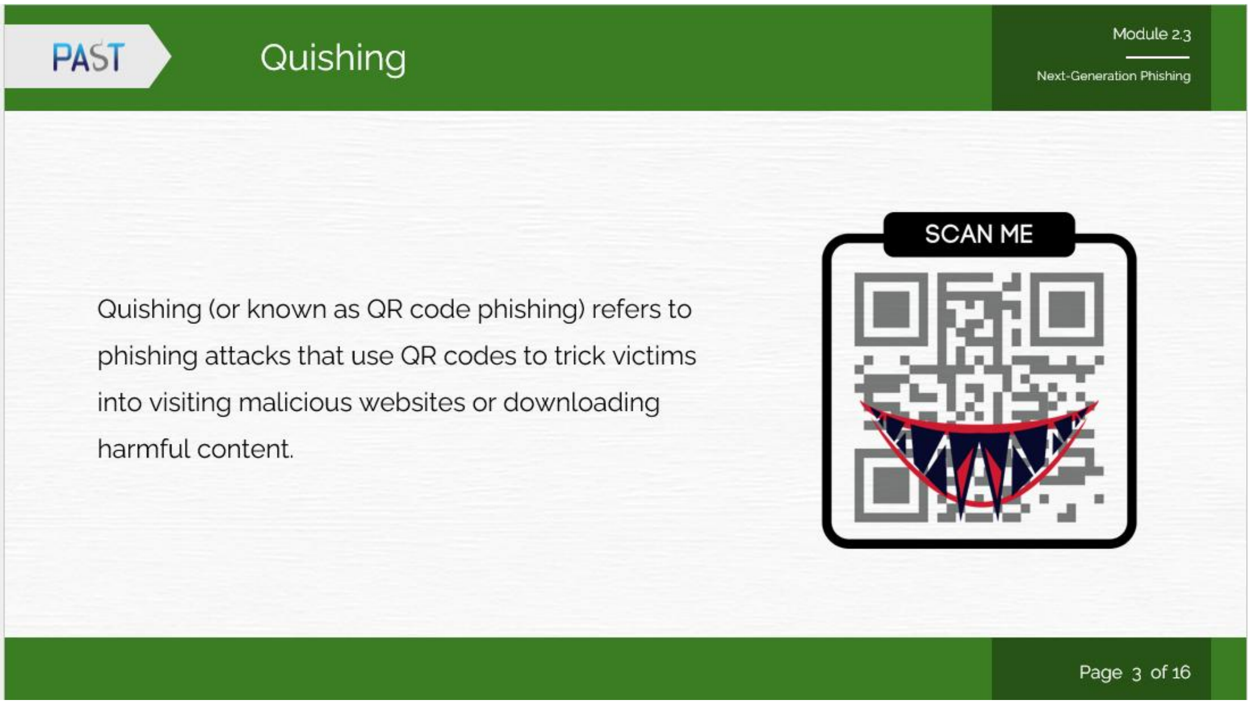
Phishing Assessment

Module 2.3: Next-Generation Phishing

Table of Contents

1. Quishing



PAST

Quishing

Module 2.3

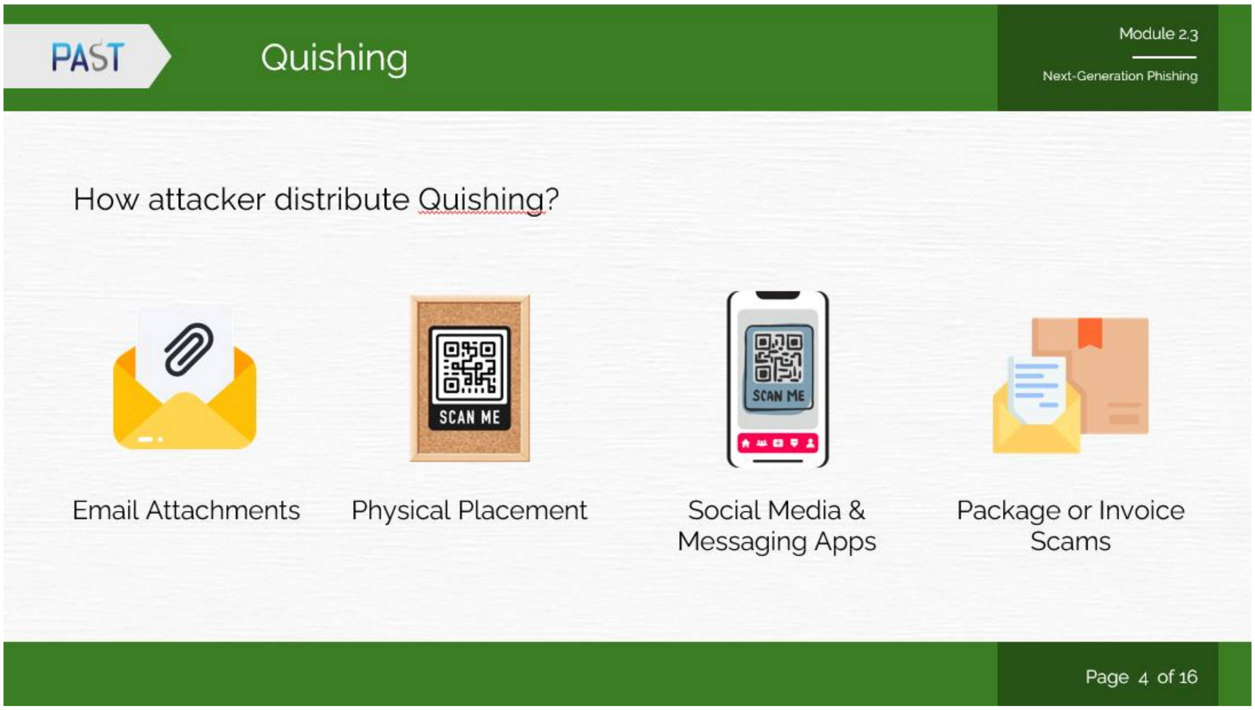
Next-Generation Phishing

Quishing (or known as QR code phishing) refers to phishing attacks that use QR codes to trick victims into visiting malicious websites or downloading harmful content.

