

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					
Date:	14/12/2023					
Project Title: Implementation of methods to raise employee's cy awareness in small businesses with small-scale IT						

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.

<u>ALL</u> 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.

Inf. Sec Awareness Knowledge Evaluation



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.

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

 Table I – Research dataset

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.

muter One formation (Franklan)		
nputer Configuration (Enabled)		
No settings defined.		
er Configuration (Enabled)		
olicies		
Windows Settings		
Scripts		
,		
Administrative Templates		
references		
Windows Settings		
Files		
File (Target Path: C:\Screen\img.bmp)		
Folders		
Folder (Path: C:\Screen)		
Screen (Order: 1)		
Conserved		
General		
Action	Update	
Attributes		
Path	C\Screen	
Read-only	Disabled	
Hidden	Disabled	
Archive	Enabled	
Common		
Options		
Stop processing items on this extension if an error occurs on this item	No	
Run in logged-on user's security context (user policy option)	No	
Remove this item when it is no longer applied	No	

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.

	Preferences		bida
L	Windows Settings		1100
L			hide
L	Files		hide
L	File (Target Path: C:\Screen\img.bmp)		
L	ima hma (Order, 1)		hide
L			hide
L	General		hide
L	Action	Penlace	1100
L	Properties	repare	
L	Source file(s)	\\ipu-az-dc01\sysvol\IPU.LOCAL\scripts\screen\img.bmp	
L	Destination file	C.\ Screen\ img.bmp	
L	Suppress errors on individual file actions	Disabled	
L	Attributes		
L	Read-only	Disabled	
L	Hidden	Disabled	
L	Archive	Enabled	
T.			

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.

ser Configuration (Enabled)				
Policies				
Windows Settings				
Scripts				
Administrative Templates				
Policy definitions (ADMX files) retrieved from the local con	nputer.			
Desktop/ Desktop				
Policy	Setting		Comment	
Desktop Wallpaper	Enabled			
Wallpaper Name:		C:\screen\img.bmp		
Example: Using a local path: C:\windows\web\wa	lipaper\ home.jpg			
Example: Using a UNC path: \\Server\Share\Cor	.jpg			
Wallpaper Style:		Fit		
Policy	Setting		Comment	
Enable Active Desktop	Enabled			
Allows HTML and IDEC Wallsaner				
Allows HT Mc and SPEG Waipaper				

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.

Us	ser Configuration (Enabled)		hide
F	Policies		hide
1	Windows Settings		hite
1	Scripts		hide
	Logon		hide
	For this GPO, Script order: Not configured		hide
	Name	Parameters	
	C:\Windows\SYSVOL\sysvol\IPU.LOCAL\scripts\cc	/screens.bat	

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".

General Trigo	gers Actions	Conditions	Settings	History						
Name:	Update Scree	nSaver image	5							
Location:	١									
Author:	IPU\masterip	eu -								
Description:										
Security opt When runn masteripu	ions ing the task, u	se the followir	ng user acc	:ount:						
Run onl	y when user is	logged on								
O Run who	ether user is lo	gged on or no	ot							
Do	Do not store password. The task will only have access to local resource									
Run wit	h highest privi	leges								
Hidden	Configu	ure for: Wind	lows Serve	r 2019						

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.

G	eneral	Triggers	Actions Con	ditions S	Settings	History					
	When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.										
	Trigge	er	Details							Status	
	Daily		At 21:17	every day	- After tr	iggered, r	epeat ev	ery 1 hou	r for a dura	Enabled	
	Daily		At 21:47	every day	- After tr	iggered, r	epeat ev	ery 1 hou	r for a dura	Enabled	

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.

· ·										
G	General	Triggers	Actions	Conditions	Settings	History				
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command								command.		
	Action		De	tails						
	Start a	program	"C:	\Users\masteri	ipu\Deskto	op\Ramdo	n Scrennsaver.bat"			

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.

Edit Phishing C	Prass F11 to evit full screen	← Back to Campaigns
Note: A campaign will st	art 10 minutes after it is activated or created.	
Campaign Name	Group A - Wall/Phis	
Send to	All Users Specific Groups 3	
	Group A - Wall+Phis ×	
Frequency	One-time Weekly Biweekly Monthly Quarterly	
Start Time	 	•
Sending Period	○ Send all emails when the campaign starts ③	
	Send emails over 3 working days	
	Define Working Days and Hours Using Time Zone: (GMT+00:00) ③	
	Image: 09:00 to Image: 17:00	
	Sun ♥ Mon ♥ Tues ♥ Wed ♥ Thur ♥ Fri Sat	
Track Activity	3 weeks after the sending period ends (?)	
	Track Replies to Phishing Emails (?)	
	Custom Reply-to Address Domain 🛞	
	reply.xyz12 @ ipu 2fa.telefon-de.com 🔻	
	Keep reply content for later review ③	
	Record out-of-office replies	
Template Categories	Group A - Wall/Phis × Full Random (Random email to each user)	Preview
	Send Localised Emails ⑦	
Difficulty Rating	All Ratings	
Phish Link Domain	Random Domain	
Landing Page	Cybersecurity Starter Kit: Phishing	
Add Clickers to	Select Group	
	Send an email report to account admins after each phishing test	
	Hide from Reports ③	
	Update Campaign	

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									
Users									
Status:	Active - Type: All -		🛓 Generate CSV			Search by email or name	۹. ۵.		
\Box	\$ User	\$ PPP	† Risk	Groups	Joined on	Added on ⑦	Actions		
		2%	16.3	Staff, Training IT, Monthly learners, Group A - Wall+Phis	28/02/2022	26/08/2023			
		10%	32	Staff, Monthly learners, Group A - Wall+Phis	07/03/2022	26/08/2023			
		0%	17.1	Staff, Monthly learners, Group A - Wall+Phis	31/07/2023	28/08/2023			
		0%	16.5	Staff, Monthly learners, Group A - Wall+Phis	10/08/2023	28/08/2023			
	1	2%	14.5	Staff, Monthly learners, Group A - Wall+Phis	07/03/2022	26/08/2023			
		0%	16.4	Staff, Monthly learners, Group A - Wall+Phis	15/05/2023	26/08/2023	-		
		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.



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.

Phishing Email Templates									
Overview Campaigns Emai	Templates Landing Pages Domains Ignored IPs	Reports	Phishing Terr	nplates (Beta)					
My Templates System Templates	Community Templates								
System Categories	English (Ireland) Show Hidden Items		Search	1		Q			
All Templates 24751	Template Name	Updated	Difficulty	Category	Act	ions			
QR Code (136)	Dunnes: Claim your £10 off! (Link)	17/10/2019	★★★ ☆☆	English (Ireland)	ø	•			
Coronavirus/COVID-19 Phishing 95				(including)					
Coronavirus Alerts (Not PST) (1)	Bank of Ireland: Welcome to Bank of Ireland! (Link)	21/03/2019	★★★ ☆☆	English (Ireland)	Ø				
Coronavirus Alerts (Branded) (N 11)	Adverts: Win 250 Euro! (Link)	*****	English	0	•				
Reported Phishes of the Week 10				(Ireland)					
Current Event of the Week 1	Dropbox Data Breach: Security Breach Involving User Information (Link)	08/09/2021	****	English (Ireland)	Ø				
Current Event of the Month				English					
Scam of the Week (Not PST)	Insh Rail: Your Booking Was Cancelled (Link)	07/01/2020	*** *	(Ireland)	0	•			
Scam of the Week (Branded) (N 1	Coronavirus - Communicable Disease Management Policy (Link) (Spoofs Domain)	12/03/2020	****	English (Ireland)	Ø	•			

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.

Gro	Dup A - Wall/Phis Show Hidden Items	Sea	Search			
	Template Name	Updated	Difficulty	Category	Acti	ons
	Maui wildfire fundraiser (Link) (Spoofs Domain)	27/08/2023	★★★★ ☆	Group A - Wall/Phis	0	
	ZixCorp: Sarah Butler has sent you a secure file (Link)	27/08/2023	****	Group A - Wall/Phis	0	•
	Your request was successfully completed (Link) (Spoofs Domain) (Branded)	27/08/2023	****	Group A - Wall/Phis	0	C
	eFax: Your Customer has sent an eFax message - 4 Pages (Link)	27/08/2023	★★★★ ☆	Group A - Wall/Phis	0	C
	Apples: You recently requested a password reset for your Apples ID (Link)	27/08/2023	***	Group A - Wall/Phis	0	
	Microsot: We detected a suspicious application on your system (Link)	27/08/2023	★★★★ ☆	Group A - Wall/Phis	0	
	Amazom: Check Gift Card Balance (Link)	27/08/2023	★★★★ ☆	Group A - Wall/Phis	0	•
	Amazom: Your Account has been disabled (Link)	27/08/2023	★★★ ☆☆	Group A - Wall/Phis	0	C
Shov	v 25 🜩 per page		Page 2 of 2	< < 1	2 >	>>

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.

Campaign: Group A - Wall/Phis ← Back to Campaign: Veekly from category: Group A - Wall/Phis Campaign ran from 28/08/2023 through 23/10/2023							
Overview Phishing Security Tests				🛓 Download	All Failures		
Subject	Status	Started on	Number of Users	Phish-prone %			
Random emails from category: Group A - Wall/Phis	Closed	23/10/2023	7	0%	·		
Random emails from category: Group A - Wall/Phis	Closed	16/10/2023	7	0%	•		
Random emails from category: Group A - Wall/Phis	Closed	09/10/2023	7	14.29%	-		
Random emails from category: Group A - Wall/Phis	Closed	02/10/2023	7	0%	•		
Random emails from category: Group A - Wall/Phis	Closed	25/09/2023	7	14.29%	•		
Random emails from category: Group A - Wall/Phis	Closed	18/09/2023	7	0%	•		
Random emails from category: Group A - Wall/Phis	Closed	11/09/2023	7	0%	•		
Random emails from category: Group A - Wall/Phis	Closed	04/09/2023	7	0%	•		
Random emails from category: Group A - Wall/Phis	Closed	28/08/2023	5	0%	-		

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 = "A1:131",

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)