Click Wisely

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Email and Data Management

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers the importance of managing email content in compliance with data retention regulations and cybersecurity best practices.

Purpose:
- Reminds employees about the hazards of using the email system for long-term storage of messages and attachments.
- Reviews best practices for securing information received via email.

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: Email and Data Management or Keep a Clean Inbox digital image
- Entity's data retention schedule

Email Poses Unique Security Hazards

We all know that email is great for communicating with colleagues, partners and clients, but we need to remember that it is actually risky to keep messages in our email accounts long term.

Threat actors are constantly hunting for valuable information to steal and use to extort money from [name of your entity]. When we keep valuable information, such as sensitive personal data, in our email, we create an unnecessary and avoidable vulnerability. Also, all of the contacts in our account can be targeted with phishing attacks in turn.

Here's an example of an actual data breach:

- An employee had more than a decade of emails saved in his email account. His account was hacked, which gave the bad actors access to years' worth of email contacts, personal information and documents that were saved in the messages and attachments.
- The threat actors then proceeded to target all of the email contacts with phishing attacks and had access to hundreds of people's personal information.
- On top of the expenses to remove the malware released on the employer's system, the hacked organization had to pay for sending hundreds of breach notifications, credit monitoring services for those whose information was leaked and public relations coaching.

We need to ask ourselves, if our email accounts were hacked, what information and how much would be readily available to threat actors?

Our 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.

We Must Balance Data Retention and Protection

As public entity employees, we must adhere to our statutory data retention requirements while protecting the private data we have to maintain.

So, we need to be strategic with how we receive and maintain sensitive data. As threat actors find new ways to exploit technology and systems, it is vital that we do everything we can to reduce the threat landscape.

Here are four ways we can do this.

1. Only Keep Information and Records That We Need for as Long as We Need Them

We have a records retention schedule that we must follow. This schedule tells us how long to keep official records. It also means that once that retention period has expired, we no longer must keep the data, and we can destroy it. We should be destroying data we no longer must keep or need for a business purpose as soon as we can.

This reduces the amount of information that is vulnerable should a breach occur.

In the example I described earlier, had the employee destroyed unnecessary emails and attachments as soon as they were no longer needed, the number of people whose personal information was compromised would have been dramatically reduced.

Here's what you should do:

- Review our records retention policy, noting what information you have that is an official record, what is not and how the retention schedule applies to that. If you have questions about the retention schedule, see me or connect with [name of individual responsible for the retention schedule].
- Make time on a regular basis, at least annually, to securely destroy files to comply with the retention schedule or your business purpose needs. This is a legitimate and important part of your job, so please schedule time for this.

2. Treat Email as a Pass Through System, Not a Storage System

You should think of email as you do your physical mailbox. It is the place where you open messages and either trash them or file them securely elsewhere. You don't permanently keep sensitive documents in a mailbox at the end of your driveway, so you should not keep sensitive data in your business email account.

3. Eliminate Practices That Use Email as a Backup

If you save emails as a way to track work or as a personal backup, please change this to limit what bad actors could potentially gain access to. What may have once been an efficiency and trusted back up, now is a vulnerability and a liability to our organization.

[Instructor Note: Choose which of the next two paragraph fits your organization's system.]
Once an email is uploaded to our document management or customer relationship management system, you should fully remove the original message from the email system. This means deleting it from the Deleted box and copies from the Sent box, too. *[Instructor Note: Add details about this for your specific system here.]*

If an email message or attachment needs to be retained, you should move it to a secure place, such as our private network drive. After emails have been saved outside of your email, delete them fully from your account to avoid unnecessary duplication. This means deleting it from the Deleted box and copies from the Sent box, too. *[Instructor Note: Add details about this for your specific system here.]*

4. Encrypt Sensitive Emails

When you must use email to send or receive sensitive information, such as medical, personally identifiable or financial information and the like, be sure it is encrypted. This means that only the sender and receiver have credentials to open the message. *[Instructor Note: Add details here about how your organization's encrypted email works.]*

DISCUSSION QUESTIONS

- If you are not sure about whether an email can be destroyed, what should you do?
- How else can we best maintain email and data security?

Email and Data Management Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

- Remind employees about the hazards of using the email system for long-term storage of messages and attachments.
- Reviews best practices for securing information received via email.

RESOURCES

- Minnesota Statutes, Chapter 138.17, subdivision 7
- Your entity's records retention schedule

REVIEW

Did the training meet the stated goals?

[add comments here]

How can the training be improved?

[add comments here]

TRAINER COMMENTS

[comments added here]

Attendance Record

Training Session Email and Data Management

Trainer Training Date

Participant Name (printed)	Participant Signature