



# PHISHING AWARENESS TRAINING

PROTECT YOURSELF AND YOUR ORGANIZATION

MUHAMMAD QASIM @CODEALPHA

# WHAT IS PHISHING?

- **Definition:** Phishing is a type of cyber attack where attackers impersonate legitimate organizations via email, text message, or other communication channels to steal sensitive information.
- **Types of Phishing Attacks:**
  - Email Phishing
  - Spear Phishing
  - Whaling
  - Smishing (SMS Phishing)
  - Vishing (Voice Phishing)

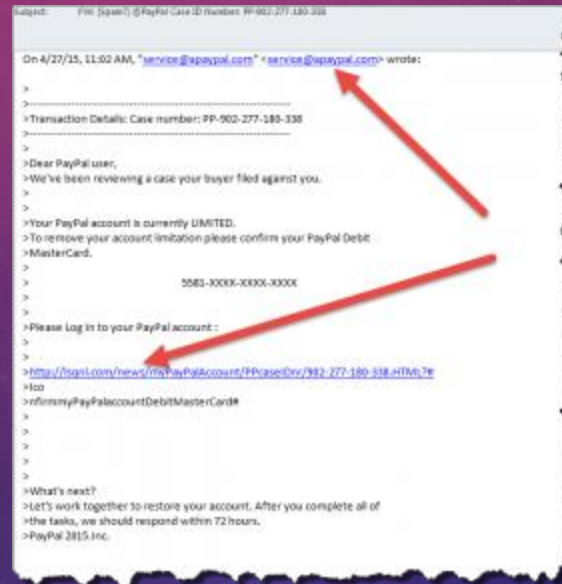




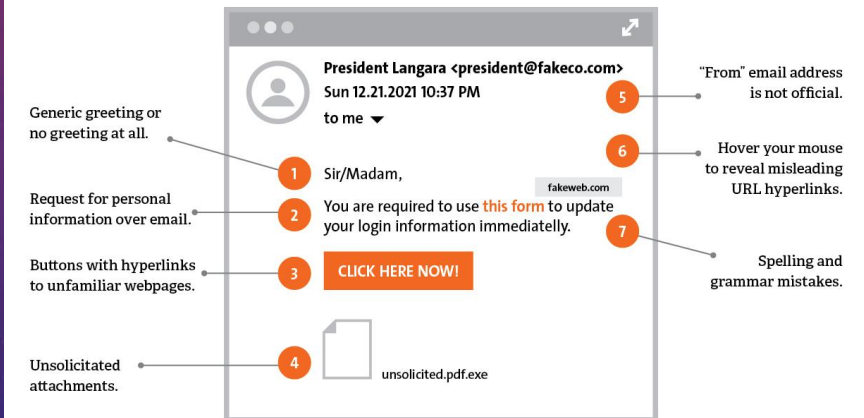
# HOW TO SPOT PHISHING EMAILS

## Common Signs:

- Suspicious sender addresses
- Poor grammar and spelling
- Urgent or threatening language
- Unusual attachments or links

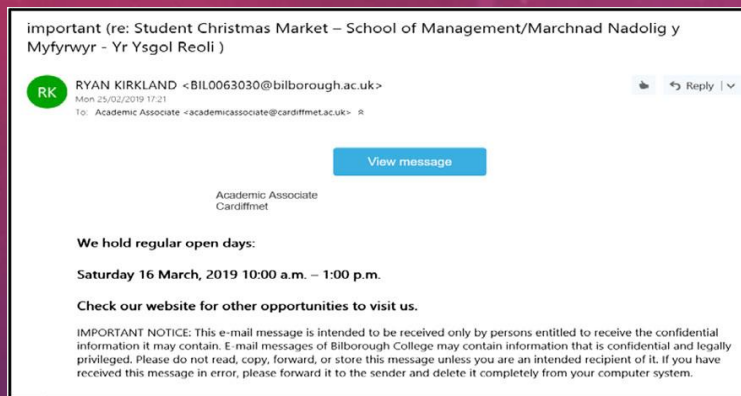


## Seven signs of a phishing email.



Adapted from SecurityMetrics, 7 Signs of a Phishing Email

# REAL-LIFE EXAMPLES



FROM: [accounts@paypal.com](mailto:accounts@paypal.com)

