Table of Contents –

[Duty 1) – Threat Inquiry from Jason’s TI Team (30 minutes) 2](#_Toc178345202)

[Duty 1a) - Access CVE (vulnerability) / Security Incident 2](#_Toc178345203)

[Duty 1b) Check the product of CVE / Security Incident affect HKMA 3](#_Toc178345204)

[Duty 2) Phishing Email Handling (1-2 hours) 4](#_Toc178345205)

[Duty 2a) Access Jira Ticket 4](#_Toc178345206)

[JIRA ticket comment template 5](#_Toc178345207)

[Duty 2b) In-depth Procedures for Analysis 6](#_Toc178345208)

[1) Recipient + 2) Sender Email Address + 4) URL + 5) Attachment 6](#_Toc178345209)

[3) Sender IP address 8](#_Toc178345210)

[6) Conclusion 10](#_Toc178345211)

[Duty 3 – Police Force 14](#_Toc178345212)

# Duty 1) – Threat Inquiry from Jason’s TI Team (30 minutes)

## Duty 1a) - Access CVE (vulnerability) / Security Incident

**Ping Yong Leelalertwijit**

(At 10am)

Hello Yong, may I know if this morning have any CVE / Security Incident? Thanks

(At 3pm)

Hello Yong, may I know if this afternoon have any CVE / Security Incident? Thanks

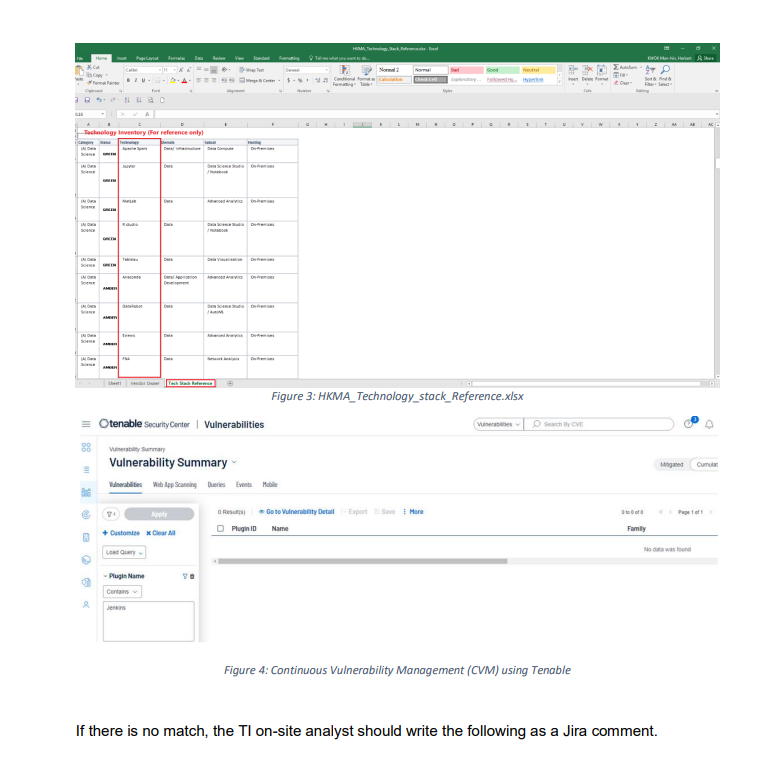
## Duty 1b) Check the product of CVE / Security Incident affect HKMA

Step 1) You can check HKMA using product according to **below list**:

1. [HKMA Inventory List](https://masp.hkma.gov.hk/sites/SOCFilingDB/Lists/SOC%20Filing%20Database/DispForm.aspx?ID=100&Source=https%3A%2F%2Fmasp%2Ehkma%2Egov%2Ehk%2Fsites%2FSOCFilingDB%2FLists%2FSOC%2520Filing%2520Database%2FBy%2520Category%2Easpx%3Fweb%3D1&ContentTypeId=)
2. [HKMA Internal Tenable](https://172.28.80.24/) – May need grant access

Step 2) If confirm the affected product used in HKMA, Report to Alex Li via Nxtchat/Go to his seat

Screenshot of Inventory list & Tenable below



# Duty 2) Phishing Email Handling (1-2 hours)

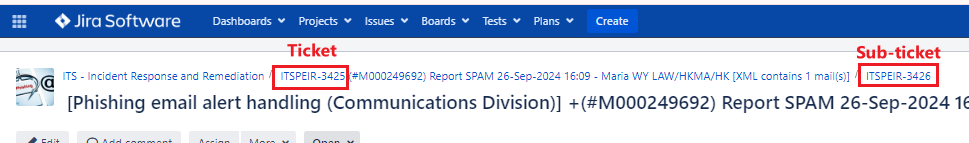
## Duty 2a) Access Jira Ticket

Step 1) Access ITSPEIR <https://jira.intra.hkma.gov.hk/issues/?jql=project%20%3D%20ITSPEIR%20AND%20issuetype%20%3D%20Sub-task%20ORDER%20BY%20created%20DESC>

Step 2) Click the ticket whose status is ‘OPEN’

If the ticket’s status is ‘OPEN’, it implies it has not been analysed.

