MCIT
Minnesota Counties Intergovernmental Trust

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Mobile Device Security

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers best practices to use on mobile devices in the field to secure data.

Purpose: Reminds employees about the importance of security on all devices, not just office computers, to prevent data breaches and malware.

Preparation: Read and become familiar with this Quick Take. *Change as needed to reflect procedures and personnel in your department.*

Handouts: Quick Review of Data Security—Mobile Device Security

Notes: Organizations are encouraged to adopt a mobile device policies for employer-issued and employee-owned devices. Review any policies in place prior to giving this Quick Take and adjust as necessary.

MOBILE DEVICE SECURITY HAZARDS

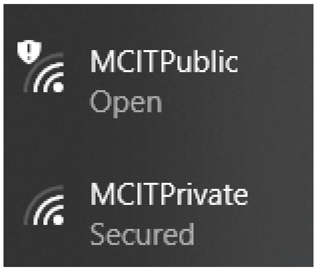
Although most of us are aware of and vigilant against the hazards of viruses, phishing and other hacking attempts when using a computer, we may be less aware that these hazards also apply to mobile devices. As more and more devices are connected to the Internet, it is important to remember that malware can affect mobile devices, including phones, laptops and tablets. However, lost or stolen equipment can also lead to a data breach as easily as a malware infection.

IT professionals work to protect our systems, but it takes all of us doing our part to keep our systems and data secure. Please pay attention.

BEST PRACTICES FOR MOBILE DEVICE SECURITY

The following best practices can help improve mobile device security:

- Limit the amount of data stored on the device. Although devices are often used to access information, sometimes they can store and retain information. Whenever possible, do not store sensitive data on mobile devices.
- Mobile equipment should be protected with a secure password and locked when inactive.
- When transmitting private or sensitive data, always use a secure network. These networks typically require a password to access. [*Instructor Prompt:* See photo for example of secure and open WIFI connections.]
- Any private or nonpublic data should be encrypted.
- Mobile devices should be updated regularly as systems or apps are improved.



- Keep devices with you or locked in secure locations away from others. Consider hiding these items from view when storing them in vehicles or other locations to deter theft.
- Avoid using the device in an area where others nearby can view the screen.
- Use and regularly update trusted antimalware or security tools for your mobile devices.
- If devices are removed from service, transferred to new users or sold, all private data should be securely wiped prior to transfer.
- Mobile devices issued by an organization should be equipped with a system that allows IT professionals to remotely wipe or lock a device that has been lost to theft or negligence.
- Above all, remember that simply using a mobile device does not guarantee immunity from viruses or hacking. If you would not do something with your work computer, do not do it with your mobile device. Maintain a healthy skepticism.

IF A DEVICE IS MISSING OR YOU SUSPECT A DATA BREACH

- Do not panic and make the situation worse by complying with instructions from malicious programs or hackers.
- Report the situation to a supervisor or IT.
- Follow IT and supervisor directions and the policies of our organization.

DISCUSSION QUESTIONS

- How else can we maintain the security of mobile devices?

Mobile Device Security Session Planning and Review

Trainer Training Date

Department(s)

TRAINING GOALS

- Employees recognize that mobile devices are also vulnerable to malware and data breaches.
- Employees are aware of and follow best practices when using mobile devices.
- Employees understand how to respond to a suspected security attack or data breach involving mobile devices.

RESOURCES

- "Security Tip: Protecting Portable Devices: Data Security," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- "Security Tip: Protecting Portable Devices: Physical Security," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- "Security Tip: Protecting Portable Devices: Defending Cell Phones and PDAs Against Attack," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- "Guidelines for Managing the Security of Mobile Devices in the Enterprise (Publication 800-124 Revision 1)," National Institute of Standards and Technology, NIST.gov
- "Employee-owned Technology in the Workplace (BYOD Bring Your Own Device)," Minnesota Counties Intergovernmental Trust, MCIT.org/resource/

REVIEW

Did the training meet the stated goals?

How can the training be improved?

TRAINER COMMENTS

Attendance Record

Training Session Mobile Device Security

Trainer

Training Date

Participant Name (printed)	Participant Signature