

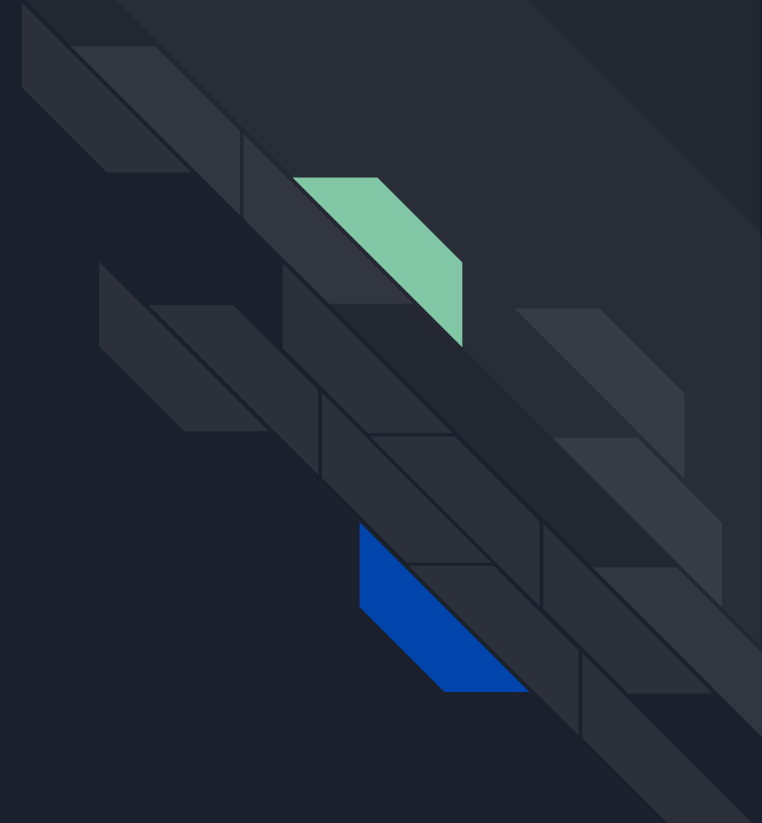


# Phishing Awareness

By Yashika Wadhwani

# Contents

1. Introduction to Phishing
2. How Phishing Works
3. Types of Phishing Attacks
4. Recognizing Phishing Emails
5. Avoiding Phishing Websites
6. Social Engineering Tactics
7. Preventive Measures
8. Reporting Phishing Attempts
9. Conclusion



# Introduction

**Definition of Phishing:** Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in electronic communication.

**Importance of Phishing Awareness:** Phishing attacks are becoming increasingly sophisticated and prevalent, posing significant risks to individuals and organizations.

**Impact of Phishing Attacks:** Data breaches, financial losses, reputation damage, and loss of trust are common consequences of successful phishing attacks.






# How Phishing Works

## Phases of a Phishing Attack:

1. Planning: Attackers identify targets and gather information.
2. Delivery: Phishing emails or messages are sent to potential victims.
3. Exploitation: Victims are manipulated into revealing sensitive information.
4. Installation: Malware or malicious code is installed on victim's devices.
5. Command & Control: Attackers gain control over compromised systems.



# Types of Phishing Attacks (1/3) - Email Phishing

**Standard Phishing Emails:** Mass emails sent to a large number of recipients.

**Spear Phishing:** Targeted emails customized for specific individuals or organizations.

**Whaling:** Targeting high-profile individuals, such as executives or celebrities, for financial gain or espionage.

# Types of Phishing Attacks (2/3) - Phishing Websites

**Fake Login Pages:** Spoofed websites designed to mimic legitimate login pages of banks, social media platforms, or other online services.

**Spoofed Websites:** Websites with URLs and content that appear legitimate but are controlled by attackers.

**Pharming:** Redirecting users to malicious websites through DNS spoofing or manipulation.





# Types of Phishing Attacks (3/3) - Social Engineering

**Pretexting:** Creating a fabricated scenario or pretext to manipulate individuals into disclosing confidential information.

**Baiting:** Luring victims with the promise of something desirable, such as free software or prizes, to extract sensitive information.

**Tailgating:** Gaining unauthorized access to secure areas by exploiting the courtesy or trust of authorized individuals.

**Quid Pro Quo:** Offering a benefit or service in exchange for sensitive information.

# Recognizing Phishing Emails

## Red Flags to Watch For:

1. Unsolicited Requests
2. Urgency or Threats
3. Poor Grammar/Spelling
4. Generic Greetings



**Examples of Phishing Emails:** Provide visual examples of phishing emails highlighting these red flags.

**Hovering over Links:** Demonstrating how to hover over links to reveal actual URLs and verify legitimacy.





# Avoiding Phishing Websites

**Checking Website URLs:** Encourage users to check for HTTPS, domain name legitimacy, and SSL certificates.

**Verifying SSL Certificates:** Look for the padlock icon and verify SSL certificates to ensure secure connections.

**Using Browser Security Features:** Enable phishing filters and browser security settings to detect and block phishing websites.



# Social Engineering Tactics

**Manipulation Techniques Used by Attackers:** Exploiting human psychology, emotions, and trust to deceive victims.

**Building Trust and Authority:** Creating a false sense of trust or urgency to manipulate victims into taking action.

**Exploiting Human Psychology:** Leveraging emotions such as fear, curiosity, or greed to elicit responses from victims.



# Preventive Measures

## Education and Training:

Conduct regular phishing awareness training sessions for employees.

Implement simulated phishing campaigns to educate users about phishing tactics.

## Technical Solutions:

Deploy email filtering and spam detection systems to block phishing emails.

Utilize web filtering and URL reputation services to identify and block malicious websites.

Recommend anti-phishing browser extensions for additional protection.

## Security Best Practices:

Enable two-factor authentication (2FA) for enhanced account security.

Keep software and systems updated to patch known vulnerabilities.

Use strong, unique passwords and password managers to store credentials securely.

Verify requests for sensitive information by contacting the sender through trusted channels.



# Reporting Phishing Attempts

**Internal Reporting Procedures:** Provide guidelines for reporting phishing attempts within the organization, including whom to contact and what information to provide.

**Reporting to External Authorities:** Encourage reporting phishing attempts to external organizations such as CERT/CSIRT or anti-phishing organizations for further investigation and action.





# Conclusion

**Recap of Key Points:** Summarize the key concepts covered in the presentation, including the types of phishing attacks, red flags to watch for, and preventive measures.

**Importance of Vigilance and Awareness:** Emphasize the importance of remaining vigilant and continually educating oneself about evolving phishing tactics.

**Commitment to Phishing Prevention:** Encourage the audience to take proactive steps to protect themselves and their organizations from phishing attacks.



THANKYOU