Slide 1 - Introduction

Text Captions

Hello, and welcome to the Annual Security Awareness Training.
Before we get started, let’s talk about course navigation.

Moving around in this course is easy. You can use the Forward and Backward buttons to navigate, or you can jump around in the course using the Table of Contents.

There’s audio in this course. Listen or read the screen and follow any instructions you see.
Audio is included in the Security Awareness Training 2023 video.

I'm Preston Jennings, Vice President of Information Security and Chief Information Security Officer for Trinity Health.

I'm excited to introduce this Security Awareness Training and stress its importance to you personally. It's not just another annual security awareness course. This course was created fresh from the ground up to educate you on the greatest cybersecurity threats we're defending against here at Trinity Health. This content was selected by our own Security Team based on cyber-attacks we are seeing at our ministries on a daily basis. And as always, many of the same safe cybersecurity habits taught here, directly apply to your personal life outside of Trinity Health.

Year over year, the healthcare industry continues to be a top priority target for bad actors due to the concentration of sensitive personal, health, and financial information. These bad actors seek two primary objectives: first, disruption of services; and second, the data itself. Both disruption of care for our patients and confidential data loss carry a severe impact of both our patient's safety, and to our Trinity Health Mission. Now, let's talk about our safety here at Trinity Health and the need for you to be security aware.

At Trinity Health, we take the protection of confidential data, especially protected health information known as PHI, very seriously. Our Security Team monitors over 100 billion events a month, to identify an average of over 150 suspicious security events. In fact, as you're watching this video now, there's a good chance we're investigating some sort of suspicious activity in our network.

The most frequent security incidents we experience at Trinity Health include: first, real malicious phishing messages and threat actors attempting to access our systems. Second, attempted installation of unauthorized software that contains malicious code on our devices. And, third, hackers trying to gain unauthorized access to our systems using stolen user credentials.

We're doing everything possible to keep Trinity Health safe but that requires all of us being security aware, having good security habits, and reporting incidents. Here's another important fact – on average, daily, we incur at least one unique phishing attack targeting our colleagues.

Your reporting of suspicious email messages using the Outlook "Report Phishing" button has never been more critical because when reported, these messages go directly to the Security Team to analyze for nefarious behavior. And the quicker we know about it, the quicker we can remove the malicious messages from our colleagues mailboxes and protect our network.

Before I close, I have one more request for you that will benefit the security of our network and data – if you've not already, please download and use the Microsoft Authenticator App. The Authenticator App significantly lowers the risk of cybercriminals accessing our systems.

The app is now also the primary method for forgotten password resets, which bolsters our security posture even more. If you're not already using the Microsoft Authenticator App, please download and do so. I sincerely hope you'll enjoy the course and learn important new security behaviors. Thank you for all you do to keep patient and Trinity Health confidential information safe.
TogetherSafe Behaviors to Prevent Security Incidents

TogetherSafe and being cybersafe require many of the same good behaviors. You will learn the warning signs of security threats and behaviors which increase security.

- **Prepare for the Process and Manage the Task**
  - Exercise Strong Password Guidelines
  - Utilize Multi-factor Authentication (MFA)
  - Recognize Role Based Actions

- **Communicate Clearly**
  - Demonstrate Safe Email Practices

- **Questioning Attitude**
  - Recognize Social Engineering Techniques and Phish Warning Signs

- **Attention to Detail**
  - Use Devices Safely
  - Keep Systems and Information safe

- **Support the Team**
  - Report Security Incidents

Click each icon to learn more.

**Text Captions**

TogetherSafe and being cybersafe require many of the same good behaviors. Each of the TogetherSafe shields will provide you the structure to raise awareness and behave safely. During the lesson you will explore each shield. Click each icon to learn more.

Click each icon to learn more.
Text Captions

In healthcare, good security behavior is like good hand hygiene habits; they should be performed consistently. Both are necessary behaviors which go hand-in-hand. Cybersecurity basics include a variety of good habits starting with using strong passwords, Multifactor Authentication also called MFA, and recognizing role-based actions you can take.
Slide 6 – Vignette 1

Text Captions

Audio is included in the Vignette 1 video.

