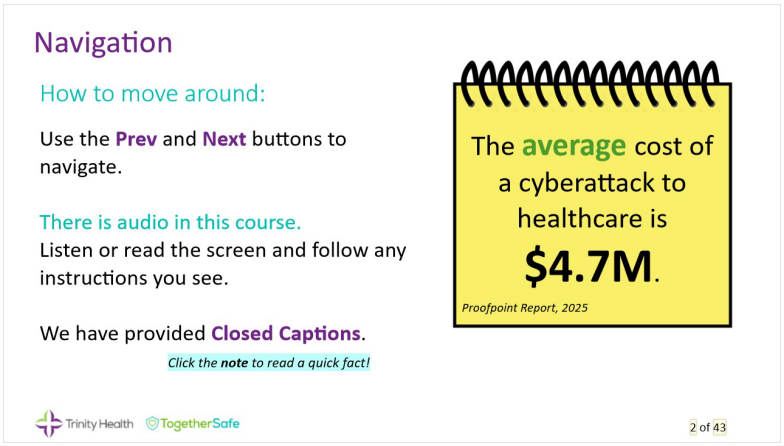
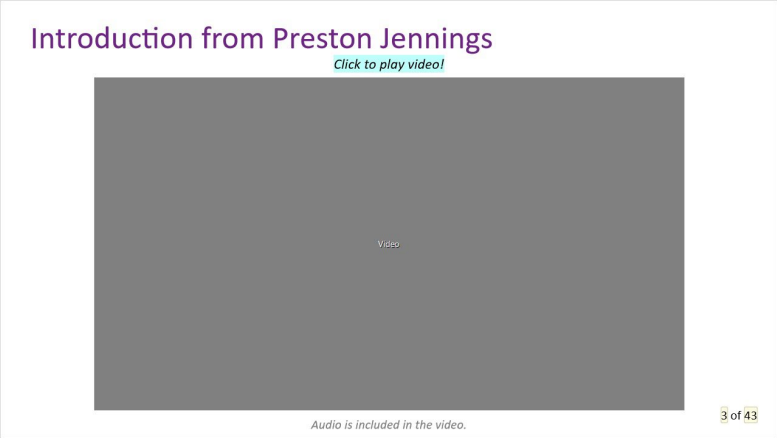
Security Awareness 2026

1. Intro Slides

Security Awareness



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 a nnually to keep you current on the greatest threats we all need to defend against. We're doing our utmo st to have you learn and apply this important information.

This same cybersecurity awareness training actually earned two separate international awards for learni ng 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 commu nities 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 usin g the report phishing button.

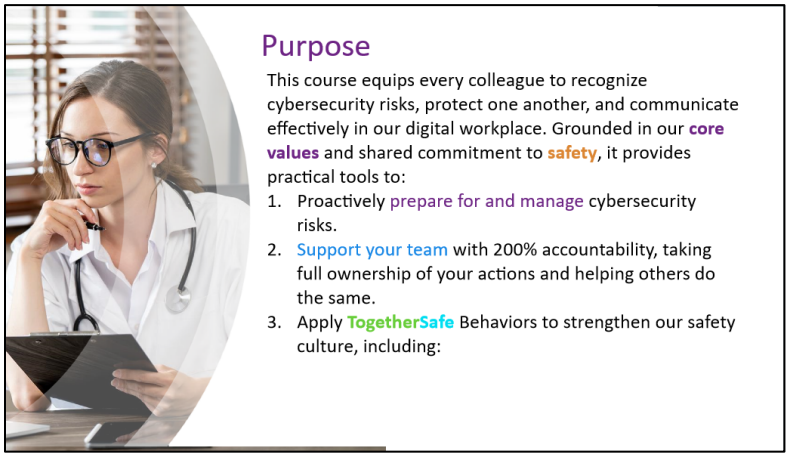
Did you know the report phishing button is now connected to artificial intelligence software that can im mediately stop a cyberattack, reporting it to our security team and enabling our teams to address similar attacks impacting other colleagues?

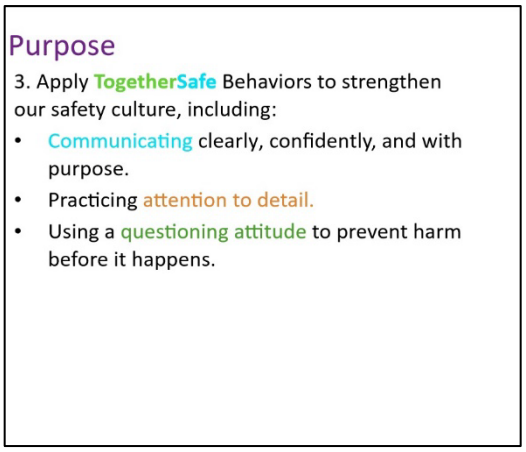
When in Doubt, Click the Trout!

