Overview

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.

Training Objective

You will learn the security basics needed to avoid and report the greatest cybersecurity threats we’re defending against 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. Many of these same safe cybersecurity habits taught here, also directly apply to your personal life outside of Trinity Health.

CTRL+Click HERE to play the Preston Jennings Introductory Video (3-minutes)
**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 Multifactor 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

---

**Password Guidelines - Do**

**DO**

✔ Get creative!
  - Passphrases or sentences are tougher to crack
  - The longer a password, the stronger the password

✔ Use:
  - 12-15 characters minimum
  - Combine uppercase letters (A-Z), lowercase letters (a-z), numeric digits (0-9) and special characters (@,%,#,?)
  - Example: MyD@gsTheSweetest1!
Password Guidelines – Do Not

**DO NOT**

- Reuse previous passwords
  - Use the same passwords at multiple sites, (e.g., personal email, work, LinkedIn, Spotify, bank, etc.)
- Use single words found in the dictionary.
- Use easy to guess passwords such as Trinity23!, Spring2023!, Winter2023?
- Write passwords down or save them on a piece of paper.

Multi-factor Authentication

Sometimes called 2-factor authentication, Multi-factor Authentication (MFA) provides a higher degree of security to identify the individual attempting to access a network because it requires a secondary source to validate the user’s 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.

Think before you “Approve” MFA

If you aren’t actively trying to log in yourself, don’t “Approve” an Authenticator prompt.
Safely Use Devices

Keep Devices safe
- Position the screens so no one passing by can see information.
- Initialize screen savers 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.
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.

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.

[Images of a doctor at a desk and email icons]
Malicious Phish Warning Signs

Follow These Practices To Keep Your Data Safe

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

Brilliant Tip of the Day: SLOW DOWN AND PAUSE

Phishing Warning Signs

This simulation duplicates a real, malicious phish that Trinity Health colleagues were susceptible to.

1. Always be careful when reviewing messages from external sources.
2. Do you recognize this sender? Do you know Jameson Matthews or edoctransfer?
3. Were you expecting this message?
4. Why is there no logo or contact information? Why is there no way to call the sender to verify its legitimacy?
5. Do not click on links unless you verify the email is legitimate.
Reporting Incidents

- Use the Outlook “Report Phishing” Button to report suspicious email messages.
- Use ServiceNow Self Service to report all other security incidents:
  - Select “Something is Broken” / “Report an Incident”

Help with Security Questions

- Email askcybersecurity@trinity-health.org for security questions or comments
- Ask your Supervisor

Be a Guardian! Together, we must all be security aware, have good security habits, and report incidents to keep our patients and information systems safe.