# Phishing Awareness Training Module

Welcome to this interactive online module on phishing awareness. This training is designed to help you understand phishing attacks, recognize them, and protect yourself and your organization. We'll cover key topics with explanations, examples, visuals, and quizzes to test your knowledge.

Navigate through the sections below. At the end of each quiz, check the answers provided.

## Section 1: What is Phishing?

Phishing is a cyber attack where attackers impersonate trustworthy entities to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal data. It often occurs via email, but can also happen through SMS (smishing), phone calls (vishing), or fake websites.

Common goals:

- Steal login credentials
- Install malware
- Commit financial fraud

Phishing exploits human psychology rather than technical vulnerabilities.

## Section 2: Recognizing Phishing Emails

Phishing emails often look legitimate but contain red flags. Here's how to spot them:

### Key Signs:

- **Unexpected or Urgent Requests**: Emails demanding immediate action, like "Your account will be suspended unless you click here."
- **Suspicious Sender**: Check the email address – it might mimic a real one (e.g., support@paypa1.com instead of support@paypal.com).
- **Generic Greetings**: "Dear User" instead of your name.
- **Spelling/Grammar Errors**: Poor language can indicate a scam.
- **Suspicious Links or Attachments**: Hover over links to see the real URL; avoid unknown attachments.
- **Requests for Sensitive Info**: Legitimate companies rarely ask for passwords via email.

## Examples:

Here's an example of a phishing email pretending to be from a university about password expiration.

Another common one is a fake PayPal alert about account limitations.

GoToMeeting Phishing Email Example | Hook Security

And a Citibank impersonation claiming suspicious activity.

Most Common Phishing Email Examples - Keepnet

## Section 3: Recognizing Fake Websites

Fake websites are designed to mimic real ones to capture your data. They often link from phishing emails.

### Key Signs:

- **URL Mismatches**: Look for typosquatting (e.g., pay-pal.com instead of paypal.com). Check for HTTPS and a valid certificate.
- **Poor Design or Errors**: Subtle differences in logos, fonts, or layout.
- **Unexpected Pop-ups or Requests**: Asking for info that doesn't make sense.
- **No Contact Info**: Legitimate sites have clear ways to reach them.
- **Browser Warnings**: Modern browsers flag suspicious sites.

### Examples:

Compare a real vs. fake PayPal login page – note the URL difference.

5 Recent Examples of Fake Websites | Memcyco

A fake government site offering COVID-19 financial support, asking for personal details.

COVID-19 Phishing Templates to Fake Government Website | Proofpoint US

## Section 4: Social Engineering Tactics Used by Attackers

Social engineering manipulates people into divulging information. Phishing is a subset, but tactics include:

- **Pretexting**: Creating a fabricated scenario to obtain info (e.g., pretending to be IT support).
- **Baiting**: Offering something enticing, like a free download infected with malware.
- **Tailgating**: Following someone into a secure area (physical social engineering).
- **Quid Pro Quo**: Offering help in exchange for info (e.g., "I'll fix your computer if you give me access").
- **Authority Impersonation**: Posing as a boss or law enforcement to pressure compliance.
- **Urgency and Fear**: Creating panic to bypass rational thinking.

Attackers research targets via social media for spear-phishing (targeted attacks) or whaling (high-profile targets).

## Section 5: Best Practices and Tips to Avoid Phishing

Protect yourself with these habits:

- **Verify Sources**: Contact the sender through official channels, not the email's links.
- **Use Security Tools**: Enable two-factor authentication (2FA), use antivirus software, and email filters.
- **Be Skeptical**: If it seems too good to be true or overly urgent, pause and check.
- **Educate and Report**: Share knowledge with colleagues; report suspicious emails to IT.
- **Regular Updates**: Keep software patched to close vulnerabilities.
- **Password Management**: Use unique, strong passwords and a manager.
- **Training**: Participate in simulations to practice spotting phishing.

Tip: Hover over links on desktop or long-press on mobile to preview URLs.

## Section 6: Real-World Examples

Phishing has caused massive damage. Here are notable cases:

- **Google and Facebook (2013-2015)**: A scammer impersonated a vendor, sending fake invoices that tricked the companies into wiring over $100 million.
- **Colonial Pipeline (2021)**: A phishing attack led to ransomware, shutting down fuel supply and costing millions in ransom and disruptions.
- **Sony Pictures (2014)**: Phishing emails stole credentials, leading to data leaks of emails, films, and personal info.
- **Ubiquiti Networks (2015)**: Impersonating executives, attackers tricked transfers of $46 million.
- **Recent Campus Scams (2025-2026)**: Examples include fake scholarship schemes and domain listing scams targeting universities.

These show how even large organizations fall victim – vigilance is key.

## Section 7: Interactive Quizzes

Test your knowledge! Answer the questions, then scroll to see the correct answers.

### Quiz 1: Spot the Phishing Email

Which is a red flag in an email?
A) Personalized greeting with your name
B) Urgent demand to update password via link
C) Clear sender from official domain
D) Attached file from known contact

### Quiz 2: Fake Website Detection

A website URL is "secure-bank.com/login" but the real bank is "banksecure.com". This is likely:

A) Legitimate

B) Typosquatting phishing

C) A secure redirect

D) Browser error

## Quiz 3: Social Engineering Tactic

An email from your "boss" asking for gift card codes urgently is an example of:

A) Pretexting

B) Authority impersonation

C) Baiting

D) Quid pro quo

## Quiz 4: Best Practice

What should you do if you receive a suspicious email?

A) Click the link to check

B) Reply asking for more info

C) Report to IT and delete

D) Forward to friends for opinion

**Answers:** (Highlight or scroll to reveal)

Quiz 1: B

Quiz 2: B

Quiz 3: B

Quiz 4: C

Congratulations on completing the module! Remember, staying alert is your best defense against phishing. If you have questions, consult your organization's security team.