



CYBER SECURITY

PHISHING AWARENESS TRAINING

(Understanding, Identifying, and Preventing Phishing Attacks)

A CYBERSECURITY AWARENESS MODULE

Presented By:

Parineeta Kapoor

Intern at CodeAlpha

15 June , 2025





INTRODUCTION TO PHISHING

WHAT IS PHISHING?

“The Cybercrime of Deception”

- Phishing is a type of cyber-attack where attackers trick users into revealing sensitive information like passwords, OTPs, bank details, or login credentials by pretending to be a trustworthy entity — usually through emails, websites, or messages.
 1. Often disguised as legitimate emails or websites
 2. Uses psychological manipulation (fear, urgency, reward)
 3. Targets both individuals and organizations
 4. Easy to fall for, but dangerous in impact



💡 90% of all cyber attacks begin with a phishing email.
— Verizon Data Breach Report



COMMON TRAITS OF PHISHING EMAILS

HOW TO RECOGNIZE A PHISHING EMAIL ?

(Red Flags You Should Never Ignore)

- **✗ Unusual sender address**

e.g., support@amaz0n-secure.com instead of amazon.com

- **! Grammatical errors or awkward language**

“Your account are suspended” types

- **⚠ Urgency or fear-based tone**

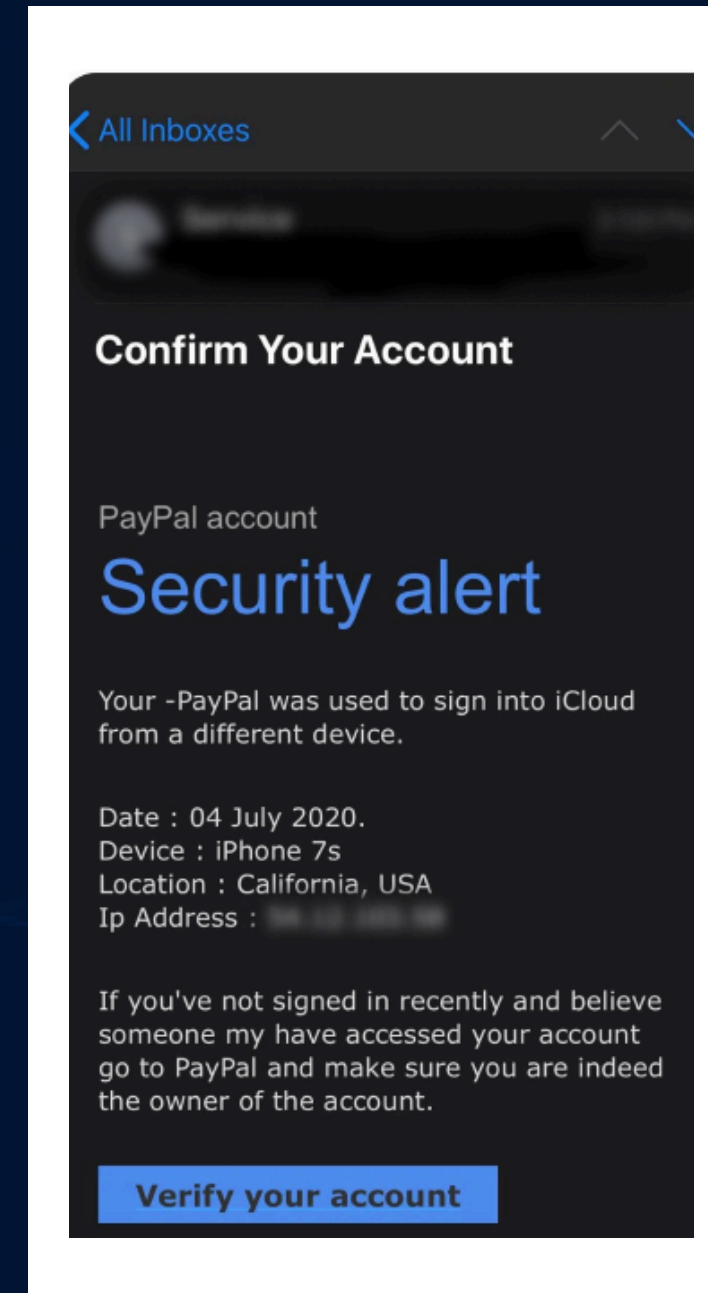
“Act now or your account will be locked!”