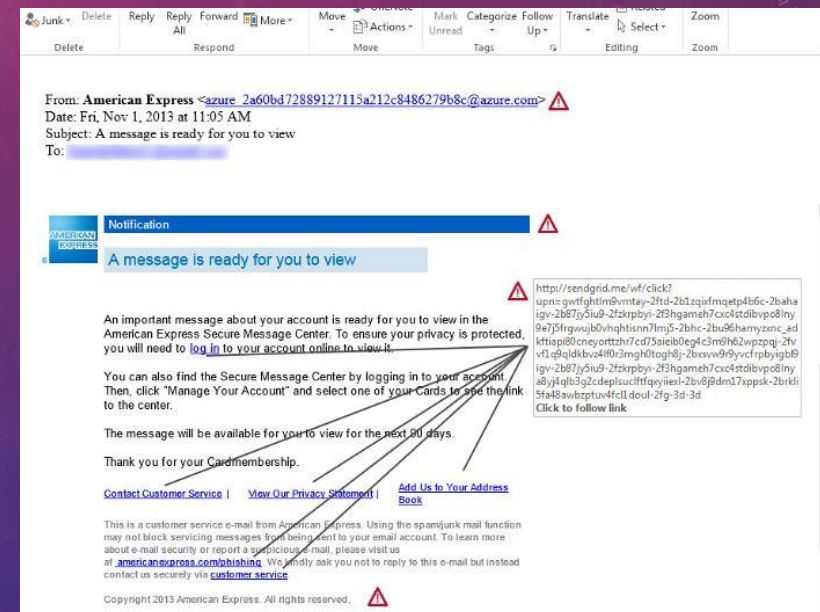
SUBJECT: Suspicious account activity

Dear Customer,

We have detected suspicious behaviour on your PayPal account. As such we have suspended all activity on your account until your recent transactions can be verified. To resolve this issue please visit [www.paypal.com](http://www.paypal.com) and log in using your username and secure password. Please note that your account will remain suspended until this issue is resolved.

