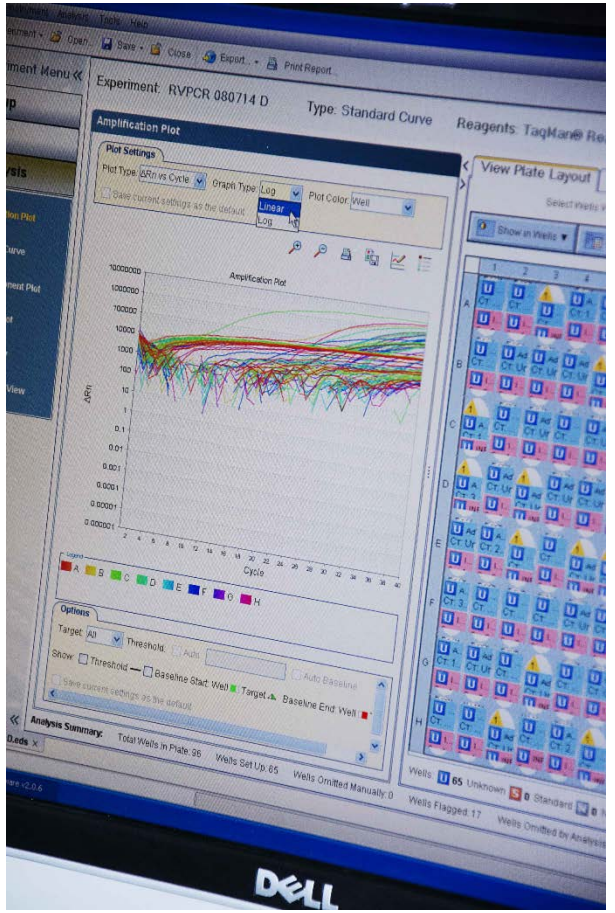
CDC/Holly Patrick, MS, MPH

Confidential Information—Personally Identifiable 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).
- Information identifying personally owned property, such as vehicle registration number or title number and related 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



CDC/Jessie Blount

Acceptable Use

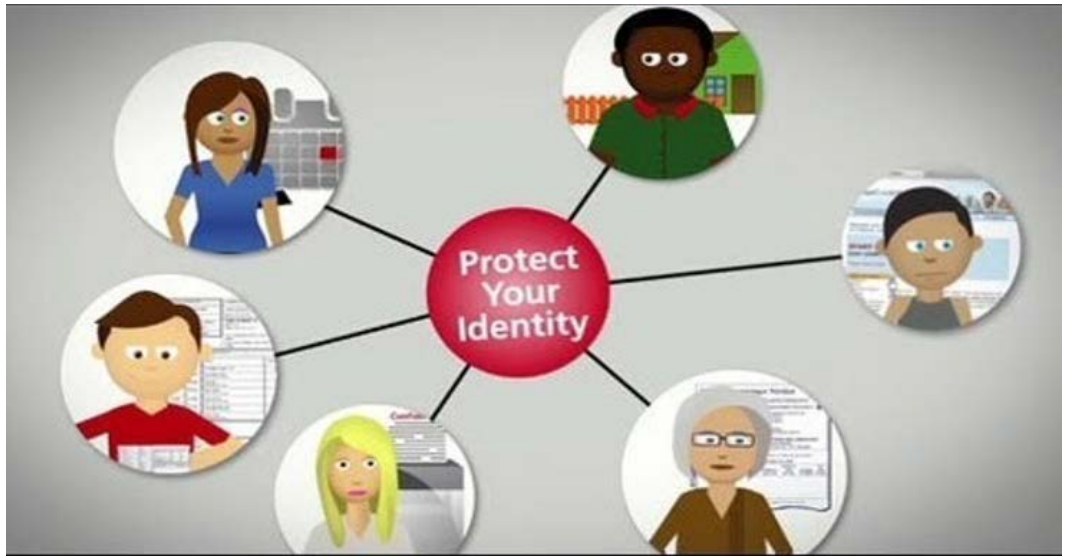
Information resources are State of Texas strategic assets that must be managed as valuable resources:

- 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 their job responsibilities.

