PHISHING AWARENESS

Done by: SAKTHI A

WHAT IS PHISHING?

Phishing is a type of cyber attack where attackers trick people into sharing personal information like passwords, bank details, or OTPs.

It usually happens through fake emails, websites, or messages.

TYPES OF PHISHING

Email Phishing

Email phishing is the most widely used method, where attackers send fake emails that appear to be from trusted sources like banks, social media platforms, or companies.

Spear phishing

Spear phishing is a more personalized and targeted attack. Unlike general phishing emails, spear phishing emails are crafted specifically for one individua or organization.

Smishing & Vishing

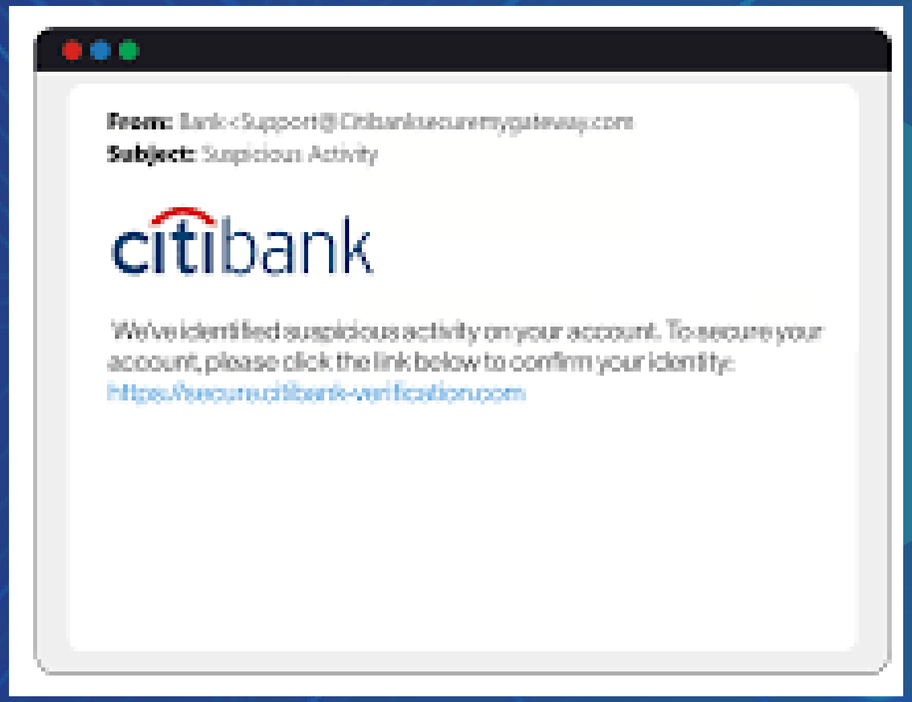
Smishing and vishing are phishing attempts through SMS (smishing) and voice calls (vishing). In smishing, victims receive text messages claiming to be from their bank or a government service, with links asking them to verify details or update their KYC.

HOW TO SPOT A PHISHING EMAIL

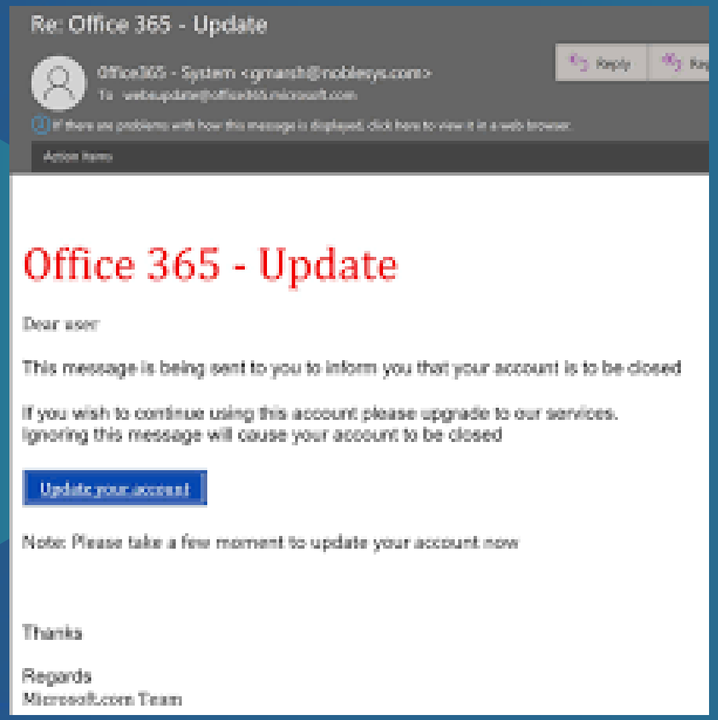
- Spelling or grammar mistakes
- Urgent tone (e.g., “Your account will be blocked”)
- Suspicious links (hover to check URL)
- Unfamiliar sender
- Attachments you weren’t expecting

