MCIT
Minnesota Counties Intergovernmental Trust

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Password Security

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers secure passwords and how to keep passwords secure.

Purpose: Educates employees about the importance of password security and creating strong passwords.

Preparation:
- Read and become familiar with this Quick Take. *Change as needed to reflect procedures and personnel in your department.*
- Review any password policies prior to the training and revise the script and handouts as needed to fit with current policies.

Handouts: Quick Review of Data Security—Password Security

Passwords and Security

Passwords are an important line of defense for any computer or electronic information system. Because passwords are required to access or operate devices, programs or locations, they are a common target for hackers. Creating strong passwords and keeping them secret is vital to maintaining data security.

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

Secure Passwords

If your password is easily guessed, such as the word "password," it is not secure. Some best practices to create and secure strong passwords are include the following:

- Use passwords or phrases that are a mix of capital and lowercase letters, numbers and special characters. This makes them more complex and harder to guess.
- Avoid using words that can be found in a dictionary. Deliberate misspellings or using numbers/symbols for letters can help. Using the "at" (@) symbol for the letter A or the number one for the letter "L" are some common examples. [*Instructor Prompt:* Ask for more examples.]
- Use unique passwords for each program, device, service and location. Having one password for everything might be easier to remember, but it gives others access to multiple systems and devices if they can guess the one password.
- Longer passwords are generally more secure than shorter passwords. Passphrases are a good way to make longer passwords while still being easy to remember. A statement, such as "dogs are awesome" could be a password if the spaces between the words are removed, (e.g. dogsAreawesome). This can be made even stronger if certain letters are replaced with numbers, special characters or abbreviations, such as replacing the letter "o" with the number zero or shortening the word "are" to the letter "r", (e.g. d0gsRawes0me).
- Change passwords regularly, using the same rules from complexity we've already discussed.

This document is intended for general purposes only and should not be construed as legal or coverage advice on any specific matter.

- Avoid storing or writing down passwords in an easy-to-find location.
- Do not share passwords with anyone.

Discussion Questions

- How else can we protect our passwords?
- What do we do if we forget our passwords?

Password Security Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

- Employees understand the importance of passwords.
- Employees know how to create secure passwords.
- Employees take care to prevent others from learning their passwords.

RESOURCES

- "Security Tip: Choosing and Protecting Passwords," United States Computer Emergency Readiness Team, Department of Homeland Security, US-CERT.gov
- Password Construction Guidelines and Password Protection Policy, SANS—Consensus Policy Resource Community, SANS.org

REVIEW

Did the training meet the stated goals?

How can the training be improved?

TRAINER COMMENTS

Attendance Record

Training Session Password Security

Trainer

Training Date

Participant Name (printed)	Participant Signature