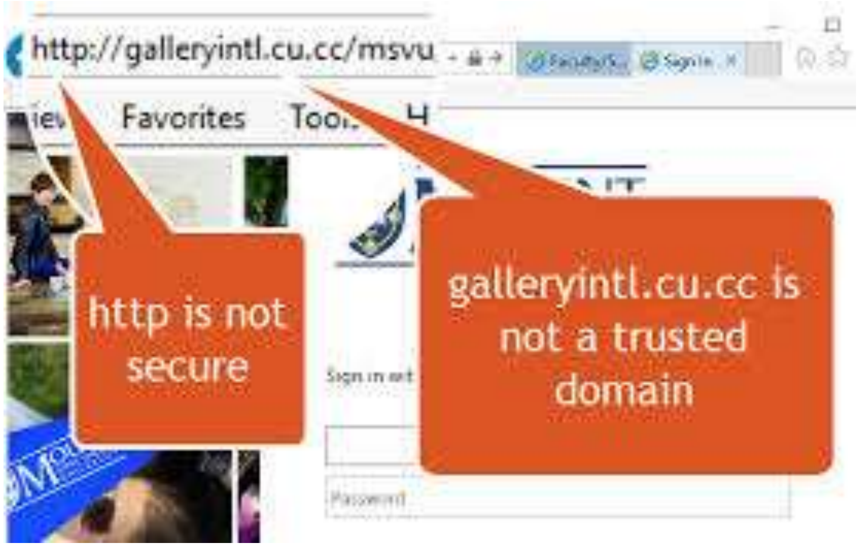
Phishing Awareness: Don’t Get Hooked!

*A Cyber Security Internship Project by **Sai Tarun***

***Presented for:** CodeAlpha Internship Program*

What is Phishing?

•Phishing is a **deceptive attempt to trick individuals** into revealing personal or financial information through fake communication, often via **email, SMS, or websites**.



http is not secure

galleryintl.cu.cc is not a trusted domain

•Mimics trusted brands or people.

•Creates urgency or fear.

•A leading cause of data breaches.

Types of Phishing Attacks

- **Email Phishing:** Mass emails pretending to be from trusted services.
- **Spear Phishing:** Personalized attacks on individuals.
- **Whaling:** Targeting top executives.
- **Smishing:** Phishing via SMS.
- **Vishing:** Voice-based phishing (fake calls).

How to Recognize Phishing

✕ **Suspicious sender address** (e.g., support@paypa1.com)

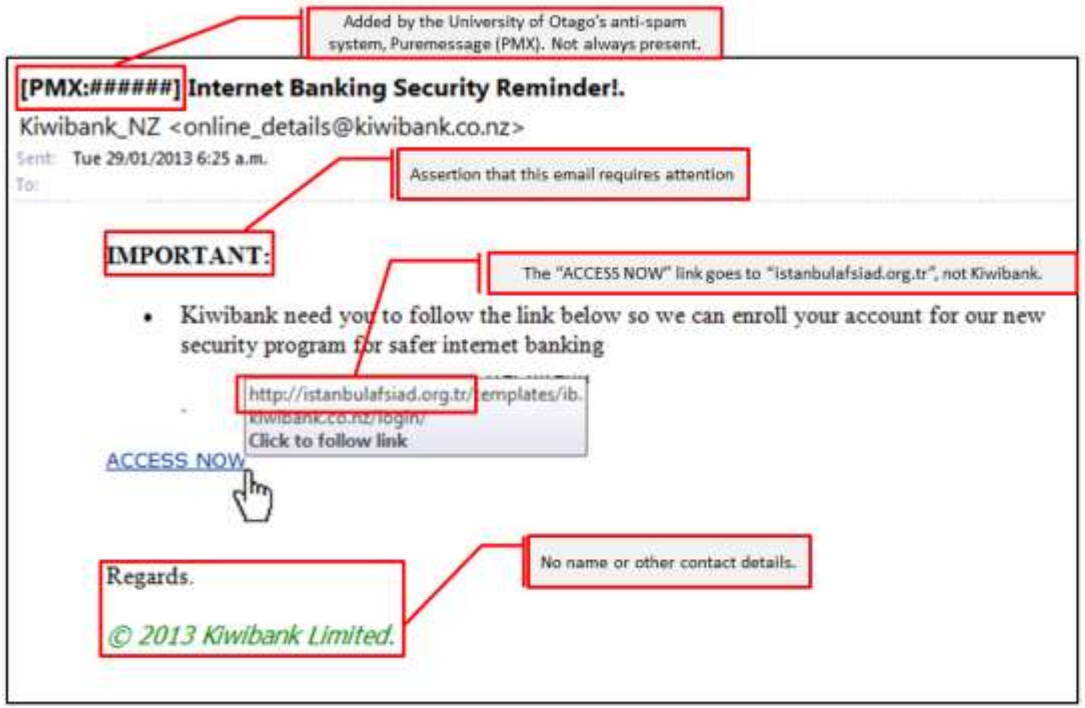
✕ **Spelling and grammar mistakes**

✕ **Generic greetings** like “Dear User” or “Valued Customer”

✕ **Links that don’t match the real site** (hover to check!)

