Phishing Awareness Training

This presentation will cover the definition and importance of phishing awareness, common types of attacks, and tips for recognizing phishing attempts.

PP

by Preyas Pandya

What is Phishing?

Definition

Phishing is a type of cyberattack where criminals use deceptive tactics to trick victims into revealing sensitive information, such as passwords or financial details. This information is then used for identity theft or fraud.

Importance

Phishing attacks are becoming increasingly sophisticated and common. It is crucial to understand the dangers of phishing and know how to protect yourself and your organization.

Types of Phishing Attacks

Email Phishing

Unsolicited emails sent to a large group of people, often with malicious links or attachments.

Spear Phishing

Targeted emails sent to specific individuals with personalized information to appear legitimate.

Whaling

A type of spear phishing targeting high-profile individuals, such as CEOs or executives.

Smishing

Phishing attacks delivered through SMS messages, often mimicking official notifications.

Vishing

Phishing attacks conducted over the phone, usually involving spoofed caller IDs and convincing scripts.

Email Phishing

Subject Line

Subject lines may use urgency, fear, or curiosity to encourage opening the email.

Sender Address

Sender addresses may be misspelled or unfamiliar, and the email may not have an official domain.

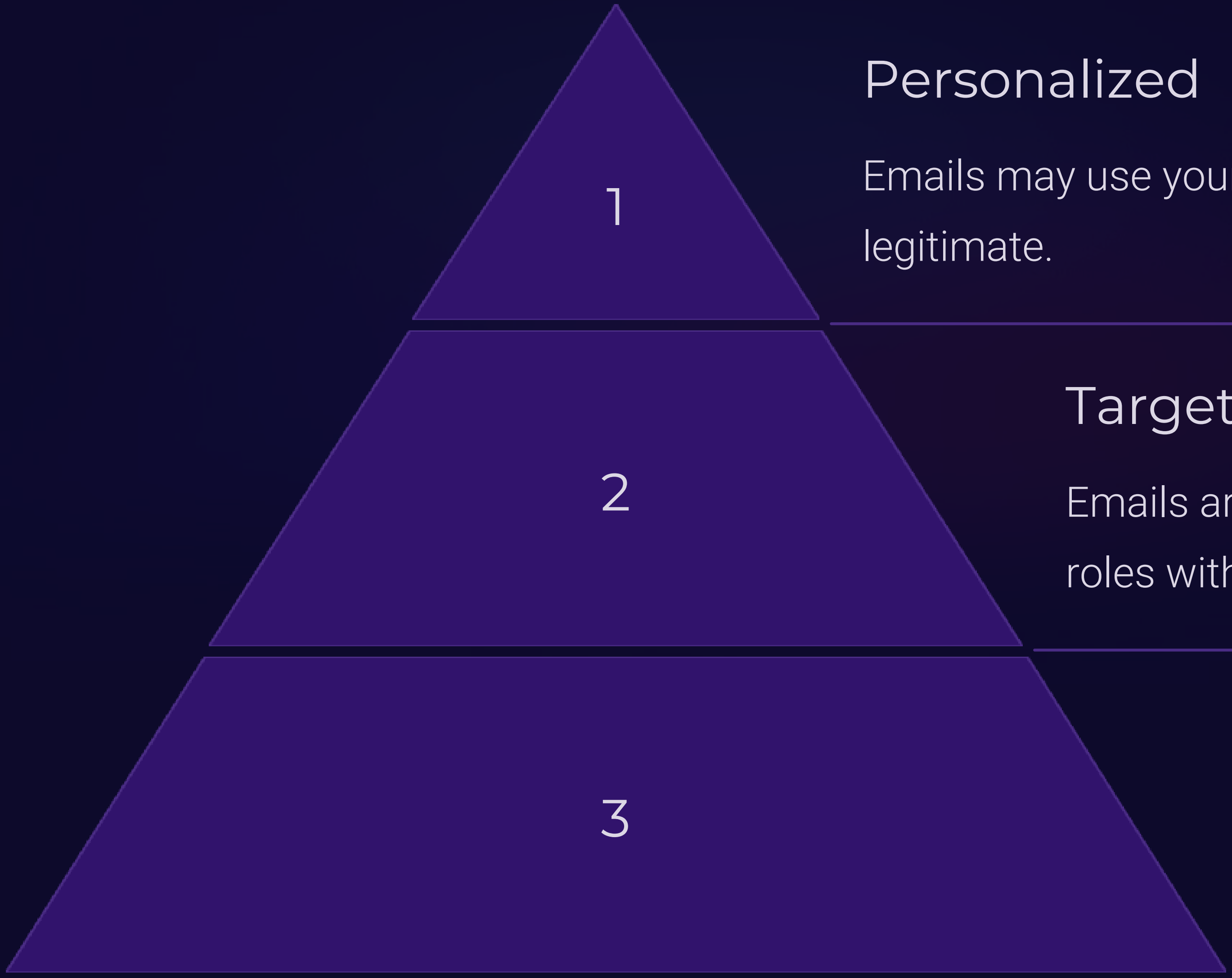
Attachments

Be wary of attachments, especially if you were not expecting them or if the file type is unexpected.

Links

Hover over links to verify they lead to the expected destination, and avoid clicking on shortened or suspicious URLs.

Spear Phishing



Personalized

Emails may use your name, company, or other personal information to appear legitimate.

Targeted

Emails are often sent to individuals who work in specific departments or roles within an organization.

Sophisticated

Emails may be crafted to mimic legitimate communications, making them harder to detect as phishing attacks.

