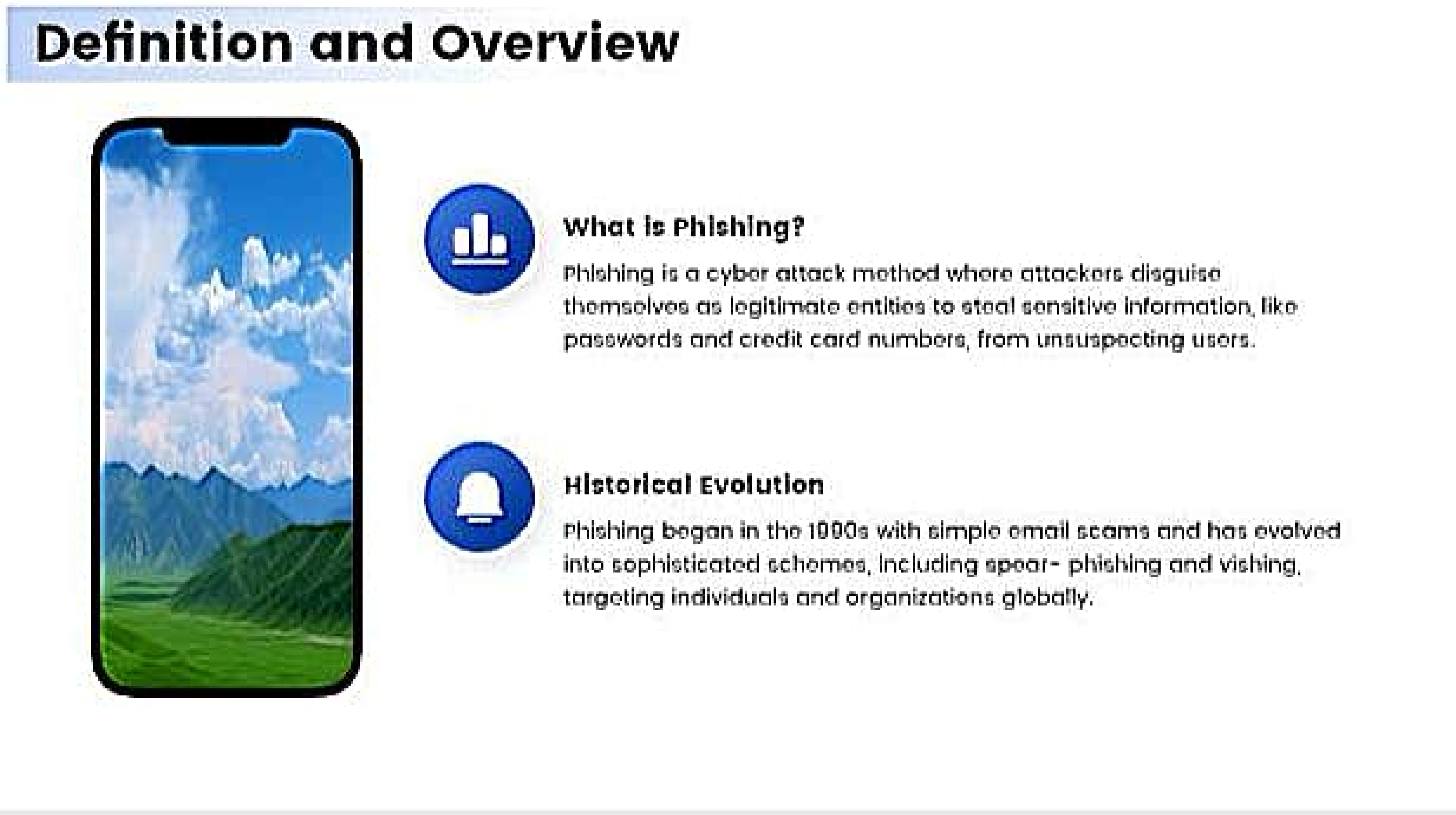
PHISHING AWARNEESS

- This presentation aims to raise awareness about phishing attacks, empowering individuals to recognize and avoid phishing attempts, including malicious emails, fake websites, and social engineering schemes.
- We'll begin by discussing what phishing is and why attackers use this method.



Definition and Overview

What is Phishing?

Phishing is a cyber attack method where attackers disguise themselves as legitimate entities to steal sensitive information, like passwords and credit card numbers, from unsuspecting users.

Historical Evolution

Phishing began in the 1990s with simple email scams and has evolved into sophisticated schemes, including spear- phishing and vishing, targeting individuals and organizations globally.

02

Types of Phishing Attacks

Email Phishing

Common Techniques

Email phishing involves sending deceptive emails that appear to come from a legitimate source to trick the recipient into revealing sensitive information.

Recognizing Indicators

Indicators of email phishing include unfamiliar senders, suspicious links, urgent language, and unexpected attachments aimed at extracting personal data or login credentials.

