
PHISHING AWARENESS TRAINING
PROTECT YOURSELF AND YOUR ORGANIZATION
MUHAMMAD QASIM @CODEALPHA

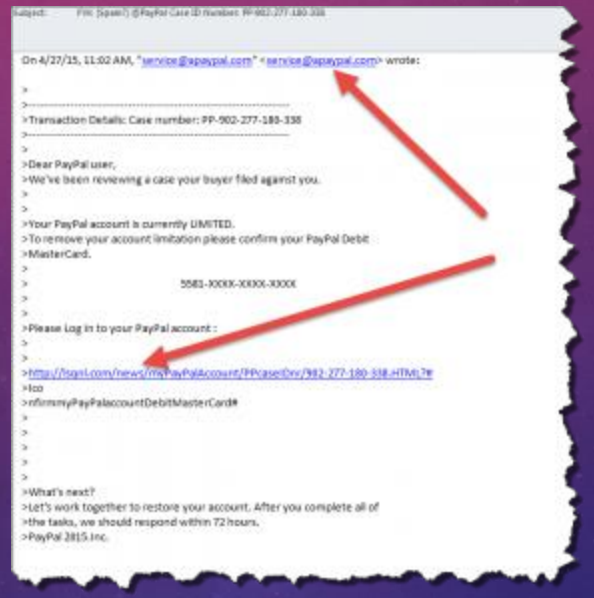
WHAT IS PHISHING?

- **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)

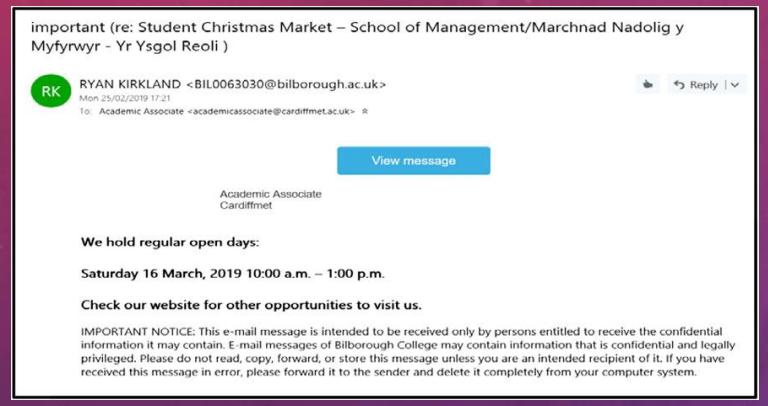
HOW TO SPOT PHISHING EMAILS

Common Signs:

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



REAL-LIFE EXAMPLES



important (re: Student Christmas Market – School of Management/Marchnad Nadolig y Myfyrwyr - Yr Ysgol Reoli)

RK RYAN KIRKLAND <BIL0063030@bilborough.ac.uk>
Mon 25/02/2019 17:21
To: Academic Associate <academicassociate@cardiffmet.ac.uk>

Reply

View message

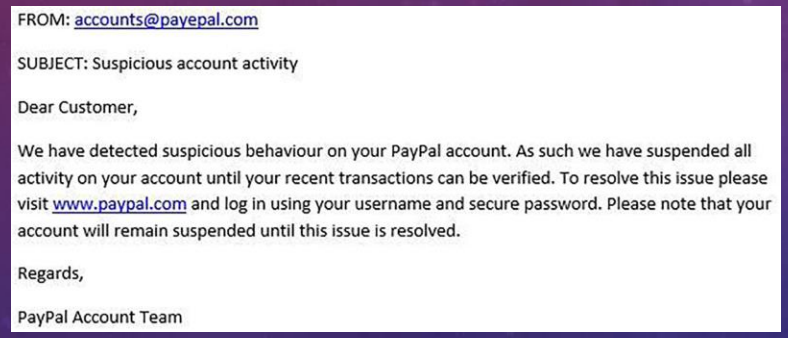
Academic Associate
Cardiffmet

We hold regular open days:

Saturday 16 March, 2019 10:00 a.m. – 1:00 p.m.

Check our website for other opportunities to visit us.

IMPORTANT NOTICE: This e-mail message is intended to be received only by persons entitled to receive the confidential information it may contain. E-mail messages of Bilborough College may contain information that is confidential and legally privileged. Please do not read, copy, forward, or store this message unless you are an intended recipient of it. If you have received this message in error, please forward it to the sender and delete it completely from your computer system.



