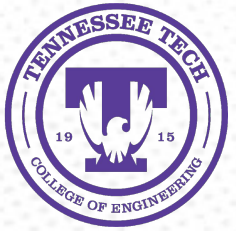
CyberSecurity: Shared Responsibility

Tennessee Tech CSAT Seminar

Presented by Students of IT Security 5570

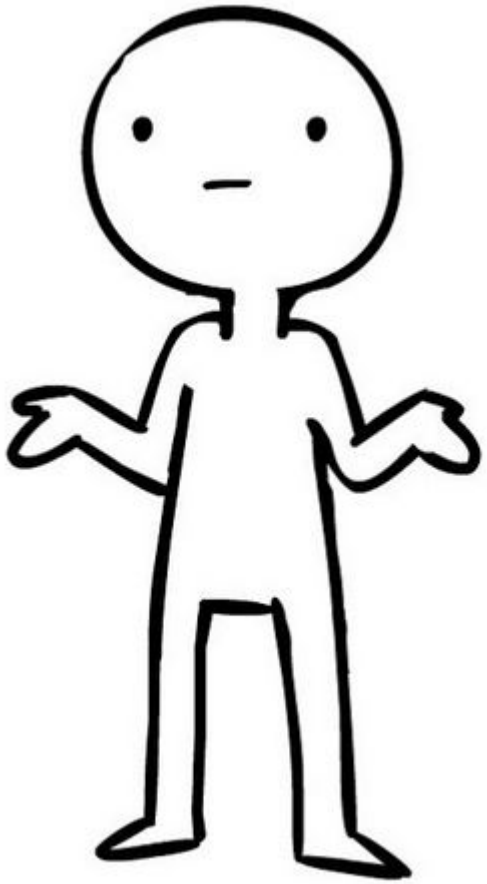


What is Cyber Security?

"Let's talk Cyber..."

Cyber Security Is...

- Practicing security on the internet
- Keeping your computer secure
- Preventing Hackers/Threats/Bad Actors
- Techniques to protect organization
- Keeping your information private



Here at Home…

It's a shared responsibility to ensure the security of our community here at Tennessee Tech!

Importance

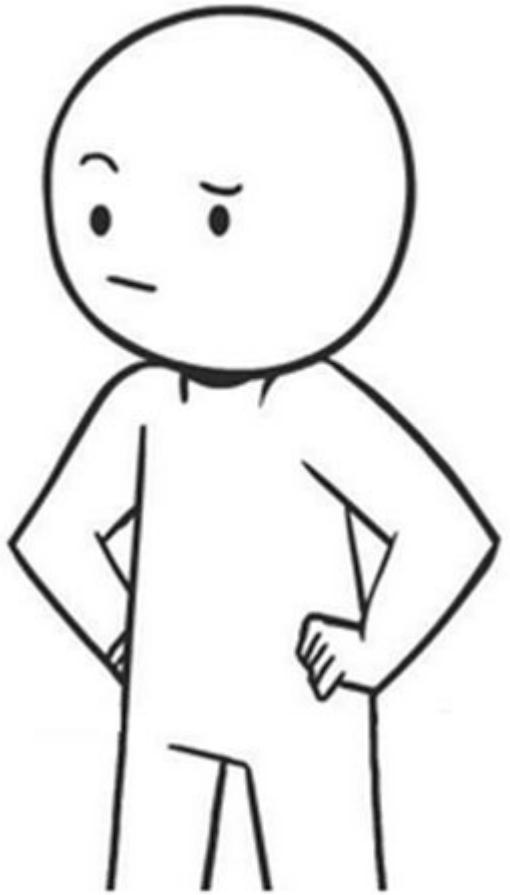
"What matters"

- According to Verizon 2019 Data Breach Investigation Report, human error accounted for 35% of data breaches in the education sector
- Emails leaks are a common attack vector
- 1/4 of breaches in the education sector were the result of web application attacks, often via phishing links to phony login pages
- 53% of data compromised is stolen credentials
- Of those stolen credentials, more than 80% of which were used in other hacking breaches (using the same password in multiple places!)

What You'll Hear About From Us

"Coming up..."

- Phishing
- SMiShing
- Vishing
- Social Engineering
- Malware
- Ransomware
- Cyber Physical Attacks
- Passwords
- Policies



Phishing

"Got a hook!"

So you took the bait and you're here.

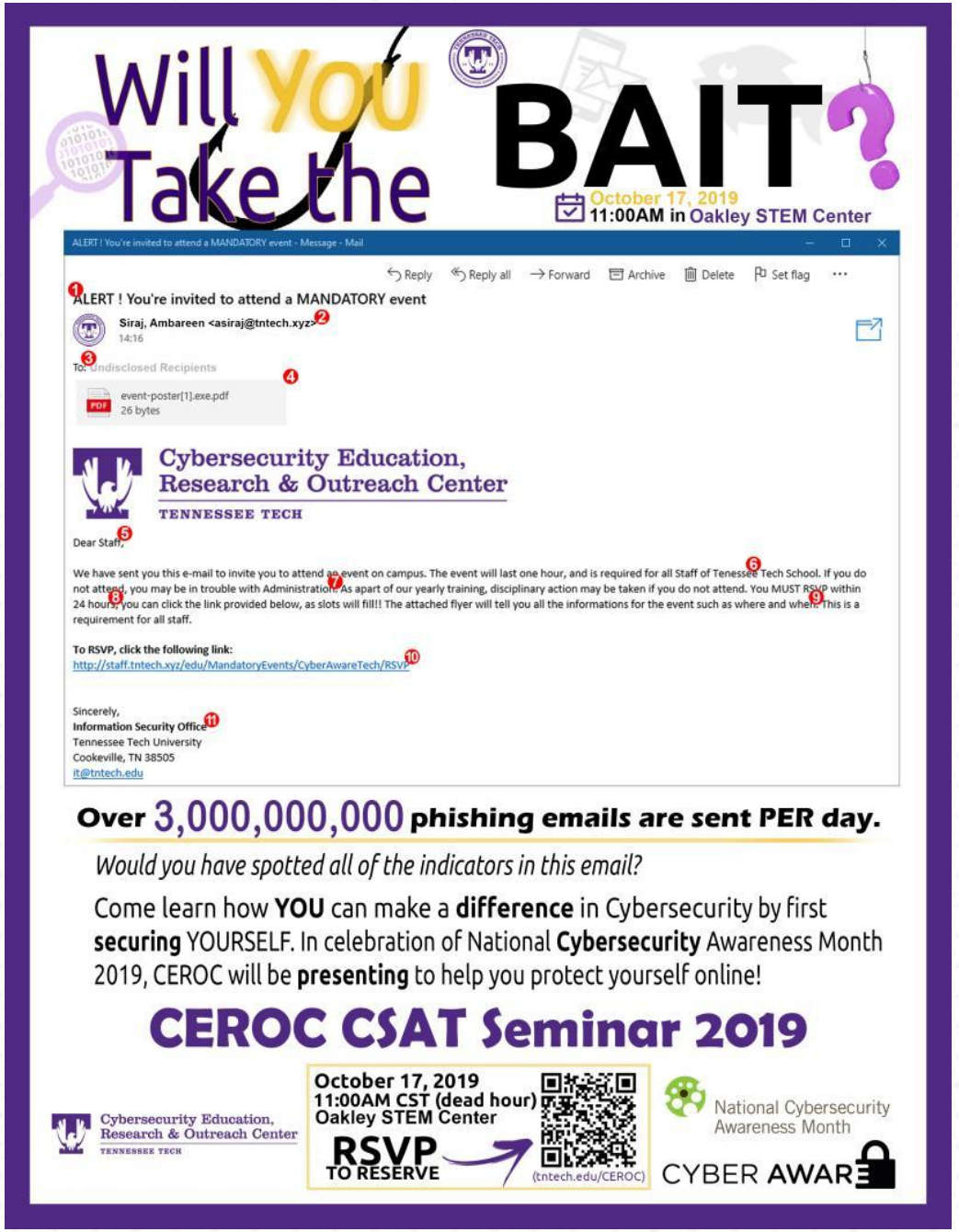
The main theme of the flyer was **Phishing**…

But what is Phishing?

