National College of Ireland

Configuration Manual

MSc Research Project
MSc Cybersecurity

Jonas Schweizer
Student ID: X21168776

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Jonas Luis Schweizer
Student ID:	X21168776
Programme:	MSc Cybersecurity **Year:** 2023
Module:	Academic Internship
Lecturer:	Ross Spelman
Submission Due Date:	14/12/2023
Project Title:	Implementation of methods to raise employee's cybersecurity awareness in small businesses with small-scale IT teams.
Word Count:	2314 **Page Count:** 12

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: Jonas Luis Schweizer

Date: 13/12/2023

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

Jonas Schweizer
Student ID: X21168776

1 Data Gathering

The research paper data was gathered using Microsoft Forms. Both evaluation forms and participants consent agreement were delivered using this solution.

1.1 Evaluation Forms

Microsoft Forms was used to collect the answer of the 30 participants that answered the 42 questions from the first and second evaluation forms. The questions and answers have been added to the ICT Solution Artefact as their length was too large to be inserted here. Figure 1 shows the summary of number of participants and average time per evaluation. The first evaluation form is called "Inf. Sec Awareness Knowledge Evaluation", and the second form is called "End of Training Knowledge Evaluation". The first evaluation form contains 1 more answer as a staff member has left the organisation during the training period.

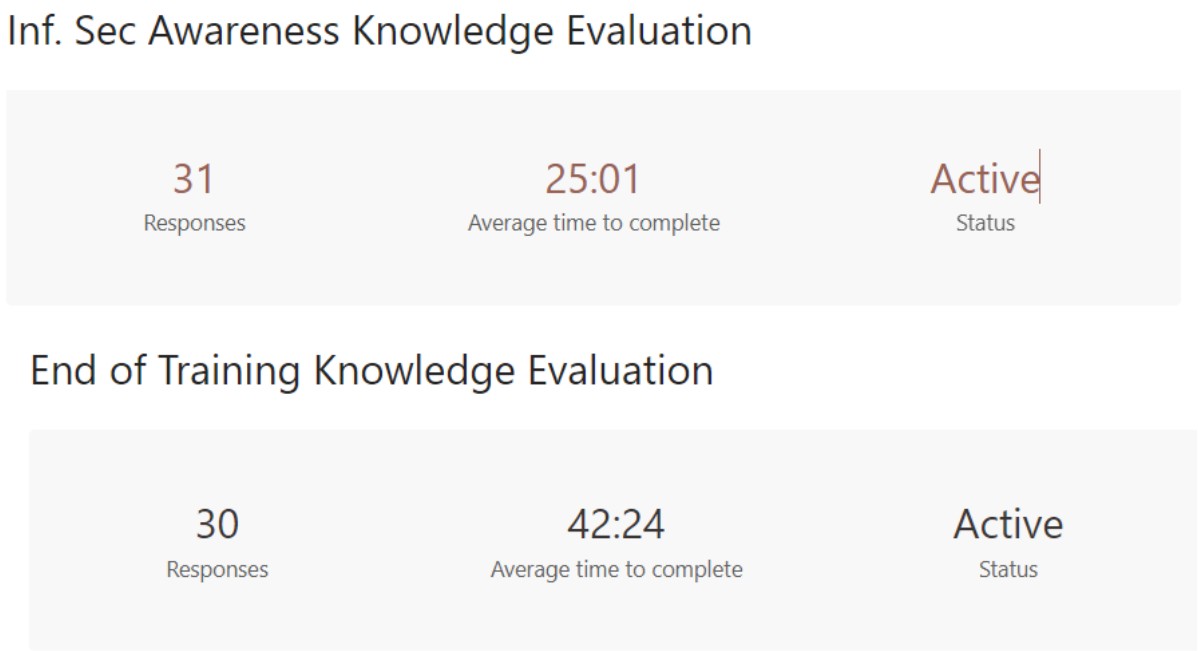


Figure 1 – Microsoft Forms summary of responses.

1.2 Full Dataset

In this section, the dataset that was used to record all the data collected from the research will be displayed. This dataset was used in section 6 of the academic internship for evaluation of the research. More details on what each column stands for are presented in the research paper.

Table I – Research dataset

Group	ID	Outcome	Completed	timestaff	timeit	Metric
B	13	0	100	173	70	0
A	35	5	0	0	192	0.026041667
C	24	8	100	426	110	0.072727273
D	23	2	100	236	130	0.015384615
D	20	-2	100	279	130	-0.015384615
A	29	0	0	0	192	0
B	28	3	0	0	70	0.042857143
D	11	0	100	210	130	0
D	7	0	100	252	130	0
B	6	5	100	251	70	0.071428571
B	16	2	100	205	70	0.028571429
A	34	3	0	0	192	0.015625
B	19	-2	100	244	70	-0.028571429
C	12	-8	100	395	110	-0.072727273
B	22	7	100	197	70	0.1
A	33	3	0	0	192	0.015625
A	31	3	0	0	192	0.015625
B	25	0	100	149	70	0
D	26	-2	100	301	130	-0.015384615
D	17	0	100	339	130	0
C	9	5	100	294	110	0.045454545
C	5	0	100	243	110	0
C	15	-7	100	924	110	-0.063636364
C	21	10	100	336	110	0.090909091
D	14	0	63.83	148	130	0
A	30	0	0	0	192	0
C	18	3	20	50	110	0.027272727
D	4	5	0	0	130	0.038461538
A	32	0	0	0	192	0
B	10	0	100	289	70	0

2 Wallpaper Images Configuration

The wallpaper configuration was separated in two sections. The first section was the setup of Windows Server Group Policy Objects (GPO) and server scripts to allow the wallpaper images to automatically rotate without the need of manual intervention. The second section was to select relevant and informative image wallpapers from the cybersecurity awareness tool to be displayed in the computers' desktop.

2.1 GPO Setup

Windows Server provides a simple desktop wallpaper GPO that can set one wallpaper image to be deployed across organisation computer. However, the method below describes the process for creating a windows policy to automatically change the wallpaper of staff without

the need of manually replacing the image every day as this was the set frequency for the project.

