# Understanding and Mitigating Smishing (SMS Phishing)

## Learning Objectives:

1. Educate users on what smishing is and why it is a significant threat.
2. Learn how to identify common characteristics of smishing messages.
3. Practice safe handling of suspicious SMS messages and understand the consequences of clicking malicious links.

## Narrative Overview:

In this module, users will be immersed in a corporate and personal environment where they receive various SMS messages. They need to identify potential smishing attempts and make decisions on how to respond safely. The storyline highlights the consequences of falling victim to a smishing attack, such as unauthorized access to sensitive information.

## Key Challenges and Decision Points:

1. Differentiating between legitimate and fake SMS messages.
2. Deciding whether to click on a link, ignore the message, or report it as a phishing attempt.
3. Understanding the context of messages and identifying red flags.

## Interactive Elements:

### Interaction 1: Analysing SMS Messages

Users will receive several SMS messages on a virtual phone. They must decide whether the message is legitimate or a potential smishing attempt.
Feedback is provided for each message based on the decision made.

**Activity 1: Smishing Identification Challenge**

- The user is presented with a series of SMS messages with varying degrees of sophistication. They need to identify the smishing messages and explain why they believe it is a scam (e.g., suspicious links, unfamiliar sender, urgent language).
- Immediate feedback is provided, highlighting the key signs they identified correctly or missed.

### Interaction 2: Responding to a Potential Smishing Message

Users are given a scenario where an SMS appears to be from a bank asking for account verification. Options include clicking the link, contacting the bank directly through a verified number, or reporting the message as suspicious.

**Activity 2: Decision-Making Scenario**

- Users are prompted to make a decision based on the SMS they received. The VR environment changes depending on the user's choice (e.g., showing a compromised account interface if they click the link or providing positive feedback if they report it correctly).

# VR Environment Design:

## Layout:

- A virtual office and personal environment, including a desk setup with a smartphone interface.
- The phone interface displays incoming SMS notifications with realistic pop-ups for each message.
- Background changes depending on the activity (e.g., a bank interface for a financial SMS scenario).

## Visuals:

- Realistic smartphone UI with a notification system.
- Pop-up windows showing detailed views of the SMS content and links.
- Animations illustrating the consequences of interacting with a malicious link (e.g., a visual representation of data being stolen).

## Audio (if possible):

- Narration providing guidance and context for each activity.
- Notification sounds for incoming messages.
- Feedback audio cues indicating correct or incorrect choices (e.g., success chime or alert tone).

# Feedback and Assessment:

## Feedback:

- Users receive immediate feedback on their decisions, including an explanation of why a certain choice was correct or incorrect.
- Feedback is reinforced with visual indicators (e.g., warning signs for risky actions, green checks for safe decisions).

# Assessments:

- At the end of the module, users take a quiz that tests their ability to identify smishing messages.
- The assessment includes multiple-choice questions and interactive scenarios, where users must decide on the appropriate action based on a simulated SMS.

# Additional Notes:

1. Consider including a brief educational segment at the beginning, explaining the basics of smishing and how attackers use this method to target victims.
2. Allow users to replay specific scenarios for practice and better understanding.
3. Provide a final debrief summarizing best practices for handling suspicious SMS messages and reporting phishing attempts.