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

Published by Articulate® Storyline www.articulate.com

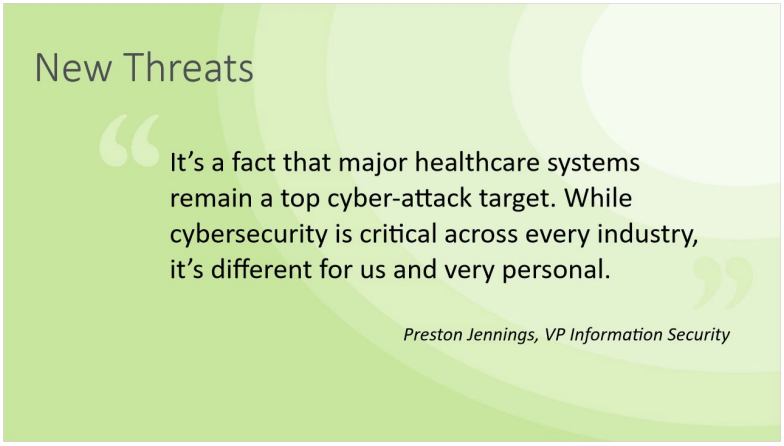
Purpose





2. New threats

New Threats

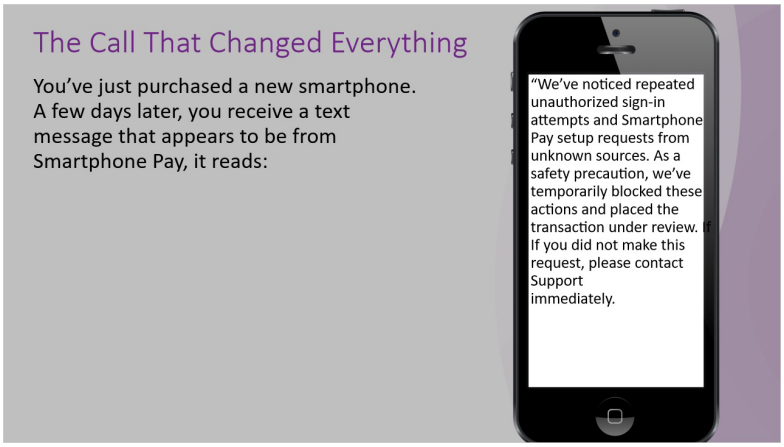


Staying Ahead of Cybersecurity Threats

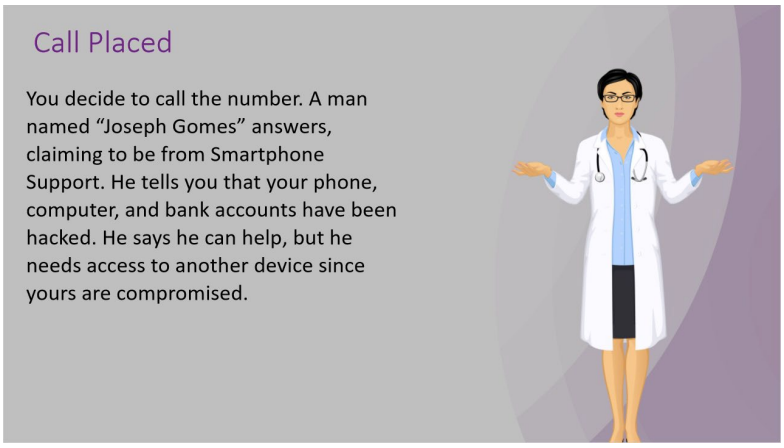
Cyberattacks Are Evolving

The Call That Changed Everything

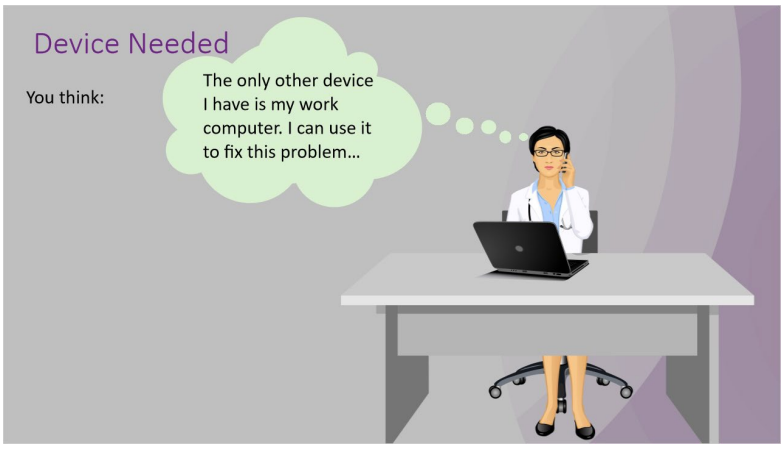
The Call That Changed Everything



Call Placed

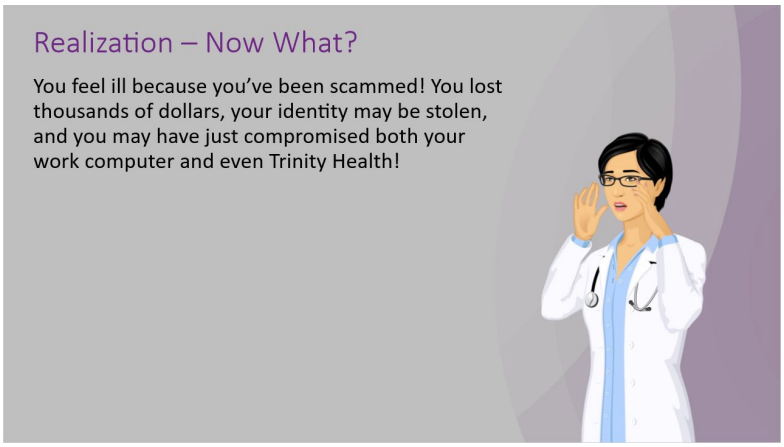


Device Needed



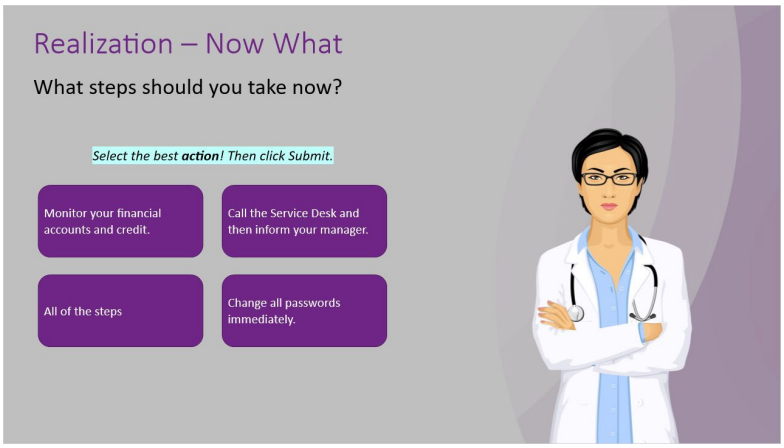
Threat

Realization – Now What?



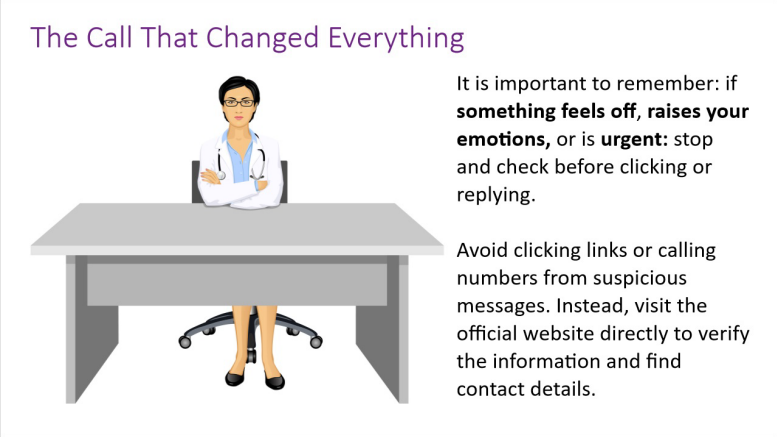
Realization Activity

(Pick One)

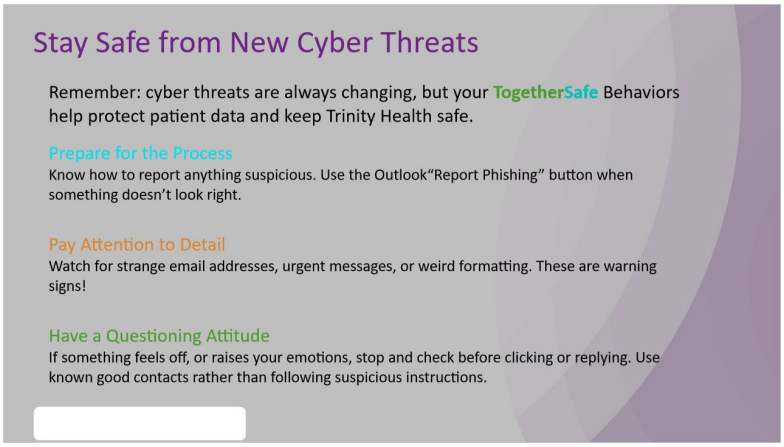


Correct	Choice
X	All of the steps
	Monitor your financial accounts and credit.
	Call the Service Desk and then inform your manager.
	Change all passwords immediately.

