

# Security Awareness 2026

## 1. Intro Slides

### Security Awareness



#### Navigation

How to move around:

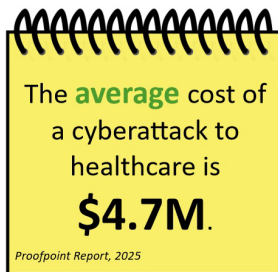
Use the **Prev** and **Next** buttons to navigate.

There is audio in this course.

Listen or read the screen and follow any instructions you see.

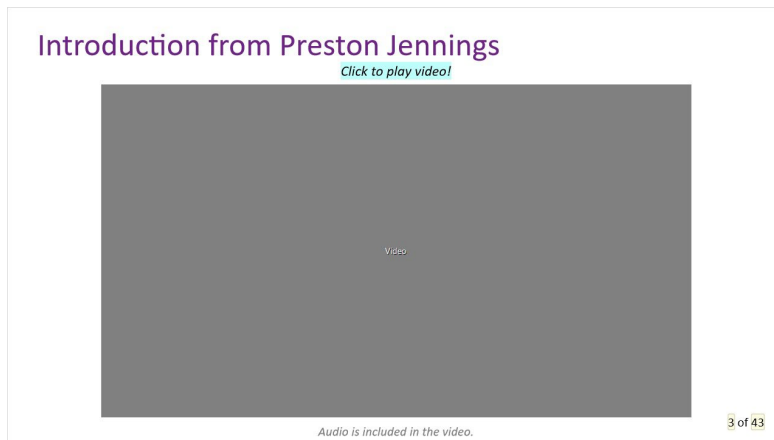
We have provided **Closed Captions**.

[Click the note to read a quick fact!](#)



Proofpoint Report, 2025

## Introduction Video



### Transcript:

Welcome. I'm Preston Jennings, Vice President and Chief Information Security Officer for Trinity Health. I appreciate that as a Trinity Health colleague, you're being assigned a wide variety of training. I'm excited to personally introduce this year's updated Cybersecurity Awareness Training to you. As always, much of the same cybersecurity defense information you'll learn applies both at work and home.

It's a fact that major healthcare systems remain a top cyberattack target.

As a Trinity Health colleague, you're truly acting as our frontline of defense against cyberattacks.

And because of that, our own cybersecurity team consistently refreshes this in-house created training annually to keep you current on the greatest threats we all need to defend against. We're doing our utmost to have you learn and apply this important information.

This same cybersecurity awareness training actually earned two separate international awards for learning and development in recent back-to-back years.

No matter your role, as a healthcare professional, we all must make cybersecurity a top priority.

As technical users, we're all protecting patients, medical devices, confidential data, information systems, and even our mission itself. Being TogetherSafe and cyber safe are very much intertwined.

While cybersecurity is critical across every industry, it's different for us and very personal.

Our daily security habits, good and bad, can directly impact the safety and care of patients in the communities we serve, and in many cases, that's our own immediate family and friends.

Everyone must consistently use good security habits and remain alert to report suspicious messages using the report phishing button.

Did you know the report phishing button is now connected to artificial intelligence software that can immediately stop a cyberattack, reporting it to our security team and enabling our teams to address similar attacks impacting other colleagues?

When in Doubt, Click the Trout!

I hope you enjoy this training and learn something new to apply. Thank you for all you do to support patients and defend Trinity Health.

## Purpose



### Purpose

This course equips every colleague to recognize cybersecurity risks, protect one another, and communicate effectively in our digital workplace. Grounded in our **core values** and shared commitment to **safety**, it provides practical tools to:

1. Proactively **prepare for and manage** cybersecurity risks.
2. **Support your team** with 200% accountability, taking full ownership of your actions and helping others do the same.
3. Apply **TogetherSafe** Behaviors to strengthen our safety culture, including:

### Purpose

3. Apply **TogetherSafe** Behaviors to strengthen our safety culture, including:

- **Communicating** clearly, confidently, and with purpose.
- Practicing **attention to detail**.
- Using a **questioning attitude** to prevent harm before it happens.

## 2. New threats

### New Threats

#### New Threats

“ It’s a fact that major healthcare systems remain a top cyber-attack target. While cybersecurity is critical across every industry, it’s different for us and very personal. ”

*Preston Jennings, VP Information Security*

## Staying Ahead of Cybersecurity Threats

### Staying Ahead of Cybersecurity Threats



#### Attention to Detail

Helps us spot subtle signs of cyber threats, like unusual activity or small inconsistencies.



