Task 03: Phishing Email Identification and Handling Report:

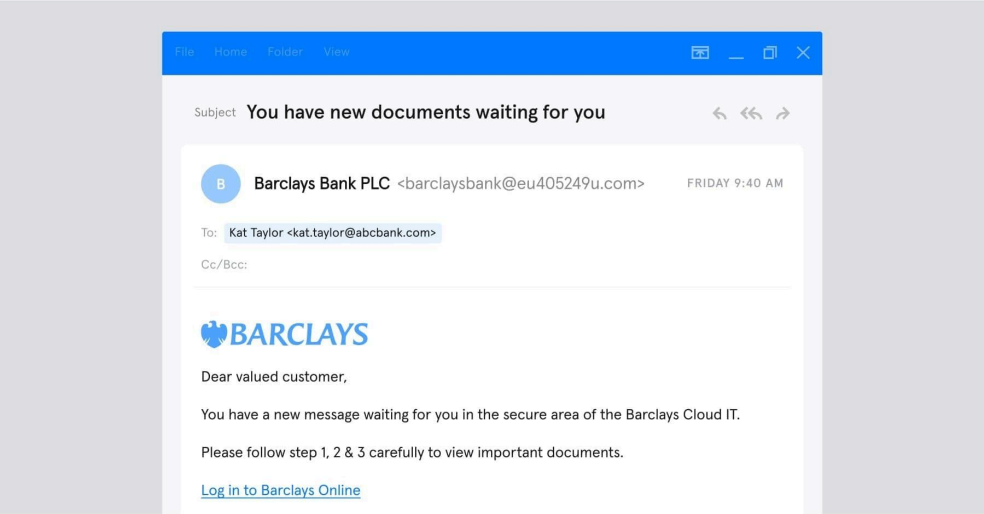
Task Title: Recognize and Handle Phishing Attempts

Introduction:

Phishing attacks are a prevalent form of cybercrime in which malicious actors attempt to deceive individuals into revealing sensitive information, such as login credentials, personal data, or financial information. This report aims to educate individuals on the common signs of phishing emails, provide best practices for recognizing and handling them, and explain how to report such incidents effectively.

Common Signs of Phishing Emails:

1. **Suspicious Sender's Email Address:**



Subject You have new documents waiting for you

Barclays Bank PLC <barclaysbank@eu405249u.com> FRIDAY 9:40 AM

To: Kat Taylor <kat.taylor@abcbank.com>

Cc/Bcc:

Dear valued customer,

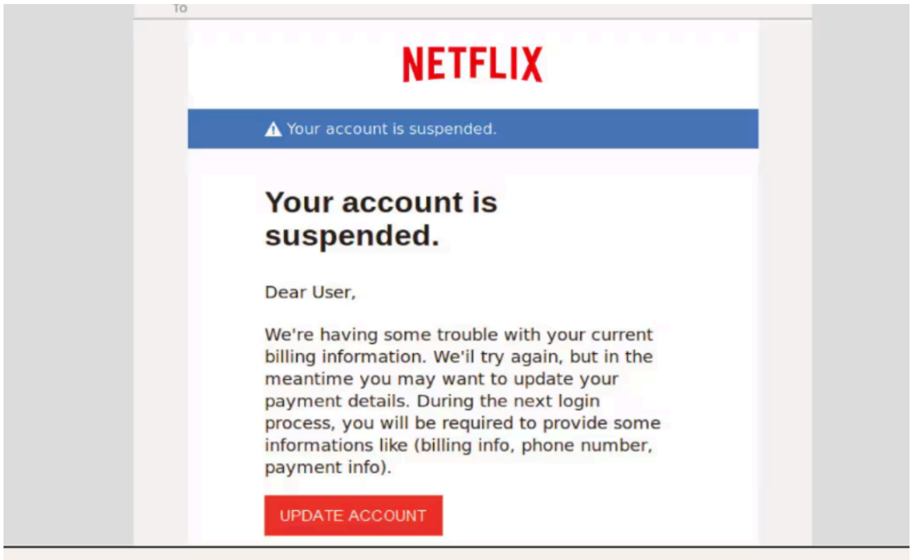
You have a new message waiting for you in the secure area of the Barclays Cloud IT.

