CODE ALPHA

PROTECTING YOURSELF FROM PHISHING ATTACKS

Muhammad Shoaib Ishaq Khan

INTRODUCTION

- **Phishing**, is a common threat, involves impersonation to obtain sensitive information, often passwords.
- Attackers use deceptive links and attachments, costing companies millions and risking employee safety.
- Our goal is to keep both the business and the staff safe from harm.

TYPES OF PHISHING ATTACKS

Social Engineering

Manipulating individuals to divulge confidential information.
Examples: Impersonation, emotional manipulation.

Website Phishing

Fraudulent websites imitating legitimate ones.
Examples: Fake login pages, malicious websites.

Email Phishing

Deceptive emails to extract information.
Examples: Fake security alerts, account verification requests.

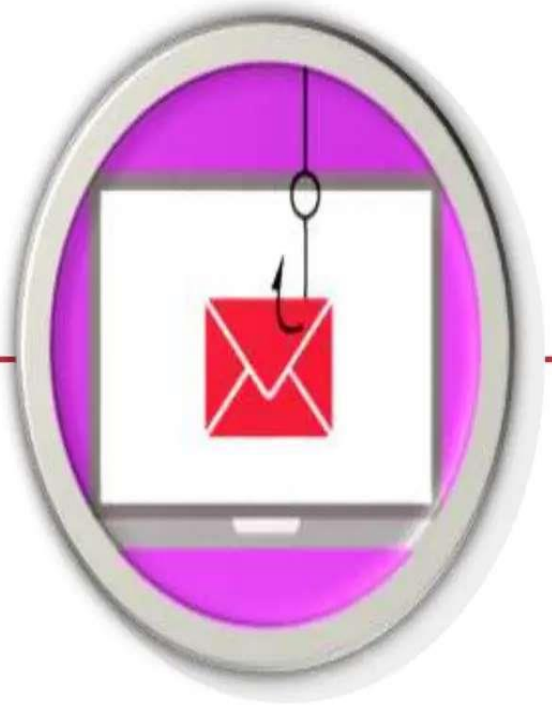
COMMON CHARACTERISTICS OF PHISHING ATTEMPTS

- Urgency: Creating a sense of immediate action.
- Unexpected Emails: Receiving unsolicited emails.
- Suspicious Links: Hover over links to preview URLs
- Requests for Personal Information: Be cautious.

RECOGNIZING PHISHING EMAILS

Check the Sender's Email Address.

Look for Spelling and Grammar Mistakes.



Verify Email Content.

Hover Over Links to Preview URLs.

RECOGNIZING PHISHING WEBSITES

Check the URLs.

Look for HTTPS.

Verify Website Legitimacy.

Be Cautious with Pop-Up Forms.

SOCIAL ENGINEERING TACTICS

Impersonation Techniques.

Manipulation of Trust.

Exploiting Human Emotions.