Phishing is a scam. Usually in the form of fraudulent emails or web-pages, that seem to be legitimate and are designed to fool the user, but really cause harm.

How big of an impact does it have?

- ➔ Phishing accounts for 90% of data breaches
- ➔ 66% of malware is installed via email
- ➔ Average data breaches cost $3.86m (big bucks)
- ➔ Phishing has grown 65% from 2018 to 2019
- ➔ About 1.5m phishing websites made monthly
- ➔ 76% of businesses report being victims
- ➔ 30% of phishing messages are opened
- ➔ Security breaches increased 11% since 2018
- ➔ Americans report about 60% were phished

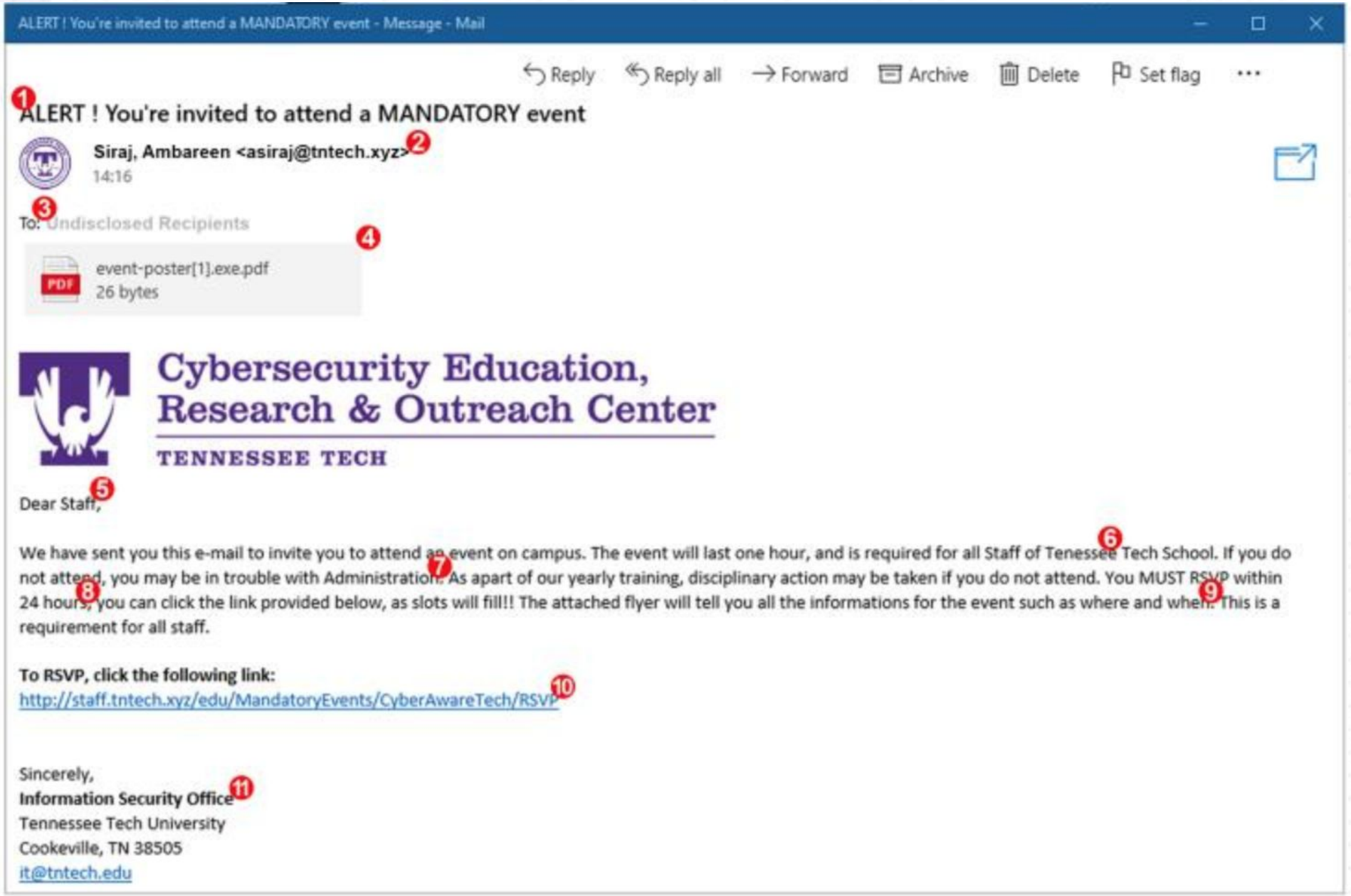


Phishing

"A closer look.."

You may have noticed the email in the flyer

… but could you find all 11 issues by yourself?



Phishing

"Diving Deep"

Spot the Red Flags!

So.. what are the 11 issues and indicators in the email?

1. Subject name defines unnecessary urgency (URGENT, ALERT, etc)
2. The sender is using a fake domain (tntech.xyz instead of tntech.edu)
3. The sender does not explicitly define your email or a group of emails (such as STUDENTS-ALL or YourUsername)
