Task 2 Example Answer

Task 2 Example Answer:

What kind of attack has happened, and why do you think so?

- In a **phishing** attack, the perpetrator pretends to be a reputable entity or person via email to obtain sensitive information like login credentials. In this case, the attacker disguised as the company's HR by asking employees to update their timesheets.
- **Malware** is intrusive software designed to harm or exploit computers. In this case, the user executed a phishing attack payload that may have installed malware onto their system. As users cannot open a Word document that they have always been able to open, this could be ransomware or a virus.

  As a cyber security analyst, what are the next steps to take? List all that apply.
- Begin documenting the investigation.
- Prioritise handling the incident based on factors such as functional impact, information impact and recoverability effort.
- Advise users to change and strengthen all logins, passwords and security questions.

  How would you contain, resolve and recover from this incident? List all answers that apply.
- Identify and mitigate all exploited vulnerabilities.
- Attempt to remove malware from all hosts affected.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.
- Stay alert and continue to monitor for any similar future activity.

  What activities should be performed post-incident?
- Follow-up report detailing everything that occurred.
- Hold a lesson-learnt meeting.
- Educate: Create a cyber awareness program for employees. Such programs help employees identify future phishing emails.