CDC/Sally Ezra

Protect Your Personal Information

Federal Trade Commission. Onguard Online. Retrieved from https://www.consumer.ftc.gov/media.



- Take a moment to view Video 1:
  Protecting Personal Information – Five Ways to Help Protect Your Identity by the Federal Trade Commission
  - Watch at either:
    - FTC website https://www.consumer.ftc.gov/media/video-0023-five-ways-help-protect-your-identity
    - YouTube https://youtu.be/lp_8cvNm_vE

Authorized Software

- Any software installed or copied on any Information Resource must be legally licensed and managed.
- The following general categories of software are prohibited on all workplace information resources, unless authorized by your facility's IT Security Officer:

    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.

- Your IT department/IT Security Officer will provide a list of prohibited software and may add to the list as new threats are discovered.

Business/Research Partner Access

Business partners play an important role in the educational research and outreach strategic priorities at your facility. Many times, these partners will need access to information resources and data. Partners must:

- Have a legitimate educational or business purpose;
- Comply with all operating policies, including the IT security policies;
- Provide a governmental-issued identification card; and
- Only have access to the data required for the business purpose.

Email

Phishing emails are designed to trick you into giving away your username and password to computer hackers on the Internet. Your workplace will **NEVER** ask you for your password.

If you have responded to one of these emails and **provided your username and password**, please change your password immediately, and contact your IT department for additional assistance.

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

Email

The following cybersecurity practices are recommended to protect yourself and your workplace's 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
- Keep current on critical system updates:
    - Windows Users: Contact your IT department
    - Mac Users: Contact your IT department

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips at:
https://www.ready.gov/cybersecurity
https://us-cert.cisa.gov/ncas/tips
https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

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.

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.

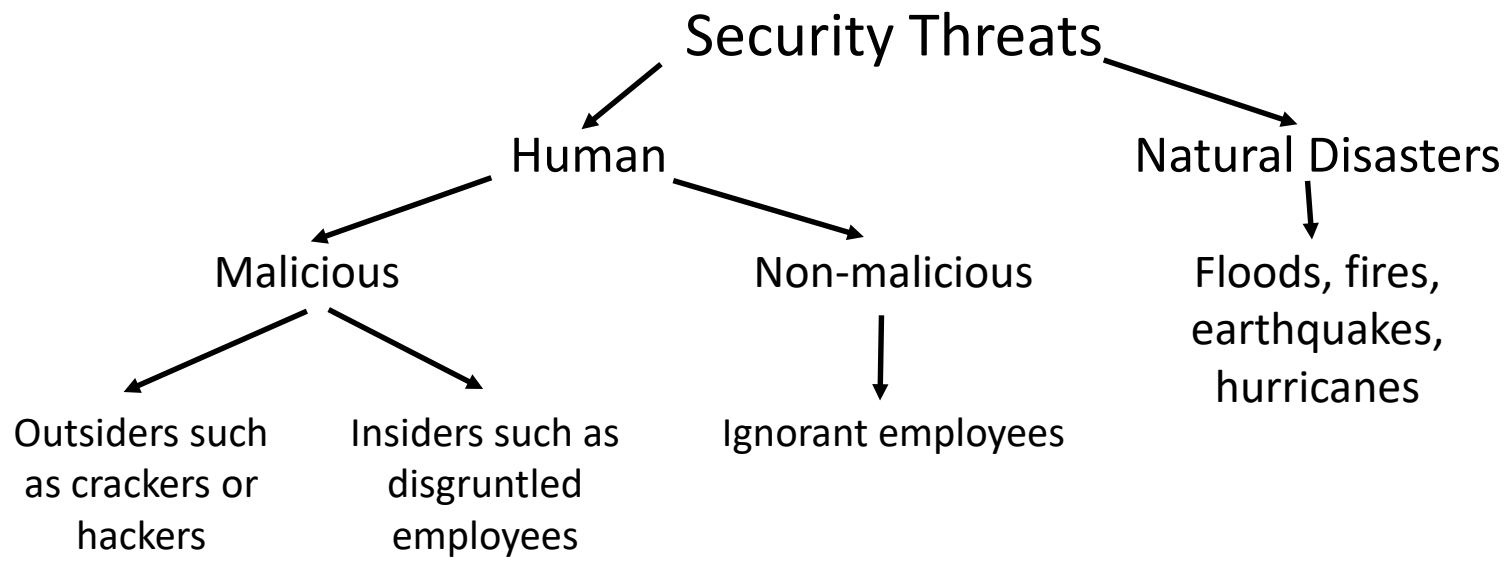
e) All of the above.

