

PHISHING AWARENESS TRAINING

Stay Safe from Online Scams



Presented by: Nandini Nath
BSc IT (Cyber Security) | Internship Project

INTRODUCTION



- Phishing is one of the most common cyber-attacks today.
- It tricks people into sharing sensitive data like passwords, OTPs, or bank info.
- Attackers use fake emails, websites, SMS, or phone calls.
- **Impact** : Identity theft, financial fraud, and data breaches.

Types of Phishing

- **Email Phishing** : Fake mails asking for login info.
- **Spear Phishing** : Targeted attack on individuals or organizations.
- **Smishing** : Fraudulent SMS with malicious links.
- **Vishing** : Fake phone calls pretending to be from trusted entities.
- **Website Phishing** : Fake portals that look like real websites.

TYPES OF PHISHING



Email Phishing



Spear Phishing



Smishing



Vishing



Website Phishing

How to Recognize Phishing Emails

- Signs of phishing emails:
- Suspicious sender address (e.g., support@paypa1.com).
- Urgent or threatening language.
- Poor grammar and spelling mistakes.
- Unusual attachments or requests.
- Hovering over the link shows a fake/mismatched URL.



security-update@gmail.com

Suspicious sender

We detected an unusual sign-in attempt

Hello,

We recently prevented an attempt to sign in to your account from an unrecognized device. Please review the details below:

02/20/2024

3:12PM PST

Grammar errors

London, United Kingdom

If you were not this person, please sign in to your account and update your password.

[Sign in](#)

Link hover

The Security Team

How to Recognize Fake Websites

- Key checks:
- Fake or misspelled URLs (e.g., paypa1.com instead of paypal.com).
- No HTTPS / invalid SSL certificates.
- Poor-quality design, blurry logos.
- Pop-ups demanding personal or banking info.



Social Engineering Tactics

- Attackers manipulate human psychology to trick users :
 - Fear: 'Your account has been hacked!'
 - Greed: 'You won a lottery!'
 - Curiosity: 'See this shocking news!'
 - Authority: 'This is your bank/government officer.'



Best Practices & Tips

☐ ☒ Stay Safe with These Practices:

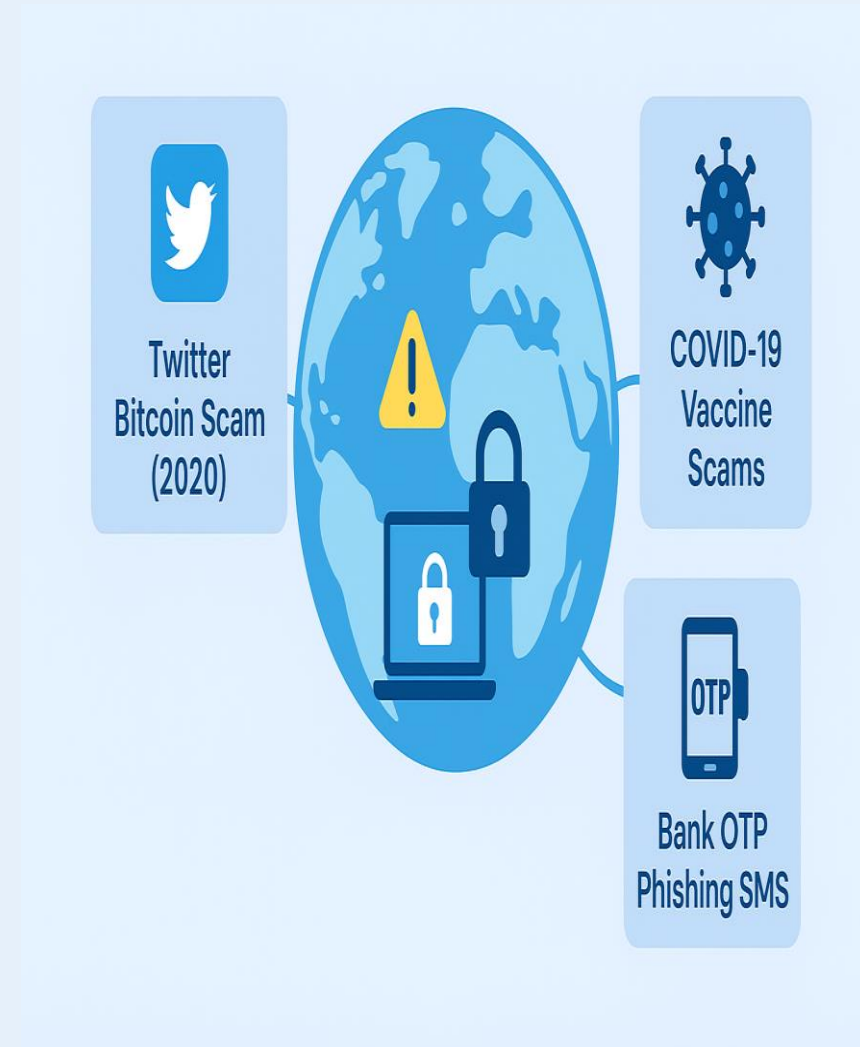
- Do NOT click suspicious links.
- Always verify sender's email or caller ID.
- Use strong, unique passwords.
- Enable Two-Factor Authentication (2FA).
- Keep system & antivirus updated.
- Report suspicious activity to IT/security team.



Real-World Examples


❑ Case Studies :

1. Twitter Bitcoin Scam (2020) :
Verified accounts hijacked to promote crypto scam.
2. COVID-19 Vaccine Scams :
Fake registration portals stole personal data.
3. Bank OTP Phishing SMS :
Criminals tricked users into sharing OTPs.




Interactive Quiz


Q1: You get an email from your bank asking to 'verify account' via a link. What should you do?

- a) Click link immediately
- b) Delete/Report it 
- c) Forward to friends


Q2: Which is a phishing sign?

- a) Secure HTTPS website
- b) Sender email: support@bank123fake.com 
- c) Professional layout

Q3: You receive an SMS claiming you won a prize and asking to click a link. What should you do?

- a) Click the link to claim
- b) Ignore/Delete the SMS 
- c) Reply with your details

Q4: Which of the following is a safe practice?

- a) Using the same password for all accounts
- b) Checking the URL before logging in 
- c) Clicking on pop-ups for quick login

Conclusion

❑ Key Takeaways :

- Recognize → Protect → Report
- Be alert to suspicious emails & websites.
- Stay safe by following cyber hygiene practices.
- Thank You 🙏 – Stay Cyber Safe!



**STAY SAFE
ONLINE**