Page 3 of 16

Quishing refers to phishing attacks that use QR codes to trick victims into visiting malicious websites or downloading harmful content. Attackers leverage QR codes as a phishing method because they are widely used for convenience in accessing links, payment portals, and other digital services, especially on mobile devices.

Creating a Malicious QR Code: Attackers generate a QR code that links to a phishing website, downloads malware, or captures sensitive data. The code often redirects to fake login pages, fraudulent payment portals, or malicious apps.



PAST

Quishing

Module 2.3

Next-Generation Phishing

How attacker distribute Quishing?

Email Attachments

Physical Placement

Social Media & Messaging Apps

Package or Invoice Scams

Page 4 of 16

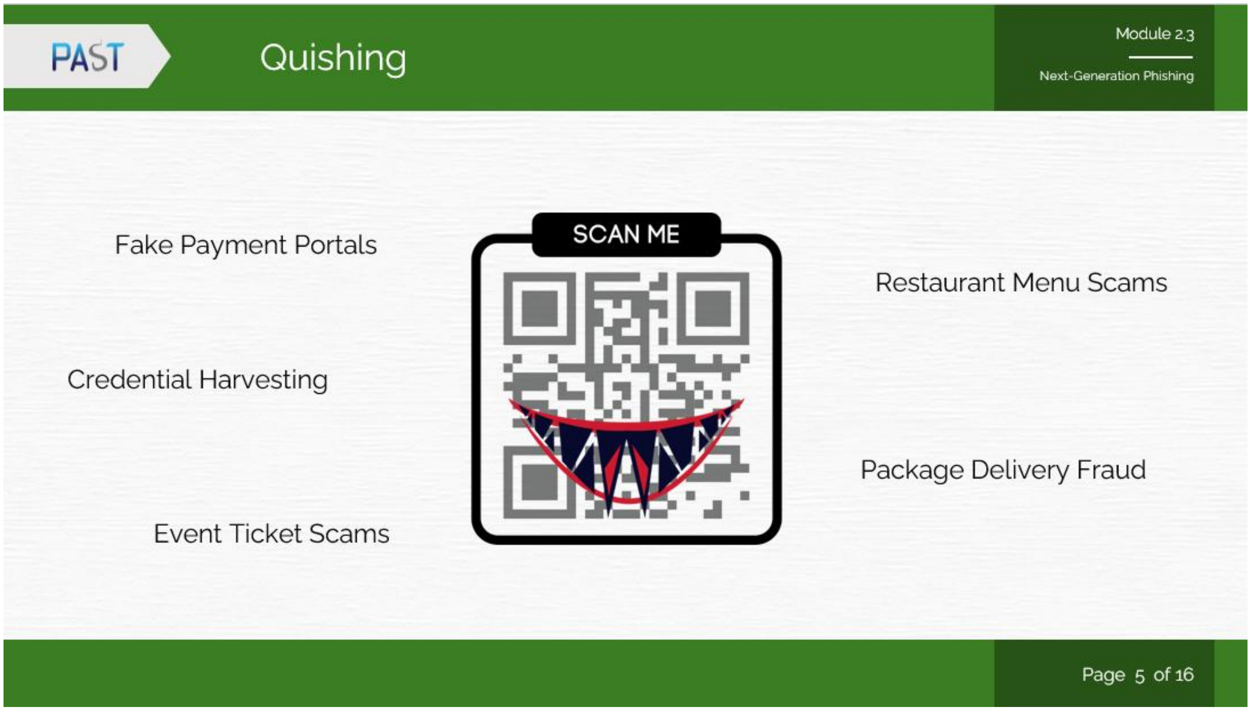
How do attackers distribute Quishing?

Email Attachments: The QR code is embedded in phishing emails, urging users to scan it to verify accounts, make payments, or view documents.

Physical Placement: Codes are placed on posters, flyers, or public locations, such as restaurants, transportation hubs, or event venues.

Social Media and Messaging Apps: Attackers share the QR code in posts or direct messages.

Package or Invoice Scams: Fake QR codes are included on printed invoices or package delivery slips.



PAST

Quishing

Module 2.3

Next-Generation Phishing

Fake Payment Portals

Credential Harvesting

Event Ticket Scams

Restaurant Menu Scams

Package Delivery Fraud

Page 5 of 16

Examples of Quishing Scenarios

Fake Payment Portals: A fake utility bill includes a QR code that redirects to a fraudulent payment page. The victim enters their payment details, which are stolen by the attacker.

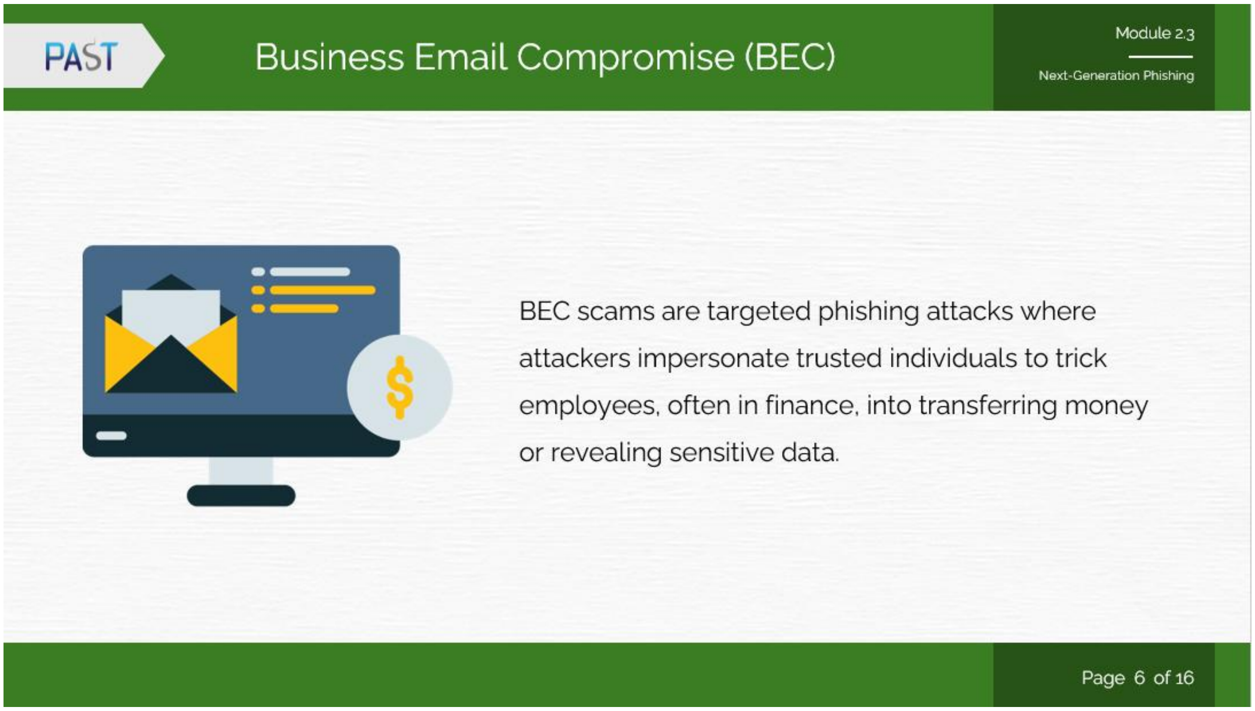
Credential Harvesting: An email claims to be from a service provider, asking the recipient to scan a QR code to verify their account. The code redirects to a fake login page that captures credentials.

Event Ticket Scams: A poster advertising a popular event includes a QR code to "buy tickets." Scanning it leads to a phishing site that collects personal and payment details.

Restaurant Menu Scams: Attackers place stickers with fake QR codes over real QR codes on restaurant tables. Scanning the fake code downloads malware or redirects to a phishing site.

Package Delivery Fraud: Victims receive a delivery slip with a QR code claiming to offer tracking details. Scanning the code installs spyware or directs the victim to a phishing page.

2. Business Email Compromise (BEC)



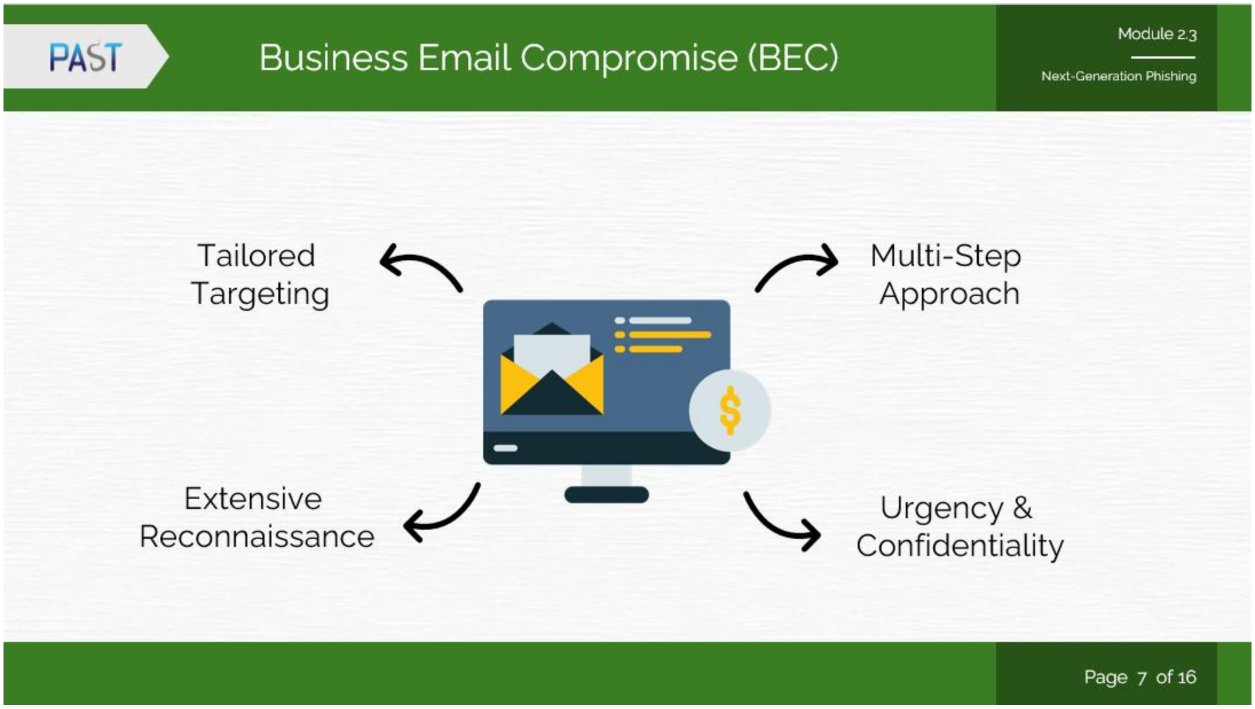
Business Email Compromise (BEC)

Module 2.3
Next-Generation Phishing

BEC scams are targeted phishing attacks where attackers impersonate trusted individuals to trick employees, often in finance, into transferring money or revealing sensitive data.

Page 6 of 16

BEC scams are highly targeted phishing attacks where attackers impersonate trusted individuals or organizations to deceive employees, often in financial departments, into transferring funds or disclosing sensitive information.



PAST

Business Email Compromise (BEC)

