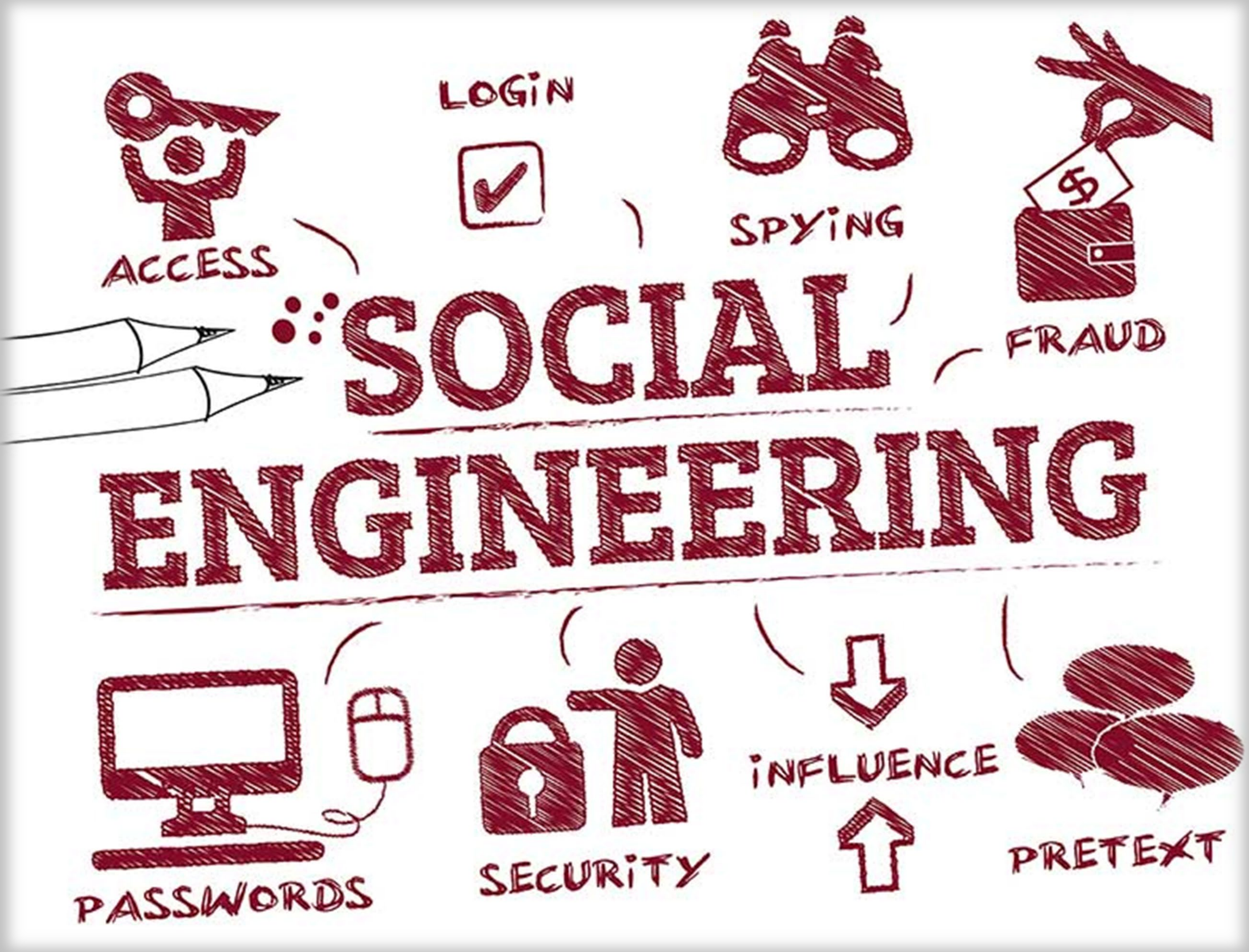
Cybersecurity Capstone

Bill Rohrman Jr.