- **🔗 Suspicious links or attachments**

Hover shows different URL than displayed

- **📄 Request for sensitive info**

Like password, OTP, or bank PIN



If it looks urgent, too good to be true, or asks for personal info — pause. Think before you click.



SPOTTING FAKE WEBSITES

HOW TO IDENTIFY FAKE OR SPOOFED WEBSITE

Don't Just Click — Check Before You Trust!

-  **Suspicious URL structure**

amazon-support.xyz instead of amazon.in

Use of hyphens, extra words, or odd extensions (.net, .xyz, .top)

-  **No HTTPS or broken padlock icon**

Especially on login or payment pages

-  **Poor design or low-quality logo**

Stretched logos, weird fonts, pixelated layout

-  **Immediate pop-ups asking for login info or OTP**

Legit sites never ask this instantly

-  **Email/Phone form pre-filled or asking for “verification”**

Social engineering trap



Always double-check the web address. Fake sites look real — until they steal real data.



SOCIAL ENGINEERING TACTICS

THE HUMAN HACK: SOCIAL ENGINEERING TRICKS

Because Hackers Don't Just Break Systems — They Break Trust

- 🤖 **Fear or Panic Creation**

"Your bank account will be blocked in 2 hours!"

- 🎁 **Temptation with Rewards**

"Congratulations! You've won ₹50,000 — verify your account now."

- 👤 **Authority Impersonation**

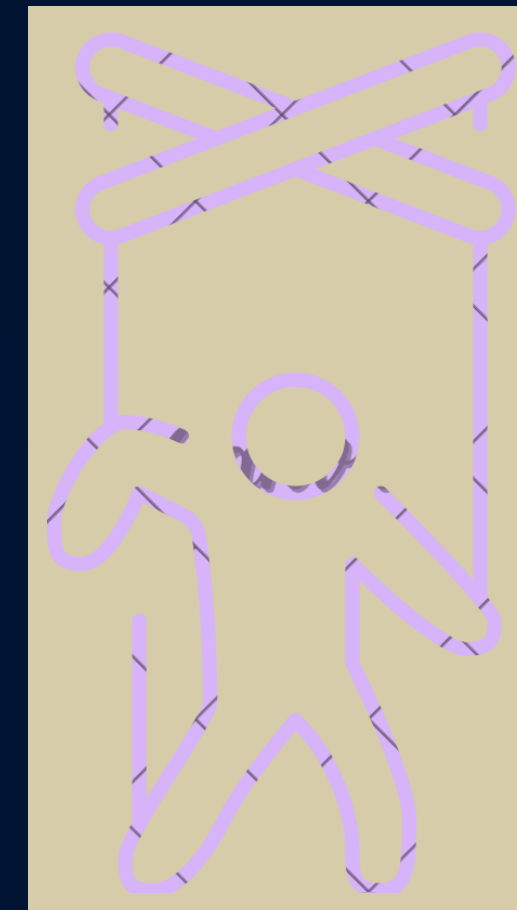
Pretending to be a manager, CEO, bank official, or even a government agency

- ❤️ **Emotional Manipulation**

Fake romantic interest, family emergencies, or donation appeals

- ⌚ **Urgency Without Time to Think**

"You have 5 minutes to respond or lose access."



MINI CASE

A friend of mine clicked on a fake HR email asking for updated bank details. Salary was diverted to a scammer's account. (Makes it personal + relatable)

If they want your emotions, they want your data.



TYPES OF PHISHING ATTACKS

PHISHING COMES IN MANY FORMS

Different Names, Same Dangerous Game

1. 📧 EMAIL PHISHING

The most common type — fake emails mimicking trusted entities

2. 📱 SMISHING (SMS PHISHING)

Phishing via text messages — often with fake links or fake delivery updates

Example: “Your parcel is stuck. Click here to release it.”

