

# Security Awareness 2025

## 1. Intro Slides

### 1.1 Security Awareness



#### **Audio:**

Hello and welcome to Trinity Health Security Awareness course.

### 1.3 Introduction Video



#### Key Points:

- **Frontline Defense:** As a Trinity Health colleague, you play a crucial role in defending against cyberattacks, making cybersecurity a top priority for everyone, regardless of their role.
- **Annual Training Updates:** The cybersecurity awareness training is updated annually by the in-house cybersecurity team to keep everyone informed about the latest threats and defense strategies. This training has also received international recognition for its quality.
- **Impact of Security Habits:** Good security habits are essential as they directly impact the safety and care of patients, medical devices, and confidential data. Reporting suspicious messages using the report phishing button is a critical part of this defense, now enhanced with AI software to stop cyberattacks immediately.

## 1.4 Objectives

**Wrap Up**

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

|                                                                                                                          |                                                                                      |                                                                                                                     |                                                                                                 |                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|                                         |     |                                    |                |  |
| <b>Prepare for the Process and Manage the Task</b>                                                                       | <b>Communicate Clearly</b>                                                           | <b>Questioning Attitude</b>                                                                                         | <b>Attention to Detail</b>                                                                      | <b>Support the Team</b>                                                           |
| <ul style="list-style-type: none"><li>• Using Strong Passwords</li><li>• Utilizing Multi-factor Authentication</li></ul> | <ul style="list-style-type: none"><li>• Demonstrating Safe Email practices</li></ul> | <ul style="list-style-type: none"><li>• Recognizing Social Engineering Techniques and Phish Warning Signs</li></ul> | <ul style="list-style-type: none"><li>• Keeping Systems, Devices and Information Safe</li></ul> | <ul style="list-style-type: none"><li>• Reporting Security Incidents</li></ul>    |

26 of 27

### Audio:

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.

## 2. Prepare for the process

### 2.1 Prepare for the Process and Manage the Task

**Prepare for the Process and Manage the Task**

- Exercise Strong Password Guidelines
- Utilize Multi-factor Authentication (MFA)



5 of 27

### Audio:

In healthcare, good cybersecurity habits are like good hand hygiene—they need to be practiced consistently. Both are essential and work together to keep everyone safe. Cybersecurity basics include habits like using strong passwords and setting up multi-factor authentication (MFA) for added security.

## 2.2 Password Guidelines

### Password Guidelines

*Drag and drop each item to the correct field.  
Click **Submit** to confirm your choices.*

Get Creative! Passphrases and sentences are harder to crack.

Combine symbols, upper and lower case characters.

Reuse passwords on more than one account/site.

Use easy to guess passwords.

Create long passwords.

Use single words found in the dictionary.

Write passwords down.

Use your Trinity Health password anywhere else.

✓ Do

✗ Do Not

6 of 27

Activity for colleagues to indicate which passwords to practice or not practice.

| Password Guidelines                                          | Practice - Do or Do Not |
|--------------------------------------------------------------|-------------------------|
| Get Creative! Passphrases and sentences are harder to crack. | Do                      |
| Combine symbols, upper and lower case characters.            | Do                      |
| Write passwords down.                                        | Do Not                  |
| Use your Trinity Health password anywhere else.              | Do Not                  |
| Use easy to guess passwords.                                 | Do Not                  |
| Use single words found in the dictionary.                    | Do Not                  |
| Reuse passwords on more than one account/site.               | Do Not                  |
| Create long passwords.                                       | Do                      |

## 2.3 Multi-factor Authentication



### Multi-factor Authentication

- MFA is an authentication method that uses two or more distinct mechanisms to validate a user's identity, rather than just a simple username and password combination.
- Users may receive a verification prompt to their mobile device when authenticating to MFA-enabled **Trinity Health applications**.
- At **work**, colleagues who interface with third parties should always enable MFA on their application(s) when available to protect Trinity Health confidential information.
- At **home**, enable MFA when the option is available to ensure both your privacy and security at financial institutions, etc.