Module 2.3

Next-Generation Phishing

Tailored Targeting

Multi-Step Approach

Extensive Reconnaissance

Urgency & Confidentiality

Page 7 of 16

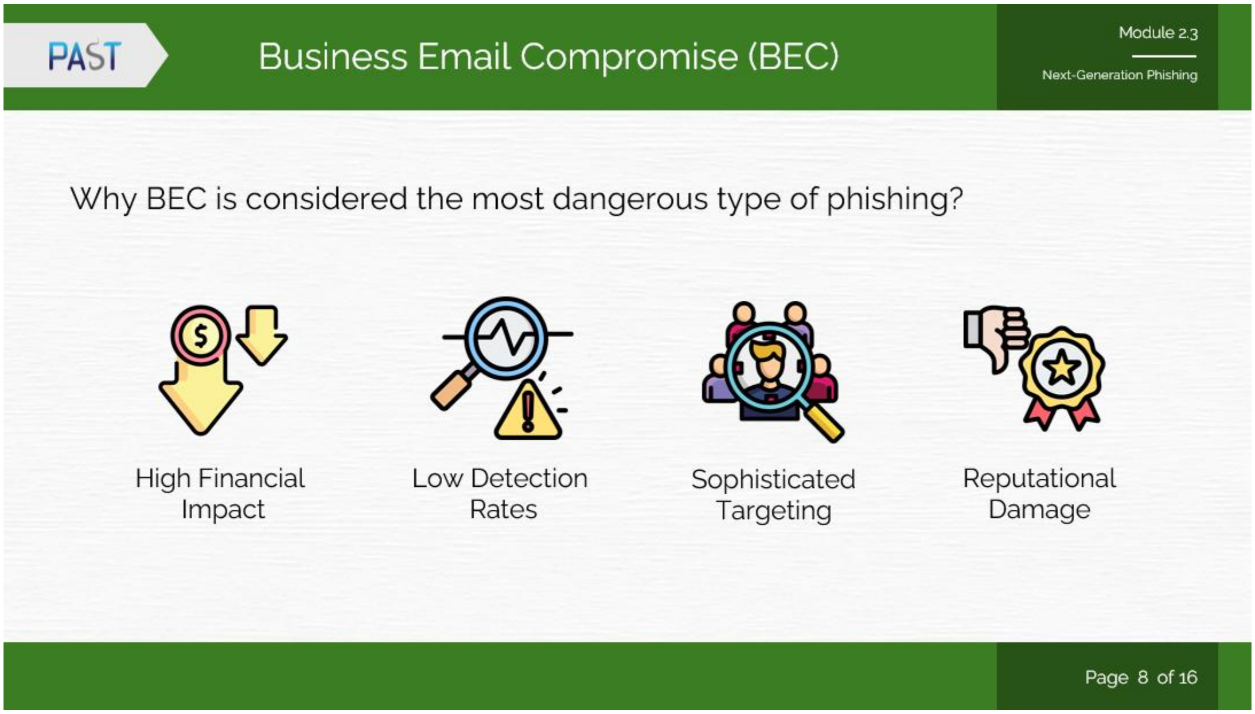
Key Characteristics of Sophisticated BEC Scams:

Tailored Targeting: Attackers focus on finance teams, payroll departments, or C-suite executives with authority over funds or sensitive data.

Extensive Reconnaissance: Scammers often study their targets by monitoring company websites, social media, or employee LinkedIn profiles to gather information about organizational hierarchies and processes.

Multi-Step Approach: Scams often begin with initial compromises (e.g., phishing or malware) to infiltrate an organization’s email system and observe communications before launching the main attack.

Use of Urgency and Confidentiality: Messages often stress urgent deadlines or confidentiality to prevent employees from verifying the requests with colleagues or supervisors.



PAST

Business Email Compromise (BEC)

Module 2.3

Next-Generation Phishing

Why BEC is considered the most dangerous type of phishing?

High Financial Impact

Low Detection Rates

Sophisticated Targeting

Reputational Damage

Page 8 of 16

Why is BEC is Most dangerous type of phishing?

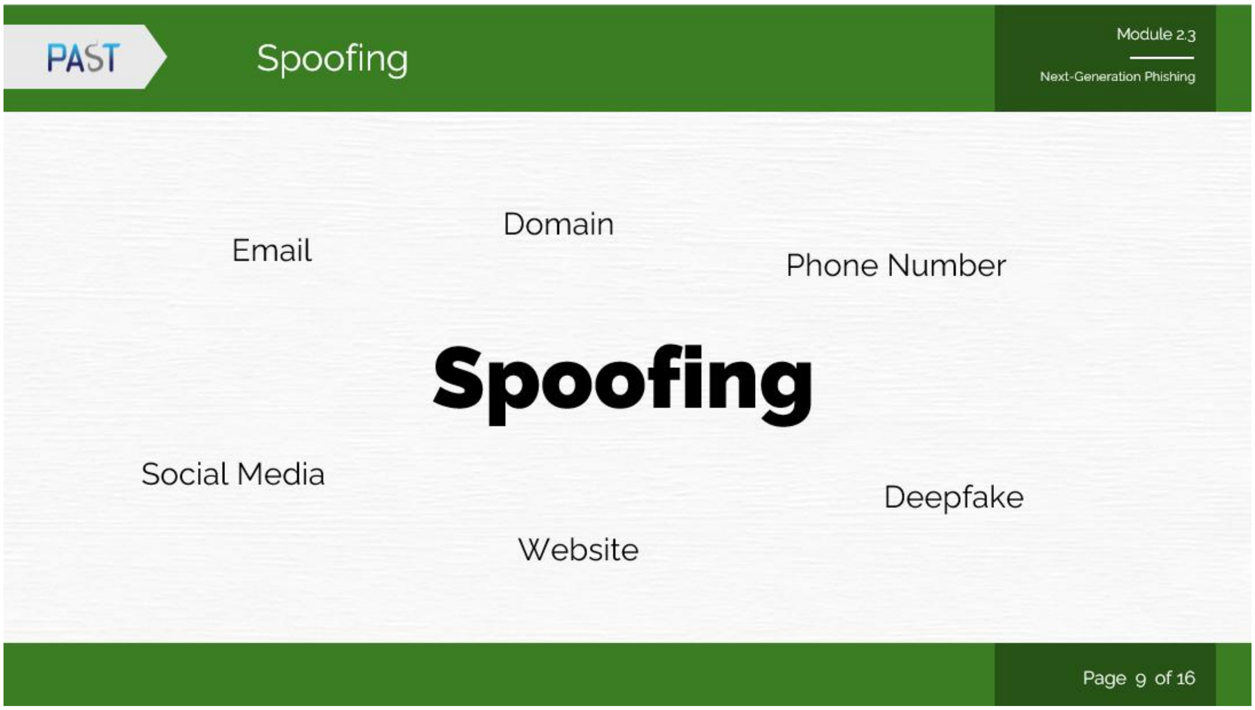
High Financial Impact: Attackers impersonate high-ranking executives, suppliers, or business partners, tricking employees into transferring large sums of money to fraudulent accounts.