FROM: accounts@payepal.com

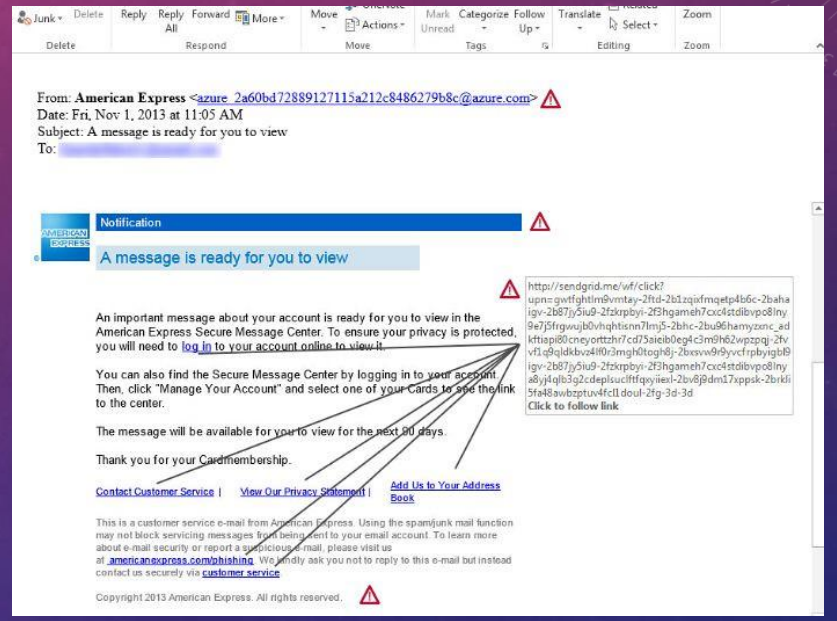
SUBJECT: Suspicious account activity

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 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



Junk Delete | Reply Reply All Forward More | Move Actions | Mark Unread Categorize Follow Up | Translate Select | Zoom

From: **American Express** <azure_2a60bd72889127115a212c8486279b8c@azure.com>
Date: Fri, Nov 1, 2013 at 11:05 AM
Subject: A message is ready for you to view
To:

Notification

A message is ready for you to view

http://sendgrid.me/wf/click?upn=gwtfghtlm9vmtay-2ftd-2b1zqixfmqetp4b6c-2bahaigv-2b87jy5iu9-2fzkrpbyi-2f3hgameh7cxc4stdibvpo8lny9e7j5frgwvujb0vhqhtisnn7lmj5-2bhc-2bu96hamyzxnc_adkftiapi80cneyorttzhr7cd75aieib0eg4c3m9h62wpzpqj-2fvvf1q9qldkbvz4lf0r3mgh0togh8j-2bxsvw9r9yvcfrpbyigbl9igv-2b87jy5iu9-2fzkrpbyi-2f3hgameh7cxc4stdibvpo8lnya8yj4qlb3g2cdeplsuclftfqxyiiexl-2bv8j9dm17xppsk-2brkli5fa48awbzptuv4fcl1doul-2fg-3d-3d
Click to follow link

An important message about your account is ready for you to view in the American Express Secure Message Center. To ensure your privacy is protected, you will need to log in to your account online to view it.

You can also find the Secure Message Center by logging in to your account. Then, click "Manage Your Account" and select one of your Cards to see the link to the center.

The message will be available for you to view for the next 90 days.

Thank you for your Cardmembership.

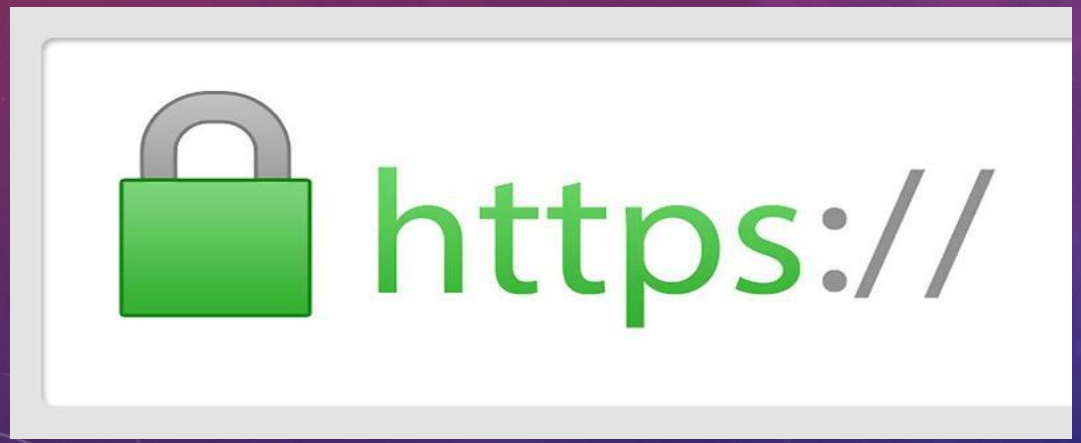
Contact Customer Service | View Our Privacy Statement | Add Us to Your Address Book

