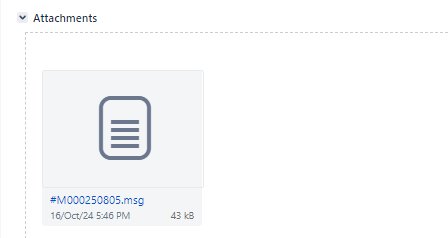
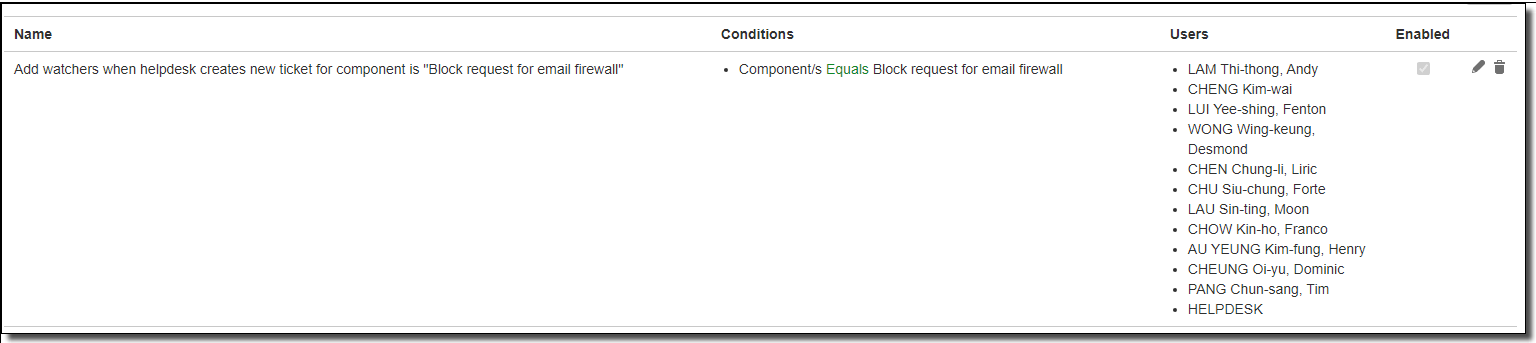
**Last update on 18 October 2024**

**Communications Team**

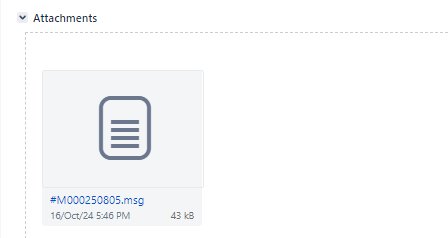
**User guide on creating Jira ticket for handling phishing email incident**

|  |  |
| --- | --- |
| Members of the Helpdesk Team | 1. Go to <https://jira.intra.hkma.gov.hk/projects/ITSPEIR/> 2. Click Create button 3. Input case no and email subject in Summary 4. Choose “Block request for email firewall” 5. Copy and paste email content in Description 6. Browse and insert attachment (in .msg format) 7. Change Assignee to “CHOW Tin-tik, Timmy” and click Create button 8. Add “CHOW Kin-ho, Franco”, “AU YEUNG Kim-fung, Henry”, “CHU Siu-chung, Forte “, “LAU Sin-ting, Moon”, "PANG Chun Sang, Tim", "Helpdesk". “LUI Yee-shing, Fenton “ and “Lam Thi-thong, Andy” in Watchers. 9. Create sub-task for SOC      1. Add Summary, Component and Description 2. **Phishing email impersonating (Communications) case**   Summary: [Phishing email impersonating (Communications)] + Main task summary  e.g.  [Phishing email impersonating (Communications)] (#M000207533) Report SPAM 07-Dec-2022 11:04 - Ang LI/HKMA/HK [XML contains 1 mail(s)]  Component: Phishing email alert handling (Communications/Settlement team)  Description:  As user has reported phishing email impersonating Communications Team, please kindly help to take the following actions for the alert. Thank you.  Provide recipients list of the email  Provide investigation result of the email?  Modify the Priority to “Medium”    Click “Create”     1. **Phishing email alert handling (Communications) case**   Summary: [Phishing email alert handling (Communications)] + Main task summary  e.g.  [Phishing email alert handling (Communications)] (#M000207533) Report SPAM 07-Dec-2022 11:04 - Ang LI/HKMA/HK [XML contains 1 mail(s)]  Component: Phishing email alert handling (Communications/Settlement team)  Description:  As user has reported phishing email, please kindly help to take the following actions for the alert. Thank you.   * Provide recipients list of the email * Provide investigation result of the email     Modify the Priority to “Medium”    Click “Create” |
| Members of the Mail Team | 1. Click the Comment button 2. Input comment and click Add button. 3. Click “In Progress” button. |
| Members of the Mail Team | 1. Input comment and click Add button. 2. Identify the type of email (Unwanted, Spam, Phishing) and remark in the comment. 3. The analyst forwards the reported email to the PwC mailbox (xxxx@darklab.hk), which automatically processes and classifies the email type.   Note: The table below outlines the correspondence between each type of email and its associated manual procedures and follow-up actions:   |  |  | | --- | --- | | Type of Email | Manual Procedures / Follow-up | | Spam | Not applicable, unless specifically requested by the Communications/Settlement Team. | | Phishing | Determine if the phishing campaign is targeting HKMA.   * Check for any malicious links or attachments in the campaign. * Investigate if similar patterns or campaigns have been observed from known malicious actors. | | Spoofing | Determine if the spoofing campaign is attempting to impersonate HKMA.   * Examine the email content for indicators such as malicious offers, financially related requests, or ransom notes. * Investigate if similar patterns or campaigns have been observed from known malicious actors. |   Remark: If the email contains confidential or sensitive information, the user should refrain from forwarding it externally and if necessary, alert on-site analyst “Kwok Man-Hin, Herbert” to perform the necessary analysis.   1. Change Assigneeto “LI Kwok-ho, Alex”. |
| Members of the Mail Team | 1. Reply the email on behalf of “its-operations@hkma.gov.hk” to users (who report the email) with content      1. Comment and mention the attachment. 2. Attach the sent email into the sub-ticket, AD(IT)(ITS)3 marks it as ‘Done’. |

Annex – Watcher List



**Settlement Team**

**User guide on creating Jira ticket for handling phishing email incident**

|  |  |
| --- | --- |
| Members of the Helpdesk Team | 1. Go to <https://jira.intra.hkma.gov.hk/projects/ITSPEIR/> 2. Click Create button 3. Input case no and email subject in Summary 4. Choose “Block request for email firewall” 5. Copy and paste email content in Description 6. Browse and insert attachment (in .msg format) 7. Change Assignee to “CHOW Tin-tik, Timmy” and click Create button 8. Add “CHOW Kin-ho, Franco”, “AU YEUNG Kim-fung, Henry”, “CHU Siu-chung, Forte “, “LAU Sin-ting, Moon”, "PANG Chun Sang, Tim", "Helpdesk". “LUI Yee-shing, Fenton “ and “Lam Thi-thong, Andy” in Watchers. 9. Create sub-task for SOC      1. Add Summary, Component and Description 2. **Phishing email impersonating (Settlement) case**   Summary: [Phishing email impersonating (Settlement)] + Main task summary  e.g.  [Phishing email impersonating (Settlement)] (#M000207533) Report SPAM 07-Dec-2022 11:04 - Ang LI/HKMA/HK [XML contains 1 mail(s)]  Component: Phishing email alert handling (Communications/Settlement team)  Description:  As user has reported phishing email impersonating Settlement Team, please kindly help to take the following actions for the alert. Thank you.  Provide recipients list of the email  Provide investigation result of the email?  Modify the Priority to “Medium”    Click “Create”     1. **Phishing email alert handling (Settlement) case**   Summary: [Phishing email alert handling (Settlement)] + Main task summary  e.g.  [Phishing email alert handling (Settlement)] (#M000207533) Report SPAM 07-Dec-2022 11:04 - Ang LI/HKMA/HK [XML contains 1 mail(s)]  Component: Phishing email alert handling (Communications/Settlement team)  Description:  As user has reported phishing email, please kindly help to take the following actions for the alert. Thank you.   * Provide recipients list of the email * Provide investigation result of the email     Modify the Priority to “Medium”    Click “Create” |
| Members of the Mail Team | 1. Click the Comment button 2. Input comment and click Add button. 3. Click “In Progress” button. |
| Members of the Mail Team | 1. Input comment and click Add button. 2. Identify the type of email (Unwanted, Spam, Phishing) and remark in the comment. 3. Change Assigneeto “LI Kwok-ho, Alex”. |
| Members of the Mail Team | 1. Reply the email on behalf of “its-operations@hkma.gov.hk” to users (who report the email) with content      1. Comment and mention the attachment. 2. Attach the sent email into the sub-ticket, AD(IT)(ITS)3 marks it as ‘Done’. |

Annex – Watcher List

