WiCyS Futures Resources

POWERPOINT PRESENTATION

- https://www.cisa.gov/sites/default/files/2024-05/9-12%20Cybersecurity%20Education%20Resources_Final_05022024.pptx

ONLINE RESOURCES

- Phishing Stats
  - https://upgradedpoints.com/credit-cards/phishing-facts-statistics-2024/
- MFA (Multi Factor Authentication)
  - https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661
  - https://www.onelogin.com/learn/what-is-mfa
  - https://www.lockheedmartin.com/en-us/suppliers/news/features/2023/cybersecurity-mfa.html
  - https://www.sentinelone.com/cybersecurity-101/identity-security/what-is-multi-factor-authentication-mfa/
- Password Game:
  - https://neal.fun/password-game/
- Credit Card Statistics and Awareness
  - https://upgradedpoints.com/credit-cards/credit-card-fraud-and-id-theft-statistics/
  - https://upgradedpoints.com/credit-cards/30-credit-card-scams-to-avoid/

Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation grant awarded to Tennessee Tech University, WiCyS has become a nonprofit organization offering many benefits for its members.

The WiCyS Conference is an excellent opportunity for companies to connect with female students and professional candidates to recruit them into cybersecurity jobs! More than half the attendees are students seeking opportunities, who have been accepted through the WiCyS scholarship program that sponsorships help to support.

Contact **info@wicys.org** for details.

Phishing Simulation Challenge [1]

OBJECTIVE:

Teach students how to recognize phishing attempts and understand the importance of cybersecurity awareness.

MATERIALS NEEDED:

- A selection of real-looking phishing emails (you can create mock emails based on common phishing tactics).
- A set of legitimate emails for comparison.
- Scoring sheets for each group.
- Whiteboard or poster board for tallying scores.

INSTRUCTIONS:

1. **Introduction (10 minutes):**
   - Briefly explain what phishing is and why it's a significant cybersecurity threat.
   - Discuss common signs of phishing emails (e.g., poor grammar, suspicious links, urgency).
2. **Group Formation (5 minutes):**
   - Divide students into small groups of 4-5.
3. **Email Review (20 minutes):**
   - Distribute a mix of phishing and legitimate emails to each group.
   - Instruct them to review the emails and classify each one as either "phishing" or "legitimate" on their scoring sheets.
   - Encourage discussion within the groups about their reasoning.
4. **Presentation (15 minutes):**
   - Have each group present their classifications and reasoning to the class.
   - Discuss any differences in opinions and clarify any misconceptions.
5. **Scoring (10 minutes):**
   - Award points for each correct identification. You could also give bonus points for explaining why certain emails were classified as phishing.
6. **Reflection/Conclusion (10 minutes):**
   - Conclude with a discussion on the importance of being cautious with emails and sharing tips for avoiding phishing scams in real life.
   - Follow-Up:
     - Consider creating a visual poster of key takeaways from the activity, such as "Top 5 Signs of Phishing," that can be displayed in the classroom.
     - This activity is engaging, promotes teamwork, and effectively teaches students to recognize phishing attempts, which is a crucial aspect of cybersecurity awareness!

[1] Generated using Chat GPT

women in CYBERSECURITY
WiCyS
wicys.org

Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation grant awarded to Tennessee Tech University, WiCyS has become a nonprofit organization offering many benefits for its members.

The WiCyS Conference is an excellent opportunity for companies to connect with female students and professional candidates to recruit them into cybersecurity jobs! More than half the attendees are students seeking opportunities, who have been accepted through the WiCyS scholarship program that sponsorships help to support.

Contact **info@wicys.org** for details.

Phishing Scavenger Hunt [1]

OBJECTIVE:

Students will learn to identify phishing attempts and understand safe online practices.

MATERIALS NEEDED:

- Printed examples of phishing emails and legitimate emails (mix them up)
- Markers or stickers for correct answers
- A timer

SETUP:

1. **Prepare Email Examples:** Create 6-8 examples of emails, with half being phishing attempts and half being legitimate. Ensure they include common signs of phishing, like suspicious links or poor grammar.
2. **Print and Cut:** Print each email on separate sheets, cutting them out so they can be spread out on a table or board.

INSTRUCTIONS:

1. **Introduction (2 minutes):** Briefly explain what phishing is and why it's important to recognize it. Share a couple of common signs to look for.
2. **Scavenger Hunt (8 minutes):**
   - Place the email examples on a table.
   - Divide students into small groups of 3-4.
   - Each group has 5 minutes to discuss and identify which emails they believe are phishing attempts.
   - Ask them to mark their choices with a sticker or write them down.
3. **Review and Discuss (5 minutes):**
   - Go through each example as a class, asking groups to share their thoughts on which emails they identified as phishing and why.
   - Discuss the correct answers, highlighting key features of phishing emails and reinforcing the importance of skepticism when interacting online.
4. **Reflection/Conclusion:**
   - Wrap up by encouraging students to apply what they learned to their own online activities. Emphasize the significance of staying informed about cybersecurity threats.
   - This exercise is quick, interactive, and instills critical thinking about online safety!

