PHISHING ATTACKS

A GROWING THREAT

LEARN HOW TO RECOGNIZE AND AVOID PHISHING EMAILS, WEBSITES, AND SOCIAL ENGINEERING TACTICS

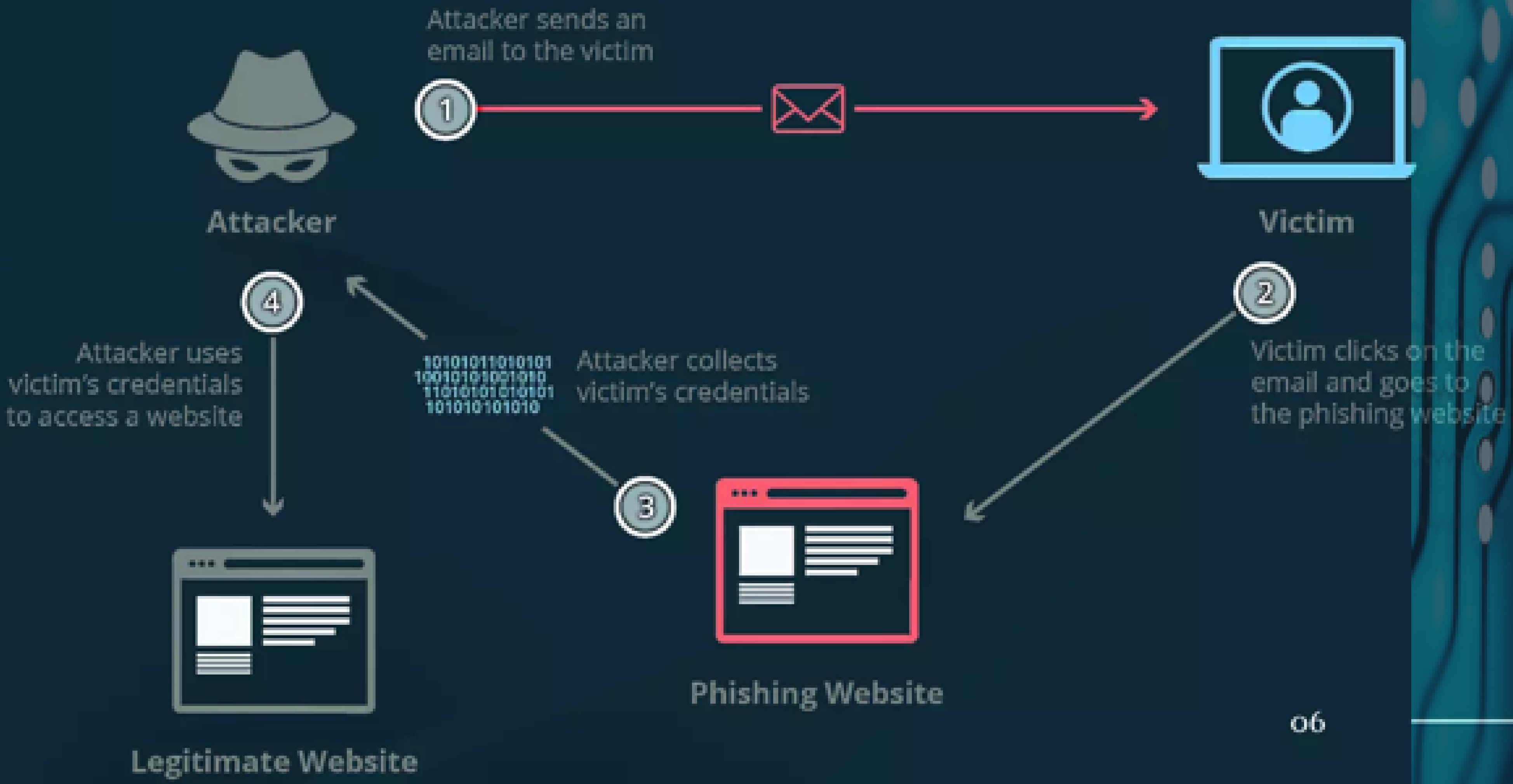
INTRODUCTION

- Phishing is a type of social engineering attack where attackers use email, phone, or text messages to trick victims into revealing sensitive information such as passwords, credit card numbers, or personal data.
- Phishing attacks are a type of cybercrime where attackers use deception to trick victims Into revealing sensitive information.
- Examples :

Phishing attacks can take many forms, including:

  - Email phishing: Attackers send fake emails that appear to be from a legitimate source, asking for sensitive information.
  - Spear phishing: Targeted attacks on specific individuals or organizations. Etc.

Typical Scenario of Phishing Attacks



Attacker

Victim

1 Attacker sends an email to the victim

2 Victim clicks on the email and goes to the phishing website

3 Attacker collects victim's credentials

4 Attacker uses victim's credentials to access a website

Phishing Website

Legitimate Website

TYPES OF PHISHING ATTACKS :

❑ **DECEPTIVE PHISHING :** THE MOST COMMON TYPE, WHERE ATTACKERS SEND FAKE EMAILS OR MESSAGES THAT APPEAR TO BE FROM A LEGITIMATE SOURCE.

❑ **SPEAR PHISHING :** TARGETED ATTACKS ON SPECIFIC INDIVIDUALS OR ORGANIZATIONS.

❑ **WHALING :** TARGETED ATTACKS ON HIGH-LEVEL EXECUTIVES OR OFFICIALS.

❑ **SMISHING :** PHISHING ATTACKS VIA SMS OR TEXT MESSAGES.

❑ **VISHING :** PHISHING ATTACKS VIA VOICE CALLS.

HISTORY OF PHISHING : (A)

- ❑ **1990 :** THE FIRST PHISHING ATTEMPT IS RECORDED ON AMERICA ONLINE HACKER ATTEMPT TO STEAL LOGIN CREDENTIALS PERSONAL INFORMATION FROM AOL TO RESELL ONLINE.

- ❑ **2000 :** THE RISE OF E-COMMERCE ENCOURAGES CYBER CRIMINALS TO CREATE SPOOFED WEBSITES. IMPERSONATING POPULAR DOMAIN LIKE PAYPAL & E BAY.

  THEY USED EMAIL WORM PROGRAMS TO SEND OUT SPOOFED EMAILS TO PAY PAL CUSTOMERS .

- ❑ **2008 :** CURRENCY ARE LAUNCHED THIS INCREASES THE CREATION OF MALWARE AS IT IS EASIER FOR CYBER CRIMINALS TO SECURELY RECEIVE PAYMENT FROM THEIR VIC.

HISTORY OF PHISHING : (B)

❑ IN LATE 2008, BITCOIN AND OTHER CRYPTOCURRENCIES ARE LAUNCHED. THIS ALLOWS TRANSACTIONS USING MALICIOUS SOFTWARE TO BE SECURE AND ANONYMOUS, CHANGING THE GAME FOR CYBERCRIMINALS.

❑ **2013 :** PHISHING BECOMES THE PRIMARY TECHNIQUE TO DELIVER RANSOMWARE.

❑ **2019 :** CYBER CRIMINALS BEING HIDING MALICIOUS CODE INSIDE IMAGE FILES TO SLIP THROUGH USER’S ANTI – VIRUS SOFTWARE.

COMMON CHARACTERISTICS OF PHINSHING :

- ❑ Urgency : Creating a sense of immediate action.
- ❑ Unexpected Emails : Receiving unsolicited Emails.
- ❑ Suspicious Links : Hover Over links to preview URLs.
- ❑ Request for Personal Information: Be Cautious.

RECOGNIZING PHISHING EMAILS

Check the sender's Email Address.

Look for Spelling and Grammer 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 Form

SOCIAL ENGINEERING TACTICS

Impersonation Techniques.

Manipulation of Trust.

Exploiting Human Emotions.

Awareness of Social Media Manipulation.

BEST PRACTICES FOR AVOIDING PHISHING

❑ Be cautious with emails and websites that ask for personal information.

❑ Verify the identity of the person or company.

❑ Use strong and unique passwords.

❑ Keep your antivirus software and operating system up to date.

❑ Use two-factor authentication whenever possible.

ANTI-PHISHING SOFTWARE (A)

1. Email Security Solutions

Proofpoint: Offers advanced email protection against phishing, spam, and Malware.

Mimecast: Provides email security with targeted threat protection against spear-phishing and other Attacks.

Barracuda: Features email protection with real-time threat intelligence to block phishing Emails.

2. Web Filtering and Protection

OpenDNS by Cisco: Blocks malicious websites and provides phishing protection at the DNS layer.

Webroot: Delivers real-time anti-phishing through web filtering and endpoint protection.

3. Browser Extensions

McAfee Web Advisor: Warns about risky websites and helps prevent phishing Attacks.

ANTI-PHISHING SOFTWARE (B)

Avira Browser Safety: Blocks harmful websites and phishing attempts.

4. Multi-Factor Authentication (MFA)

Duo Security: Provides two-factor authentication to add an extra layer of Security.