#### Questioning Attitude

Encourages us to challenge assumptions, verify sources, and investigate anomalies.

Together, these behaviors empower us to detect and respond to emerging risks before they escalate.

6 of 43

## Cyberattacks Are Evolving

### Cyberattacks Are Evolving

#### Phishing & Social Engineering

Emotional manipulation designed to trick you into clicking, downloading, or sharing sensitive information

#### Ransomware

Malicious software that locks systems until a ransom is paid

#### Smishing & Vishing

Scams via text and voice calls

#### AI Generated Threats

Deepfakes and impersonation tactics



## The Call That Changed Everything

### The Call That Changed Everything

#### Your personal device isn't just personal anymore.

In today's connected world, what happens on your phone, tablet, or home computer can directly impact the safety of patients and Trinity Health.



Personal devices often lack enterprise-level protections.

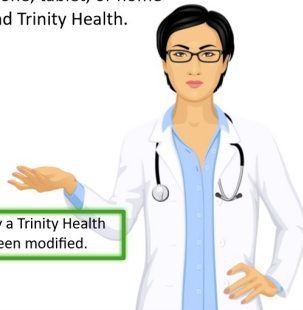


Malware or phishing attacks on personal accounts can spread to corporate systems.



Remote work and mobile access increase exposure.

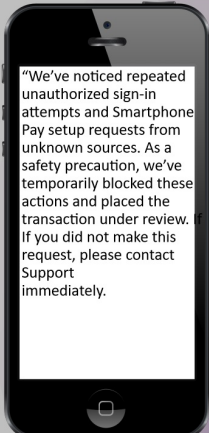
The following scenario is based on an actual event experienced by a Trinity Health colleague. To protect the individual's privacy, some details have been modified.



## The Call That Changed Everything

### The Call That Changed Everything

You've just purchased a new smartphone. A few days later, you receive a text message that appears to be from Smartphone Pay, it reads:



"We've noticed repeated unauthorized sign-in attempts and Smartphone Pay setup requests from unknown sources. As a safety precaution, we've temporarily blocked these actions and placed the transaction under review. If you did not make this request, please contact Support immediately."

## Call Placed

### Call Placed


You decide to call the number. A man named "Joseph Gomes" answers, claiming to be from Smartphone Support. He tells you that your phone, computer, and bank accounts have been hacked. He says he can help, but he needs access to another device since yours are compromised.



## Device Needed

### Device Needed

You think:



The only other device I have is my work computer. I can use it to fix this problem...

## Threat

Threat




Joseph claims Smartphone company accidentally refunded you \$10,000 and shows you a fake bank screen. He says that you must return the money or face arrest. He threatens to report you to the FTC and have you charged with theft.

Panicked and pressured, you follow his instructions—only to realize too late that it was all a scam.

## Realization – Now What?

Realization – Now What?

You feel ill because you've been scammed! You lost thousands of dollars, your identity may be stolen, and you may have just compromised both your work computer and even Trinity Health!



## Realization Activity


(Pick One)

Realization – Now What

What steps should you take now?

Select the best **action!** Then click Submit.


Monitor your financial accounts and credit.	Call the Service Desk and then inform your manager.
All of the steps	Change all passwords immediately.



Correct	Choice
X	All of the steps
	Monitor your financial accounts and credit.
	Call the Service Desk and then inform your manager.
	Change all passwords immediately.

## The Call That Changed Everything

### The Call That Changed Everything



It is important to remember: if **something feels off, raises your emotions, or is urgent**: stop and check before clicking or replying.

Avoid clicking links or calling numbers from suspicious messages. Instead, visit the official website directly to verify the information and find contact details.

## Stay Safe from New Cyber Threats

### Stay Safe from New Cyber Threats

Remember: cyber threats are always changing, but your **TogetherSafe** Behaviors help protect patient data and keep Trinity Health safe.

**Prepare for the Process**  
Know how to report anything suspicious. Use the Outlook "Report Phishing" button when something doesn't look right.

**Pay Attention to Detail**  
Watch for strange email addresses, urgent messages, or weird formatting. These are warning signs!

**Have a Questioning Attitude**  
If something feels off, or raises your emotions, stop and check before clicking or replying. Use known good contacts rather than following suspicious instructions.

### 3. Passwords & AI Guidelines


#### Passwords and AI Guidance

Passwords and AI Guidance


“ At **work** or **home**, one of the foremost cybersecurity defenses is using long, complex passwords or passphrases that are unique. When password information is captured, an 8-character password can be cracked in minutes, while complex **15+ character passwords take years to crack.** ”

#### Using Passwords Safely

Using Passwords Safely



 **Attention to Detail**

Use strong, unique passwords and only enter them in secure, trusted systems.

