[Date]

Assessment One

Develop ICT Solution

Wells International College

NATALIA 18171

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Natalia Büttner | ID | 18171 |

Contents

[Case scenario 2](#_Toc94716194)

[Heaven Systems internal IT Service Agreement 3](#_Toc94716195)

[Task 1: Scope issue 4](#_Toc94716196)

[**Protect yourself from phishing attempts** 5](#_Toc94716197)

[Task 2: Selected solutions with Presentation 5](#_Toc94716198)

[Presentation 6](#_Toc94716199)

[**Search Index** 8](#_Toc94716200)

[**REFERENCE:** 8](#_Toc94716201)

All my assessments and working, could be found: https://luthiienn.github.io/ictby18171/

**Assessment 1 – Presentation**

***Instructions:***

You need to analyse a case scenarios and complete tasks mentioned after scenario.

You need to demonstrate your develop ICT solution ability to identify the solution, determine client support and manage the team in development an awareness of cyber security in workplace.

***Duration:***

Trainer will set the duration of the assessment.

***Evidence required:***

|  |  |  |
| --- | --- | --- |
| *Tasks* | *Evidence* | *Submission* |
| Identifying issue and | A complete issue report and selected solution, including a presentation. | Presentation in front of the class and the trainer. Also, in printing |

# Case scenario

Established in 1999 with offices located throughout the western Sydney, Heaven Systems is a world-class, full-service provider of residential, commercial, and logistics-based transportation solutions for businesses and individuals. Many of the world’s largest, most respected corporations rely on the company’s unwavering commitment to innovation, quality, and customer service to move their employees, offices, and industrial facilities—domestically and internationally—anywhere in the world. Heaven Systems was experiencing an increase of phishing emails that were reaching employee inboxes and introducing the risk of a data breach. As phishing attacks increased, productivity slowed down while end users waited for IT to investigate the suspicious emails. “Phishing emails were getting more specific and sophisticated, and we worried that an employee might open one and cause serious damage,” said David Potter, IT Director at Heaven Systems. While there are multiple layers of security to filter email as it enters Heaven Systems’ network, it’s still possible for some targeted phishing emails to slip through and get into employee in-boxes. For this reason, IT must rely on end users to determine whether an email is safe to open. But it’s not always easy to tell. “For instance,” said Potter, “one area of the company was getting phishing emails that looked legitimate. They appeared to come from a customer, but the attachment was malicious.” Refer to employee background statistic show below:



To help employees identify phishing emails, IT holds annual training to show them what red flags to look for. Then, IT sends mock phishing attacks to test them. If a user clicks on a couple simulated phishing emails, they’re required to take the security training again. Human nature being what it is, some users were ignoring legitimate email because they didn’t want to make a mistake that would require them to take the training again. Others decided to play it safe and send every questionable email they received to IT to see if it was OK. While IT recognized the obvious threats, even they had to question some of the attachments. “You can imagine the amount of time we spent investigating emails,” said Potter. “It took about an hour per email to copy the attachment to a USB drive and then spin up a machine to test the file off network,” he explained. “That’s valuable time that IT could spend doing other things.”

You are work as an IT project manager assigned by Potter to handle this problem in the company. The company decide to use the system to detect a Spear-Phishing. To accelerate suspicious email analysis and response, Heaven Systems implemented MailMon, an automated phishing incident reporting and response service that empowers end users to report suspicious emails directly from the inbox. MailMon runs on Microsoft Exchange 2013 or newer and Office365; it is deployed to end users as an Outlook plug-in, including Outlook App for Android and iOS devices.

You and your friend are 10 years’ experience staff in the company. After you evaluate the MailMon, it generates a report in the complex form, many of the staff including a current IT department are not familiar with the system. Potter approved on new project team recruitment, and HR organised 3 **new graduated** IT staffs joining your team. Potter would like your team to gain more awareness on this cyber security incidence.



Figure: MailMon Monitoring Sample

# Heaven Systems internal IT Service Agreement

|  |  |  |
| --- | --- | --- |
| **Severity Level** | **Description** | **Target Response** |
| 1 (Outage) | Entire Company Server down | Immediately |
| 2 (Critical) | Entire Department Server down | Within 15 Minutes |
| 3 (Urgent) | Staff computer down | Within 1 hours |
| 4 (Important) | Staff computer not work properly or potential for interrupt their routine work | Within 3 hours |
| 5 (General) | Upgrade software  Training request | Within 48 hours |

# Task 1: Scope issue

Now, in the mid of November, you are required to prepare the report for the management team on company security awareness. The report should indicate:

1. The company current issue:

Heaven Systems was experiencing an increase of phishing emails that were reaching employee inboxes and introducing the risk of a data breach. As phishing attacks increased, productivity slowed down while end users waited for IT to investigate the suspicious emails.

More ICT security issue attached in the end of this assessments

The company faces the increase of phishing emails, but employees don’t have enough ability to handle them.

**Phishing Methods**

Phishing attempts most often begin with an email attempting to obtain sensitive information through some user interaction, such as clicking on a malicious link or downloading an infected attachment.

• Through link manipulation, an email may present with links that spoof legitimate URLs; manipulated links may feature subtle misspellings or use of a subdomain.

• Phishing scams may use website forgery, which employs JavaScript commands to make a website URL look legitimate.

• Using covert redirection, attackers can corrupt legitimate websites with malicious pop-up dialogue boxes that redirect users to a phishing website.

• Infected attachments, such as .exe files, Microsoft Office files, and PDF documents can install ransomware or other malware.

Phishing scams can also employ phone calls, text messages, and social media tools to trick victims into providing sensitive information.

**Types of Phishing Attacks**

Some specific types of phishing scams use more targeted methods to attack certain individuals or organizations.

**Email phishing:**

Scammers create emails that impersonate legitimate companies and attempt to steal your information. This is the type that the company Heaven Systems is having issues with.

**Spear Fishing:**

Spear phishing email messages won’t look as random as more general phishing attempts. Attackers will often gather information about their targets to fill emails with more authentic context. Some attackers even hijack business email communications and create highly customized messages.

**Clone Phishing:**

Attackers are able to view legitimate, previously delivered email messages, make a nearly identical copy of it—or “clone”—and then change an attachment or link to something malicious.

**Whaling:**

Whaling specifically targets high profile and/or senior executives in an organization. The content of a whaling attempt will often present as a legal communication or other high-level executive business.

**Pop-up phishing:**

Fraudulent pop-ups trick users into installing malware.

1. Brief for possible solution to identified issue. Each solution must be assessed on
   * commercial potential
   * suitability for the target audience or purpose
   * feasibility of implementing solution

Refer: learners guide, [Phishing - scam emails | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/threats/phishing)

How to Prevent Phishing Attacks:

Organizations should educate employees to prevent phishing attacks, particularly how to recognize suspicious emails, links, and attachments. Cyber attackers are always refining their techniques, so continued education is imperative.

Some tell-tale signs of a phishing email include:

• ‘Too good to be true’ offers

• Unusual sender

• Poor spelling and grammar

• Threats of account shutdown, etc., particularly conveying a sense of urgency

• Links, especially when the destination URL is different than it appears in the email content

• Unexpected attachments, especially .exe files

Additional technical security measures can include:

• Two Factor Authentication incorporating two methods of identity confirmation—something you know (i.e., password) and something you have (i.e., smartphone)

• Email filters that use machine learning and natural language processing to flag high-risk email messages. DMARC protocol can also prevent against email spoofing.

• Augmented password logins using personal images, identity cues, security skins, etc.

• Check emails legitimacy by contacting the relevant business or organisation (using contact details sourced from the official company website).

• Stay informed on the latest threats

• Before you click a link (in an email or on social media, instant messages, other web pages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognise or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video or web page without directly clicking on the suspicious link.

• Do not open any email if you do not clear where it came from.

• Take time to confirm the relevant company email or web site address.

• Call or email follow the office site info to confirm true or false.

# Task 2: Selected solutions with Presentation

[ACSC - What is Phishing on Vimeo](https://vimeo.com/497805556)

1. Conduct a brainstorm on identified issue
2. Compare an idea solution for identified issue
3. Selected the solution and communicate to stakeholder (Your trainer)

a. **Prepare some (10-15) presentation slides** to present the following items to your trainer (All group members have to present equally)

* + Identified issue
  + Brainstorming evidence
  + Selected solution

1. Record feedback from your trainer and finalised the solution

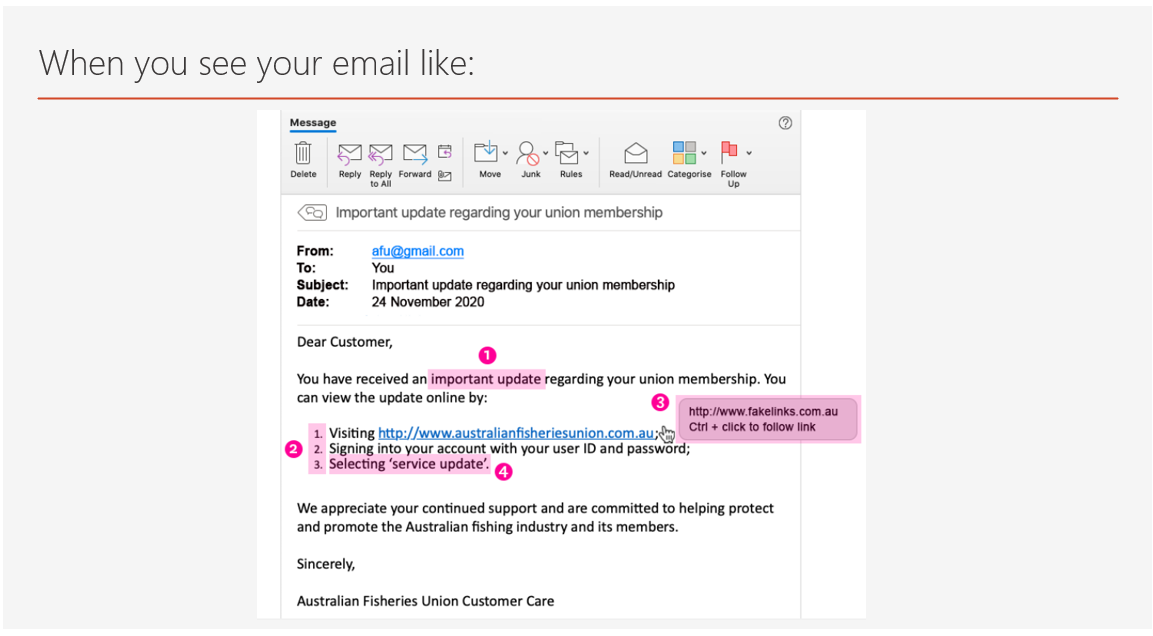
# Presentation

You could use Google Slides to create your presentation.

Refer: <https://www.youtube.com/watch?v=o7wvajrAxUQ>

A red box with white text

Description automatically generated with low confidence



A screenshot of a email

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a email

Description automatically generated with low confidence

A screenshot of a computer error

Description automatically generated with low confidence

A picture containing text, screenshot, font, number

Description automatically generated

A screenshot of a computer error message

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with low confidence

A picture containing text, screenshot, font

Description automatically generated

A picture containing text, screenshot, font, number

Description automatically generated

# **Search Index**

B

Brainstorming 6

C

cybercriminals 5

D

detect a Spear 3

H

Heaven Systems 4

I

idea solution 6

P

phishing attacks 2

phishing emails 2

# **REFERENCE:**

Please visit my site: https://luthiienn.github.io/ictby18171/

A screenshot of a computer

Description automatically generated with medium confidence