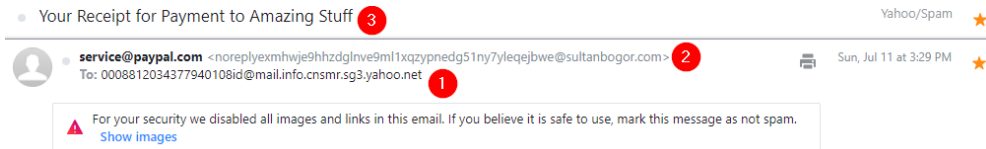


PRACTICE: EXERCISE - SOCIAL ENGINEERING
THM: PHISHING EMAILS IN ACTION
NAME: WAN MUHAMMAD IRFAN BIN MOHD ISA

1. Cancel your PayPal order

- The sender name is service@paypal.com, but the actual email address is gibberish@sultanbogar.com.



- The "Cancel the order" button uses a shortened URL. Checking the HTML reveals it redirects to google.com.

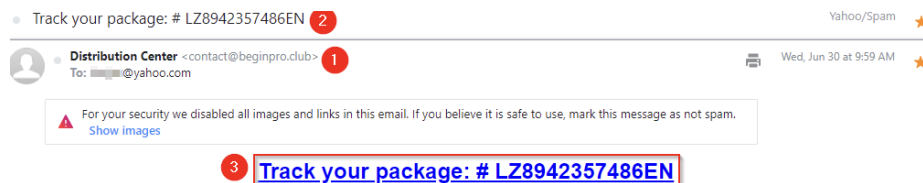
```
<!-- CTA text 17/21 -->
<td bgcolor="#0070BA" align="center" valign="middle" style="padding:13px
90px 13px 90px; display: block; color:#ffffff !important; text-decoration:none; white-space: nowrap;
-webkit-print-color-adjust: exact; display: block; font-family:Calibri, Trebuchet, Arial, sans serif;
font-size:17px; line-height:21px; color:#ffffff !important;border-radius:25px;" class="ppsans
mobilePadding9"><a type="Link" isLinkToBeTracked="true" target="_blank"
linkId="e854f9fff3d47fb841257f9bebb4d1b6" style="text-decoration:none;color:#ffffff !important;
white-space: nowrap;" href="https://is.gd/6oCJ4m?#-u7g?ah7Jel1">Cancel the order</a></td>
<!-- end CTA text --></tr>
```

V

- Question: What phrase does the gibberish sender email start with?
- The gibberish email starts with noreply.

2. Track your package

- The subject line contains a fake tracking number to create interest.
- Checking the email source reveals a hidden image named Tracking.png. This is a tracking pixel used to notify the attacker when the email is opened.

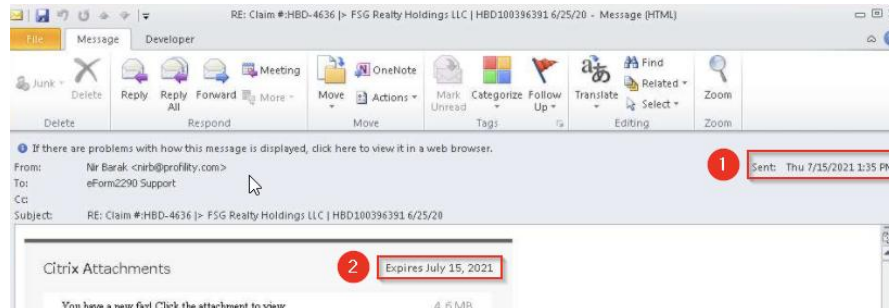


- Question: What is the root domain for each URL? Defang the URL.
- The root domain for the malicious link is devret[.]xyz

