

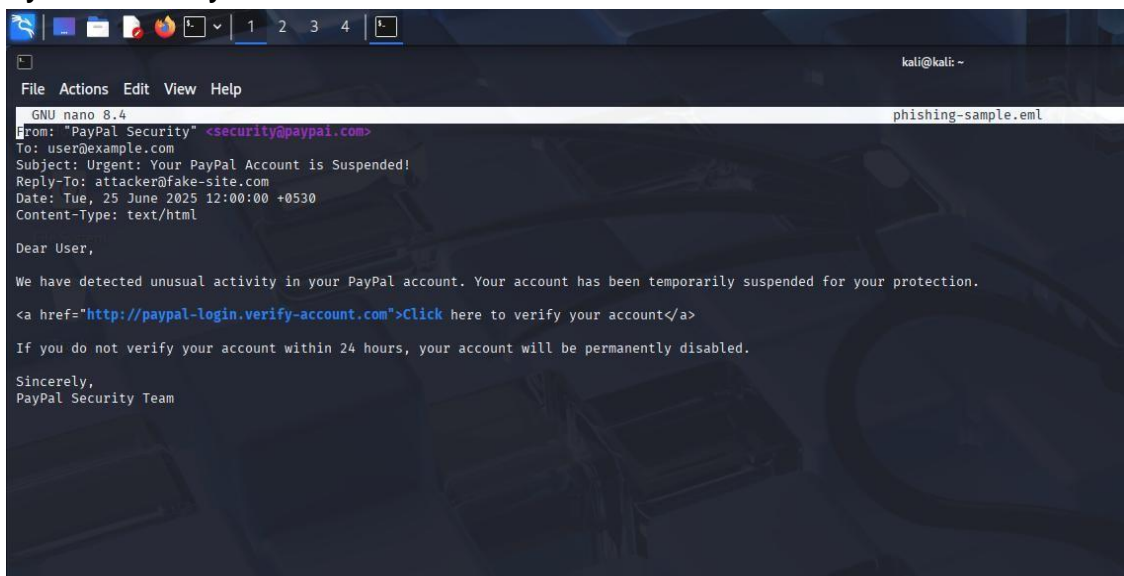
Task 2: Analyze a Phishing Email Sample.

Hints/Mini Guide:

1. Obtain a sample phishing email (many free samples online).
2. Examine sender's email address for spoofing.
3. Check email headers for discrepancies (using online header analyzer).
4. Identify suspicious links or attachments.
5. Look for urgent or threatening language in the email body.
6. Note any mismatched URLs (hover to see real link).
7. Verify presence of spelling or grammar errors.
8. Summarize phishing traits found in the email.

1. Obtain a sample phishing email.

- To begin analyzing phishing techniques, the first step is to obtain a sample phishing email.
- This can be sourced from publicly available phishing databases, online security forums, or educational repositories such as PhishTank, SpamArchive, or GitHub repositories dedicated to cybersecurity research.