The Call That Changed Everything

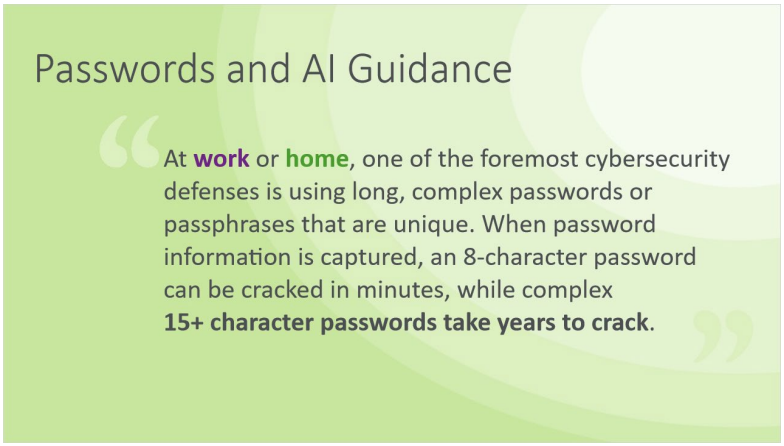


Stay Safe from New Cyber Threats

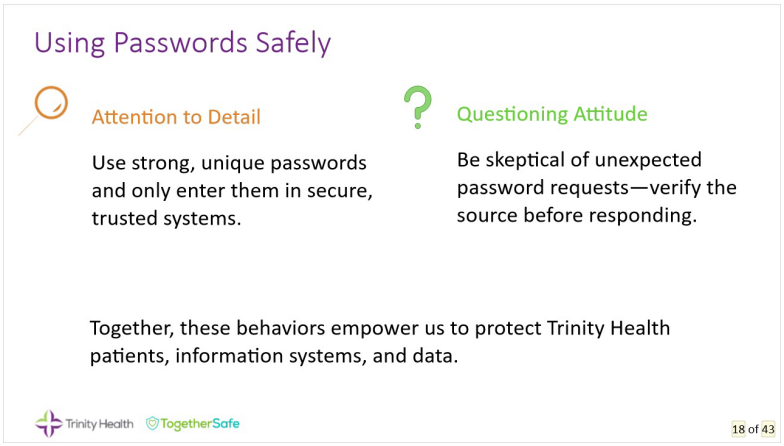


3. Passwords & AI Guidelines

Passwords and AI Guidance

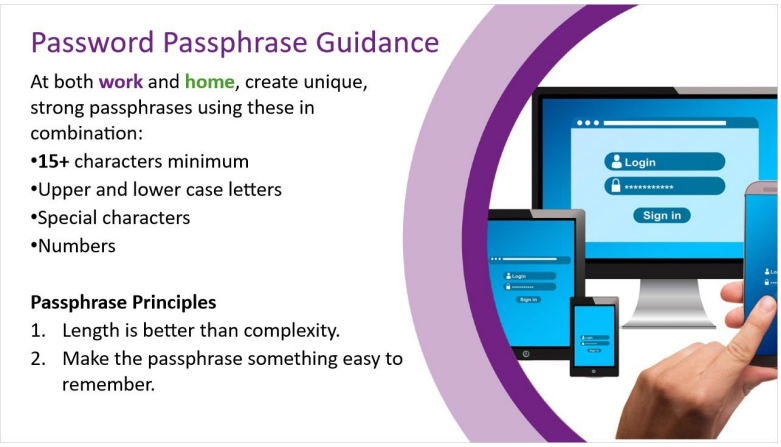


Using Passwords Safely



Password Guidance

Password Passphrase Guidance

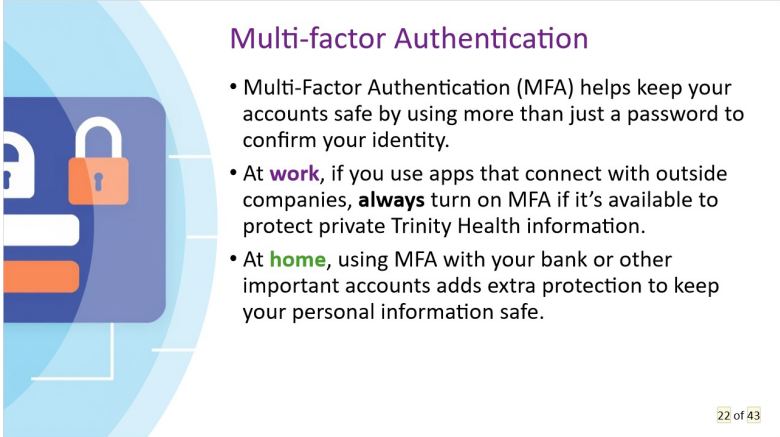


Notes:

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

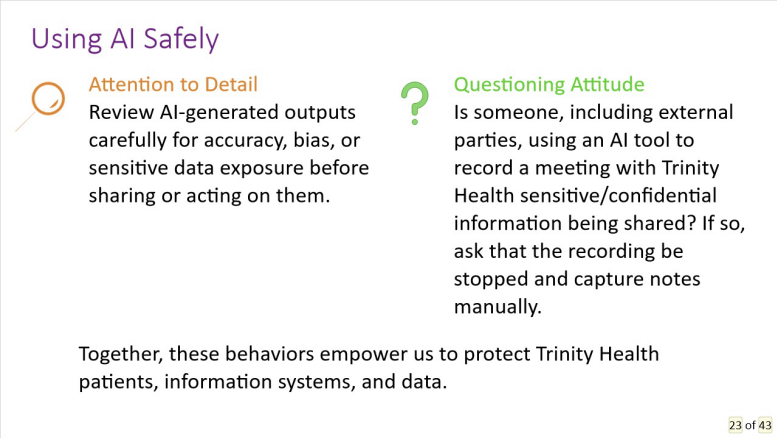
Multi-factor Authentication



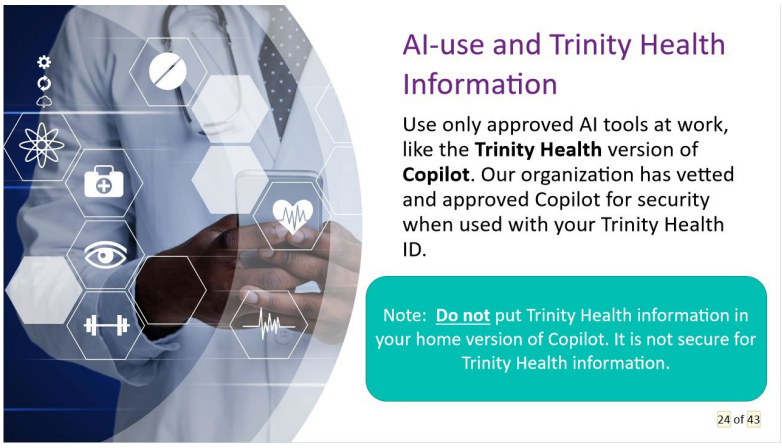
Notes:

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



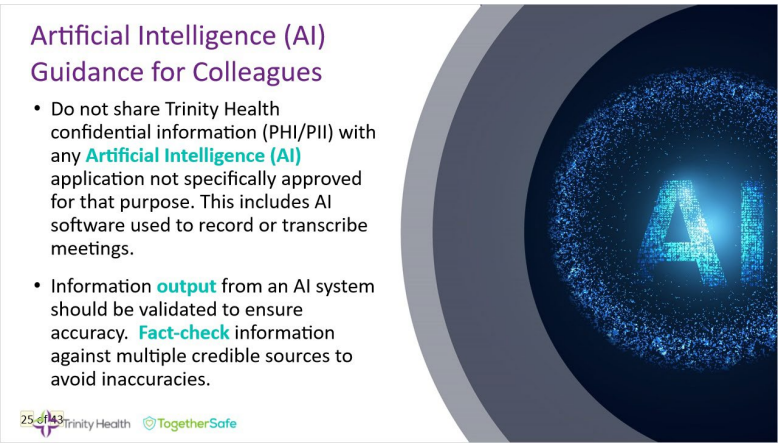
AI-use and Trinity Health Information



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.

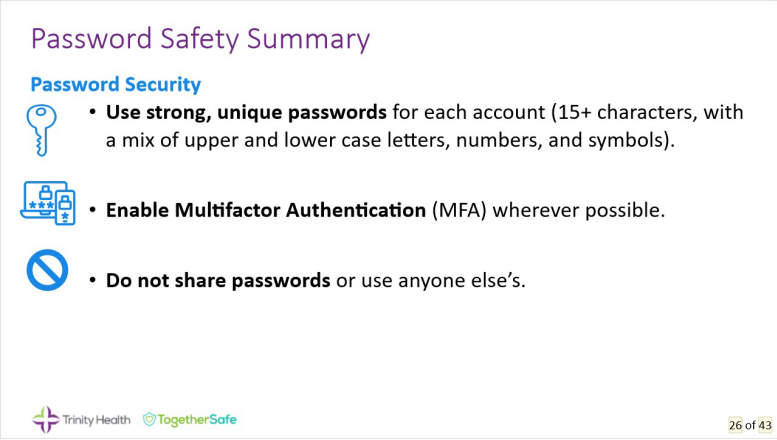
Artificial Intelligence (AI) Guidance for Colleagues



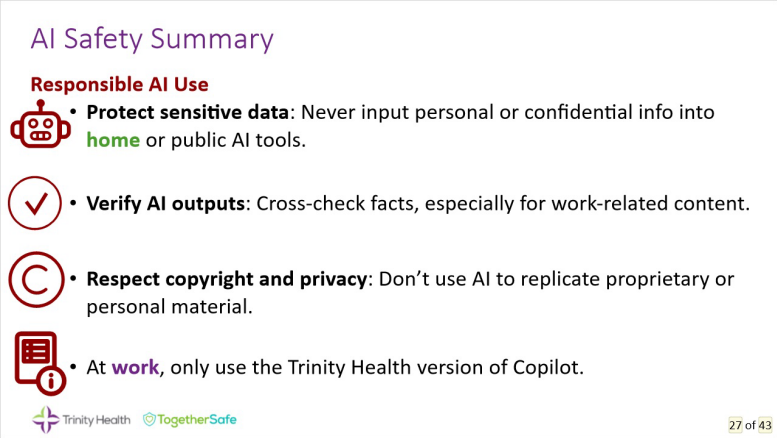
Notes:

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



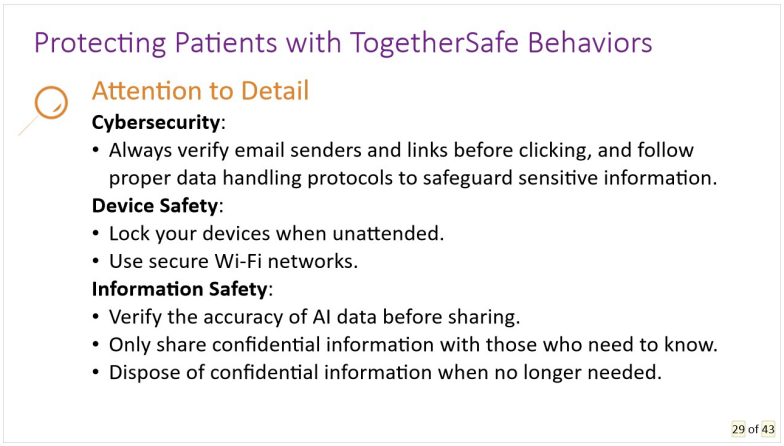
AI Safety Summary



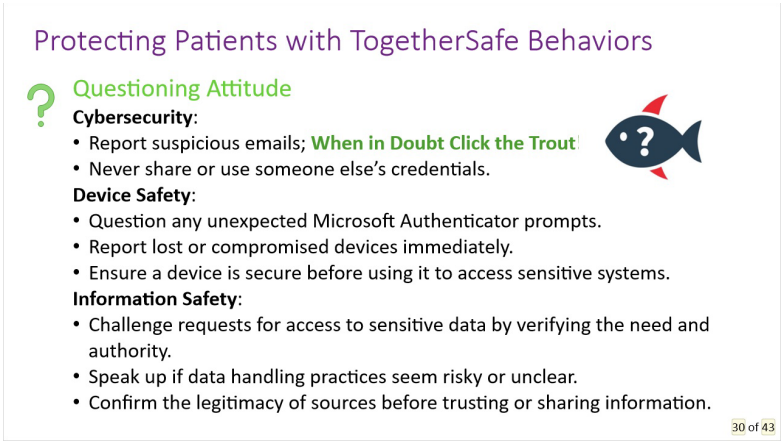
4. Cybersecurity Safety Behaviors

Cybersecurity Safety Behaviors

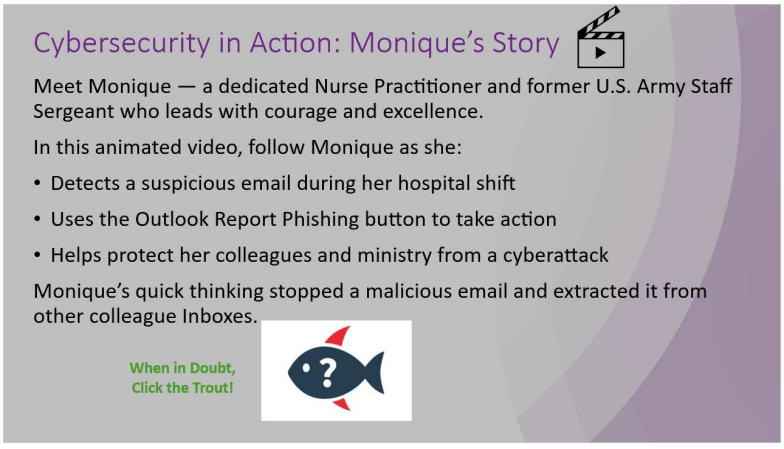
Protecting Patients with TogetherSafe Behaviors



Protecting Patients with TogetherSafe Behaviors



Cybersecurity in Action: Monique's Story



Monique and the Malicious Phish

Transcript:

Monique is a highly motivated nurse practitioner who gets things done right and leads everywhere she g oes. 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 teach es 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 wheel s.

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? Tha t'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.

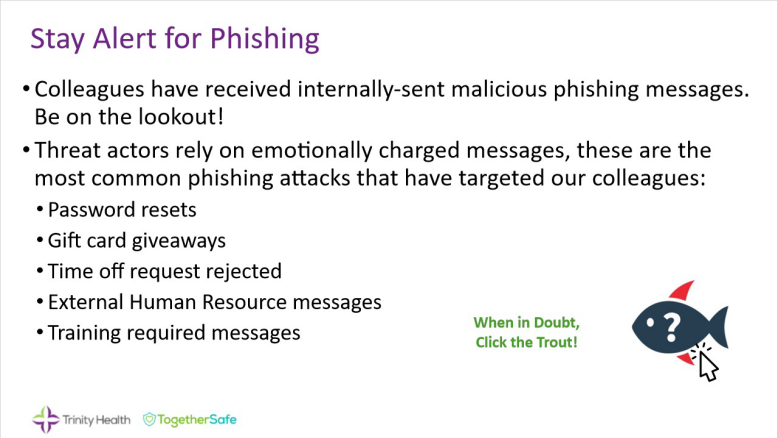
And there's no Trinity Health logo or any other information to confirm it's from HR.