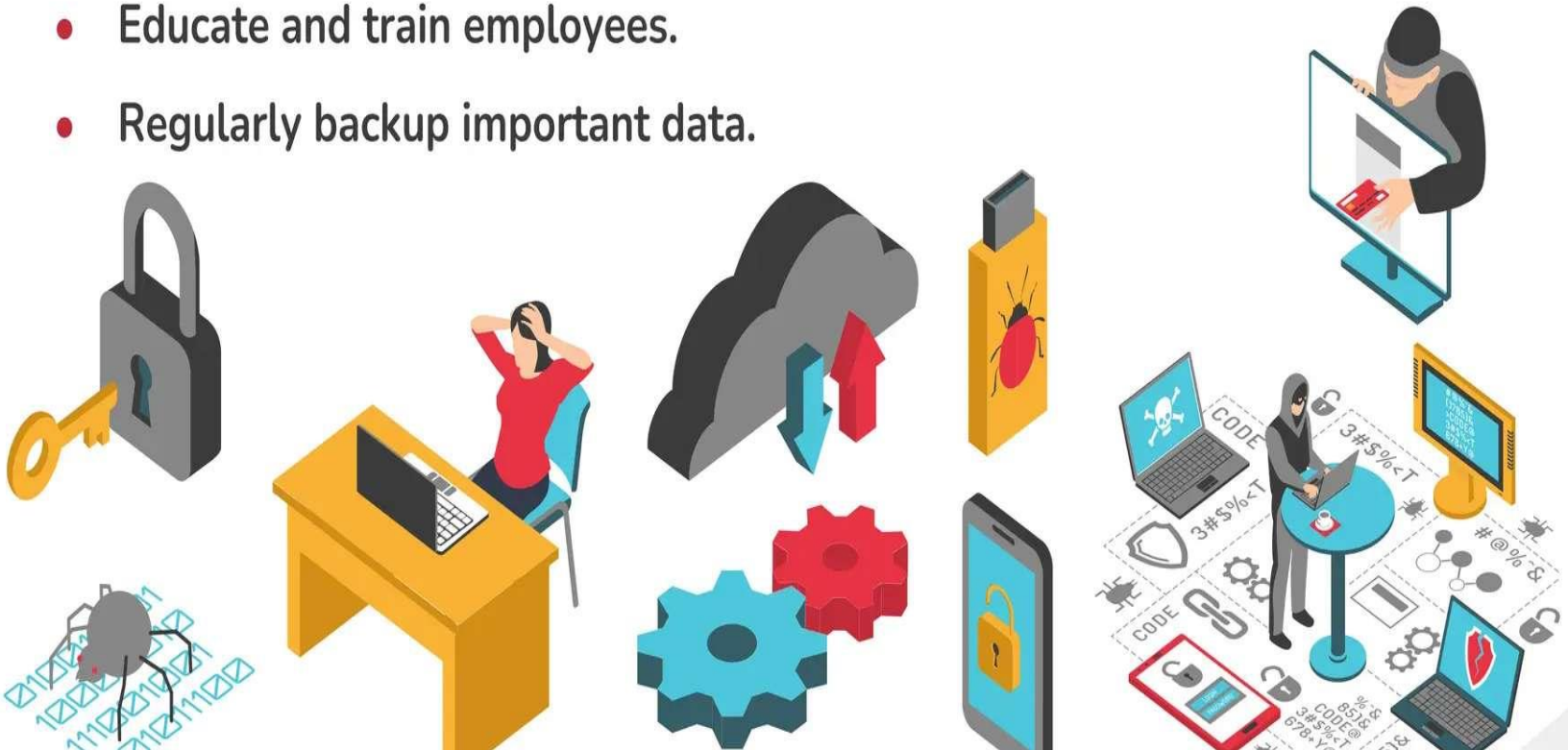
Awareness of Social Media Manipulation.

PROTECTING PERSONAL INFORMATION

- Never Share Passwords via Email.
- Use Two-Factor Authentication.
- Verify Requests for Sensitive Information.
- Be Cautious with Personal Information Sharing.

BEST PRACTICES FOR AVOIDING PHISHING

- Keep software updated and use security software.
- Educate and train employees.
- Regularly backup important data.



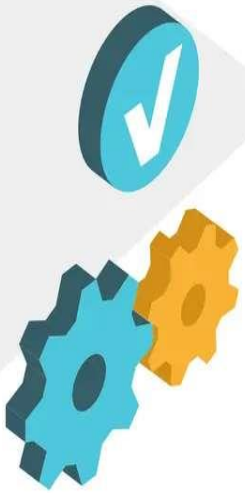
CASE STUDIES

- **Attack :**

Global Enterprises fell victim to a phishing attack as cybercriminals posed as a trusted vendor, deceiving the finance department into urgently altering payment details for an invoice. The undetected fraudulent payment led to financial loss and strained vendor relationships, only discovered when the legitimate vendor inquired about the overdue payment.

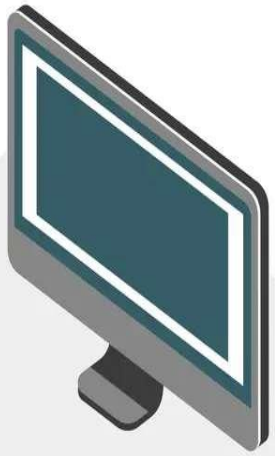
- **Lessons Learned :**

Global Enterprises strengthened vendor payment protocols with robust verifications and approvals. They introduced role-specific phishing training for the finance team, emphasizing red flag recognition and trusted channels for payment verification.



FINAL WORDS

Phishing attacks will continue to happen in the future. *It is up to the organization and its employees to learn from past mistakes and not repeat them*. Employees can educate themselves on how to stop phishing emails. Organizations can deploy the best phishing protection solutions to deal with such situations effectively. Furthermore, organizations must include case studies related to past incidents in the employee education and training programs.



THANKS

I want to express my gratitude for your time and active involvement in today's presentation, focusing on safeguarding against phishing attacks. Your engagement enhances our collective understanding and commitment to strengthening cybersecurity measures.