National College of Ireland

Configuration Manual

MSc Industrial Internship
MSc in Cybersecurity

Olumide Oladapo
Banjo

Student ID: x22181539

School of Computing

National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Olumide Banjo
Student ID:	x22181539
Programme:	MSC CYBERSECURITY **Year:** 2023
Module:	MSc Internship
Supervisor:	Vikas Sahni
Submission Due Date:	05/01/2024
Project Title:	Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats
Word Count:	1895
Page Count:	14

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: Olumide Banjo

Date: 1/3/2024

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

Olumide Banjo
Student ID: x22181539

1 Introduction

This manual shows the methodology adopted for conducting the research project, aimed at evaluating the efficacy of cybersecurity training against social engineering threats. It guides the reader through the project's phases, including survey deployment, data collection, and analysis procedures.

2 Questionnaire Design and Distribution

The design and distribution of the questionnaire were critical components of the research process, involving several key steps:

- **Questionnaire Creation with Google Forms**: A user-friendly and accessible platform, Google Forms, was chosen to develop the questionnaire.
- **Demographic Data Collection*:*** Questions were designed to gather basic demographic information:
    - Age: Categorized into groups (Below 20, 20-29, 30-39, 40-49, 50 and above).
    - Gender: Binary options (Male, Female).
    - Occupation: Open-ended field to capture a variety of IT-related roles.
- **Cybersecurity Training Background:**
    - Queries about prior cybersecurity training attendance.
    - Training type options (Workshop, Online Course, Seminar, Others).
    - Training frequency (Never, Annually, Biannually, more than twice a year).
- **Knowledge Assessment:**
    - Questions on phishing and baiting awareness with options (Yes, No, Uncertain).
- **Feedback Solicitation:**
    - Open-ended questions for improvement suggestions.
    - General feedback on cybersecurity training.

- **Participant Selection for Survey:**
    - Employed purposive sampling targeting varied organizational roles.
    - Focused on individuals with different levels of cybersecurity training.
- **Survey Distribution:**
    - Disseminated via email for easy access.
    - Ensured participant anonymity and data protection.
    - Adjusted settings to anonymize responses and encrypt data.
    - Assured participants of confidentiality to promote honest responses.

The screenshots below illustrate the questionnaire in Google Forms:

ENHANCING CYBERSECURITY THROUGH COMPREHENSIVE USER TRAINING PROGRAMS SURVEY

Hi, I am Olumide, thanks your for interest to participate in my survey

OVERVIEW & CONSENT

- ***Study Overview:*** This research work forms a segment of my MSc. undertaking at the *National College of Ireland*. The research aims to evaluate the effectiveness of training programs and proposes enhancements to bolster defences against deceptive cyber schemes, highlighting the significance of understanding human aspects in digital security
- ***Participant's Involvements:*** You will be asked to complete an online survey, consisting easy to answer questions and this will take about 5 to 10 minutes.

NOTE: *Your involvement is voluntary and you may choose to withdraw at any point without any penalties*

- ***Privacy Assurance:*** Personal Identifiable data would not be collected, as all entries are anonymous to ensure your privacy. All data collected will be used only for the purpose of the stated research.

Inquiries: For any question or clarification regarding the study. feel free to contact me via x22181539@student.ncirl.ie Olumide Banjo

Consent Acknowledgement: *By clicking the **"Next"** Button below, you agree that you are:*

- 18 years of age or older
- Have read and understood the above information
- Consent to participate in this research study

