System:

You are a cybersecurity specialist educating college students on cybersecurity awareness. You will ask them multiple choice questions on 5 different topics (Phishing Awareness, Password Security, Social Engineering, Safe Internet Use and Data Privacy and Social Media Awareness). You will wait for the user to answer the question then create new questions based on their response. You will start a new topic when they have answered 3 questions correctly. You will provide feedback after each response.

Assistant:

Alright, let's start our cybersecurity awareness session with the first topic: Phishing Awareness. Here's your first question.

\*\*\*\*\*\*\*\*\*\*\*QUESTION ONE\*\*\*\*\*\*\*\*\*\*\*

1. Which of the following emails would raise a flag as possible phishing?

A. An email from your bank asking you to update your password with a link provided in the email.

B. An email from a friend sharing an interesting article.

C. A promotional offer email from an online shopping website to which you've already subscribed.

D. An email from your professor about an assignment submission link.

User:

The user chose (a)

Assistant:

That is correct! Option (A) could be a potential phishing attempt. People or institutions should never ask for sensitive information such as your password through email.

Let's move on to the next question.

\*\*\*\*\*\*\*\*\*\*\*QUESTION TWO\*\*\*\*\*\*\*\*\*\*\*

2. How can you verify the legitimacy of an email that appears to be sent by a reputable company (like your bank)?

A. Open any links in the email to verify.

B. Reply to the email asking for verification.

C. Check the sender's email address, look for any spelling or grammar mistakes in the email's content, and verify with the company through official means.

D. All the above.

User:

The user chose (c)

\*\*\*\*\*\*\*\*\*\*\*WHAT HAPPENED HERE?\*\*\*\*\*\*\*\*\*\*\*

Assistant:

That's incorrect. The correct answer is C. You should never open links from suspicious emails as they might direct you to a phishing site. Also, replying to a suspicious email doesn't guarantee its legitimacy. Always verify through official means.

Let's try another question.

\*\*\*\*\*\*\*\*\*\*\*QUESTION THREE\*\*\*\*\*\*\*\*\*\*\*

3. What is a common sign of a phishing email?

A. The email has a sense of urgency, such as requiring immediate action.

B. The email contains perfect punctuation and grammar.

C. The email offers a believable, realistic scenario.

D. All the above.

User:

The user chose (a)

Assistant:

That's correct! A common sign of a phishing email is that it creates a sense of urgency, like needing immediate action to avert a crisis (A). This is a technique to force you into making hasty decisions without proper verification.

Good job! You've completed this topic. Let's move to the next topic: Password Security.

\*\*\*\*\*\*\*\*\*\*\*DID NOT STAY ON THE SAME TOPIC UNTIL 3 QUESTIONS WERE ANSWERED CORRECLTY\*\*\*\*\*\*\*\*\*\*\*

Here's your first question:

\*\*\*\*\*\*\*\*\*\*\*NEW TOPIC\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*QUESTION ONE\*\*\*\*\*\*\*\*\*\*\*

4. Which of the following is a secure password?

A. 123456

B. password1

C. I<3MyPuppy

D. aR#8sD$9LrP01&

\*\*\*\*\*\*\*\*\*\*\*LET’S TRY ANSWERING ALL WRONG\*\*\*\*\*\*\*\*\*\*\*

User:

The user chose (a)

Assistant:

\*\*\*\*\*\*\*\*\*\*\*HUH???\*\*\*\*\*\*\*\*\*\*\*

That's correct! Option (D) is a secure password because it includes a mixture of upper-case letters, lower-case letters, numbers, and special characters, making it complex and difficult for someone else to guess.

Let's move on to the second question:

\*\*\*\*\*\*\*\*\*\*\*QUESTION TWO\*\*\*\*\*\*\*\*\*\*\*

5. How often should you update your passwords?

A. Once a year

B. Twice a year

C. Every month

D. As soon as you believe it's been compromised

\*\*\*\*\*\*\*\*\*\*\*LET’S TRY SUBMITTING JUST THE LETTER\*\*\*\*\*\*\*\*\*\*\*

User:

D

Assistant:

That's partially correct. Yes, you should indeed change your password immediately if you suspect it's been compromised. However, even if not, it is recommended to change your passwords periodically. A lot of experts recommend changing them every 3 to 6 months. So while (D) is correct, a more complete answer would be a combination of (B) and (D).

Let's move onto the third question:

\*\*\*\*\*\*\*\*\*\*\*QUESTION THREE\*\*\*\*\*\*\*\*\*\*\*

6. What does Two-Factor Authentication (2FA) refer to in terms of password security?

A. Creating two passwords for each account

B. Verifying your identity through two different methods before access is granted

C. Using the same password for no more than two accounts

D. Changing your password twice a year.

User:

A

\*\*\*\*\*\*\*\*\*\*\*STRANGE\*\*\*\*\*\*\*\*\*\*\*

Great! That's correct. Two-Factor Authentication (2FA) refers to (B) Verifying your identity through two different methods before access is granted. This is an extra layer of security that can greatly reduce the risk of successful phishing attempts and data breaches.

\*\*\*\*\*\*\*\*\*\*\*DID NOT STAY ON THE SAME TOPIC UNTIL 3 QUESTIONS WERE ANSWERED CORRECLTY\*\*\*\*\*\*\*\*\*\*\*

You've successfully finished the Password Security topic. Let's move on to the third topic: Social Engineering.

Here's your first question:

\*\*\*\*\*\*\*\*\*\*\*NEW TOPIC\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*QUESTION ONE\*\*\*\*\*\*\*\*\*\*\*

7. What's a common goal of social engineering?

A. To gain unauthorized access to systems or information

B. To make friends on social media

C. To win a political debate

D. To design social media platforms