T +61 2 9283 4388 | F +61 2 9283 0748 | E info@wic.nsw.edu.au
Lower Ground, 101 Sussex St, Sydney NSW 2000 Australia | www.wic.nsw.edu.au
ABN: 19 080 559 600 | CRICOS CODE: 01856K | RTO: 90501

[Date]

Assessment One

Develop ICT Solution

Wells International College

YESID ALBERTO GIRON GIRON - 70403

Name of Student	YESID ALBERTO GIRON GIRON	ID	70403

CONTENTS

All my assessments and working, could be found: https://wellsjohn220.github.io/ictsolution

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:

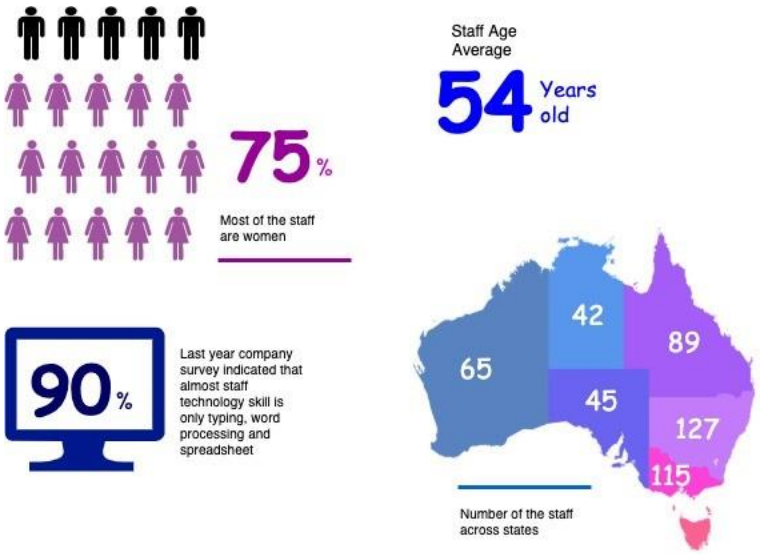
Trainer will set the duration of the assessment.

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.

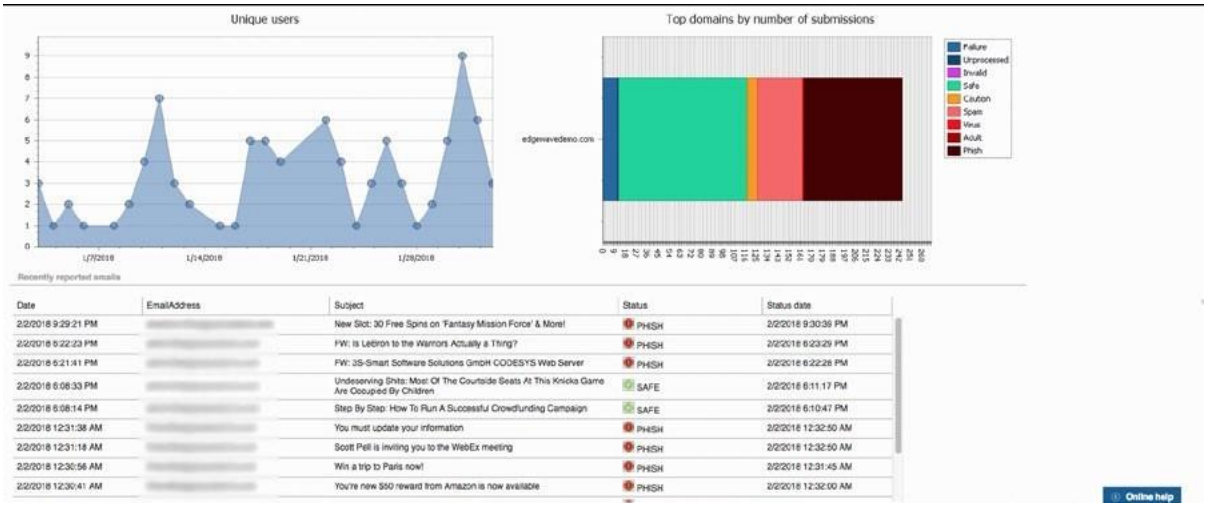


Figure: MailMon Monitoring Sample

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 (Reference):

   The company face the increase of phishing emails, but staff not enough ability to handle.

Phishing attacks are indeed a significant concern for organizations, and they can lead to data breaches with serious consequences. Let's explore this further:

What is a Data Breach?

A data breach occurs when unauthorized individuals gain access to an organization's data, including sensitive information. It can result in financial losses, reputational damage, and legal repercussions. One common vector for data breaches is phishing.

1. **Phishing Attacks:**

- Phishing involves sending fraudulent emails, text messages, or social media content that appears legitimate to trick recipients into revealing sensitive information or clicking on malicious links.
- These attacks exploit human psychology, often impersonating trusted entities (such as banks, colleagues, or service providers) to deceive users.
- Once a user falls for the phishing attempt, their credentials or personal data may be compromised.

2. **Statistics and Trends:**

- In the US, phishing attacks accounted for 36% of all data breaches in 2023.
- During the fourth quarter of 2023, 1,339 brands were targeted by phishing attacks.
- The number of unique phishing sites (attacks) reached 5 million in 2023.
- Phishing attacks were the second costliest source of compromised credentials.

3. **Recent Breaches:**

- The Verizon 2024 Data Breach Investigations Report highlighted the rapid exploitation of zero-day vulnerabilities and the effectiveness of ransomware attacks.

- The ASD Cyber Threat Report 2022–23 by the Australian Signals Directorate (ASD) emphasized the persistence of state and non-state actors targeting Australia's networks. Emerging technologies like artificial intelligence add complexity to the threat landscape.

4. **Mitigation Strategies:**

- Organizations should educate employees about phishing awareness and best practices.
- Implement multi-factor authentication to protect against stolen credentials.
- Regularly update security protocols and invest in cyber resilience efforts.

Remember, vigilance and proactive measures are crucial in defending against phishing attacks and preventing data breaches. If you suspect a phishing email, report it promptly to your IT department.

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: Phishing - scam emails | Cyber.gov.au

Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures').

PROTECT YOURSELF FROM PHISHING ATTEMPTS

The best way to protect yourself from phishing attempts is to stay abreast of current threats, be cautious online and take steps to block malicious or unwanted messages from reaching you in the first place.

Take the following steps to protect yourself from phishing attempts:

- Don't click on links in emails or messages, or open attachments, from people or organisations you don't know.
- Be especially cautious if messages are very enticing or appealing (they seem too good to be true) or threaten you to make you take a suggested action.
- 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.
- If you're not sure, talk through the suspicious message with a friend or family member, or check its legitimacy by contacting the relevant business or organisation (using contact details sourced from the official company website).

- Use a spam filter to block deceptive messages from even reaching you.
- Understand that your financial institution and other large organisations (such as Amazon, Apple, Facebook, Google, PayPal and others) would never send you a link and ask you to enter your personal or financial details.
- Use safe behaviour online. Learn how to use email safely and browse the web safely.
- Stay informed on the latest threats – sign up for the ACSC Alert Service. You can also find information about the latest scams on the Australian Government's Scamwatch website.

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…

ask 2: Selected solutions with Presentation

ACSC - What is Phishing on Vimeo

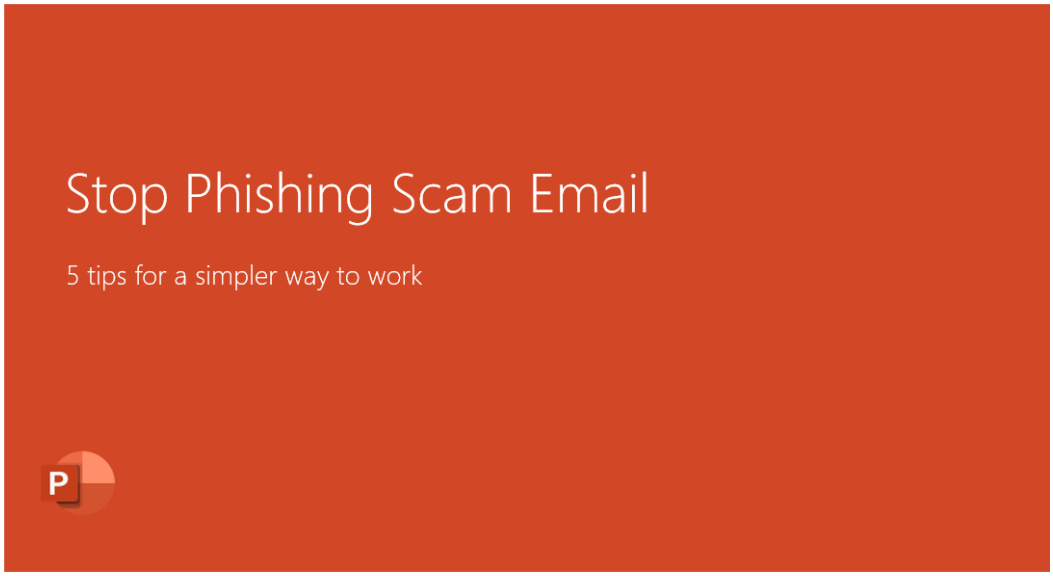
1. Conduct a brainstorm on identified issue
2. Compare an idea solution for identified issue
3. Selected the solution and communicate to stakeholder (Your trainer)
    a. **Prepare some (10-15) presentation slides** to present the following items to your trainer (All group members have to present equally)
        - Identified issue
        - Brainstorming evidence
        - Selected solution
4. Record feedback from your trainer and finalised the solution

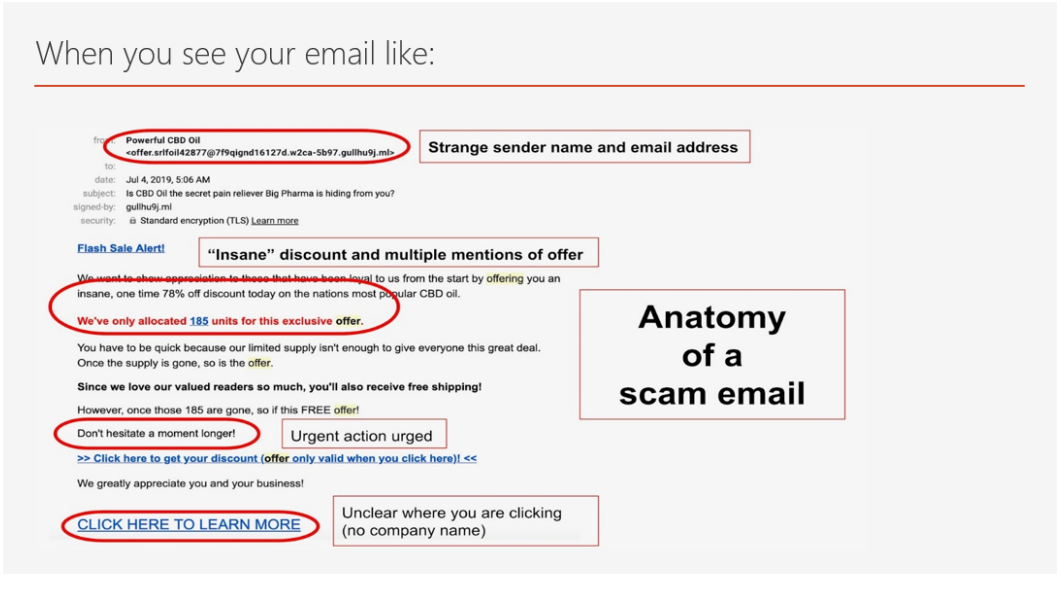
https://docs.google.com/presentation/d/1xnsuAvAFTw9J1BhJFn6mnWDaXNITQbAOErlPgnwSWnk/edit?usp=sharing

PRESENTATION

You could use Google Slides to create your presentation.

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





SEARCH INDEX

REFERENCE:

Please visit my site: [12345 John (wellsjohn220.github.io)]