CITE Training Coordinator

TechTraining@pvamu.edu

PVAM


ACCESS
LOGIN
SPYING
FRAUD
SOCIAL ENGINEERING
PASSWORDS
SECURITY
INFLUENCE
PRETEXT

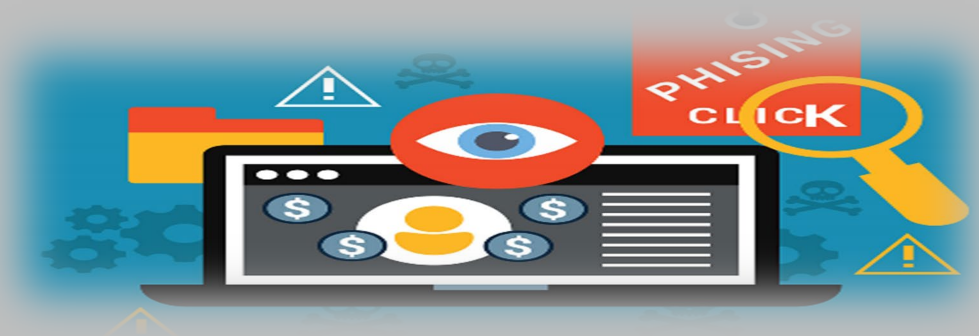
Trojans and Worms

Key Loggers

Remote Access Software

Credential Harvesting

Ransomware



Types

- Email

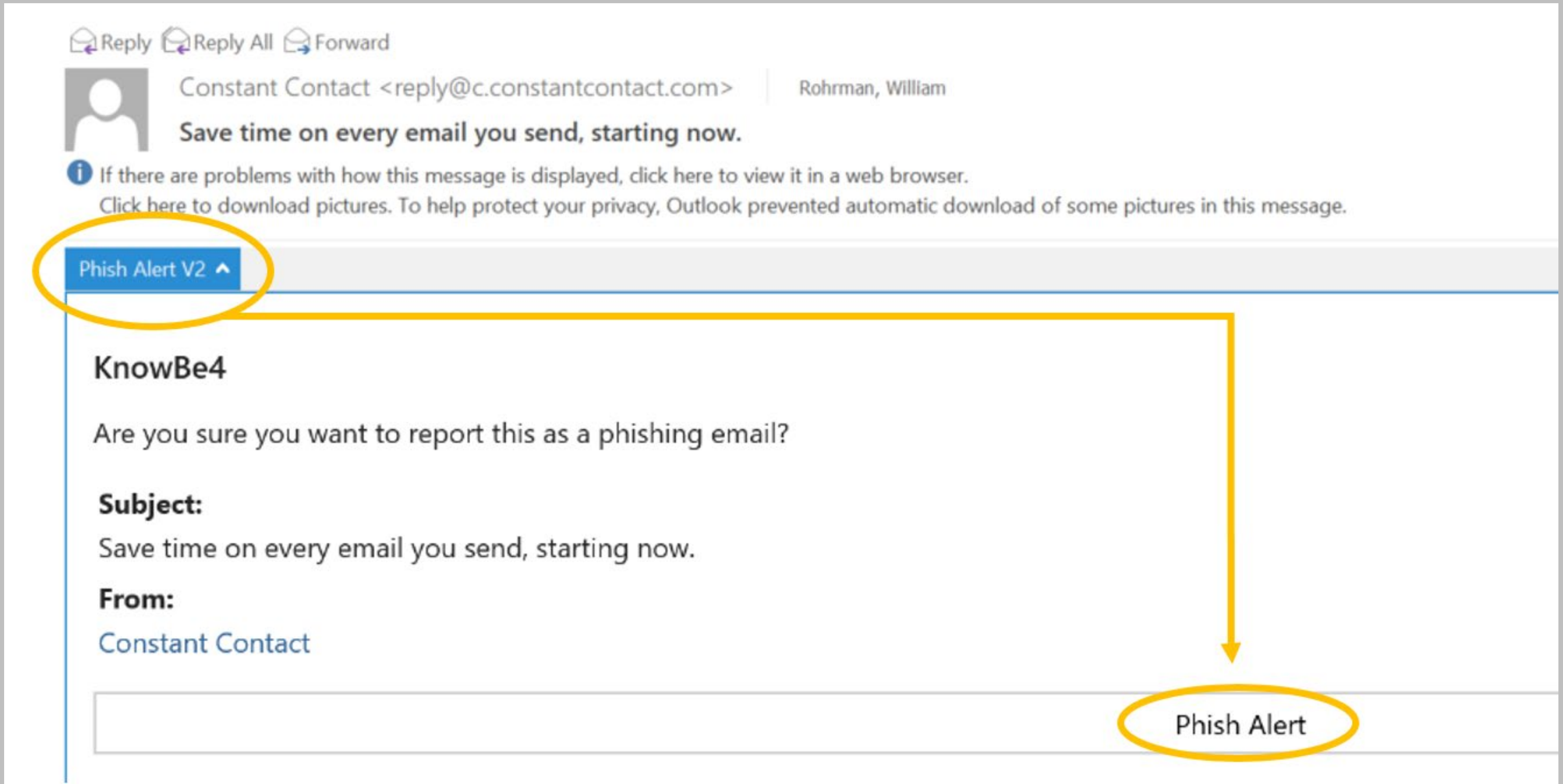
- Text

- Websites

Indicators

- Misspellings and grammatical errors
- Emails from unknown sources.
- Email address discrepancy.
- Unexpected links or attachments.
- Urgent sounding tone/requests.
- URL domains

Phish Alert V2 Button



Constant Contact <reply@c.constantcontact.com> Rohrman, William

Save time on every email you send, starting now.

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

KnowBe4

Are you sure you want to report this as a phishing email?

Subject:
Save time on every email you send, starting now.

From:
Constant Contact

Once email is validated and proved to be safe, it will be returned to your inbox.

If a security event occurs, disconnect from the Wi-Fi immediately
and contact the Help Desk at 936-261-2525

Safe Working Environment

Secure your Work Environment

Observant

- Working location/files
- Audience

Careful

- Viewable Information
- Desk, Tables, etc.

Cautious

- Personal Email
- Phishing Attempts

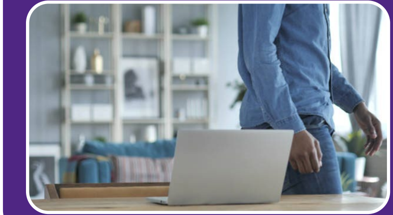
Secure Your Work Environment

WiFi Connections

- Turn off Wi-Fi connections until you're ready to connect to a secure connection.
- Work devices – connect to "**pvmobilnet**"
- Make sure to download the new Safe Connect software using the key: **pvamuwifi**.
- Personal devices – connect to "**PVAMU Guest**"
  - You will need to login in to Safe Connect here as well, but this should be your personal email.
