PHISHING EMAIL DETECTION & AWARENESS REPORT

CYBER SECURITY INTERNSHIP – TASK 2

CYBER SECURITY REPORT
FUTURE INTERNS PROGRAM
PREPARED BY
MAHADEV SAI CHANDRA

Introduction

PHISHING IS A SOCIAL ENGINEERING ATTACK WHERE CYBERCRIMINALS ATTEMPT TO TRICK USERS INTO REVEALING SENSITIVE INFORMATION SUCH AS PASSWORDS, BANKING DETAILS, OR PERSONAL DATA. THIS REPORT ANALYZES SAMPLE EMAILS TO IDENTIFY PHISHING INDICATORS AND EDUCATE USERS ON HOW TO RECOGNIZE AND AVOID SUCH THREATS.

TOOLS USED

- MANUAL EMAIL ANALYSIS
- PUBLIC PHISHING AWARENESS EXAMPLES
- VISUAL INSPECTION OF EMAIL CONTENT

METHODOLOGY

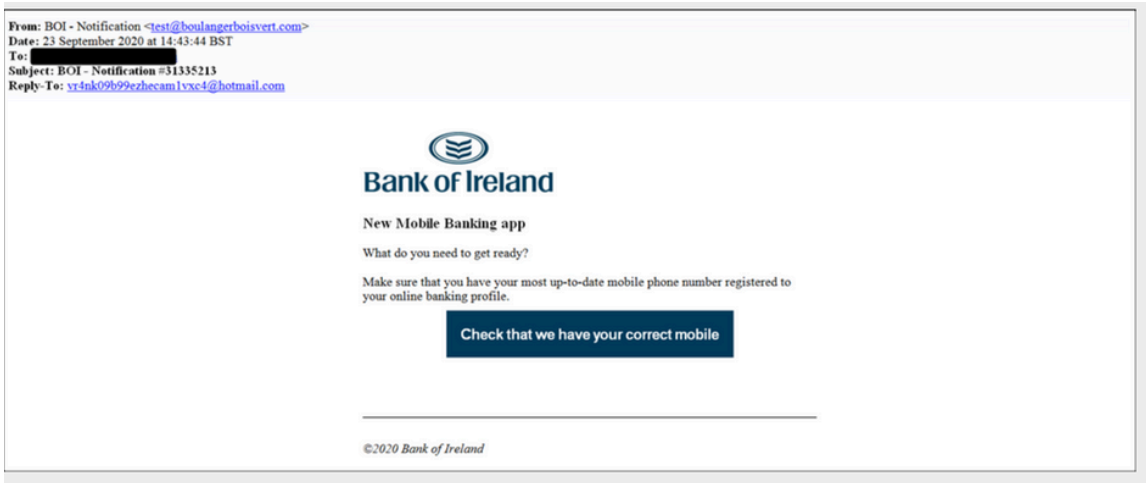
THE ANALYSIS WAS CONDUCTED BY REVIEWING EMAIL CONTENT, SENDER DETAILS,
AND EMBEDDED LINKS. EACH EMAIL WAS CLASSIFIED AS PHISHING OR SAFE
BASED ON COMMON PHISHING INDICATORS. NO REAL USER INTERACTION WAS
PERFORMED.

MAIL CLASSIFICATION SUMMARY (TABLE)

Email	Key Indicators	Classification
Bank of Ireland alert	Fake sender, misleading link	Phishing
365 credit card notice	Urgency, fake URL	Phishing
Amazon gift card info	Legit sender, no threat	Safe

CASE STUDY - 1

Phishing Email Example – Bank of Ireland



CLASSIFICATION: PHISHING

PHISHING INDICATORS IDENTIFIED:

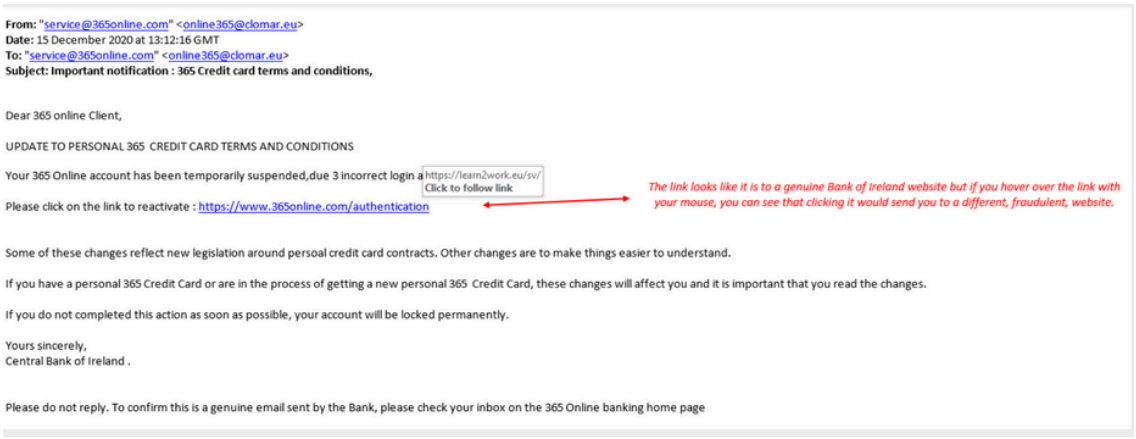
- SPOOFED SENDER EMAIL ADDRESS
- MISMATCHED REPLY-TO ADDRESS
- FAKE BANKING REQUEST
- EMBEDDED MISLEADING LINK

RISK EXPLANATION (SIMPLE LANGUAGE):

IF A USER CLICKS THE LINK, ATTACKERS MAY STEAL BANKING CREDENTIALS, LEADING TO FINANCIAL LOSS AND ACCOUNT COMPROMISE.

