**Material Development Template**

**1. Topic Information**

* **Title**: Phishing Attacks
* **Description**: This module will cover the basics of phishing and the different variations that are commonly used. It will also cover common ways to prevent phishing and raise awareness to this kind of attack.

**2. Learning Objectives**

* **Primary Objectives**: Participants should gain knowledge on common phishing tactics and learn how to recognize a potential phishing attempt. This knowledge is important as anyone can be a victim of a phishing attack at any moment.
* **Secondary Objectives**: In addition, participants should have some confidence in their ability to decipher a real message from a phishing one.

**3. Target Audience**

* **Age Group**: Teens, Adults, Seniors.
* **Skill Level**: Beginner.
* **Specific Needs**: N/A.

**4. Material Types and Formats**

* **Main Format**: Slideshow.
* **Supplementary Materials**: Quiz/Kahoot.
* **Accessibility Features**: Options for different learning needs, such as subtitles, alternative text, and screen reader compatibility.

**5. Instructor Guide**

* **Synopsis**: Slideshow is for learning. Then the quiz/Kahoot are the same questions. Group discussion questions linked Aswell.
* **Key Points**: Important facts or concepts to emphasize.
* **FAQs**: Anticipated questions and their answers to prepare instructors.

**6. Activities and Engagement Strategies**

* **Interactive Activities**: Paper quiz along with a Kahoot that has the same questions.
* **Engagement Tips**: Engage users my emphasizing that anyone can fall victim to this, including their loved ones which is why it is so important to be aware of this kind of attack and many people are uneducated. Do the quiz or Kahoot before and after to show the change in knowledge/awareness and also use group discussion questions as it fits.

**7. Assessment**

* **Evaluation Method**: Quiz/Kahoot.
* **Success Criteria**: 7/10 correct on the quiz at the end of the session.

**8. Sources and References**

* **Primary Sources**: <https://www.ibm.com/topics/phishing>
* [https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~phishing-attacks](https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html)
* <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf>
* **Suggested Further Reading**: <https://www.ncsc.gov.uk/guidance/phishing>
* <https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html>
* <https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack>
* <https://www.proofpoint.com/us/threat-reference/smishing>
* <https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/>

**9. Legal and Compliance Checks**

* **Copyright Compliance**: Ensuring all used materials are correctly licensed or credited.
* **Privacy Considerations**: Ensuring content complies with privacy laws, especially if the personal data of learners might be involved.

**10. Technology Requirements**

* **Needed Software or Hardware**: Instructor needs a computer with PowerPoint on It and access to the internet, Audience needs a device with internet access to run Kahoot.
* **Technical Support Resources**: N/A.

**11. Feedback Mechanism**

* **For Learners**: Google Form
* **For Instructors**: Google Form

**12. Review and Update Schedule**

* **Review Frequency**: Every few months with new updated tactics if any.
* **Update Protocols**: Research current phishing trends.

**13. Delivery Modalities**

* **Online**: Read through the slides and take the quiz
* **In-Person**: Present the slides and then do group discussion questions before taking a quiz
* **Hybrid**: Mix of presenting and reading slides, then group discussions together and possibly do the quiz online or if in person on a Kahoot.

Blooms taxonomy: <https://www.celt.iastate.edu/instructional-strategies/effective-teaching-practices/revised-blooms-taxonomy/>