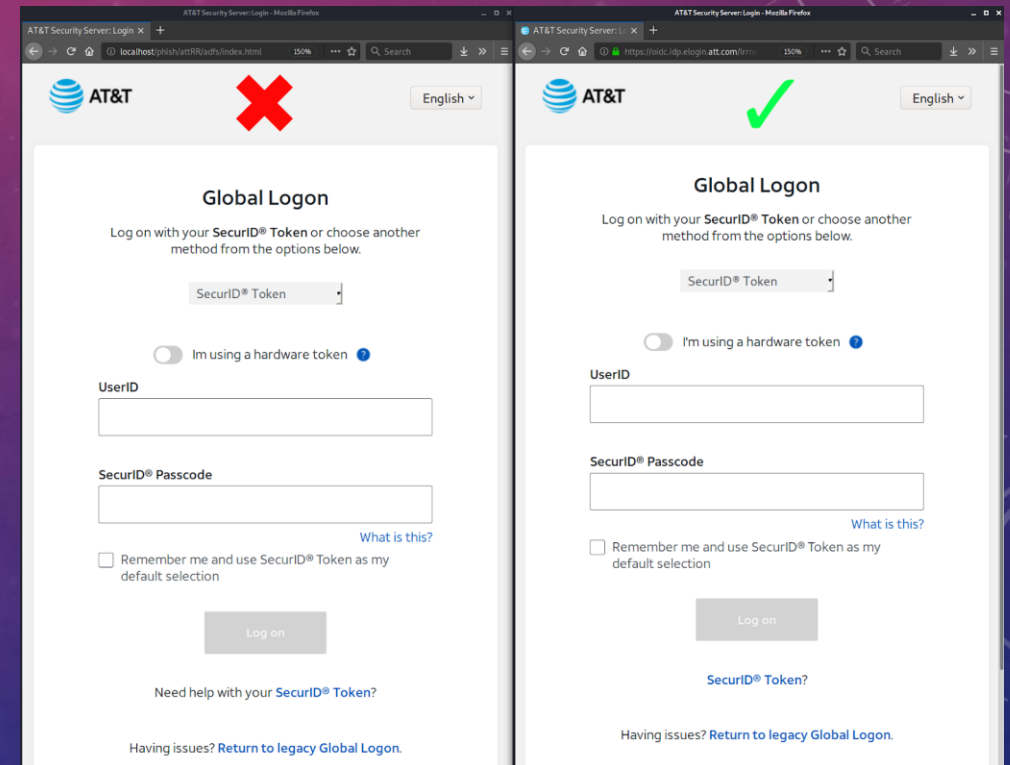
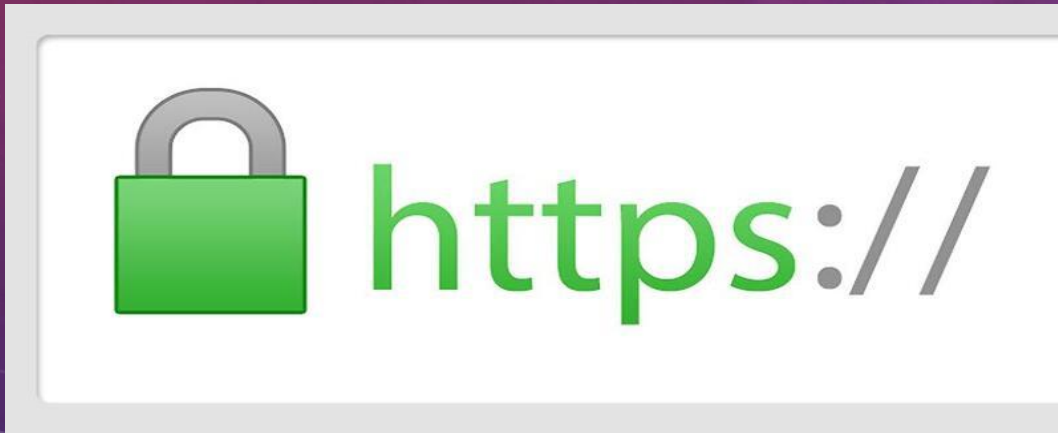
Regards,

PayPal Account Team



# IDENTIFYING PHISHING WEBSITES

- **Checking URL Legitimacy:** Hover over links to check the actual URL
- **Look for HTTPS:** Ensure the site uses HTTPS





# PHISHING WEBSITE EXAMPLES

A screenshot of a web browser displaying a phishing page designed to look like the PayPal login interface. The browser's address bar shows the URL "paypal--accounts.com" with a "Not Secure" warning. The page features the PayPal logo at the top. Below it are two input fields: "Email or mobile number" and "Password". At the bottom is a blue "Log In" button.

A screenshot of a web browser displaying a phishing page designed to look like the Facebook sign-up page. The browser's address bar shows the URL "www.sanagustinturismo.co/Facebook/". The page has a blue header with the Facebook logo and a login section with "Email" and "Password" fields. Below the header, there is a promotional banner for the Facebook mobile app. To the right, there is a "Sign up" section with fields for Name, Surname, Your email, Re-enter your email address, Password, Gender, and Date of Birth (Day, Month, Year). A "Sign up" button is at the bottom.

A screenshot of a web browser displaying a phishing page designed to look like the Bank of America sign-in page. The browser's address bar shows the URL "secure.bankofamerica.com/login/sign-in/signon2screenixombd.com". The page features the Bank of America logo and a "Sign In" button. Below the logo is a red banner that says "Your Online ID". There is a section for "Please enter your Online ID" with a text input field and a "Sign In" button. To the right, there is a "Quick help module" with links for "Where do I enter my Passcode" and "Forgot or need help with my Online ID". At the bottom, there is a "Secure area" section with links for "Privacy & Security" and "Service Agreement".