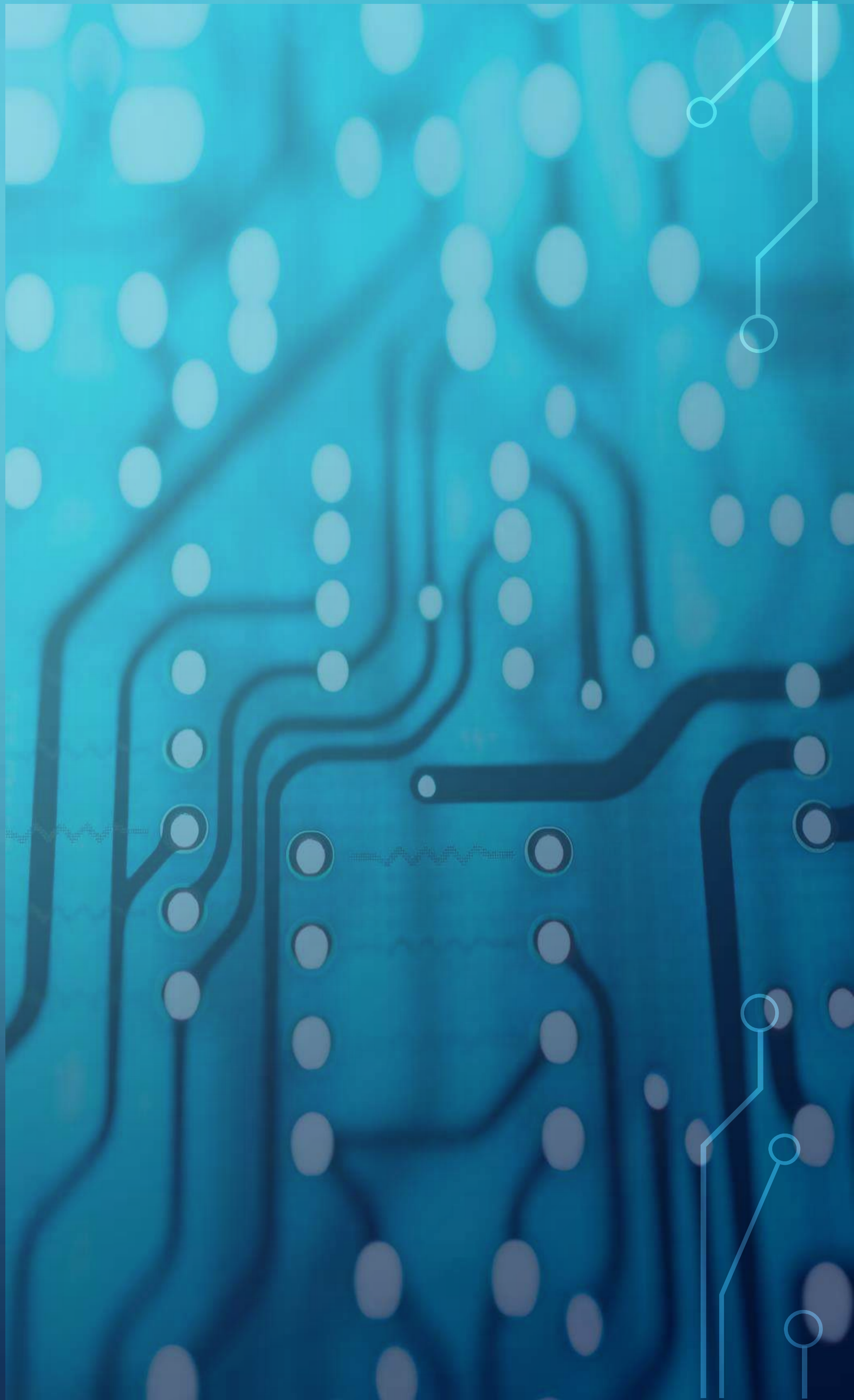
Google Authenticator: Offers a free app for two-step verification to protect accounts from Phishing.

5. Educational Websites and Courses

Coursera: Offers courses on cybersecurity, including phishing prevention and Awareness.

Udemy: Provides a variety of courses on phishing awareness and cybersecurity best Practices.

SANS Security Awareness: Specializes in security awareness training programs for organizations.



ANTI-PHISHING SOFTWARE (C)

6. Government Resources

US-CERT (United States Computer Emergency Readiness Team): Provides alerts, tips, and guidelines on preventing phishing and other cyber Threats.

FTC (Federal Trade Commission): Offers information on how to recognize, report, and protect against phishing Scams.

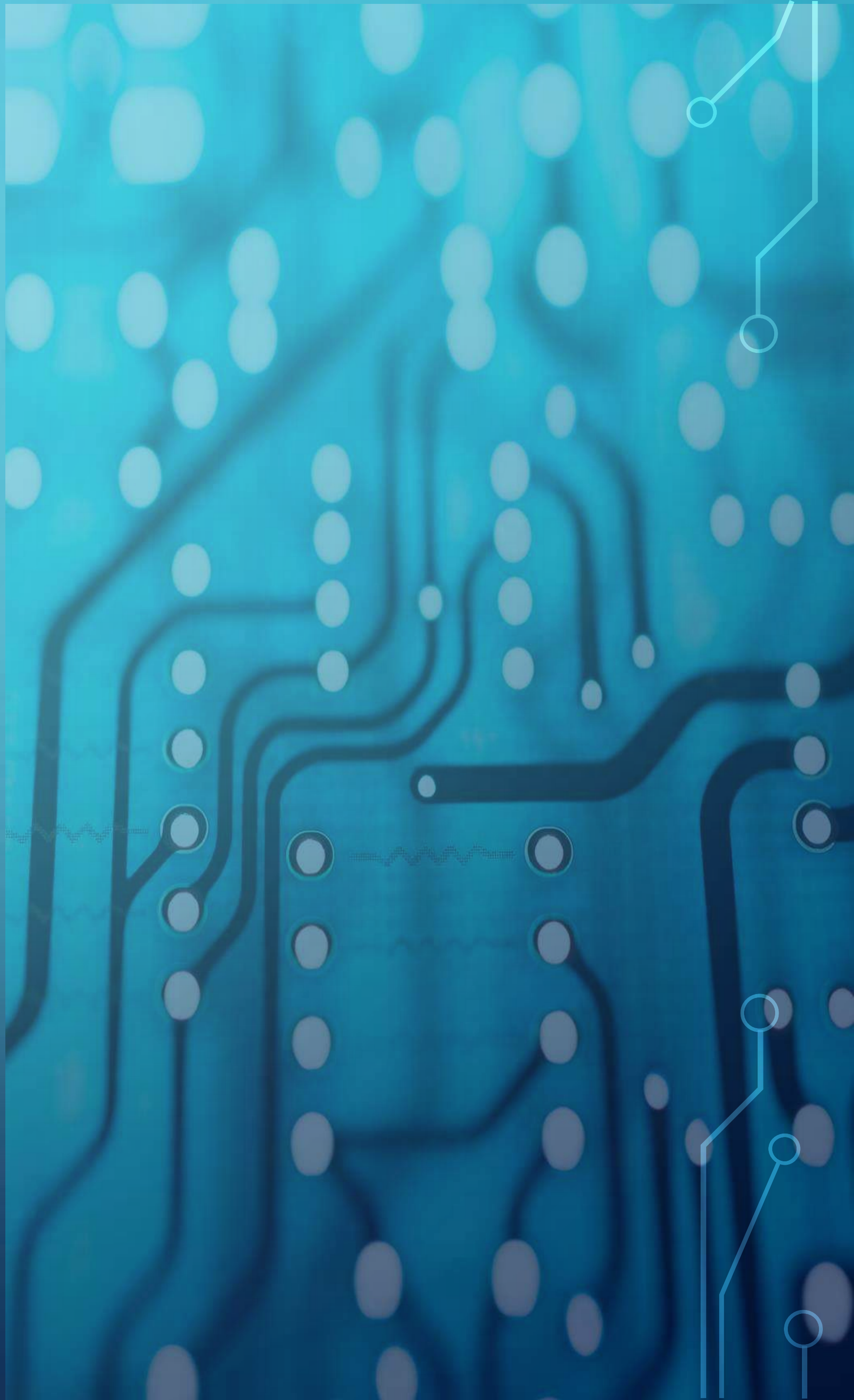
CISA (Cybersecurity and Infrastructure Security Agency): Provides resources and tools to enhance cybersecurity awareness and Defense.

7. Non-Profit Organizations

Anti-Phishing Working Group (APWG): A global coalition focused on combating phishing and other cyber crimes through research and sharing best Practices.

Cybercrime Support Network (CSN): Provides support and resources for individuals and businesses affected by cybercrime, including phishing.

Many more Anti-Phishing Software.



CONCLUSION

□ Phishing attacks are a serious threat to individuals and organizations.

□ By recognizing the characteristics of phishing emails and websites, and following best practices for avoiding phishing attacks, you can significantly reduce the risk of falling victim to these scams.

□ Remember to always be cautious when clicking on links, verifying email senders, and using strong passwords.

□ No Single Technology will completely stop Phishing Attack.

THE END