Phishing Awareness Training

~ By Pinak Raval

Why This Training Matters

91%

Cyberattacks

Start with phishing emails targeting employees like you

$12K

Average Cost

Per successful phishing attack on small businesses

15%

Success Rate

Of employees click malicious links in phishing emails

Every employee is a potential target and your first line of defense against cybercriminals.

What is Phishing?

The Definition

Phishing is a cybercrime where attackers impersonate legitimate organizations to steal sensitive information like passwords, credit card numbers, or personal data.

Think of it as digital fraud - criminals casting a wide net to catch unsuspecting victims.

Common Targets

- Login credentials
- Financial information
- Personal identification
- Company data access
- System permissions

Recognizing Phishing Emails

1

Suspicious Sender

Check for misspelled domains, generic greetings, or unexpected senders claiming urgent action needed.

2

Urgent Language

Watch for phrases like "Act now!" "Verify immediately!" or threats of account suspension.

3

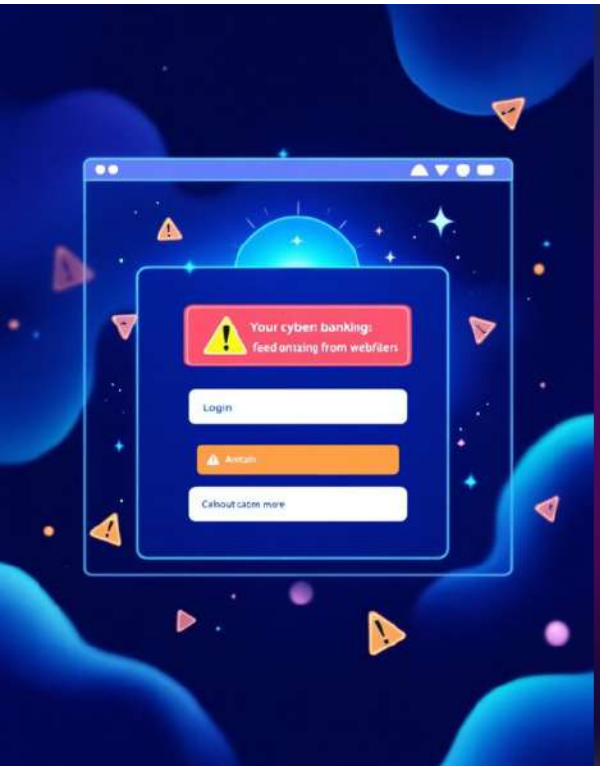
Suspicious Links

Hover over links to preview destinations. Look for shortened URLs or domains that don't match.

4

Poor Quality

Notice spelling errors, grammar mistakes, or unprofessional formatting and design.



Fake Website Red Flags

URL Inconsistencies

Look for subtle misspellings in web addresses (like "amazom.com" instead of "amazon.com")

Missing Security Indicators

Check for HTTPS (the lock icon) and valid security certificates before entering sensitive data

Design Inconsistencies

Notice outdated layouts, broken images, or design elements that don't match the legitimate site

Social Engineering Tactics

Authority

Impersonating executives, IT support, or government agencies to create pressure and bypass skepticism.

Urgency

Creating artificial time pressure to force quick decisions without proper verification.

Fear

Threatening account closures, legal action, or security breaches to panic victims into compliance.

Trust

Using familiar branding, personal information, or mutual connections to appear legitimate.

Real-World Example: The Executive Scam

> *"This is Sarah from the CEO's office. We need you to process an urgent wire transfer for a confidential acquisition. Please send $50,000 to this account immediately and don't discuss this with anyone."*

Red Flags Present:

- Urgent financial request
- Requests secrecy
- Bypasses normal procedures
- Uses authority pressure

Proper Response:

- Verify through official channels
- Call the CEO directly
- Follow company protocols
- Report to IT security

Best Practices: Your Defense Strategy

01

Stop and Think

Pause before clicking links or downloading attachments. Take time to evaluate the request carefully.

02

Verify the Source

Contact the sender through official channels to confirm legitimacy before taking any action.

03

Use Multi-Factor Authentication

Enable 2FA on all accounts to add an extra layer of security even if passwords are compromised.

04

Keep Software Updated

Install security updates promptly and use reputable antivirus software with real-time protection.

05

Report Suspicious Activity

Forward phishing attempts to IT security and delete the original message immediately.

Quick Knowledge Check

Scenario 1

You receive an email from "IT Support" asking for your password to "update security settings." What do you do?

Answer: Never share passwords via email. Contact IT directly to verify.

Scenario 2

A link in an email shows "amazon.com" but when you hover, it displays "amazorn-security.net." Is this safe?

Answer: No! The actual destination doesn't match the display text.

Remember: You Are Our Best Defense

Stay Vigilant

Trust your instincts. If something feels suspicious, it probably is. Take time to verify before acting.

Ask for Help

When in doubt, reach out to IT security or your supervisor. It's better to ask than become a victim.

Keep Learning

Cyber threats evolve constantly. Stay informed about new phishing techniques and security updates.

Questions? Contact IT Security at security@company.com or extension 2847.