4. There is a suspicious looking attachment with an executable extensions (extensions such as .exe, .bat, .vbs, etc)
5. The email addresses a broad audience, instead of providing detail (such as Dear User, Dear Staff, or To All)
6. There is a Spelling error of the word Tennessee (many phishing attacks come from foreign countries that make spelling and grammatical errors)
7. The sender makes needless threats or suggests repercussions for not complying (such as "Administrative Action" or "Your account will be deleted!"
8. The sender makes a response time-critical (provides strict time limits to rush a user from reading the entire email)
9. The email is vague of a time and place and suggests clicking the attachment (this can be real, but often is a trap to click a malicious attachment)
10. There is a malicious or deceiving URL (points to a fake tntech.edu website)
11. The email is signed off essentially anonymously (no indicator who actually sent the email, just a general signature)

Up Next.... SMiShing

SMiShing

"An attack on your phone"

What is it?

- SMiShing a form of phishing
- When someone tries to fool you to gain information via text or SMS

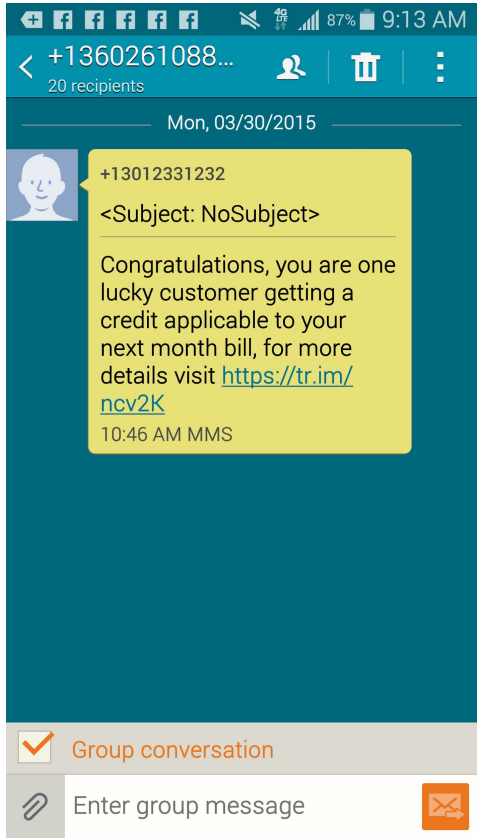
Why is it a concern?

- Texting is the most common use of a smartphone
- Smartphones have security limitations
- Android devices are targeted due to the flexible software it provides customers (and criminals!)
- Apple's iOS has a good rep for security, but no mobile device is immune from a phishing attack… it's up to the user to identify and prevent it!

SMiShing

"How to protect yourself"

- Refuse to take the bait—don't respond.
- Do not store your credit card or banking information on your smartphone.
- Look for suspicious numbers that don't look like real mobile phone numbers.
- Regard "urgent" security alerts and you-must-act-now offers or deals as warning signs of a hacking attempt.
- A financial institution will not send you a text message asking you to update your account information or confirm your ATM code.
- Report all SMiShing attacks to the Federal Communication Commission (FCC) to help protect others.



SMiShing

“Don’t take the bait!”

- The attack can only do damage if you take the bait.
- SMiShing is a social engineering technique and requires action on the victims part.
- It depends on fooling the victim into cooperating by clicking a link or providing information.
- The best protection against these attacks is to do nothing at all.
- As long as you don't respond, a malicious text cannot do anything.
- Ignore it and it will go away.

Up Next....
Vishing

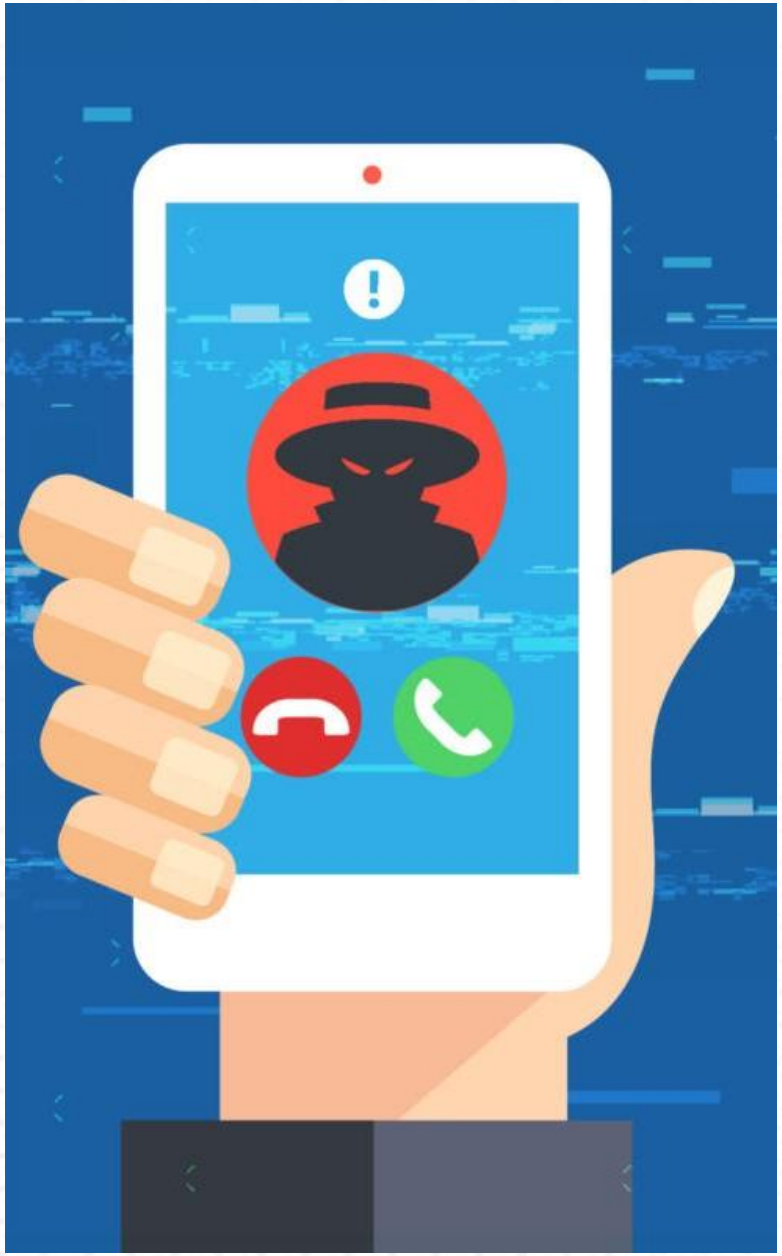
Vishing

"What is it?"

Similar to phishing, **Vishing**, is a form of deception and fraud where an attack will try to obtain information.

Unlike phishing that is done over web and email, vishing is performed via phone call.

Voice + Phishing = Vishing



Vishing

"How is it done?"

So how do they pull it off?

- Callers will spoof legitimate phone numbers to try and trick you into thinking it is a real call
  - The location the call is coming from can even be spoofed and changed!
- A caller will pretend to be a legitimate business or service calling to get you intrigued

They'll tell you...

  - Something of yours expired
  - Something of yours is compromised
  - You're eligible for free offers
  - You have won a prize

- They will tell you anything you want to hear in an attempt for to get you to visit a website or give out personal information to them!

Vishing

"Stopping it..."

There are ways to help defend yourself!

- You can add your phone number to the national "Do Not Call" registry.
  You can do this by...
  - Visiting FTC website @ https://donotcall.gov/register/reg.aspx
  - Calling the FTC @ 1-888-382-1222
- Don't give out information immediately when asked
  - Wait to hear if the call is legitimate
  - Ask information to verify it is an actual company making a legitimate call
- Be weary of unknown numbers
  - Don't pick up suspicious numbers or to calls you aren't expecting
- In general, be aware of what vishing is and be educated to recognize it!

Social Engineering

"Playing with words"

- **Social Engineering** is tricking a person into revealing sensitive information or performing an action, instead of using technical hacking/cracking techniques

- Social Engineering exploits human nature
  - Carelessness
  - Helpfulness
  - Helplessness
  - Comfort zone
  - Fear
  - Curiosity
  - Greed

Malware

“What is it?”

Malware is something that everyone on the internet has to deal with at one point or another when using their computer

- Malware comes in many different types, with many different objectives
- Not all malware is created equally
- Malware can be annoying and post risk, but there are ways to protect yourself

Malware

"Types of Malware"

There are many types of malware…

- Virus: The most common type
- Trojan Horse: Designed to look like legitimate software
- Spyware: Made to collect data on a device
- Ransomware: Encrypts all the user's data (more to come on this type)
- Worms: Designed to spread to other devices by themselves
- Adware: Spams the user with advertisements
- & other types... but these are the big names

Malware

"Preventing It"

So.. how do we stop malware? You're in luck, there's solutions!

- Install a antivirus software and routinely run a scan with the most up to date version
  - Good tools include.. Malwarebytes, Windows Defender, Avast, & others
- Keep your Operating System up to date
- Think before you click a suspicious link or web page
- Create regular backups
  - 3-2-1 backups ensure you keep multiple copies of important data
- Use strong passwords that are unique for every account

Up Next....
Ransomware

Ransomware

“Held at ransom?”

Ransomware is a special type of malware that is designed to hold your computer at ransom behind a paywall to get your important stuff back!

- Ransomware will lock-up your system by blocking usage or by locking your files
- Modern types of ransomware use military-grade encryption to prevent decryption
  - This means normal anti-virus software cannot remove ransomware
  - An infected person would be forced to pay to get the decryption keys and get their files back!

Ransomware

“Don’t get caught up!”

How do you prevent it? The simple answer…

Don’t download it!

Don’t:

- Click suspicious links
- Fall for phishing attacks, and download malicious email attachments
- Don’t install things that you don’t know where they came from, or if they are legitimate

Ransomware

"How to break free"

Sadly… there isn't a lot to do once infected.