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

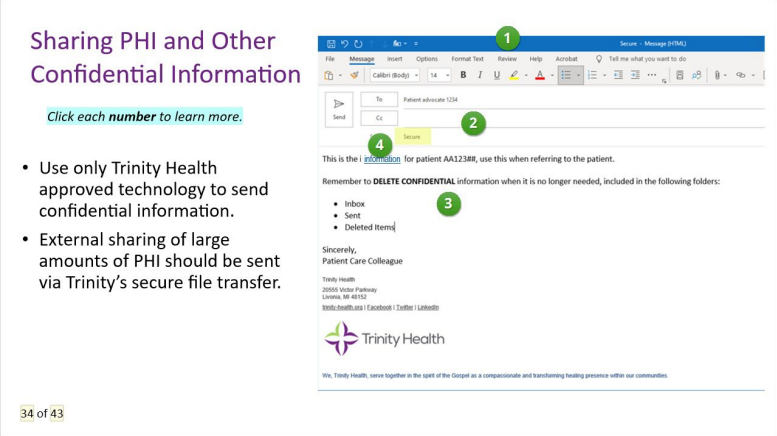
Speaker 1

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

Stay Alert for Phishing



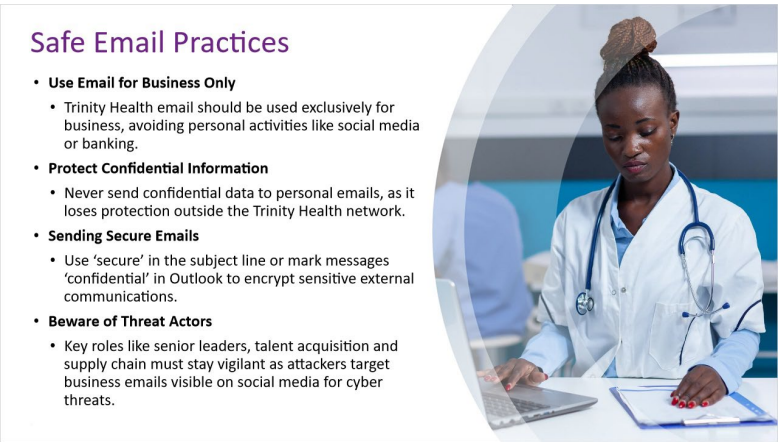
Sharing PHI and Other Confidential Information



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.

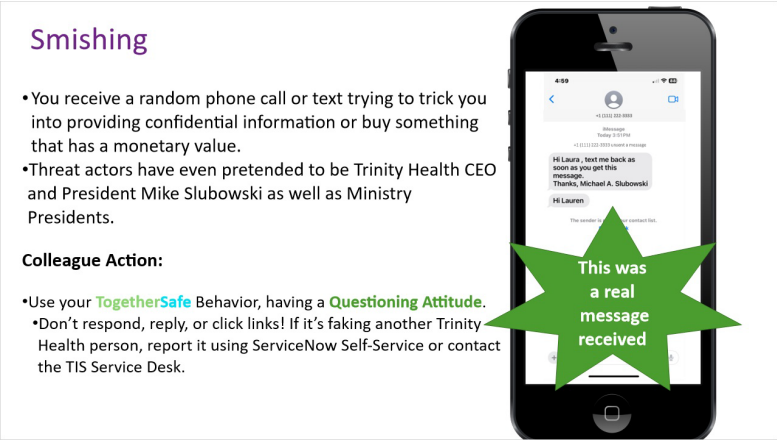
Safe Email Practices



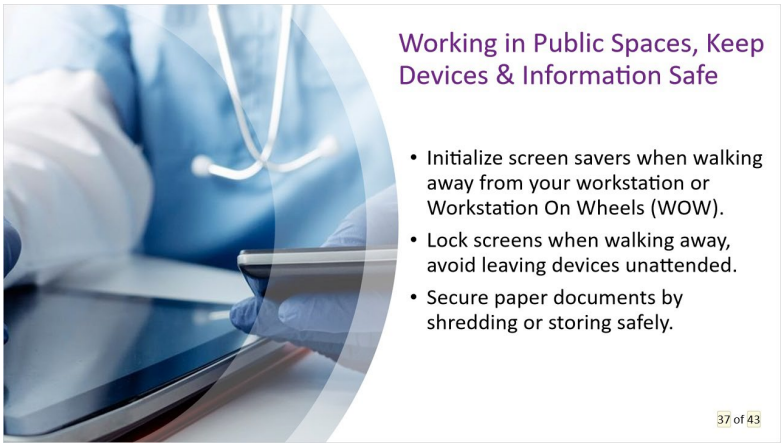
Notes:

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



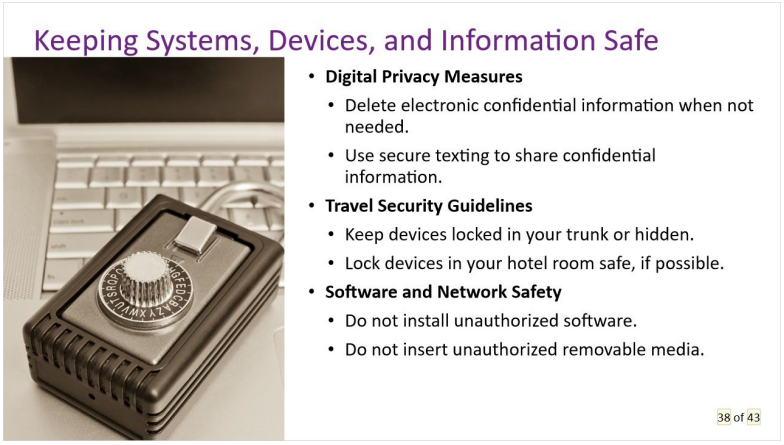
Working in Public Spaces, Keep Devices & Information Safe