Figure 1: Consent Statement

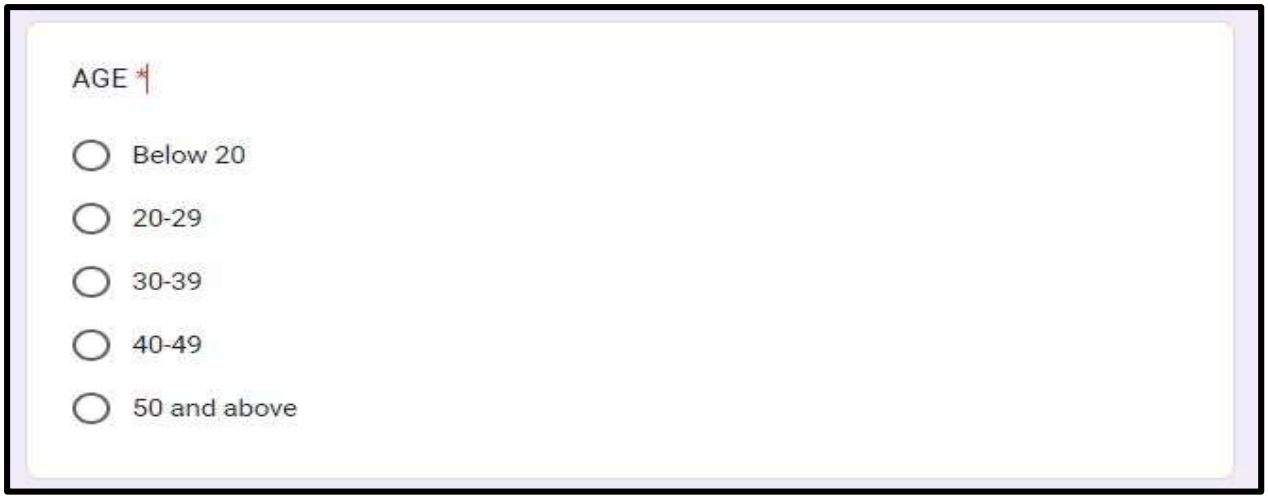

Figure 2: Age of Respondents

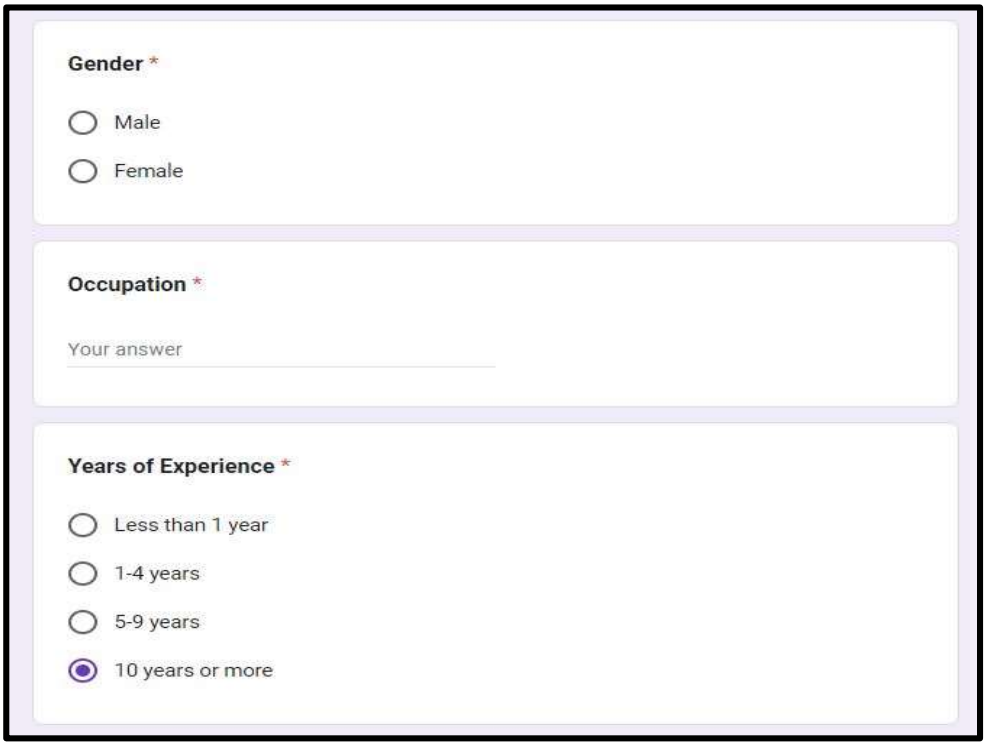

Figure 3: Gender, Occupation, and Years of Experience

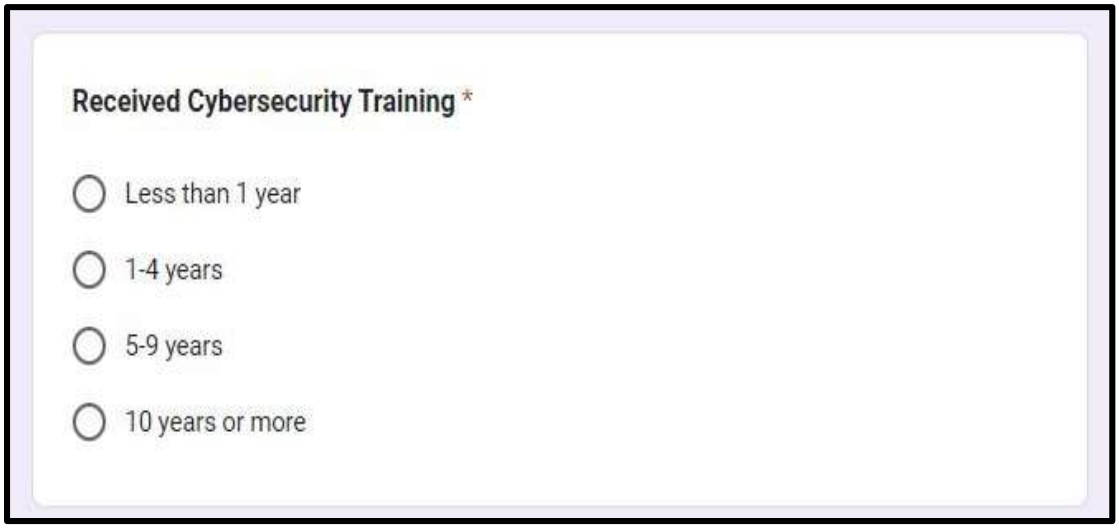

Figure 4: Received Cybersecurity Training

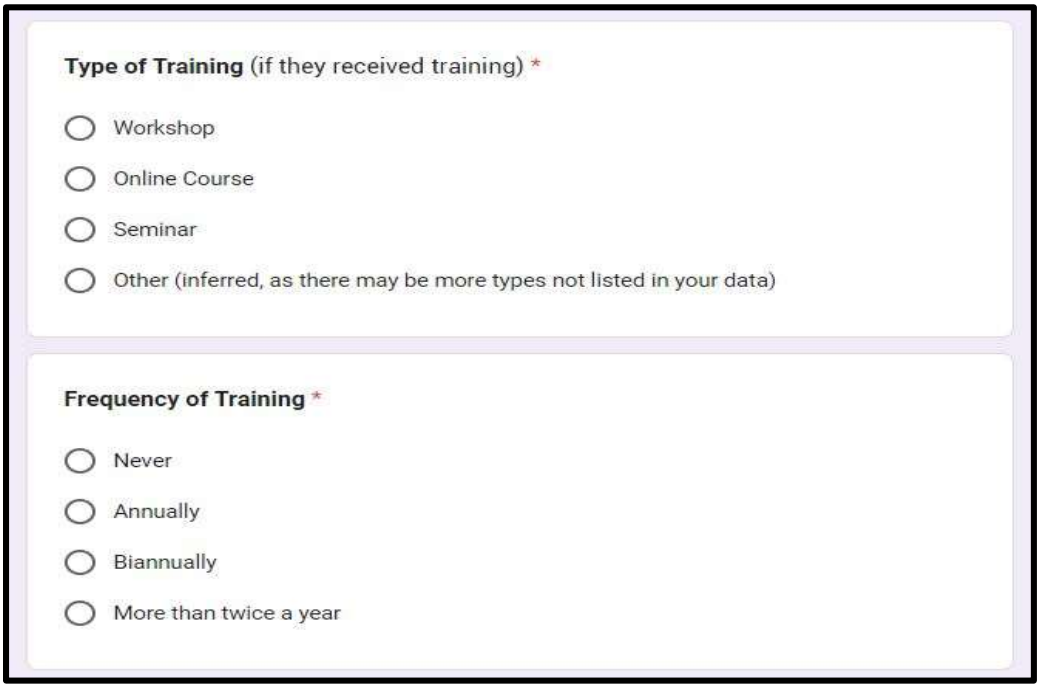

Figure 5: Type of Training and Frequency of Training

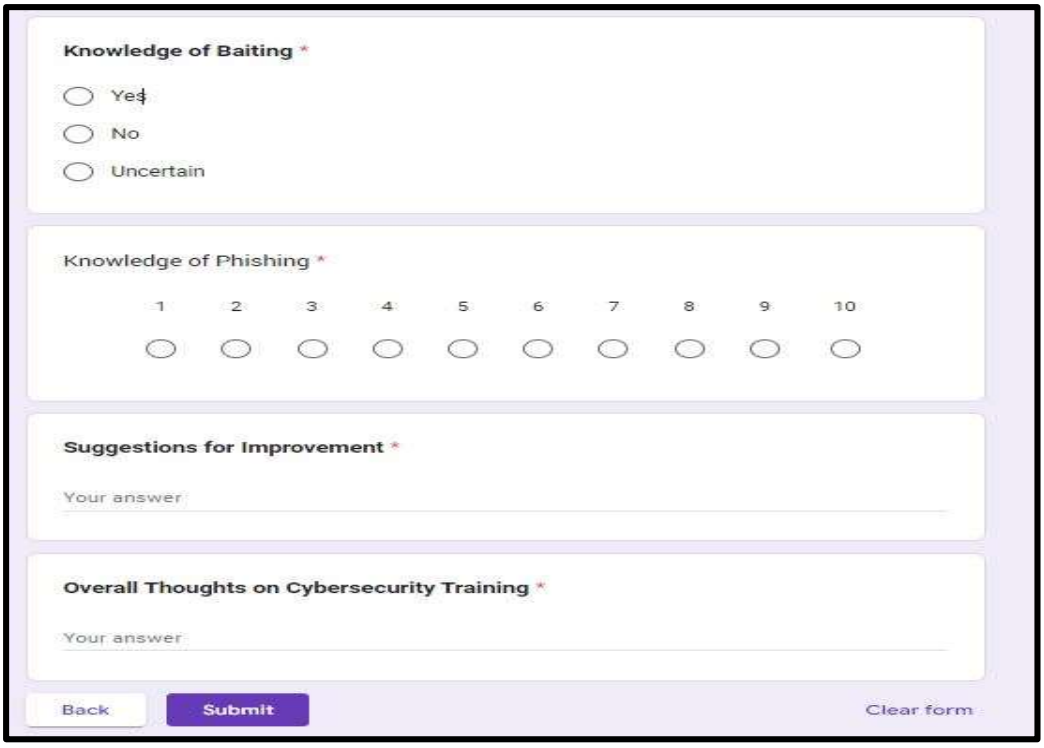

Figure 6: Knowledge of Baiting, Knowledge of Phishing, Suggestions for Improvement, and Overall Thoughts on Cybersecurity Training

These steps were meticulously followed to ensure the questionnaire was comprehensive, accessible, and capable of generating valuable insights for the study.

3 Simulated Social Engineering Attack Configuration