As a reminder; the following cybersecurity practices are recommended to protect yourself and your workplace's 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
- Keep current on critical system updates.

Where Do IT Security Threats Come From?

Schudel & Smith (Cisco), 2008



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 workplace'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

Your workplace has procedures in place for reporting computer security incidents as outlined in your policies, which you should review.

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

- For virus & worm infections, compromised systems, or improper use complaints, contact your **IT Department**;
- For potential criminal acts (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact your **IT Department, Information Security Officer, Chief Information Officer, or Information Resources Manager.**

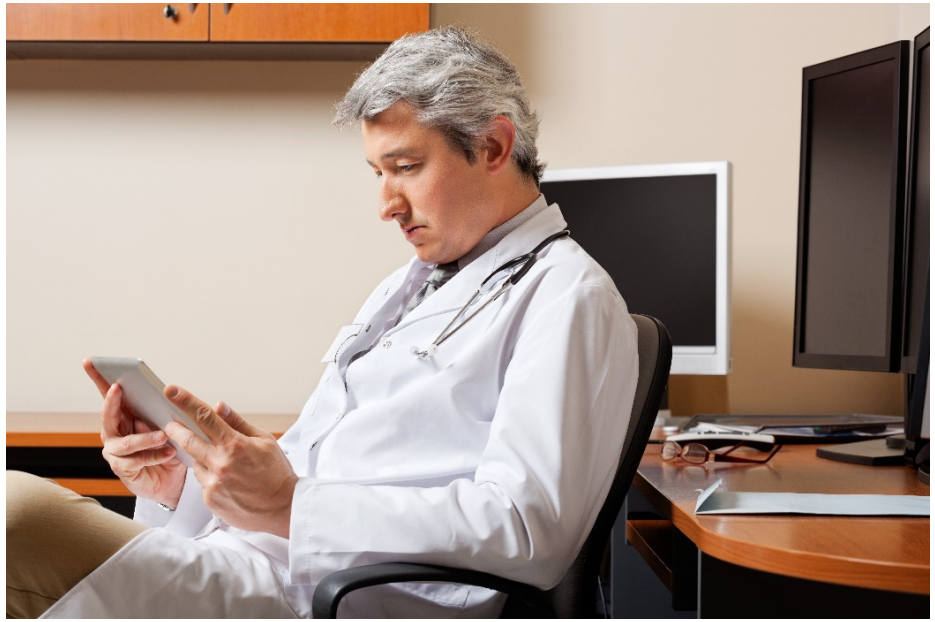
Internet Use Policy

- Software that uses the internet must incorporate vendor-supplied security patches.

- Files downloaded from the Internet must be scanned for viruses using approved IT virus detection software with up-to-date virus definition files.

Internet Use Policy

- Websites and applications must comply with your workplace's acceptable use policy.
- All user activity on your facility's information resources assets is subject to logging and review.
- All workplace IT services accessed via the internet, hosted locally or elsewhere (with prior workplace IT approval), must comply with the internet use policy.



Internet Use

- Your workplace’s internet or intranet access may not be used for personal gain, political gain, or non-workplace personal solicitations.
- No workplace confidential or sensitive data will be made public.
- All confidential workplace 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 your workplace or interfere with the normal performance of an employee's work duties.

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.