There are preventive and responsive ways to deal with ransomware…

Preventive (incase you get infected)**:**

- Create regular backups of your data
  - Create backups to external hard-drives or cloud devices
  - Use backup services like BackBlaze for automated backups
- Prepare your system to be able to be re-installed as needed

Responsive (if you get infected)**:**

- Consult IT staff or the helpdesk to see if your data is recoverable
- Reinstall your device as needed
- Learn from your mistake, and prevent it from happening again

Cyber Physical Attacks

"Physical threats"

Cyber Physical consists of the physical devices and systems that you encounter

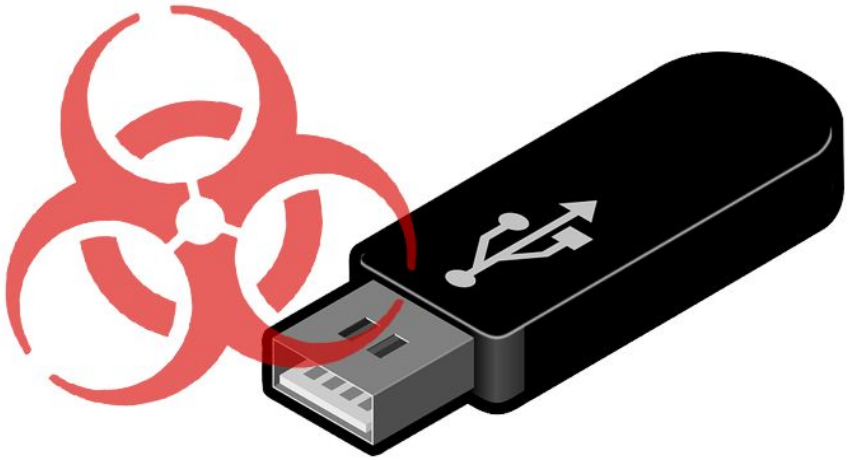
- Cyber Physical Attacks include attacks on:
  - Hardware
  - External storage devices
  - Internet of Things
  - Digital systems

Cyber Physical Attacks

"The importance of"

Why being aware is important…

- Attacks can hitch a ride on USB storage devices or flash drives and smartphones, smart watches, and even signal devices such as key fobs.
- Frighteningly versatile
- Very difficult to identify and detect
- Difficult to remove



Preventive methods….

- Don't plug in random devices

Cyber Physical Attacks

"Examples"

- "2008 cyber attack on the US"
- Alexas
- Rubber Ducky
- Network enabled printers

Up Next....
Passwords

Passwords

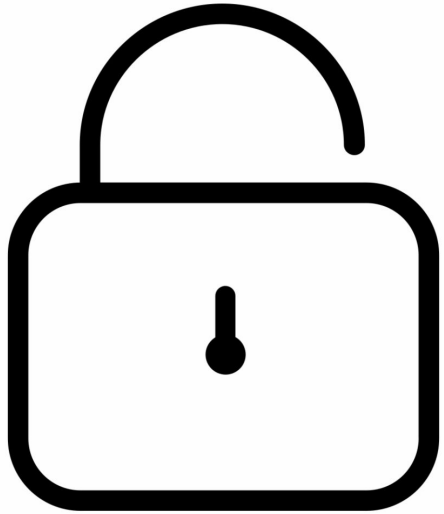
"Everyone has them"

Passwords are simply strings of characters.

They grant you access to to things, everyone has at least one but likely many.

Passwords can be categorized on how critical they are to a user…

- **High Security:** For anything where your personal life can be affected by compromise.
  - Includes things like your financial information, computer login, etc.
- **Medium Security**: For communication platforms and messaging apps
  - Includes websites like facebook, whatsapp, etc
- **Low Security**: For non critical websites
  - Includes things like forums, newsletters, trials, etc



Passwords

“Making them safe”

How do we make them safe? Passwords should...