ICU RN Margaret, occasionally provided her work email address when signing up for volunteer activities and other frequently visited sites. This made staying on top of her busy personal life and frequent volunteerism a little simpler.
Margaret also universally used the same easy to remember password Spring 2023 both at work and home on various social media sites such as Facebook and LinkedIn. Margaret's credentials, which included her work email address and weak reused password were stolen from a popular social media site and posted on the "Dark Web". Another nation state sponsored bad actor then used Margaret's stolen credentials to sign on to the Trinity Health network.
While busy in the ICU, taking care of an injured patient. Margaret received a random multi-factor authentication (MFA) prompt on her phone, generated by the bad actor's network Sign-in. Thinking little of it, Margaret hit "Approve" to the MFA prompt considering it another IT generated thing or whatever.
The bad actor was now successfully signed on to the Trinity Health network and immediately does a password reset. Margaret was now locked off the network when signing in next. The bad actor analyzes Margaret's full network, Access Privileges.
His PHI quest continues attempting to open a myriad of SharePoint files. Fortunately, the bad actor was thwarted initially. Margaret didn't have access privileges to most of the SharePoint files containing confidential information because she didn't have a direct need-to-know.
The owners who saved the SharePoint files, containing PHI had properly limited access to the small number of colleagues who actually had a direct need-to-know. But with persistence and no report of the random MFA prompt by Margaret to the Service Desk, the bad actor successfully found an ICU department archive loaded with PHI dating back over three years. The bad actor successfully downloaded a series of files containing PHI from thousands of patients.

Colleague Takeaways.

• Do not use your work email address for non-business purposes.
• Always use long, complex passwords and never reuse them.
• Do not use work passwords on personal sites.
• Never "Approve" a random MFA prompt, report it to the TIS Service Desk.

File access on SharePoint and elsewhere should always share information on a need-to-know basis.
Margaret's poor security habits clearly created the opportunity for the bad actor to attack Trinity Health.

In the end, if Margaret would have reported the random MFA prompt to the service desk instead of hitting "Approve" the bad actor's cyber-attack would have been stopped.
Margaret can take steps to be safer with information, part of the steps will be to ensure password safety. Click each check to learn more.
Text Captions
The following are behaviors that should be avoided. Click each x to learn more.
Text Captions

Multifactor authentication is another safeguard to keeping your information safe. Sometimes called 2-factor authentication, Multifactor Authentication provides a higher degree of security to identify the individual attempting to access a network because it requires a secondary source to validate the users’ identity.

If you haven’t done so already, download the Microsoft Authenticator App. This app greatly lowers the risk of cybercriminals accessing our systems. The app is now also the primary method for password resets, which bolsters our security even more.
Slide 10 – Think before you accept MFA

Text Captions
Think before you approve Multifactor Authentication.

If you aren’t actively trying to log in yourself, don’t “Approve” an Authenticator prompt.
You play a role

Select the role to view more specific security actions you can take.

- Patient Care
- Administrative, Finance
- Supply Chain - Sourcing

- If emailing patient information externally, mark it “secure” in the subject line to encrypt the message.
- If texting, use approved Trinity Health technology or communicate via the patient portal.
- Lock your computer screens or Workstation On Wheels (WOW) when you walk away.
- Never share your login credentials with anyone.
- Do not plug your phone into medical devices or computers to charge.
- Slow down and watch out for email phishing attacks.

- Share only the information that needs to be shared. Share it securely.
- Slow down and watch out for email phishing attacks.
- Delete information when no longer needed in accordance with Ministry retention policies.
- Do not plug your phone into computers to charge.

- Be sure emails are from trusted vendors and not a bad actor attempting to trick you.
- Ensure vendors who handle our sensitive information, undergo a security risk assessment.
- Do not plug your phone into computers to charge.

Slide 11 – You play a role

Text Captions

You play a role in information safety.

Click each icon to view the security actions you can take.
As you prepare to use safe behaviors it is important to communicate using devices and email correctly. Communicate Safely and never overshare.
Slide 13 – Vignette 2

Text Captions

Audio is included in the Vignette 2 video.

The nation state sponsored Bad Actor opens Margaret's Outlook mailbox and begins searching for large spreadsheets and other files containing confidential PHI. He begins his search in her inbox. Nothing.

Margaret was diligent to save off all files containing PHI in her OneDrive. OneDrive and SharePoint are Trinity Health approved storage locations, which both store PHI safely by encrypting it at rest and do proper data backups.

Margaret also diligently deleted all PHI files from her OneDrive when no longer needed. Those are excellent security behaviors. Next, the bad actor opens Margaret’s Deleted Items folder in search of PHI files. Success.

Although Margaret kept her Inbox cleared of PHI files, she didn’t remove the files from her Deleted Items folder by selecting Empty Folder. Next up for the bad actor he searches through Margaret’s Sent Items folder. Success.

It turns out that Margaret sent a large spreadsheet report containing PHI on a weekly basis. The bad actor downloaded multiple large spreadsheets containing PHI from Margaret’s Sent Items and Deleted Items folders. It was another successful day for the bad actor.

Colleague Takeaways.

• Do not use your mailbox as a file repository.
• Consistently delete all PHI in your Inbox, Sent Items and Deleted Items folders.
• Save files with confidential information from your mailbox folders in approved storage locations such as OneDrive and SharePoint for encryption of data at rest and proper data backups.
Safe PHI Email Usage

1. Use only Trinity Health approved technology to send confidential information. External sharing of large amounts of PHI should be sent via Trinity's secure file transfer.

