[Date]

Assessment One

Develop ICT Solution

Wells International College

Tomohiro 70351

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Tomohiro Matsuyama | ID | 70351 |

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://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:***

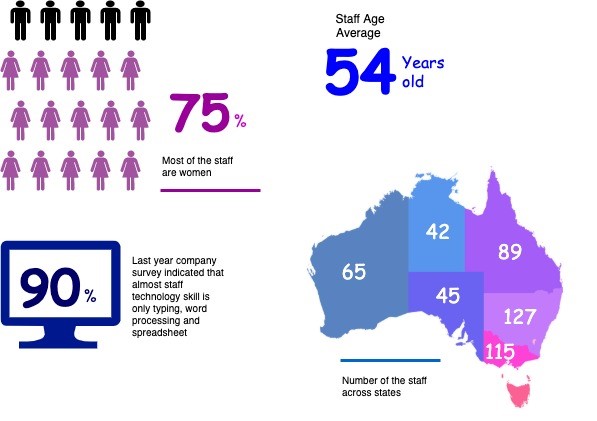
Trainer will set the duration of the assessment.

***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.

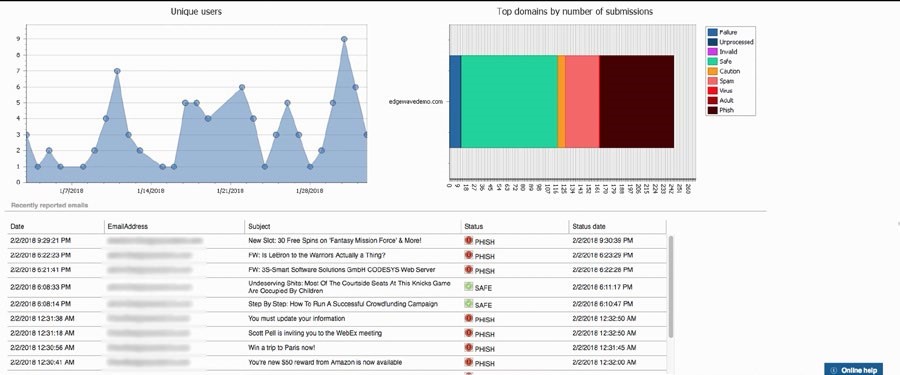


Figure: MailMon Monitoring Sample

# 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.



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

**What is phishing?**

phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

## **WHAT STEPS CAN ORGANISATIONS TAKE TO PROTECT AGAINST PHISHING ATTACKS?**

* **Include security awareness in your organisation’s culture.**By raising awareness of the signs and dangers of phishing attacks, the employees will be able to identify them; be less likely to fall for them; or at least be able to flag an issue and report it to you so you can take timely steps to contain the incident.
* **Use spam filters or secure email gateways to block deceptive emails from reaching VPS employees.**  
  Spam filters and secure email gateways monitor incoming emails for unwanted or fraudulent content. Once identified, they prevent them from ever reaching an employee’s inbox.
* **Enable multifactor authentication (MFA) and anomaly login policies.**Even if an employee provides information to a scammer, these measures decrease a scammer’s ability to gain access to the employee’s work account and increase your ability to detect and respond to incidents in a timely manner.
* **Report phishing attempts to the authorities.**You should report phishing attempts to the Government Cyber Incident Response services  by emailing  to them who can help you respond to the incident. You should also report security incidents by emailing a copy of their incident notification them or contacting them for privacy advice.

## **WHAT STEPS CAN EMPLOYEES TAKE TO PROTECT AGAINST PHISHING ATTACKS?**

* **Watch out for fake links or attachments.**  
  Where you suspect an email to be a phishing attempt, contact your IT team. Do not open any attachments, click any links or forward the email to another device.
* **Do not provide information to unverified sources.**  
  If you are unsure about whether you should be providing your information, check with your Privacy Officer or IT team. If the email is from someone familiar but the contents appear surprising or suspicious, contact them on the phone number you already hold to verify if they actually sent it.
* **If you receive a phishing email, notify your IT department.**If you think you have fallen for a phishing attempt or notice suspicious activity on your device, immediately disconnect from the internet and notify your IT team. Do not shut down or restart your device.