7 of 27

### Audio:

- MFA is an authentication method that uses two or more distinct mechanisms to validate a user's identity, rather than just a simple username and password combination.
- When requested to authenticate into Trinity Health applications, the preferred method to validate your identity is a number matching verification prompt sent to your mobile device.
- At work, colleagues who interface with third party suppliers should always enable MFA when available. to protect Trinity Health confidential information.
- At home, enable MFA when the option is available to ensure both your privacy and security at financial institutions, etc.

## 3. Communicate Clearly

### 3.1 Communicate Clearly and Correctly

#### Communicate Clearly and Correctly

- Demonstrate safe email practices.



8 of 27

#### Audio:

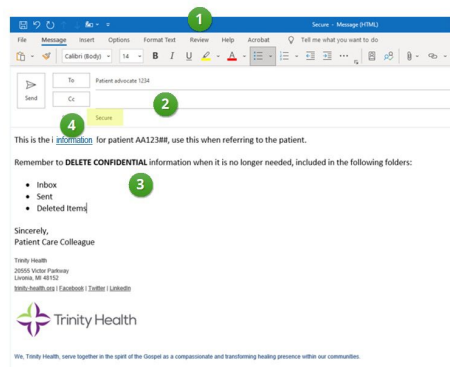
As you prepare to use safe behaviors, it is important to communicate using devices and email correctly. Communicate clearly and correctly. Demonstrate safe email practices.

### 3.2 Sharing PHI and Other Confidential Information

#### Sharing PHI and Other Confidential Information

[Click each number to learn more.](#)

- 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.



9 of 27

#### Audio:

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. Click each number to learn more.

### 3.3 Email Usage

#### 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.
- Use your Trinity Health email address for business purposes only, and not for any personal reasons such as social media, blogs, banking, doctor, school, shopping, etc.



10 of 27

#### Audio:

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. Use your Trinity Health email address for business purposes only, and not for any personal reasons such as social media, blogs, banking, doctor, school, shopping, etc.

## 4. Questioning Attitude

### 4.1 Questioning Attitude

#### Questioning Attitude

- Recognize Social Engineering and Phish Warning Signs



11 of 27

#### Audio:

Professional criminals often try to trick people by playing with their emotions. They want you to take some kind of action, like clicking a link, downloading an attachment, entering your login details, or visiting a specific website. Whenever you get emails or texts, it's important to be cautious and ask yourself if they seem suspicious. This section will teach you how to spot the warning signs of social engineering and phishing tricks.

---

## 4.2 Monique and the Malicious Phish



### Key Points:

- **Leadership and Dedication:** Monique is a highly motivated nurse practitioner and former staff sergeant in the U.S. Army, known for her leadership and dedication.
- **Cybersecurity Vigilance:** Monique is proactive in cybersecurity, teaching others to detect and report suspicious emails using the Outlook Report Phishing button.
- **Incident Handling:** Monique identified a phishing email by recognizing warning signs such as an external warning banner, misspellings, and incorrect grammar. Her prompt reporting helped remove the malicious email from multiple mailboxes, preventing a potential cyberattack attacks.



## Phone SmiShing and Vishing Definition

### Social Engineering Attacks

| Term                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Phone SMiShing and Vishing |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Rogue (Unknown) USB Drives |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Spear Phishing             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Tailgating                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                            | <b>Phone SMiShing and Vishing -</b> <p>You receive a random phone call or text trying to trick you into providing confidential information or buy something that has a monetary value.</p> <ul style="list-style-type: none"><li>Threat actors have even pretended to be Trinity Health CEO and President Mike Slubowski as well as Ministry Presidents.</li></ul> <b>Colleague Action:</b> <ul style="list-style-type: none"><li>Don't respond! Report it using ServiceNow Self-Service or contact the TIS Service Desk.</li></ul> |

13 of 27

## Spear Phishing Definition (Slide Layer)

### Social Engineering Attacks

| Term                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Phone SMiShing and Vishing |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Rogue (Unknown) USB Drives |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Spear Phishing             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Tailgating                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                            | <b>Spear Phishing -</b> <p>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.</p> <b>Colleague Action:</b> <ul style="list-style-type: none"><li>Report the suspicious email using the Outlook "Report Phishing" button. All reported messages are immediately analyzed whether they are Malicious, Spam or Safe.</li></ul> |

When in Doubt,  
Click the Trout!



