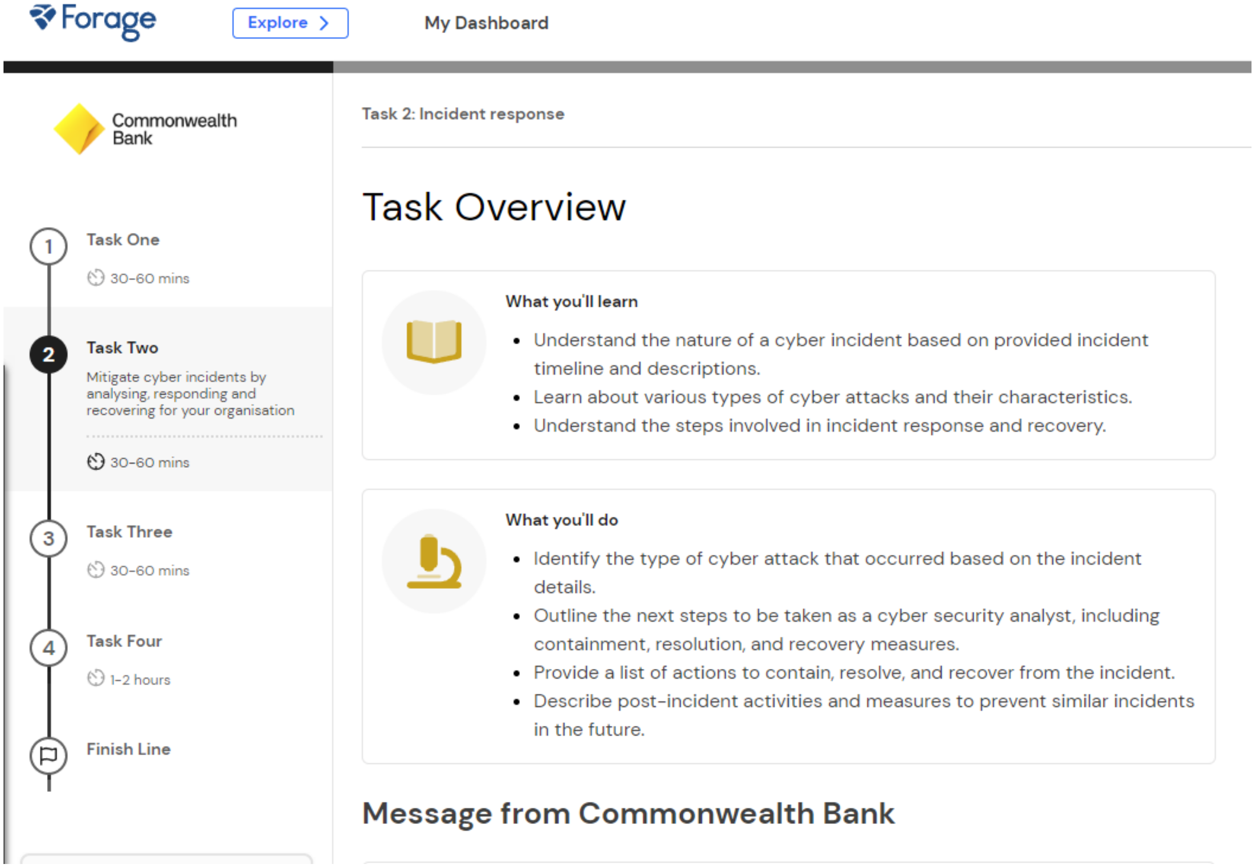
Task 2: Incident Response



Task One
30-60 mins

Task Two
Mitigate cyber incidents by analysing, responding and recovering for your organisation
30-60 mins

Task Three
30-60 mins

Task Four
1-2 hours

Finish Line

Task 2: Incident response

Task Overview

What you'll learn

- Understand the nature of a cyber incident based on provided incident timeline and descriptions.
- Learn about various types of cyber attacks and their characteristics.
- Understand the steps involved in incident response and recovery.

What you'll do

- Identify the type of cyber attack that occurred based on the incident details.
- Outline the next steps to be taken as a cyber security analyst, including containment, resolution, and recovery measures.
- Provide a list of actions to contain, resolve, and recover from the incident.
- Describe post-incident activities and measures to prevent similar incidents in the future.

Message from Commonwealth Bank

Task 2: Incident response

Task Overview

What you'll learn

- Understand the nature of a cyber incident based on provided incident timeline and descriptions.
- Learn about various types of cyber attacks and their characteristics.
- Understand the steps involved in incident response and recovery.

What you'll do

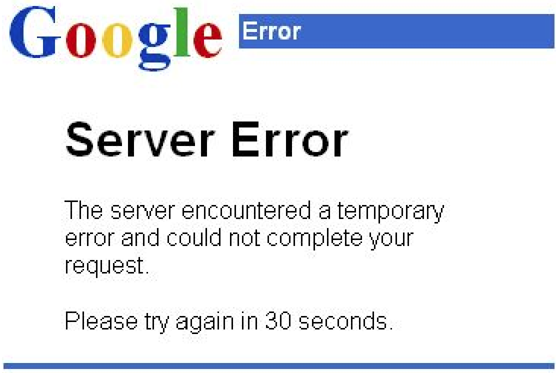
- Identify the type of cyber attack that occurred based on the incident details.
- Outline the next steps to be taken as a cyber security analyst, including containment, resolution, and recovery measures.
- Provide a list of actions to contain, resolve, and recover from the incident.
- Describe post-incident activities and measures to prevent similar incidents in the future.

Task 2: Incident response

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.

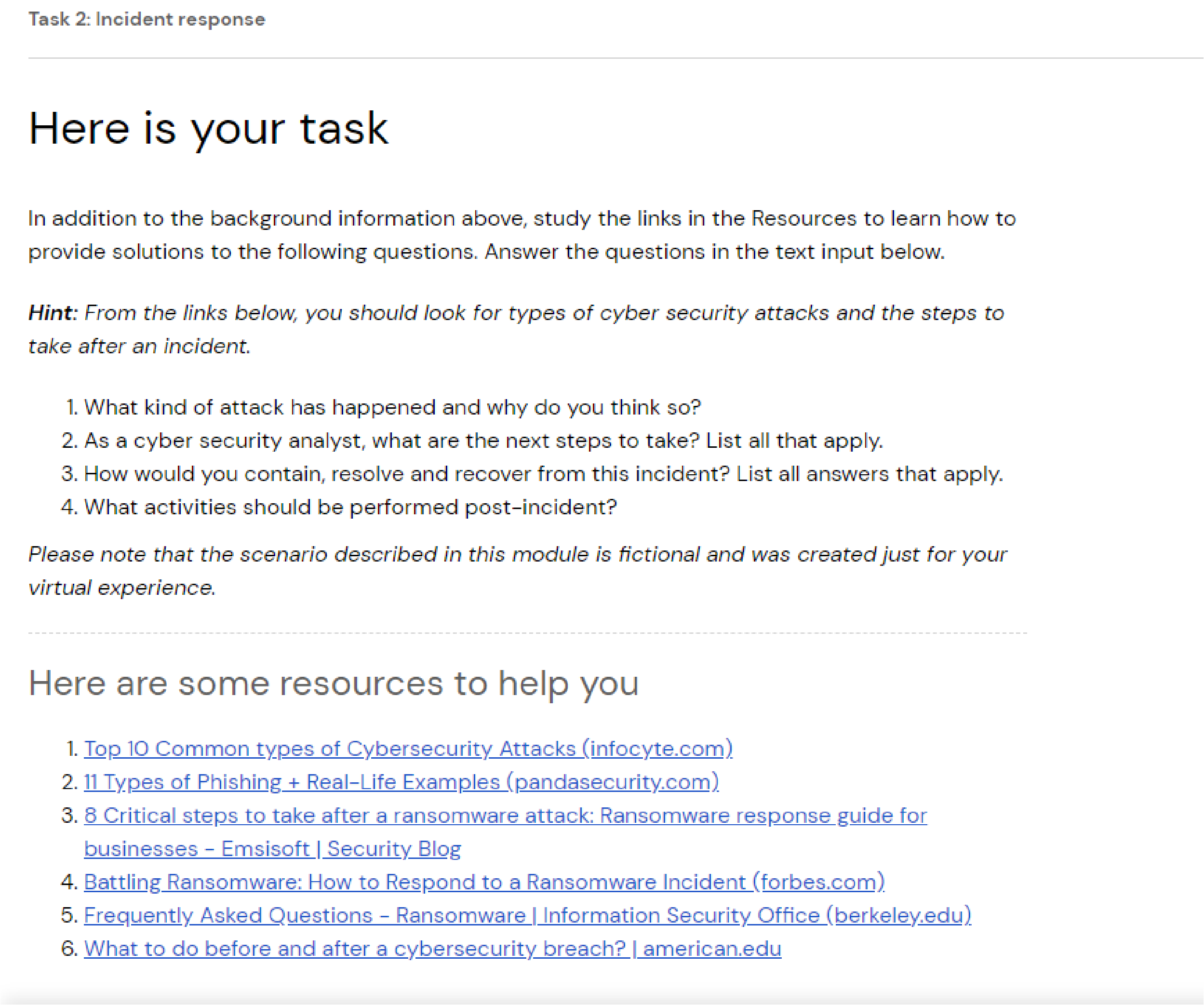


Server Error

The server encountered a temporary error and could not complete your request.

Please try again in 30 seconds.

- 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.



Task 2: Incident response

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)
2. 11 Types of Phishing + Real-Life Examples (pandasecurity.com)
3. 8 Critical steps to take after a ransomware attack: Ransomware response guide for businesses - Emsisoft | Security Blog
4. Battling Ransomware: How to Respond to a Ransomware Incident (forbes.com)
5. Frequently Asked Questions - Ransomware | Information Security Office (berkeley.edu)
6. What to do before and after a cybersecurity breach? | american.edu

My Answer:

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

- Based on the scenario, it appears to be an email phishing attack. A malicious actor was able to successfully manipulate and impersonate themselves as an HR representative disguised as coming from a reliable source. The bank employee clicked on the malicious link, compromising their credentials on a fake login page.
- As more colleagues clicked on the malicious link, they submitted their usernames and passwords, and downloaded Malware, which executed a phishing attack payload onto their system. Users were unable to open Word documents that they once were able to open.

2. As a cyber-security analyst, what are the next steps to take? List all that apply.

- Document the investigation

- Survey the damage: Perform an internal investigation to determine the impact on critical business functions, that way we can identify the attacker, discover the unknown security vulnerabilities, and determine what improvements need to be made to the company's computer systems.
- 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 that were affected.
- Keep the attack from spreading.
- Re-route the network traffic, filter or block traffic and isolate all, or parts of the compromised network.
- Return affected systems to an operationally restored state.
- Confirm affected systems are functioning normally and the data is accessible.
- Stay alert and maybe implement a HIPS or some type of IPS- Intrusion Prevention System.

4. What activities should be performed post-incident?

- Document the recovery process
- Follow-up with a detailed report of everything that occurred.
- Learn from the breach with a “Lessons Learned” session.
- Create a Cyber awareness program with all of the employees and educate them on Phishing emails to help prevent future attacks.

Example Answer

Great work! Take a look at the example answer below to see how a professional would have attempted this task. Think about what you did well and how you can improve.

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.
    - Prioritize 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.