# HOW TO AVOID PHISHING ATTACKS

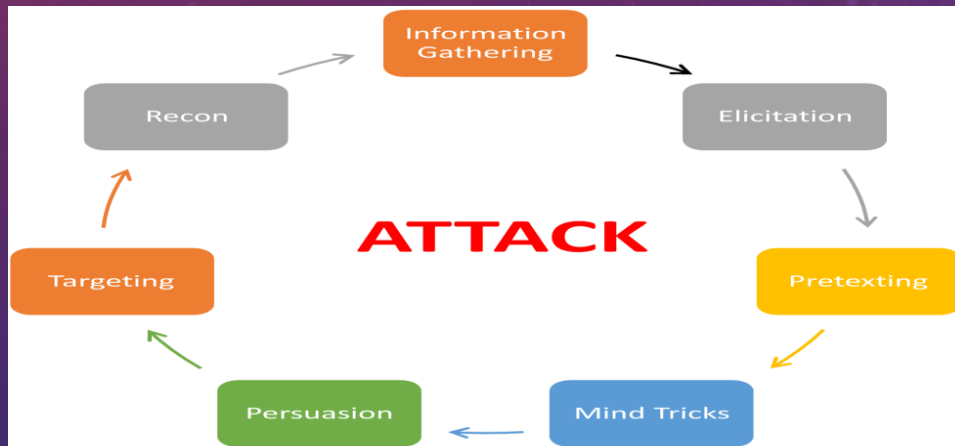
- Do not click on suspicious links
- Verify the sender before providing personal information
- Use anti-phishing tools and software
- Regularly update your software and security settings



# UNDERSTANDING SOCIAL ENGINEERING

## Common Techniques:

- Pretexting
- Baiting
- Quid Pro Quo
- Tailgating



- **Incident:** In 2016, a group of hackers used social engineering to trick an employee at a large technology company into revealing sensitive information.
- **Technique:** Pretexting - The attackers posed as IT support staff and contacted the employee, claiming they needed to verify the employee's login credentials due to a supposed security issue.
- **Outcome:** The employee, believing the request was legitimate, provided their login details. The attackers then used this information to gain access to the company's internal network, resulting in a significant data breach.
- **Lesson:** Always verify the identity of individuals requesting sensitive information, even if they appear to be from within the organization.



# HOW TO REPORT PHISHING ATTACKS

- **Do Not Interact:** Do not click any links or download any attachments from the suspected phishing message.
- **Collect Evidence:** Take a screenshot of the email or website, including the URL and any suspicious elements.
- **Report Internally:**
  - Forward the email to your IT or security team.
  - Include any relevant details about how you received the message and any actions you took.
- **Report Externally:**
  - For emails: Forward the email to the Anti-Phishing Working Group at [reportphishing@apwg.org](mailto:reportphishing@apwg.org).
  - For websites: Report the URL to Google Safe Browsing or Microsoft SmartScreen.
- **Follow Up:** Monitor for any response or further instructions from your IT or security team.



# CONCLUSION AND QUESTIONS

## Summary of Key Points:

- **Phishing Awareness:** Understanding what phishing is and the different types of attacks.
- **Recognition:** Identifying the signs of phishing emails and websites.
- **Prevention:** Steps to avoid falling victim to phishing attacks.
- **Social Engineering:** Awareness of common social engineering tactics.
- **Reporting:** Knowing how to report phishing incidents effectively.

## Closing Remarks:

- Thank you for participating in the training.
- Stay vigilant and always verify the authenticity of suspicious messages.





# THANK YOU

PRESENTED BY :  
MUHAMMAD QASIM - AS PART  
OF CODEALPHA INTERNSHIP