Please follow step 1, 2 & 3 carefully to view important documents.

Log in to Barclays Online

- Phishing emails often come from email addresses that resemble legitimate ones but contain small, deliberate variations (e.g., “support@banking1.com” instead of “support@banking.com”).
- Always inspect the sender’s email address closely to verify its authenticity

2. Urgent or Threatening Language:



To

NETFLIX

⚠ Your account is suspended.

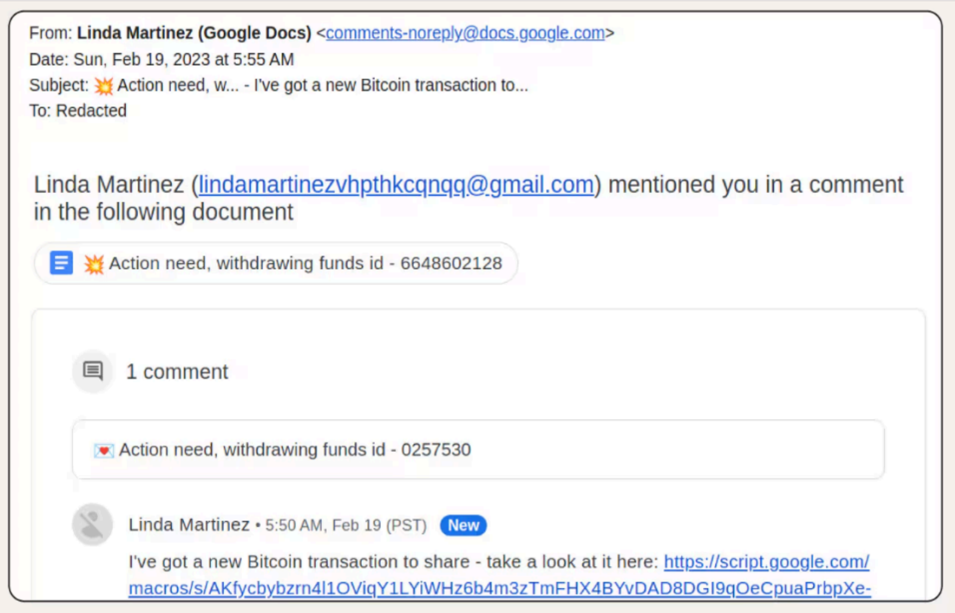
Your account is suspended.

Dear User,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details. During the next login process, you will be required to provide some informations like (billing info, phone number, payment info).

- Phishing emails commonly use urgent, threatening, or alarming language to pressure the recipient into acting quickly. For example: "Your account will be suspended in 24 hours unless you respond."
- Legitimate organizations typically do not use such urgent language in unsolicited emails.

3. Suspicious Links and Attachments:



From: **Linda Martinez (Google Docs)** <comments-noreply@docs.google.com>
Date: Sun, Feb 19, 2023 at 5:55 AM
Subject: 💥 Action need, w... - I've got a new Bitcoin transaction to...
To: Redacted

Linda Martinez (lindamartinezvhpthkcqnqq@gmail.com) mentioned you in a comment in the following document

💥 Action need, withdrawing funds id - 6648602128

1 comment

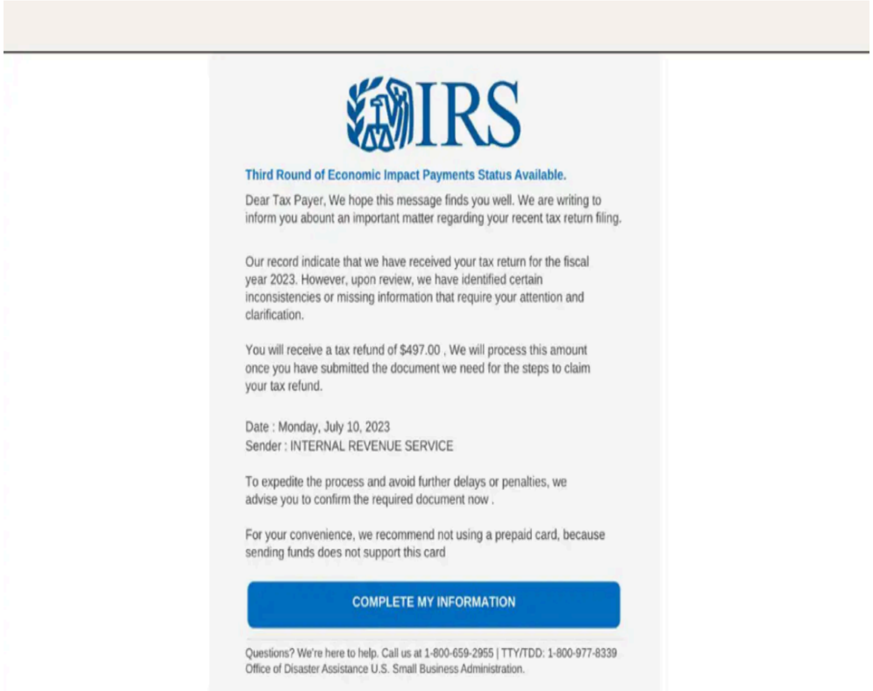
💌 Action need, withdrawing funds id - 0257530

Linda Martinez • 5:50 AM, Feb 19 (PST)

I've got a new Bitcoin transaction to share - take a look at it here: https://script.google.com/macros/s/AKfycbybzrn4l1OViqY1LYiWHz6b4m3zTmFHX4BYvDAD8DGI9qOeCpuaPrbpXe-

    - Phishing emails often contain malicious links or attachments. Links may appear to direct to a trusted website, but upon closer inspection, they may lead to fraudulent sites.Users might receive deceptive Google Docs phishing emails that appear to be from friends, coworkers, or a business offering a great deal. The emails contain a malicious link to a supposed shared Google Doc. This link leads to a fake or [unsafe website] mimicking the Google sign-in page, where entering credentials grants scammers access to the user's Google account.
    - Avoid clicking on any links or opening attachments in unsolicited emails.

4. **Generic Greetings:**



Third Round of Economic Impact Payments Status Available.

Dear Tax Payer, We hope this message finds you well. We are writing to inform you abount an important matter regarding your recent tax return filing.

Our record indicate that we have received your tax return for the fiscal year 2023. However, upon review, we have identified certain inconsistencies or missing information that require your attention and clarification.

You will receive a tax refund of $497.00 , We will process this amount once you have submitted the document we need for the steps to claim your tax refund.

Date : Monday, July 10, 2023
Sender : INTERNAL REVENUE SERVICE

To expedite the process and avoid further delays or penalties, we advise you to confirm the required document now .

For your convenience, we recommend not using a prepaid card, because sending funds does not support this card

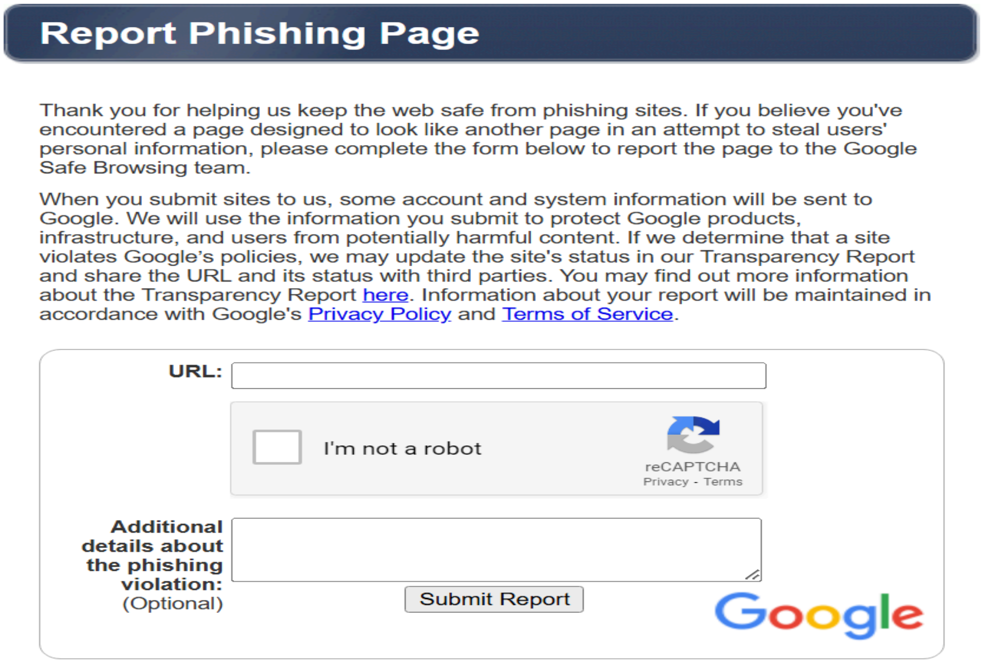
Questions? We're here to help. Call us at 1-800-659-2955 | TTY/TDD: 1-800-977-8339
Office of Disaster Assistance U.S. Small Business Administration.

    - Phishing emails typically use general greetings like "Dear Customer" or "Dear User" instead of addressing the recipient by name.
    - Reputable companies address their customers by their registered name.

5. **Unsolicited Requests for Sensitive Information:**
    - Phishing attempts frequently ask for sensitive personal details, such as passwords, Social Security numbers, or credit card information. Legitimate companies do not request such information via email.

Handling Phishing Emails:

1. **Do Not Click on Links or Open Attachments**:
    - If you suspect an email is phishing, do not interact with it by clicking on any links or downloading attachments. Doing so may trigger malware downloads or redirect you to malicious websites.
2. **Verify the Sender's Information**:
    - If the email is supposedly from a service or company you use, reach out directly to the official customer service number or website to verify whether the communication is legitimate. Always use verified contact methods rather than those provided in the email.
3. **Report Phishing Attempts**:



Report Phishing Page

Thank you for helping us keep the web safe from phishing sites. If you believe you've encountered a page designed to look like another page in an attempt to steal users' personal information, please complete the form below to report the page to the Google Safe Browsing team.

When you submit sites to us, some account and system information will be sent to Google. We will use the information you submit to protect Google products, infrastructure, and users from potentially harmful content. If we determine that a site violates Google's policies, we may update the site's status in our Transparency Report and share the URL and its status with third parties. You may find out more information about the Transparency Report here. Information about your report will be maintained in accordance with Google's Privacy Policy and Terms of Service.

- Email platforms like Gmail, Outlook, and Yahoo have built-in phishing reporting tools. Use these features to report suspicious emails.
- Users can also report phishing emails to specialized platforms such as ReportPhishing or to relevant government bodies.

4. **Delete the Email**:
   - Once an email has been reported, delete it from your inbox to prevent accidental interaction with it in the future.
5. **Use Anti-Phishing Software**:
   - Install and maintain anti-phishing software or browser extensions that can automatically detect and block phishing attempts.

Conclusion:

Phishing emails are a significant cybersecurity threat, but with the right knowledge and vigilance, individuals can effectively protect themselves. By recognizing common signs of phishing attempts, reporting suspicious emails, and adopting preventive measures, users can significantly reduce the risks associated with phishing. Remember, if in doubt, always verify the legitimacy of the message by contacting the organization directly through trusted channels.