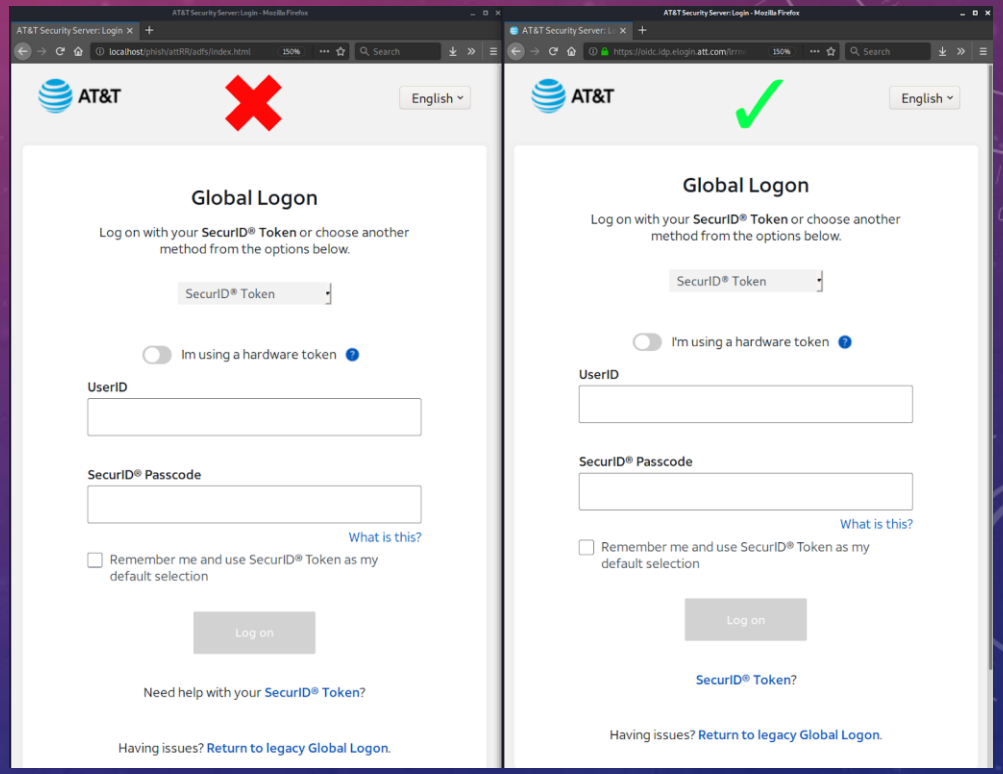
This is a customer service e-mail from American Express. Using the spam/junk mail function may not block servicing messages from being sent to your email account. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us securely via customer service.

Copyright 2013 American Express. All rights reserved.

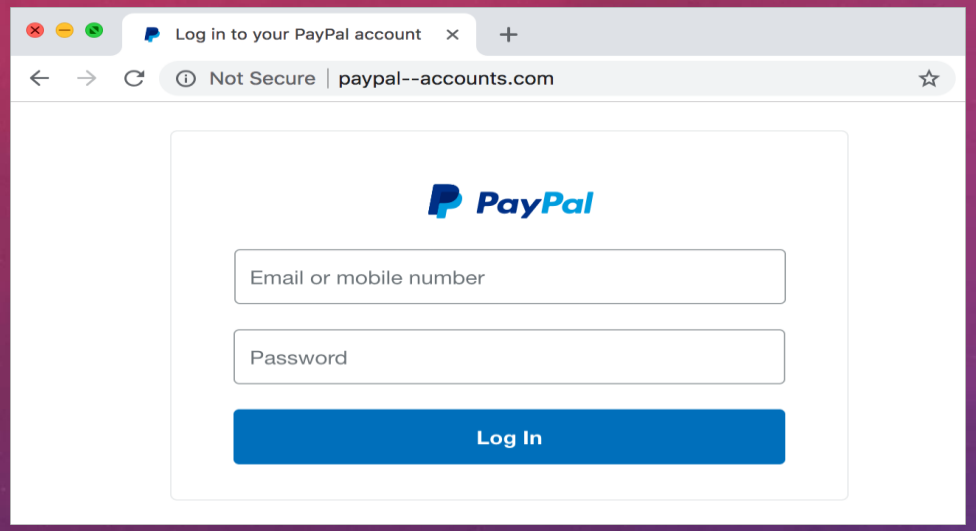
IDENTIFYING PHISHING WEBSITES

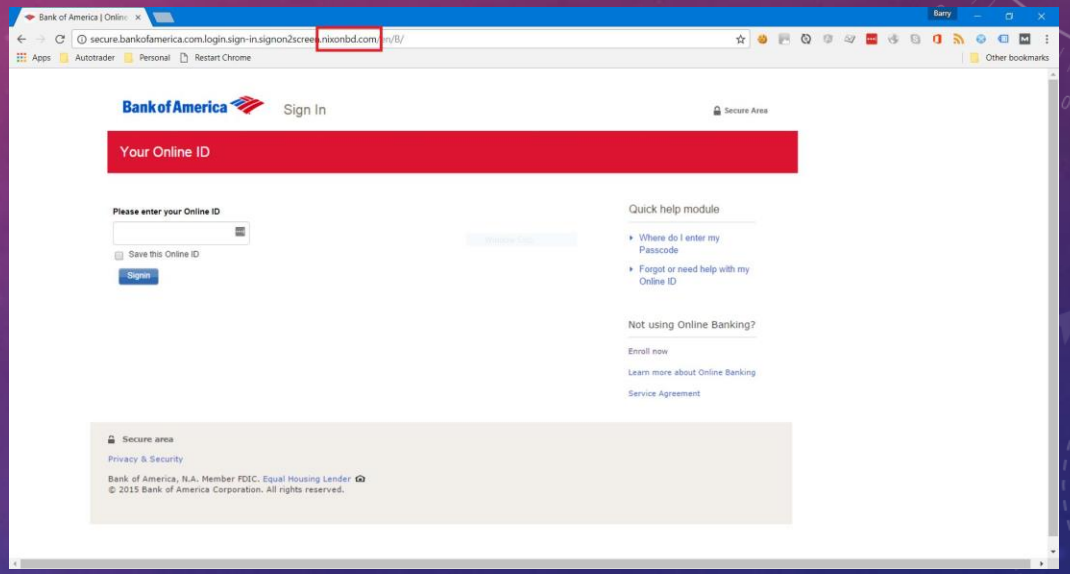
- **Checking URL Legitimacy**: Hover over links to check the actual URL
- **Look for HTTPS**: Ensure the site uses HTTPS

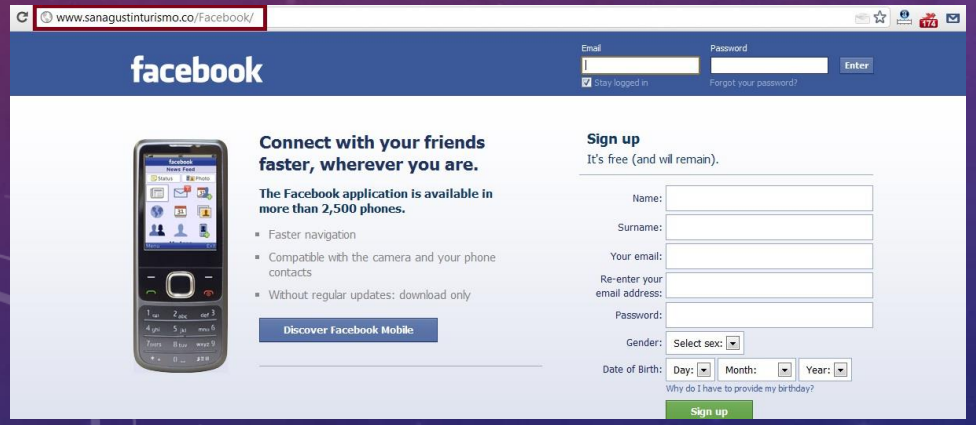




PHISHING WEBSITE EXAMPLES







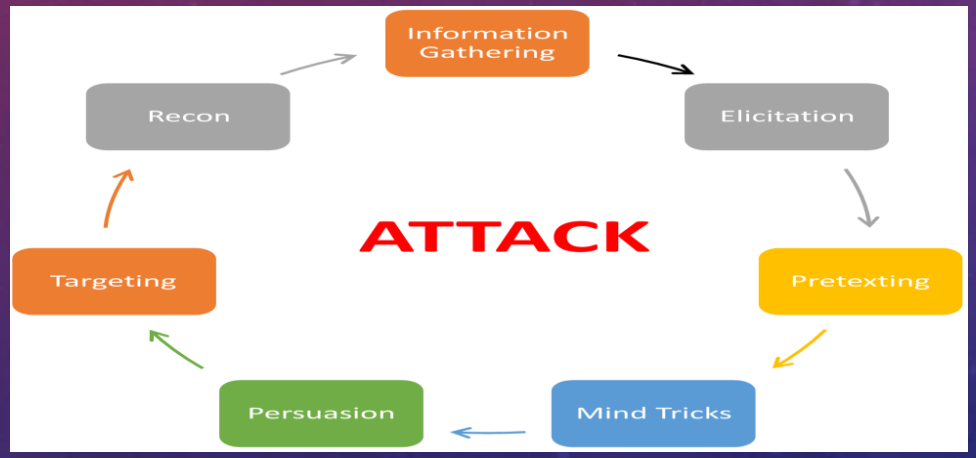
HOW TO AVOID PHISHING ATTACKS

- 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.
- 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

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