Week 1 Worksheet Identify threats

|  |  |
| --- | --- |
| Name: | Nathan Bransby |
| Student ID: | V141198 |

# Part 1: Identify need for cyber awareness training

1. Examine the phishing email below. Graphical user interface, text

   Description automatically generated

Describe how awareness training could reduce the likelihood that staff will click on the Cancel Transaction link.

|  |
| --- |
| Training awareness can prevent the likelihood that staff are fooled by phishing email scams by providing staff with the basic knowledge on how to identify elements in an email that aren’t official, such as:   * Un-official addresses * Requests for personal information * Requesting money or immediate action regarding sensitive info * Dodgy links. |

# Part 2: Can you spot when you’re being phished?

1. Click the link below to take the Google phishing quiz.

[Google Phishing Quiz](https://phishingquiz.withgoogle.com/)

1. Take a screen shot of your result and paste in the box

|  |
| --- |
|  |

# Part 3: 9 steps in developing awareness program

1. List the 9 ways to create cyber training

|  |
| --- |
| 1. Focus on situations that are most likely to happen and to those most vulnerable  2. Understand potential security risks and situations directly from staff members.  3. Create targeted messages to individuals based on the security issues faced.  4. Use multiply channels to deliver smaller (more digestible) messages.  5. Create leadership roles where senior staff lead by example  6. Challenge beliefs of safety as people tend to underestimate cyber threats.  7. Use consistent vibrant color cues that are associated with emergency/urgency  8. Keep content engaging (aka gamify)  9. Identify suspicious behavior changes and measure their impacts, so it can be surveyed, monitored & reported. |