3. 📞 VISHING (VOICE PHISHING)

Phone calls pretending to be from bank/tech support asking for OTPs or details

“Sir, we’re from XYZ Bank. Please verify your card number...”

4. 🌐 SPEAR PHISHING

Targeted attack on a specific person or group using personal info

Usually disguised as a colleague or boss.

5. 🏢 WHALING

High-level phishing targeting CEOs, managers, or senior officials

“Urgent payment request from the Director” type of mails



No matter the form — if they ask for sensitive data unexpectedly, it’s probably a phish.



BEST PRACTICES TO AVOID PHISHING

PROTECT YOURSELF: BEST PRACTICES TO STAY SAFE

Prevention is Better Than a Data Breach!

-  **DON'T SHARE PERSONAL INFO OVER EMAIL/SMS**

NO LEGIT COMPANY EVER ASKS FOR PASSWORDS OR OTPS THIS WAY

-  **USE STRONG, UNIQUE PASSWORDS FOR EACH ACCOUNT**

AND STORE THEM IN A PASSWORD MANAGER

-  **KEEP SOFTWARE & ANTIVIRUS UPDATED**

UPDATES FIX VULNERABILITIES HACKERS EXPLOIT

-  **NEVER CLICK SUSPICIOUS LINKS**

HOVER TO PREVIEW THE URL FIRST — IF IT LOOKS OFF, DON'T CLICK

-  **VERIFY EMAIL ADDRESSES & PHONE NUMBERS**

CHECK SPELLING, DOMAIN, AND WHETHER IT MATCHES OFFICIAL RECORDS

-  **ENABLE MULTI-FACTOR AUTHENTICATION (MFA)**

EVEN IF YOUR PASSWORD IS LEAKED, MFA KEEPS YOUR ACCOUNT SAFE



When in doubt, throw it out. No email or call is worth risking your data.





REAL-WORLD PHISHING EXAMPLES

WHEN PHISHING GOT REAL

True Stories, True Losses

3 REAL CASES



“If it can happen to tech giants, it can happen to anyone.”

• 1. GOOGLE & FACEBOOK (2013–2015)

- A LITHUANIAN HACKER TRICKED EMPLOYEES WITH FAKE INVOICES AND EMAILS
- LOSS: \$100 MILLION
- ☒ **LESSON:** ALWAYS VERIFY VENDOR EMAILS & PAYMENT REQUESTS

• 2. SONY PICTURES HACK (2014)

- PHISHING EMAIL LED TO HACKERS BREACHING SONY'S NETWORK
- RESULT: DATA LEAKS, EMPLOYEE INFO, UNRELEASED FILMS STOLEN
- ☒ **LESSON:** ONE CLICK CAN COMPROMISE THE ENTIRE COMPANY

• 3. ICICI BANK (INDIA, 2020)

- FAKE SMS ABOUT BLOCKED DEBIT CARD LED CUSTOMERS TO PHISHING SITE
- RESULT: DOZENS OF CUSTOMERS LOST MONEY
- ☒ **LESSON:** NEVER CLICK ON LINKS FROM UNKNOWN TEXTS



INTERACTIVE QUIZ

QUICK QUIZ – ARE YOU PHISH-PROOF?

Test your phishing awareness in 5 quick questions!

- 🎯 Click below and check your score instantly.
- 📌 Submit the quiz and click “View Score” to know how safe your clicks really are.



[Take the Quiz Now →](#)



Scan & Test Yourself Now!








CONCLUSION

 **STAY CYBER-SAFE, STAY AWARE!**

“Think before you click — because one mistake can cost more than money.”

Phishing is not just a scam — it’s a trap waiting for one wrong click.

-  Be smart. Be alert.
-  Always verify links, emails, and unexpected messages.
-  Cybersecurity begins with YOU.

THANK YOU FOR YOUR TIME AND ATTENTION.

“You’re now one step ahead of phishing attackers!”

Thank You