✕ **Urgent threats** like “Account will be blocked in 24 hrs!”

✕ **Unexpected attachments or pop-ups**



Added by the University of Otago’s anti-spam system, Puremessage (PMX). Not always present.

[PMX:######] Internet Banking Security Reminder!.

Kiwibank_NZ <online_details@kiwibank.co.nz>

Sent: Tue 29/01/2013 6:25 a.m.

To:

Assertion that this email requires attention

IMPORTANT:

The “ACCESS NOW” link goes to “istanbulafsiad.org.tr”, not Kiwibank.

- Kiwibank need you to follow the link below so we can enroll your account for our new security program for safer internet banking

http://istanbulafsiad.org.tr/templates/ib.
kiwibank.co.nz/login/
Click to follow link

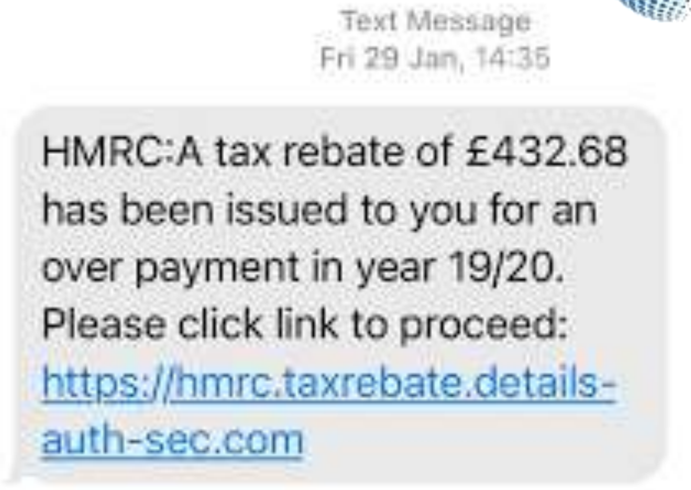
ACCESS NOW

Regards.

© 2013 Kiwibank Limited.

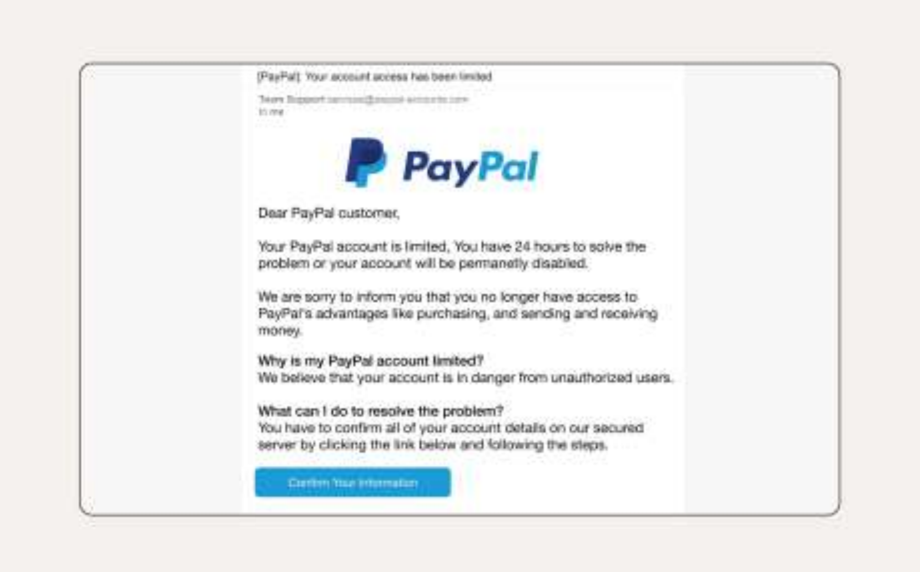
No name or other contact details.

Real-World Examples



Text Message
Fri 29 Jan, 14:35

HMRC:A tax rebate of £432.68 has been issued to you for an over payment in year 19/20. Please click link to proceed: https://hmrc.taxrebate.details-auth-sec.com



[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

- A fake PayPal email with “Click here to secure your account”.
- A cloned bank login page.
- A fake job offer email.

Quiz - Test Your Awareness!

01

Q1: What is a common sign of a phishing email?
A) Uses personal greeting
B) Contains urgent threats
C) Comes from your manager

02

Q2: What should you do if you receive a suspicious email?
A) Open and inspect it
B) Click the link to check
C) Report or delete it

03

Q3: What is “vishing”?
A) Voice phishing
B) SMS phishing
C) Email with viruses

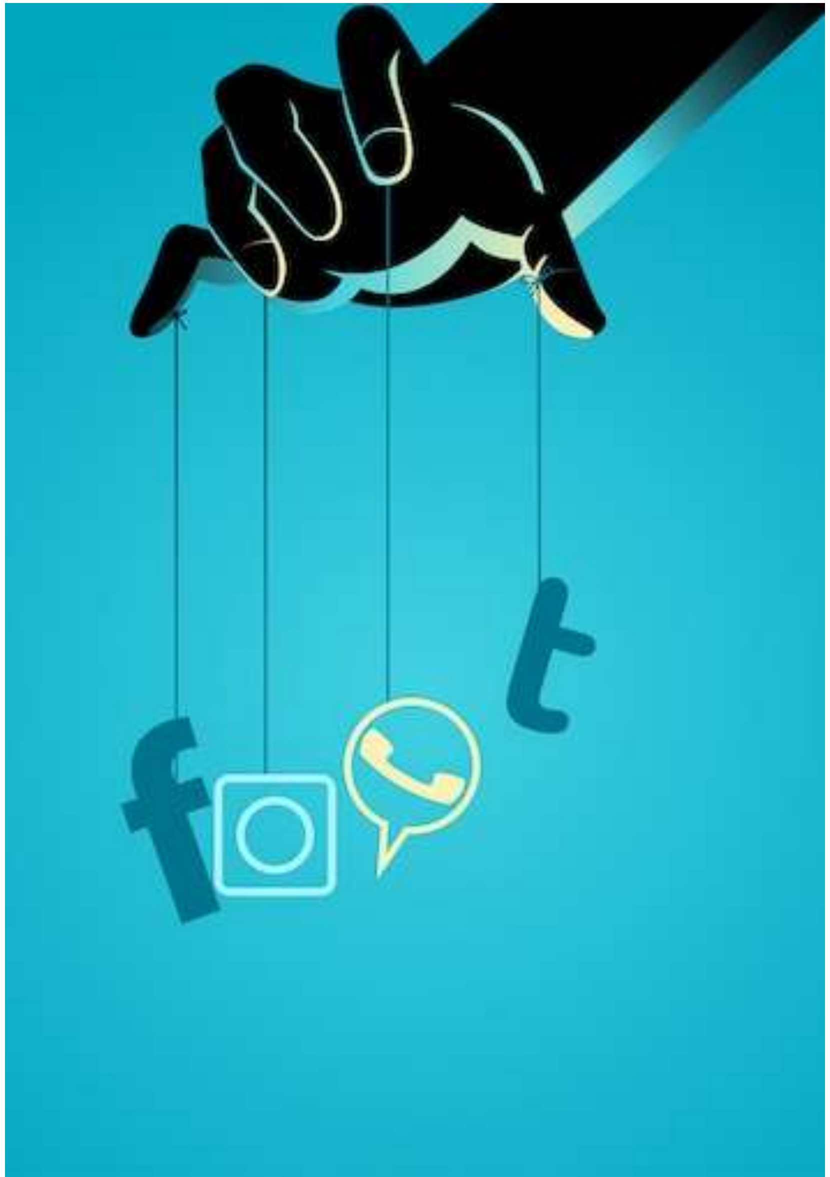
Answers :
Q1 : B
Q2 : C
Q3 : A

Social Engineering Tactics

Phishing works by **manipulating human behavior**, not just technology.

Common tactics:

- **Fear/Urgency:** "Account blocked!"
- **Reward:** "You’ve won a voucher!"
- **Authority:** "From your bank CEO"
- **Curiosity:** "See who viewed your profile"



Best Practices to Avoid Phishing

- Type URLs manually
- Enable 2-Factor Authentication
- Don’t open unknown attachments
- Always verify sender
- Report phishing attempts

Tools to Detect Phishing

Top Tools:

PhishTank – Real-time phishing database

VirusTotal – Scans URLs/files

Google Safe Browsing

WOT (Web of Trust)

Gmail/Outlook Spam Filters

Conclusion

- Stay informed, stay cautious.
- Think before you click!
- Share knowledge with your friends/family.
- Report phishing emails to protect your organization.

“**Awareness is the first step in cybersecurity.**”

References

Content:

- https://www.phishing.org
- https://www.cyber.gov.au
- https://www.consumer.ftc.gov
- Microsoft Security Intelligence Reports
- Proofpoint 2023 Phishing Report