Assessment One

Develop ICT Solution

17/02/2024

Wells International College

purevdulam urambayar 18821

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student | Purevdulam | ID | 18821 |

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://puujeu.github.io/ICT-DIPLOMA-T1/**](https://puujeu.github.io/ICT-DIPLOMA-T1/)

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 is a leading provider of transportation solutions. Founded in 1999. Offices located throughout western Sydney, Australia.

**Services**: Provider of residential, commercial, and logistics-based transportation solutions.

**Client**: Many of the world's largest and most respected corporations.

**Commitment**: Unwavering commitment to innovation, quality, and customer service.

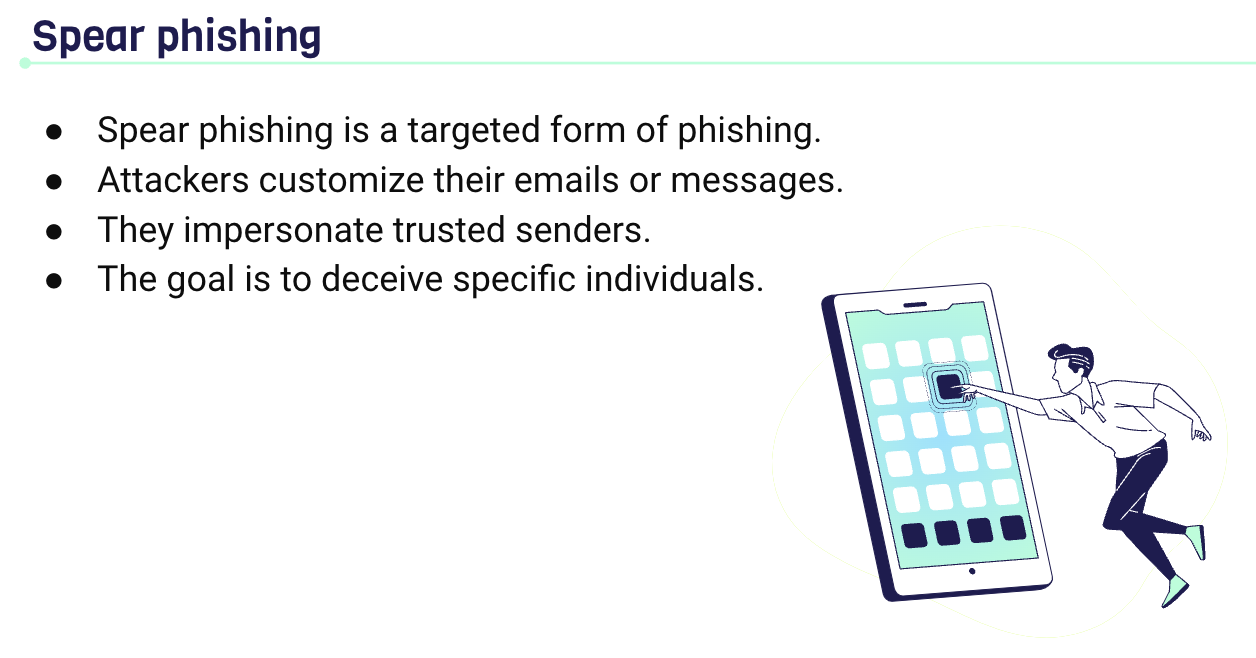
**Phishing Threat:** Experiencing an increase in phishing emails reaching employee inboxes, posing a risk of data breach and productivity slowdown.

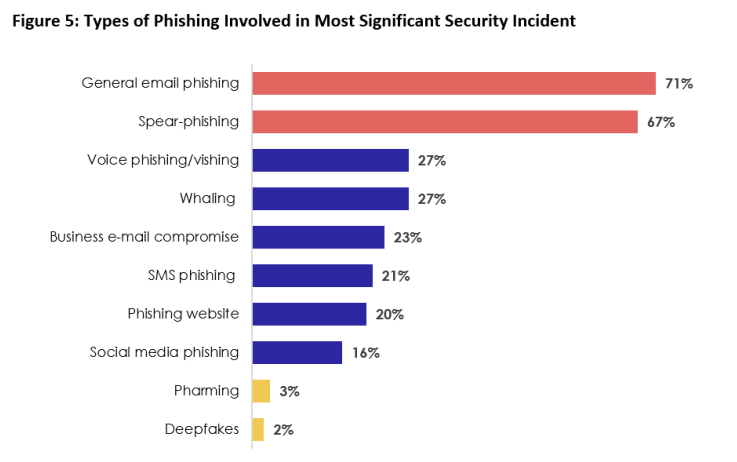
The company is facing a significant rise in phishing attacks targeting its employees' email inboxes. These phishing attempts have become increasingly sophisticated.

The rise in phishing attacks presents a serious threat to the company's cybersecurity.

What is the phishing?

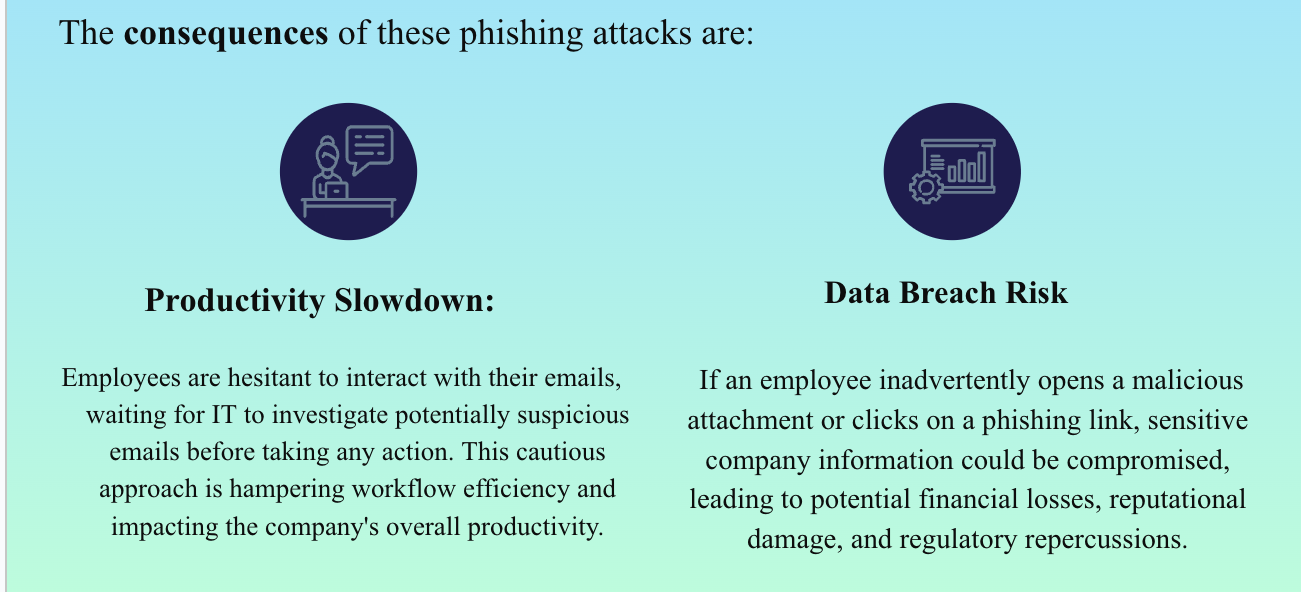
Phishing is a type of cyber-attack where attackers attempt to trick individuals into providing sensitive information such as usernames, passwords, credit card details, or other personal information. This is typically done through deceptive emails, text messages, or other communication methods that appear to be from a legitimate source, such as a bank, social media platform, or a trusted organization.





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

The consequences of these phishing attacks are:



There are four solutions:

1. **SOLUTION 1 - Enhanced Email Filtering System**
   * Commercial Potential: High
     + Email filtering systems can be commercially viable as they are widely available from various vendors and can be tailored to specific business needs.
   * Suitability for Target Audience or Purpose: Moderate to High
     + Suitable for organizations of all sizes, including Heaven Systems, to enhance email security.
     + However, effectiveness may vary based on the sophistication of phishing attacks and the level of customization required.
   * Feasibility of Implementation: Moderate to High
     + Implementation may require initial investment in purchasing or upgrading existing email filtering systems.
     + Ongoing maintenance and updates are necessary to adapt to evolving phishing tactics.
2. **SOLUTION 2 - Employee Training and Awareness Programs**
   * Commercial Potential: Moderate
     + While there may be costs associated with developing and delivering training programs, the long-term benefits in terms of reduced security incidents and improved employee vigilance can outweigh the initial investment.
   * Suitability for Target Audience or Purpose: High
     + Employee training and awareness programs are essential for all staff members at Heaven Systems to recognize and respond to phishing attacks effectively.
     + Programs can be tailored to different departments and roles within the organization.
   * Feasibility of Implementation: High
     + Training programs can be developed internally or outsourced to cybersecurity training providers.
     + Regular training sessions and updates ensure ongoing employee awareness and preparedness.
3. **SOLUTION 3 -Multi-Factor Authentication**

* Commercial Potential: Moderate to High
  + MFA solutions are commercially available from various vendors and offer scalable options suitable for businesses of different sizes.
* Suitability for Target Audience or Purpose: High
  + MFA enhances security by requiring additional verification steps beyond passwords, making it suitable for all employees at Heaven Systems.
  + Particularly effective for securing access to critical systems and applications.
* Feasibility of Implementation: Moderate to High
  + Implementation may require integration with existing IT infrastructure and systems.
  + Training and support for employees may be necessary to ensure smooth adoption and usage of MFA solutions.

1. SOLUTION 4 - Incident Response Plan Development

* Commercial Potential: Moderate
  + While incident response planning may not generate direct revenue, it is essential for mitigating the financial and reputational costs of security incidents.
* Suitability for Target Audience or Purpose: High
  + An incident response plan is critical for all organizations, including Heaven Systems, to effectively manage and mitigate the impact of phishing attacks and other security incidents.
* Feasibility of Implementation: High
  + Development of an incident response plan involves collaboration between IT, security teams, and other relevant stakeholders.
  + Regular testing and updating of the plan ensure its effectiveness in addressing evolving threats.

# 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.

**Here is the my presentation link:** <https://docs.google.com/presentation/d/13IRifA_w2DzF2q00SMKEZvDkYYOY3GZV2beAZM6ESL0/edit?usp=sharing>

**Please visit my site:** <https://puujeu.github.io/ICT-DIPLOMA-T1/>