# 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)

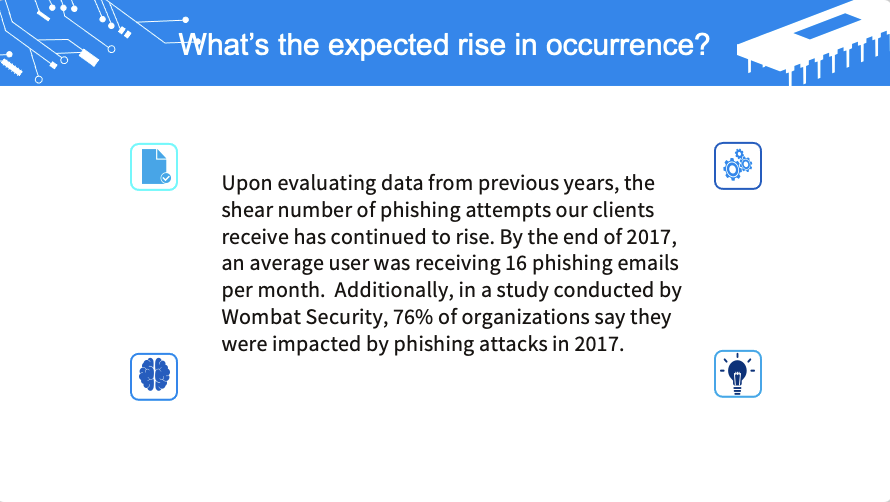
a. **Prepare some (10-15) presentation slides** to present the following items to your trainer (All group members have to present equally)

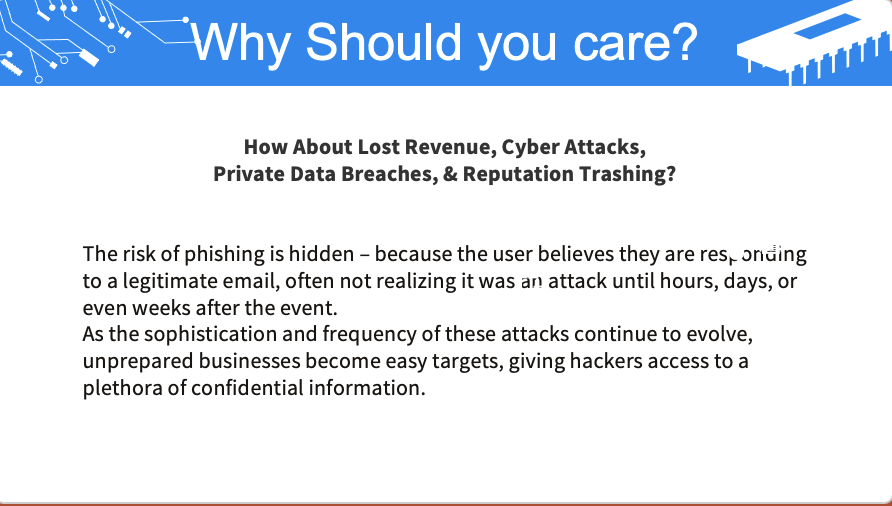
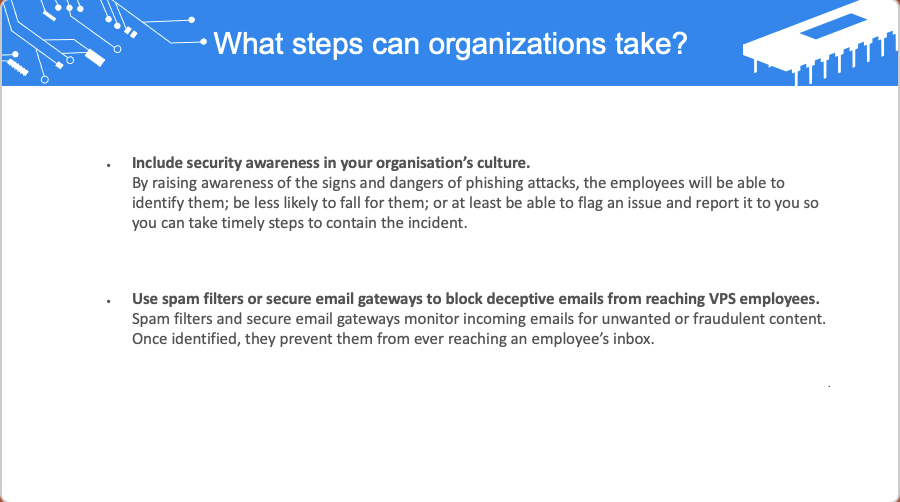
* + Identified issue
  + Brainstorming evidence
  + Selected solution

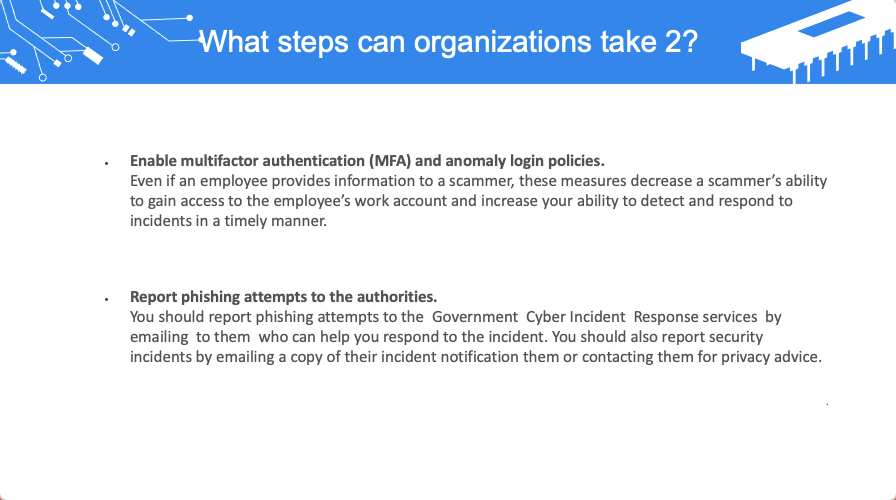
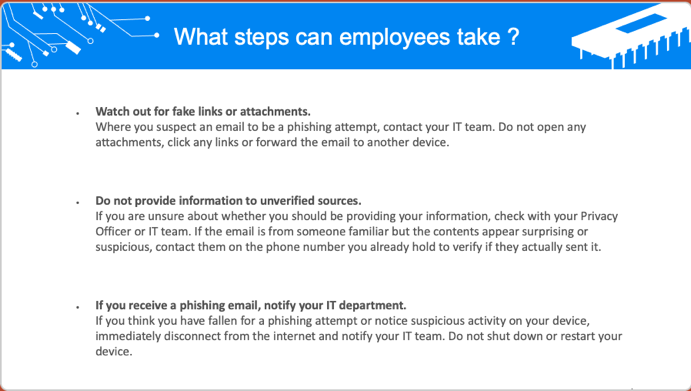
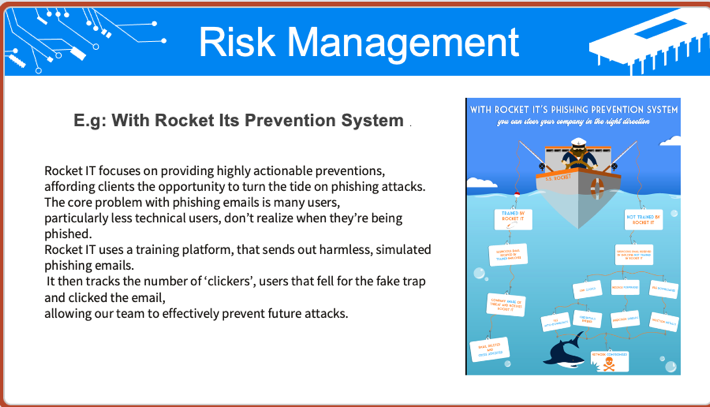
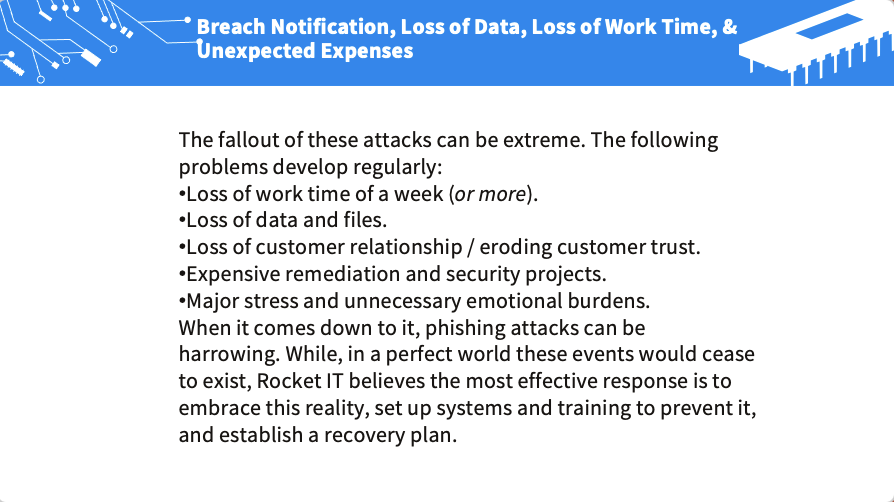
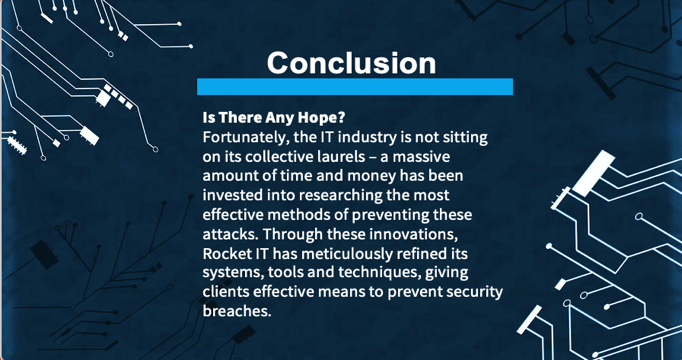
1. Record feedback from your trainer and finalised the solution

# Presentation

You could use Google Slides to create your presentation.

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

******

******

# **Search Index**

B

Brainstorming 6

C

cybercriminals 5

D

detect a Spear 3

H

Heaven Systems 4

I

idea solution 6

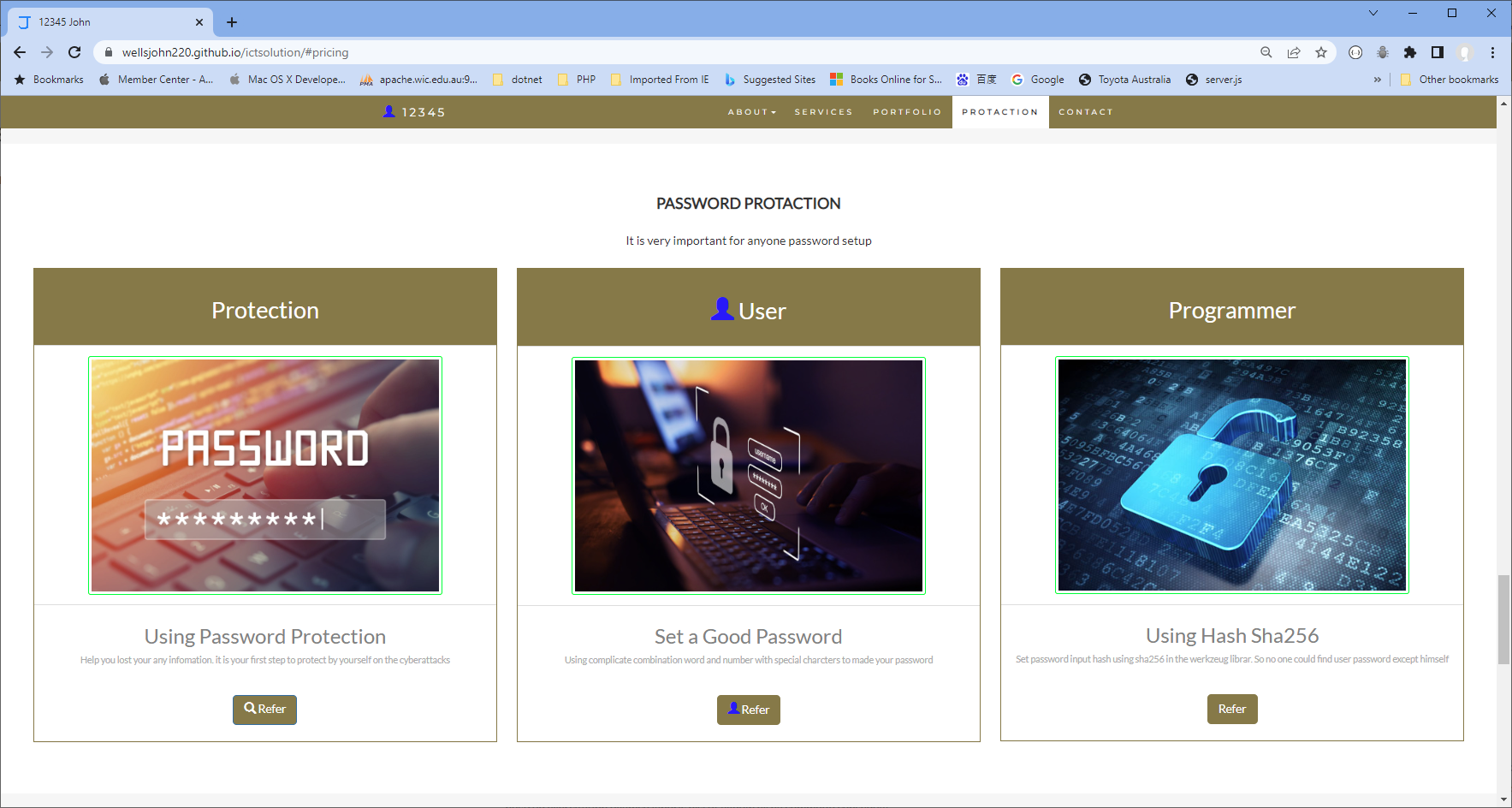
P

phishing attacks 2

phishing emails 2

# **REFERENCE:**

Please visit my site: <https://wellsjohn220.github.io/>



See my case study about ICT security case

My database injection study

Communication safe example:

My computer work environment: