Configuration Manual

Industrial Internship
MSc Cybersecurity

Sabahath Rizwana Palappurath Showkath
Student ID: 21151474

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Sabahath Rizwana Palappurath Showkath

Student ID: 21151474

Programme: MSc Cybersecurity **Year:** 2022

Module: Industrial Internship

Lecturer: Vikas Sahni

Submission Due Date: 06/01/2023

Project Title: Cyber Awareness Initiative Using Gamification

Word Count: 1170 **Page Count:** 16

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sabahath Rizwana Palappurath Showkath

Date: 06/01/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Sabahath Rizwana Palappurath Showkath
21151474

1 Introduction

This document has been created to discuss the steps involved in the implementation of the research project – “Cyber Awareness Initiative Using Gamification”. The configuration manuals provide a detailed step-by-step process of how the study was conducted. The research aims to determine *What is the effect of empowering employees via cybersecurity awareness?*

This implementation involves the use of a systematic process developed to monitor employee participation in the cyber awareness campaign conducted by an organisation by showing them their performance and progress.

1.1 Data Gathering

1.1.1 Human Resources

The participants were a group of employees from whom the least and appropriate of amount of data were collected to successfully complete this project. Data for each participant was gathered by providing the phishing simulation team the name and email ID of the participants who agreed to take part in the research.

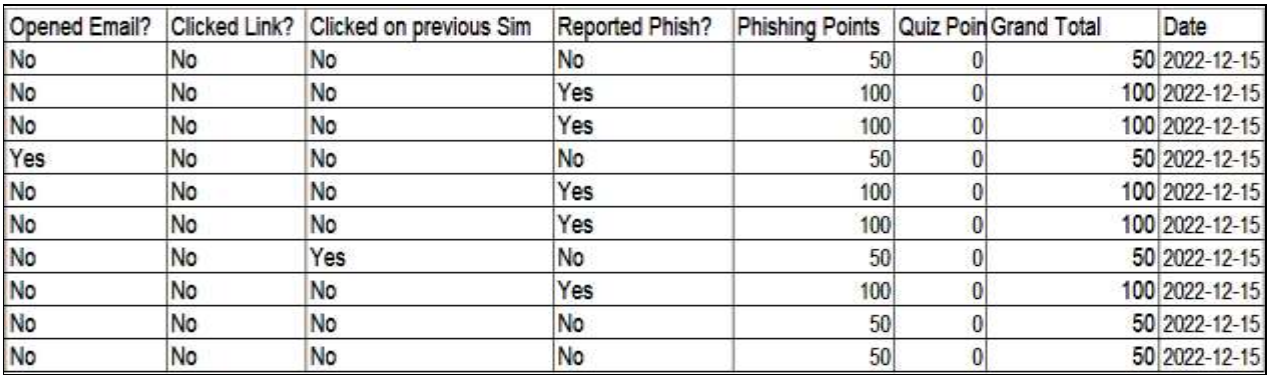
1.1.2 Cloud Storage Resources

Cloud services of the Google platform available in the organisation were used for the storage of the data, the drive was terminated which ensures that the data were purged without violating any ethical or privacy concerns.

1.1.3 Process

1. Participants within a team were contacted first to explain the experiment and retrieve consent for using their simulated phishing mail response and cyber awareness quiz results.
2. Data protection team and phishing simulation team were contacted to explain the research and request the data required from them for the participants who gave consent to participate in the research.
3. The phishing simulation team was provided the name and email ID of the participants.
4. When the results of simulated phishing mail responses were obtained from the team, the following data were stored:
    - Name (Data type - General)
    - Email ID (Data type - General)
    - Location (Data type - General)
    - Date (Data type - Date)

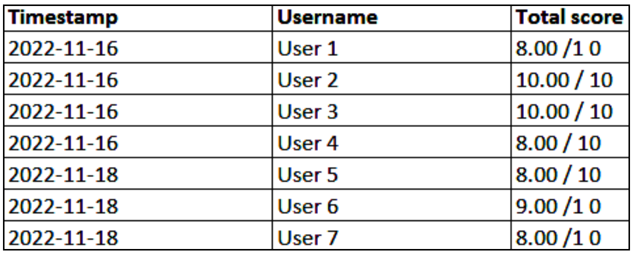
- Got phished in the previous simulation (Data type - General)
- Opened the phishing mail (Data type - General)
- Clicked the link (Data type - General)
- Reported the mail as a phishing mail (Data type - General)



Opened Email?	Clicked Link?	Clicked on previous Sim	Reported Phish?	Phishing Points	Quiz Poin	Grand Total	Date
No	No	No	No	50	0	50	2022-12-15
No	No	No	Yes	100	0	100	2022-12-15
No	No	No	Yes	100	0	100	2022-12-15
Yes	No	No	No	50	0	50	2022-12-15
No	No	No	Yes	100	0	100	2022-12-15
No	No	No	Yes	100	0	100	2022-12-15
No	No	Yes	No	50	0	50	2022-12-15
No	No	No	Yes	100	0	100	2022-12-15
No	No	No	No	50	0	50	2022-12-15
No	No	No	No	50	0	50	2022-12-15

1 - Google sheet containing simulated phishing mail results

5. The following data were obtained and stored when the cyber awareness quiz which was created using Google Forms was conducted:
   - Email ID (Data type - General)
   - Date (Data type - Date)
   - Quiz results (Data type - General)
   - Participant consent