- Be cautious with the Wi-Fi connections you use.
- Do not log into your personal accounts or shop online using public networks – never assume you are safe.
- Do not let your guard down while away from the office.

Password Usage

- Strong Passwords Protect You!
- Do not use PV passwords for personal business or vice versa.
- Password reuse is a major source of information breaches.
- Do not recycle passwords or use password enumeration, i.e. Winter 2020, Winter 2021.



Desktop/Laptop Discipline

- Always lock your device when walking away.
- Keep your device updated.
- Do not turn off your antivirus.

Secure Your Equipment

* Use privacy setting on your browser if entering sensitive information.

* Create different account credentials for login and installs.

Always use two factor authentication.

Consider using a DNS protection service like Open Doors or Quad 9. They are free and can help block malicious files from being downloaded onto your system.

Restart your Wi-Fi router every two days. A simple restart will clear attack attempts and improve your internet speed.

Update all your smart devices such as TV, Speakers, Phones, Fish Tanks, router(s).

Participants (3)
Panelists (3)
Viewers (0)
Joanna Jiang (Host, me, participant ID:18)
Jill Sanders
Leo Wang
Mute All
Unmute All
More
Chat
From Me to Everyone:
How is everyone?
Let me know if you have any questions, I would love to answer.
From Me to Leo Wang (Privately)
Can you hear me?
Let's keep the conversation going?
From Me to All Panelists:
Great job, guys
To: All Panelists
Type message here...
End Meeting

Zoom Security – Pre Meeting

Do not use Personal Meeting ID for Public Meetings.