13 of 27

## Rogue USB Drive Definition (Slide Layer)

### Social Engineering Attacks

| Term                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Phone SMiShing and Vishing |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Rogue (Unknown) USB Drives |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Spear Phishing             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Tailgating                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                            | <b>Rogue USB Drives -</b> <p>Threat actors randomly drop USBs in Trinity Health parking lots and facilities. Some USBs even include the Trinity Health logo. Once plugged into a Trinity Health device, malware executes which may provide access to our information systems and data.</p> <b>Colleague Action:</b> <ul style="list-style-type: none"><li>Do not insert the rogue USB into any device! Report it using ServiceNow Self-Service or contact the TIS Service Desk.</li></ul> |

13 of 27

## Phishing Definition (Slide Layer)

### Social Engineering Attacks

| Term                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing                   | <b>Phishing -</b><br><br>The most common cyberattack by threat actors is the act of sending emails or other messages pretending to be from reputable companies to entice individuals to reveal confidential information such as PHI, PII, passwords, etc.<br><br><b>Colleague Action:</b> <ul style="list-style-type: none"><li>• If the message seems suspicious or raises your emotions, use the Outlook "Report Phishing" Button to report it.</li></ul> |
| Phone SMiShing and Vishing |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Rogue (Unknown) USB Drives |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Spear Phishing             |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Tailgating                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

When in Doubt,  
Click the Trout!



13 of 27

## Tailgating Definition (Slide Layer)

### Social Engineering Attacks

| Term                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Phishing                   | <b>Tailgating -</b><br><br>Tailgating is a physical security breach that occurs when someone follows another person through a secured door or into a protected area without using their badge or having proper authorization.<br><br><b>Colleague Action:</b> <ul style="list-style-type: none"><li>• Be aware of your surroundings and do not allow others to gain access with you.</li><li>• Report the activity immediately.</li><li>• Do not put yourself in jeopardy by attempting to physically stop the unauthorized person yourself.</li></ul> |
| Phone SMiShing and Vishing |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Rogue (Unknown) USB Drives |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Spear Phishing             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Tailgating                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

13 of 27

## 4.4 Have a Questioning Attitude if an Email Raises your Emotions



### Have a Questioning Attitude if an Email Raises your Emotions

These are examples of emotionally charged emails:

- Password resets
- Gift card giveaways
- Time off request rejected
- External Human Resource messages

When in Doubt,  
Click the Trout!



14 of 27

Notes:

- These are examples of emotionally charged emails.
- Password resets
- Gift card giveaways
- Time Off Request rejected
- External Human Resources messages
- When in Doubt, Click the Trout!

## Phish Warning Signs

[Click each number to learn more.](#)





15 of 27

### Notes:

Phish Warning Signs.

This message mirrors a real malicious phish that cyber attacked a health ministry. Click each number to learn more.

## 4.6 Malicious Phish Warning Signs Activity

(Drag and Drop, 10 points, 2 attempts permitted)

### Malicious Phish Warning Signs Activity

The boxes contain information about an email you have received. Review the items in the boxes.

**Drag and Drop the item to *More Likely* if the information shows it could contain a malicious phish.**  
**Drag and Drop the item to *Less Likely* if the item does not indicate a malicious phish.**

|                                                                     |                                                                                               |                                                                    |                                                                        |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------|------------------------------------------------------------------------|
| Message does not contain the Trinity Health External Warning Banner | Message containing the External Warning banner is requesting that you enter your credentials. | Title or message that implies urgency or raises emotions           | Asking you to respond or act. i.e., click links, download attachments. |
| Misspelled words or phrases.                                        | Message sent during normal hours.                                                             | Message includes official signature and valid contact information. |                                                                        |

More Likely

Less Likely

16 of 27

| Drag Item                                                                                     | Drop Target        |
|-----------------------------------------------------------------------------------------------|--------------------|
| Message does not contain the Trinity Health External Warning Banner                           | Less Likely Target |
| Misspelled words or phrases.                                                                  | More Likely Target |
| Message includes official signature and valid contact information.                            | Less Likely Target |
| Message sent during normal hours.                                                             | Less Likely Target |
| Message containing the External Warning banner is requesting that you enter your credentials. | More Likely Target |
| Title or message that implies urgency or raises emotions                                      | More Likely Target |
| Asking you to respond or act. i.e., click links, download attachments.                        | More Likely Target |

| Drag and drop properties                                      |
|---------------------------------------------------------------|
| Return item to start point if dropped outside any drop target |
| Snap dropped items to drop target (Snap to center)            |

**Feedback when correct:**

That's right! You selected the correct responses.

**Feedback when incorrect:**

You did not select the correct responses.

**Notes:**

---

The boxes contain information about an email you have received. Review the items in the boxes.  
Drag and drop the item to the **More** Likely area if the information shows it could contain a malicious phish.  
Drag and drop the item to the **Less** Likely area if the item does not indicate a malicious phish.  
Click Submit when finished.

## 4.7 Joe and the Questionable Request

Joe and the Questionable Request

[Click to play video!](#)

Video

This slide does not include narration. Audio is included in the video.

17 of 27

Highlight key points

Notes:

## 5. Attention to Detail

### 5.1 Attention to Detail

Attention to Detail

- Use devices safely.
- Keep systems and information safe.



18 of 27

Notes:

Along with watching for the cyber attacks, it is important to be aware of your surroundings. Use devices safely, keep systems and information safe.

## 5.2 Keep Devices and Information Safe



### Keep Devices and Information Safe

When working in public spaces, keep devices and information safe:

- Initialize screen savers when walking away from your workstation or Workstation On Wheels (WOW).
- If taking devices offsite, do not leave them unattended.

19 of 27

### Notes:

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 working offsite, always take your device with you.

## 5.3 Artificial Intelligence (AI) Guidance for Colleagues

### Artificial Intelligence (AI) Guidance for Colleagues

- Do not share Trinity Health confidential information (PHI/PII) with any **Artificial Intelligence (AI)** application not specifically approved for that purpose. This includes AI software used to record/transcribe meetings.
- Information **output** from an AI system should be validated to ensure accuracy. **Fact-check** information against (multiple) credible sources to avoid inaccuracies.



20 of 27

### Notes:

Artificial Intelligence (AI) is being used more and more. We are providing some guidance while using AI.

Do not share Trinity Health confidential information (PHI /PII) with any **Artificial Intelligence (AI)** application not specifically approved for that purpose. This includes AI software used to record/transcribe meetings.

Information **output** from an AI system should be validated to ensure accuracy.

**Fact-check** information against (multiple) credible sources to avoid inaccuracies.

## 5.4 AI-use and Trinity Health Information



### AI-use and Trinity Health Information

AI applications such as ChatGPT, Otter.ai, and Gemini are **not** approved for use with Trinity Health confidential (PHI/PII) information.

If Trinity Health **confidential information** is shared with an unapproved AI application, it can **directly** lead to data leakage and violates both Trinity Health Security Policies and regulatory obligations.

21 of 27

### Notes:

AI applications such as ChatGPT, Otter.ai, and Gemini are **not** approved for use with Trinity Health confidential (PHI/PII) information.

If Trinity Health **confidential information** is shared with an unapproved AI application, it can **directly** lead to data leakage and violates both Trinity Health Security Policies and regulatory obligations.

## 5.5 Safely Use Devices

### Safely Use Devices

Remote Working

Meetings

Printed Information

Electronic Data

Traveling

Software

Click each **Tab** to learn more.

22 of 27

Delete this screen

### Notes:

Select each tab to review more steps to maintain safety when working.

## Remote WorkingLayer (Slide Layer)

**Safely Use Devices**

Remote Working Meetings Printed Information Electronic Data Traveling Software

**Remote Working**

When working remotely:

- Keep screens from view of others.
- Find a private space to work.
- Lock the screen when you walk away from your computer.



22 of 27

## MeetingLayer (Slide Layer)

**Safely Use Devices**

Remote Working Meetings Printed Information Electronic Data Traveling Software

**Meetings**

When conducting virtual meetings without others physically present:

- Use headsets or ear buds when others nearby might overhear.
- Use a private space away from other people when discussing confidential information.



22 of 27

## Printed InformationLayer (Slide Layer)

**Safely Use Devices**

Remote Working Meetings Printed Information Electronic Data Traveling Software

**Printed Information**

- Keep your desktop free of papers.
- Secure or lock hardcopy.
- Shred documents when no longer needed, with supervisor approval.



