Phishing Attacks: Awareness & Prevention Module

-By
DARSHWANA ALLAM

WHAT IS PHISHING?

Phishing is a type of cyberattack where attackers:

- Pretend to be trusted entities (banks, companies, friends)
- Trick users into sharing sensitive data
- Use emails, messages, calls, or fake websites

Common targets:

- Passwords
- OTPs
- Credit/debit card details
- Personal information

INTRODUCTION TO PHISHING ATTACKS

Phishing is one of the most common and dangerous cyberattacks today. It is a fraudulent attempt by attackers to trick users into revealing sensitive information such as passwords, OTPs, bank details, or personal data. Attackers usually pretend to be trusted organizations like banks, government agencies, companies, or even friends. Phishing attacks can happen through emails, SMS, phone calls, social media, and fake websites. The main goal is to exploit human trust rather than technical weaknesses.

WHY PHISHING IS A SERIOUS CYBER THREAT?

Phishing is a major threat because it is easy to execute and highly effective. A single phishing email can cause financial loss, identity theft, or complete account takeover. For organizations, phishing can lead to data breaches, loss of customer trust, and legal consequences. As digital banking, online shopping, and remote work increase, phishing attacks continue to grow rapidly.

TYPES OF PHISHING ATTACKS:

- **Email Phishing** – Fake emails pretending to be legitimate
- **Spear Phishing** – Targeted attacks on specific individuals
- **Smishing** – Phishing via SMS/text messages
- **Vishing** – Phishing via phone calls
- **Clone Phishing** – Legitimate email copied and modified

