Lab 06: Testing email phishing messages

Table of Contents

Goals:

- Test email phishing messages for content detected as suspicious by different providers.

Requirements:

- Microsoft 365 user accounts created in a previous setup document.
- A personal or work email address that can be used for sending and receiving messages.

Email test example #1: Suspicious message text

1. Log in to your own email address, and send the message below to the Alice user on your Microsoft Azure subdomain.

To:

```
alice@<YOUR SUBDOMAIN NAME>.onmicrosoft.com
```

Subject:

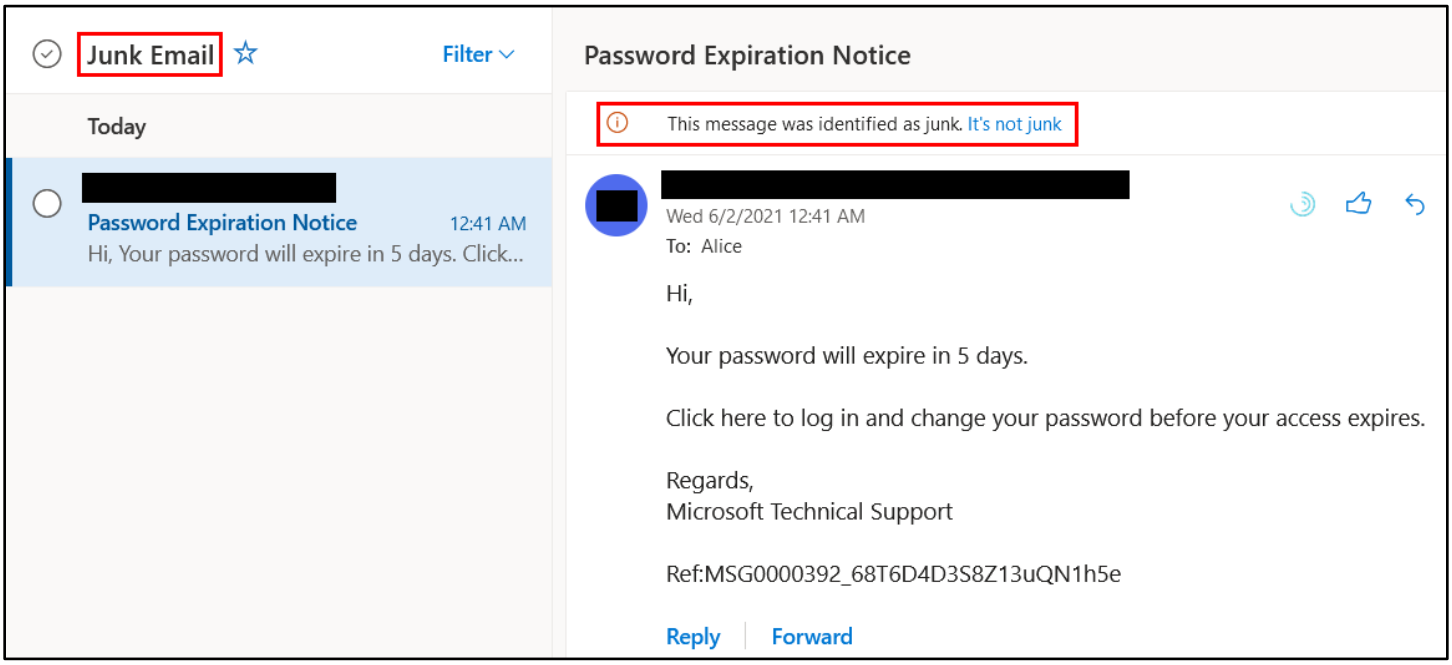
```
Password Expiration Notice
```

Message body:

```
Hi,

Your password will expire in 5 days.

Click here to log in and change your password before your access expires.

Regards,
Microsoft Technical Support

Ref:MSG0000392_68T6D4D3S8Z13uQN1h5e
```