22 of 27



## Electronic Data Layer (Slide Layer)

### Safely Use Devices

Remote Working

Meetings

Printed Information

Electronic Data

Traveling

Software

#### Electronic Data

Handling Electronic PHI

- Delete all PHI from repositories, e.g. SharePoint, Teams, etc., when no longer needed.
- Delete all PHI in your Outlook mailbox including Inbox, Sent and Deleted Items folders. **Do not use your mailbox as a file repository.**



22 of 27

## TravelingLayer (Slide Layer)

### Safely Use Devices

Remote Working

Meetings

Printed Information

Electronic Data

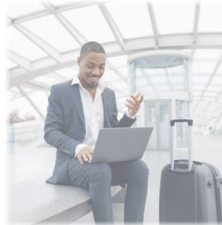
Traveling

Software

#### Traveling

When Traveling:

- Lock devices in the trunk if leaving the vehicle unattended.
- Keep devices secure.
  - Do not leave devices unattended in public places.
  - Do not place devices in checked luggage.
- Lock devices in your hotel room safe when unattended.



22 of 27

## Software Layer (Slide Layer)

### Safely Use Devices

Remote Working

Meetings

Printed Information

Electronic Data

Traveling

Software

#### Software

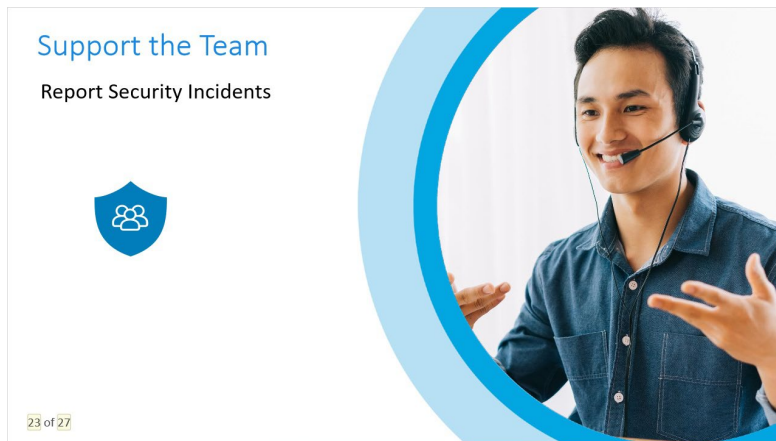
- **Never** load unauthorized software to a Trinity Health device.
- All Trinity Health approved software undergoes a rigorous security assessment to avoid vulnerabilities and impacts.



22 of 27

## 6. Support the Team

### 6.1 Support the Team



#### Notes:

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

### 6.2 Jenny Sue and the Badgeless Tailgater



Highlight key points

## 6.3 Report Lost or Stolen Devices

### Report Lost or Stolen Devices

Immediately report all Trinity Health devices and personal devices containing Trinity Health Protected Health Information (PHI) or Personally Identifiable Information (PII) that are lost or stolen.



1. Notify the TIS Service Desk at (888) 667-3003.
2. Contact your supervisor.

25 of 27

### Notes:

Immediately report all Trinity Health devices, and personal devices containing Trinity Health Protected Health Information (PHI), or Personally Identifiable Information (PII) that are lost or stolen. Notify the TIS Service Desk at (888) 667-3003 and contact your supervisor.

## 7. Wrap Up

### 7.1 Wrap up

### Wrap Up

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



#### Prepare for the Process and Manage the Task

- Using Strong Passwords
- Utilizing Multi-factor Authentication



#### Communicate Clearly

- Demonstrating Safe Email practices



#### Questioning Attitude

- Recognizing Social Engineering Techniques and Phish Warning Signs



#### Attention to Detail

- Keeping Systems, Devices and Information Safe



#### Support the Team

- Reporting Security Incidents

26 of 27

### Notes:

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.

## 7.2 Next Steps

### Next Steps

You've reached the end of this course.

Thank you for your time and attention!

Close this window to return to the course page.

Your next step will be to give your feedback on this learning experience.

27 of 27

Delete Next steps