Spear Phishing

01.

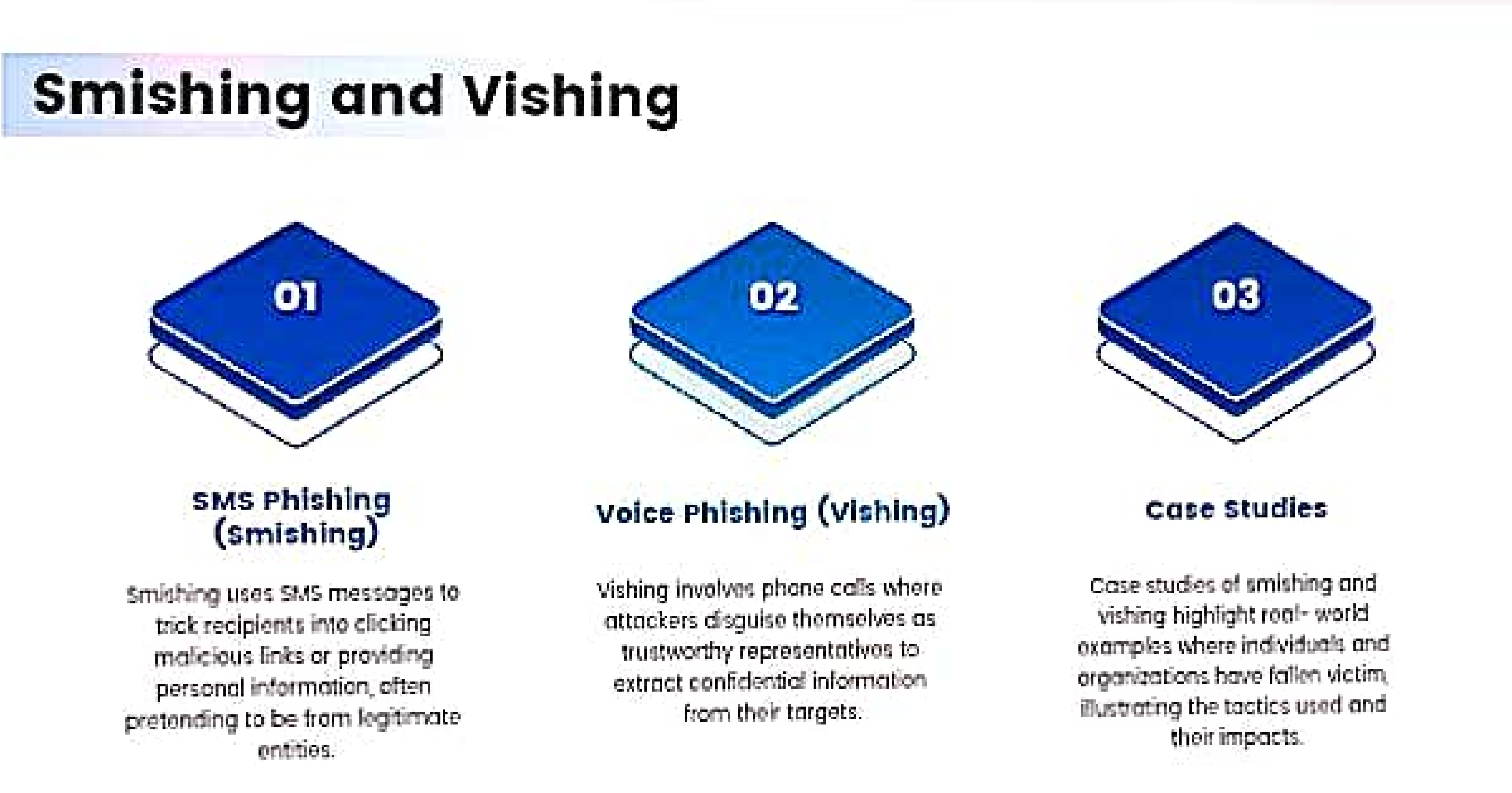
Targeted Nature

Spear phishing is a more targeted attack where cyber criminals gather detailed information about the victim to personalize their deceptive messages.

02.

High-Profile Examples

High- profile spear phishing examples include attacks on major corporations and government entities, often leading to significant data breaches and financial loss.



Smishing and Vishing

01

SMS Phishing (Smishing)

Smishing uses SMS messages to trick recipients into clicking malicious links or providing personal information, often pretending to be from legitimate entities.

02

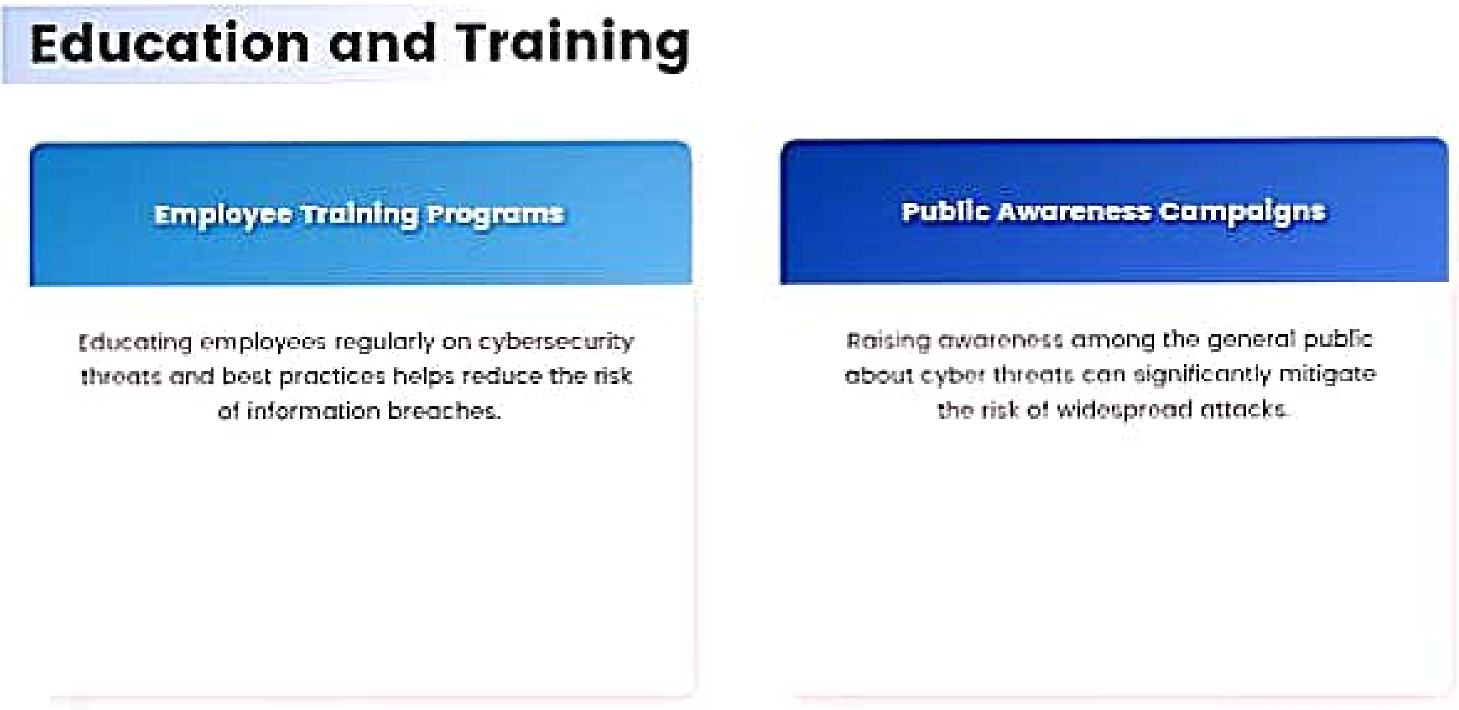
Voice Phishing (Vishing)

Vishing involves phone calls where attackers disguise themselves as trustworthy representatives to extract confidential information from their targets.

03

Case Studies

Case studies of smishing and vishing highlight real- world examples where individuals and organizations have fallen victim, illustrating the tactics used and their impacts.



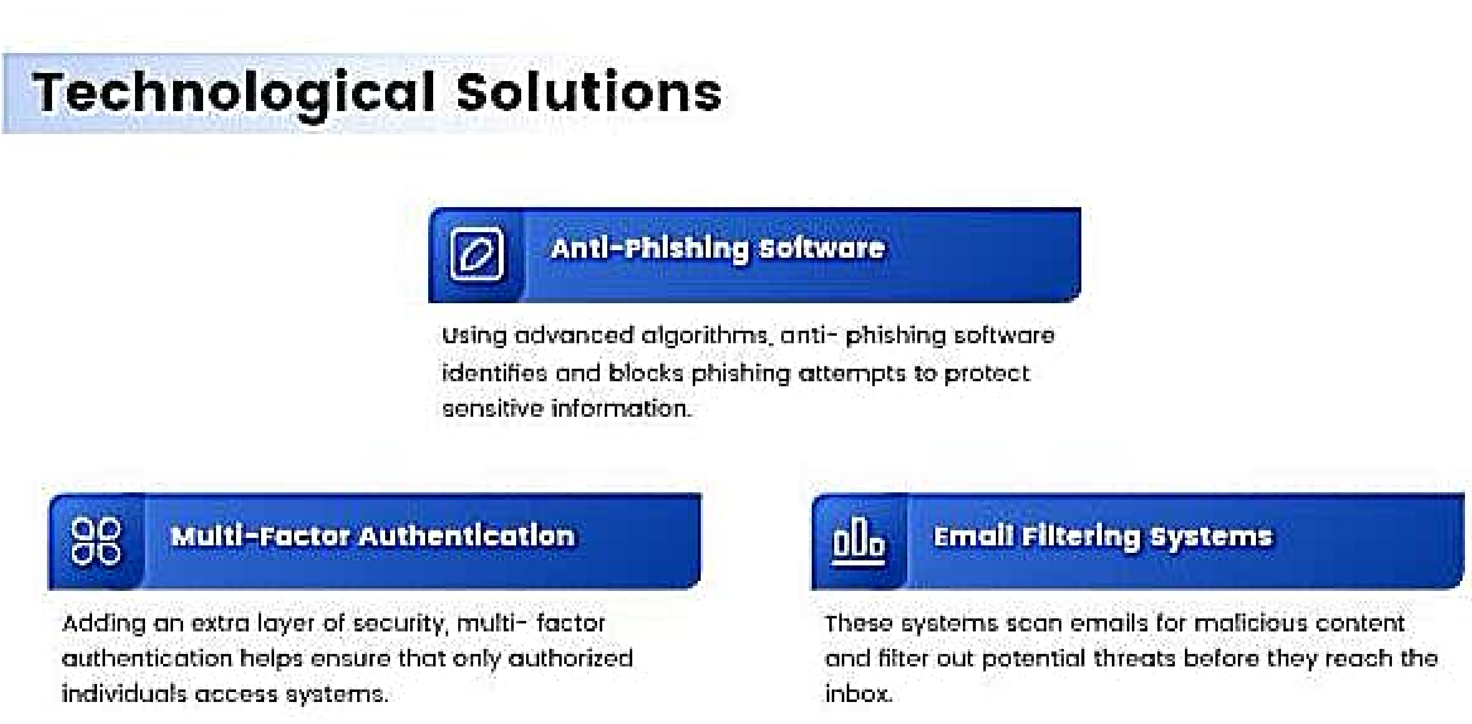
Education and Training

Employee Training Programs

Educating employees regularly on cybersecurity threats and best practices helps reduce the risk of information breaches.

Public Awareness Campaigns

Raising awareness among the general public about cyber threats can significantly mitigate the risk of widespread attacks.



Technological Solutions

Anti-Phishing Software

Using advanced algorithms, anti- phishing software identifies and blocks phishing attempts to protect sensitive information.

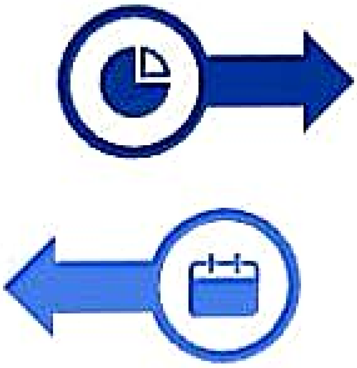
Multi-Factor Authentication

Adding an extra layer of security, multi- factor authentication helps ensure that only authorized individuals access systems.

Email Filtering Systems

These systems scan emails for malicious content and filter out potential threats before they reach the inbox.

Identifying a Phishing Attack



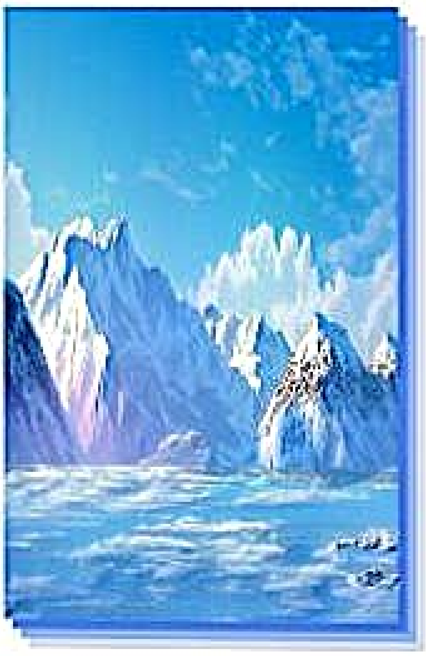
Early Warning Signs

Recognizing early warning signs such as unexpected emails requesting sensitive information, poor grammar, and suspicious links can help in identifying phishing attacks quickly.

Reporting Procedures

Establish procedures for reporting suspected phishing attacks internally and externally to ensure timely action and containment.

Mitigation Strategies



01.

Containment Measures

Containment measures include isolating infected systems and preventing the spread of malicious activity within the network.

02.

Recovery Plans

Recovery plans involve steps to restore data, systems, and services to normal operation following a phishing attack.

03.

Post-Incident Analysis

Post- Incident analysis examines the attack's root causes, impact and effectiveness of the response to improve future defenses.

Thank you!