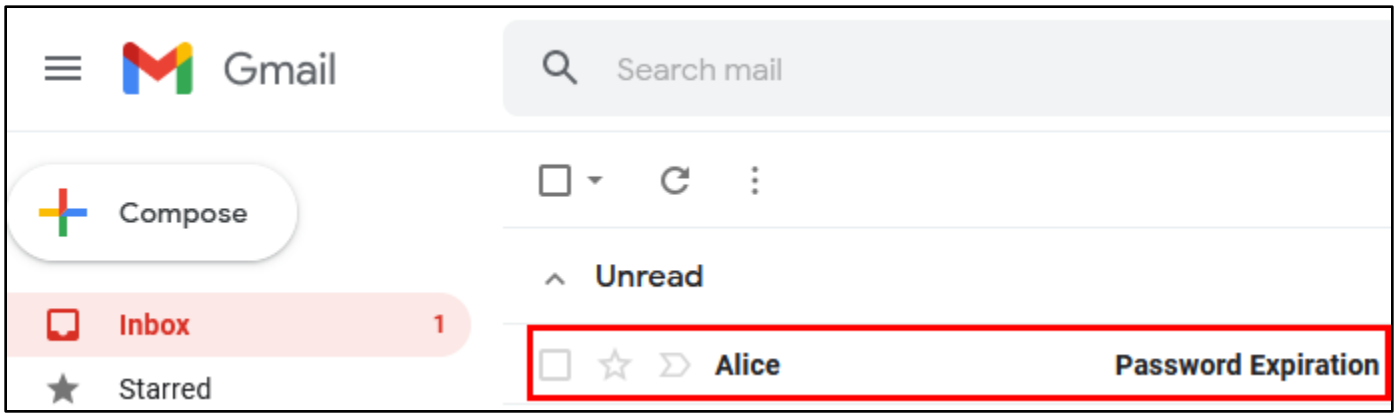

2. After you send the message, log in to Alice's email by visiting the URL below. Then check to see if the message arrived in Alice's inbox or if it went to her Junk folder instead.

```
https://outlook.office365.com
```

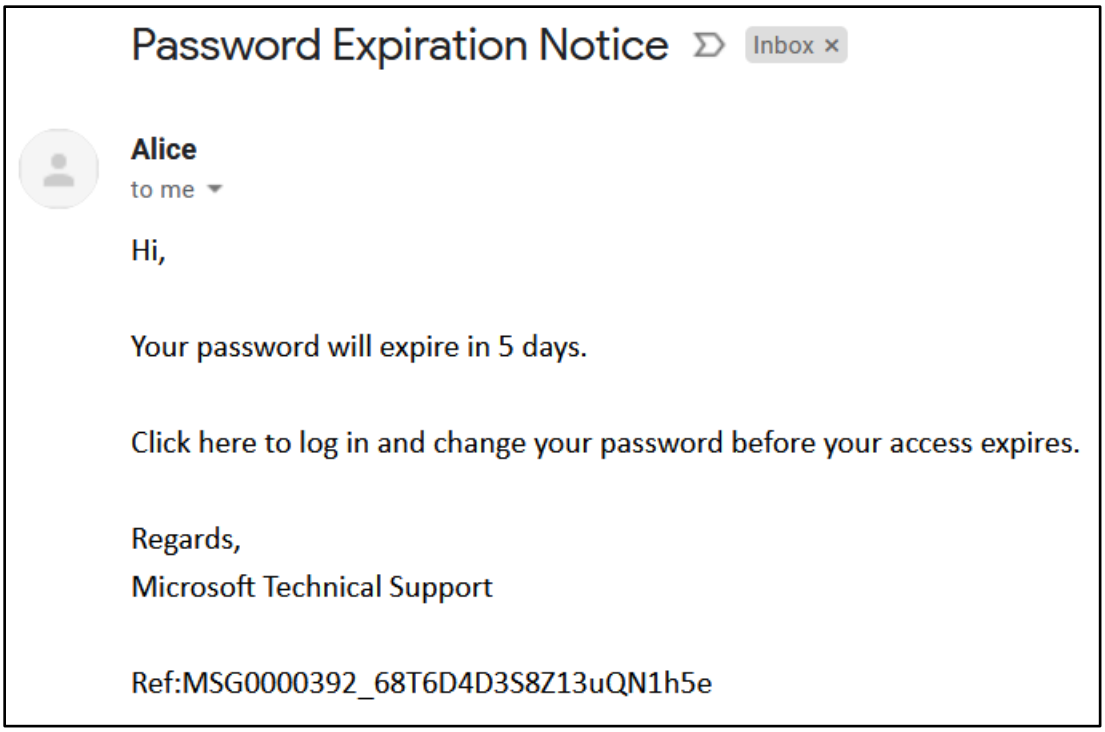


Suspicious Email Message Delivered to Junk Folder

3. In the example above, no links or attachments are included in the email message, so the text in the subject or message body may be causing the message to be flagged as Junk (if not the sender or the sender's server). See if you can modify the text in the subject or the body so that the message has the same meaning but is no longer delivered to the Junk folder. Or, if the message wasn't flagged as junk, see if you can change the text so that the message **does** get flagged.
4. After you've completed step 3, try sending the message in the other direction - from Alice to your personal email account, and see if it gets flagged as junk. When testing the message text used for this lab exercise, I noticed that Microsoft services found the message suspicious, but Gmail did not.



Message Not Flagged as Suspicious by Gmail



Message Body as Seen on Gmail

Email test example #2: Suspicious links

1. Suspicious links and attachments can also cause a message to be filtered out, even if the message text doesn't get detected. Links are often considered especially suspicious if the link text does not match the URL the link references. Test sending another email message, but this time include a link in the message that references a different URL than the link text. An example is shown below.

Subject:

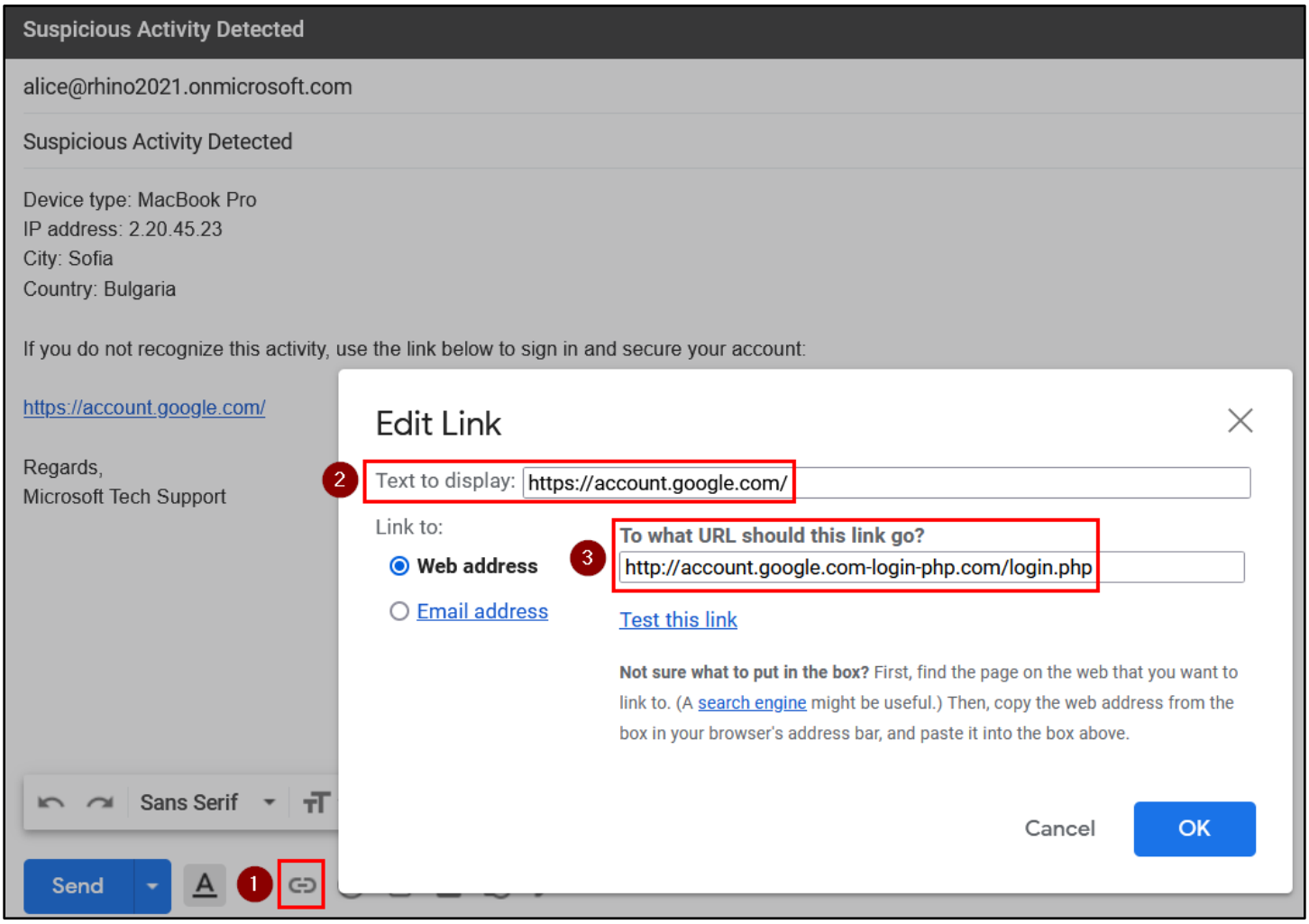
```
Suspicious Activity Detected
```

Message body, with link text shown in red:

```
Device type: MacBook Pro
IP address: 2.20.45.23
City: Sofia
Country: Bulgaria

If you do not recognize this activity, use the link below to sign in and secure
your account:

https://account.google.com/

Regards,
Microsoft Tech Support
```

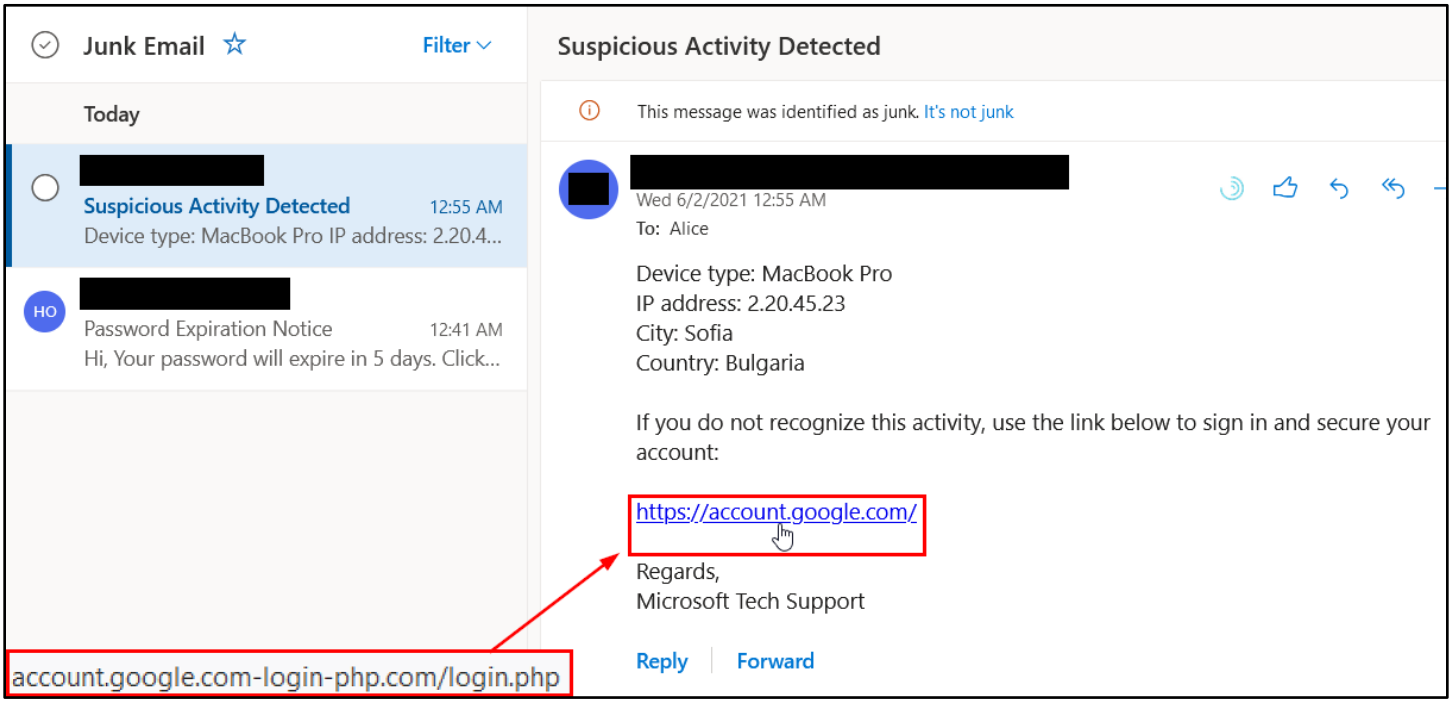
Actual URL referenced by the link:


```
http://account.google.com-login-php.com/login.php
```

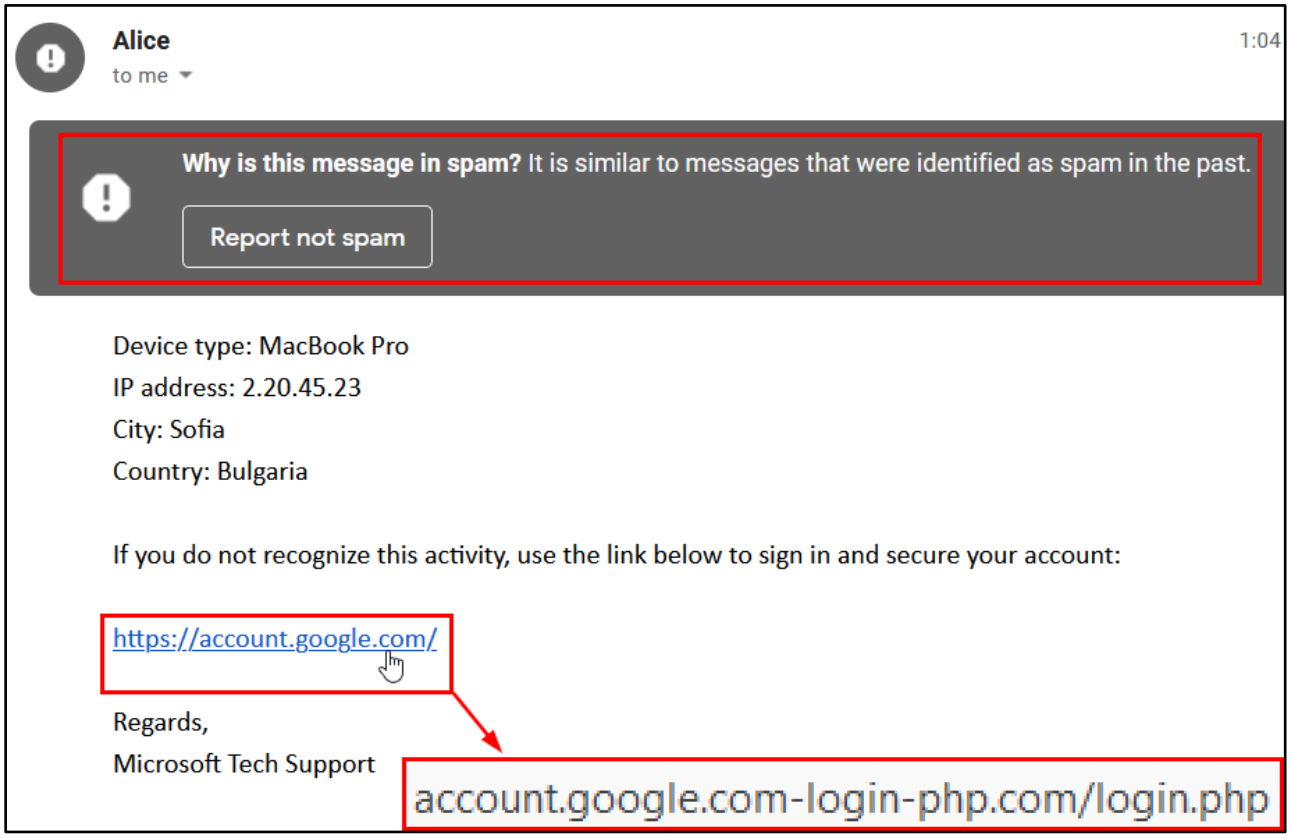


Creating the Suspicious Link in Gmail

2. As before, try sending this message both from your personal email address to Alice, and from Alice to your personal email address.



Email Containing a Spoofed Link Marked as Junk by Outlook.com



A Similarly Suspicious Email Flagged as Spam by Gmail