A screenshot of a Kali Linux terminal window. The terminal shows a nano editor editing a file named 'phishing-sample.eml'. The email content is displayed in the editor, featuring a spoofed 'PayPal Security' header with a suspicious email address, a subject line about a suspended account, and a body with urgent language and a link to a fake verification page. The terminal window has a dark theme and shows standard Linux desktop icons at the top.

```
GNU nano 8.4 phishing-sample.eml
From: "PayPal Security" <security@paypal.com>
To: user@example.com
Subject: Urgent: Your PayPal Account is Suspended!
Reply-To: attacker@fake-site.com
Date: Tue, 25 June 2025 12:00:00 +0530
Content-Type: text/html

Dear User,

We have detected unusual activity in your PayPal account. Your account has been temporarily suspended for your protection.

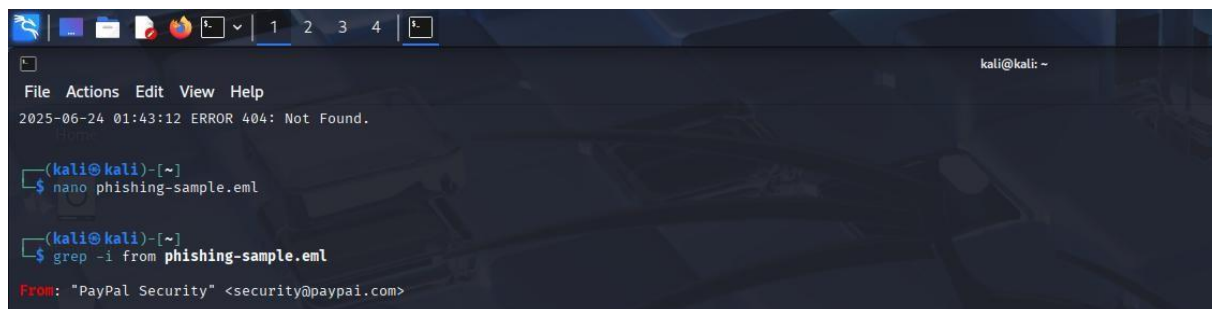
<a href="http://paypal-login.verify-account.com">Click here to verify your account</a>

If you do not verify your account within 24 hours, your account will be permanently disabled.

Sincerely,
PayPal Security Team
```

2. Examine sender's email address for spoofing.

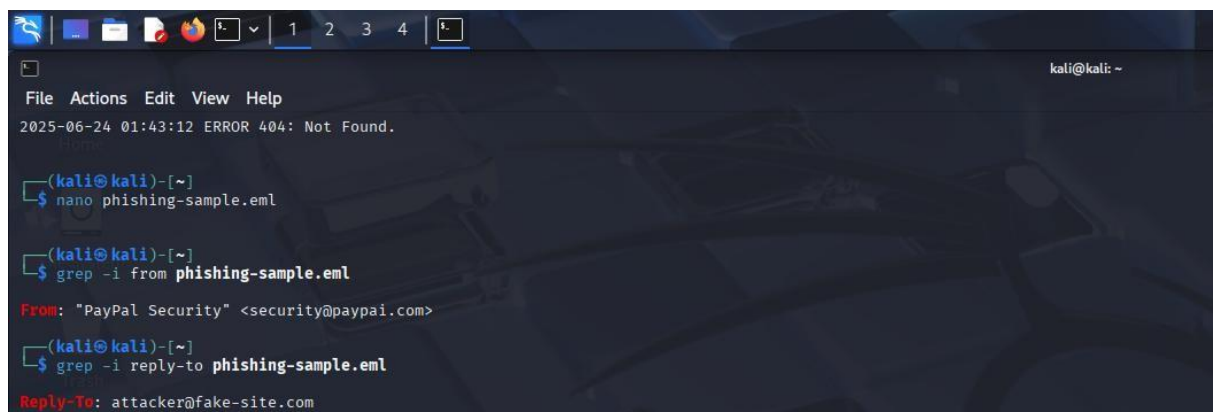
- After obtaining the phishing email, the next crucial step is to examine the sender's email address to detect any signs of spoofing.
- Spoofed addresses often appear to be from legitimate sources at first glance but may contain subtle anomalies such as misspelled domains, unusual characters, or unexpected sender names.

A terminal window on a Kali Linux system. The user has opened a file named 'phishing-sample.eml' in nano. They then run the command 'grep -i from phishing-sample.eml'. The output shows a red 'From:' header: 'PayPal Security' <security@paypai.com>. The terminal title bar shows 'kali@kali: ~' and the window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
kali@kali: ~  
File Actions Edit View Help  
2025-06-24 01:43:12 ERROR 404: Not Found.  
  
(kali@kali)-[~]  
$ nano phishing-sample.eml  
  
(kali@kali)-[~]  
$ grep -i from phishing-sample.eml  
From: "PayPal Security" <security@paypai.com>
```

3. Check email headers for discrepancies.

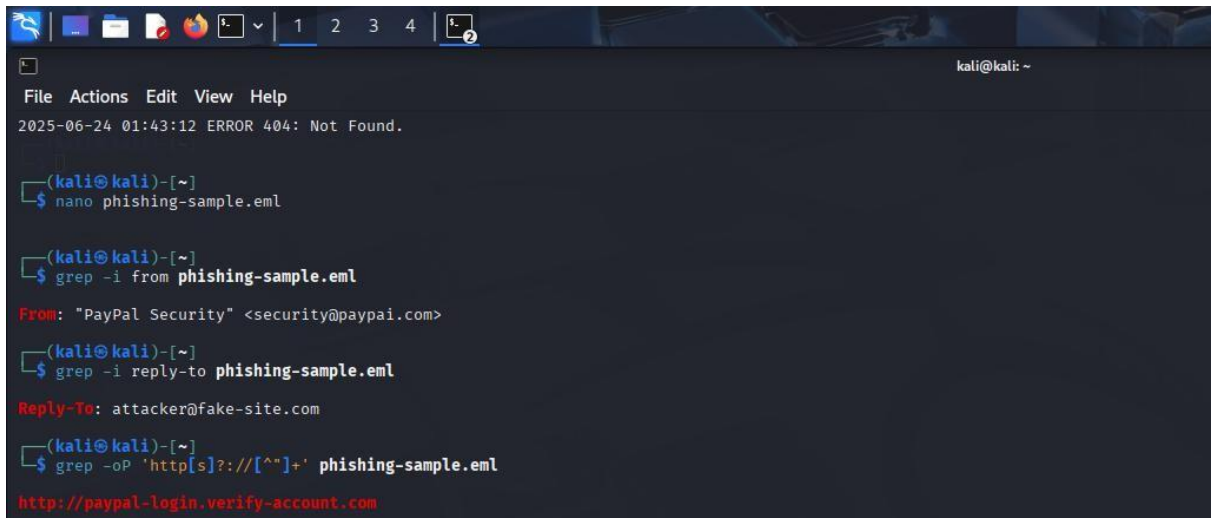
- Checking the email headers is a vital step in identifying phishing attempts, as headers contain detailed technical information about the email's journey from sender to recipient.
- By reviewing the "Received" lines, one can trace the path the email took through various mail servers, helping to spot inconsistencies in the sender's identity or originating IP address.
- This technical inspection helps confirm whether the email was forged or altered in transit, strengthening the overall phishing analysis.

A terminal window on a Kali Linux system, similar to the previous one. The user runs the command 'grep -i reply-to phishing-sample.eml'. The output shows a red 'Reply-To:' header: 'attacker@fake-site.com'. The terminal title bar shows 'kali@kali: ~' and the window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
kali@kali: ~  
File Actions Edit View Help  
2025-06-24 01:43:12 ERROR 404: Not Found.  
  
(kali@kali)-[~]  
$ nano phishing-sample.eml  
  
(kali@kali)-[~]  
$ grep -i from phishing-sample.eml  
From: "PayPal Security" <security@paypai.com>  
  
(kali@kali)-[~]  
$ grep -i reply-to phishing-sample.eml  
Reply-To: attacker@fake-site.com
```

4. Identify suspicious links or attachments.

- One of the most dangerous elements in a phishing email is the presence of suspicious links or attachments.
- These are often designed to trick the recipient into clicking on a malicious website or downloading malware onto their system.
- To identify suspicious links, hover the mouse pointer over hyperlinks in the email to reveal the actual URL—often it won't match the text displayed.

A terminal window on a Kali Linux system. The user has run several commands to analyze a file named 'phishing-sample.eml'. The first command is 'nano phishing-sample.eml'. The second is 'grep -i from phishing-sample.eml', which returns 'From: "PayPal Security" <security@paypal.com>'. The third is 'grep -i reply-to phishing-sample.eml', which returns 'Reply-To: attacker@fake-site.com'. The fourth is 'grep -oP 'http[s]?://[^\"]+' phishing-sample.eml', which returns 'http://paypal-login.verify-account.com'. The terminal output is as follows:

```
(kali@kali)-[~]
$ nano phishing-sample.eml

(kali@kali)-[~]
$ grep -i from phishing-sample.eml
From: "PayPal Security" <security@paypal.com>

(kali@kali)-[~]
$ grep -i reply-to phishing-sample.eml
Reply-To: attacker@fake-site.com

(kali@kali)-[~]
$ grep -oP 'http[s]?://[^\"]+' phishing-sample.eml
http://paypal-login.verify-account.com
```

5. Look for urgent or threatening language in the email body.

- Phishing emails often use urgent or threatening language in the body of the message to create a sense of panic and pressure the recipient into acting quickly without thinking.
- Common phrases include warnings like “Your account will be suspended,” “Immediate action required”.

A terminal window on a Kali Linux system, identical to the one above. It shows the same sequence of commands and output for analyzing 'phishing-sample.eml'. The terminal output is as follows:

```
(kali@kali)-[~]
$ nano phishing-sample.eml

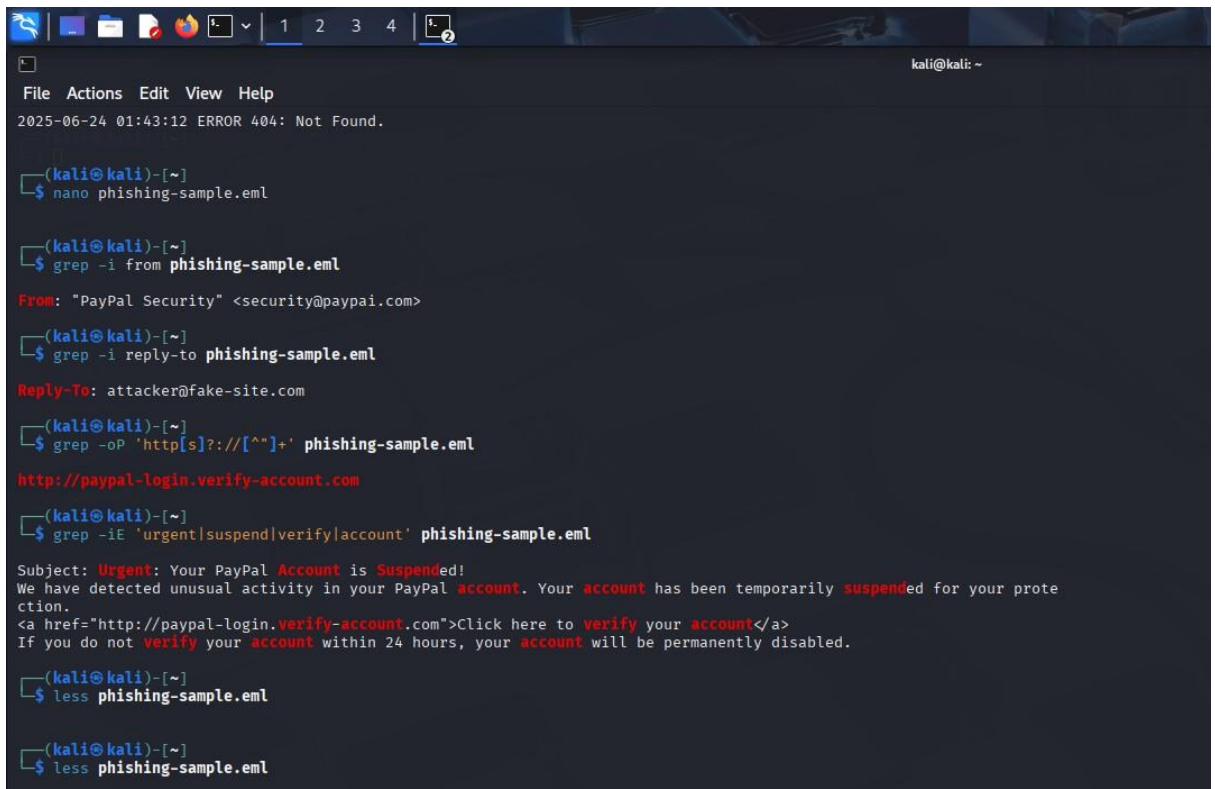
(kali@kali)-[~]
$ grep -i from phishing-sample.eml
From: "PayPal Security" <security@paypal.com>

(kali@kali)-[~]
$ grep -i reply-to phishing-sample.eml
Reply-To: attacker@fake-site.com

(kali@kali)-[~]
$ grep -oP 'http[s]?://[^\"]+' phishing-sample.eml
http://paypal-login.verify-account.com
```

6. Note any mismatched URLs & Verify presence of spelling or grammar errors.

- In the provided phishing email sample, two clear red flags stand out: mismatched URLs and language issues.
- The hyperlink shown in the email body “<http://paypal-login.verify-account.com>” appears to imitate a legitimate PayPal address but actually redirects to a suspicious, misleading domain.
- This mismatch is a strong indicator of phishing, as attackers often craft URLs that visually resemble trusted domains to deceive recipients into clicking. Additionally, a closer look at the email text reveals spelling and grammar inconsistencies.
- For example, the phrase “suspended for your protection” contains an unnatural space, and the overall language is overly aggressive and alarmist—such as “Urgent: Your PayPal Account is Suspended!” This type of emotional manipulation, paired with poor grammar and deceptive links, is a classic phishing tactic used to exploit user trust and urgency.



```
kali@kali: ~  
File Actions Edit View Help  
2025-06-24 01:43:12 ERROR 404: Not Found.  
  
(kali@kali)-[~]  
$ nano phishing-sample.eml  
  
(kali@kali)-[~]  
$ grep -i from phishing-sample.eml  
From: "PayPal Security" <security@paypai.com>  
  
(kali@kali)-[~]  
$ grep -i reply-to phishing-sample.eml  
Reply-To: attacker@fake-site.com  
  
(kali@kali)-[~]  
$ grep -oP 'http[s]?://[^\s]+' phishing-sample.eml  
http://paypal-login.verify-account.com  
  
(kali@kali)-[~]  
$ grep -iE 'urgent|suspend|verify|account' phishing-sample.eml  
Subject: Urgent: Your PayPal Account is Suspended!  
We have detected unusual activity in your PayPal account. Your account has been temporarily suspended for your protection.  
<a href="http://paypal-login.verify-account.com">Click here to verify your account</a>  
If you do not verify your account within 24 hours, your account will be permanently disabled.  
  
(kali@kali)-[~]  
$ less phishing-sample.eml  
  
(kali@kali)-[~]  
$ less phishing-sample.eml
```

8. Summarize phishing traits found in the email.

- Based on the analysis of the phishing-sample.eml file, several clear indicators of a phishing attempt were identified. The email claims to be from “PayPal Security” using the address security@paypai.com, which is a spoofed domain (note the misspelling of "paypal").
- Additionally, the “Reply-To” field is set to attacker@fake-site.com, showing a mismatch designed to redirect responses to a malicious actor. The content of the email uses alarming language such as “Urgent,” “Account is Suspended,” and threats of permanent disabling to pressure the victim into acting quickly.
- A suspicious link <http://paypal-login.verify-account.com> was embedded, attempting to mimic a legitimate PayPal login page.
- There are also noticeable spelling and formatting errors, such as “protection,” further suggesting it's not from a reputable source.
- These combined traits spoofed sender, mismatched reply address, phishing link, urgency, and language mistakes strongly indicate that this is a fraudulent phishing email designed to steal user credentials.