Phishing Awareness Training

What Is Phishing?

Phishing is a cyberattack where attackers trick people into revealing sensitive information such as:

- Passwords
- Credit card numbers
- Bank details
- Company credentials

Attackers usually pretend to be trusted organizations (banks, IT support, delivery services, managers).

Types of Phishing Attacks

- Email Phishing
- Spear Phishing
- Whaling
- Smishing
- Vishing

Email Phishing

Fake emails asking you to click links or open attachments.

Spear Phishing

Targeted attacks aimed at specific individuals or departments.

Whaling

Phishing attacks targeting executives or senior management.

Smishing

Phishing via SMS is done

Vishing

Phishing via phone calls

How to Recognize Phishing Emails and Fake Websites

1. Sender Email Address Inspection

Attackers often spoof or slightly modify email addresses.

Warning Signs:

Misspelled domains

Example: support@paypa1.com instead of support@paypal.com

Extra characters or unusual domains

Example: @paypal-security.co or @secure-paypal.net

Display name looks correct but email address is fake

Tip: Always check the full email address, not just the display name.

2. Urgent, Threatening, or Emotional Language

Phishers create panic to stop you from thinking.

Examples:

“Your account will be locked in 24 hours”

“Immediate action required”

“Suspicious activity detected”

Real companies give notice and don’t pressure you immediately.

3. Generic or Unusual Greetings

Legitimate companies usually address you by name.

🚩 Red Flags:

“Dear Customer”

“Dear User”

Social Engineering Tactics Used by Attackers

Social engineering is the practice of **manipulating people** into giving up confidential information or performing actions that compromise security. Instead of hacking systems, attackers **hack human behavior**.

1. Authority

Attackers pretend to be someone in a position of power.

How It Works:

Impersonating managers, CEOs, IT staff, or government officials

Using job titles, signatures, or logos to appear legitimate

Example:

"This is the IT department. Send your login credentials immediately to avoid account suspension."

Why It Works: People are conditioned to obey authority figures.

2. Urgency

Attackers create time pressure to force quick decisions.

How It Works:

Threats of account suspension

Example:

"Your account will be locked in 30 minutes if you don't respond."

Why It Works: Panic reduces critical thinking.

3. Fear and Intimidation

Attackers scare victims into compliance.

How It Works:

Claiming suspicious activity

Fake security alerts or legal threats

Example:

"We detected illegal activity on your account. Immediate action required."

Why It Works: Fear triggers impulsive reactions.

4. Scarcity

Attackers create a sense of limited availability.

How It Works:

Limited-time deals

Threats of losing access or benefits

Example:

"Only 2 hours left to secure your account."

Why It Works: Scarcity increases perceived value and urgency.

5. Impersonation

Attackers pretend to be someone legitimate.

How It Works:

Using fake email addresses, phone numbers, or websites

Spoofing caller ID or company branding

Example:

"This is your bank's fraud department."

Why It Works: Visual and verbal cues create credibility.

6. Pretexting

Attackers create a believable story to extract information.

How It Works:

Fake scenarios (audits, emergencies, troubleshooting)

Gradual information gathering

Example:

"I'm a vendor doing a system check. Can you confirm your .

Best practices and tips to avoid falling victim in detail

1. Think Before You Click

Attackers rely on quick, emotional reactions.

Best Practices:

Pause and analyze every unexpected message

Be suspicious of urgent or threatening language

Ask yourself: *Was I expecting this message?*

Slowing down is one of the strongest defenses.

2. Verify the Sender's Identity

Never trust an email or message at face value.

Best Practices:

Check the full email address, not just the display name

Verify requests by contacting the sender through a known, official channel

Be cautious of emails from external or unfamiliar domains

Internal requests for sensitive data should always be verified.

3. Never Share Sensitive Information

Legitimate organizations will **never ask** for this data via email or phone.

- **Never Share:**
- Passwords
- One-time passwords (OTP)
- PINs
- Full credit card or bank details
- Security question answers

If someone asks for these, it's a scam.

4. Use Strong, Unique Passwords

Weak or reused passwords increase risk.

Best Practices:

Use long passwords (12–16 characters minimum)

Combine uppercase, lowercase, numbers, and symbols

Never reuse passwords across multiple accounts

Use a reputable password manager

One compromised password should not expose all accounts.

Real-world phishing examples

Example 1. Fake Bank Alert Email
Email Subject: *Urgent: Unusual Activity Detected*
Message Content:
"We detected suspicious activity on your account. Please click the link below to verify your identity or your account will be suspended."
Link: https://secure-bankverify-login.com
Red Flags:
Urgent and threatening language
Suspicious link domain
Request to verify sensitive information
Correct Action: Do not click. Visit the bank's official website manually or call customer support.

Example 2: CEO Fraud (Business Email Compromise)

Email From: “CEO Name” (spoofed address)

Message Content:

“I’m in a meeting. Need you to urgently purchase gift cards and send me the codes.”

Red Flags:

Urgent request

Unusual payment method

Request for secrecy

Authority pressure

Correct Action: Verify through a phone call or internal messaging system.

Example 3: Fake Delivery Notification

Email Subject: *Your Package Is On Hold*

Message Content:

"Your package could not be delivered. Open the attached invoice to reschedule."

Attachment: Delivery_Invoice.zip

Red Flags:

Unexpected attachment

ZIP file (common malware carrier)

No tracking number or sender verification

Correct Action: Delete the email and track deliveries only through official courier websites.

Interactive Quiz (For Engagement)

Quiz 1: Identify the Phishing Sign
Which of the following is a strong phishing indicator?

A. Personalized email greeting
B. Proper grammar
C. Urgent demand for action
D. Known sender

☑ **Correct Answer:** C

Quiz 2: Safe or Unsafe?

You receive an email from IT asking you to confirm your password.

A. Safe

B. Unsafe

✅ **Correct Answer:** B

Explanation: IT will never ask for passwords via email.

Quiz 3: Link Inspection

You hover over a link that shows:

https://paypal.account-security-update.com

Is this legitimate?

A. Yes

B. No

✅ **Correct Answer:** B

Explanation: The real domain is account-security-update.com, not PayPal.

Quiz 4: What Should You Do?

You accidentally clicked a phishing link but didn’t enter information.

A. Ignore it

B. Restart computer

C. Report to IT/security

D. Forward to friends

☑ **Correct Answer:** C

Quiz 5: Choose the Best Response

Your “manager” texts you asking for an OTP code urgently.

A. Share the OTP

B. Ask for confirmation via another channel

C. Ignore company policy

D. Respond immediately

☑ **Correct Answer:** B

Thank You …

By: Rushali Rathod