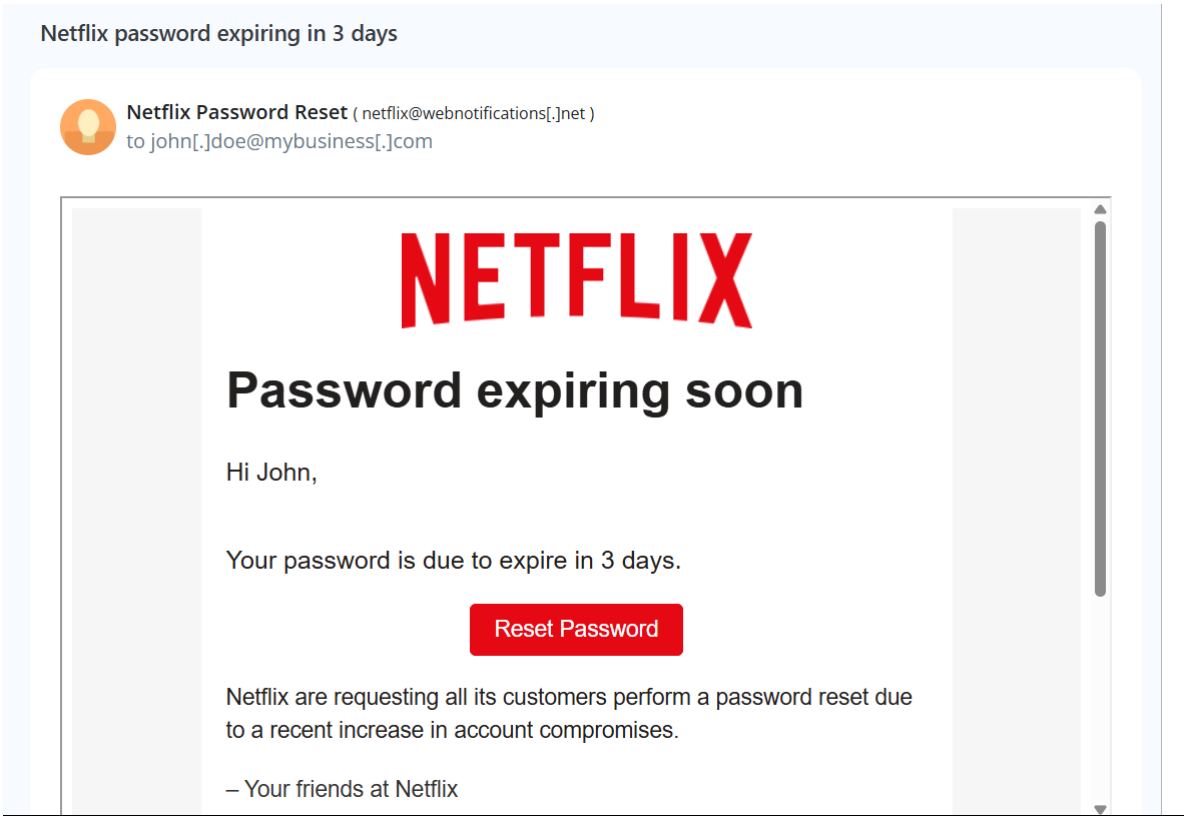
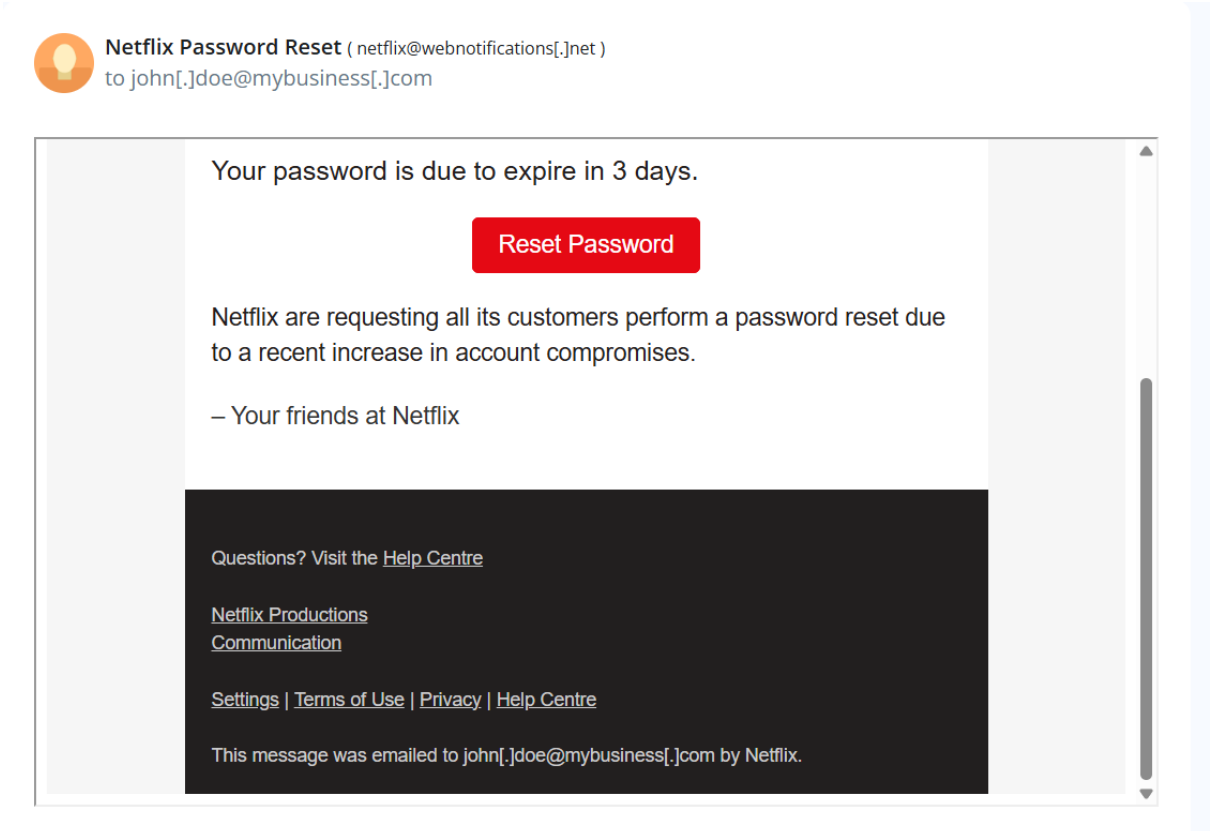
Task 2

