**Here is the background information on your task**

As a member of the cyber security division, your team must handle this incident and the team lead has assigned the issue to you. Below is the timeline of events:

* 10:30 a.m. – The IT Service Desk receives a report from one of your colleagues at the bank that they have received an email from HR telling all employees to update their timesheets in the company’s support portal so the timesheets can be approved on time by their line managers against the next pay day. The colleague clicked the link in the email that opened what looked like the portal. However, following the employee's input of the user credentials, an unfamiliar error page appeared like the one below.

A screenshot of a computer

Description automatically generated

* 2:00 p.m. – Eight more reports of emails similar to the one reported earlier are received by the IT Service Desk. Upon further investigation, it was found that 62 colleagues across the Risk Department received the same email over the course of two days.  The emails directed the users to a fake website to steal their usernames and passwords and download a harmful program.
* 3:50 p.m. – The IT Service Desk receives calls and emails from more colleagues that the file-shares are not opening and they receive an error when trying to open a Word document they have always been able to open.

**Here is your task**

In addition to the background information above, study the links in the Resources to learn how to provide solutions to the following questions. Answer the questions in the text input below.

***Hint:*** *From the links below, you should look for types of cyber security attacks and the steps to take after an incident.*

1. What kind of attack has happened and why do you think so?
2. As a cyber security analyst, what are the next steps to take? List all that apply.
3. How would you contain, resolve and recover from this incident? List all answers that apply.
4. What activities should be performed post-incident?

*Please note that the scenario described in this module is fictional and was created just for your virtual experience.*

**Here are some resources to help you**

1. [Top 10 Common types of Cybersecurity Attacks (infocyte.com)](https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks)
2. [11 Types of Phishing + Real-Life Examples (pandasecurity.com)](https://www.pandasecurity.com/en/mediacenter/tips/types-of-phishing/)
3. [8 Critical steps to take after a ransomware attack: Ransomware response guide for businesses - Emsisoft | Security Blog](https://blog.emsisoft.com/en/36921/8-critical-steps-to-take-after-a-ransomware-attack-ransomware-response-guide-for-businesses/)
4. [Battling Ransomware: How to Respond to a Ransomware Incident (forbes.com)](https://www.forbes.com/sites/forbestechcouncil/2018/12/27/battling-ransomware-how-to-respond-to-a-ransomware-incident/?sh=b464b4864dc6)
5. [Frequently Asked Questions - Ransomware | Information Security Office (berkeley.edu)](https://security.berkeley.edu/faq/ransomware/)
6. [What to do before and after a cybersecurity breach? | american.edu](https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf)

**Here is your task**

In addition to the background information above, study the links in the Resources to learn how to provide solutions to the following questions. Answer the questions in the text input below.

***Hint:*** *From the links below, you should look for types of cyber security attacks and the steps to take after an incident.*

1. What kind of attack has happened and why do you think so?
2. As a cyber security analyst, what are the next steps to take? List all that apply.
3. How would you contain, resolve and recover from this incident? List all answers that apply.
4. What activities should be performed post-incident?

**Task 2 Example Answer:**

1. 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.
2. 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.
3. 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.
4. 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.