2. Internal sharing of PHI should be only the “minimum necessary” with those colleagues who need the information to do their job.

3. Enter “Secure” in the Subject Line, to encrypt the message before sending externally.

4. Remember to delete messages containing PHI from your Inbox, Sent, and Deleted Items folders.

5. When sharing PHI internally via email, use file links versus attachments for greater protection.

Text Captions
Margaret helps to teach us a lesson, when sharing Patient Health Information through email keep these guidelines in mind. Click each number to learn more.
Email Usage

Do not send confidential Trinity Health information to your own personal email address (Gmail, Yahoo, etc.).

- Trinity Health confidential information is no longer protected and secure once sent externally to a personal mailbox.

Text Captions

Do not send confidential Trinity Health information to your own personal email address such as Gmail, yahoo etc.

Trinity Health confidential information is no longer protected and secure once sent externally.
Text Captions

Professional criminals are trying to trick you by playing on your emotions. They always want you to do something or take action; like clicking a link, downloading an attachment, entering your user login credentials, visiting a site, etc. When receiving emails or text messages approach them with a questioning attitude. This section will help you recognize social engineering and phish warning signs.
Text Captions

Audio is included in the Vignette 3 video.

Even though senior financial analyst Bob was always flooded with incoming email, he consistently paused to look for the warning signs of a malicious phish, especially if the message had the external warning banner.

Unless Bob expected the message or confirmed the source, Bob never clicked the links, downloaded attachments or ever entered his credentials. He considered himself to be the Trinity Health front line of defense, and rightfully so.

Then, on one beautiful day in Detroit, when it wasn’t overcast, raining or snowing, Bob received this email from Jenny Robinson. Bob’s human firewall senses immediately perked up when he saw the external warning banner.

I don’t know a Jenny Robinson. I’ve never heard of a securefileshares.com email domain. Even though it does state, this link will work for Trinity Health colleagues. That could definitely be another sneaky trick. There’s no corporate logo or ID. There’s no way to verify or call. This looks like a bad actor using the curiosity approach to get me to click the link.

I’m not falling for this trick. I’m reporting it using the report phishing button. When in doubt, click the trout.

Bob was the first colleague to report the phishing message to the security team. The security team analyzed the phishing email within a sandbox safe environment and determined the message was indeed a malicious phish. Blocked the sender’s email address to prevent further malicious messages sent to Trinity Health. Purged all emails from that sender sitting in other colleague mailboxes to prevent others from clicking on the phish. Reset passwords for two colleagues who did click on the link and may have provided their user credentials to the phish.

Bob’s quick actions resulted in no confidential data being compromised, and Trinity Health Information Systems were once again protected.
Social Engineering Leverages Emotional Triggers

These are the emotionally charged phishing topics which colleagues clicked the most:

- Check Eligibility for a Computer Refresh
- Satisfaction Survey to Enroll in a Gift Card Giveaway
- Time Off Request Denied
- Password Reset Required Today

Text Captions

Watch for Emotional Triggers. These are examples of the most emotionally charged phishing topics which colleagues clicked the most; a warning to check the eligibility for a computer refresh, satisfaction survey to enroll for a gift card giveaway, time off request denied, and password reset required today.

These are some social engineering attacks that Trinity Health has experienced. Select each Social engineering attack type to reveal the colleague action you can take.
Click the Social Engineering Attack type to reveal the colleague action.

**Phone SMiShing & Vishing**
You receive a random phone call or text trying to trick you into providing confidential information or buy something that has monetary value.
- Threat actors have even pretended to be both CEO & President Mike Sulowski and other Ministry Presidents.

**Rogue (Unknown) USB Drives**
Threat actors randomly drop USBs in TH parking lots and facilities. Some USBs even include a TH logo. Once plugged into a TH device, malware executes which may provide access to our information systems and data.

**Spear Phishing**
This is a more sophisticated phishing attempt that targets a specific person using personalized information to make the email appear legitimate. Frequently, social media accounts, i.e., LinkedIn, Facebook, etc. are a primary source of collecting personalized data on you.

**Colleague Action**
- **Don’t respond!** Report it using ServiceNow Self Service or contact the TIS Service Desk.
- **Never plug an unknown USB into any device.** Report it using ServiceNow Self Service or contact the TIS Service Desk.
- **Report the suspicious email using the Outlook “Report Phishing” Button.** This is the fastest way to send the message directly to the security team.

---

**Slide 19 – Social Engineering Attacks**

**Text Captions**
Some of the phishing warning signs are below. One or more of these may exist, but always trust your gut and validate with the sender if you are unsure.

