Cyber Security Internship

Task 2 : Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

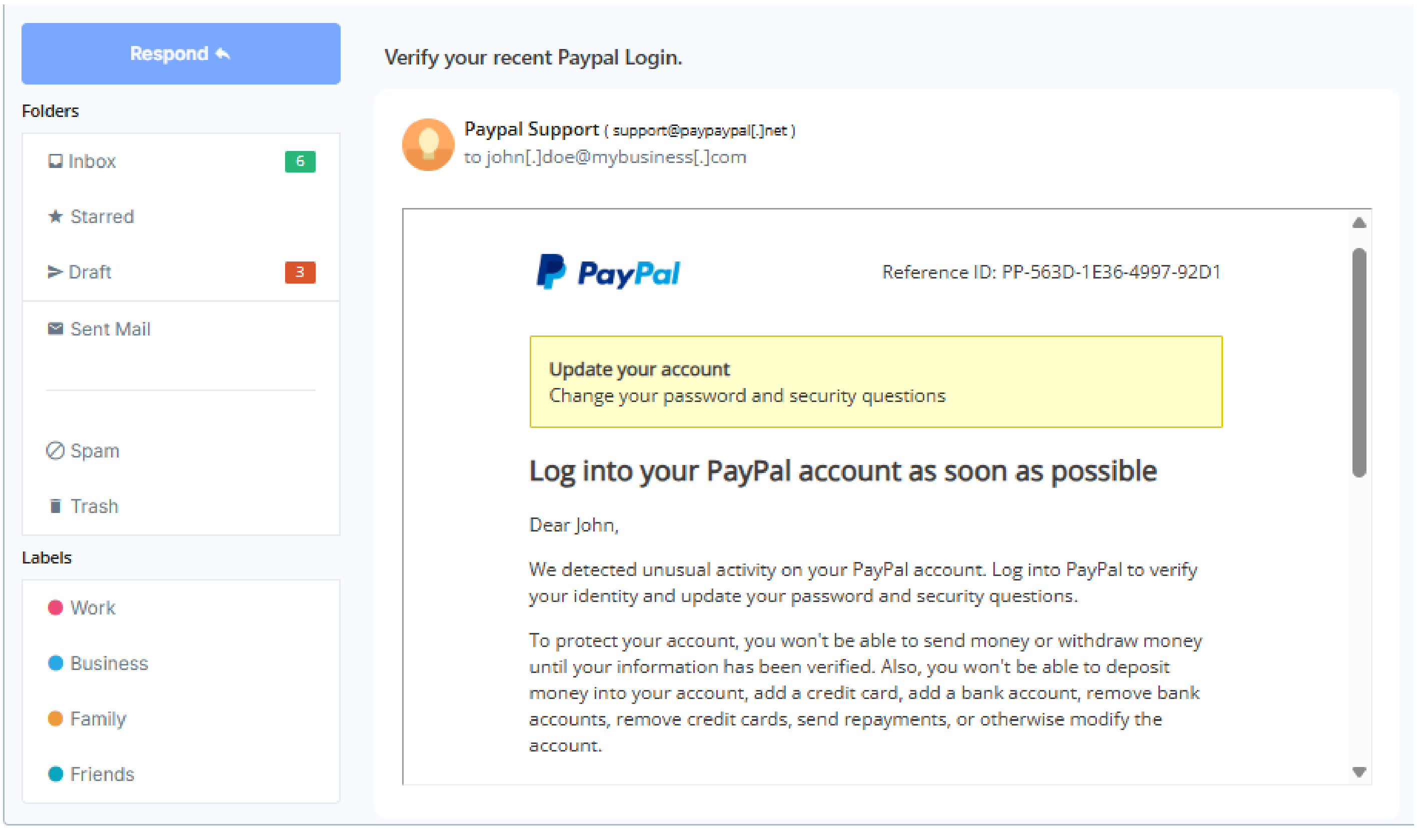
Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found

1.Obtain a sample phishing email (many free samples online).

Paypal

Phishing Email Example



Verify your recent Paypal Login.

Paypal Support (support@paypaypal[.]net)
to john[.]doe@mybusiness[.]com

Reference ID: PP-563D-1E36-4997-92D1

Update your account
Change your password and security questions

Log into your PayPal account as soon as possible

Dear John,

We detected unusual activity on your PayPal account. Log into PayPal to verify your identity and update your password and security questions.

To protect your account, you won't be able to send money or withdraw money until your information has been verified. Also, you won't be able to deposit money into your account, add a credit card, add a bank account, remove bank accounts, remove credit cards, send repayments, or otherwise modify the account.

2.Examine sender's email address for spoofing.

We can see the typo in mail id: **Paypal Support** (support@paypaypal[.]net)

Here the typo is: paypaypal

3.Check email headers for discrepancies (using online header analyzer).

From: Paypal Support (support@paypaypal[.]net)

Return-Path: john[.]doe@mybusiness[.]com

Received: from [194.38.20.89] (Russia IP for PayPal?)

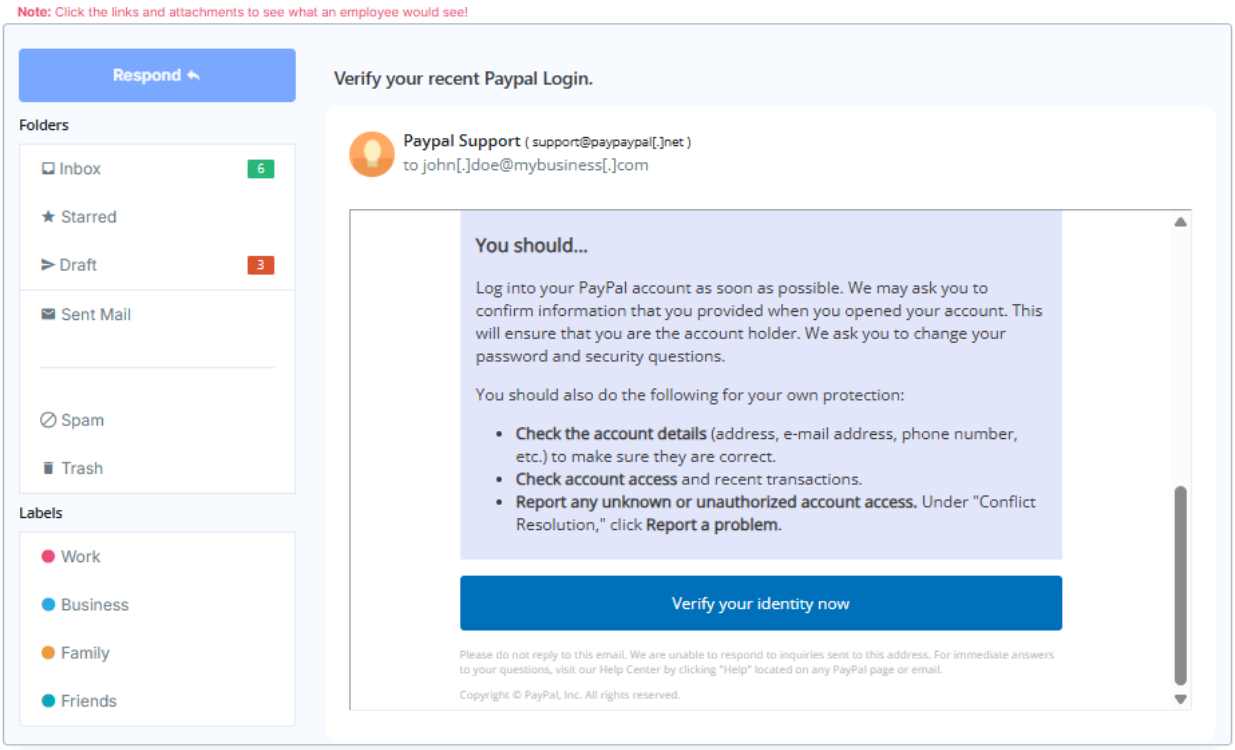
Reply-To: support@paypaypal.net

SPF (Sender Policy Framework) : fail

DKIM (DomainKeys Identified Mail): fail

DMARC: fail (policy=reject)

4. Identify suspicious links or attachments



Note: Click the links and attachments to see what an employee would see!

Verify your recent Paypal Login.

Paypal Support (support@paypaypal[.]net)
to john[.]doe@mybusiness[.]com

You should...

Log into your PayPal account as soon as possible. We may ask you to confirm information that you provided when you opened your account. This will ensure that you are the account holder. We ask you to change your password and security questions.

You should also do the following for your own protection:

- **Check the account details** (address, e-mail address, phone number, etc.) to make sure they are correct.
- **Check account access** and recent transactions.
- **Report any unknown or unauthorized account access.** Under "Conflict Resolution," click **Report a problem**.

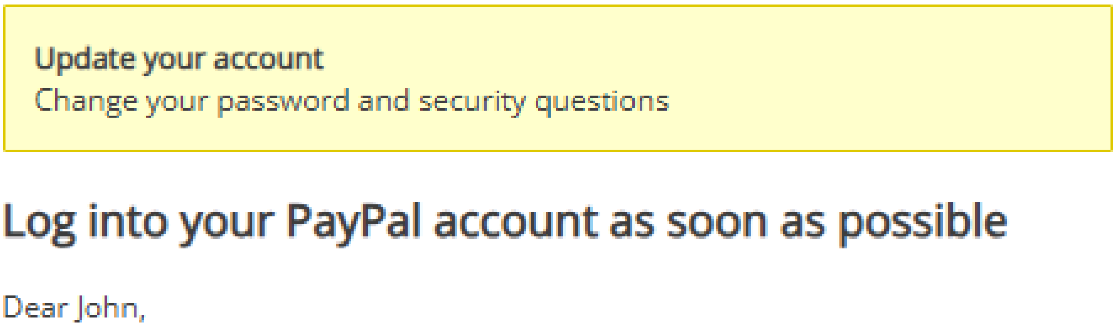
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © PayPal, Inc. All rights reserved.

Here we have Hover over button with a malicious link in blue color.

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

“Log into your PayPal account as soon as possible”



Update your account
Change your password and security questions

Log into your PayPal account as soon as possible

Dear John,

6. Note any mismatched URLs (hover to see real link)

http://paypal.com/email-paypal-account?email=account-update-request

7. Verify presence of spelling or grammar errors.

Log “into” your PayPal account as soon as possible: into – in to

Log “into” PayPal to verify your identity and update your password and security questions: into – in to

Report any unknown or “unauthorized” account access. Under "Conflict Resolution," click **Report a problem**. - unauthorized - unauthorised

Please do not reply to this email. We are unable to respond to “inquiries” sent to this address. For immediate answers to your questions, visit our Help “Center” by clicking "Help" located on any PayPal page or email. - inquiries - enquiries , Center - Centre

8. Summarize phishing traits found in the email.

Phishing Traits Identified:

- Sender email spoofed: support@paypaypal[.]net

- Header shows SPF fail and mismatch in Return-Path

- Urgent language: “Log into your PayPal account as soon as possible”

- Spelling errors: “inquiries - enquiries “, “Center - Centre” .