🛡️ Phishing Alert Ticket Response by Jordan Butler

Ticket Status:

Escalated (per playbook Step 3.2)

Ticket Comments:

Summary of Alert:
A phishing alert was generated after a password-protected spreadsheet was downloaded by an employee from a suspicious email. Upon analysis, the attachment's hash was submitted to a threat intelligence platform and was confirmed to be **malicious**.

Incident Details:

- **Alert Severity:** Medium
- **Attachment Type:** Password-protected `.xlsx` file
- **Email Source:** Unknown external sender
- **Method of Detection:** Suspicious file download alert
- **Analysis Performed:** File hash submitted to VirusTotal; result returned as known malicious
- **User Impact:** Employee may have opened a malicious file

Action Taken:
Following the **Phishing Incident Response Playbook**, the alert was thoroughly reviewed:

1. **Step 1:** Phishing alert received and ticket opened
2. **Step 2:** Evaluated the alert details, including sender/receiver info, file type, and behavior
3. **Step 3.0:** Confirmed the email **contained an attachment**
4. **Step 3.1:** Verified the attachment's hash using a trusted threat intel source (VirusTotal)
5. **Step 3.2:** Hash was confirmed malicious → **Ticket escalated**

Justification for Escalation:
Based on the playbook guidance, any phishing alert involving **confirmed malicious attachments** must be escalated. This file presents a risk of further compromise or lateral

movement. Escalation ensures containment and eradication steps are taken by Tier 2 analysts or Incident Response personnel.

Next Steps Recommended:

- Notify Level 2 SOC analyst
- Isolate the affected endpoint
- Conduct deeper forensic analysis
- Notify user and educate on phishing awareness
- Update threat detection rules/signatures if needed