Task 2: Analyse a Phishing Email Sample

Step 1: - Obtain a sample phishing email (https://caniphish.com/phishing-email-examples)





Step 2: - Check email headers for discrepancies

Headers Found

Header Name	Header Value
From	Netflix Password Reset <netflix@webnotifications[.]net>
To	ramshivomgaur0258@gmail.com
Subject	Password expiring soon

Received Header

```
From: Netflix Password Reset <netflix@webnotifications[.]net>
To: ramshivomgaur0258@gmail.com
Subject: Password expiring soon

Email Body:
NETFLIX

Password expiring soon

Hi Prashant,

Your password is due to expire in 3 days.

[Reset Password] 🔴 (Red button)

Netflix are requesting all its customers perform a password reset due to a recent increase in account compromises.

- Your friends at Netflix

Footer:

Questions? Visit the [Help Centre]

Netflix Productions
Communication

[Settings] | [Terms of Use] | [Privacy] | [Help Centre]

This message was emailed to prashantmall@mybusiness[.]com by Netflix
```

Step 3: - Identify suspicious links or attachments.

🔎 **Phishing Indicators Found in the Email:**

1. Suspicious Sender Address

- **Shown:** netflix@webnotifications[.]net
- **Red Flag:** This is **not** an official Netflix domain (official domains usually end with @netflix.com). The suspicious domain is attempting to impersonate Netflix.

---

2. Urgency and Threat Language

- **Phrases like:**
  - "Your password is due to expire in 3 days."
  - "Netflix are requesting all its customers..."
- **Red Flag:** Creates **fear or urgency** to make the user click without thinking — a classic phishing tactic.

---

3. Call to Action Button

- **"Reset Password"** button is prominent and emotionally triggering.
- **Red Flag:** These buttons often lead to **phishing sites** that steal login credentials. (You'd need to hover and inspect the URL to confirm.)

---

4. Grammatical and Stylistic Errors

- **Error:** "Netflix are requesting..."
  - Correct grammar would be: "Netflix **is** requesting..."
- **Red Flag:** Phishing emails often come from non-native speakers and contain small but suspicious grammar mistakes.

---

5. Mismatched URLs (Check by Hovering)

- If you hover over any link (like the "Reset Password" button or "Help Centre"), the actual URL **might differ** from the visible text.
- **Red Flag:** This technique is used to hide malicious URLs behind trustworthy-looking text.

---

6. Generic Greeting

- "Hi John," is used here, which is semi-personalized but could still be spoofed.

- Most phishing emails either use generic greetings ("Dear user") or try to guess names based on the email address.

---

7. Spoofed Branding

- Fake Netflix logo and color scheme are used to appear authentic.
- **Red Flag:** It **mimics** the branding well, but that doesn't mean it's genuine — always check the sender and link.

---

8. Lack of Personal Account Information

- Netflix usually references part of your username/account info for authenticity.
- The email **does not mention your account details**, which is suspicious.

Step 4: - Look for urgent or threatening language in the email body.

🔴 **Urgent or Threatening Language in the Email Body:**

1. **“Your password is due to expire in 3 days.”**
    - **Why it’s suspicious:** This creates a sense of **urgency** and fear that you might lose access to your account if you don’t act immediately.
2. **“Reset Password” (bold red button)**
    - **Why it’s suspicious:** The prominent red color and imperative tone add psychological pressure. It’s meant to **push the user into clicking quickly**.
3. **“Netflix are requesting all its customers perform a password reset...”**
    - **Why it’s suspicious:** Makes it sound like **everyone is doing it**, making the recipient feel compelled to follow along.

Step 5: - Note any mismatched URLs

🔍 **Mismatched URL Indicators (Based on Image):**

1. “Reset Password” Button

- **Visible Text**: Reset Password
- **Expected Legit URL**: https://www.netflix.com/ or something under the **netflix.com** domain.
- **Analysis**: If the hover link doesn't belong to `netflix.com` (e.g., `.xyz`, `.click`, `secure-netflix-login.com`), it's a **mismatched and malicious URL**.

Step 6: - Verify presence of spe ling or grammar errors.

✍️ **Spelling and Grammar Errors in the Email:**

Incorrect Grammar:

“Netflix are requesting all its customers perform a password reset…”

✅ **Correct form should be:**

“Netflix is requesting that all its customers perform a password reset…”

❌ **Problem: Subject-verb disagreement (“Netflix” is a singular entity, so it should use “is”).**

Unnatural Phrasing:

“Your password is due to expire in 3 days.”

⚠️ **This phrase isn't incorrect, but companies typically use more professional wording like:**

“For your security, your password will expire in 3 days.”

“Your friends at Netflix”

⚠️ **Unprofessional tone — large companies like Netflix usually sign off more formally.**

Expected: “The Netflix Team” or “Netflix Support”.

"spe ling" (in the task hint itself)

This is a typo in the instructions you're following, not in the email — but it's worth recognizing!

Step 7: - Summarize phishing traits found in the email.

🛡️ **Phishing Traits Identified in the Email Sample**

1. Suspicious Sender Address

- **From: netflix@webnotifications[.]net**
- ✅ **Legitimate Netflix emails come from: @netflix.com**
- ❌ **This domain (webnotifications.net) is unrelated to Netflix — likely spoofed.**

---

2. Urgent/Threatening Language

- **Text: *“Your password is due to expire in 3 days.”***

- ❗ **Urges the user to act immediately, a classic phishing technique to create panic and bypass rational judgment.**

---

3. Suspicious Link/Button

- **Button: "Reset Password"**
- ⚠️ **Hovering over the link likely reveals a non-Netflix domain (e.g., not netflix.com).**
- ❌ **Clicking it may lead to a fake login page or malware.**

---

4. Grammar and Language Issues

- **Error: *"Netflix are requesting…"***
  - ❌ **Incorrect subject-verb agreement. It should be "Netflix is requesting…"**
- **Unprofessional tone: *"Your friends at Netflix"***
  - **Unusual phrasing for official corporate communication.**

---

5. Generic Greeting

- **Example: *"Hi John"***
  - **While it uses a name, this can be easily faked. Real Netflix emails often use full names or account info.**

---

6. Misleading Branding

- **Includes Netflix logo and colors to look authentic.**
- ⚠️ **Appearance alone doesn't confirm legitimacy — phishing emails often clone brand layouts.**