

Phishing Awareness Training

Understanding, Recognizing, and Preventing Cyber Threats



What is Phishing?

Phishing is a cyberattack that uses deceptive communications to trick individuals into revealing sensitive information, such as login credentials, financial data, or personal details.

Deceptive Tactics

Attackers use fraudulent emails, websites, and messages designed to look legitimate.

Targeted Information

The primary goal is to steal login credentials, financial data, and other personal information.

Growing Threat

Over 90% of data breaches begin with phishing. Attacks are increasingly sophisticated, often leveraging AI-crafted scams and deepfakes.

Recognizing Phishing Emails: Key Signs

- **Generic Greetings:** *"Dear Customer"* instead of your name.
- **Suspicious Sender Addresses:** Mismatched or unusual email domains.
- **Urgent/Alarming Language:** Threats of account suspension or immediate action required.
- **Unexpected Requests:** Asking for personal or financial information without context.
- **Poor Grammar/Spelling:** Though less common with AI-generated scams, still a red flag.

Identifying Fake Websites



URL Anomalies

Look for subtle misspellings (e.g., "goooogle.com") or unusual domain extensions (.xyz, .biz).



Security Certificates

Check for "HTTPS" in the URL and a valid padlock icon. Lack of these or an invalid certificate is a warning.



Hover Over Links

Before clicking, hover your mouse over links to preview the actual destination URL. If it differs from the displayed text, be wary.



Mimicry

Fake sites often perfectly mimic trusted brands and logos. Always double-check the URL.

Social Engineering Tactics Used by Attackers

Attackers exploit human psychology and trust to manipulate victims into taking specific actions.

Urgency & Fear

Creating a sense of immediate crisis to bypass rational thought, prompting quick, unverified actions.

Impersonation

Pretending to be trusted contacts, IT support, or executives (e.g., "CEO fraud") to gain credibility.

Spear Phishing

Highly personalized attacks based on extensive research about the target, making them seem highly legitimate.

Vishing & Smishing

Using phone calls (vishing) or SMS messages (smishing) as alternative vectors to deliver deceptive messages.

Best Practices to Avoid Phishing Attacks



- **Think Before You Click:** Never click links or open attachments from unknown or suspicious sources.
- **Verify Requests:** Always verify unexpected requests for information by contacting the sender through a separate, known communication channel (e.g., calling them directly, not replying to the email).
- **Enable MFA:** Use multi-factor authentication (MFA) on all accounts whenever possible; it adds an extra layer of security.
- **Keep Software Updated:** Ensure your operating system, web browser, and security software are updated automatically to patch vulnerabilities.

Reporting and Responding to Phishing Attempts

1

Report Immediately

Report suspicious emails or messages to your IT or security team. Most organizations have a dedicated method for this.

2

Do Not Forward

Do not forward phishing emails to others, as this can spread the malicious content or accidental clicks.

3

Disconnect Devices

If you suspect your device has been compromised, disconnect it from the network immediately to prevent further damage.

4

Follow Protocols

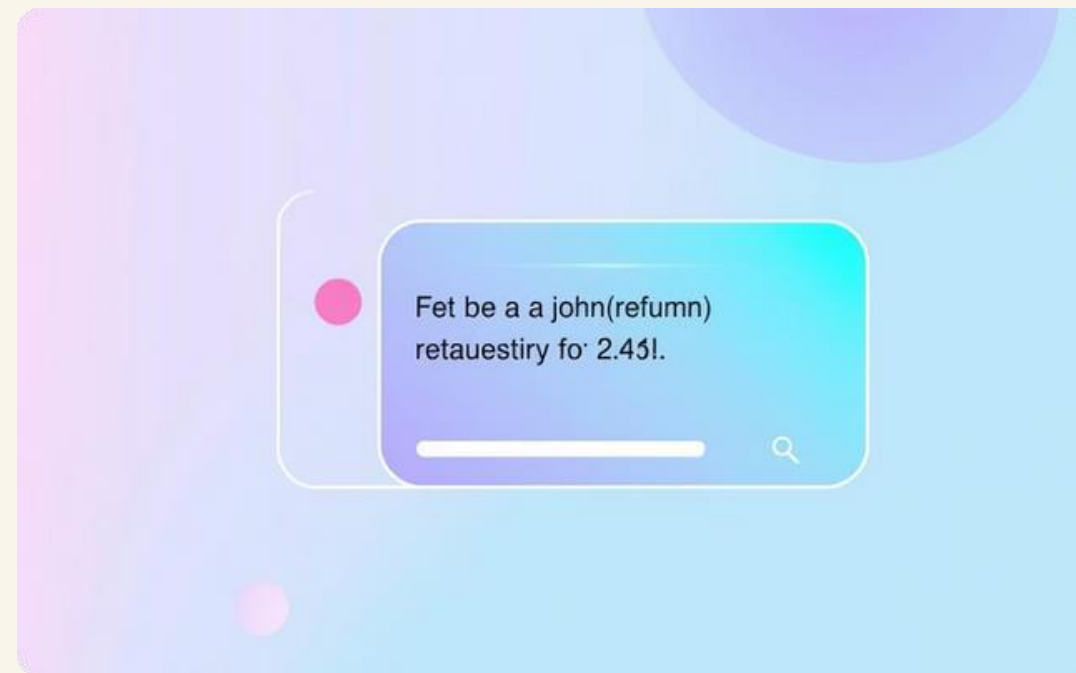
Adhere to your organization's incident response protocols. Your quick action can mitigate significant risks.

Real-World Phishing Examples



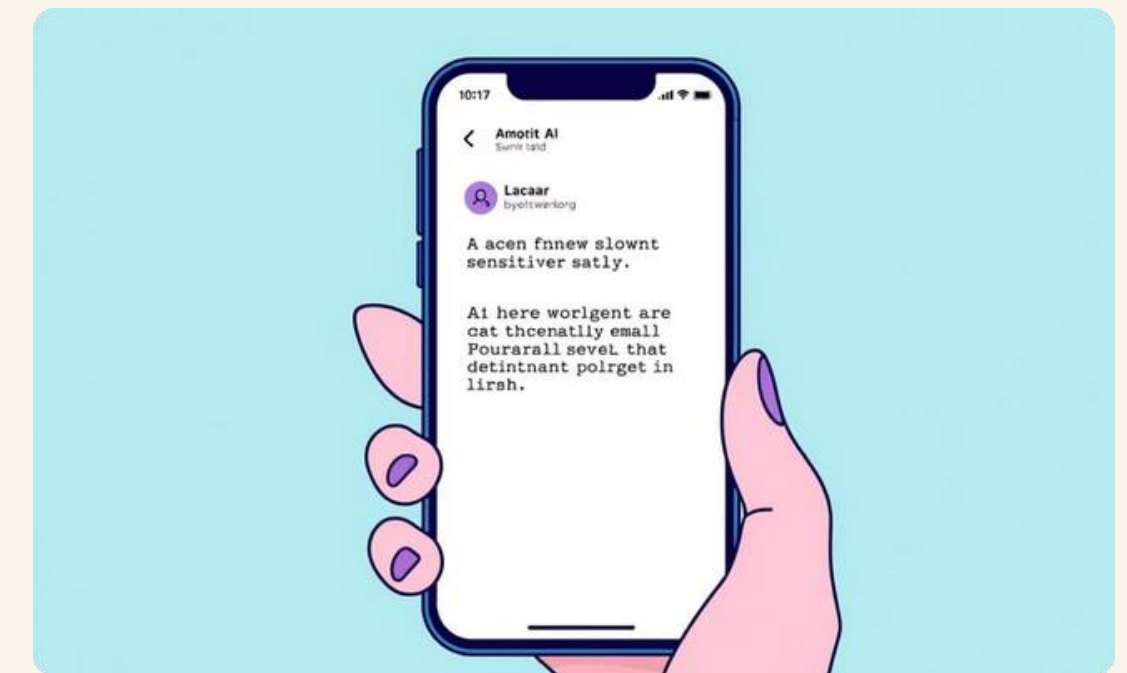
- Fake Bank Alert

An email pretending to be from your bank asking you to click a link to "update your account information" due to suspicious activity.



- SMS Scam (Smishing)

A text message offering a fake government refund or prize, asking you to click a link to claim it.



- AI-Generated Impersonation

An email mimicking a coworker's style, requesting urgent action or sensitive data, generated with advanced AI.

Interactive Quiz: Spot the Phishing Email

Below are three sample emails. Can you identify which one is a phishing attempt and why?

Email A

Subject: Your Order Shipped!

Body: "Dear [Your Name], Your recent order #12345 has shipped. Track it here: track.legit-store.com"

Clue: Personalized greeting, legitimate-looking URL.

Email B

Subject: Account Suspension Alert!

Body: "Dear User, Your account will be suspended in 24 hours if you do not verify your details immediately. Click here: verify-account.co"


Clue: Generic greeting, urgent tone, suspicious URL.

Email C

Subject: Meeting Reminder

Body: "Hi John, Just a reminder for our meeting tomorrow at 10 AM. See the agenda attached. [Attachment: agenda.pdf]"

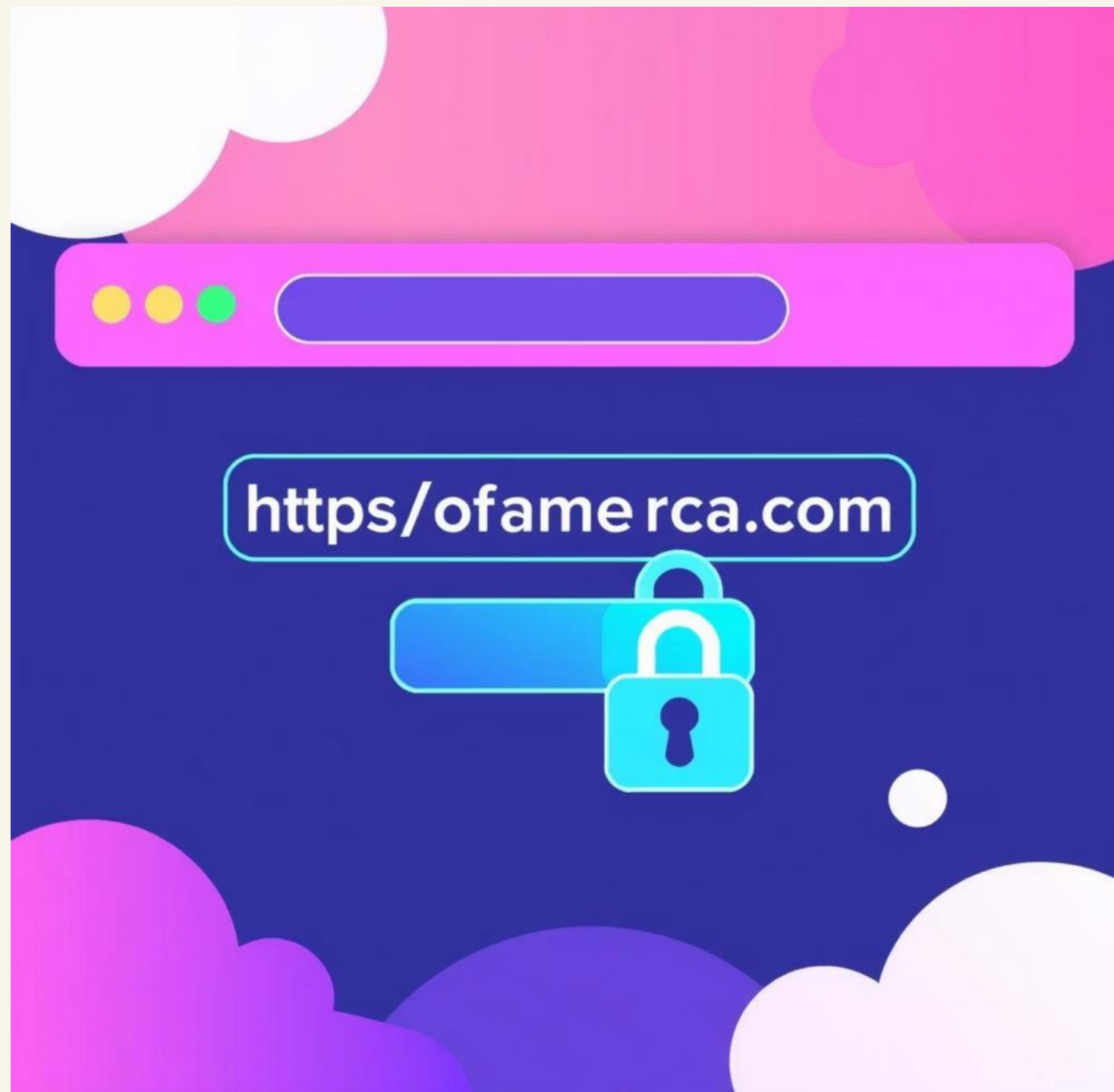
Clue: Personalized, expected content, common attachment type.

 **Answer:** Email B is a phishing attempt due to the generic greeting, urgent language, and suspicious domain "verify-account.co".

Interactive Quiz: Identify the Fake Website

Examine these two login page screenshots. Which one is fake and what are the suspicious elements?

Website A



Website B

