Phishing Awareness Training

Cyber Security Internship - CodeAlpha

Prepared by: Miti Bhanushali

What Exactly is Phishing?

Phishing is a deceptive cyber attack where malicious actors impersonate a trusted entity or organisation to steal sensitive personal or financial information.

This typically involves tricking users into revealing crucial data like passwords, bank account details, credit card numbers, or One-Time Passwords (OTPs).

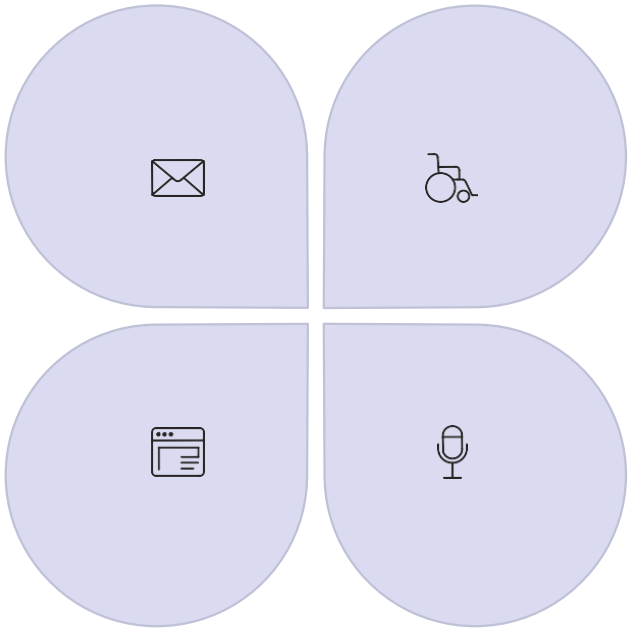
The Many Forms of Phishing Attacks

Email Phishing

The most common type, using mass emails to impersonate legitimate companies.

Fake Websites

Creating highly convincing but fraudulent web portals to harvest credentials.



SMS Phishing (Smishing)

Attacks delivered via deceptive text messages, often containing urgent links.

Voice Phishing (Vishing)

Using fraudulent phone calls to manipulate victims into sharing data.

Attackers utilise various vectors to deploy their traps, making it essential to be vigilant across all communication channels.

Understanding the Phishing Attack Lifecycle

01

1. Initial Contact

The attacker dispatches a fake message, email, or communication, often containing a fabricated sense of urgency or threat.

02

2. Malicious Click

The unsuspecting user is deceived into clicking a malicious link or downloading a contaminated attachment embedded in the message.

03

3. Deceptive Interface

The user is directed to a fraudulent website that is meticulously designed to look exactly like the authentic login page or portal.

04

4. Data Compromise

The user, believing the site is genuine, proceeds to input their sensitive personal information or credentials.

05

5. Data Theft

The attacker successfully captures and steals the entered data, using it for identity theft, financial fraud, or further cyber infiltration.

Detecting a Phishing Email

Unknown Sender Address

The 'From' email address does not match the supposed sender's official domain.

Urgency and Threats

Messages demanding immediate action, threatening account suspension, or promising sudden financial gains.

Linguistic Errors

The presence of glaring spelling or grammar mistakes, which are typically absent in professional corporate communications.

Suspicious Hyperlinks

Links that point to a different URL than the text indicates, or attachments that look unusual.

Fake Email Domains

The domain is subtly misspelled (e.g., amaz0n.com instead of amazon.com) or uses a non-standard extension.

Key Indicators of Fake or Spoofed Websites

Even if a website looks identical to a trusted one, scrutinise the details before submitting any information.

Unusual URL Structure

The web address contains odd characters, extra words, or deviates significantly from the official domain name.

Missing HTTPS Security

The address starts with "http://" instead of the secure "https://", and the padlock icon is absent in the browser bar.

Subpar Design Quality

The site features low-resolution images, inconsistent branding, or general poor functionality compared to the real portal.

Overly Sensitive Data Requests

The site immediately demands excessive personal or financial details that a legitimate login page would not typically require.

Case Study: Anatomy of a Bank Phishing Scam

The Scenario

A user receives an email, seemingly from their trusted bank, claiming their account has been temporarily locked due to unusual activity.

> "Action Required: Your account is restricted. Click here immediately to verify your details and prevent permanent closure."

The Hook

The embedded link directs the user to a cleverly disguised phishing site that mimics the bank's actual login page.

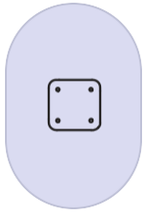
The Outcome

Upon entering their username and password, the credentials are instantly transmitted to the attacker, leading to account takeover and potential financial loss.

> Always navigate to your bank's website directly by typing the URL, never by clicking links in suspicious emails.

Essential Best Practices for Cyber Safety

Proactive security measures are your first line of defense against sophisticated phishing attempts.

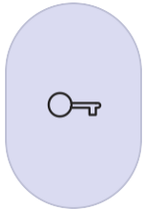


Verify Before You Click

Always hover your mouse over a link to view the actual destination URL before clicking it.

Enable 2FA/MFA

Implement Two-Factor Authentication (2FA) on all critical accounts to add an essential security layer.



Strong Passwords

Use unique, complex passwords for different services and consider using a reputable password manager.

Never Share OTPs

One-Time Passwords are confidential and should never be shared with anyone over email, text, or phone call.

Scrutinise Sender

Meticulously check the full email address and domain of the sender, especially for financial or HR-related messages.

Quick Check: Are You Phishing-Aware?

1 Is it safe to click a hyperlink from an unknown sender's email if it looks like a legitimate company's link?

Answer: No. Always verify the link's true destination by hovering over it, or manually type the website address.

2 Do legitimate banks or corporations ever ask for your OTP or full password via email or text message?

Answer: Never. Any request for confidential verification codes or full passwords is a definite red flag.

3 Should you trust an urgent or threatening email that demands immediate action to avoid an account shutdown?

Answer: Treat all urgent, unexpected communications with extreme suspicion. These are classic manipulation tactics used in phishing.

Conclusion: Your Role in Cyber Defense

Vigilance is Power

While phishing attacks are becoming increasingly sophisticated and numerous, user awareness remains the single most effective defense against them.

- Always stay alert and look for warning signs.
- Verify the source of any communication before acting on it.
- Protect your personal and corporate information rigorously.

Thank you. Stay safe online!