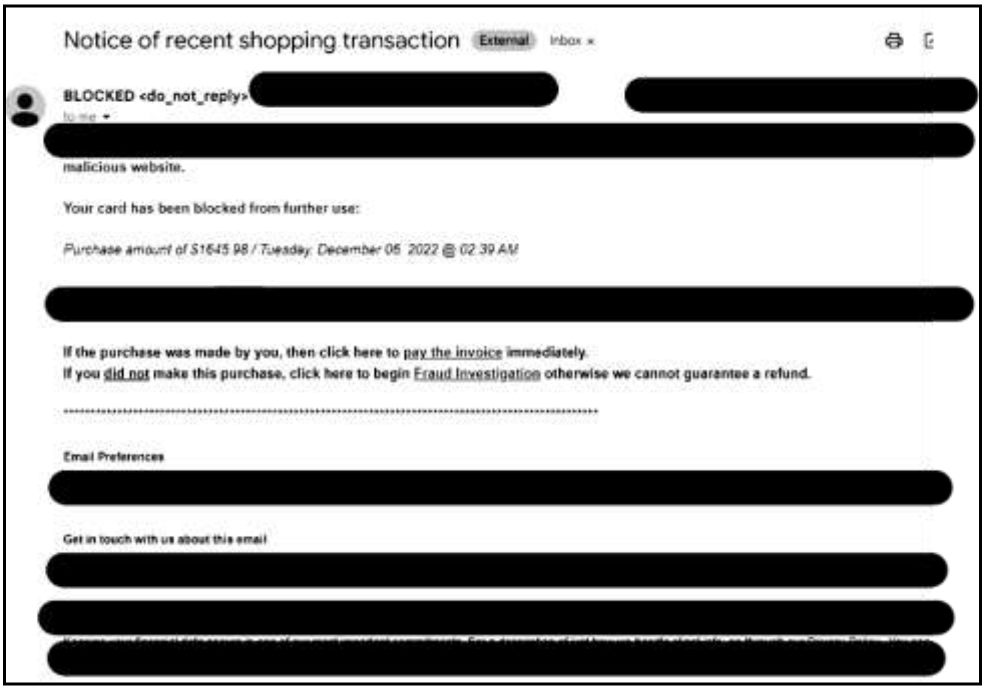


Timestamp	Username	Total score
2022-11-16	User 1	8.00 /1 0
2022-11-16	User 2	10.00 / 10
2022-11-16	User 3	10.00 / 10
2022-11-16	User 4	8.00 / 10
2022-11-18	User 5	8.00 / 10
2022-11-18	User 6	9.00 /1 0
2022-11-18	User 7	8.00 /1 0

2 - Google sheet containing quiz results

1.2 Phishing Mails Simulation

1. The phishing mails were generated by a dedicated team within the organisation.
2. The responses to the phishing mails were stored by the data protection team within the organisation.
3. The responses and related data of the participants of the research were extracted and stored securely in a Google Sheet in the organisation's Drive and retrieved when needed.
4. Sample phishing mail shown below:



Notice of recent shopping transaction External Inbox ×

BLOCKED <do_not_reply>[redacted] [redacted]

to me

[redacted]
malicious website.

Your card has been blocked from further use:

Purchase amount of $1645 98 / Tuesday December 05 2022 @ 02 39 AM

[redacted]

If the purchase was made by you, then click here to pay the invoice immediately.
If you did not make this purchase, click here to begin Fraud Investigation otherwise we cannot guarantee a refund.

****

Email Preferences

[redacted]

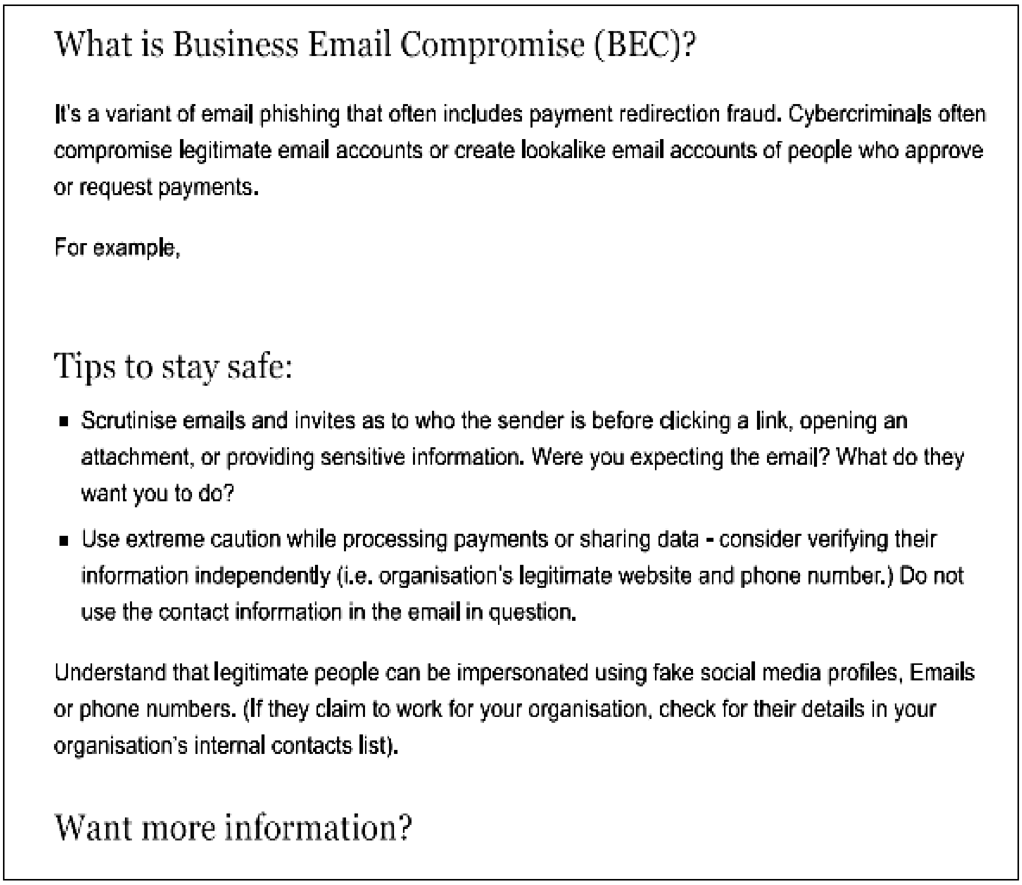
Get in touch with us about this email

[redacted]

3 - Simulated phishing mail

1.3 Cyber Awareness Program

1. As part of the cyber awareness program every week one article on a cyber-attack topic was created by the team that is responsible for running the phishing simulations.
2. The articles were released in the internal portal for employees over the course of four weeks. The articles explained the following:
    a. The type of the cyber attack
    b. Essential tips to stay safe
    c. Steps to report to relevant teams within the organisation which would be applicable to all the participants of this research.



What is Business Email Compromise (BEC)?

It's a variant of email phishing that often includes payment redirection fraud. Cybercriminals often compromise legitimate email accounts or create lookalike email accounts of people who approve or request payments.