 **Questioning Attitude**

Be skeptical of unexpected password requests—verify the source before responding.

Together, these behaviors empower us to protect Trinity Health patients, information systems, and data.

 Trinity Health  TogetherSafe 18 of 43

#### Password Guidance



**Password Guidance**

- **NEVER** share your passwords or passphrases, especially your work credentials, and avoid using the same ones across multiple accounts or sites.
- **NEVER** reuse passwords or passphrases, especially your work password.
- Use Passphrases:
  - Chocol@telceCre@m!
  - HappyDog!Loves2Run
  - I W@nt 2 GO Hike!

## Password Passphrase Guidance


### Password Passphrase Guidance

At both **work** and **home**, create unique, strong passphrases using these in combination:

- 15+ characters minimum
- Upper and lower case letters
- Special characters
- Numbers

#### Passphrase Principles

1. Length is better than complexity.
2. Make the passphrase something easy to remember.



### Notes:

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.

## Can You Spot Risky Password Behaviors Activity

### Can You Spot Risky Password Behaviors Activity

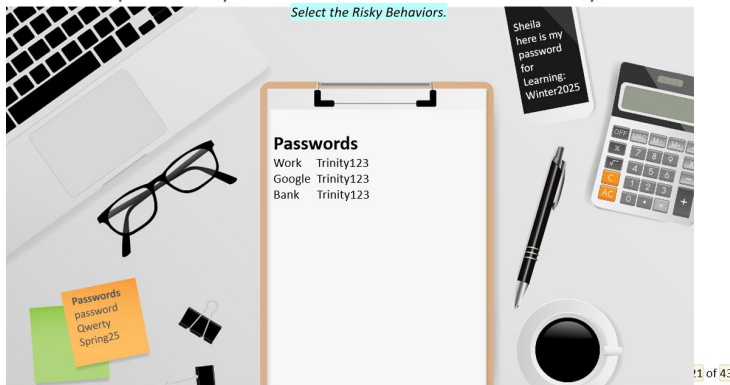


This activity highlights risky password behaviors. Start the activity and select the risky password behaviors you see.


[Click to start Activity](#)

1 of 43

## Can You Spot Risky Password Behaviors Activity



## Multi-factor Authentication



### Multi-factor Authentication

- Multi-Factor Authentication (MFA) helps keep your accounts safe by using more than just a password to confirm your identity.
- At **work**, if you use apps that connect with outside companies, **always** turn on MFA if it's available to protect private Trinity Health information.
- At **home**, using MFA with your bank or other important accounts adds extra protection to keep your personal information safe.

22 of 43

### Notes:

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.

## Using AI Safely

### Using AI Safely



#### Attention to Detail

Review AI-generated outputs carefully for accuracy, bias, or sensitive data exposure before sharing or acting on them.



#### Questioning Attitude

Is someone, including external parties, using an AI tool to record a meeting with Trinity Health sensitive/confidential information being shared? If so, ask that the recording be stopped and capture notes manually.

Together, these behaviors empower us to protect Trinity Health patients, information systems, and data.

23 of 43

## AI-use and Trinity Health Information



### AI-use and Trinity Health Information

Use only approved AI tools at work, like the **Trinity Health** version of **Copilot**. Our organization has vetted and approved Copilot for security when used with your Trinity Health ID.

Note: **Do not** put Trinity Health information in your home version of Copilot. It is not secure for Trinity Health information.

24 of 43

### Notes:



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

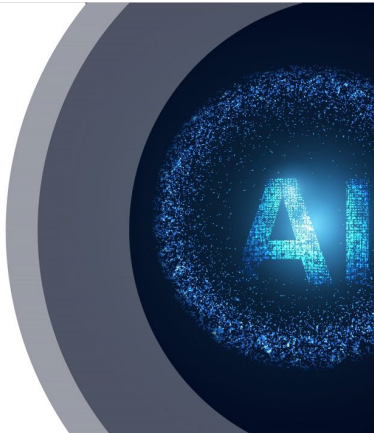
If Trinity Health **confidential information** is shared with an unapproved AI application, it can **directly** lead to data leakage and violates both Trinity Health Security Policies and regulatory obligations.

## 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 or transcribe meetings.
- Information **output** from an AI system should be validated to ensure accuracy. **Fact-check** information against multiple credible sources to avoid inaccuracies.

25 of 43  



### 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.

## Password Safety Summary

### Password Safety Summary

#### Password Security

-  • **Use strong, unique passwords** for each account (15+ characters, with a mix of upper and lower case letters, numbers, and symbols).
-  • **Enable Multifactor Authentication (MFA)** wherever possible.
-  • **Do not share passwords** or use anyone else's.

  26 of 43

## AI Safety Summary

### AI Safety Summary

#### Responsible AI Use



- **Protect sensitive data:** Never input personal or confidential info into **home** or public AI tools.



- **Verify AI outputs:** Cross-check facts, especially for work-related content.



- **Respect copyright and privacy:** Don't use AI to replicate proprietary or personal material.



- **At work,** only use the Trinity Health version of Copilot.

## 4. Cybersecurity Safety Behaviors

### Cybersecurity Safety Behaviors

#### Cybersecurity Safety Behaviors

“ Over the last year, 2,920 malicious phish were reported by individual colleagues, resulting in over 45,000 malicious phish being removed from other colleague mailboxes before they could be clicked. ”

*Preston Jennings, VP Information Security*

## Protecting Patients with TogetherSafe Behaviors

### Protecting Patients with TogetherSafe Behaviors



#### Attention to Detail

##### Cybersecurity:

- Always verify email senders and links before clicking, and follow proper data handling protocols to safeguard sensitive information.

##### Device Safety:

- Lock your devices when unattended.
- Use secure Wi-Fi networks.

##### Information Safety:

- Verify the accuracy of AI data before sharing.
- Only share confidential information with those who need to know.
- Dispose of confidential information when no longer needed.

29 of 43

## Protecting Patients with TogetherSafe Behaviors

### Protecting Patients with TogetherSafe Behaviors



#### Questioning Attitude

##### Cybersecurity:

- Report suspicious emails; **When in Doubt Click the Trout!**
- Never share or use someone else's credentials.



##### Device Safety:

- Question any unexpected Microsoft Authenticator prompts.
- Report lost or compromised devices immediately.
- Ensure a device is secure before using it to access sensitive systems.

##### Information Safety:

- Challenge requests for access to sensitive data by verifying the need and authority.
- Speak up if data handling practices seem risky or unclear.
- Confirm the legitimacy of sources before trusting or sharing information.

30 of 43

## Cybersecurity in Action: Monique's Story

### Cybersecurity in Action: Monique's Story



Meet Monique — a dedicated Nurse Practitioner and former U.S. Army Staff Sergeant who leads with courage and excellence.

In this animated video, follow Monique as she:

- Detects a suspicious email during her hospital shift
- Uses the Outlook Report Phishing button to take action
- Helps protect her colleagues and ministry from a cyberattack

Monique's quick thinking stopped a malicious email and extracted it from other colleague Inboxes.

When in Doubt,  
Click the Trout!



## Monique and the Malicious Phish



### Transcript:

Monique is a highly motivated nurse practitioner who gets things done right and leads everywhere she goes. It's just how she's wired since bravely serving as a staff sergeant in the United States army. Everyone views Monique as the best of the best. Thank you for your service, Monique.

When it comes to cybersecurity, not only is Monique fiercely protective of her health ministry, she teaches others around her how to detect and report suspicious email with the Outlook report phishing button. One early morning in the hospital, Monique was checking her work email from her workstation on wheels.

### Speaker 2

Oh my gosh. My paycheck may be wrong. Hey. Wait a minute. It has the external warning banner.

HR would never send me a message with the external banner. And who's HR at safe payroll dot com? That's not a Trinity Health email address.

It definitely raised my emotions and has a sense of urgency.

Those are warning signs.

There's a misspelling, and it's grammatically incorrect.

And there's no Trinity Health logo or any other information to confirm it's from HR.

I'm reporting this. When in doubt, I'm clicking the trout.

### Speaker 1

A few minutes later, Monique receives an email stating the message was malicious. Bam. Monique's reporting just extracted the malicious email from seventy other colleague mailboxes and stopped a cyberattack.

## Stay Alert for Phishing

### Stay Alert for Phishing

- Colleagues have received internally-sent malicious phishing messages. Be on the lookout!
- Threat actors rely on emotionally charged messages, these are the most common phishing attacks that have targeted our colleagues:
  - Password resets
  - Gift card giveaways
  - Time off request rejected
  - External Human Resource messages
  - Training required messages

When in Doubt,  
Click the Trout!

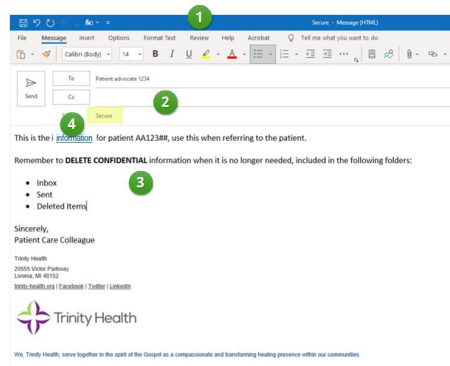


## Sharing PHI and Other Confidential Information

### 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.



34 of 43

### Notes:

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.

## Safe Email Practices

### Safe Email Practices

- **Use Email for Business Only**
  - Trinity Health email should be used exclusively for business, avoiding personal activities like social media or banking.
- **Protect Confidential Information**
  - Never send confidential data to personal emails, as it loses protection outside the Trinity Health network.
- **Sending Secure Emails**
  - Use 'secure' in the subject line or mark messages 'confidential' in Outlook to encrypt sensitive external communications.
- **Beware of Threat Actors**
  - Key roles like senior leaders, talent acquisition and supply chain must stay vigilant as attackers target business emails visible on social media for cyber threats.



### Notes:

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.

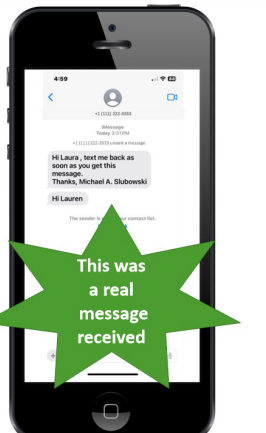
## Smishing

### Smishing


- You receive a random phone call or text trying to trick you into providing confidential information or buy something that has a monetary value.
- Threat actors have even pretended to be Trinity Health CEO and President Mike Slubowski as well as Ministry Presidents.

#### Colleague Action:

- Use your **TogetherSafe** Behavior, having a **Questioning Attitude**.
- Don't respond, reply, or click links! If it's faking another Trinity Health person, report it using ServiceNow Self-Service or contact the TIS Service Desk.



## Working in Public Spaces, Keep Devices & Information Safe



### Working in Public Spaces, Keep Devices & Information Safe

- Initialize screen savers when walking away from your workstation or Workstation On Wheels (WOW).
- Lock screens when walking away, avoid leaving devices unattended.
- Secure paper documents by shredding or storing safely.

37 of 43

### 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.

## Keeping Systems, Devices, and Information Safe



### Keeping Systems, Devices, and Information Safe

- **Digital Privacy Measures**
  - Delete electronic confidential information when not needed.
  - Use secure texting to share confidential information.
- **Travel Security Guidelines**
  - Keep devices locked in your trunk or hidden.
  - Lock devices in your hotel room safe, if possible.
- **Software and Network Safety**
  - Do not install unauthorized software.
  - Do not insert unauthorized removable media.

38 of 43

### Notes:

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

## Reporting Security Incidents & Support

### Reporting Security Incidents & Support

**Immediate Incident Reporting**


- Immediately report lost or stolen devices containing sensitive data to the TIS Service Desk and your supervisor.

**Non-Urgent Support Requests**

- Non-urgent security issues can be addressed by submitting a ServiceNow Self Service ticket for timely assistance.

**Cybersecurity Assistance**

- Email [AskCybersecurity](#) provides expert help for security questions or concerns.



39 of 43

### Notes:

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

## 5. Wrap Up

### Thank You

Thank You

“ For your continued vigilance to keep our patients, data and information systems safe.

**You** are the Front Line of Defense at Trinity Health. ”

## Apply TogetherSafe Behaviors to be Cybersafe

### Apply TogetherSafe Behaviors to be Cybersafe

- **Prepare for the Process and Manage the Task**
  - Use strong passwords
  - Utilize Multi-factor Authentication
- **Attention to Detail**
  - Keep systems, devices and information safe
- **Clear Communication**
  - Demonstrate safe email practices
- **Questioning Attitude**
  - Recognize social engineering techniques and phish warning signs



## Key Takeaways

### Key Takeaways

- Stay alert to threats like phishing, ransomware, and AI scams.
- Use strong passwords and enable Multi-Factor Authentication (MFA).
- Only use approved AI tools, never share PHI/PII with unapproved applications.
- Report suspicious activity via ServiceNow or the TIS Service Desk.

Your vigilance keeps our patients, colleagues, and data safe.

Thank you for doing your part!



## Next Steps

### Next Steps

You've reached the end of this course.

Thank you for your time and attention!



43 of 43

## Notes: