IT Security

IT Security

ITSecurity@utmck.edu

305-4357

THE UNIVERSITY OF TENNESSEE
MEDICAL CENTER

Wisdom for Your Life.

Objectives

- Understand Information Security and your role in protecting our data
- Understand Phishing and how it affects the organization
- Learn about Malware and the common methods of infection
- Learn the importance of password security
- Understand Social Engineering

Information Security

- **Information Security** is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.

- **The goal of the IT Security team** is to protect the confidentiality, integrity, and availability of all data in the organization.

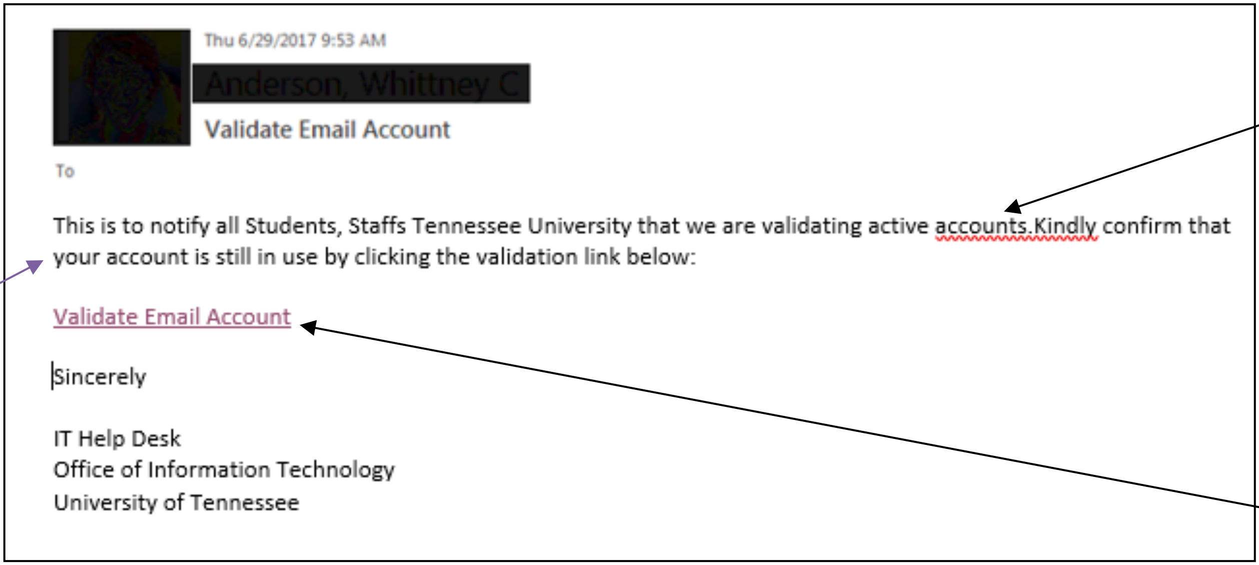
- **Information Security is everyone’s responsibility**. Our organization can have the latest and greatest technology, but it is up to everyone in the organization to protect UHS data and keep it out of the hands of attackers. **Everyone is a target**, regardless of role in the organization.

- If you notice any suspicious activities on organizational computers, networks, or emails, **please report these suspicious events to the Technical Support Center** (305-4357) **immediately**.

Phishing

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords, credit card numbers, or PHI.

The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or open an attachment.



Thu 6/29/2017 9:53 AM
[redacted]
Validate Email Account

To

This is to notify all Students, Staffs Tennessee University that we are validating active accounts.Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

IT Help Desk
Office of Information Technology
University of Tennessee

Strange language or "seems off"

Asking for information we should already have or know

Asking for Account Verification

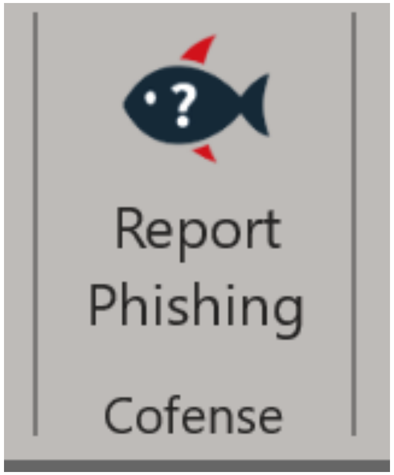
Example of a phishing email

Phishing [continued]

- **Two of the most common ways** to conduct a phishing attack is to attach an infected file to the email or place a link within the email in-which users mistakenly enter credentials (username/password) in the fraudulent website.

- **Attackers can design emails to appear as if they are sent by UTMCK accounts**. If you receive an email from a UTMCK account that appears suspicious, it is always better to contact the person sending the email directly and ask if it was legitimately sent or contact Technical Support immediately.

