CYBER SECURITY

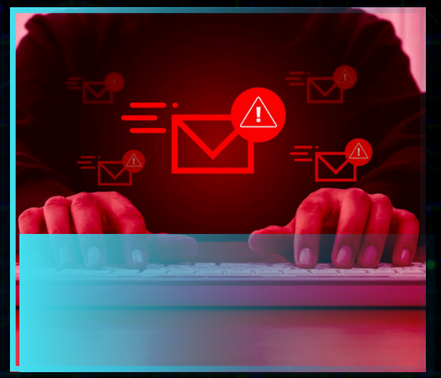
STAY SAFE ONLINE

Recognize Phishing Attacks

1. Suspicious emails: Be cautious of emails that are not addressed to you by name, contain spelling and grammar mistakes.
2. Unusual sender: Check the sender's email address to see if it's legitimate. Scammers often use fake email addresses that may look similar to those used by legitimate companies.
3. Urgent or threatening tone: Phishing emails often try to create a sense of panic or fear to prompt you into taking action.

Avoid Phishing Attacks

1. Verify the sender: If you're unsure about the sender's identity, contact the company directly using a phone number or email address you know is legitimate.
2. Don't click on suspicious links: Avoid clicking on links from unknown senders, as they may lead to phishing websites or download malware.
3. Use strong passwords: Use unique, strong passwords for all accounts, and avoid using the same password across multiple sites.



WHAT IS PHISHING ?

Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data, downloading malware or otherwise exposing themselves to cybercrime.

Phishing attacks are a form of social engineering. Unlike other cyberattacks that directly target networks and resources, social engineering attacks use human error, fake stories and pressure tactics to manipulate victims into unintentionally harming themselves or their organizations.

In a typical phishing scam, a hacker pretends to be someone the victim trusts, like a colleague, boss, authority figure or representative of a well-known brand.

PHISHING EMAILS

Urgent or Threatening Language

Creates panic to force quick action (e.g., "Your account will be locked").

Suspicious Email Address

Slight misspellings or odd domain names (e.g., @amazOn-support.com).

Generic Greetings

Dear Customer" instead of your name.

Unexpected Attachments

Especially ZIP, EXE, or Word files with macros—can contain malware.

Fake or Misleading Links

Hover to preview links; phishing links often look similar but are fake.

FAKE WEBSITES

Points to Identify Fake or Phishing Websites:

1. Suspicious URL or Domain Name
   - Look for misspellings, extra characters, or wrong domain endings (e.g., .net instead of .com).
   - Example: www.paypa1.com instead of www.paypal.com.
2. No HTTPS (No Lock Icon)
   - Legit sites use HTTPS (secure connection).
   - Lack of a lock symbol in the address bar is a red flag.
3. Poor Design and Layout
   - Low-quality images, inconsistent fonts, or broken links indicate a fake site.
4. Pop-Ups Asking for Credentials
   - Fake sites often display urgent pop-ups to steal usernames, passwords, or card info.

SOCIAL ENGINEERING TACTICS

1. Phishing

- Fake emails or messages that appear to be from trusted sources.
- Goal: Steal passwords, credit card numbers, or install malware.

2. Vishing (Voice Phishing)

- Phone calls pretending to be from a bank, tech support, or government.
- Tactics: Creating urgency ("Your account is compromised!") to steal data.

3. Smishing (SMS Phishing)

- Fake SMS messages with malicious links or urgent warnings.
- Common trick: "Your package is delayed, click to reschedule."

BEST PRACTICES

- ✅ Verify Sender Information
- Check the sender's email address and look for spelling errors or suspicious domains.
- 🔗 Be Cautious with Links & Attachments
- Hover over links to preview the URL before clicking. Avoid downloading unexpected files.
- 🔒 Use Strong Passwords & Enable 2FA
- Create complex passwords and secure your accounts with two-factor authentication.
- 🔄 Keep Software Updated
- Regularly update your operating system, browser, and apps to patch security vulnerabilities.
- 🛡️ Use Antivirus & Anti-Phishing Tools
- Install and regularly update reliable antivirus and anti-phishing software.

TO AVOID PHISHINGS

Tips to Avoid Phishing

1. Think Before You Click
   - Never click suspicious links in emails, texts, or pop-ups.
   - Hover over links to check the real URL.
2. Verify the Sender
   - Check the email address carefully.
   - If unsure, contact the sender using official contact details (not from the email).
3. Use Strong, Unique Passwords
   - Don't reuse passwords across sites.
   - Use a password manager to create and store them securely.
4. Enable Two-Factor Authentication (2FA)
   - Adds an extra layer of security, even if your password is stolen.

REAL WORLD PROBLEMS

Google & Facebook Scam (2013–2015)
Attack: A Lithuanian hacker tricked employees from Google and Facebook into sending over $100 million to fake invoices using a spoofed company email.
How: He created fake emails posing as a legitimate hardware vendor.
Lesson: Even tech giants can fall victim to well-crafted phishing.

Target Data Breach (2013)
Attack: Attackers used phishing emails to compromise a third-party HVAC vendor.
How: Once inside the vendor's system, attackers moved into Target's network.
Impact: Credit/debit card info of 40 million customers stolen.
Lesson: Phishing doesn't always target the victim directly — third parties are a weak link.

Twitter Bitcoin Scam (2020)
Attack: Hackers gained access to Twitter's admin tools via a phishing attack on employees.
How: They used social engineering and a fake login portal.
Impact: Took over high-profile accounts (Elon Musk, Obama, Apple, etc.) and promoted a crypto scam.

INTERACTIVE QUIZ

❓ *1. What are some common characteristics of phishing emails?*

- *A. Spelling or grammatical errors*
- *B. Urgent or threatening language*
- *C. Suspicious links or attachments*
- *D. All of the above* ✅

🌐 *2. How can you verify the authenticity of a website?*

- *A. Look for HTTPS in the URL*
- *B. Check the domain spelling*
- *C. Click without checking*
- *D. Both A & B* ✅

🚨 *3. What should you do if you suspect a phishing attack?*

- *A. Ignore it and delete*
- *B. Report it to your IT/security team* ✅
- *C. Reply and ask for confirmation*
- *D. Share with others to warn them*

CONCLUSION

- *Stay alert for suspicious messages and links.*
- *Double-check URLs and sender details before clicking.*
- *Never share personal or financial information blindly.*
- *Report phishing attempts to protect yourself and others.*

THANK YOU