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

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

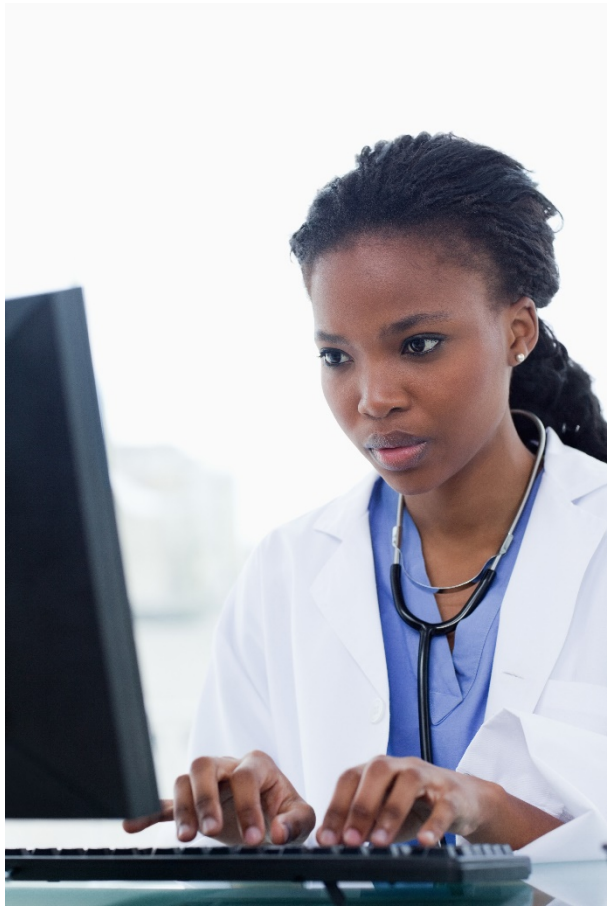
a) Printer
b) Network-attached copiers
c) Scanners
d) Fax machines
e) All of the above

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.

Personal laptops, mobile devices, and desktops that connect to the workplace network are subject to your facility's IT monitoring, security, and management standards.

a) True

b) False



Personal laptops, mobile devices, and desktops that connect to the workplace network are subject to your facility's IT monitoring, security, and management standards.

---

a) **True**

b) False

All hardware connected to the your workplace's network is subject to your facility's IT management, security, and monitoring standards.

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

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. IT staff and IT business partners will not ask for user account passwords and neither should anyone else. If you experience someone requesting your password, please report the incident immediately to the Information Security Officer in the IT Department.