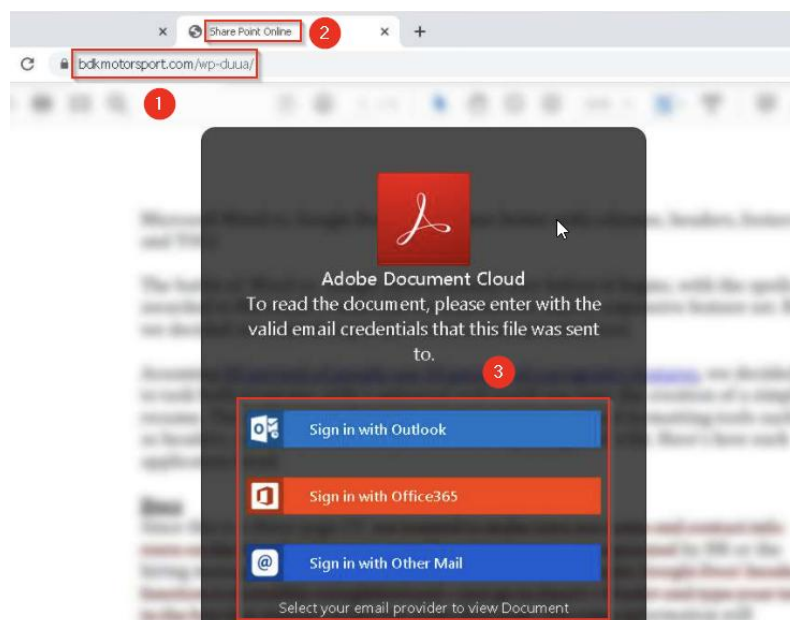
PRACTICE: EXERCISE - SOCIAL ENGINEERING
THM: PHISHING EMAILS IN ACTION
NAME: WAN MUHAMMAD IRFAN BIN MOHD ISA

3. Select your email provider to view document

- Credential harvesting via brand impersonation (OneDrive/Adobe).
- High sense of urgency (claim that the link expires today).



- Clicking the "download" button leads to a fake login page designed to steal credentials.



- Question: This email sample used the names of a few major companies, their products, and logos such as OneDrive and Adobe. What other company name was used in this phishing email?
- Another company name used in this email is citrix.

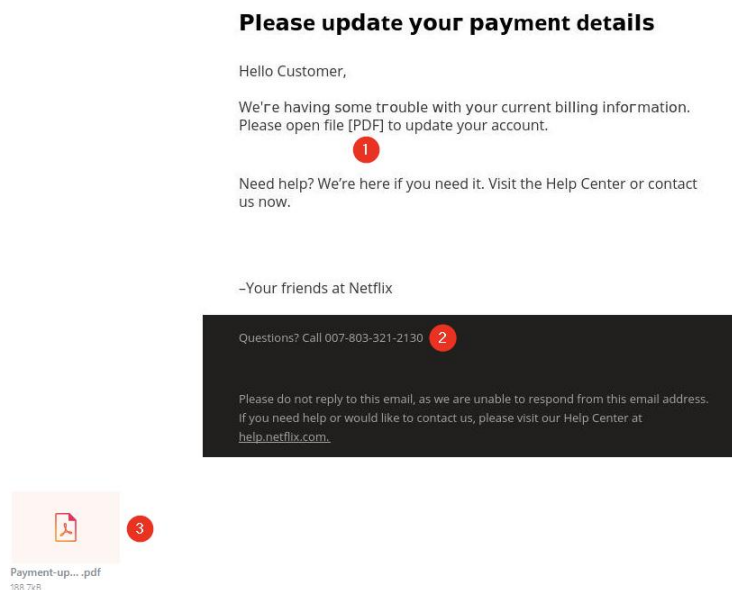
PRACTICE: EXERCISE - SOCIAL ENGINEERING
THM: PHISHING EMAILS IN ACTION
NAME: WAN MUHAMMAD IRFAN BIN MOHD ISA

4. Please update your payment details

- Impersonating Netflix.
- Multiple typos in the email body (misspelling "Netflix").

```
<div><b>From:</b><b>Netflix billing <mailto:99@musacombl.online></div><div><b>Sent:</b> Wednesday, March 10, 2021, 09:08:23 AM EST</div><div><b>Subject:</b><b>Netflix ID Suspended</div><div><br></div><div><div id="ydp9e457468yiv9006393007"><div dir="ltr"><img src="cid:c31abd8f-2247-e81c-a76b-afb361b5b1e5@yahoo.com" alt="accountid11.jpg" style="margin-right: 25px; width: 100%; max-width: 800px;"
```

- The email claims the account is suspended and includes a malicious PDF attachment titled "Update Payment Account."