The GPO was created with the name SETA Wallpaper. Figure 2 displays the first part of the configuration which deployed the creation of a new folder in the staff computers.

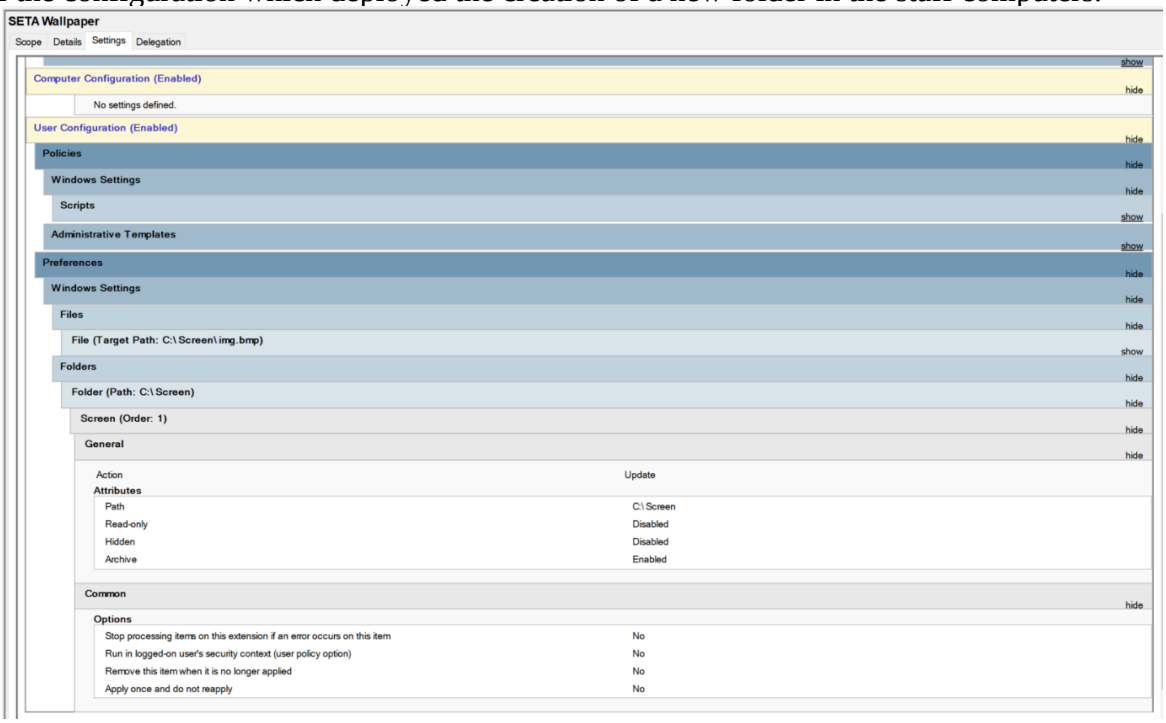


Figure 2 – Windows GPO folder creation.

Within the same GPO, we can set the image file to be copied from the source location to the local drive of the staff computer. Figure 3 shows the setting, source and destination files.

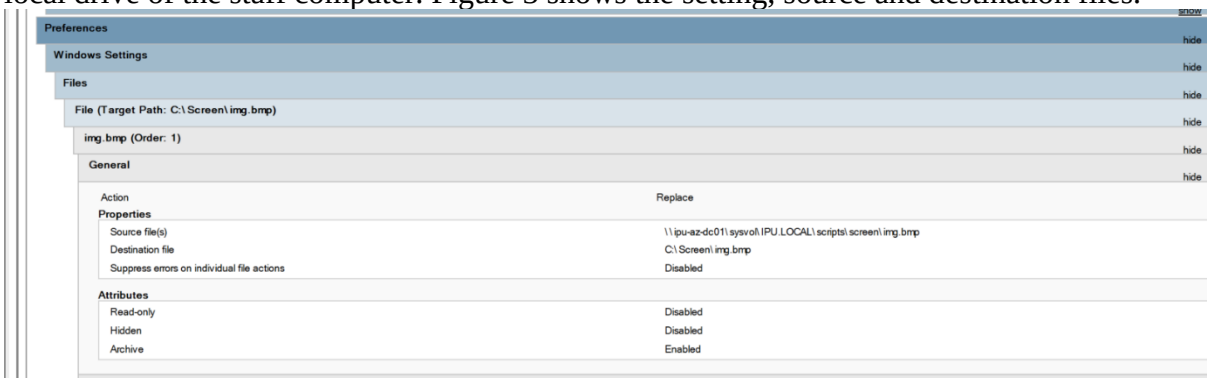


Figure 3 – Windows GPO file replacement.

It is now necessary to use the standard GPO setting to point out image file location and its name. Figure 4 shows that the location path is set to C:\screen\img.bpm, the same location we have previously set for the file to be copied.

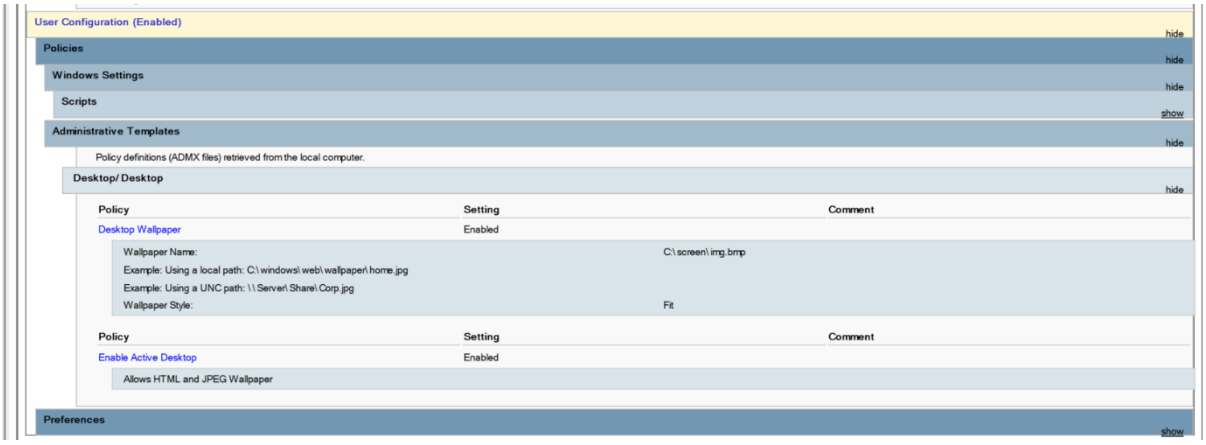


Figure 4 – Windows GPO desktop wallpaper image selection.

This script was also setup to copy the new image every time a new logon happens to the user while connected to the on-premises network.

```
mkdir C:\Screen
del /Q C:\Screen\*.*
xcopy \\ipu-az-dc01\SYSVOL\IPU.LOCAL\scripts\screen\img.bmp C:\Screen
```

Staff can be connected to the on-premises network within two scenarios:

- Being physically in the office
- Being connected via VPN.

Figure 5 shows the script being set to run in the same GPO.

Figure 5 – Windows GPO script execution.

2.1.1 Task Scheduler

In order to automatically replace the image, a scheduled task was created in the Active Directory Windows Server. Figure 6 shows the setup of the General tab of the scheduled task name “Update ScreenSaver images”.

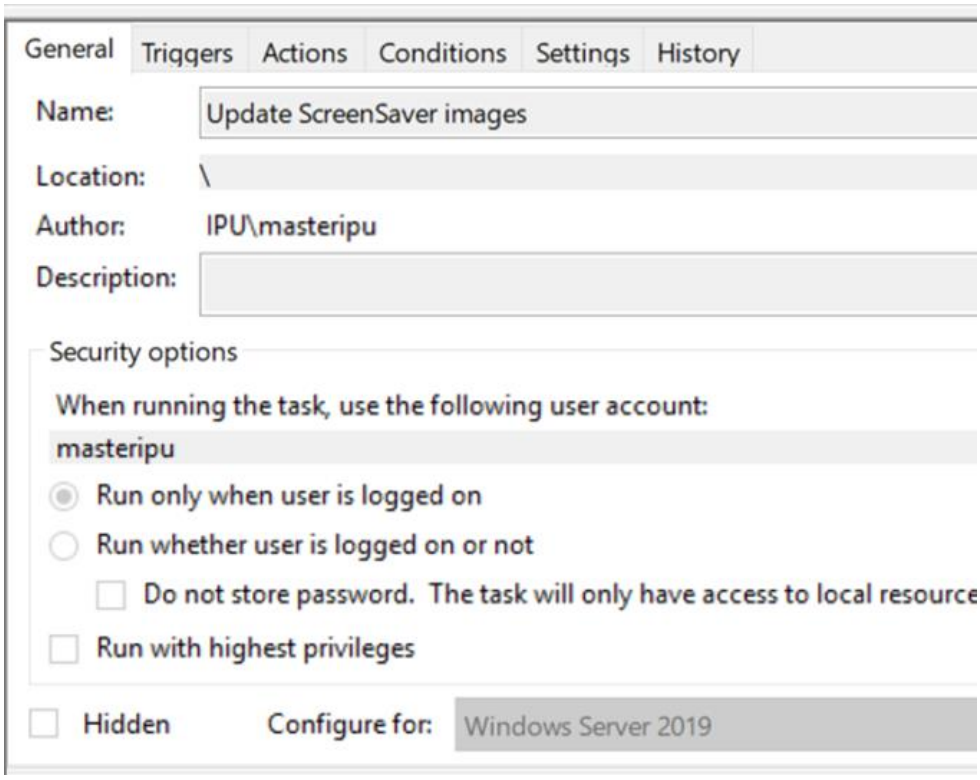


Figure 6 – Task scheduler general tab.

The trigger of the scheduled task is set to run each 30 minutes. Figure 7 shows the 2 triggers at evening time but with repetition after one hour for a duration of 24 hours.

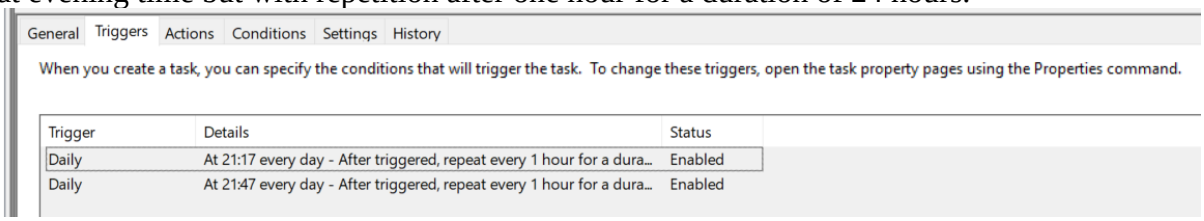


Figure 7 – Task scheduler trigger tab.

The action of the task scheduler to run the scripted located in the server desktop as Figure 8 shows.

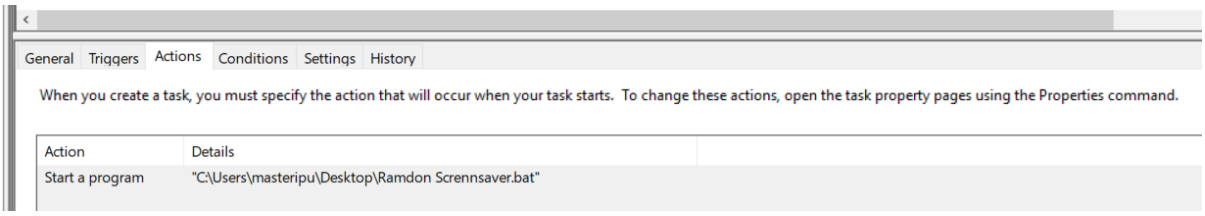


Figure 8 – Task scheduler actions tab.

The content of the script is displayed below:

```
@echo off
setlocal enabledelayedexpansion

set "sourceFolder=C:\Users\masteripu\Downloads\Img"
set "destinationFolder=C:\Windows\SYSVOL\sysvol\IPU.LOCAL\scripts\screen"
set "destinationFileName=img.bmp"

set "filesCount=0"
for %%F in ("%sourceFolder%\*.*") do (
```

```
    set /a "filesCount+=1"
    set "file[!filesCount!]=%%F"
)

if %filesCount% equ 0 (
    echo No files found in the source folder.
    exit /b
)

set /a "randomIndex=(%random% %% filesCount) + 1"
set "randomFile=!file[%randomIndex%]!"

copy /y "%randomFile%" "%destinationFolder%\%destinationFileName%"

echo File copied: %randomFile% to %destinationFolder%\%destinationFileName%

endlocal
```

The script sets source and destination folder where the file need to be copied and replace. The script also sets the file name that will be placed when the file is copied. Other parts of the script set the randomisation of the files and uses all the source and destination variables to replace the file in the destination.

2.2 Wallpaper Image Selection

Using the cybersecurity awareness tool, it is possible to navigate to the library of content and chose to display only the wallpaper images for a simpler selection. Figure 9 displays one of the 27 images that were selected in the process.

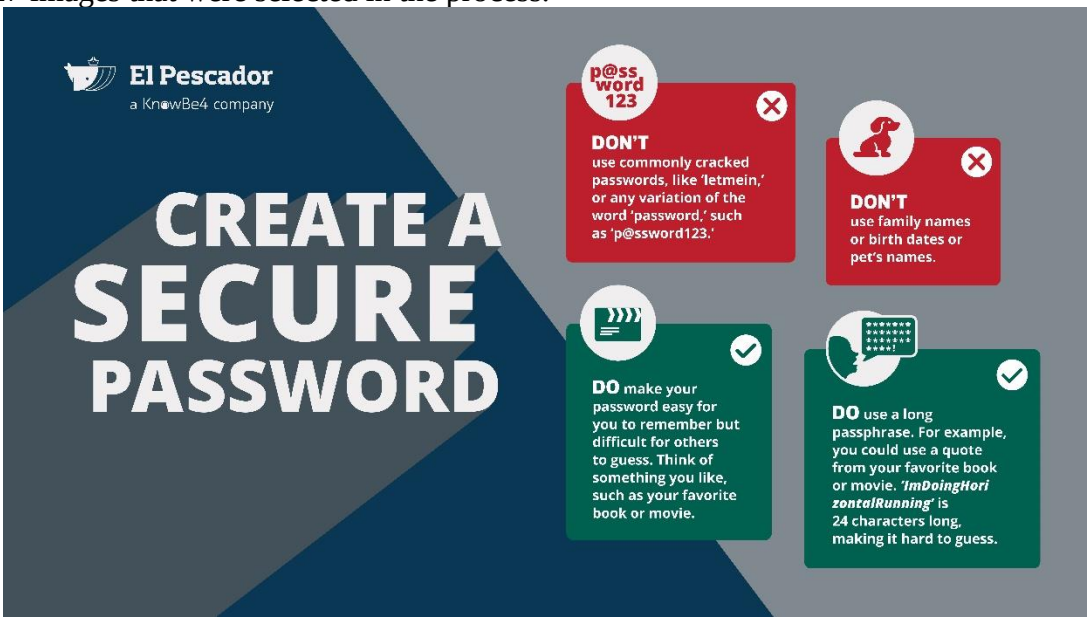


Figure 9 – Education desktop wallpaper image about secure passwords.

3 Phishing Simulation

Change the header and label to something appropriate.
Your third section. Change the header and label to something appropriate.

3.1 Setup

To create the delivery of email phishing simulations, the KnowBe4 tools was used. This is done through the Phishing Campaign feature of the tool. When creating a new campaign, the tool points out the predefined best practices and it is only necessary to adjust the section that are specific to the organisation. Figure 10 shows that the frequency of the campaign was set to weekly. The sending period was set up to business days and business hours. The specified group "Group A – Wall+Phish" was selected with the appropriate participants. The field template categories show the category that was created specifically for this campaign and "Full Random" ensures that each user will get a different template, in most cases.

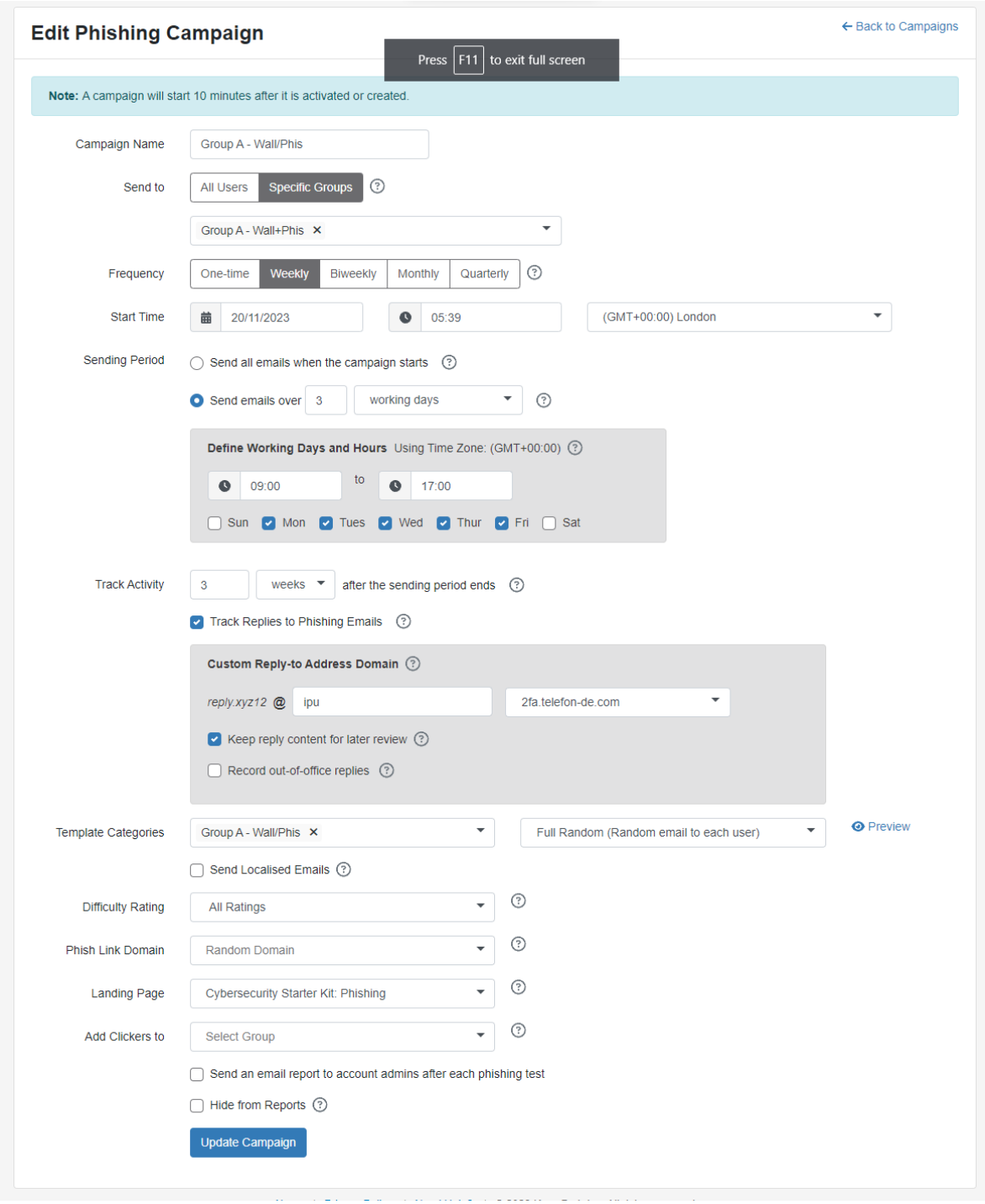
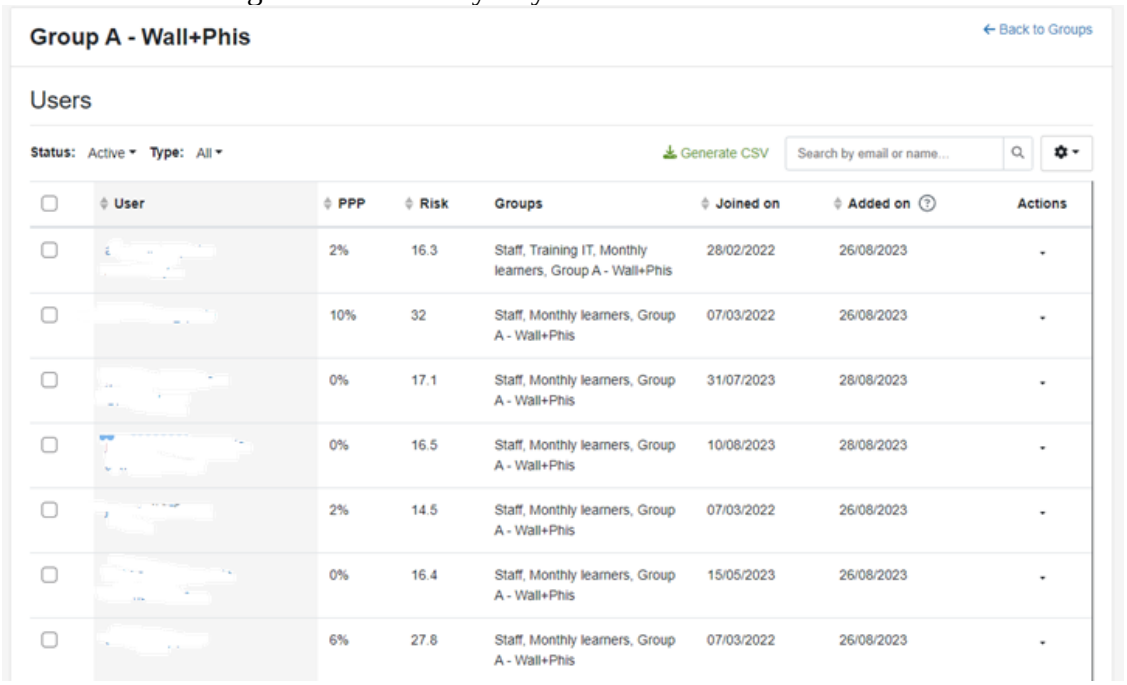


Figure 10 – KnowBe4 phishing campaign configuration page.

Figure 11 shows the seven participants of the group and other information. The names were removed from the image to ensure anonymity.



Group A - Wall+Phis

← Back to Groups

Users

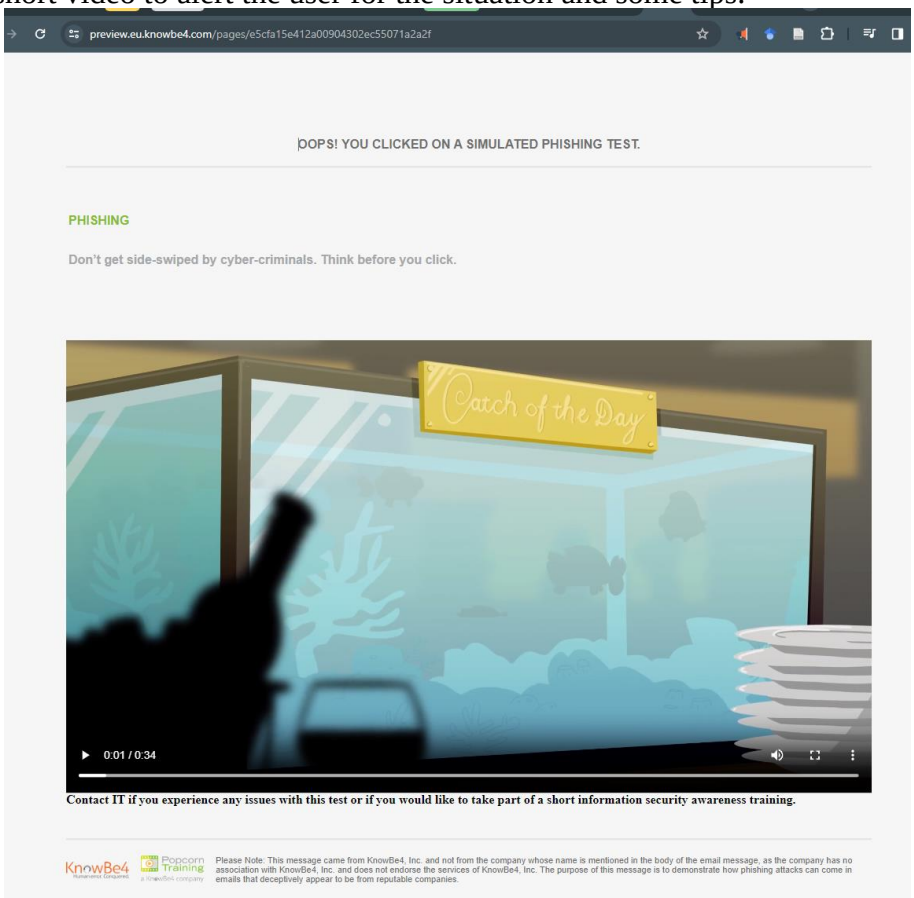
Status: Active Type: All

Generate CSV | Search by email or name...

User	PPP	Risk	Groups	Joined on	Added on	Actions
[redacted]	2%	16.3	Staff, Training IT, Monthly learners, Group A - Wall+Phis	28/02/2022	26/08/2023	
[redacted]	10%	32	Staff, Monthly learners, Group A - Wall+Phis	07/03/2022	26/08/2023	
[redacted]	0%	17.1	Staff, Monthly learners, Group A - Wall+Phis	31/07/2023	26/08/2023	
[redacted]	0%	16.5	Staff, Monthly learners, Group A - Wall+Phis	10/08/2023	26/08/2023	
[redacted]	2%	14.5	Staff, Monthly learners, Group A - Wall+Phis	07/03/2022	26/08/2023	
[redacted]	0%	16.4	Staff, Monthly learners, Group A - Wall+Phis	15/05/2023	26/08/2023	
[redacted]	6%	27.8	Staff, Monthly learners, Group A - Wall+Phis	07/03/2022	26/08/2023	

Figure 11 – Group A, wallpaper and phishing simulations group details.

Figure 12 shows the landing page selected for the campaign. The landing page is the web page that the users are redirected to when clicking on the simulated phishing. This page contains a short video to alert the user for the situation and some tips.



preview.eu.knowbe4.com/pages/e5cfa15e412a00904302ec55071a2a2f

OOPS! YOU CLICKED ON A SIMULATED PHISHING TEST.

PHISHING

Don't get side-swiped by cyber-criminals. Think before you click.

Contact IT if you experience any issues with this test or if you would like to take part of a short information security awareness training.

KnowBe4 Popcorn Training

Please Note: This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as the company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

Figure 12 – Phishing landing page for simulation failures.

3.1.1 Template Selection

Before the phishing campaign was created, the phishing templates were selected. KnowBe4 tool offers thousands of system and community templates. Only system templates were used in this project. Figure 13 shows the process of searching for templates. A left-hand side panel displays the categories of the templates and a search bar can be used to search for the template name.

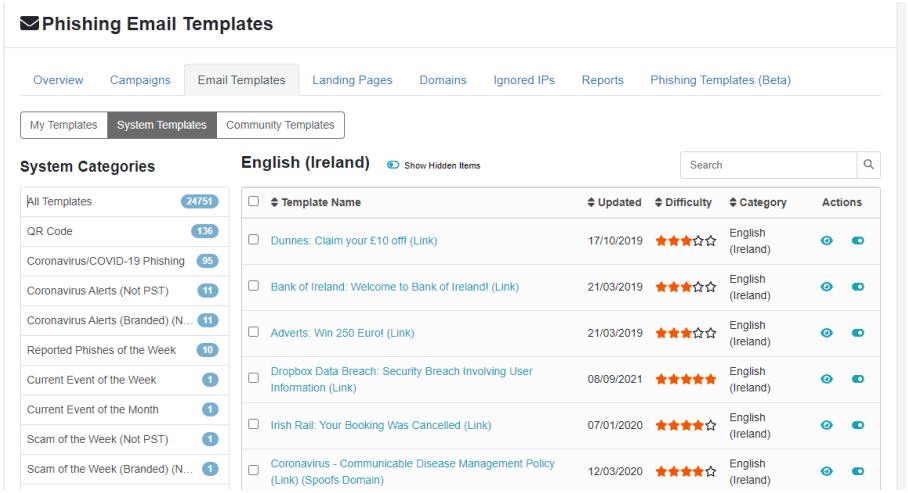


Figure 13 – KnowBe4 phishing simulation email templates library.

The templates can be previewed before the selection and the content of the email contains custom field that will automatically populate with your user information for an easy preview. Figure 13 shows a simulated template impersonation a communication from Bank of Ireland.

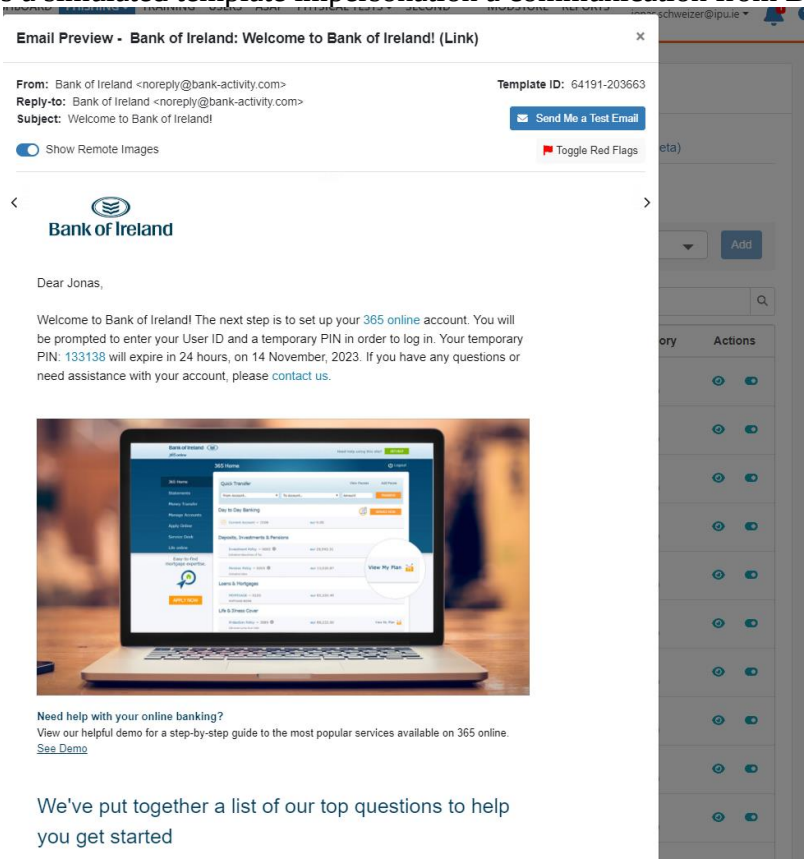


Figure 14 – Bank of Ireland simulated phishing templated.

Once the templates have been selected and added to the library, it is possible visualise all of them within the system. Figure 15 shows some of the templates selected for the phishing campaign.

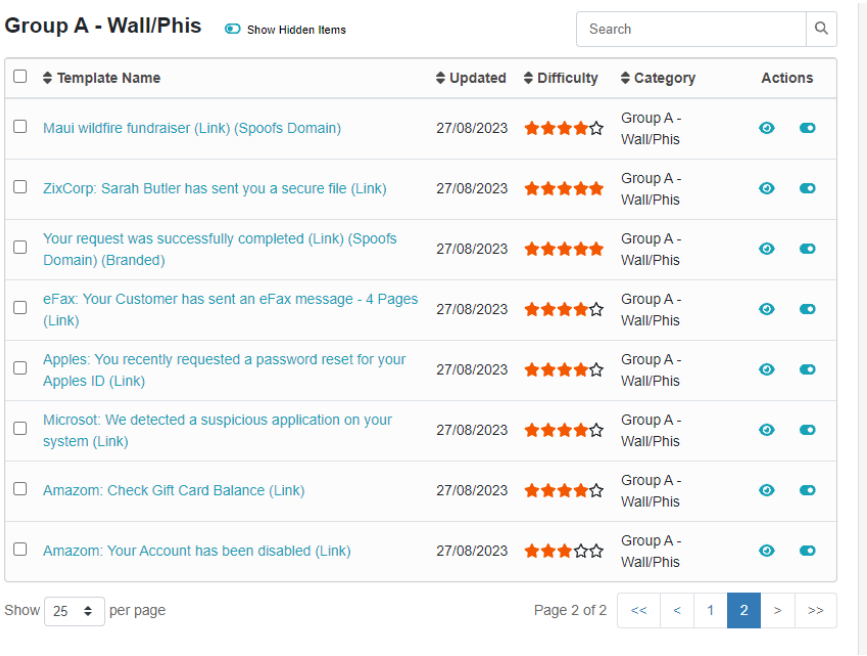


Figure 15 – Selected simulated phishing email templates library.

3.2 Phishing Results

Figure 16 shows the summary of the Group A phishing campaign. Each lines represent each time the campaign has ran. As the campaign was set to run weekly, we can see that it ran for 9 weeks. The number of participants remained seven across all weeks.

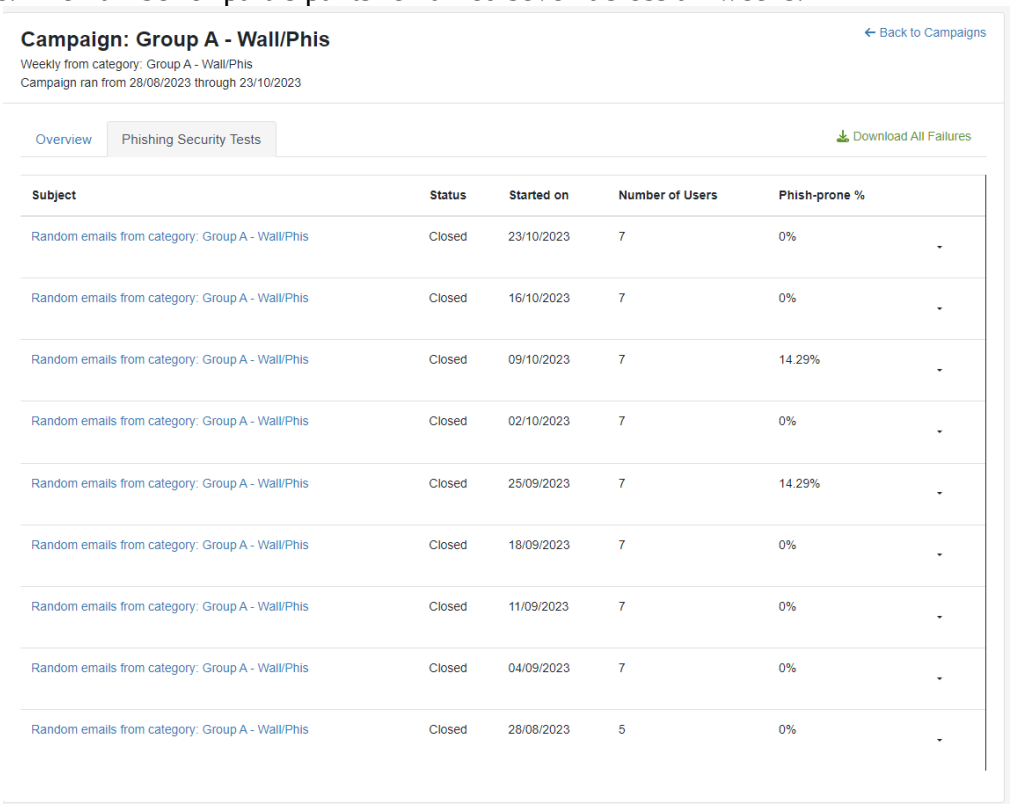


Figure 16 – Summary of the simulated phishing email campaign by week.

Figure 17 shows the overview of the campaign and the users that have failed. The users have been removed from the image to ensure anonymity.

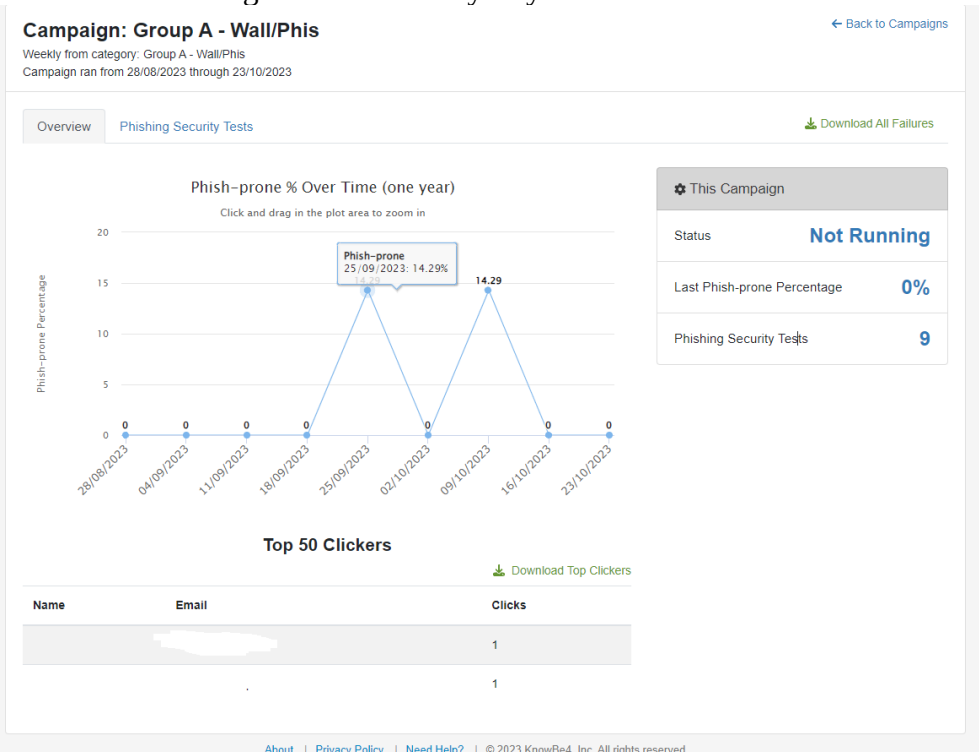


Figure 17 – Overall summary of simulated phishing email campaign.

4 Evaluation

This section will display all the commands used in R during the evaluation along with a brief explanation.

4.1 Importing Dataset

In this subsection, the commands used for data import and libraries installation will be displayed. The full dataset is presented in the previous section 1.2.

```
1. install.packages(c("ggplot2", "ggpubr", "tidyverse", "broom", "AICcmodavg"))
2. install.packages("ggcorrplot")
3. library(ggcorrplot)
4. library(readxl)
5. Fullresults <- read_excel("Thesis Results Dataset.xlsx",
6.   +     sheet = "FullResults", range = "A1:l31",
7.   +     col_types = c("text", "numeric", "skip",
8.   +                   "skip", "skip", "numeric", "numeric",
9.   +                   "numeric", "skip", "numeric", "skip",
10.  +                   "numeric"))
```

The lines one to four include commands that import different libraries that will be required to the project. Lines five to the end are a series of commands that are choosing a excel spreadsheet file and importing it with a sequence of specification. The commands are ensuring only valid column and rows of the spreadsheet are imported and setting the data type of each column as well as skipping columns that are not required.

4.2 Analysing Data

The four commands below are to view and summarise the data. The first two command display and summarise data related to the whole dataset. The last two commands summarise specific variables and returns information like minimum and maximum number as well as median and mean of the variables overall.

```
1. View(Fullresults)
2. summary(Fullresults)
3. summary(Fullresults$Outcome)
4. summary(Fullresults$Metric)
```

The commands below select two of the variables displaying the mean of the first variable selected. In this case we are displaying mean of the outcome by group.

```
1. outcomegroup_mean <- tapply(Fullresults$Outcome, Fullresults$Group, mean)
2. print(outcomegroup_mean)
```

The commands below select two of the variables displaying the mean of the first variable selected. In this case we are displaying the mean of the metric by group.

```
1. metricgroup_mean <- tapply(Fullresults$Metric, Fullresults$Group, mean)
2. print(metricgroup_mean)
```

4.3 Analysis of Variance (ANOVA)

The below commands generate the ANOVA table and displays its summary. The “aov” command is the R command used to generate the calculation. Metric is set as the dependent variable and Group as the independent variable. The command “data = Fullresults” stands for the dataset being used in the calculation. The “summary” command gives the results of the calculation and “anova” stands for the variable where the results are stored.

```
1. anova <- aov(Metric ~ Group, data = Fullresults)
2. summary(anova)
```

4.4 Analysis of Correlation

The command below analyses correlation among all the numeric variables presented in the project dataset. Line one creates a subset of the data by removing the variable Group from the “Fullresults” dataset. This variable is removed from the dataset as it is not a numeric variable. Line two generates the correlation with the reduced data, rounding the values to a maximum of two decimal places. Line three uses the “corr_matrix generated by line two and uses the command “ggcorrplot” to generate a visual plot with all the variables values in an order. Line four uses the continuation of line three with the ordering commands.

```
1. reduced_data <- subset(Fullresults, select = -Group,)
2. corr_matrix = round(cor(reduced_data), 2)
3. ggcorrplot(corr_matrix, hc.order = TRUE, type = "lower",
4. lab = TRUE)
```