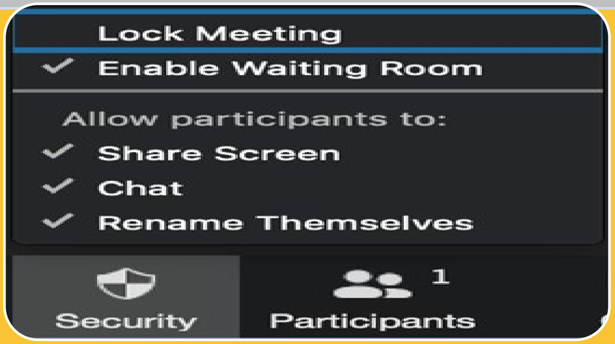
Mute Participants Upon Entry

Required A Password

Enable Waiting Rooms

Do not post links and passwords on a public forum.

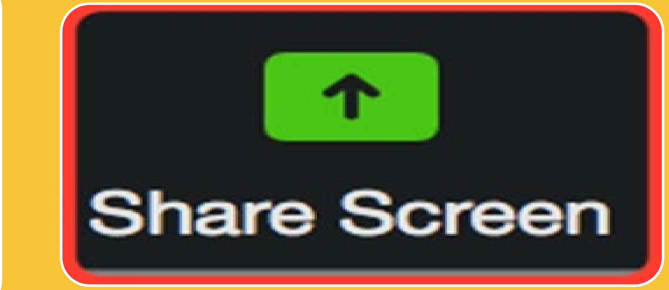
In-Meeting Settings



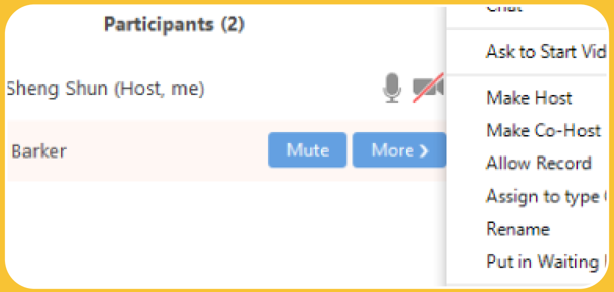
Lock Meeting
✓ Enable Waiting Room

Allow participants to:
✓ Share Screen
✓ Chat
✓ Rename Themselves

Lock The Meeting



Control Screen Share



Participants (2)

Sheng Shun (Host, me)

Barker Mute More ›

Assign a Co-Host

Kids and Technology

Online Behavior

Social Media / Internet

□ Know how they connect!

□ Select appropriate privacy settings.

□ Do not allow kids to have administrator accounts on computers to disable any protective software.

□ Many applications will not allow you to use them unless they can collect personal data. Do they really need to use that app?

□ Should never share their name, school's name, age, phone number, birth date, email or home address!

□ Think about what they post – harmful, ugly, inappropriate, etc.

Consequences

□ Predators

□ Reputation harmed

□ Post can come back to haunt you years later!

□ Be cautious of posted activity, i.e. illegal activity, etc.

□ Cyber Bullying

□ Sexting

Educate & Communicate

- ✓ Protecting your child's privacy is number 1!
- ✓ Foster good open communication with your children.
- ✓ Let your child know you are monitoring their activity.
- ✓ Teach them to never share passwords with anyone except parents. Friends can post unwanted information!
- ✓ Teach them not to "Check In" on apps.
- ✓ DO NOT friend anyone they have not met before no matter how popular they may be.
- ✓ Teach them how to spot unusual behavior and requests.

  * Tempted and dared to do unusual things through challenges, dares or pressure to fit in.
- ✓ Explain to them that everything posted online or in social media is not true.
- ✓ Predators and others love to convince your child that you are not always right!
- ✓ Almost nothing posted on the internet goes away. It is almost impossible to remove data once it is posted.

TechTraining@pvamu.edu