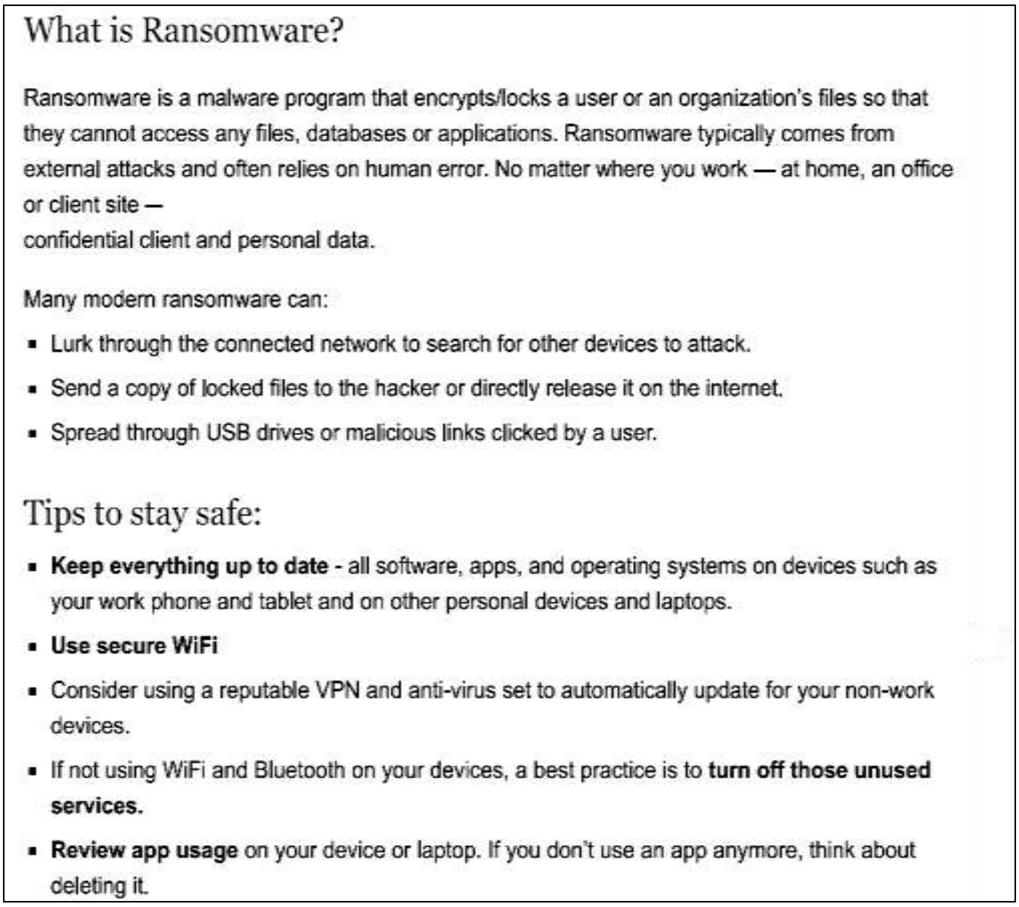
For example,

Tips to stay safe:

- Scrutinise emails and invites as to who the sender is before clicking a link, opening an attachment, or providing sensitive information. Were you expecting the email? What do they want you to do?
- Use extreme caution while processing payments or sharing data - consider verifying their information independently (i.e. organisation's legitimate website and phone number.) Do not use the contact information in the email in question.

Understand that legitimate people can be impersonated using fake social media profiles, Emails or phone numbers. (If they claim to work for your organisation, check for their details in your organisation's internal contacts list).

Want more information?



What is Ransomware?

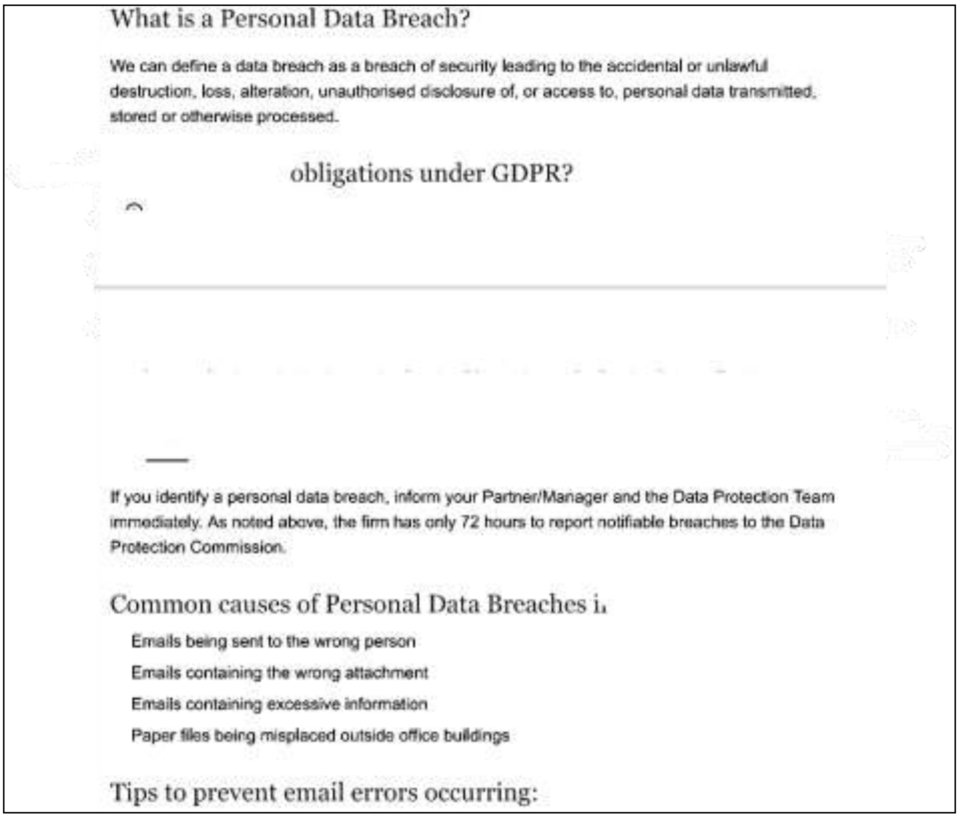
Ransomware is a malware program that encrypts/locks a user or an organization's files so that they cannot access any files, databases or applications. Ransomware typically comes from external attacks and often relies on human error. No matter where you work — at home, an office or client site —
confidential client and personal data.

Many modern ransomware can:

- Lurk through the connected network to search for other devices to attack.
- Send a copy of locked files to the hacker or directly release it on the internet.
- Spread through USB drives or malicious links clicked by a user.

Tips to stay safe:

- **Keep everything up to date** - all software, apps, and operating systems on devices such as your work phone and tablet and on other personal devices and laptops.
- **Use secure WiFi**
- Consider using a reputable VPN and anti-virus set to automatically update for your non-work devices.
- If not using WiFi and Bluetooth on your devices, a best practice is to **turn off those unused services.**
- **Review app usage** on your device or laptop. If you don't use an app anymore, think about deleting it.



What is a Personal Data Breach?

We can define a data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

obligations under GDPR?

If you identify a personal data breach, inform your Partner/Manager and the Data Protection Team immediately. As noted above, the firm has only 72 hours to report notifiable breaches to the Data Protection Commission.

Common causes of Personal Data Breaches i

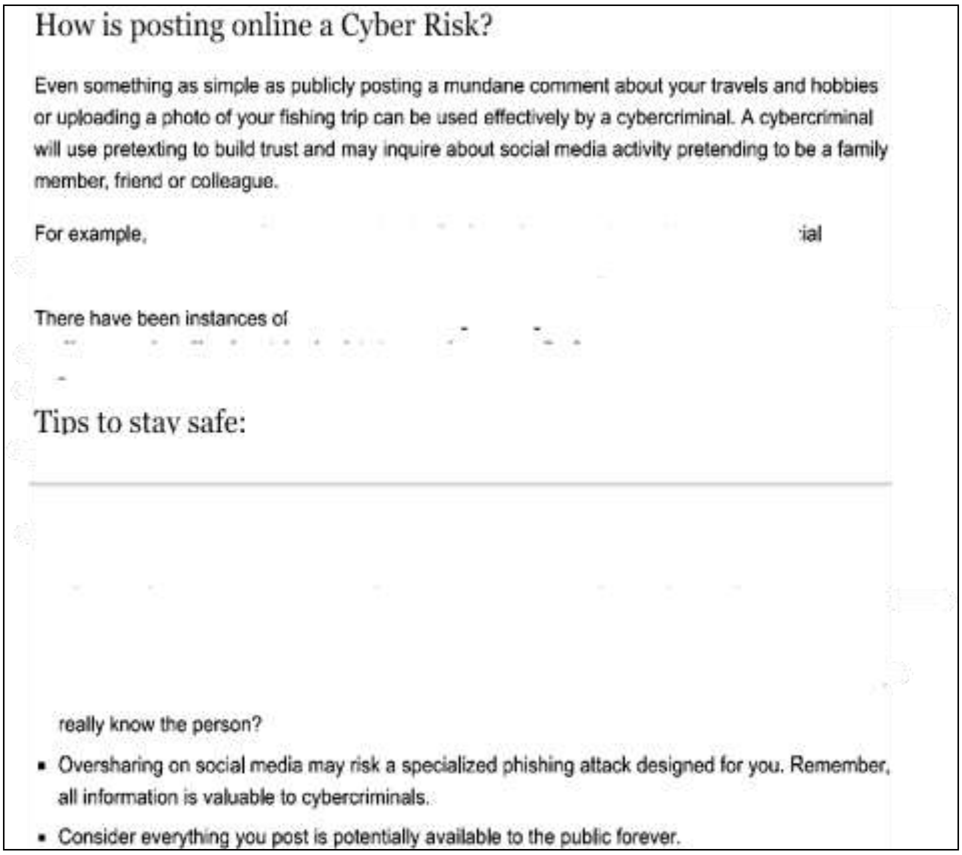
Emails being sent to the wrong person

Emails containing the wrong attachment

Emails containing excessive information

Paper files being misplaced outside office buildings

Tips to prevent email errors occurring:



How is posting online a Cyber Risk?

Even something as simple as publicly posting a mundane comment about your travels and hobbies or uploading a photo of your fishing trip can be used effectively by a cybercriminal. A cybercriminal will use pretexting to build trust and may inquire about social media activity pretending to be a family member, friend or colleague.

For example, ial

There have been instances of

Tips to stay safe:

really know the person?

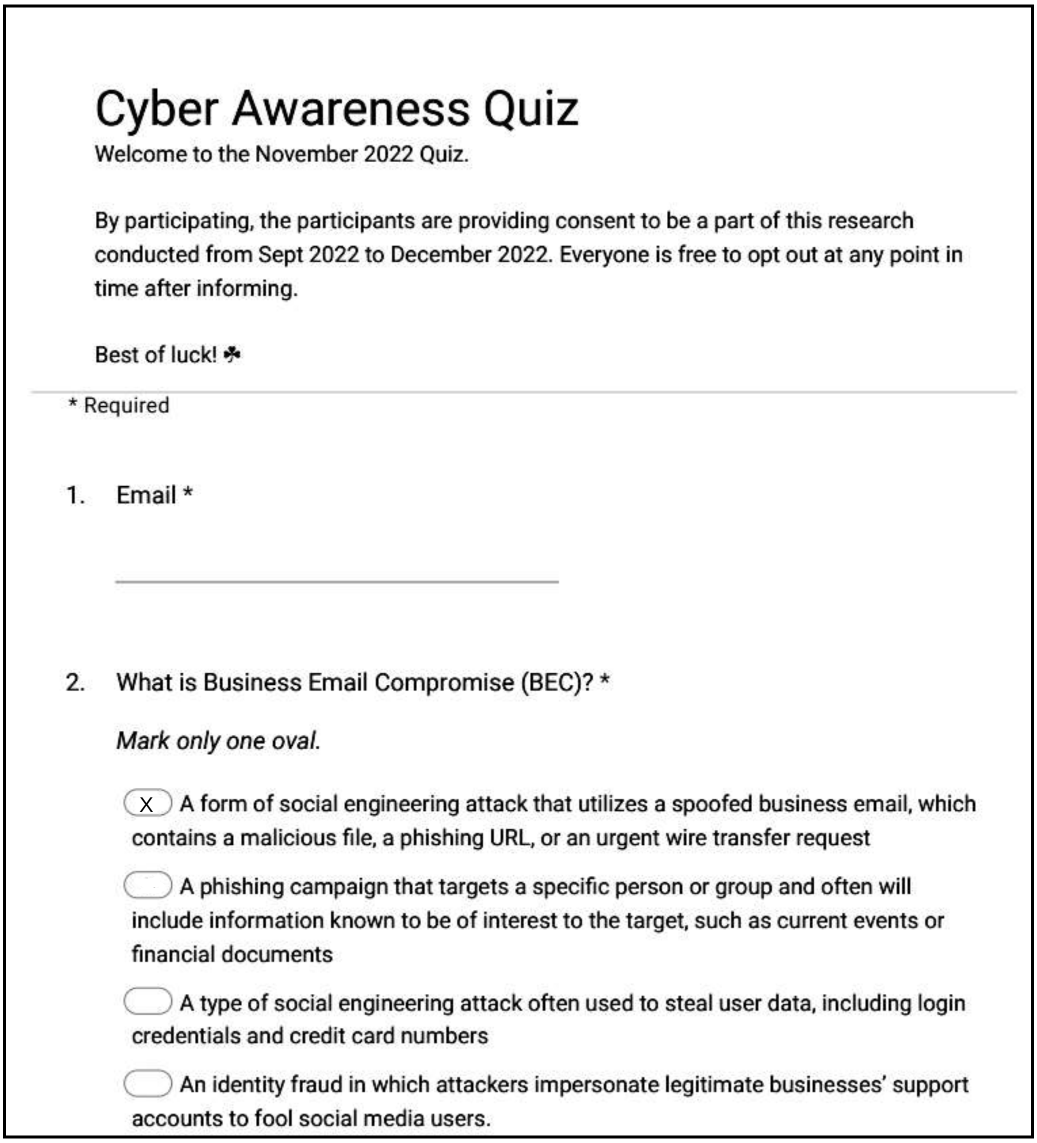
- Oversharing on social media may risk a specialized phishing attack designed for you. Remember, all information is valuable to cybercriminals.
- Consider everything you post is potentially available to the public forever.

4 - Articles related to cyber awareness

1.4 Cyber Awareness Quiz

This part of the manual talks about the creation of a questionnaire using Google Forms.

1. The quiz was conducted at the end of publishing all articles.
2. The questions of the quiz were simple and entirely based on the awareness program conducted within the organisation as shown in the images below:



Cyber Awareness Quiz

Welcome to the November 2022 Quiz.

By participating, the participants are providing consent to be a part of this research conducted from Sept 2022 to December 2022. Everyone is free to opt out at any point in time after informing.

Best of luck! ☘

* Required

1. Email *

____

2. What is Business Email Compromise (BEC)? *

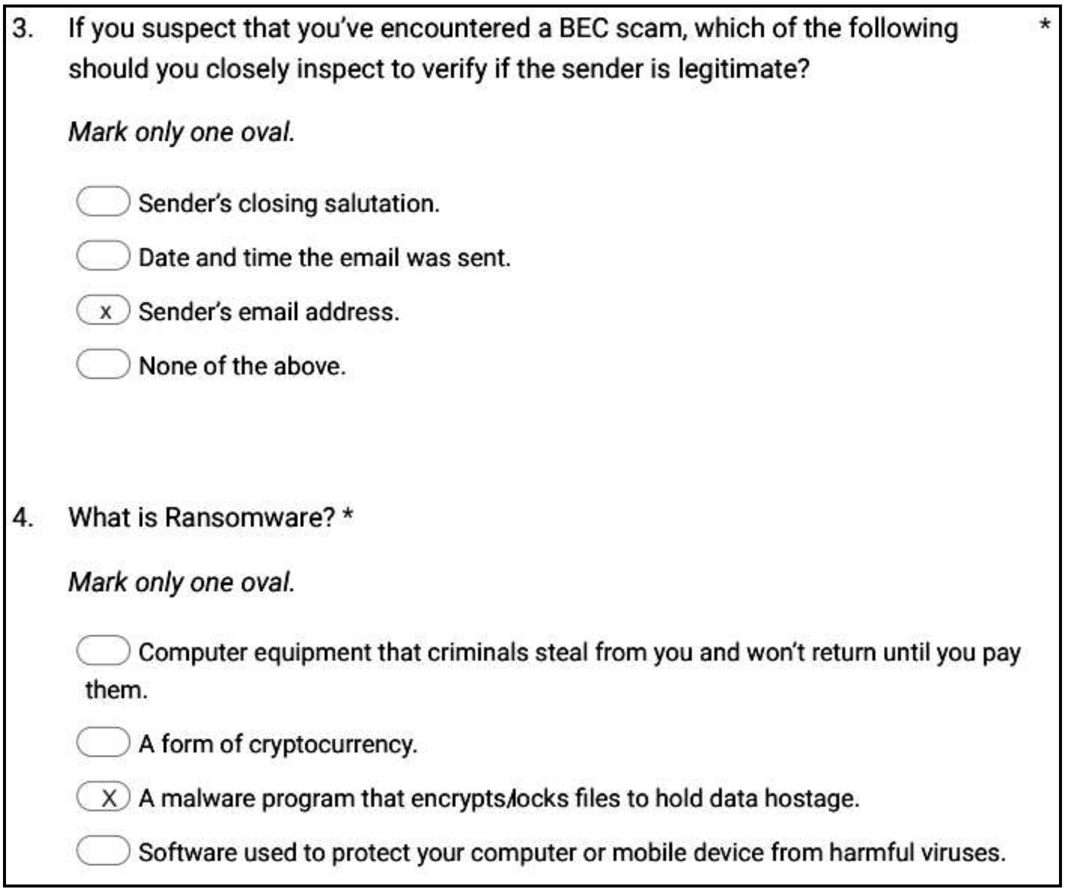
Mark only one oval.

☒ A form of social engineering attack that utilizes a spoofed business email, which contains a malicious file, a phishing URL, or an urgent wire transfer request

○ A phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents

○ A type of social engineering attack often used to steal user data, including login credentials and credit card numbers

○ An identity fraud in which attackers impersonate legitimate businesses' support accounts to fool social media users.



3. If you suspect that you've encountered a BEC scam, which of the following should you closely inspect to verify if the sender is legitimate? *

Mark only one oval.

○ Sender's closing salutation.

○ Date and time the email was sent.

☒ Sender's email address.

○ None of the above.

4. What is Ransomware? *

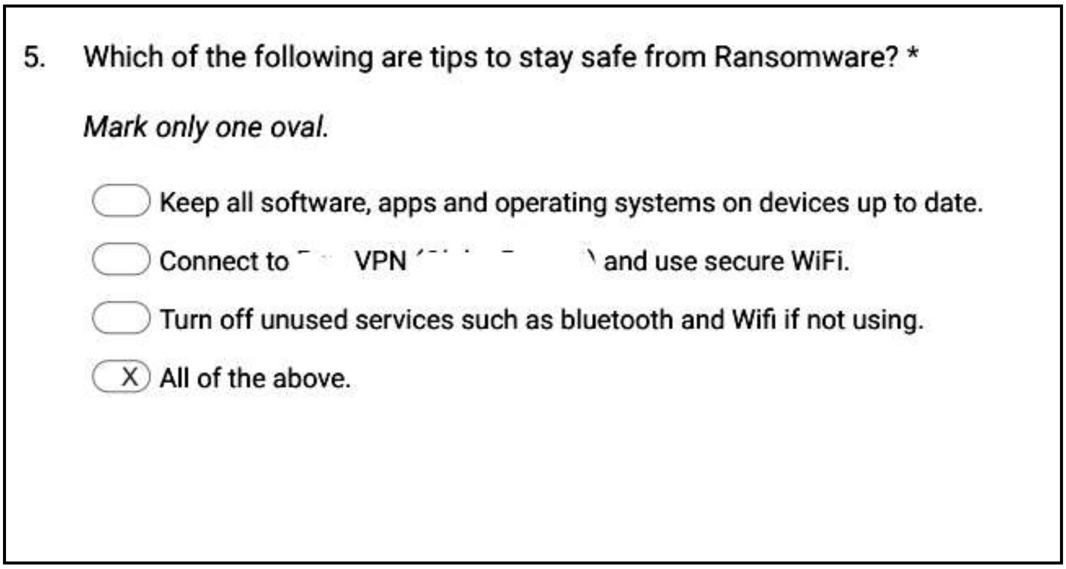
Mark only one oval.

○ Computer equipment that criminals steal from you and won't return until you pay them.

○ A form of cryptocurrency.

☒ A malware program that encrypts/locks files to hold data hostage.

○ Software used to protect your computer or mobile device from harmful viruses.



5. Which of the following are tips to stay safe from Ransomware? *

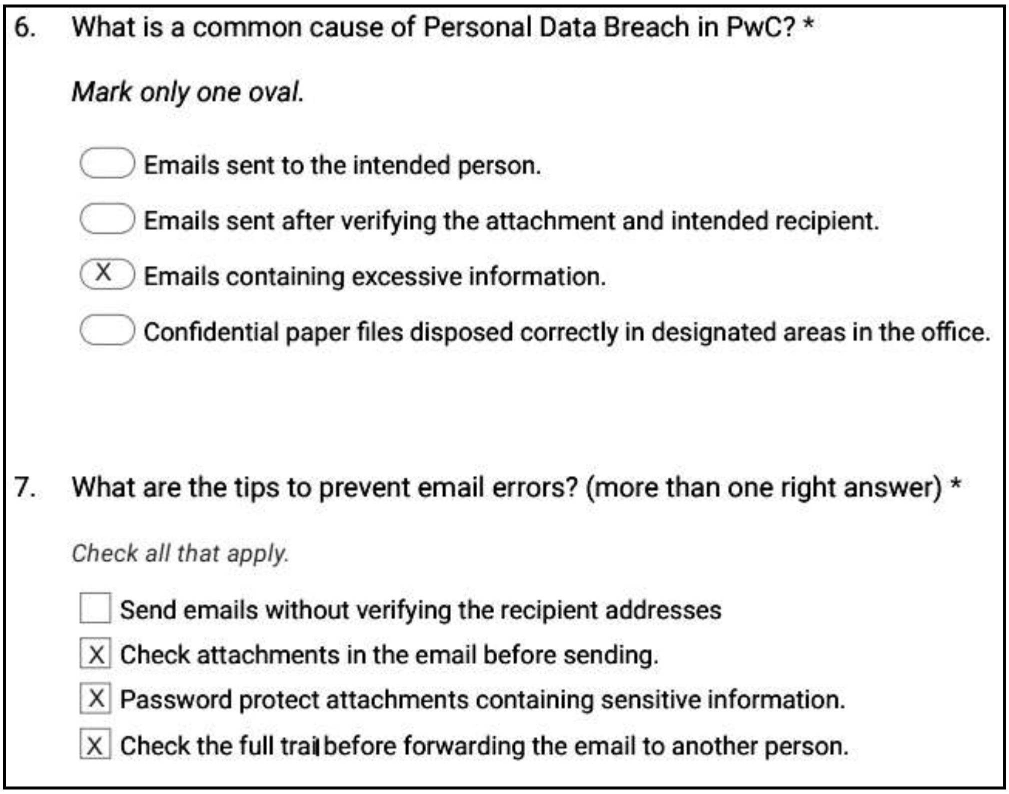
Mark only one oval.

○ Keep all software, apps and operating systems on devices up to date.

○ Connect to [redacted] VPN [redacted] and use secure WiFi.

○ Turn off unused services such as bluetooth and Wifi if not using.

☒ All of the above.



6. What is a common cause of Personal Data Breach in PwC? *

Mark only one oval.

○ Emails sent to the intended person.

○ Emails sent after verifying the attachment and intended recipient.

⊗ Emails containing excessive information.

○ Confidential paper files disposed correctly in designated areas in the office.

7. What are the tips to prevent email errors? (more than one right answer) *

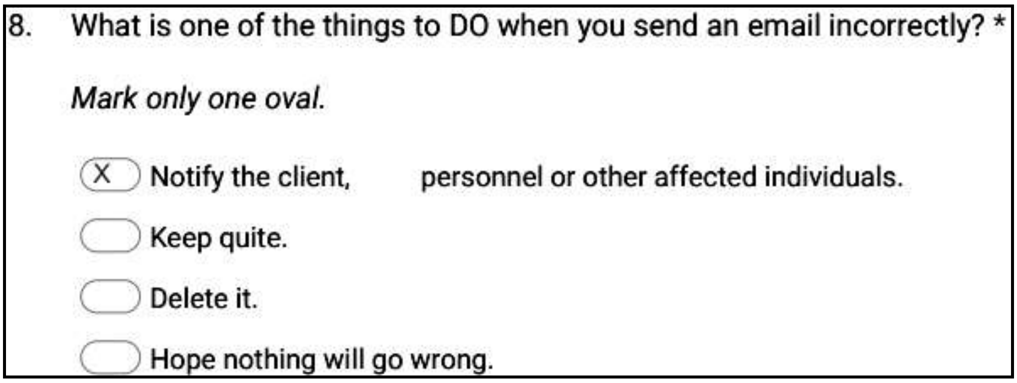
Check all that apply.

☐ Send emails without verifying the recipient addresses

☒ Check attachments in the email before sending.

☒ Password protect attachments containing sensitive information.

☒ Check the full trail before forwarding the email to another person.



8. What is one of the things to DO when you send an email incorrectly? *

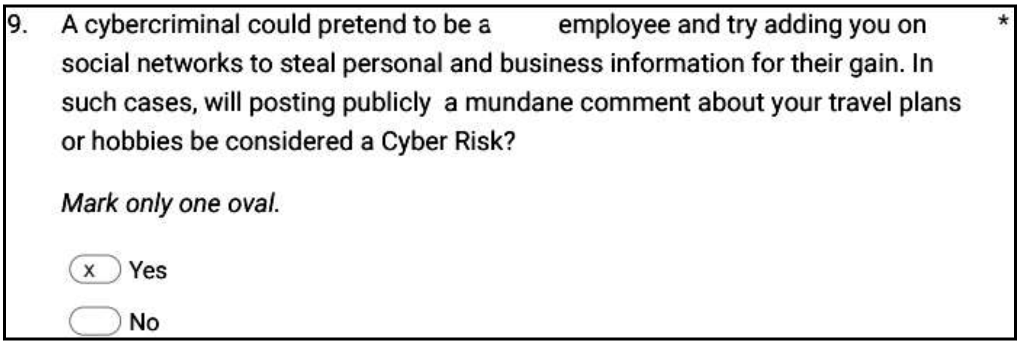
Mark only one oval.

⊗ Notify the client, personnel or other affected individuals.

○ Keep quite.

○ Delete it.

○ Hope nothing will go wrong.

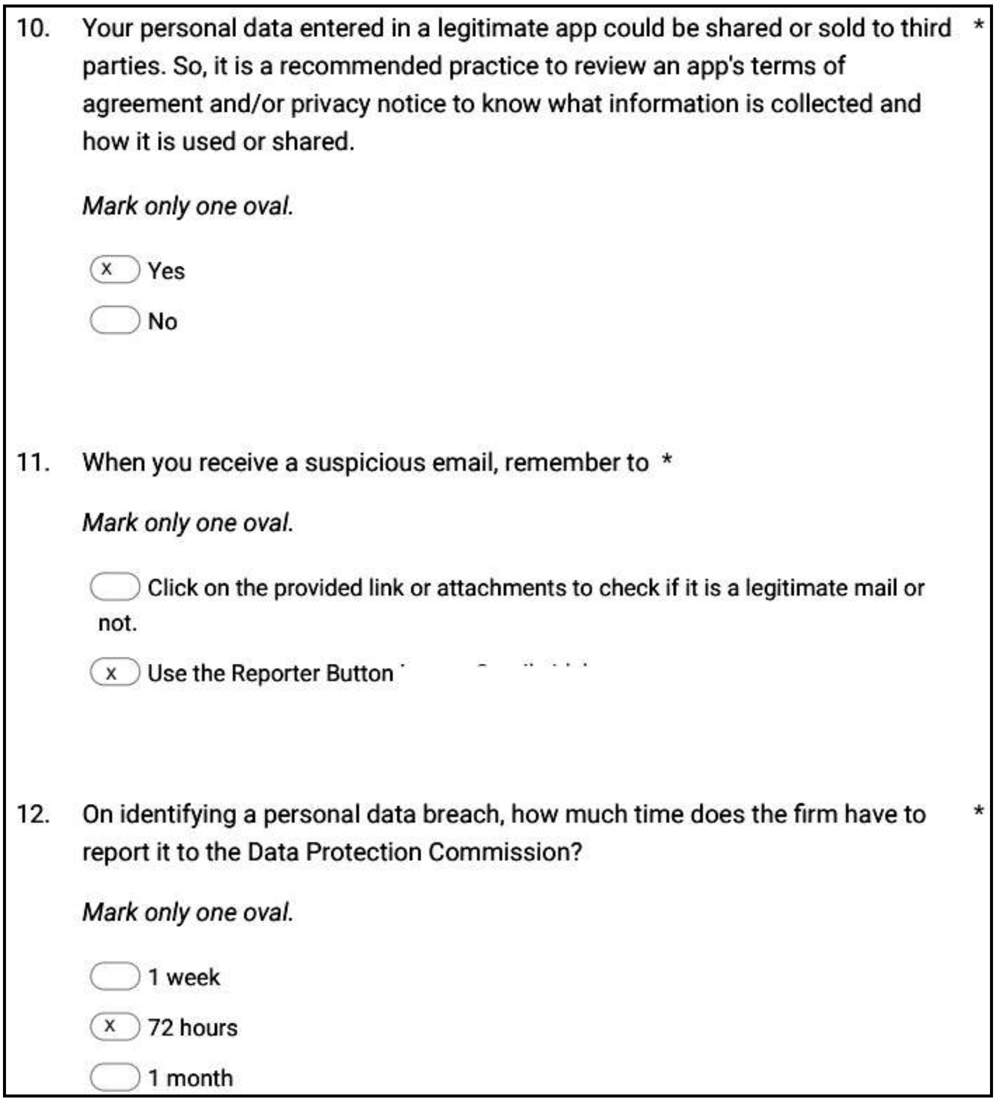


9. A cybercriminal could pretend to be a employee and try adding you on social networks to steal personal and business information for their gain. In such cases, will posting publicly a mundane comment about your travel plans or hobbies be considered a Cyber Risk? *

Mark only one oval.

⊗ Yes

○ No



10. Your personal data entered in a legitimate app could be shared or sold to third parties. So, it is a recommended practice to review an app's terms of agreement and/or privacy notice to know what information is collected and how it is used or shared. *

Mark only one oval.

☒ Yes

○ No

11. When you receive a suspicious email, remember to *

Mark only one oval.

○ Click on the provided link or attachments to check if it is a legitimate mail or not.

☒ Use the Reporter Button

12. On identifying a personal data breach, how much time does the firm have to report it to the Data Protection Commission? *

Mark only one oval.

○ 1 week

☒ 72 hours

○ 1 month

1.5 Decision-Strategy Based Model

Based on the data from the previous section, the participants were divided into categories of 2 types which is - Phished and Not Phished.

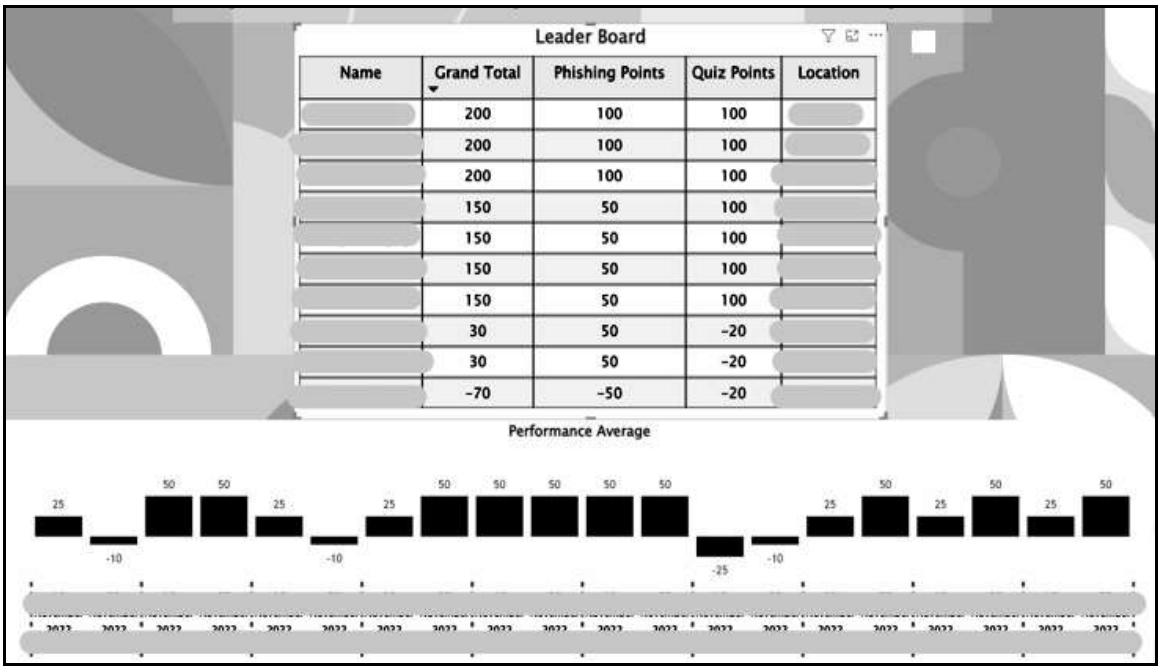
1. The participants that were phished were automatically subjected to security training videos by the dedicated team within the organisation.
2. **Points for Phished or Not Phished:**
    a. The points were *+100* points for participants that reported the phishing mail.
    b. The points were *+50* points for participants that did not report the phishing mail but also did not click the link.
    c. The points were *-50* points for the phished participants.
3. **Points for Assessment:** The topics for the quiz were published in the organisation's internal portal over the course of 1 month and a pass percentage of *80%* was set for the quiz.
    a. The participants who passed the cyber awareness quiz were awarded a total of *+100* points.
    b. The participants who failed the quiz were awarded *0* points
    c. The participants who did not attempt the quiz were awarded *-20* points.

Summary of Points

Phishing mail response points		Quiz response points	
Clicked on link	-50	Passed	+100
Ignored mail	-10	Failed	0
Reported mail	+100	Did not attempt	-20
Neither reported nor phished	+50		

1.6 Data Visualisation Resources

The data from Google Sheets were loaded to the Microsoft Power BI desktop application to visualise them using various graphs, trend lines, tables, and pie charts.

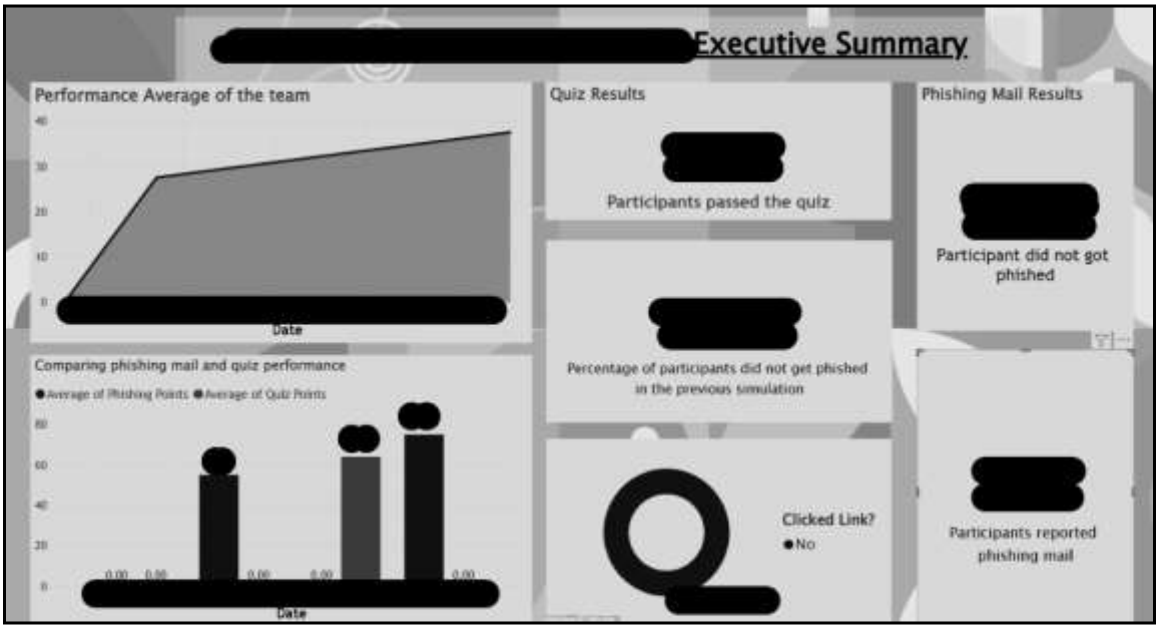


Leader Board

Name	Grand Total	Phishing Points	Quiz Points	Location
[redacted]	200	100	100	[redacted]
[redacted]	200	100	100	[redacted]
[redacted]	200	100	100	[redacted]
[redacted]	150	50	100	[redacted]
[redacted]	150	50	100	[redacted]
[redacted]	150	50	100	[redacted]
[redacted]	150	50	100	[redacted]
[redacted]	30	50	-20	[redacted]
[redacted]	30	50	-20	[redacted]
[redacted]	-70	-50	-20	[redacted]

Performance Average

5 – Leader board of participants



[redacted] Executive Summary

Performance Average of the team

Quiz Results

[redacted]

Participants passed the quiz

Phishing Mail Results

[redacted]

Participant did not got phished

Comparing phishing mail and quiz performance

[redacted]

Percentage of participants did not get phished in the previous simulation

[redacted]

Participants reported phishing mail

6 - Dashboard for management

2 Conclusion

This configuration manual contains the detailed steps pertaining to the process undertaken and is structured by the phases in sequential format of the research and ensures that it can be reused.

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Sabahath RIzwana Palappurath Showkath Student number: 21151474

Company: PwC Month Commencing: September

1. NIST Cybersecurity framework maturity assessment project
   1. Develop workshop notes based on the evidence documents received from clients.
   2. Prepare weekly status deck in advance of the weekly status calls with the client.
   3. Map the client's ERSA framework with NIST framework.
2. Research internship:
   1. Talk to stakeholders and get the required approvals for starting the project.
   2. Get consent of participants for the project
   3. Talk to data protection officer and get the approvals for getting phishing results for the target participants
   4. Talk to phishing simulation team and discuss the data required for the targeted participants and the timeline.

Employer comments

Saba has a keen interest to get things done and always reaches out to help. She displayed good understanding of technical concepts and is an eager learner.

Student Signature: Sabahath Rizwan Date: 15-10-2022

Industry Supervisor Signature: Date: 15-10-2022

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Sabahath RIzwana Palappurath Showkath Student number: 21151474

Company: PwC Month Commencing: October

1. NIST Cybersecurity framework maturity assessment project
   1. Transfer workshop responses to NIST Assessment tool and categorize the current state of the clients into strengths and constraints.
   2. Prepare weekly status deck in advance of the weekly status calls with the client.
   3. Sanitize previously used report templates for the executive summary and detailed. reports.
2. Research internship:
   1. Create a dashboard showing leader board and performance average of participants.
   2. Preparing the cyber awareness quiz for the participants.
   3. Retrieve the first phishing simulation results, analyse it and map points based on participants getting phished or not phished.
   4. Engage participants by showing their performance till date.

Employer comments

Saba was very hands-on and always comes in prepared. The engagement managers were extremely satisfied with her work.

Student Signature: Date: 15-11-2022

Industry Supervisor Signature: Date: 15-11-2022

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Sabahath RIzwana Palappurath Showkath Student number: 21151474

Company: PwC Month Commencing: November

1. NIST Cybersecurity framework maturity assessment project
   1. Work with the team in preparing the executive summary report.
   2. Work with the team in preparing the detailed report.
   3. Prepare weekly status deck in advance of the weekly status calls with the client.
2. Research internship:
   1. Design the leader board for participants
   2. Design executive summary dashboard consisting of trend line of performance, critical data for the management who make critical business decisions
   3. Retrieve the quiz results, analyse it and map points based on participants passing, failing or ignoring the quiz.
   4. Engaging participants by showing their performance till date.
   5. Retrieve the last phishing simulation results, analyse it and map points based on participants getting phished or not phished.
   6. Reward the winners

Employer comments

Saba was very diligent in her work and takes initiative. She managed her time effectively and delivered quality results. Overall intership performance has been brilliant.

Student Signature: Date: 15-12-2022

Industry Supervisor Signature: Date: 15-12-2022