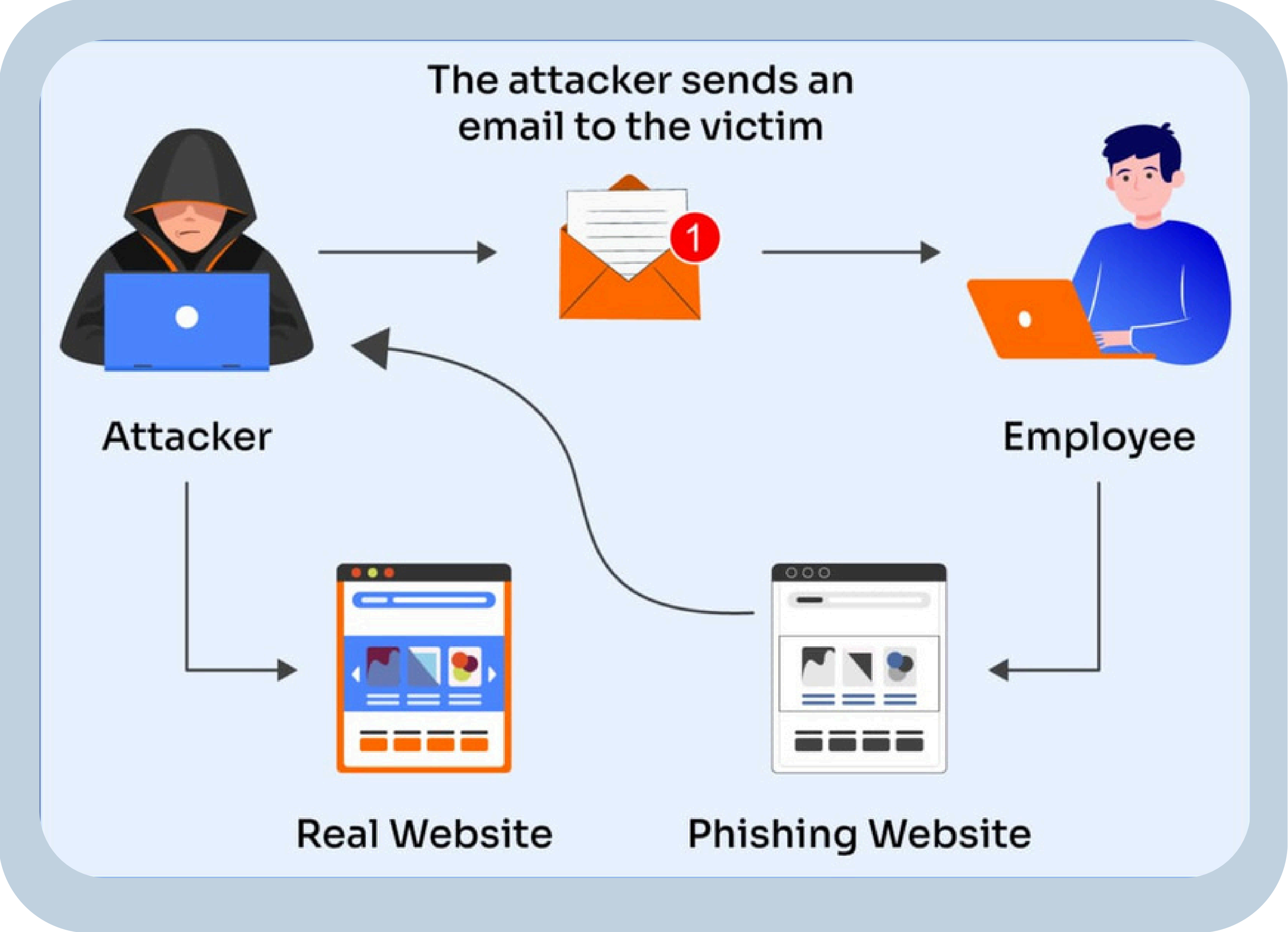
HOW TO IDENTIFY PHISHING EMAILS

- Phishing emails often contain urgent messages such as account suspension warnings or security alerts. They may use generic greetings like "Dear User" instead of your name. The sender’s email address may look similar to a real one but contains small changes. These emails frequently include suspicious links or attachments and may contain spelling or grammar mistakes. Legitimate companies never ask for passwords or OTPs through email.

HOW TO IDENTIFY FAKE WEBSITES

- Fake websites are designed to look almost identical to real websites. They often use slightly misspelled domain names, lack proper HTTPS security, or show certificate warnings. These sites may ask for unnecessary personal or financial information. Attackers commonly create fake login pages for banks, payment apps, and social media platforms to steal user credentials.

SOCIAL ENGINEERING TACTICS USED BY ATTACKERS



Attackers manipulate human psychology:

- **Fear:** "Your account is compromised"
- **Urgency:** "Act within 10 minutes"
- **Authority:** Pretending to be officials or IT staff
- **Greed:** Fake rewards or prize winnings
- **Trust:** Pretending to be friends or coworkers

Phishing attacks rely on social engineering techniques that manipulate human emotions. Attackers use fear by claiming security threats, urgency by demanding quick action, authority by pretending to be officials or managers, greed by offering prizes or rewards, and trust by impersonating friends or coworkers. Recognizing these tactics helps users pause and think before reacting.

REAL-WORLD PHISHING SCENARIOS

A common phishing scenario is a fake bank email stating suspicious activity and asking users to click a link to verify details. Another example is a message claiming a prize win or delivery update. These links usually redirect to fake websites that collect login credentials, OTPs, or card details, leading to financial fraud.

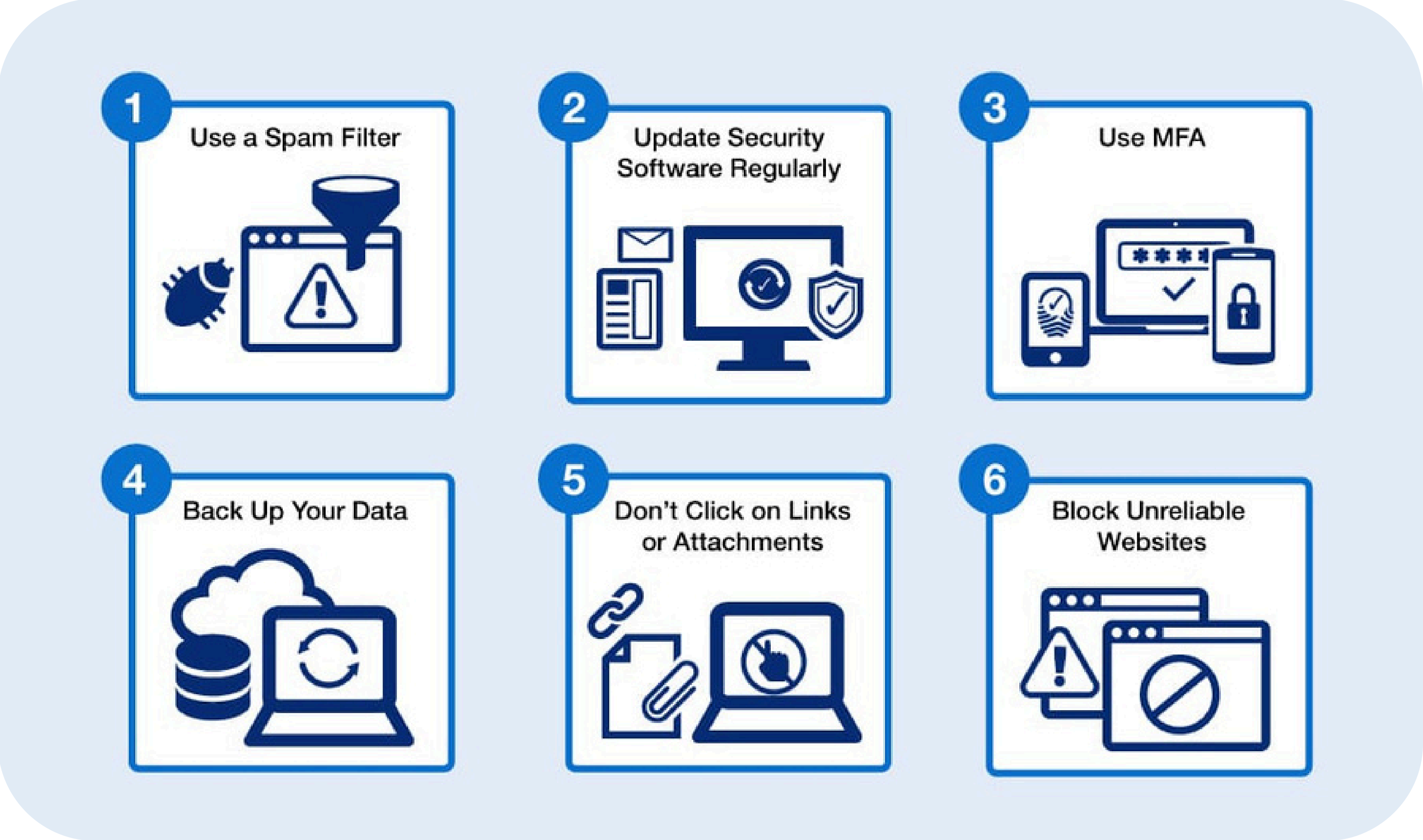
Email Example: "Your bank account has suspicious activity. Click here to verify your details immediately."

🔍 What’s wrong?

- Creates panic
- Suspicious link
- Asks for sensitive data

BEST PRACTICES TO PREVENT PHISHING ATTACKS

To avoid phishing, users should never click on suspicious links or download unknown attachments. Passwords and OTPs should never be shared with anyone. Always verify messages using official websites or customer support numbers. Use strong, unique passwords and enable two-factor authentication. Keeping devices and software updated adds an extra layer of security.


1
Use a Spam Filter
2
Update Security Software Regularly
3
Use MFA
4
Back Up Your Data
5
Don't Click on Links or Attachments
6
Block Unreliable Websites

- Never click suspicious links
- Do not share OTPs or passwords
- Verify sender identity via official channels
- Use strong, unique passwords
- Enable two-factor authentication (2FA)
- Keep software and browsers updated

WHAT TO DO IF YOU SUSPECT PHISHING

- If you receive a phishing message, do not respond or click on any links. Report the message and delete it. If you have already clicked a link or shared information, immediately change your passwords, enable two-factor authentication, inform your bank or organization, and scan your device for malware. Acting quickly can reduce damage.

    - Do not respond
    - Do not click links or download files
    - Report the email/message
    - Delete it
    - Change passwords if already clicked

CONCLUSION

Phishing attacks exploit human behavior rather than technical flaws. Awareness, alertness, and verification are the best defenses against phishing. Always think before clicking, verify suspicious messages, and report phishing attempts. Cybersecurity is a shared responsibility, and informed users are the strongest line of defense.

Thank You