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



Notes:

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

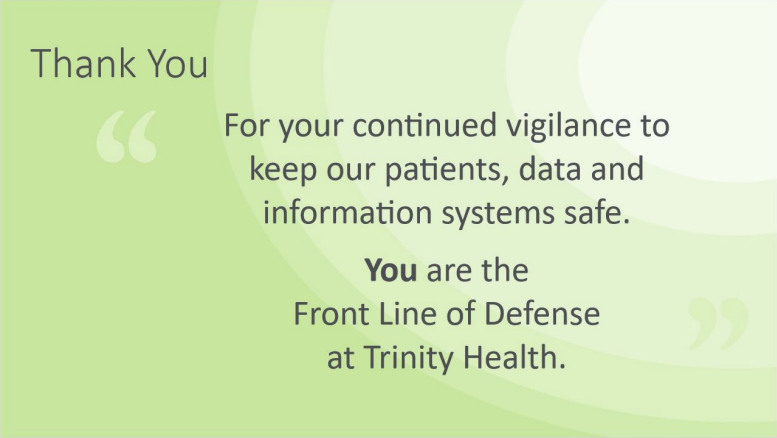
Reporting Security Incidents & Support

Notes:

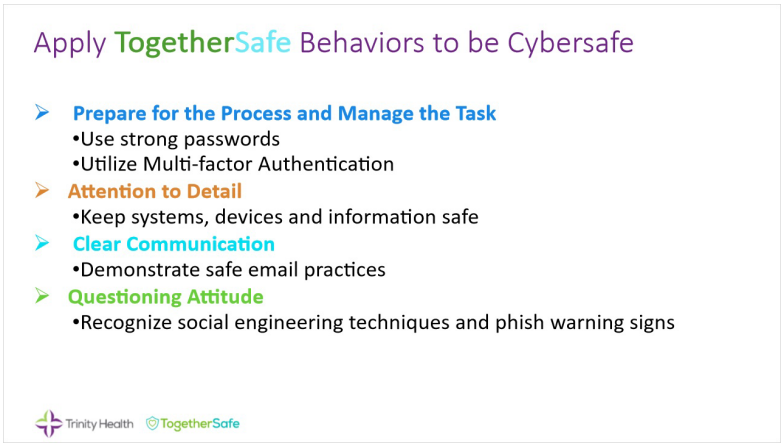
Part of your role is keeping information secure and reporting potential incidents to keep the team and organization safe.

5. Wrap Up

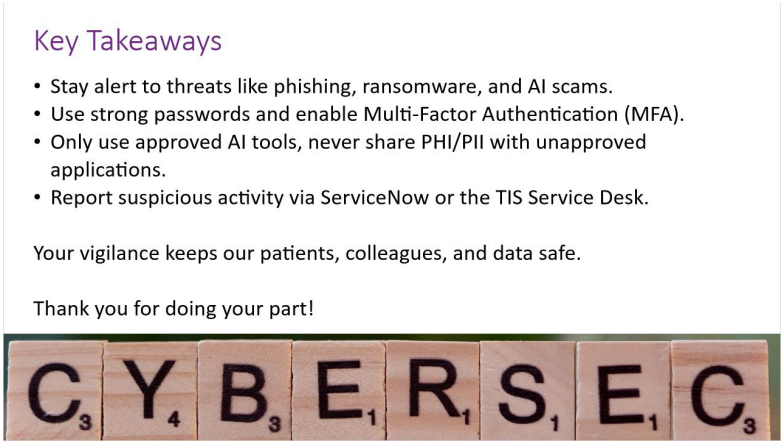
Thank You



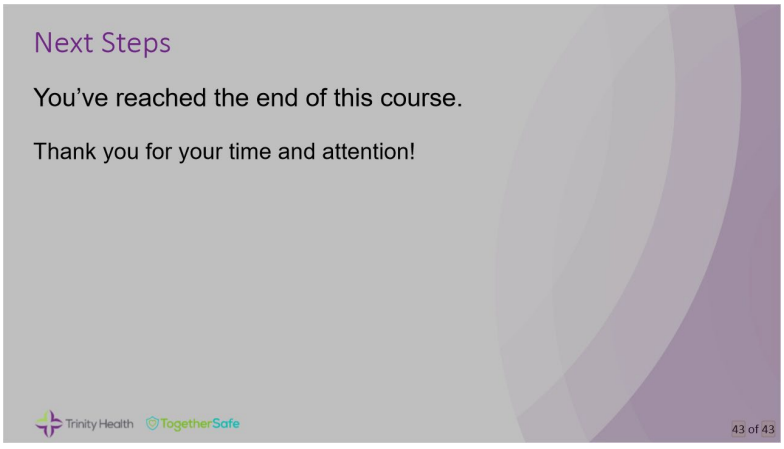
Apply TogetherSafe Behaviors to be Cybersafe



Key Takeaways



Next Steps



Notes:
