Stay Safe Online: Phishing Awareness Training

Learn how to recognize phishing attacks
Protect your personal & company data

What is Phishing?

Phishing is a cyberattack where criminals impersonate trusted organizations to steal sensitive information such as passwords and bank details.

Common forms:

Email

SMS (Smishing)

Phone calls (Vishing)

Fake websites

How Phishing Works

1. Attacker sends a fake message

A deceptive message is crafted to look legitimate.

2. Victim clicks a link or attachment

The user is tricked into interacting with the malicious content.

3. Information is stolen or malware installed

Sensitive data is compromised or the device is infected.

Real-World Example: SMS Phishing (Smishing)

Message: Your package is on hold. Click here to confirm delivery.

Red Flags:

- ⚠️ Unknown sender
- ⚠️ Shortened link
- ⚠️ Creates urgency

Real-World Example: Email Phishing

Subject: Your Account Has Been Suspended

Sender: support@paypa1.com

Red Flags:

- 🚨 Fake domain
- 🚨 Urgent language
- 🚨 Link asking for login details

Real-World Example: Fake Website

Website looks like a bank login page

Red Flags:

- ⚠ Misspelled URL
- ⚠ No contact information
- ⚠ Asks for sensitive data

Social Engineering Techniques Used by Attackers

What is Social Engineering?

Social engineering is a manipulation **technique** used by attackers to trick people into giving up confidential information by exploiting human emotions, trust, and behavior rather than technical vulnerabilities.

Common Social Engineering Techniques (Part 1)

1 Urgency

How it works: Attackers pressure victims to act quickly before thinking.

Why it works: People panic and respond without verifying.

Defense tip: Pause and verify before taking any action.

2 Fear and Intimidation

How it works: Attackers scare victims using threats.

Why it works: Fear reduces rational thinking.

Defense tip: Legitimate organizations don't threaten users via email or SMS.

3 Impersonation

How it works: Attackers pretend to be trusted individuals or organizations.

Why it works: People naturally trust authority figures.

Defense tip: Always verify the sender using official contact channels.

Common Social Engineering Techniques (Part 2)

4 Trust and Familiarity

How it works: Attackers build trust by pretending to know you.

Why it works: People are more likely to help someone they "know."
Defense tip: Verify identities—even if the person seems familiar.

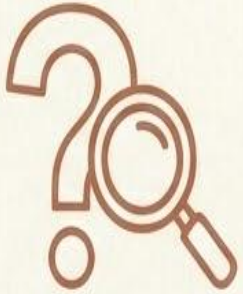
5 Greed and Rewards

How it works: Attackers lure victims with benefits.

Why it works: People like free rewards and quick gains.

Defense tip: If it sounds too good to be true, it probably is.

6 Curiosity



How it works: Attackers exploit human curiosity.

Why it works: People want to know what others are saying.

Defense tip: Be cautious of unexpected links or files.

Common Social Engineering Techniques (Part 3)

7 Authority

How it works: Attackers pretend to be someone in power.

Why it works: People hesitate to question authority.

Defense tip: Follow proper verification procedures—always.

8 Reciprocity

How it works: Attackers do something small to make you feel obligated.

Why it works: People feel pressured to return favors.

Defense tip: Never exchange sensitive information for favors.

9 Scarcity

How it works: Attackers create a sense of limited opportunity.

Why it works: Fear of missing out (FOMO).

Defense tip: Take time to verify before responding.

Recognizing Phishing Emails

Key indicators to look out for:

- ⚠ Suspicious sender address
- ⚠ Generic greetings
- ⚠ Spelling or grammar errors
- ⚠ Unexpected attachments
- ⚠ Urgent requests

Best Practices

- Do not click suspicious links
- Verify requests separately
- Use multi-factor authentication
- Keep software updated
- Report phishing immediately

Question 1: Spot the Phishing Email

You receive this email:

From: support@paypa1.com
Subject: Urgent – Account Verification Required
"Your PayPal account will be suspended in 24 hours. Click the link below to verify your identity."

What should you do?

A. Click the link immediately
B. Reply to the email with your details
C. Delete the email and ignore
D. Report the email and verify through the official PayPal website

✅ **Correct Answer: D**
Explanation:
The sender's email address is fake (paypa1.com). The email creates urgency and asks for sensitive information.

Question 2: SMS (Smishing) Attack

Message received:

"Your delivery is on hold. Confirm your address now: bit.ly/9kJX2"

What is the safest action?

A. Click the link
B. Reply "STOP"
✅ C. Ignore and check delivery status on the official courier website
D. Forward the message to friends

✅ **Correct Answer: C**
Explanation:
Shortened links and urgent delivery messages are common smishing tactics.

Question 3: True or False

A website with HTTPS and a padlock icon is always safe.

- [ ] A. True
- [x] B. False

✅ **Correct Answer: B (False)**
Explanation:
Attackers can also use HTTPS. Always check the full domain name.

Question 4: CEO Fraud Scenario

You receive a message:

"Hi, this is the CEO. I need you to urgently buy gift cards and send me the codes. Keep this confidential."

What social engineering techniques are being used? (Select TWO)

✅ A. Authority
B. Curiosity
✅ C. Urgency
D. Familiarity

✅ **Correct Answers: A & C**
Explanation:
The attacker pretends to be an authority figure and pressures you to act quickly.

Question 5: Fake Website Login

You click a link and land on a website that looks like your company's login page, but the URL is:
www.company-secure-login.net

What is the red flag?

A. The page looks professional
✅ B. The URL does not match the official domain
C. The page loads fast
D. It asks for your username

✅ **Correct Answer: B**
Explanation:
Attackers use look-alike domains to trick users.

Summary

- Phishing attacks rely on deception
- Always verify before you click
- Your awareness is your best defense