# Phishing Awareness Training

Protect Yourself from Cyber Threats

# What is Phishing?

**Definition:** Phishing is a cybercrime where attackers impersonate legitimate organizations to steal sensitive information such as passwords, credit card numbers, and personal data.

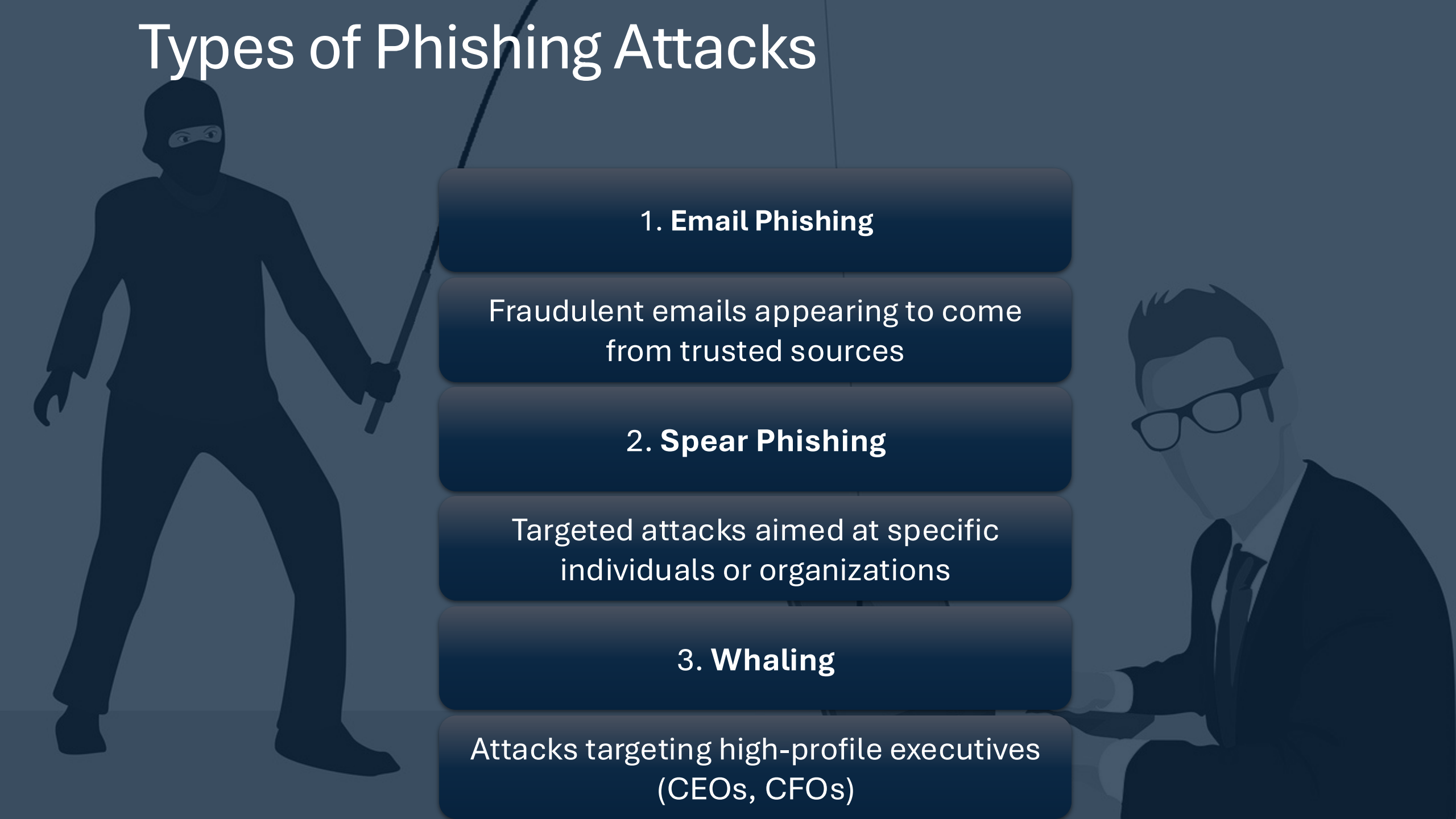
**Key Statistics:**

90% of data breaches start with phishing

1 in 4,200 emails is a phishing attempt

Average cost: $14.8 million per incident

# Types of Phishing Attacks



1. **Email Phishing**

Fraudulent emails appearing to come from trusted sources

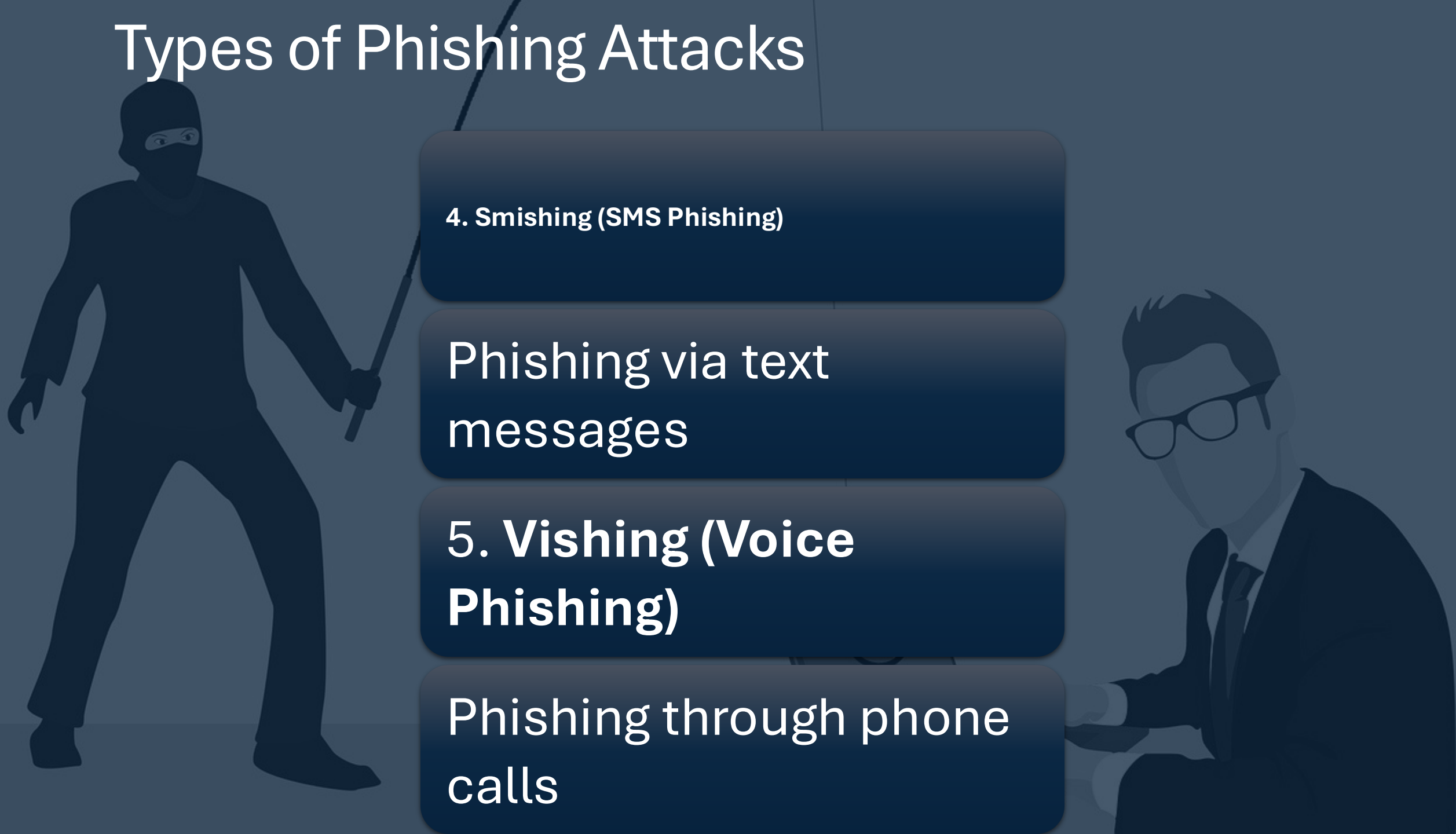
2. **Spear Phishing**

Targeted attacks aimed at specific individuals or organizations

3. **Whaling**

Attacks targeting high-profile executives (CEOs, CFOs)

# Types of Phishing Attacks



**4. Smishing (SMS Phishing)**

Phishing via text messages

5. **Vishing (Voice Phishing)**

Phishing through phone calls

# Red Flags in Phishing Emails

Warning Signs to Watch For:

✗ **Suspicious Sender Address**

- Look beyond the display name
- Check for misspellings: paypa1.com vs paypal.com

✗ **Urgent or Threatening Language**

- "Act now or lose your account!"
- "Immediate action required!"

# Red Flags in Phishing Emails

✗ **Generic Greetings**

- "Dear Customer" instead of your name

✗ **Suspicious Links & Attachments**

- Hover to reveal the real URL

✗ **Poor Grammar & Spelling**

- Professional companies proofread

# Real-World Phishing Example

From: security-alert@bankofamerica-verify.com

Subject: URGENT: Suspicious Activity Detected

Dear Valued Customer,

We have detected unusual activity on your account. For your security, we have temporarily suspended your online banking access.

To restore your account immediately, click below:
[Verify My Account Now]

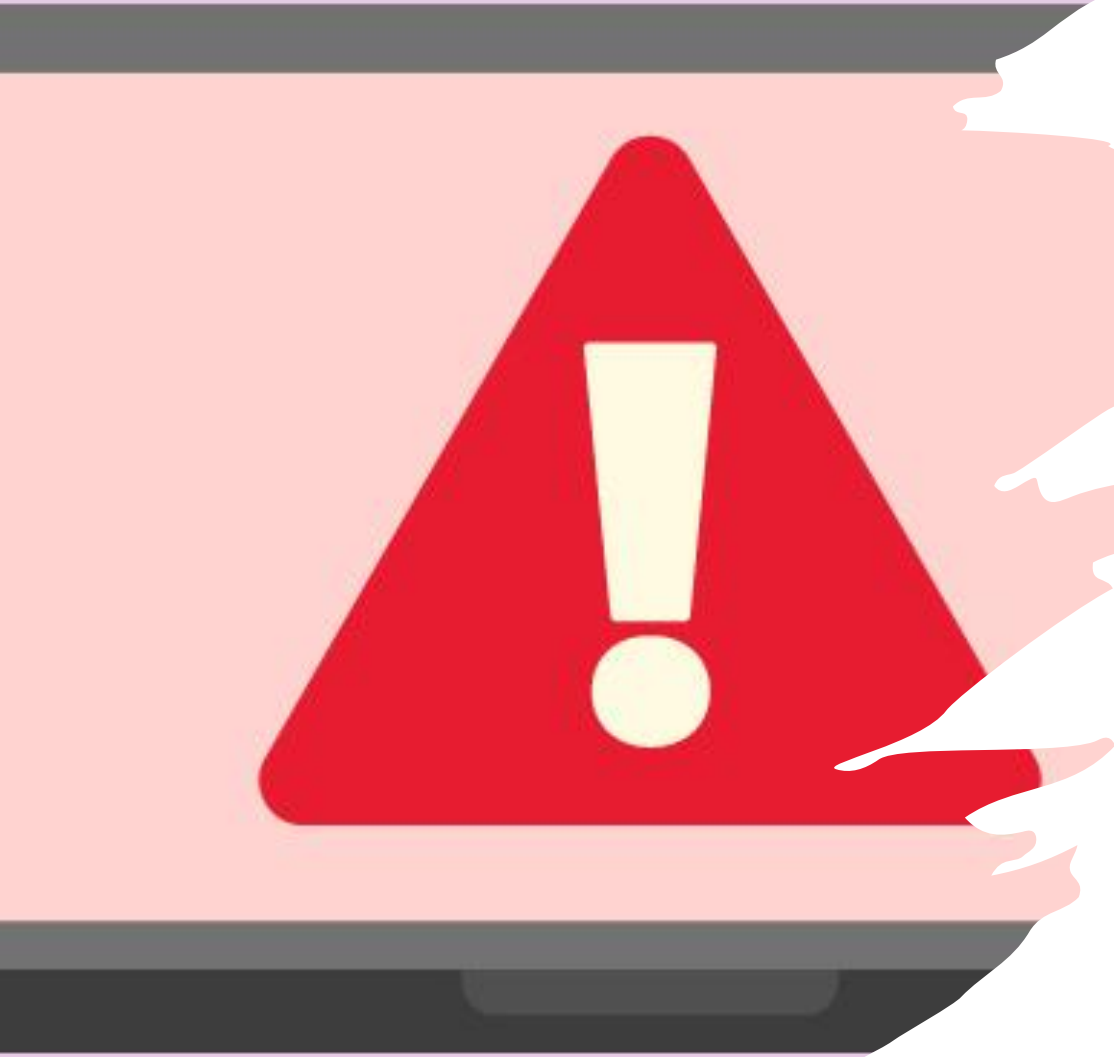
You must complete this within 24 hours or your account will be permanently closed.

Bank of America Security Team

# Red Flags Identified:

- 🚨 Fake domain: "bankofamerica-verify.com"
- 🚨 Generic greeting
- 🚨 Creates urgency and fear
- 🚨 Suspicious link
- 🚨 Threatens account closure

# Spotting Fake Websites



*Legitimate vs. Phishing URLs*

✅ *Legitimate: https://www.paypal.com*

❌ *Phishing: http://paypa1-security.com*

❌ *Phishing: https://paypal.verify-account.net*

- *Visual Clues:*

*Missing HTTPS padlock*

*Misspelled domain names*

*Extra words or hyphens*

*Unusual top-level domains (.xyz, .tk)*

# Social Engineering Tactics

Attackers manipulate human psychology to bypass security

Common Tactics:

🎭 **Pretexting** - Creating fabricated scenarios *Example:* "Hi, this is IT. We need need your password to fix a server issue."

⚡ **Urgency** - Creating time pressure *Example:* "Act in 1 hour or lose your account!"

# Social Engineering Tactics

👔 **Authority** - Impersonating someone in power *Example:* "This is the CEO, process this wire transfer now."

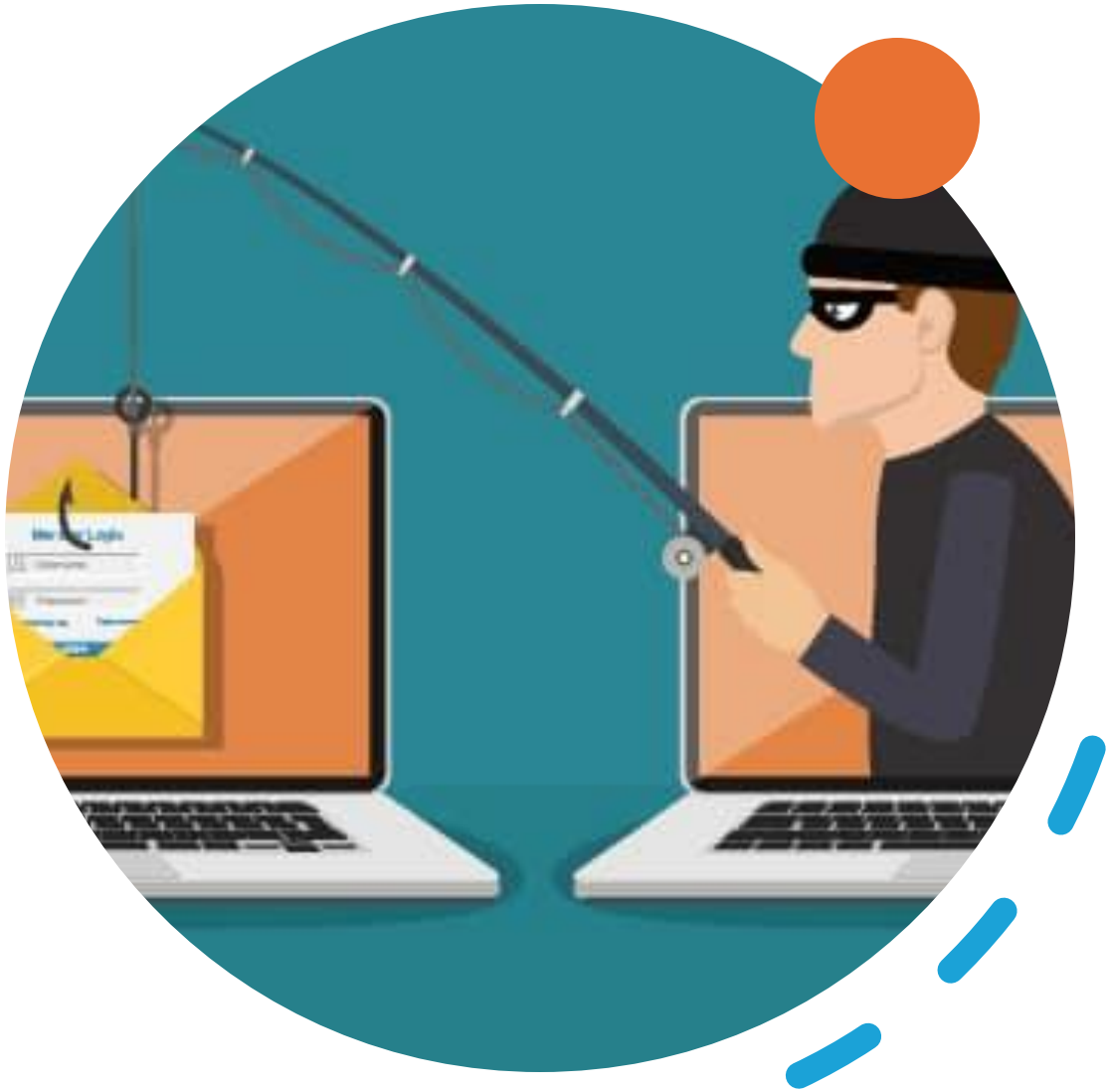
🎁 **Baiting** - Offering enticing rewards *Example:* "You've won a free iPhone!"

😊 **Trust** - Exploiting relationships *Example:* "Hey, it's your colleague from HR..."

😨 **Fear** - Threatening consequences *Example:* "IRS will file charges unless you pay immediately."

# How Phishing Works

1. **Reconnaissance** → Attacker gathers information
2. **Email Creation** → Crafts convincing fake message
3. **Delivery** → Sends to target victims
4. **Victim Action** → Clicks link or opens attachment
5. **Data Theft** → Credentials stolen or malware installed
6. **Exploitation** → Attacker uses stolen information



# Best Practices Verify Before You Trust

✅ DO:

- Hover over links to check the real URL
- Contact companies directly using official channels
- Type URLs directly into your browser
- Verify requests through separate communication
- Check sender email addresses carefully

# Best Practices Verify Before You Trust

## ❌ DON'T:

- Click links in unexpected emails
- Call phone numbers from suspicious emails
- Download attachments from unknown sources
- Share sensitive info via email
- Rush to respond to urgent requests

# Security Measures

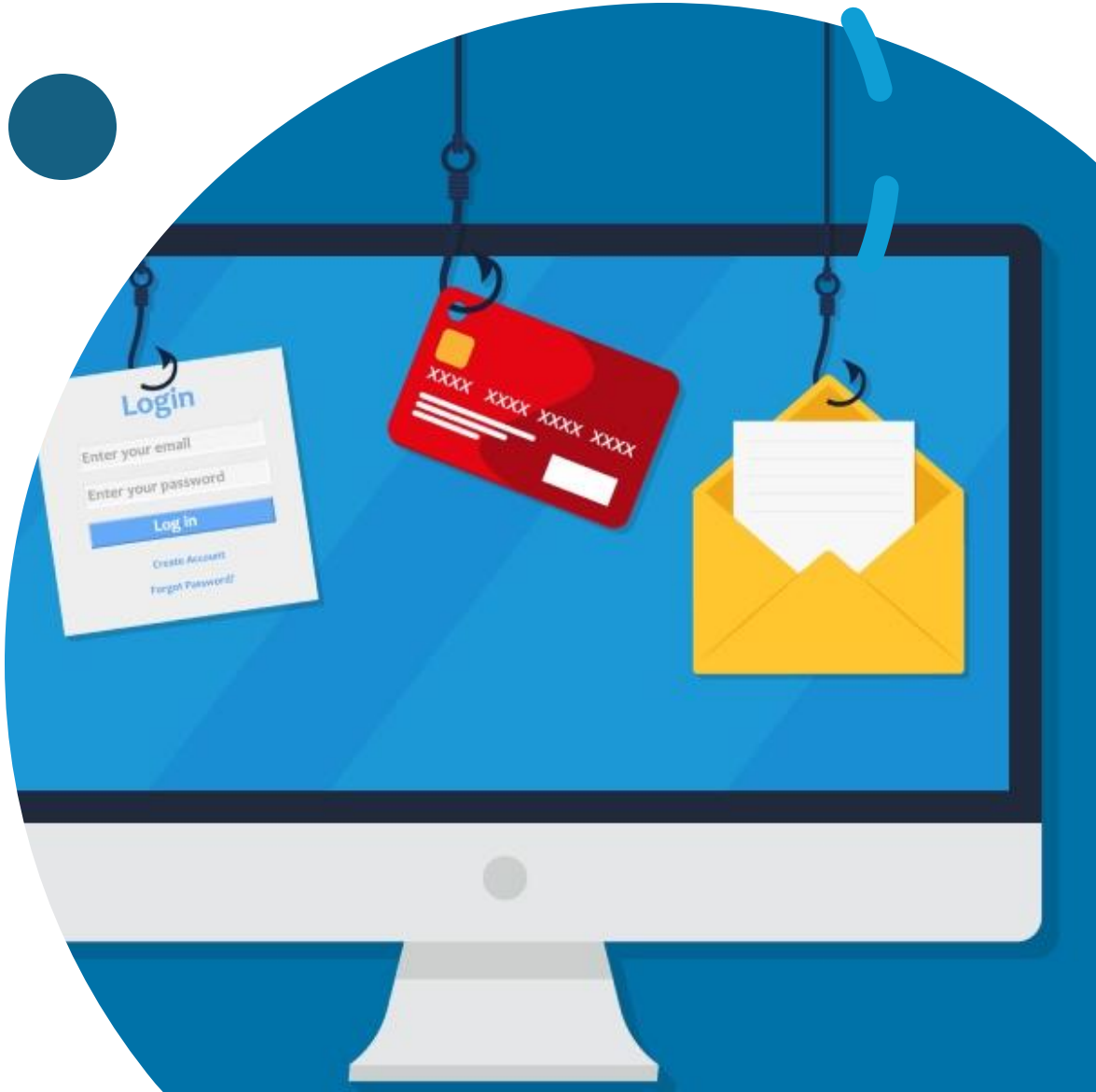
Protect Yourself:

- **Multi-Factor Authentication (MFA)** Add an extra layer of security to your accounts
- **Strong, Unique Passwords** Use a password manager for complex passwords
- **Regular Updates** Keep software and systems up to date
- **Antivirus Software** Install and maintain security software
- **Security Training** Stay informed about latest threats

# What to Do if You're Targeted

Immediate Actions:

- **DON'T PANIC** - Stay calm and assess
- **DON'T CLICK** - Avoid clicking any links
- **VERIFY** - Contact the company directly
- **REPORT** - Alert your IT/security team
- **DELETE** - Remove the suspicious email
- **CHANGE PASSWORDS** - If you clicked, change credentials
- **MONITOR** - Watch for suspicious account activity




Click to Test Your Phishing Knowledge 🎣

- Click to Test Your Phishing Knowledge 🎣