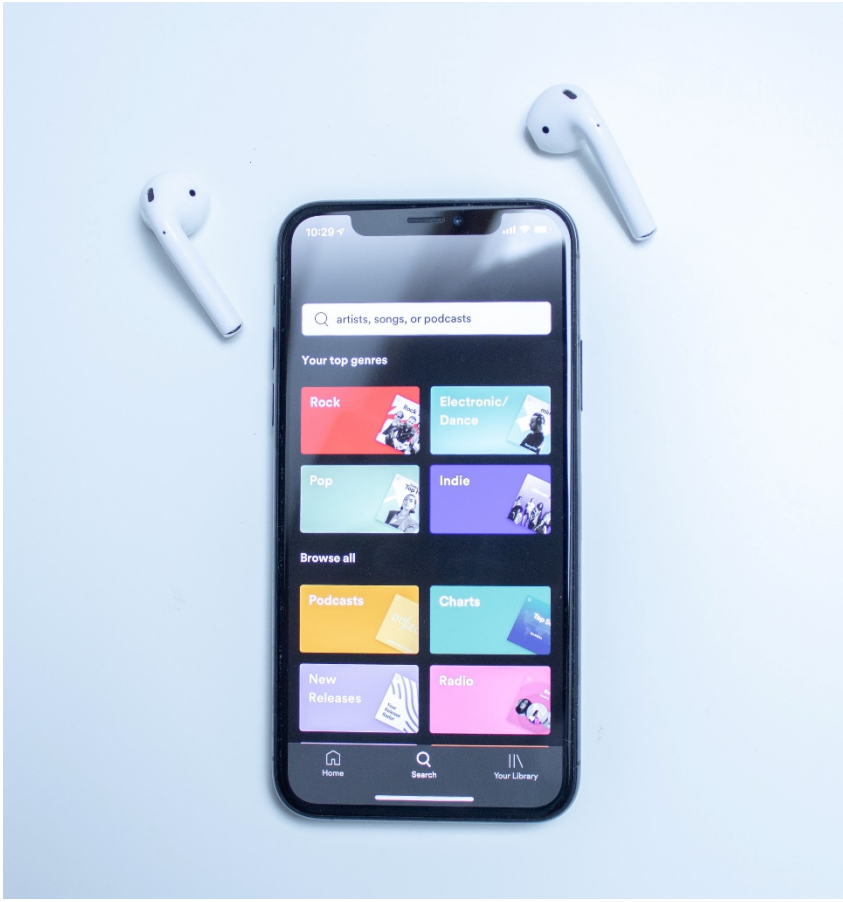
Mobile Computing

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;

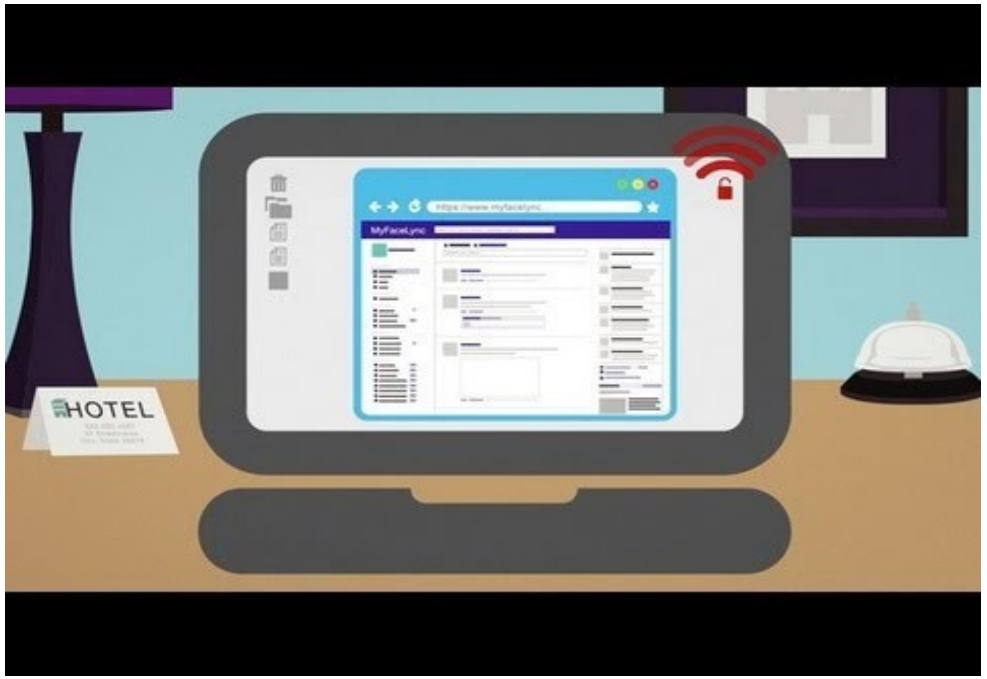
Mobile Computing

- 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

Federal Trade Commission. Onguard Online. Retrieved fromhttps://www.consumer.ftc.gov/media.



- Take a moment to view Video 2:
  Public Wi-Fi Networks – Federal Trade Commission
  - Watch at either:
    - FTC website https://www.consumer.ftc.gov/media/video-0080-public-wi-fi-networks
    - YouTube https://youtu.be/bzoEy-t8Y-8

Mobile computing devices are generally not secure and inherently at risk for data loss. As such, your workplace's _____ information 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

Mobile computing devices are generally not secure and inherently at risk for data loss. As such, your workplace's _____ information 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

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

Privacy Policy

CDC / Jessie Blount

Privacy policies are used to establish the limits and expectations for the users of workplace information resources. Internal users should have no expectation of privacy with respect to information resources.