Step 3) Open both ticket and sub-ticket



Ticket 🡪 Show Email Content

Sub-ticket 🡪 Drop ticket comment

Step 4) Mark the ticket and sub-ticket as ‘In Progress’, change the assignee to ‘Li Kwok Ho, Alex’.

## JIRA ticket comment template

1. Recipient  
[Recipients.csv]

2. Sender email address

|  |  |
| --- | --- |
| **Email address** | **Reputation** |
| %Email% | VT: %score, e.g., 0/94% AbuseIPDB: %Number of report by users%  [Screenshot of domain] |

3. Sender IP address

|  |  |
| --- | --- |
| **IP address** | **Reputation** |
| %Sender IP% | VT: %score, e.g., 0/94% AbuseIPDB: %Number of report by users% |

4. URL

|  |  |  |
| --- | --- | --- |
| **URL** | **Reputation** | **Screenshot** |
| %URL in Email% | - | - |

   
5. Attachment

|  |  |  |
| --- | --- | --- |
| **Attachment** | **Reputation** | **Screenshot** |
| %Attachment in Email% | - | - |

6. Conclusion  
%Reason to support the email belongs to unwanted/spam/phishing category%

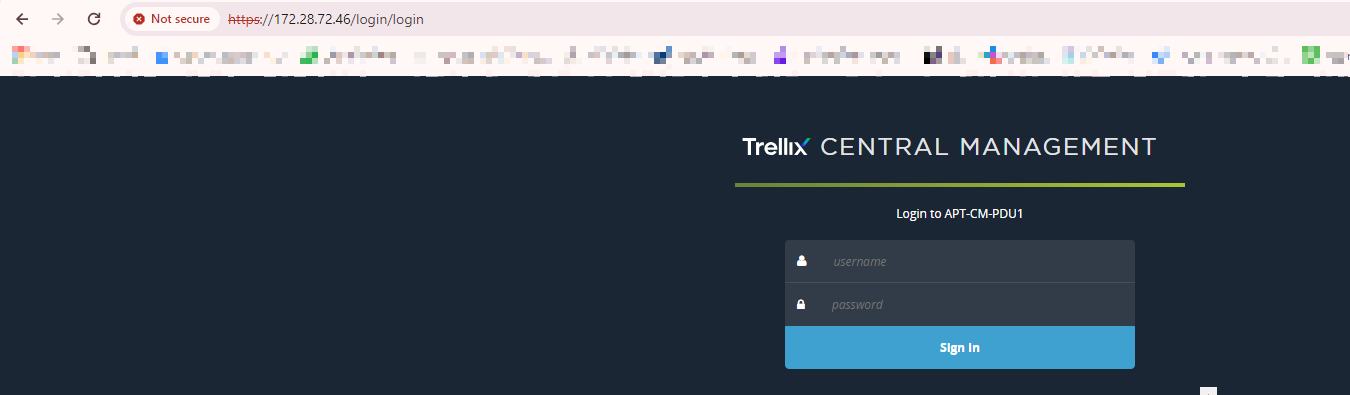
This appear to be %unwanted/spam/phishing% email.

## Duty 2b) In-depth Procedures for Analysis

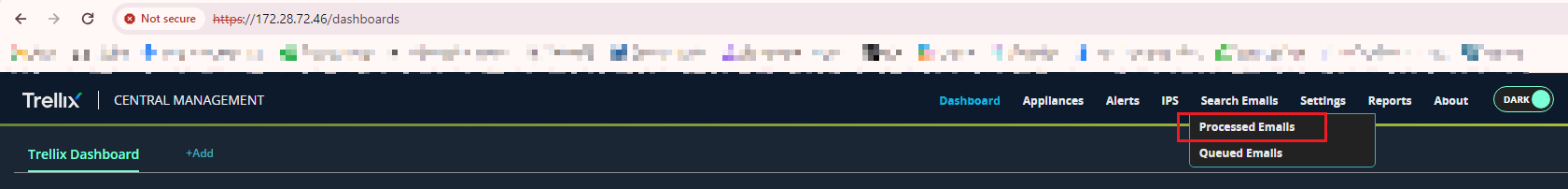
### 1) Recipient + 2) Sender Email Address + 4) URL + 5) Attachment