CASE STUDY - 2

Phishing Email Example – Credit Card Update



From: "service@365online.com" <online365@clomar.eu>
Date: 15 December 2020 at 13:12:16 GMT
To: "service@365online.com" <online365@clomar.eu>
Subject: Important notification : 365 Credit card terms and conditions,

Dear 365 online Client,

UPDATE TO PERSONAL 365 CREDIT CARD TERMS AND CONDITIONS

Your 365 Online account has been temporarily suspended,due 3 incorrect login a https://learn2work.eu/sv/
Click to follow link

Please click on the link to reactivate : https://www.365online.com/authentication

The link looks like it is to a genuine Bank of Ireland website but if you hover over the link with your mouse, you can see that clicking it would send you to a different, fraudulent, website.

Some of these changes reflect new legislation around persoal credit card contracts. Other changes are to make things easier to understand.

If you have a personal 365 Credit Card or are in the process of getting a new personal 365 Credit Card, these changes will affect you and it is important that you read the changes.

If you do not completed this action as soon as possible, your account will be locked permanently.

Yours sincerely,
Central Bank of Ireland .

Please do not reply. To confirm this is a genuine email sent by the Bank, please check your inbox on the 365 Online banking home page

CLASSIFICATION: PHISHING

PHISHING INDICATORS IDENTIFIED:

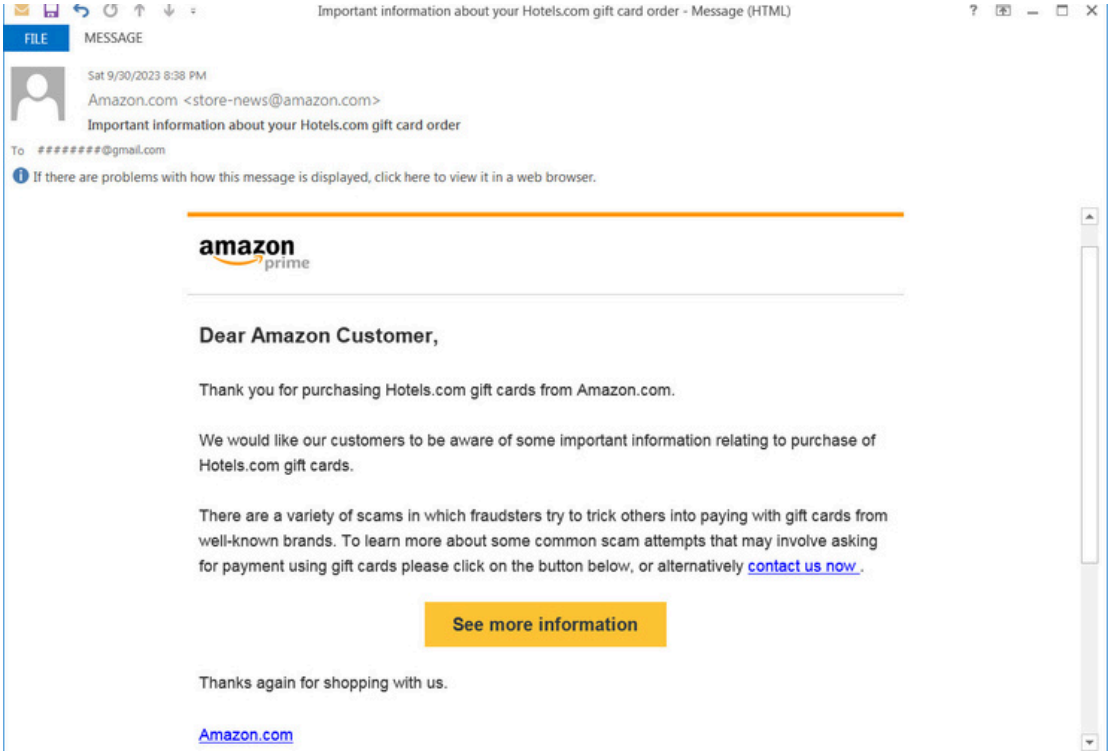
- URGENT LANGUAGE CREATING FEAR
- SUSPICIOUS LINK REDIRECTING TO A FAKE WEBSITE
- GENERIC GREETING
- UNOFFICIAL SENDER DOMAIN

RISK EXPLANATION:

THIS EMAIL ATTEMPTS TO PRESSURE USERS INTO CLICKING A MALICIOUS LINK, WHICH COULD RESULT IN STOLEN PERSONAL OR FINANCIAL INFORMATION.

CASE STUDY - 3

Legitimate Email Example – Amazon



CLASSIFICATION: SAFE

Legitimate Indicators Observed:

- Official sender domain (amazon.com)
- Informational message only
- No request for passwords or OTP
- No urgent or threatening language

Security Assessment:

This email is a legitimate notification and does not pose a phishing risk. It follows safe communication practices.

PHISHING PREVENTION & AWARENESS

- Always verify sender email addresses
- Do not click suspicious or shortened links
- Avoid emails with urgent threats or pressure
- Legitimate organizations never ask for passwords via email
- Enable multi-factor authentication
- Report suspicious emails immediately

CONCLUSION

This analysis demonstrates how phishing emails differ from legitimate communications. By recognizing common phishing indicators and following basic security practices, users can significantly reduce the risk of falling victim to email-based attacks. User awareness remains the strongest defense against phishing.