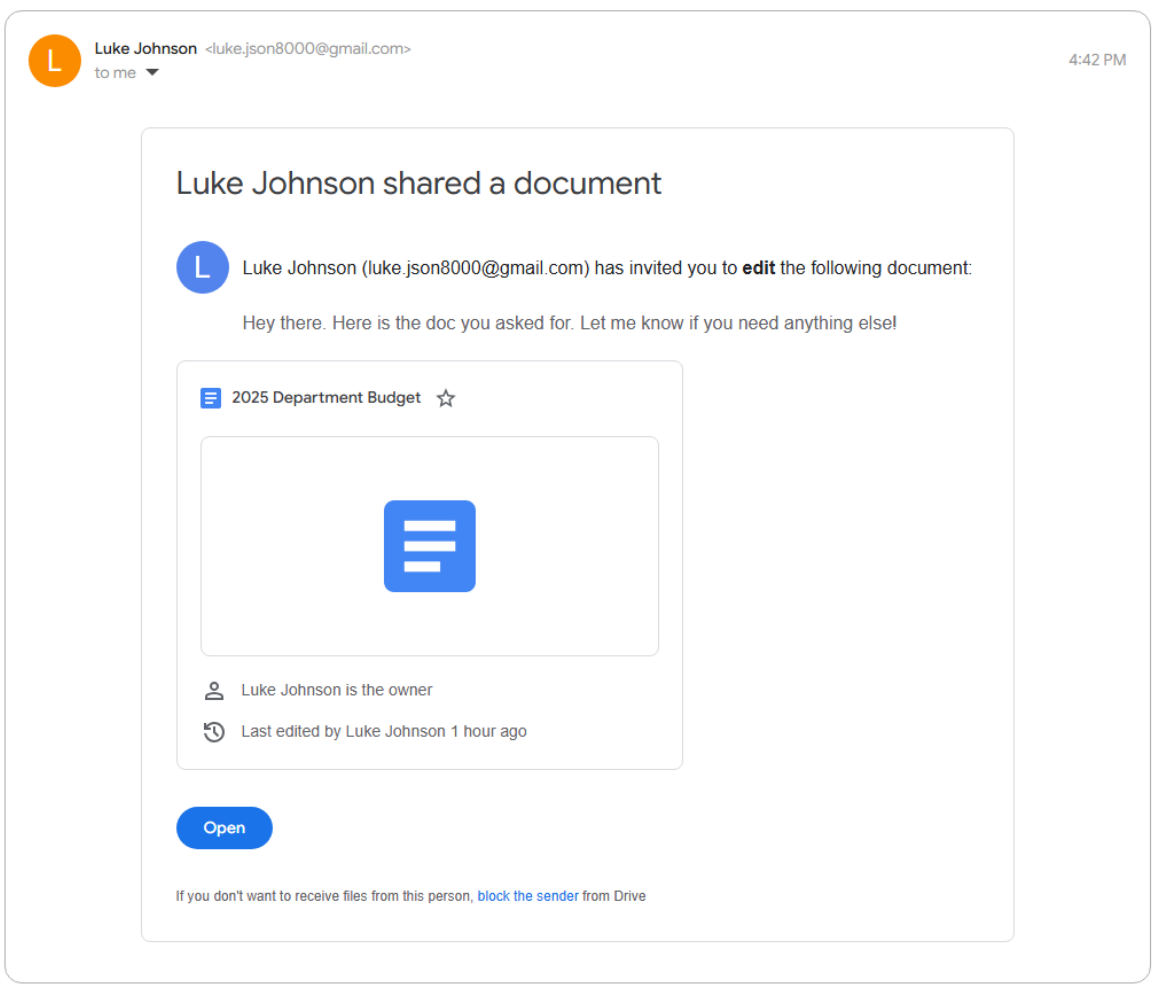
Cyber Security task – 2

Phishing Analysis Report

Introduction:

In this task, I analyzed a phishing email to understand common phishing tactics and indicators. The goal was to review the email, examine its header, links, language, and overall structure to identify signs of phishing attacks.