Step 1)

Login [Trellix APT](https://172.28.72.46/login/login) in HKMA machine

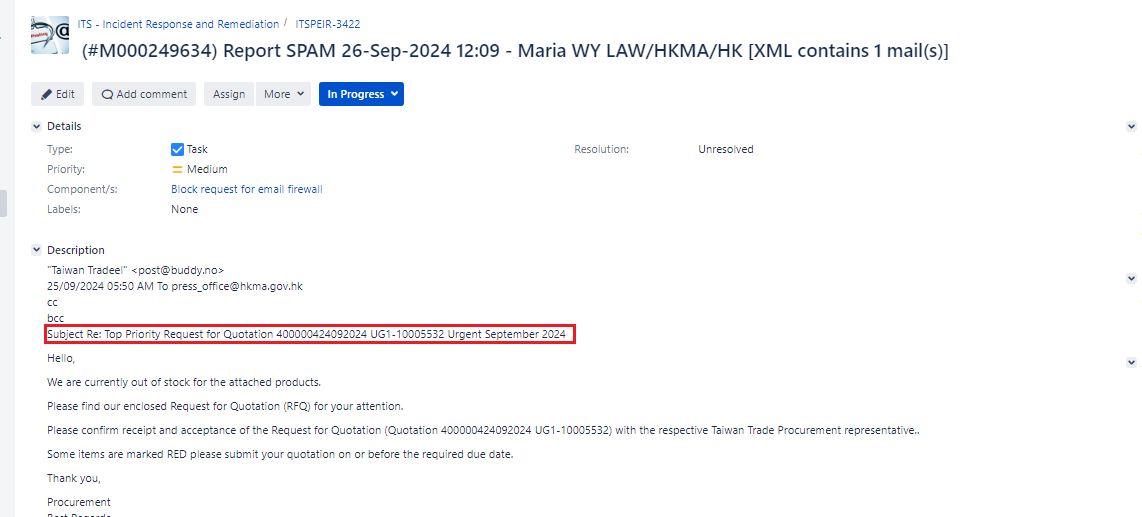


Step 2) “Search Emails” 🡺 Processed Emails

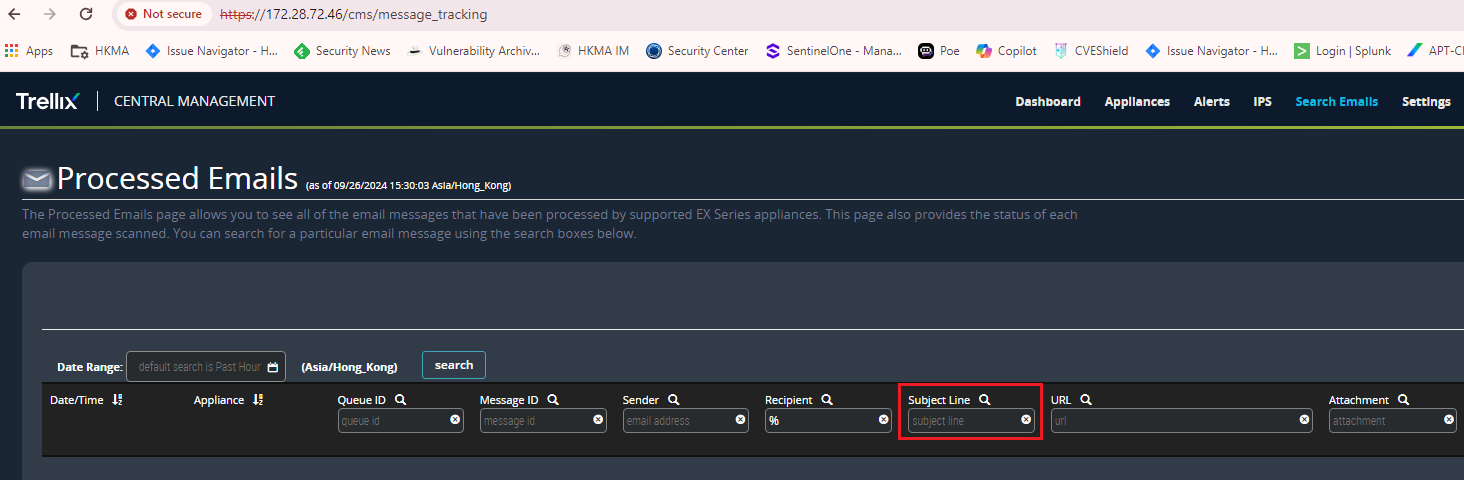


Step 3) Use the format “%Subject Title of Email%” , insert in subject line