REAL-WORLD EXAMPLES

01



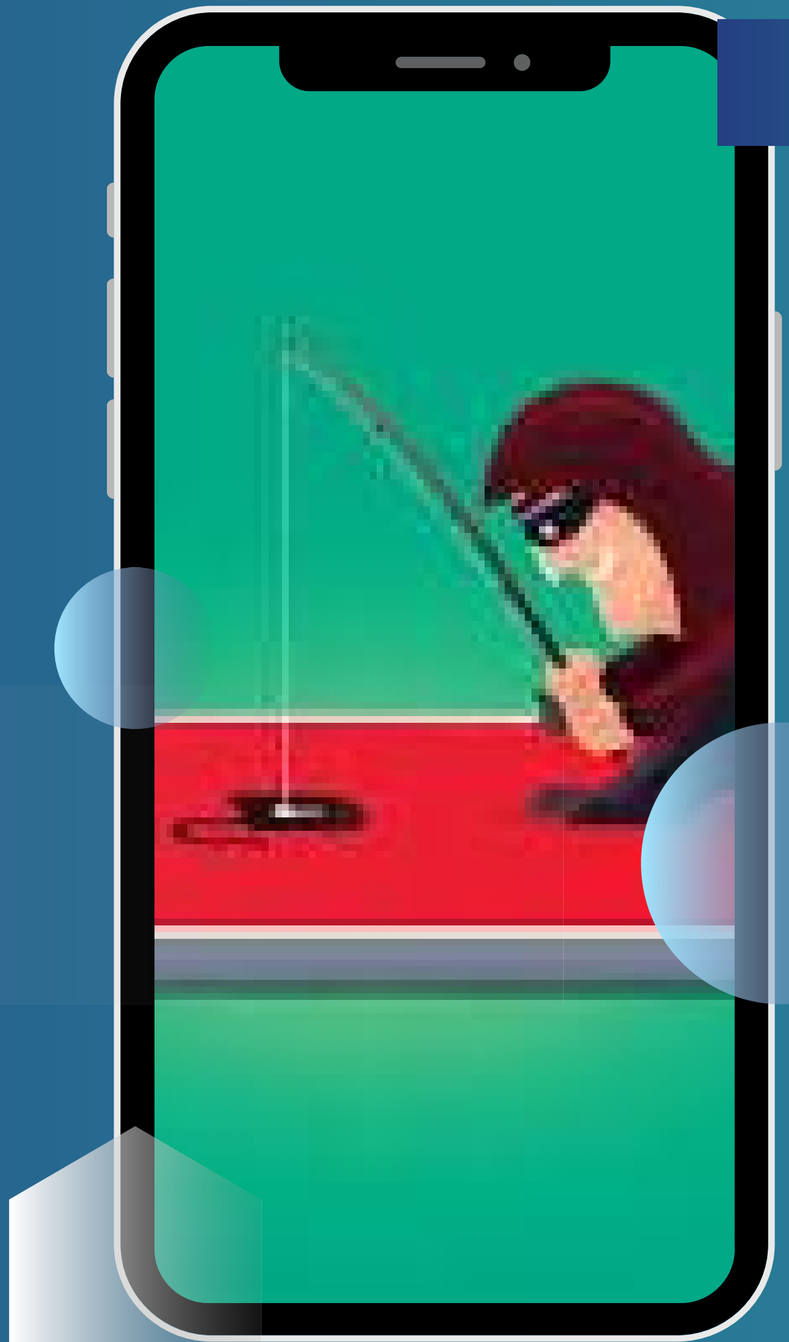
02



03

SOCIAL ENGINEERING TRICKS

- Fear: “Your account is hacked!”
- Greed: “You won a prize!”
- Curiosity: “See who viewed your profile”
- Urgency: “Do this now or else…”



HOW TO STAY SAFE

- Never click unknown links
- Don’t enter OTPs on random sites
- Use 2-Factor Authentication (2FA)
- Always check email sender
  Use updated antivirus

QUICK QUIZ

Q1. You receive an email saying “You won ₹1 Lakh!Click here.” What should you do?

A) Click the link
B) Report as spam ✅
C) Share with friends

Q2. A website looks like your bank but has spelling errors. Is it real?

A) Yes
B) No✅

THANK YOU!

Thank you for watching!
Stay safe, stay alert


BY: SAKTHI A