- **If you receive a suspicious email, whether from inside or outside the organization, please report the email to us using the Cofense Reporter in your Outlook client.**



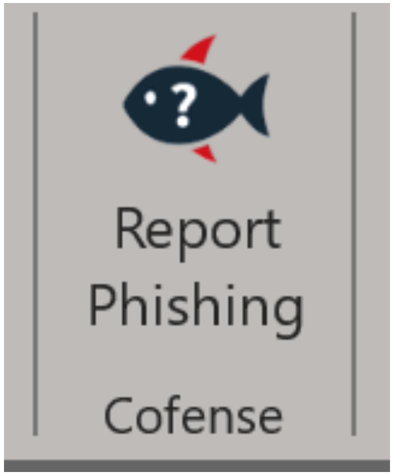
Phishing [continued]

- The Cofense Reporter is a button in your Microsoft Outlook application you can use to report suspicious emails to us automatically without needing to contact the Technical Support Center. This can help prevent you interacting with phishing emails and help keep the organization safe.

- After the email has been analyzed, a response will be sent back to you to let you know if the email is safe. Emails reported using the Cofense Reporter will be classified in one of the following categories:
  - SAFE
  - MALICIOUS
  - SPAM
  - SUSPICIOUS

- Only safe emails will be returned to your inbox.

  (Responses usually arrive in 15 minutes)



Passwords

Security measures – such as passwords – are critical when it comes to preventing the unauthorized access of computers and mobile devices. **You should never share your password with anyone, regardless of the situation or role in the organization.**

The longer and more complex your password is, the safer your account will be from attackers. Avoid short and easy to guess phrases or sequential numbers in your passwords.

-**A password like "Vols1234" is extremely easy for an attacker to guess.**

-**Try using longer phrases or mixing in different numbers, symbols, and uppercase letters and to make your password more secure.**

-**Use *iGtBaTv0825 or ItsGreatToBeATNv0L2198 rather than something simple like Vols1234)**

Passwords (continued)

There are key points of password security that users must know in order to reduce the likelihood of a hacker cracking their password and thus gaining access to their device:

- Most importantly, passwords must be long and complex.
- **Long and complex passwords require more effort and time for a hacker to guess.**
- Industry standards recommend at least fifteen characters and **a combination of characters** such as commas, percent signs, and parentheses, as well as upper-case and lower-case letters and numbers.
- Never write down passwords, as that makes it easier for the passwords to be stolen or used by someone else.
- Also, **never use the same password for two or more accounts**, as hackers who break into one account will try to use the same password to take control of others.
- If you're having trouble thinking of a strong password, pick a phrase and use the first letters from that phrase (or the phrase itself if long enough)
  - **It'sGreatToBeATennesseeVol1998 → #IgTbAtV1998!**

Malware

Malware is any software intentionally designed to cause damage to a computer, device, or network.

Malware is no longer created by just curious hobbyists or amateur hackers, but by sophisticated cyber criminals. Their goal is to make money from your infected computer, device, or network, perhaps by selling the data they’ve stolen from you.

Cyber criminals often trick people into installing malware for them. For instance, they might send you a phishing email or trick you into opening a malicious link on your computer.

If a message creates a strong sense of urgency, is confusing, or seems too good to be true, it could be an attack. Be suspicious, common sense is often your best defense.

Social Engineering

Social Engineering is a technique in-which attackers trick users into giving up sensitive information over the phone, in-person, or by email/text.

A common misconception most people have about cyber attackers is that they use only highly advanced tools and techniques to hack into people's computers or accounts. This is simply not true. **Cyber attackers have learned that often the easiest way to steal your information, hack your accounts, or infect your systems is by simply tricking you into making a mistake.**

Social Engineering (continued)

Fortunately, stopping such attacks is simpler than you may think—common sense is your best defense. If something seems suspicious or does not feel right, it may be an attack. The most common clues of a social engineering attack include:

- Someone creating a tremendous sense of urgency. **They are attempting to fool you into making a mistake.**
- Someone asking for information they should not have access to or should already know, such as your account numbers or login information.
- **Someone asking for your password**. **No legitimate organization will ever ask you for that. <u>Never believe an email when it asks for account validation/verification</u>.**

Social Engineering (continued)

- Someone pressuring you to bypass or ignore security processes or procedures you are expected to follow at work.
- **Something too good to be true**. For example, you are notified you won the lottery or an iPad, even though you never even entered the lottery.
- **Strange emails from coworkers may be an attacker using their compromised account to try and trick you** into giving up information.

