PHISHING AWARENESS TRAINING

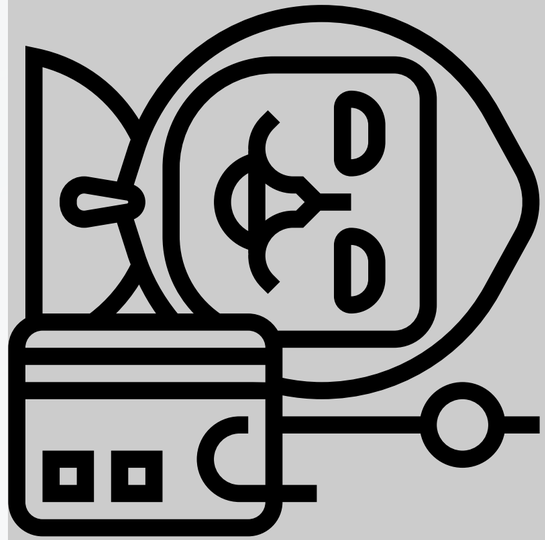
HOW TO RECOGNIZE AND AVOID PHISHING ATTACKS

INTRODUCTION

What is Phishing?

- Definition: Phishing is a type of cyber attack where attackers attempt to deceive individuals into providing sensitive information by pretending to be a trustworthy entity in electronic communications.

- How it Works: Attackers often use email, social media, or malicious websites to trick victims into revealing personal information such as usernames, passwords, and credit card numbers.



IMPORTANCE OF PHISHING AWARENESS

Why is Phishing Awareness Important?

Statistics

- Over 90% of cyber attacks start with a phishing email.
- The cost of a successful phishing attack on an organization averages $3.86 million (source: IBM).

Consequences

- Financial Loss: Direct theft of money from bank accounts.
- Data Breach: Exposure of sensitive data leading to identity theft.
- Reputational Damage: Loss of trust from customers and partners.
- Operational Disruption: Malware and ransomware can disrupt business operations.

Common Types of Phishing Attacks

01 Email Phishing

- Mass emails sent to many people.
- Common characteristics include generic greetings and urgent language.

02 Spear Phishing

- Targeted attacks on specific individuals.
- Often well-researched and personalized.

03 Whaling

- Targeting high-profile individuals like executives.
- Often involves business email compromise (BEC).

04 Smishing and Vishing

- Smishing: Phishing through SMS text messages.
- Vishing: Voice phishing over the phone.

RECOGNIZING PHISHING EMAILS

Red Flags in Phishing Emails

Suspicious Sender Addresses
Check the email address carefully for slight misspellings or unusual domains.

Generic Greetings
Phrases like “Dear Customer” instead of your name.

Urgent or Threatening Language
Claims that your account will be closed or you need to act immediately.

Unusual Attachments or Links
Unexpected files or links asking you to enter sensitive information.

ANALYZING A PHISHING EMAIL

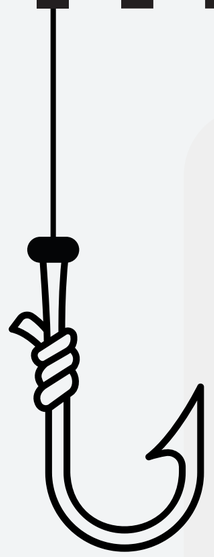
Example Email Analysis

- Red Flags Highlighted:
  Misspelled sender address
  Urgent and threatening language
  Suspicious link with an unusual domain

- Example Email: [Insert screenshot of a phishing email]
  From: “support@paypall.com” (note the misspelling of PayPal)
  Subject: “Your account is at risk!”

- Body:
  Generic greeting: “Dear User”
  Urgent language: “We have detected unusual activity on your account. Please click the link below to secure your account immediately.”
  Suspicious link: “http://paypall-security.com” (fake URL)

PHISHING WEBSITES



How to Identify a Phishing Website?

- **Check the URL**
  Look for misspellings, extra characters, or unusual domains (e.g., paypa1.com instead of paypal.com).

- **Look for HTTPS:**
  Ensure the site uses HTTPS and shows a padlock icon in the address bar.

- **Beware of Pop-Ups:**
  Be cautious if a website immediately asks for sensitive information through pop-ups.

SOCIAL ENGINEERING TACTICS

Understanding Social Engineering

- **Exploitation of Human Psychology:**
  Phishers exploit emotions such as fear, greed, and curiosity.
- **Common Tactics:**
  Pretexting: Creating a fabricated scenario to steal information.
  Baiting: Offering something enticing to get victims to disclose information.
  Quid Pro Quo: Promising a benefit in exchange for information.

BEST PRACTICES TO AVOID PHISHING

Tips to Protect Yourself

- **Verify the Source:**
  Always verify the sender’s email address and be wary of unsolicited communications.
- **Strong Passwords and Two-Factor Authentication:**
  Use complex passwords and enable two-factor authentication (2FA) on all accounts.
- **Keep Software Updated:**
  Regularly update your operating system, browser, and antivirus software.
- **Educate Yourself and Others:**
  Stay informed about the latest phishing tactics and share this knowledge with colleagues.