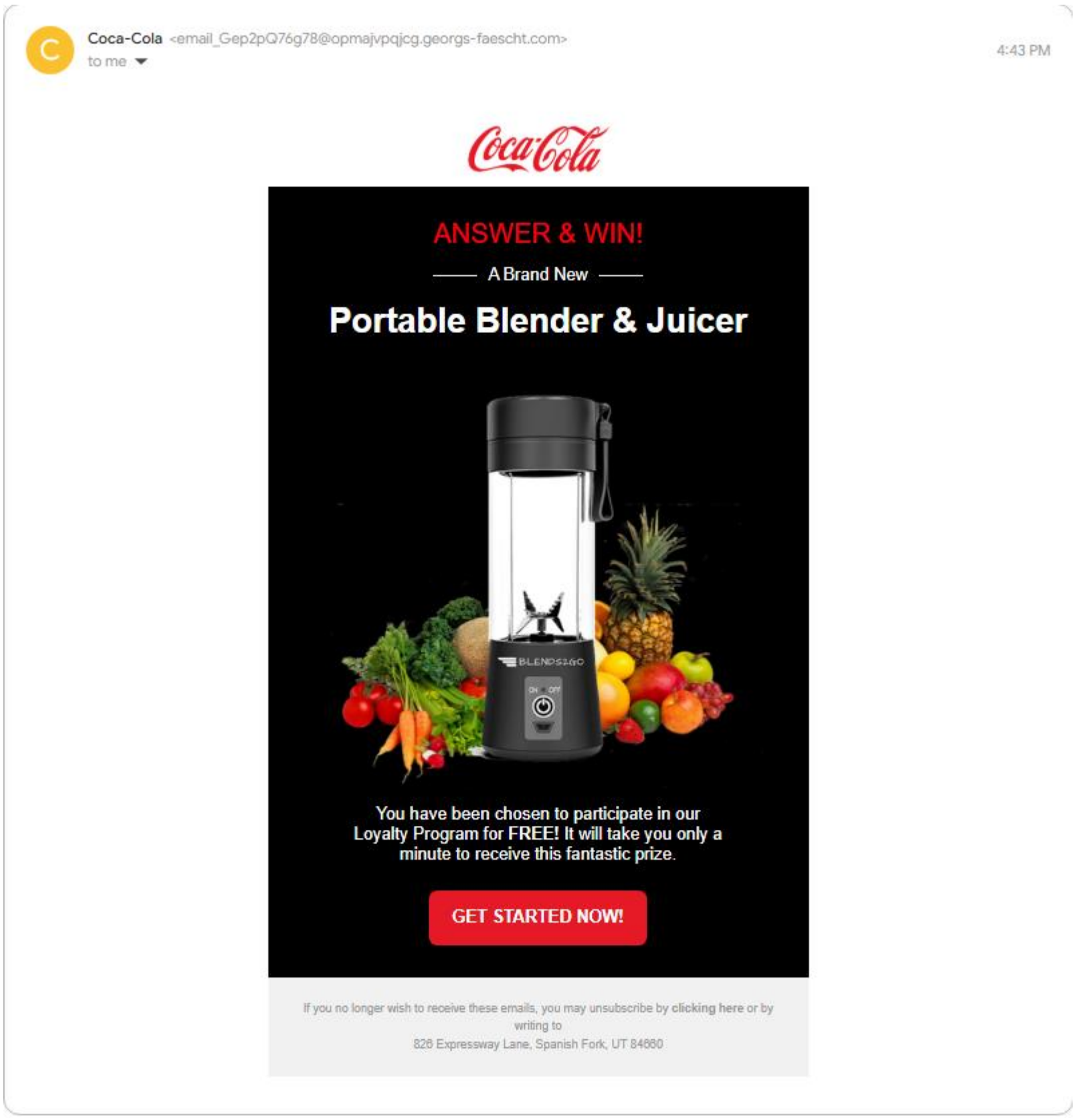
Email sample :



http://drive--google.com/d/6374pcjdsob83987cidkqwlsl9134

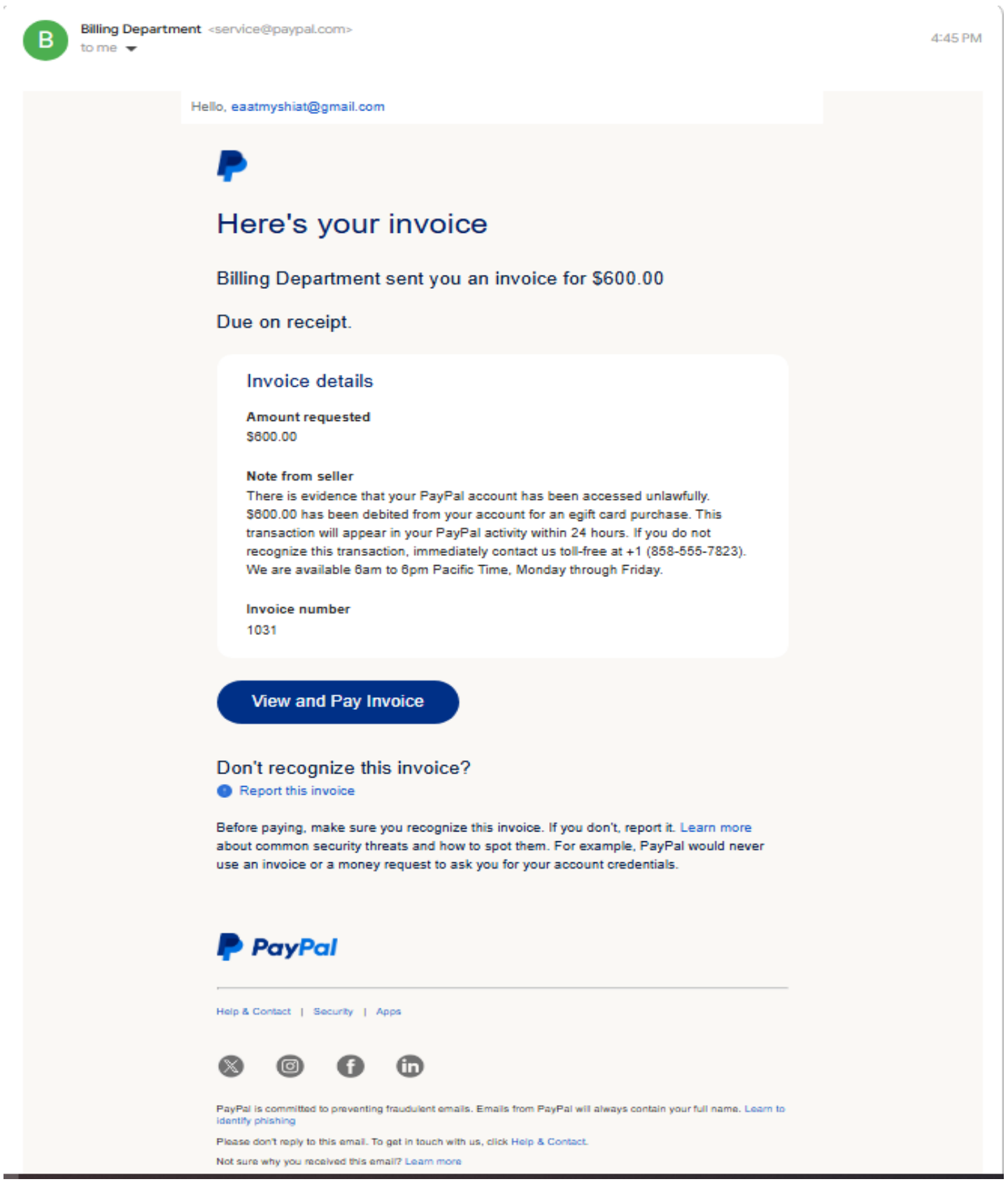
(taken from google phising quiz)

In this example , hovering over the link or using a long press will show you that it goes to the insecure imitation domain “drive—google.com”



- The email claims to be from coca cola ,but the sending address is very random……not impossible for a legitimate email ,but a sign.
- The content with the text is all in the image. While used in legitimate communications, this technique is used to avoid detection.
- The URL is designed to hide a number of redirects but avoid detection by the hosting provider by only triggering with the text after “#” (normally this is a short code used to link to a specific location on a page.)