Low Detection Rates: BEC emails often contain no malicious links or attachments, bypassing traditional email security filters.

Sophisticated Targeting: These attacks focus on high-value targets, such as financial departments or executives with the authority to approve large transactions.

Reputational Damage: A successful BEC attack can harm an organization’s reputation, eroding trust among clients, suppliers, and stakeholders.

3. Spoofing


PAST Spoofing

Module 2.3

Next-Generation Phishing

Spoofing

Email

Domain

Phone Number

Social Media

Website

Deepfake

Page 9 of 16

What Is Spoofing in Phishing?

Spoofing involves manipulating communication methods—such as email addresses, phone numbers, websites, or even identities—to appear as though they are coming from a trusted source. The goal is to deceive the target into taking an action, such as clicking a malicious link, sharing sensitive information, or making unauthorized financial transactions.

Spoofing Techniques in Phishing

Email Spoofing: Attackers forge email headers to make messages appear as if they are coming from legitimate domains or trusted contacts.

Domain Spoofing: Attackers create domains that closely resemble legitimate ones, often exploiting typos or similar-looking characters (e.g., "example.com" vs. "examp1e.com").

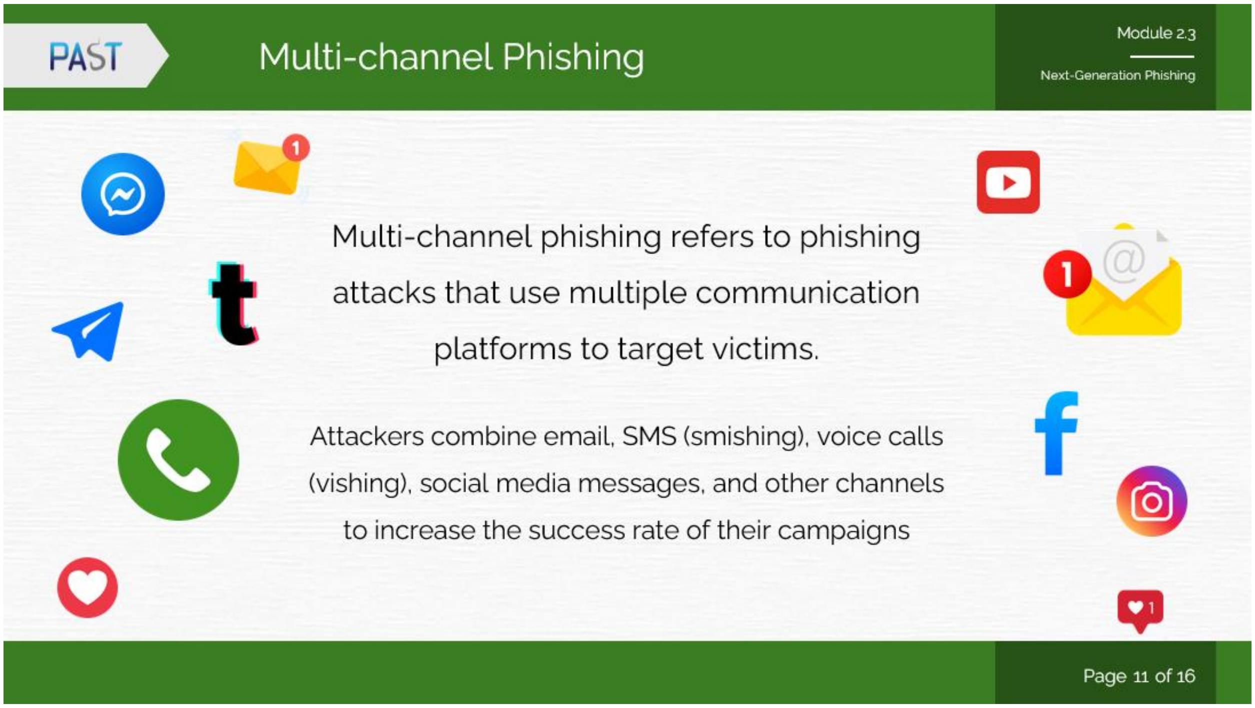
Phone Number Spoofing: Attackers manipulate Caller ID to display a trusted number, such as a bank or government agency.

Website Spoofing: Attackers create fake websites that mimic legitimate ones, often used in conjunction with phishing emails or SMS.

Social Media Spoofing: Attackers create fake profiles of trusted individuals or organizations on platforms like LinkedIn, Facebook, or Instagram.

Deepfake Spoofing: Attackers use AI-generated audio or video to impersonate trusted individuals.

4. Multi-channel phishing



PAST

Multi-channel Phishing

Module 2.3

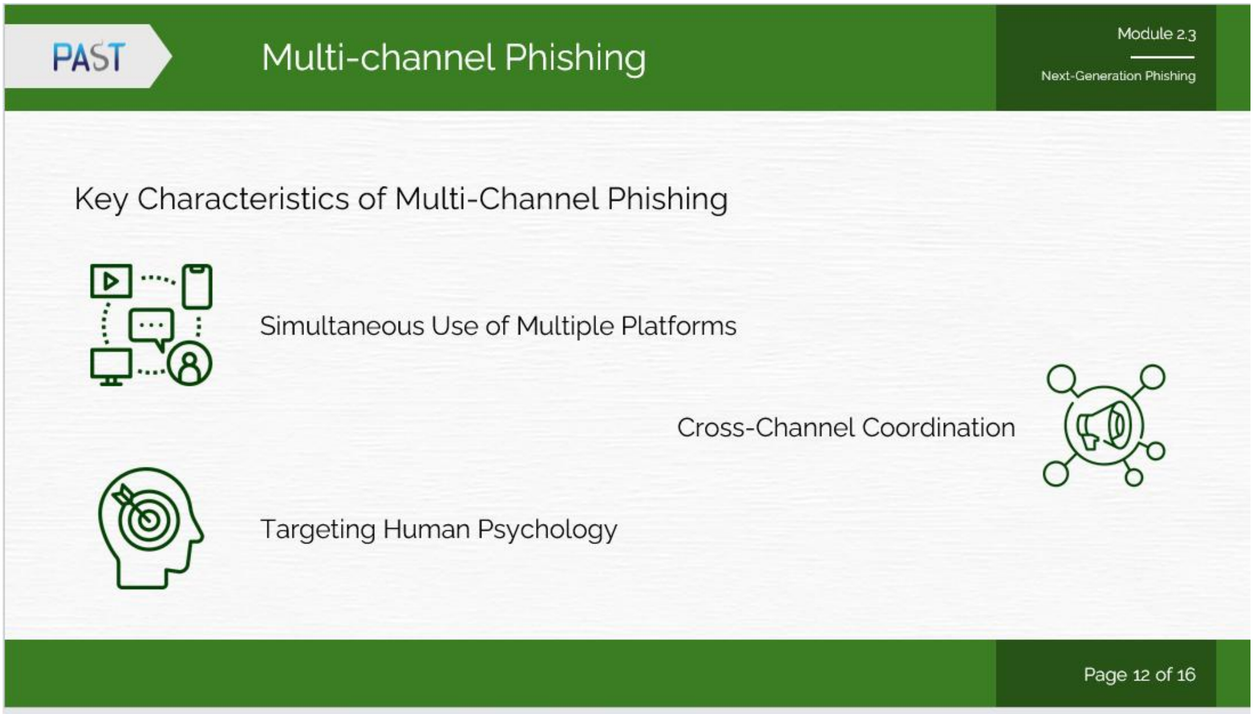
Next-Generation Phishing

Multi-channel phishing refers to phishing attacks that use multiple communication platforms to target victims.

Attackers combine email, SMS (smishing), voice calls (vishing), social media messages, and other channels to increase the success rate of their campaigns

Page 11 of 16

Multi-channel phishing refers to phishing attacks that use multiple communication platforms to target victims. Attackers combine email, SMS (smishing), voice calls (vishing), social media messages, and other channels to increase the success rate of their campaigns. This approach leverages the victim’s trust in different mediums and creates a coordinated and convincing attack scenario.



PAST

Multi-channel Phishing

Module 2.3

Next-Generation Phishing

Key Characteristics of Multi-Channel Phishing

Simultaneous Use of Multiple Platforms

Cross-Channel Coordination

Targeting Human Psychology

Page 12 of 16

Key Characteristics of Multi-Channel Phishing

- Simultaneous Use of Multiple Platforms

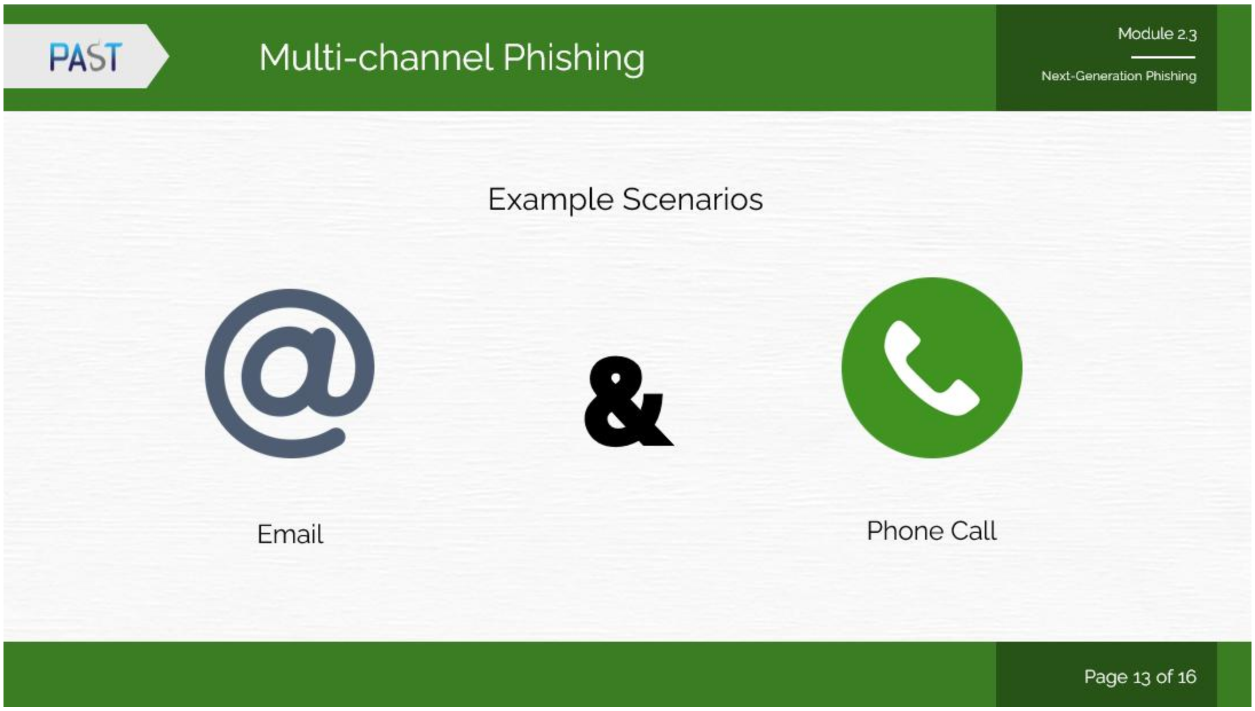
Attackers use various channels, such as email, SMS, phone calls, or social media, to contact the victim and reinforce the phishing message. The key idea is that the victim receives multiple, coordinated messages to create a sense of urgency and legitimacy.

- Cross-Channel Coordination

Each channel reinforces the phishing attempt, creating a false sense of authenticity. Instead of just simultaneous messaging, it emphasizes how one channel builds trust in another.

- Targeting Human Psychology

Attackers exploit trust, urgency, and authority using tailored messages across different platforms.



PAST

Multi-channel Phishing

Module 2.3

Next-Generation Phishing

Example Scenarios

Email & Phone Call

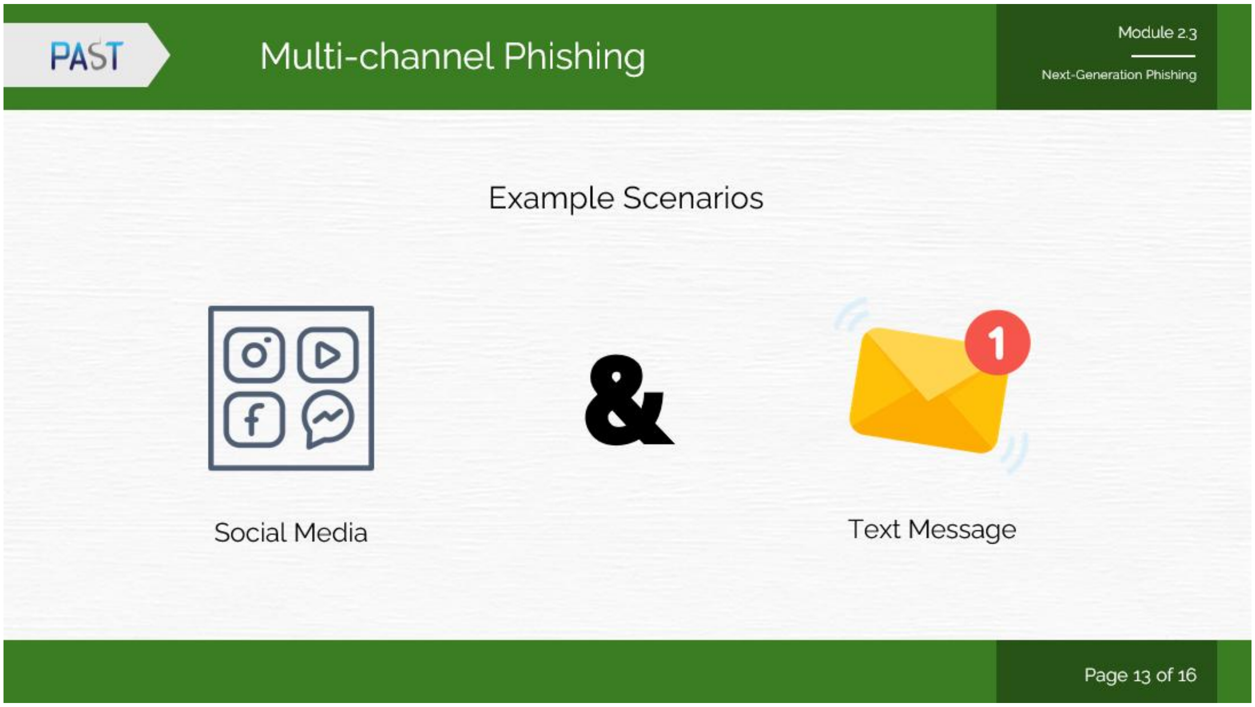
Page 13 of 16

Email and Phone Coordination

The attacker first sends an **urgent email** claiming there is a serious issue with the victim's account (e.g., bank, PayPal, corporate login).

The email provides a **fake customer service number** for the victim to call.

When the victim calls, an attacker impersonates a **support agent** and extracts sensitive information such as passwords, PINs, or financial details.



PAST

Multi-channel Phishing

Module 2.3

Next-Generation Phishing

Example Scenarios

Page 13 of 16

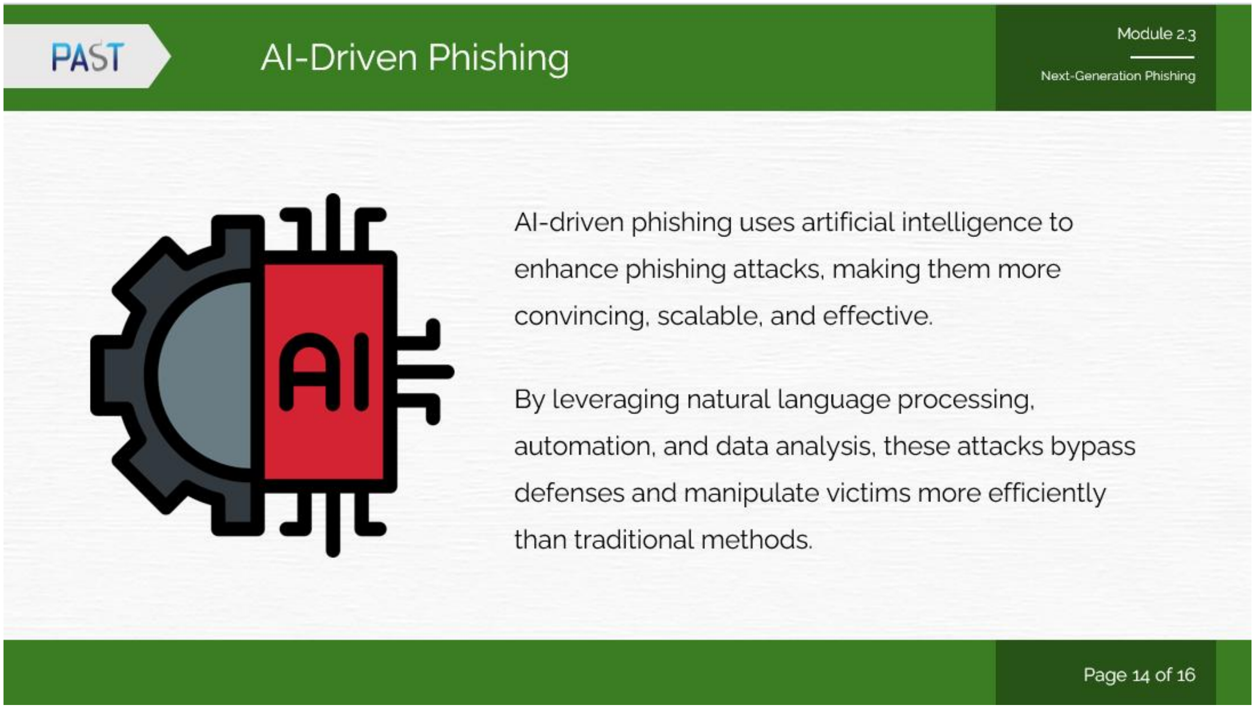
Social Media and Text Messages

Attackers first send a **phishing link** via a social media platform (e.g., Facebook, LinkedIn, Instagram, Twitter).

Shortly after, they send a text message (SMS) **referencing the same link**, reinforcing credibility and urgency.

The victim, seeing multiple notifications about the same message, assumes it’s legitimate and clicks the link, which leads to a fake login page or malware installation.

5. AI-Driven Phishing



PAST

AI-Driven Phishing

Module 2.3

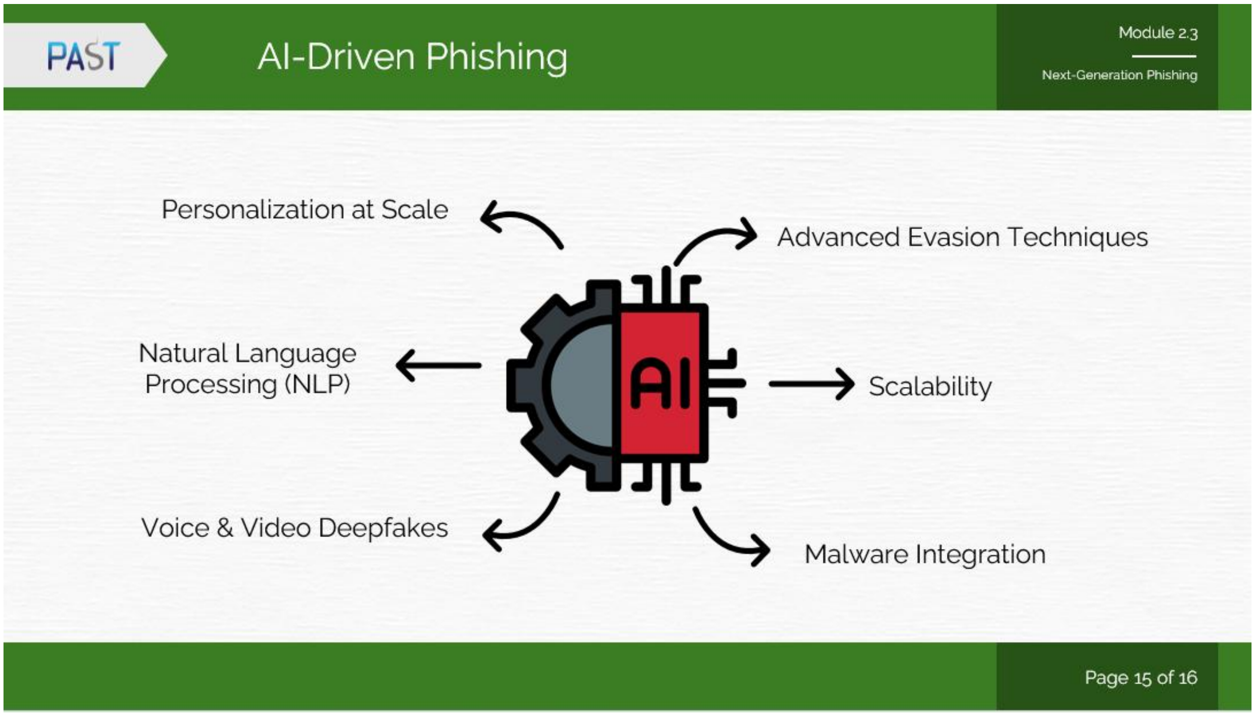
Next-Generation Phishing

AI-driven phishing uses artificial intelligence to enhance phishing attacks, making them more convincing, scalable, and effective.

By leveraging natural language processing, automation, and data analysis, these attacks bypass defenses and manipulate victims more efficiently than traditional methods.

Page 14 of 16

AI-driven phishing represents a new frontier in cybercrime, where artificial intelligence is leveraged to make phishing campaigns more convincing, scalable, and effective. These attacks go beyond traditional methods, exploiting AI's capabilities in natural language processing, automation, and data analysis to bypass defenses and manipulate victims.



PAST

AI-Driven Phishing

Module 2.3

Next-Generation Phishing

Personalization at Scale

Advanced Evasion Techniques

Natural Language Processing (NLP)

Scalability

Voice & Video Deepfakes

Malware Integration

Page 15 of 16

Key Features of AI-Driven Phishing

- Personalization at Scale

Dynamic Content Creation: AI can generate personalized phishing emails based on detailed information about the target (e.g., job role, interests, or recent activities).

Behavior Analysis: AI analyzes publicly available data, such as social media posts, emails, or online behavior, to craft messages that align with the recipient's habits and tone.

Impersonation: AI tools replicate the writing style of specific individuals, making phishing attempts appear more legitimate.

- Natural Language Processing (NLP)

AI-powered phishing emails are linguistically flawless, eliminating common spelling or grammar mistakes that often signal a phishing attempt.

NLP tools allow attackers to craft contextually appropriate messages, enhancing the perceived authenticity.

- Voice and Video Deepfakes

Voice Phishing (Vishing): AI deepfake technology can clone voices with high accuracy using minimal voice samples. Attackers use this to impersonate trusted individuals (e.g., CEOs) in real-time calls.

Video Deepfakes: AI-generated videos can impersonate executives or officials, adding a visual layer of credibility to phishing attempts.

6. Advanced Evasion Techniques

Bypassing Security Filters: AI learns the patterns of email filters and adjusts phishing emails to avoid detection.

Polymorphic Attacks: AI modifies phishing messages in real-time, creating unique variations to evade detection by signature-based security systems.

7. Scalability

AI automates the process of generating and distributing phishing campaigns, enabling attackers to target thousands of victims simultaneously without sacrificing quality or customization.

8. Malware Integration

AI-driven phishing campaigns often integrate malware delivery, such as ransomware or keyloggers, increasing the damage potential.

Examples: Attaching malware-laden documents that adapt based on the victim's operating system or email client.

Summary

Next-generation phishing techniques have become more sophisticated, utilizing advanced technologies and multi-platform strategies to enhance deception. These include Quishing (QR Code Phishing), Business Email Compromise (BEC), Spoofing, Multi-Channel Phishing, and the most advanced form, AI-Driven Phishing. As these threats continue to evolve, individuals and organizations must remain vigilant, strengthen security measures, and stay informed about emerging phishing tactics to effectively mitigate the risks of cyber deception.

- END -