IT Security Evaluation

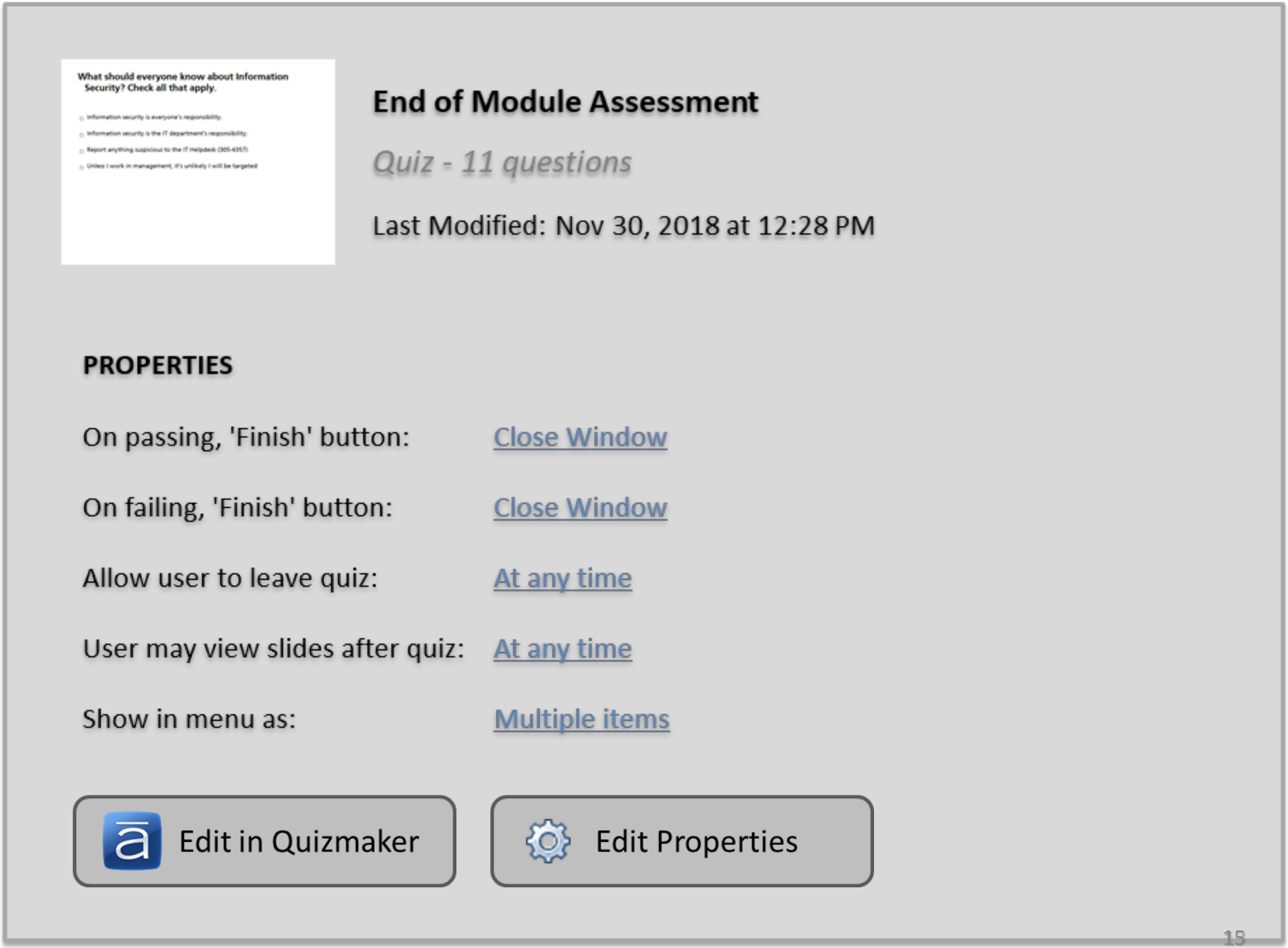
IT Security team is responsible for the protection of all UHS infrastructure and data. Accordingly, **the team requires a cybersecurity risk assessment on all new and existing vendor solutions for any application that may be used in the organization.** Doing so allows us to better identify and eliminate vulnerabilities that may pose a significant risk to patient and organizational data/systems.

Here is how to submit a request:
Please go to Service Requests – UTMC Insite (utmck.edu)

IT Project
If you need a project (multiple resources/40+ hours work effort) completed that involves Information Technology resources, click here to submit a New Project Review Request. An IT Project Manager will prepare your request for IT Leadership review.

IT Security Evaluation Only
IT Security evaluation, submit a vendor/solution evaluation request via the following link. Be sure to indicate “IT Security Signoff Only” in the form.
Click here to track your submitted request

You have now completed the module and are ready to take the assessment. Remember, you must complete and pass the assessment with an 80% in order to get credit for the module.



What should everyone know about Information Security? Check all that apply.

□ Information security is everyone's responsibility.

□ Information security is the IT department's responsibility.

□ Report anything suspicious to the IT Helpdesk (305-4357)

□ Unless I work in management, it's unlikely I will be targeted

End of Module Assessment

Quiz - 11 questions

Last Modified: Nov 30, 2018 at 12:28 PM

PROPERTIES

On passing, 'Finish' button:	Close Window
On failing, 'Finish' button:	Close Window
Allow user to leave quiz:	At any time
User may view slides after quiz:	At any time
Show in menu as:	Multiple items