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

---

a) True

b) False

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

a) True

b) False

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of your workplace are not private. The IT Department has stringent policies, procedures, and monitoring for all staff. 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.

It is the responsibility of my workplace to safeguard and secure personal information, and as an employee, I share in this responsibility.

---

a) True

b) False

It is the responsibility of my workplace to safeguard and secure personal information, and as an employee, I share in this responsibility.

---

a) **True**

b) False

A wide variety of third parties have entrusted their information to your workplace for business purposes, and all workers at your facility must safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on business need for access.

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.

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.

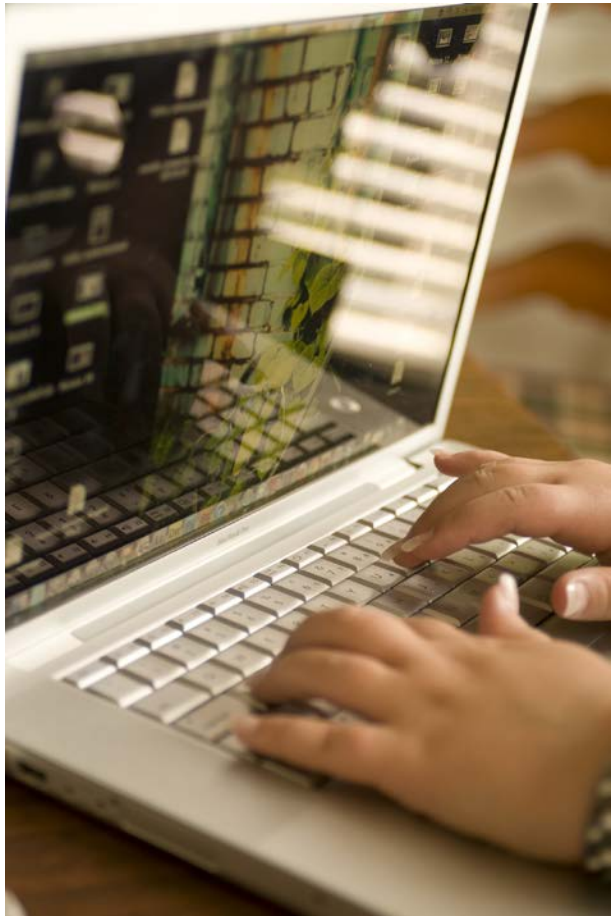
CDC/Debora Cartagena

- **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



CDC / Amanda Mills

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

a) True

b) False

A **virus** is one of the most common types of malware. They are capable of replicating and spreading to other computers by attaching to messages or programs when a recipient opens the message or launches the program.

Data and IT Equipment Disposal

- Other departments may be interested in receiving outgoing computing equipment before it reaches property surplus.

- Technology exchanges between departments make institutional technology investments last longer, extending the use of computing equipment.
  - Individuals must be authorized by the department head to post or review listed computing equipment.
  - Inventory transfer paperwork and procedures are required prior to the exchange.

- As with any equipment transfer, all operating policies and procedures apply; please view your facility's relevant policies.

- When equipment finally leaves the facility, it must be done through surplus property for adherence to State of Texas requirements.

We Are All Responsible

National Cyber Security Alliance. Stop. Think. Connect. Retrieved from https://www.stopthinkconnect.org.

- Take a moment to view Video 3: We Are All Responsible
  - Watch at this link:
    - YouTube https://youtu.be/tglYaa3lmqw

We Are All Responsible

Cybersecurity Awareness

If you have any questions about the program you have just viewed, you may contact us at:
(800) 424-4888 or Health.eduCSRequests@ttuhsc.edu
Direct your inquiries to Customer Service.
Be sure to include the program number, title, and speaker.

800-424-4888Iwww.ttuhsc.edu/health.edu

Health.edu
Texas Tech University Health Sciences Center