Security Awareness Training

Presented by
Enterprise Information Security (EIS)
Welcome

Security Awareness Training

Preston Jennings
VP Information Security & CISO
Trinity Health
Introduction

Trinity Health is inundated daily with emails (including both malicious phishing emails and junk/spam messages) coming into our environment. Although IT technologies and tools filter out over 95% of these messages, nothing is foolproof, so some messages get through our defenses and end up in your inbox. Each of us has responsibility to identify suspicious emails and report them!

Learning Objective: Learn the warning signs to help you identify malicious phishing messages, including how to display the real URL for embedded links. Then practice differentiating malicious phishing emails from junk (spam) messages.
Key Areas of Focus

In this year's course, we will discuss four key areas in more detail:

• Phishing and the danger it poses
• Understanding confidential data and how to protect it
• Spam vs. Phish
• Using mobile devices safely
The Dangers of Phishing

"Phishing." It's that annoying and often dangerous practice that plagues us all. Phishing refers to the use of fraudulent messages by scammers to try to steal sensitive information, such as credit card numbers or passwords, or to install malicious software, or "malware", on a user's computer. Phishers often use a combination of email, text messages, and fake websites to try to deceive their victims.

Phishing attempts that target a specific user, department, or organization are becoming increasingly common. These messages may appear to be from someone within the company who is in a position of trust, such as IT or Human Resources. The sender might request information such as login IDs and passwords, or ask you to update this information. They may even try to get you to click an innocent-looking link that actually deploys spyware designed to steal data.

Phishers are cunning, creative, and ruthless. That's why you've got to be suspicious of any email that looks even a little bit unusual!
Suspicious Messages

How can you identify phishing attempts? Some of the signs are obvious, while others may not be so easy to spot. Unexpected email containing suspicious attachments or unfamiliar links is especially dangerous. Most phishing email contains multiple red flags. This combination of warning signs should put you on high alert.

Explore the following messages to see how good you are at spotting the warning signs of phishing.

1. Yes, misspellings, especially of the names of well-known companies, are a strong sign that something's wrong.
2. Any messages addressed generically, especially ones regarding financial transactions, are suspicious.
3. Links within the body of a message need to be treated with extreme caution. They could take you somewhere you are not expecting. Even if you recognize the sender, it's possible that the person's account has been compromised.
Suspicious Messages

How can you identify phishing attempts? Some of the signs are obvious, while others may not be so easy to spot. Unexpected email containing suspicious attachments or unfamiliar links is especially dangerous. Most phishing email contains multiple red flags. This combination of warning signs should put you on high alert.

Explore the following messages to see how good you are at spotting the warning signs of phishing.

1. Multiple addressees on the "To" line should be examined carefully. This can be a sign of phishing.

2. Alarmist messages and threats of account closure are definitely suspicious.

3. Keep an eye out for spelling errors. Big companies and social networking sites such as LinkedIn would check their spelling in their form letters prior to sending them out.

4. Remember, beware of links within messages, especially if they don't display where they are taking you. This one is also suspicious because of the misspelling.
Suspicious Messages

How can you identify phishing attempts? Some of the signs are obvious, while others may not be so easy to spot. Unexpected email containing suspicious attachments or unfamiliar links is especially dangerous. Most phishing email contains multiple red flags. This combination of warning signs should put you on high alert.

Explore the following messages to see how good you are at spotting the warning signs of phishing.

1. Multiple unfamiliar addressees on the "To" line could be a sign that this scammer is phishing for victims.
2. Generic messages with no greeting and incorrect grammar are red flags.
3. Attachments can be serious threats. Opening them can introduce malware into your system. Any attachments, especially unexpected ones, should definitely be regarded with suspicion.
What’s in a URL?

Phishers often try to conceal dangerous links within a message. If you learn how to analyze web addresses (also known as URLs), you can spot fake websites and help protect yourself from being hacked.

A good rule of thumb is to always be sure you know where a link is really taking you. But how can you tell? In many cases, you can check the URL by simply holding your mouse pointer over the link. For example, you might receive a message that says click here. If you hover over the link, the URL will appear in the bottom of your browser or status bar, or somewhere near the link itself. This allows you to see what the name of the site is before you actually click the link.

Note: Not all systems or links reveal the URL with a hover, so always be on the lookout for other signs of phishing.
Identifying Junk (Spam) and Phishing (Malicious) Messages

Feeling confident? Good, because it's time to put those phish-spotting skills to the test by playing "Find the Phish." You'll review examples of actual email messages sent to Trinity Health colleagues. Look carefully at URLs, ask yourself the right questions, and trust your skeptical instincts to decide which messages are junk (spam) and which are potentially malicious phishing messages.

Imagine you are just logging in for the day and the first thing you like to do is go through your email. Read each of the following messages and investigate any links. Decide whether each message is JUNK (SPAM) or a PHISHING (MALICIOUS) message and then hit enter to see if you were correct.
Recognizing Phishing Emails

© 2018 Trinity Health

From: IT-Help-Desk@trinity-health.org
To: Jane@trinity-health.org
Subject: [External] IT Help Desk

Warning: This email came from the Internet!
DO NOT CLICK links included in the email, and NEVER provide your password.

CORRECT! This is an external phishing message NOT from the Trinity Information Services (TIS) IT Support Desk. It includes a suspicious link and a suspicious sender email address that is designed to make it look like a real Trinity Health email address.

Thank you for your co-operation,

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
Feeling confident? 

Example email message received, and decide whether it is a phishing or spam message. 

From: inventory-reports@trinity-health.com
To: jane@trinity-health.org
Subject: [External] Inventory Report
Attachment: Document 20080101_0001.PDF
Attachment: Document 20080101_0002.PDF

Warning: This email originated from the Internet!

DO NOT CLICK links if the sender is unknown, and NEVER provide

CORRECT! This is an external phishing message. It includes suspicious attachments you weren’t expecting. It also has a suspicious sender email address that was designed to make it look like a real Trinity Health email address.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
<ErikRuiz@interstatehotels.com>

From: email-admin@trinity-health.org
To: jane@trinity-health.org
Subject: [External] RE: IT-Help desk Service 2019

Warning: This email is from the Internet!

DO NOT CLICK links in the email, and NEVER provide your password.

CORRECT! This is an external phishing message NOT from the Trinity Information Services (TIS) IT Support Desk. It includes a suspicious link and a suspicious sender email address that is designed to make it look like a real Trinity Health email address.

Please all employees and Staff should Click Here to switch to Outlook Webmail 2019 for employees

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
From: michelle.gardner@trinity-health.org
To: jane@trinity-health.org
Subject: [External] Direct deposit change

Warning: This email is from the Internet!
DO NOT CLICK links if the sender is unknown, and NEVER provide your password.

CORRECT! This is an external phishing message using social engineering techniques. The perpetrator wants you to reply so they can validate your email address is real. Note the suspicious sender email address is designed to make it look like a real Trinity Health email address.

Michelle

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
From: Apple Promotions
To: jane@trinity-health.org
Subject: [External] Brand New Apple iPhone 11!

Warning: This email is suspected to be from the Internet!

DO NOT CLICK links if the sender is unknown, and NEVER provide your password.

CORRECT! This message is Junk (Spam)! It appears to be a business solicitation with links and a sender address that appear legitimate. Don't share your business email address for anything but business purposes.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
Identifying Phishing Emails

Feeling suspicious? Check out this example to help you identify phishing emails and trust your instincts.

Email Details:
- **From:** exec.office@trinity-health.org
- **To:** jane@trinity-health.org
- **Subject:**

> Warning: This email originated from the Internet!

> CORRECT! This is an external phishing message using social engineering techniques. The perpetrator wants you to reply so they can validate your email address is real. Note the suspicious sender email address is designed to make it look like a real Trinity Health email address.

Decide whether this message is **Junk (Spam)** or a **Phishing (Malicious)** message and click the corresponding button.
Feeling confused? Here are some examples:

- **Junk (Spam)**: This email is from an unknown source. It contains links and a sender address that appear legitimate. There is no urgent request of you, which is a technique used by bad actors to make you act quickly without thinking.

- **Phishing (Malicious)**: This email is sent from a known source but contains suspicious links and a request for personal information.

Decide whether this message is Junk (Spam) or a Phishing (Malicious) message and click the corresponding button.
Identifying Junk (Spam) and Phishing (Malicious) Messages

Feeling like you're getting too many emails and worried about getting junk mail? It's important to be on the lookout for spam and phishing emails. Here are some tips to help you identify these pesky messages:

1. **Sender:** Be cautious of emails from unknown senders.的职业电子邮件或者电子邮件的格式是否一致。
2. **Subject:** Avoid emails with suspicious or empty subjects.的职业电子邮件一般都有具体的主题。
3. **Attachments:** Be wary of attachments.的职业电子邮件一般没有附件。
4. **Links:** Clicking on links in suspicious emails can lead to malware.职业电子邮件一般没有链接。
5. **Personal Information:** Be cautious with emails requesting personal information.职业电子邮件一般不包含个人信息。

By following these tips, you can protect yourself from spam and phishing attempts. Remember, it's always better to err on the side of caution. Check marks symbolize the correct identification of spam and phishing messages. Were you a SCAM BUSTER?!
Today’s work environment is more connected than ever, whether you’re working in a hospital, physician practice, corporate office, at your virtual home office, or on the road. Although mobile devices (laptops, cell phones and tablets, etc.) and other technologies provide extensive capability and convenience, these benefits increase your responsibilities and necessitate vigilance! Especially when away from the safety of our network, there are a variety of electronic and physical threats.

Simple tasks—like sending an email from home or logging on to a hotel’s Wi-Fi network—could cause a data breach. These actions, and others, must be performed with security in mind. Doing so will protect yourself and our organization.

**Learning Objective:** How to use devices (laptops, cell phones and tablets, etc.) safely onsite and offsite.
Using Mobile Devices Safely

Do you have what it takes to defend your laptop, cell phone, and tablet—and the sensitive information they access? Test your knowledge by playing "Device Defender."

This game asks you to decide if certain actions related to working remotely on these devices are safe or risky. Make the best decisions to protect your device and the sensitive data that can be accessed from your device. Good luck!
Device Defender

**TOPIC: PASSWORDS**

Create a strong password by using a capitalized word from the dictionary and a number you can remember.  
SAFE  RISKY

Conceal passwords as contacts in a smartphone's address book for easy recall later.  
SAFE  RISKY

Use the same password for your work account as you do for your personal accounts (banking, kids school website, etc.) so you don't forget.  
SAFE  RISKY
Device Defender

**TOPIC: PASSWORDS**

Create a strong password by using a capitalized word from the dictionary and a number you can remember.

Correct. Secure passwords should include numbers, special characters, and upper- & lower-case letters. The longer the password, the stronger the password, so try to come up with short sentences you can easily remember. Using a single dictionary word is NOT secure!

Conceal passwords as contacts in a smartphone’s address book for easy recall later.

Correct. Never write down a password or store it unencrypted, especially not somewhere on or near your devices.

Use the same password for your work account as you do for your personal accounts (banking, kids school website, etc.) so you don’t forget.

Correct. Using the same passwords on multiple websites or for multiple purposes puts you at risk! If the password is compromised on one site, it can be used to access information in another.
Device Defender

**TOPIC: MONITORING YOUR DEVICE**

- **Configure devices (laptop, phone, tablet, etc.) to require a pin or password to unlock it.**
  - SAFE
  - RISKY

- **If safely leaving your device for a short interval, it’s okay to leave your screen unlocked.**
  - SAFE
  - RISKY

- **If a mobile device used to access Trinity Health information is lost temporarily or stolen, report it immediately.**
  - SAFE
  - RISKY

**ACTIVATE DEFENSES**
Device Defender

**TOPIC: PASSWORDS**

Create a strong password by using a capitalized word from the dictionary and a number you can remember.

**Correct.** Secure passwords should include numbers, special characters, and upper- & lower-case letters. The longer the password, the stronger the password, so try to come up with short sentences you can easily remember. Using a single dictionary word is NOT secure!

Conceal passwords as contacts in a smartphone's address book for easy recall later.

**Correct.** Never write down a password or store it unencrypted, especially not somewhere on or near your devices.

Use the same password for your work account as you do for your personal accounts (banking, kids school website, etc.) so you don't forget.

**Correct.** Using the same passwords on multiple websites or for multiple purposes puts you at risk! If the password is compromised on one site, it can be used to access information in another.

NEXT TOPIC
Device Defender

**TOPIC: APPLICATION ACCESS AND PERMISSIONS**

<table>
<thead>
<tr>
<th>Topic 3 of 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Only install mobile applications from a trusted source (App Store on Apple devices, and Google Play on Android devices).</strong></td>
</tr>
<tr>
<td>SAFE</td>
</tr>
<tr>
<td><strong>Restrict mobile application permissions to only what is required for the application to function (i.e., don't allow access to the camera or maps/GPS functionality unless required).</strong></td>
</tr>
<tr>
<td>SAFE</td>
</tr>
<tr>
<td><strong>Access social media sites from your work device.</strong></td>
</tr>
<tr>
<td>SAFE</td>
</tr>
</tbody>
</table>

**ACTIVATE DEFENSES**
### Device Defender

#### TOPIC: APPLICATION ACCESS AND PERMISSIONS

<table>
<thead>
<tr>
<th>Topic 3 of 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Only install mobile applications from a trusted source (App Store on Apple devices, and Google Play on Android devices).</strong></td>
</tr>
<tr>
<td><strong>Correct.</strong> Downloading or installing applications from untrusted sources may result in malware that can destroy your data/pictures or compromise your credentials.</td>
</tr>
<tr>
<td><strong>Restrict mobile application permissions to only what is required for the application to function (i.e., don't allow access to the camera or maps/GPS functionality unless required).</strong></td>
</tr>
<tr>
<td><strong>Correct.</strong> Only provide a mobile application with the minimum permissions necessary to perform its function.</td>
</tr>
<tr>
<td><strong>Access social media sites from your work device.</strong></td>
</tr>
<tr>
<td><strong>Correct.</strong> Corporate procedures state that colleagues are accountable for their internet use including content shared. Social media sites may contain documents or links that increase exposure to malware and the possibility of sensitive information leakage.</td>
</tr>
</tbody>
</table>

©2018 Trinity Health
Device Defender

You’re a security hero. You’re making the right decisions to control access to your device while working remotely. Keep it up!

To continue, click NEXT.
Protecting Confidential Data

Sending Data Safely: Internally and Externally

Malicious data thieves are working hard to steal our confidential data, including both Protected Health Information (PHI) and Personal Identifiable Information (PII). Not only must this data be protected when stored, data must also be protected when being sent to others, both inside and outside of Trinity Health. Each of us is responsible for using caution when sending data so it is not compromised along the way.

Learning Objective: How to securely transfer data internally and externally.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 1 of 6

You and a colleague are teaming up on a project, accessing files from our network. After a few hours you realize it’s time for lunch. Your colleague suggests that you save a copy of the files to your computer so that you two can continue work at the café. What should you do?

☐ Copy the files to your personal laptop and bring it along to lunch.

☐ Save files to both your smartphone and your colleague’s smartphone so you can divide and conquer.

☐ Save the files back to our network and resume your work after lunch.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

**Question 1 of 6**

You and a colleague are teaming up on a project, accessing files from our network. After a few hours you realize it’s time for lunch. Your colleague suggests that you save a copy of the files to your computer so that you two can continue work at the café. What should you do?

- Copy the files to your personal laptop and bring it along to lunch.
- Save files to both your smartphone and your colleague’s smartphone so you can divide and conquer.
- Save the files back to our network and resume your work after lunch.

**Correct**

Copies of sensitive information should never be saved to your computer or a mobile device’s local storage.

NEXT QUESTION
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 2 of 6

The email server is down, but you have some important files to send to a colleague. What’s the best way to transmit the files?

☐ Send them to the colleague using an unencrypted USB thumb drive.
☐ Use your personal email to get the colleague the files without delay.
☐ Wait until the email server comes back online.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 2 of 6
The email server is down, but you have some important files to send to a colleague. What’s the best way to transmit the files?

☐ Send them to the colleague using an unencrypted USB thumb drive.
☐ Use your personal email to get the colleague the files without delay.
☒ Wait until the email server comes back online.

Correct
Use only your work email account to send files, never a personal account. Use only encrypted USB thumb drives unless a formal Exception exists.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 3 of 6

You receive an email from a fellow colleague whom you haven't met, asking you for details regarding potentially sensitive financial information on a project. How should you respond?

☐ Copy your manager on the reply so that they can be included in the message.

☐ Encrypt the message before sending.

☐ Check that the colleague has a legitimate "need to know."
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 3 of 6

You receive an email from a fellow colleague whom you haven’t met, asking you for details regarding potentially sensitive financial information on a project. How should you respond?

☐ Copy your manager on the reply so that they can be included in the message.

☐ Encrypt the message before sending.

☐ Check that the colleague has a legitimate “need to know.”

Correct
Verify the business need-to-know of an individual before sending them sensitive information.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 4 of 6

You need to send some confidential files to our offices while offsite, but you cannot access our network. What’s the most secure way to transmit the data?

☐ Send the message from the restaurant just outside of town that offers better privacy.

☐ Purchase a Wi-Fi hotspot, connect, and then send the message.

☐ Use a VPN to connect to the network, then encrypt your message by typing the word 'secure' in the subject line.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 4 of 6

You need to send some confidential files to our offices while offsite, but you cannot access our network. What’s the most secure way to transmit the data?

☐ Send the message from the restaurant just outside of town that offers better privacy.

☐ Purchase a Wi-Fi hotspot, connect, and then send the message.

☑ Use a VPN to connect to the network, then encrypt your message by typing the word ‘secure’ in the subject line.

Correct

Untrusted networks can be used with a VPN, but even then it’s best to encrypt messages.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 5 of 6

A colleague has been working from home and needs to send you some files. To make things easier, he’s saved them to his personal cloud storage and given you the access link. What should you do?

☐ Access the files, download them to your computer, then ask the colleague to delete the files from his cloud.

☐ Have the colleague email you the encrypted files directly using his personal email account.

☐ Ask your colleague to remove the files from his personal cloud and wait until he can securely connect to our network.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 5 of 6

A colleague has been working from home and needs to send you some files. To make things easier, he’s saved them to his personal cloud storage and given you the access link. What should you do?

- [ ] Access the files, download them to your computer, then ask the colleague to delete the files from his cloud.
- [ ] Have the colleague email you the encrypted files directly using his personal email account.
- [x] Ask your colleague to remove the files from his personal cloud and wait until he can securely connect to our network.

Correct

Personal cloud solutions are prohibited. Use only approved cloud storage services or encrypted email for transmitting or saving sensitive information.

NEXT QUESTION
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 6 of 6
You are given a USB thumb drive by a colleague which contains a confidential report. Upon inserting it in your laptop, you receive a notification asking for an encryption key. Is something wrong?

☐ No, ask your colleague for the encryption key.

☐ Yes, follow-up with the IT Service Desk for assistance.

☐ Yes, remind the colleague to follow our Information Security procedures for secure data transmission.
Protecting Confidential Data

Sending Data Safely: Internally & Externally

Question 6 of 6

You are given a USB thumb drive by a colleague which contains a confidential report. Upon inserting it in your laptop, you receive a notification asking for an encryption key. Is something wrong?

☐ Yes, follow-up with the IT Service Desk for assistance.

☐ Yes, remind the colleague to follow our Information Security procedures for secure data transmission.

☐ No, ask your colleague for the encryption key.

Correct
Physical storage devices like USB thumb drives should always be protected.

CONTINUE
Protecting Confidential Data

Sending Data Safely: Internally & Externally

SECURE METHODS FOR DATA TRANSMISSION

✔ Never download sensitive data to your local device memory
✔ Use only your work email account to send files, never your personal account
✔ Verify the need to know of recipients
✔ Use VPN when offsite and always encrypt emails when appropriate
✔ Use only approved cloud storage services
✔ Use only encrypted USB thumb drives unless a formal Exception exists

OUTSTANDING!

You’re sending data securely. Keep at it, and help your colleagues keep data as safe as yourself!

To continue, click NEXT.
Protecting Confidential Data

Learning Objectives

You learned:

- The importance of making good decisions when handling data and interacting with technology.
- Warning signs that help you identify malicious phishing messages, including how to display the real URL for embedded links.
- How to differentiate between malicious phishing emails from junk (spam) messages.
- How to use devices (laptops, cell phones and tablets, etc.) safely onsite and offsite.
- How to securely transfer data internally and externally.

To continue, click NEXT.

Thank you everyone for learning to keep our colleagues’ and patients’ data safe.
Download and Review the Acceptable Use Procedure
FROM COURSE: TH - TIS - 2020 Security Awareness Training

STATUS: Completed

Instructions
Please download and review the Acceptable Use Procedure. When you have finished, please close the document and click on the next HealthStream activity to attest that you agree to its contents.

Attachment

Acceptable Use Procedure rev. 10.19.2019
FILE TYPE: pdf  UPDATED: Mar 3, 2020 at 11:02am ET

Support.
For questions, comments or to report a problem, please send an email to System Office HealthStream Administration at hqshealthstreamadmin@trinity-health.org
To be the most trusted health partner for life by safeguarding information assets while supporting the needs of our patients, physicians, colleagues and stakeholders.