Whaling

1

High-profile Targets

Whaling attacks target senior executives, CEOs, or other high-profile individuals within an organization.

2

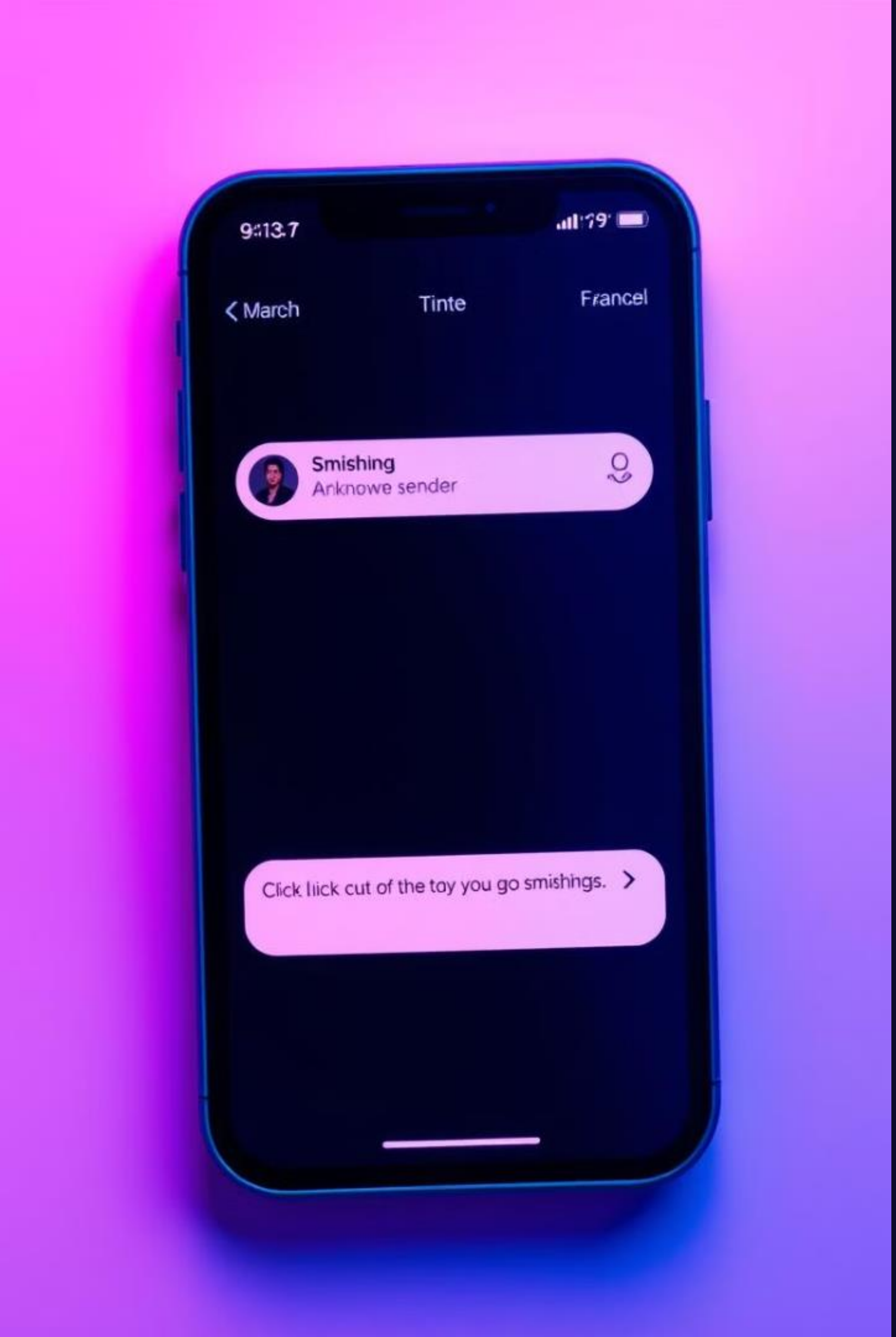
Financial Motives

The aim is to gain access to sensitive information or finances, potentially causing significant financial damage to the organization.

3

Extensive Research

Attackers conduct extensive research on their targets to tailor their emails and gain their trust.



Smishing

1. ## SMS Messages

Phishing attacks are delivered through SMS messages, often mimicking official notifications or messages from trusted sources.

2. ## Shortened Links

Messages often contain shortened URLs, making it difficult to determine the true destination of the link.

3. ## Sense of Urgency

Messages may create a sense of urgency, urging the recipient to click the link immediately.

Vishing

1

Spoofed Caller ID

Attackers use spoofed caller IDs to appear as legitimate organizations or individuals.

2

Convincing Scripts

Attackers employ convincing scripts to trick victims into divulging sensitive information, often using emotional manipulation.

3

Request for Personal Data

Attackers may ask for personal information, such as credit card numbers, passwords, or bank account details.

Signs of a Phishing Attempt

1

Urgency

Emails or messages that create a sense of urgency, demanding immediate action, may be suspicious.

2

Grammar and Spelling Errors

Phishing emails often have poor grammar and spelling errors, a sign of unprofessionalism or a lack of legitimacy.

3

Suspicious Links or Attachments

Be wary of links that redirect to unfamiliar websites or attachments from unknown senders.

4

Requests for Personal Information

Legitimate organizations rarely ask for sensitive personal information via email or SMS.

Recognizing Phishing Websites

Be cautious of websites that look similar to legitimate ones but have slight variations in the URL or logo.