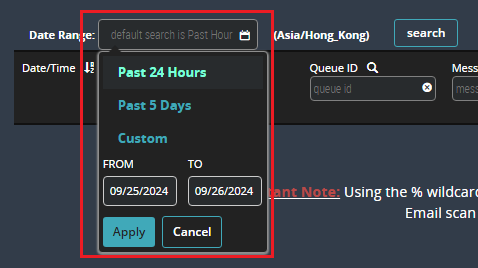
Copy from here



Paste here



Step 4) Select Date Range

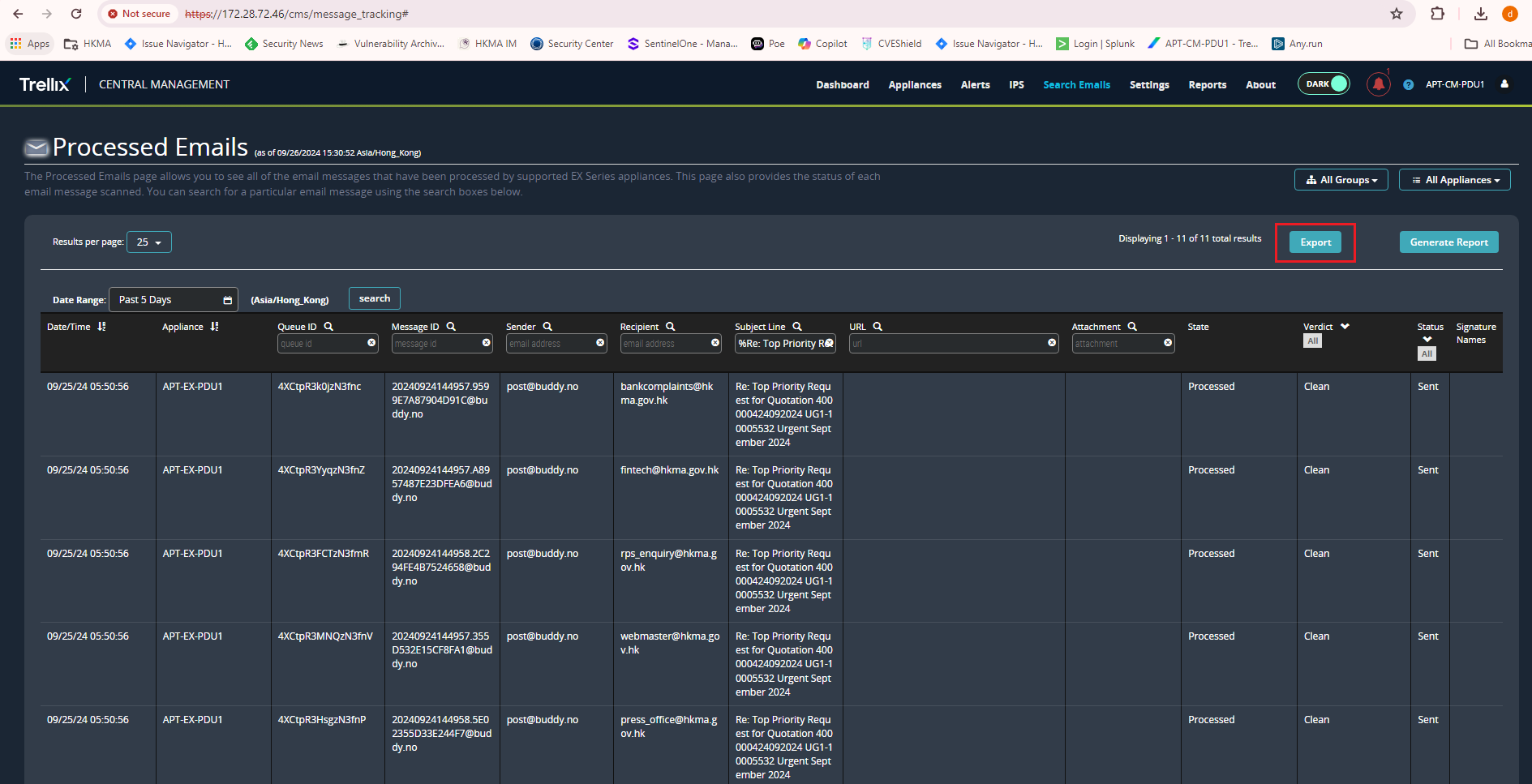


Step 5) Export as .csv if recipient > 1, upload the raw .csv onto the JIRA ticket

Step 6a) Sender Email Address can be found in column “sender”

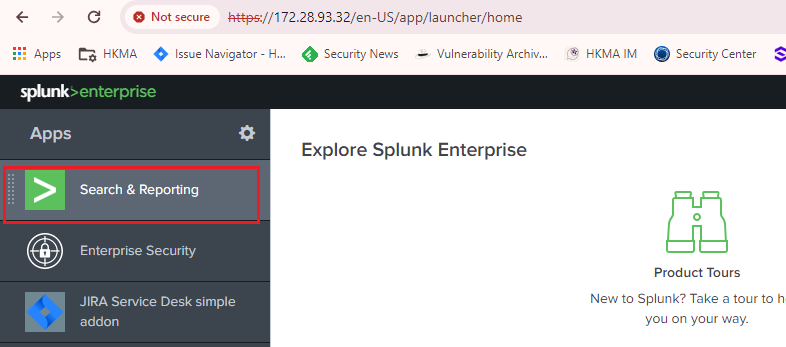
Step 6b) URL can be found in column “URL”

Step 6c) Attachment can be found in column “Attachment”



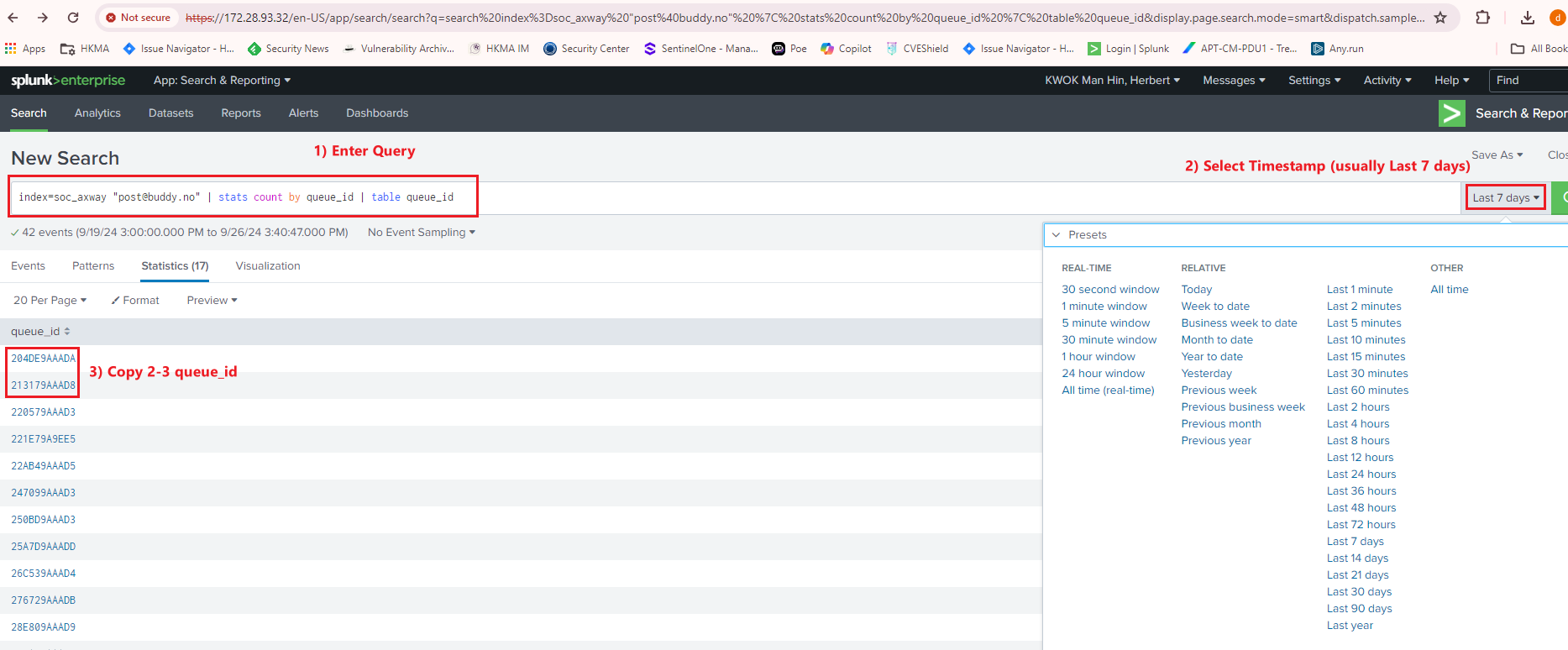
### 3) Sender IP address

Step 1) Login [Splunk](https://172.28.93.32/)

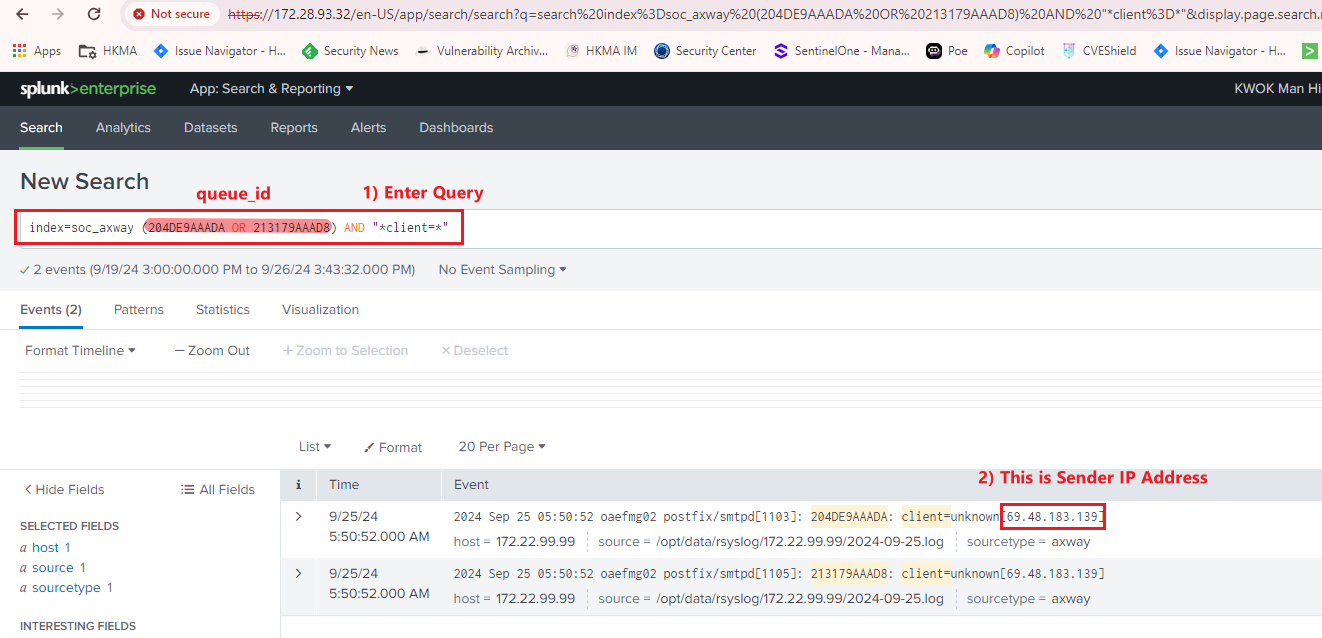
Step 2) Select “Search & Reporting”

Step 3) Enter following commands:

Step 3a) index=soc\_axway "%Sender Email (Found in Trellix APT)%" | stats count by queue\_id | table queue\_id



Step 3b) index=soc\_axway (%Queue ID%) AND "\*client=\*"



### 6) Conclusion

Step 1) Reply the email to users (who report the email) with content **(See below for “Reply Email template”)**

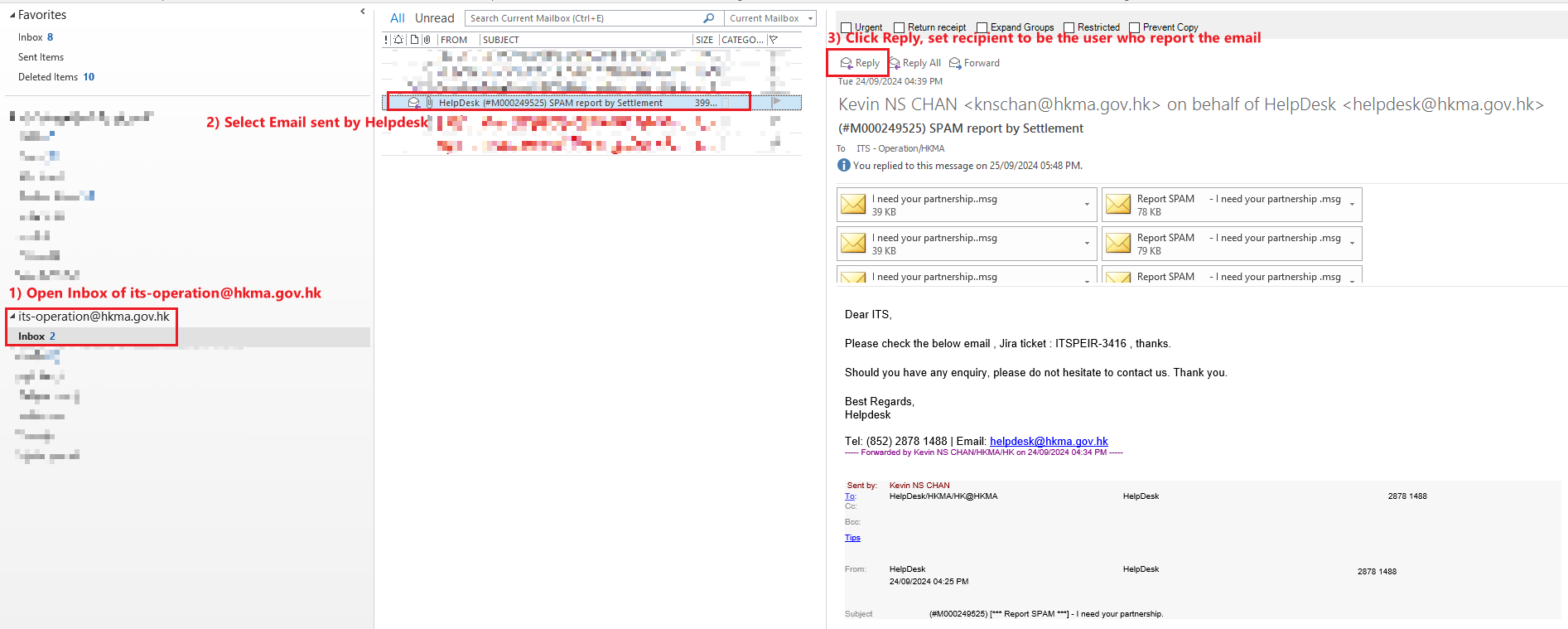
Place this content at the top of the email sent by the Helpdesk, according to the category you identify (**Unwanted, Spam, Phishing**).

Unwanted: e.g., “Think twice before printing.”

Spam: e.g., “Lure / Urgent / Top priority.”

Phishing: e.g., “Contain URL/Attachment -> Urgent -> Lure users to Enter credentials / Malware / Ransomware.”

Remember DO NOT send the email in advance.



Step 2) Check ticket with Alex Li (Go to his seat) (Explain your findings + Conclude the type of email)

Step 3) Once sign off, TI on-site analyst send the email (on behalf of [its-operations@hkma.gov.hk](mailto:its-operations@hkma.gov.hk))

Step 4) Attach the sent email into the sub-ticket, Alex Li marks it as ‘Done’.

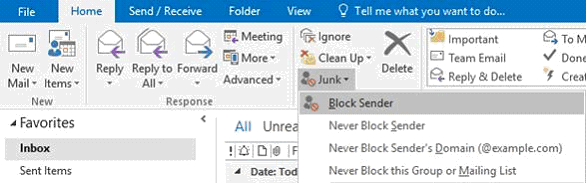
Reply Email Template - Unwanted Email

Dear User,  
  
Thank you for reporting the suspicious email from “%Email Title%”.

After investigation, there is no malicious url/attachment observed in the email. The reported email is classified as an unwanted message instead of spam.  
  
No further action is required from your side.  However, if you would like to block the sender, please follow the instructions below.  This will move future emails from the same sender to your Junk folder:

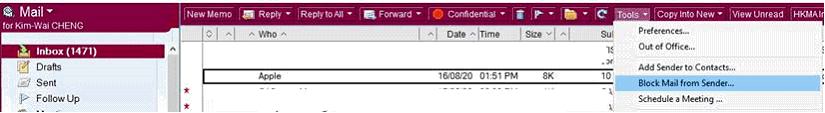
**For CMMP Users:**

1. Select the unwanted email  
2. Go to Junk > Block Sender



**For Lotus Notes Users:**

1. Select the unwanted email  
2. Go to Tools > Block Mail from Sender



Should you have any enquiries, please contact Alex Li at 5945. Thank you.

Regards,

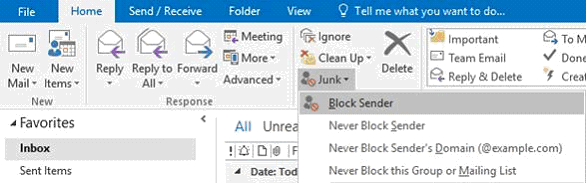
IT Security

Reply Email Template - Spam Email

Dear User,  
  
Thank you for reporting the suspicious email “%Email Title%”.  
  
After investigation. The reported email is classified as a spam email.  
  
We suggest to delete the email permanently and do not access any url/attachment embedded in the email. If you would like to block the sender, please follow the instructions below.  This will move future emails from the same sender to your Junk folder:

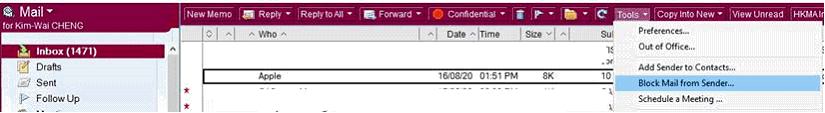
**For CMMP Users:**

1. Select the unwanted email  
2. Go to Junk > Block Sender



**For Lotus Notes Users:**

1. Select the unwanted email  
2. Go to Tools > Block Mail from Sender



Should you have any enquiries, please contact Alex Li at 5945. Thank you.

Regards,

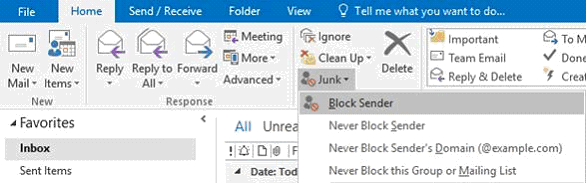
IT Security

Reply Email Template - Phishing Email

Dear User,  
  
Thank you for reporting the suspicious email “%Email Title%”.  
  
After investigation. The reported email is classified as a phishing email.  
  
We suggest to delete the email permanently and do not access any url/attachment embedded in the email. If you would like to block the sender, please follow the instructions below.  This will move future emails from the same sender to your Junk folder:

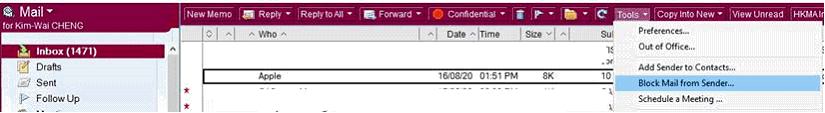
**For CMMP Users:**

1. Select the unwanted email  
2. Go to Junk > Block Sender



**For Lotus Notes Users:**

1. Select the unwanted email  
2. Go to Tools > Block Mail from Sender



Should you have any enquiries, please contact Alex Li at 5945. Thank you.

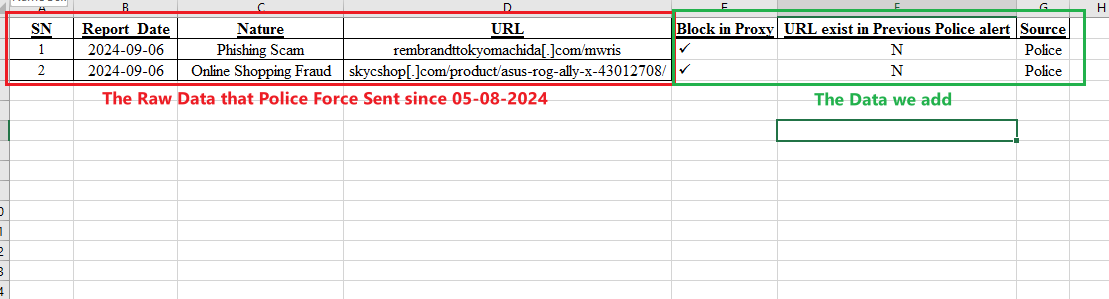
Regards,

IT Security

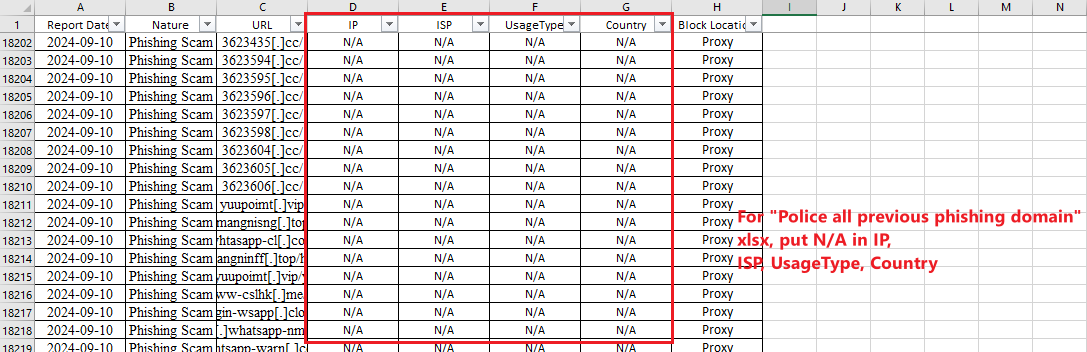
# Duty 3 – Police Force

Step 1) Paste the following column at the back

|  |  |  |
| --- | --- | --- |
| **Block in Proxy** | **URL exist in Previous Police alert** | **Source** |
|  |  |  |



Step 2) “Police all previous phishing domain” put N/A in IP, ISP, UsageType, Country



3) Other procedures remains the same