  (taken from google phishing quiz)



- This message is actually a “note from seller.” The scammer created a false sense of urgency, a common technique to trick users into action.
- The phishers are hoping you’ll call this number where they’ll continue the scam. You can verify the phone numbers of legitimate companies through their website (eg: paypal’s website)

(taken from google phising quiz)

Header analysis :

Example email:

From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

Using : MX toolbox

Header Analyzed

Email Subject: Apple Facetime Information Disclosure

Delivery Information

Relay Information

Received Delay: 0 seconds

SPF and DKIM Information

Headers Found

Header Name	Header Value
From	domain@domain-name.com
To	Your email
Subject	Apple Facetime Information Disclosure

Received Header

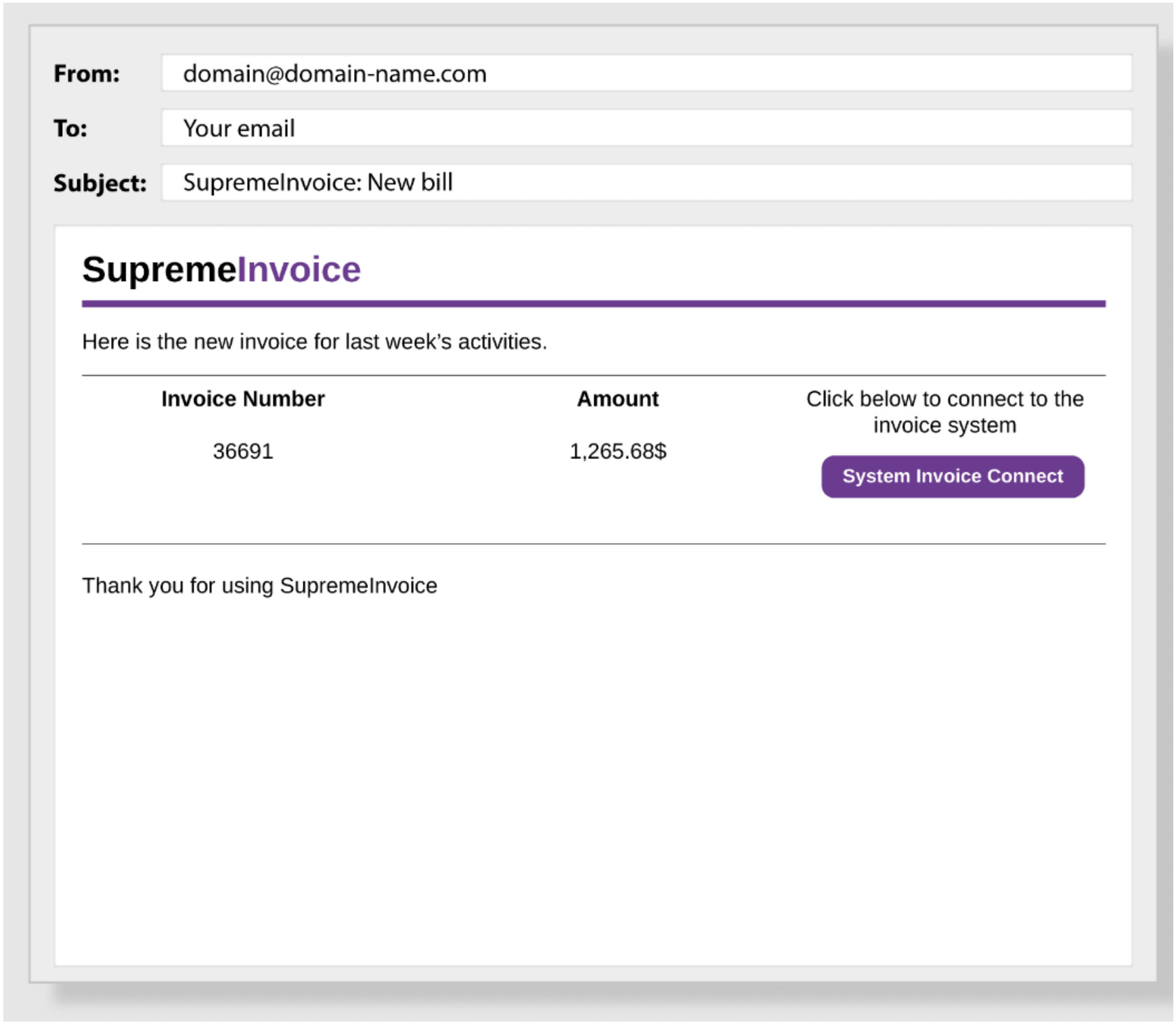
```
From: domain@domain-name.com
To: Your email
Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification
This website will be available for 72 hours.

National Security Department
```