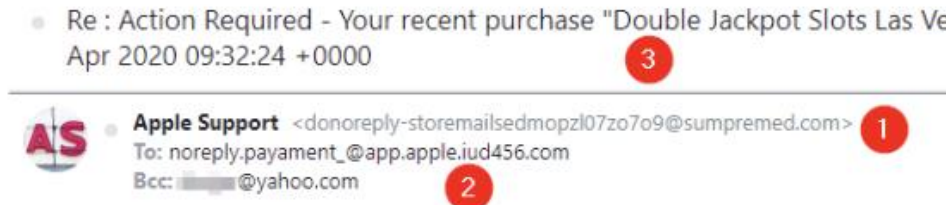


- Question: What should users do if they receive a suspicious email or text message claiming to be from Netflix?
 - Suspicious emails claiming to be from Netflix should be forwarded to phishing@netflix.com.

PRACTICE: EXERCISE - SOCIAL ENGINEERING
THM: PHISHING EMAILS IN ACTION
NAME: WAN MUHAMMAD IRFAN BIN MOHD ISA

5. Your recent purchase

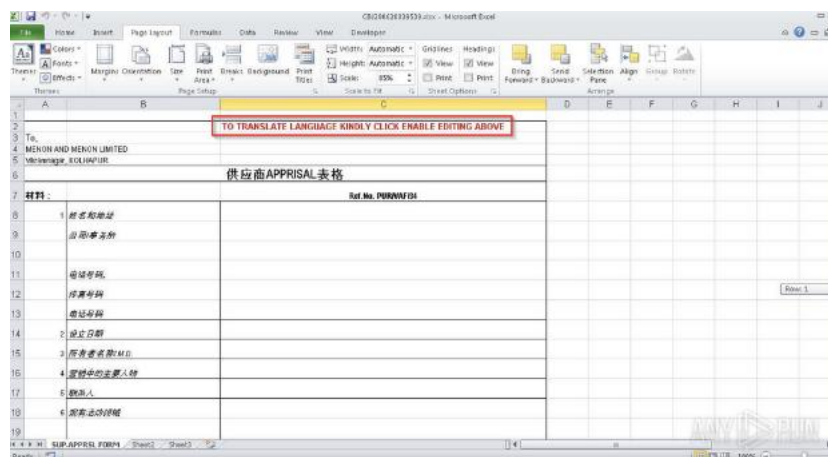
- Using BCC (Blind Carbon Copy) and Urgency.
- You are not in the "To" field; you were BCC'ed. This is common in mass phishing campaigns.
- The email mimics Apple Support. The sender's real address is gibberish@sumpremed.c



- Question: What does BCC mean?
 - Its means Blind Carbon Copy.
- Question: What technique was used to persuade the victim to not ignore the email and act swiftly?
 - The technique used to make the victim act swiftly is Urgency.

6. DHL Express Courier Shipping notice

- Malicious attachments (Excel).
- The "View as a web page" link has no destination; the only way to interact is via the attachment.
- The Excel attachment contains a payload. When run, it attempts to execute a malicious file.



- Question: What is the name of the executable that the Excel attachment attempts to run?
 - The executable the attachment tries to run is regasms.exe.

PRACTICE: EXERCISE - SOCIAL ENGINEERING
THM: PHISHING EMAILS IN ACTION
NAME: WAN MUHAMMAD IRFAN BIN MOHD ISA

7. Completion