[1] Generated using Chat GPT

Password Game [1]

OBJECTIVE:

Students will learn the principles of creating strong, secure passwords.

MATERIALS NEEDED:

- Whiteboard or flipchart
- Markers
- Handouts with password creation tips (optional)

INSTRUCTIONS:

1. **Introduction (1 minute)**
   - Briefly explain the importance of having strong passwords for online security.
   - Mention common threats like hacking and identity theft.
2. **Discuss Password Characteristics (2 minutes)**
   - Write key characteristics of a strong password on the board:
     - At least 12 characters long
     - A mix of uppercase and lowercase letters
     - Includes numbers
     - Uses special characters (e.g., @, #, $, %)
     - Avoids easily guessable information (like names, birthdays)
   - Ask students if they can think of any other tips or tricks for creating passwords.
3. **Create a Strong Password (3 minutes)**
   - Divide students into pairs.
   - Challenge each pair to create a strong password together using the characteristics discussed.
   - Encourage them to come up with a mnemonic or phrase to help remember it (e.g., "MyDogLovesToRun@5pm!").
4. **Share and Review (2 minutes)**
   - Invite a few pairs to share their password creations (without revealing the actual passwords).
   - Discuss what makes these passwords strong and whether they meet the outlined criteria.
5. **Reflection/Conclusion (2 minutes)**
   - Summarize the key points about password strength.
   - Emphasize the importance of using different passwords for different accounts and updating them regularly.
   - Optionally, introduce the concept of password managers as a way to keep track of passwords securely.
   - Encourage students to review their current passwords and consider updating them based on what they learned. Remind them that a strong password is a critical step in protecting their online identity!

[1] https://www.sciencebuddies.org/blog/boost-password-savvy-with-a-classroom-stem-game

women in CYBERSECURITY WiCyS wicys.org

Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation grant awarded to Tennessee Tech University, WiCyS has become a nonprofit organization offering many benefits for its members.

The WiCyS Conference is an excellent opportunity for companies to connect with female students and professional candidates to recruit them into cybersecurity jobs! More than half the attendees are students seeking opportunities, who have been accepted through the WiCyS scholarship program that sponsorships help to support.

Contact **info@wicys.org** for details.

Cyber-Trivia Kahoot Game [1]

OBJECTIVE:

Test students' knowledge of common threats and safe online practices

MATERIALS NEEDED:

- kahoot.com account

SAMPLE QUESTIONS:

1. TRUE or FALSE: All websites with "https" in the URL are 100% safe to use.
    a. **False:** "HTTPS" provides encryption but scammers can also use "HTTPS" meaning websites aren't always trustworthy.
2. What is a good safety practice to follow before posting something on social media?
    a. Make sure your post has a lot of hashtags to get more likes and visibility.
    b. Post immediately so that your followers see what you're doing in real time.
    c. Double check your post for any personal information or location details you do not want to be shared publicly.
    d. **Answer: C**. Be mindful of oversharing personal information like location to protect your privacy and not expose sensitive information.
3. You receive an email that looks like it's from your favorite online gaming platform, saying your account has been suspended and asking you to click a link to verify your login details. What should you do?
    a. Click the link and log in to recover your account as soon as possible
    b. Reply to the email asking for more details about why your account was suspended.
    c. Ignore the email and check your account directly by logging into the gaming platform through the official app or website.
    d. Forward the email to your friends to warn them about potential issues with their accounts.
    e. **Answer: C.** Phishing emails often try to trick you into revealing login details through fake links. It's safer to go directly to the official site or app to check for issues with your account.
4. TRUE or FALSE: Using the same password for all your online accounts is okay if the password is complex and difficult to guess.
    a. **False** - Using the same password across accounts means that if one of your accounts becomes compromised then all of your accounts are at risk of being compromised as well. Always use different passwords for important accounts.

[1] Game from Kahoot.com. Questions created by Jayda Bonnick.

women in CYBERSECURITY WiCyS wicys.org

Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation grant awarded to Tennessee Tech University, WiCyS has become a nonprofit organization offering many benefits for its members.

The WiCyS Conference is an excellent opportunity for companies to connect with female students and professional candidates to recruit them into cybersecurity jobs! More than half the attendees are students seeking opportunities, who have been accepted through the WiCyS scholarship program that sponsorships help to support.

Contact **info@wicys.org** for details.