WHAT TO DO IF YOU FALL FOR A PHISHING SCAM

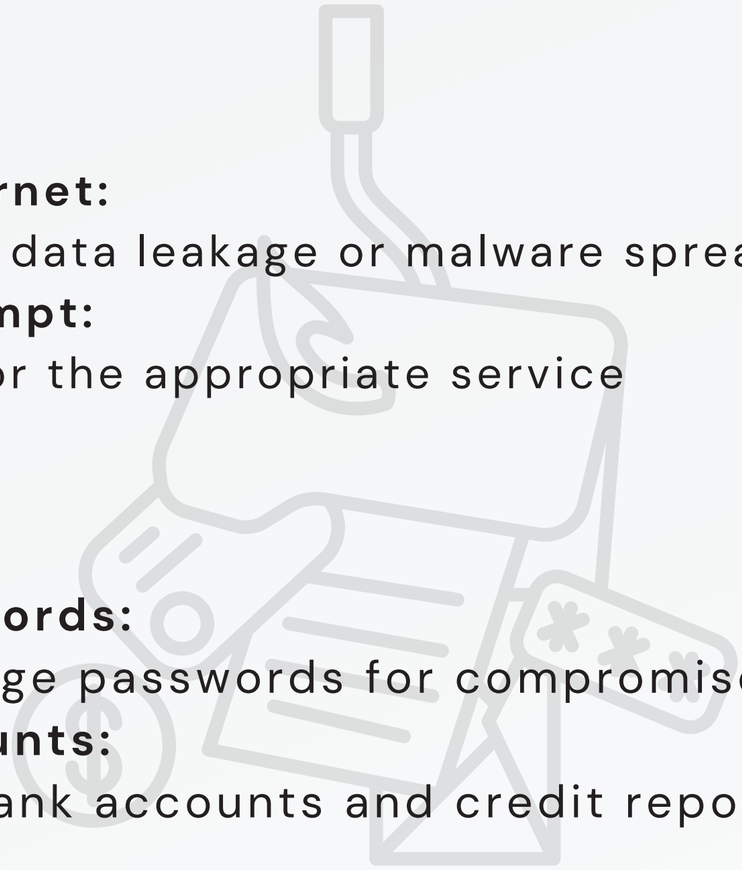
Immediate Actions

- **Disconnect from the Internet:**

This can help prevent further data leakage or malware spread.

- **Report the Phishing Attempt:**

Contact your IT department or the appropriate service provider.



- **Change Passwords:**

Immediately change passwords for compromised accounts.

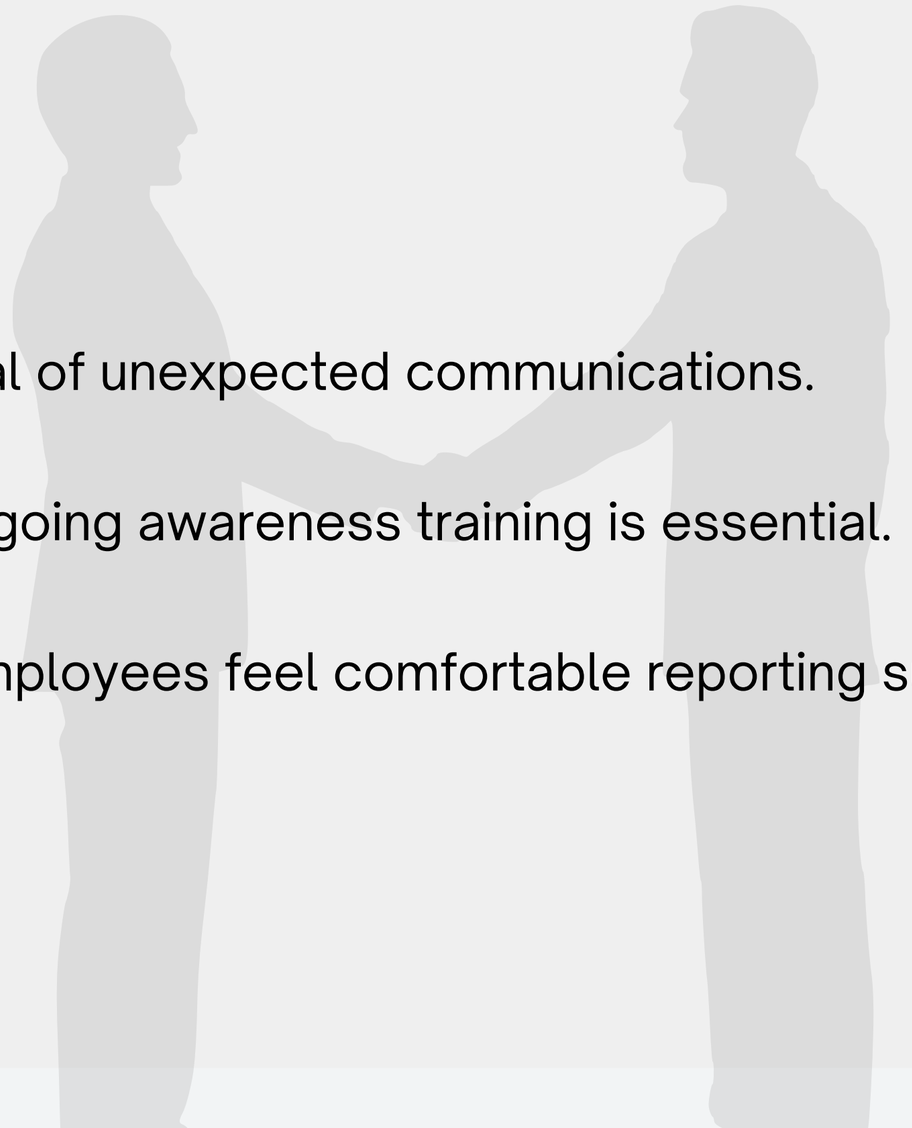
- **Monitor Accounts:**

Keep an eye on bank accounts and credit reports for unusual activity.

Conclusion

Recap of Key Points:

- **Stay Vigilant:**
  Always be cautious and critical of unexpected communications.
- **Continuous Education:**
  Phishing tactics evolve, so ongoing awareness training is essential.
- **Support System:**
  Encourage a culture where employees feel comfortable reporting suspicious activities.



THANK'S FOR WATCHING

By Mohamed Naeem