Click the Social Engineering Attack type to reveal the colleague action.
Text Captions

Some of the phishing warning signs are below. One or more of these may exist, but always trust your gut and validate with the sender if you are unsure.

Click each check to learn more about Phish Warning signs

<table>
<thead>
<tr>
<th>Follow These Practices To Keep Your Data Safe</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Look for the Trinity Health External Warning Banner. If it really is from a TH colleague, it will NOT include the banner.</td>
</tr>
<tr>
<td>✔ Did you expect the message? Should you be receiving this message on your work email?</td>
</tr>
<tr>
<td>✔ Does the title or message imply urgency or raise your emotions?</td>
</tr>
<tr>
<td>✔ Is it asking you to act or respond, i.e., click links, download attachments, provide your user credentials, reply?</td>
</tr>
<tr>
<td>✔ Do the “From” and “Reply-To” fields match?</td>
</tr>
<tr>
<td>✔ Are there misspellings or unusual words or phrases used?</td>
</tr>
<tr>
<td>✔ Should the message include an official signature, corporate logo, and/or contact information to verify their validity?</td>
</tr>
<tr>
<td>✔ Is the message sent at an unusual time, i.e., 3:30 AM?</td>
</tr>
</tbody>
</table>

Brilliant Tip of the Day: SLOW DOWN AND PAUSE
Slide 21 – Phishing Warning Signs

Text Captions
This simulation duplicates a real, malicious phish that Trinity Health colleagues were susceptible to. Click each circle to learn more.
Slide 22 – Knowledge Check

Text Captions

It is your turn to spot the warning signs. Select all the warning areas. When complete click the forward button.
We are now seeing occasional instances of malicious internal messages being sent to colleagues. This resulted from colleague compromised credentials.

These messages will have very limited warning signs. But if the message doesn’t feel right or seems unusual, call the sender, speak with your supervisor, or report it using the Outlook “Report Phishing” Button.

The example shown is from a real, internal phishing attack here at Trinity Health.
Be diligent even with text messages you receive. This is a smishing attempt made to colleagues of Trinity Health.
Along with watching for the cyber-attacks, it is important to be aware of your surroundings. Keep Trinity Health devices, data and systems safe.
While working from home and in public spaces it is important to keep remote machines safe. Make sure you are positioned so no one passing by can see your screen, initialize screensavers when walking away from your workstation or Workstation On Wheels (WOW). If taking devices offsite, do not leave them unattended.
Keeping Information and Devices Safe

**DO**
- Lock devices in the trunk if leaving the vehicle unattended.
- Keep devices secure and out of plain view if a trunk is unavailable.

**DO NOT**
- Do not leave devices unattended in public places.
- Do not place devices in checked luggage.

Text Captions
Not only do we need to be careful with email, text messages, etc., we need to be security aware when traveling and working remote.
Keeping Information and Devices Safe

Remote working
- Find a private space to work when working remotely.
- Lock the screen when you walk away from your computer.

Keep Meetings Private
- Use headsets or ear buds.
- Use a private space away from other people when discussing confidential information.

Keep Printed Information Private
- Lock or secure hardcopy confidential information to prevent others from viewing it.
- Shred when no longer needed, with supervisor approval.

Delete Electronic Data
- Delete electronic data when no longer needed.
- Select “Empty Folder” to empty your Deleted Items folder.

Select each icon to review more steps to maintain safety when working remote.

Text Captions
Select each icon to review more steps to maintain safety when working remote.
Support the Team

- Report Security Incidents

Text Captions

Part of your role is keeping information secure and reporting potential incidents to keep the team and organization safe.
Text Captions

Here are some actions you should take if your Trinity Health laptop is lost. Contact your manager, create a Service Now Ticket, or call the Service Desk.
Slide 33 – Report Phishing Attempts

Text Captions
You can stop a cyberattack by reporting suspicious emails.
The “Report Phishing” button is the fastest way to report potential phishing cyberattacks directly to Security.
Reporting Incidents

- Use the Outlook “Report Phishing” Button to report suspicious email messages.
- Submit a ServiceNow Self Service ticket or call the TIS Service Desk at 888-667-3003 for all other incidents.

Help with Security Questions
- Email AskCybersecurity for Security Questions or Comments
- Contact your local Regional Security Officer (RSO)
- Ask your Supervisor

Text Captions
Be a guardian. Together, we must all report incidents to keep our patients and information systems safe. Refer to the information shown to report incidents.
You have completed the annual security learning module. Keep Trinity Health safe and secure by practicing the TogetherSafe Behaviors to prevent Security Incidents. Remember to Prepare for the Process and Manage the Task, Communicate Clearly, present a Questioning Attitude, pay Attention to Detail and Support the Team. Close this window to return to the course page to complete the post test.