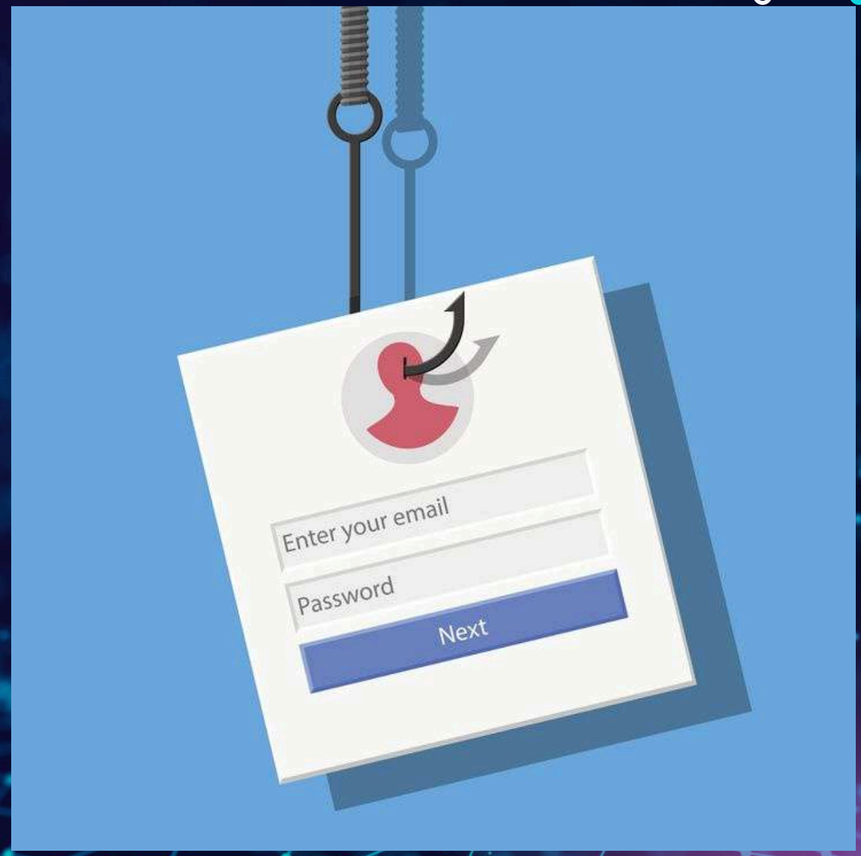
# PHISHING AWARENESS TRAINING

Stay Safe from Online Scams




-ANKITA GHOSHAL

# Understanding Phishing

- Phishing = Cybercrime that tricks you into revealing sensitive information.
- Common goals: steal passwords, credit card details, bank info, or identity.
- Delivered via: Emails, SMS, fake websites, or phone calls.
- Example: An email pretending to be from your bank asking for your login details.

# Spot the Red Flags

## Email Red Flags

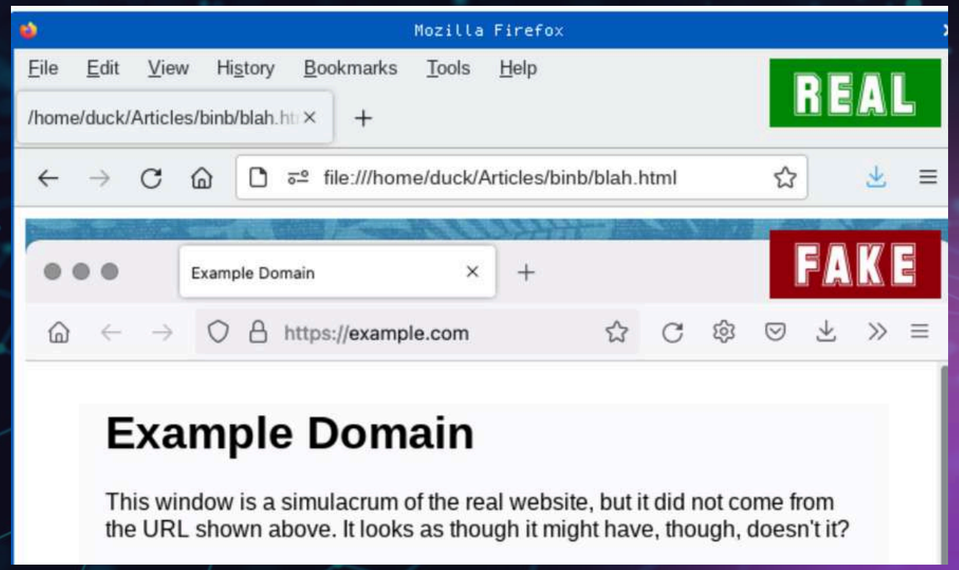
- Suspicious Sender: Check the “From” address carefully (e.g., support@paypal.com vs support@paypal.com).
- Generic Greetings: “Dear Customer” instead of your real name.
- Urgent/Threatening Language: “Act now or your account will be locked.”
- Attachments & Links: Don’t trust unexpected files or links.
- Grammar & Spelling Errors: Poorly written emails are a warning sign.

## if an Email is Fake

- Hover over links (without clicking) → check if the URL matches the official site.
- Verify the sender’s email domain (e.g., @gmail.com pretending to be a bank = fake).
- Contact the company directly through their official website/helpline instead of replying.
- If in doubt → Report the email.

## if a Website is Fake

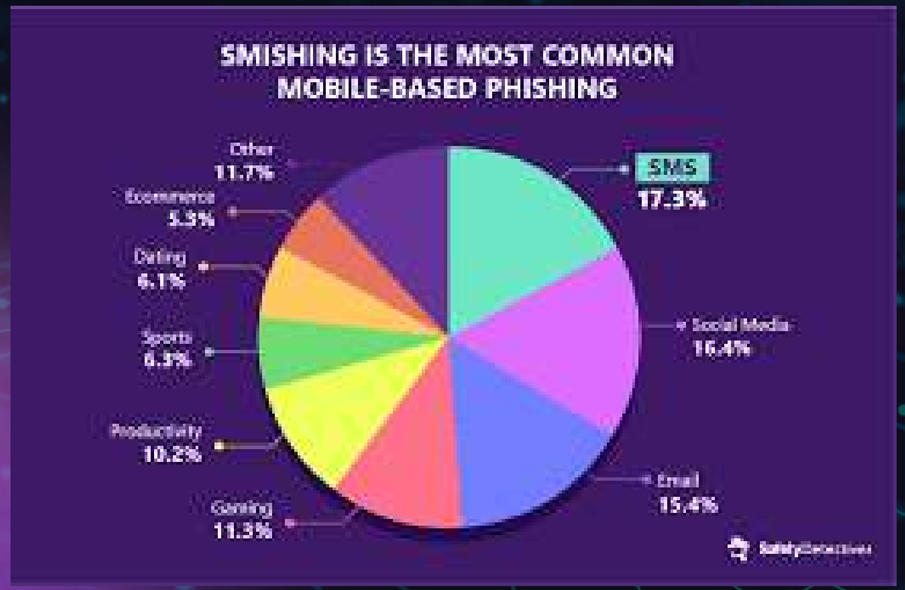
- Look for HTTPS (lock icon in browser) → but note: some fake sites also use HTTPS.
- Check the URL spelling carefully (e.g., www.paypal.com with an I instead of L).
- Use tools like Google Safe Browsing (transparencyreport.google.com).
- Be cautious of pop-ups asking for login details.



# Tricks Attackers Use

## Common Tactics

- Pretexting – Pretending to be someone you trust (boss, IT, HR).
- Baiting – Offering free downloads, USB drives, or fake offers.
- Spear Phishing – Personalized attacks targeting individuals/companies.
- Vishing – Voice phishing via fake phone calls.
- Smishing – Phishing via SMS messages with malicious links.




## Additional Tactics

- Quid Pro Quo – Attacker promises a benefit (e.g., free software/helpdesk support) in exchange for login details.
- Tailgating – Following someone into a restricted area by pretending to belong there.
- Watering Hole Attack – Setting up fake websites that the victim is likely to visit regularly.
- Business Email Compromise (BEC) – Fake emails appearing to be from executives or vendors requesting urgent payments.
- Clone Phishing – Copying a real, previously delivered email but swapping the links/attachments with malicious ones.

## Most Commonly Used (Top 3)

- Phishing Emails – The #1 method (used in >80% of attacks).
- Spear Phishing – Highly effective because it's personalized.
- Vishing & Smishing – Growing fast with mobile phone users.

# Protect Yourself from Phishing

## Email & Link Safety

- Do not click on links in suspicious emails.
- Hover over links before clicking → check if they match the official website.
- Never download attachments from unknown senders.
- Be cautious of shortened URLs (use a URL expander tool to preview).

## Password Security

- Use strong, unique passwords for each account.
- Change passwords regularly.
- Enable Multi-Factor Authentication (MFA) for all important accounts.
- Never share your password with anyone.

## Workplace & Personal Safety

- Report suspicious emails immediately to IT/security teams.
- Don’t overshare personal information on social media (attackers use it for spear phishing).
- Be aware of phone scams (vishing) and text scams (smishing).

## System & Device Security

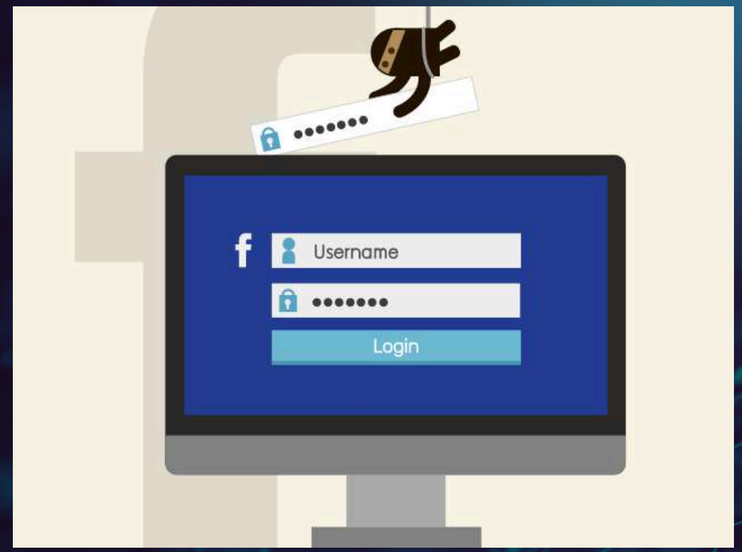
- Keep your operating system, browser, and antivirus updated.
- Install trusted security software and enable firewalls.
- Avoid using public Wi-Fi for banking or sensitive logins (use VPN if necessary).

## Verification Habits

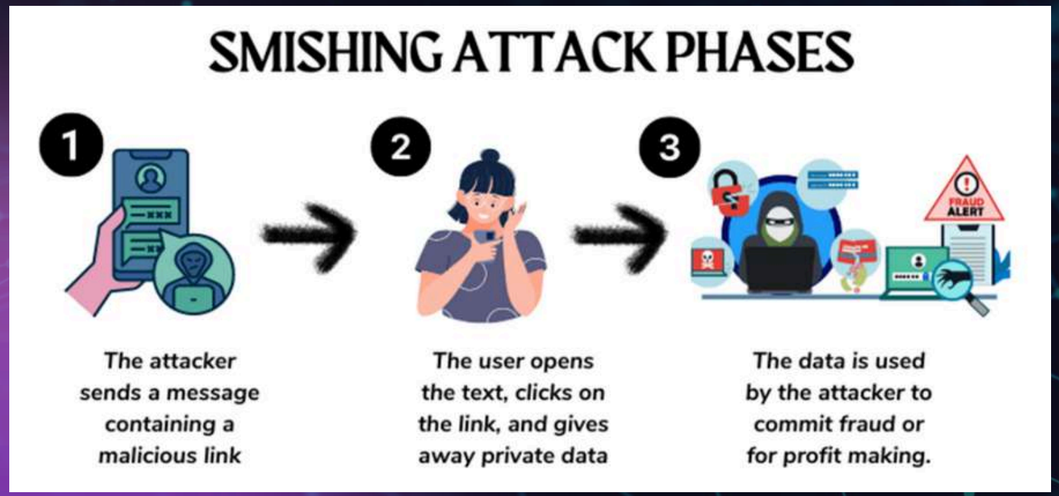
- Verify suspicious emails by contacting the company through their official website/helpline.
- Double-check sender addresses, especially for financial requests.
- If something feels “too urgent” or “too good to be true” → it probably is fake.

# Case Study - Real Phishing Attack

## Google & Facebook Phishing Scam (2013–2015




- Scenario: A Lithuanian cybercriminal named Evaldas Rimasauskas posed as a large Asian hardware supplier (Quanta Computer).
- Tactic Used: Business Email Compromise (BEC) – He sent fake invoices and contracts to Google and Facebook's finance teams using spoofed emails that looked legitimate.
- Result: Both tech giants were tricked into wiring more than $100 million to fraudulent bank accounts.
- Prevention Tip:
- Always verify payment requests via a secondary channel (e.g., phone call).
- Use strict vendor verification processes.
- Train employees to recognize BEC scams.




## UK HMRC Smishing Scam (2019)

- Scenario: UK citizens received fake SMS messages claiming to be from "HMRC" (tax authority) offering tax refunds.
- Tactic Used: Smishing – The SMS contained links to a fake HMRC site that collected victims' banking details.
- Result: Thousands of people entered sensitive data, leading to financial theft.
- Prevention Tip:
- Government agencies never ask for sensitive info via SMS.
- Always access tax/banking portals by typing the official URL manually.

# Test Your Awareness

Q1: You get an email saying: “Your account will be closed unless you click this link.”

- A) Click the link quickly.
- B) Ignore or report the email. ✅
- C) Reply with personal details.

Q2: A website looks like PayPal but the URL is paypall-login.com. What is this?

- A) Real website.
- B) Fake phishing site. ✅

Q3: Your boss emails you asking for gift cards urgently, but the email is from a Gmail address. What should you do?

- A) Buy and send the gift cards.
- B) Verify through a phone call. ✅
- C) Reply directly to the email.

# Stay Aware, Stay Safe

- Always think before you click.
- Double-check emails, links, and websites.
- Use security features like MFA.
- Report suspicious activity immediately.
- Remember: You are the first line of defense against phishing.

# THANK YOU!

FOR ANY QUERY

Email - ankitaghoshal38@gmail.com