Header Analysis performed using MX Toolbox . The results confirmed signs of phishing activity.

- The sender’s address doesn’t seem legitimate (domain-name.com), hinting it's an impersonation attempt.
- The subject line is crafted to create urgency, prompting the recipient to open and click.
- The received header confirms this is an external, potentially untrusted source.

The header lacks common security verifiers (such as SPF or DKIM), which is a strong sign of phishing.

Example 2:



From: domain@domain-name.com

To: Your email

Subject: SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	System Invoice Connect

Thank you for using SupremeInvoice

Header Analyzed

Email Subject:

Delivery Information

Relay Information

Received Delay:	0 seconds

SPF and DKIM Information

Headers Found

Header Name	Header Value
From	

Received Header

```
From:
domain@domain-name.com

To:
Your email

Subject:
Supremelnvoice: New bill

Supremelnvoice
Here is the new invoice for last week's activities.

Invoice Number  Amount  Click below to connect to the invoice system
36691   1,265.68$       System Invoice Connect
Thank you for using Supremelnvoice
```

Permanently forget this email header

- The email appears to be an invoice notification ("Here is the new invoice for last week’s activities") with an invoice number and amount ($1,265.68), prompting the recipient to click a link ("System Invoice Connect").

SPF and DKIM Status:

No valid SPF or DKIM records were found for this email. These are key email authentication methods that help verify if an email is legitimately from the claimed sender. The absence of these headers is a strong sign that the email could be phishing or spoofed.

Common Characteristics of the Phishing Emails

- **Suspicious Sender Addresses**: All examples used strange or mismatched email addresses that didn't align with trusted domains (e.g., domain@domain-name.com).
- **Generic or Urgent Greetings**: Messages like "Dear User" or urgent subject lines like "Action required" or "New Invoice" designed to pressure the reader.
- **Mismatched Links**: Links appeared legitimate in text but pointed to unrelated or dangerous websites when hovered over.
- **Spelling and Grammar Errors**: Minor inconsistencies and awkward phrasing, a common phishing sign.
- **Requests for Sensitive Information**: Messages that asked for personal information or prompted clicking links for account verification.

Techniques for Identifying Phishing Emails

- **Check the Sender**: Always review the sender's email address closely for anomalies.
- **Examine Links**: Hover over links before clicking to verify the actual URL.
- **Review Headers**: Check the email headers for inconsistencies and failed SPF/DKIM verification.
- **Look for Red Flags**: Generic greetings, urgency, threats, and unexpected attachments.

Final Conclusion

Phishing attacks are a common way hackers try to trick people online. By looking for signs like strange email addresses, urgent language, mismatched links, and errors in the message, we can spot and avoid them. Understanding how to read email headers and using online tools can also help confirm if an email is safe. Being cautious and aware is the best way to stay protected.

THANK YOU