- … be at least 8 characters of length
- … contain special characters like @#$%^&* and/or numbers
- … use a variation of UPPER and lower case
- … be unique from previous passwords you’ve used
- … not use personal information
- … be changed regularly

ITS Password Policy

Policy 852 Password Management

- Minimum 8 character in length, at least five of them unique
- At least one uppercase (A-Z)
- At least one lowercase (a-z)
- At least one numeric (0-9)
- At least one non-alphanumeric a.k.a. “special” character (~!@#$&)
- Must be changed every 90 days

DO NOT INCLUDE:

- Dictionary words in any language or common letter/number patterns
- Personal information (birthday, phone number, pet names, child’s name)
- Variations of old or related password
- Password which are the same as user ID
- Tennessee Technological University, Tennessee Tech, TTU or any derivation

Tennessee Tech Security Policies

Policy 801 Information Technology Acceptable Use

- No right to privacy
- Intellectual property
- Downloads
- Circumventing security measures
- Report incidents to ITS

Policy 850 Enterprise Information Security

- CISO creates policy; management enforces
- Balance degree/cost of protection with value and sensitivity of information
- Provide awareness and training in security responsibilities

Policy 851 Information Security Roles and Responsibilities

- Only use IT resources for your job
- Know and obey the security policy
- Disciplinary Action

Tennessee Tech Security Policies

Policy 802 Access Control

- Primarily role-based
- Default deny
- Account locks for 5 min. after 5 incorrect login attempts
- UI locks after 20 min. of inactivity
- Accounts disabled after 90 days of inactivity
- Sensitive data

Policy 854 Data Breach Notification

- Affected parties must be informed
- Responsible parties can incur fees

Policy 503 Identity Theft Prevention

Policy 131 Preventing and Reporting Fraud, Waste, or Abuse

Tennessee Tech Security Policies

Policy 855 Data Classification

Level I: Public

Level II: Internal

- For official business only
- Encryption not required

Level III: Confidential

- TTU accounts only
- Encrypt (AES-128) or lock

Level IV: Sensitive

- TTU accounts only
- Encrypt (AES-256) or lock

NIST encryption standards or written permission from CISO

Tennessee Tech Security Policies

Policy 856 Data Security and Handling

Level I: Public

- Single-pass to erase
- Reuse or recycle

Level II: Internal

- Three-pass or DoE procedure to erase
- Reuse or secure document disposal

Level III: Confidential

- Seven-pass or DoD procedure to erase
- Reuse unless assigned to TTU personnel or secure document disposal

Level IV: Sensitive

- Seven-pass or DoD procedure to erase
- Destroy or cross-cut shred

NIST best practices for Levels II– IV

Incident Reporting

Information Technology Services (ITS)

- Hours during the regular semester are Monday-Friday, 8:00am-4:30pm
- The myTECH Helpdesk is located on the main floor of the Volpe Library in suite 256.
- (931) 372-3975
- helpdesk@tntech.edu

Information Security Office

- (931) 372-3913
- ociso@tntech.edu

Resources

National Cybersecurity Awareness Month 2019

https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

STOP. THINK. CONNECT.

https://www.dhs.gov/stopthinkconnect

BeCyberSmart

https://www.dhs.gov/be-cyber-smart

NICCS Portal

https://niccs.us-cert.gov

FedVTE

https://fedvte.usalearning.gov/

Tennessee Tech Resources

Tennessee Tech Cyber Threat Bulletin

https://its.tntech.edu/display/MON/Cyber+Threat+Bulletin

Information Security Knowledge

https://its.tntech.edu/display/MON/Information+Security+Knowledge

CISO Office Training Information and Syllabus

https://its.tntech.edu/pages/viewpage.action?pageId=20676712

CISO Office Training Content

https://beaware.tntech.edu/

CEROC
110100101
001 001
1010 1101
100001010
CYBERSECURITY EDUCATION, RESEARCH AND OUTREACH CENTER

TENNESSEE TECH
19 15
COLLEGE OF ENGINEERING

Contact Us

"We are here to help"

Prescott Hall, Room 414

Office Hours: Monday - Friday 8am to 4:30pm CST

Email: ceroc@tntech.edu

Phone: (931) 372-3519

Website: https://www.tntech.edu/ceroc

Links for all resources mentioned today:

https://www.tntech.edu/ceroc/cyber_awareness_training/2019_resources