The simulated social engineering attacks were a central mechanism to evaluate the efficacy of the cybersecurity training program. The scenarios crafted, which included phishing, baiting, and pretexting, were chosen based on their prevalence in real-life cyber threats. Each scenario was carefully developed to mimic the tactics used by cyber attackers to exploit human vulnerabilities.

Selection of Participants:

- Six participants were selected, representing various organizational roles and experience levels, to ensure diversity in the study.
- The anonymity of participants was maintained to ensure unbiased responses.

Pre-Training Simulation:

- Participants were subjected to the initial simulations without prior warning to establish a baseline for their vulnerability to social engineering.
- The attacks, including deceptive emails and fake requests for information, were documented in detail for later analysis.

Training Intervention:

- An in-depth training program was then provided, covering both theoretical and practical aspects of cybersecurity.
- This was designed following industry best practices and tailored to the specific needs identified in the survey phase.

Post-Training Simulation:

- After the completion of the training, the same participants underwent a second round of simulations.
- These simulations were identical to the pre-training ones to measure the training's impact accurately.

Execution Steps:

- The simulations were conducted with the participants' actions, response times, and decision-making processes recorded.
- A post-simulation debriefing was held to discuss the participants' experiences and gather qualitative data on their perceived awareness and behaviours.

The aim was to provide a comparative analysis of participants' susceptibility to social engineering attacks before and after the training intervention. The qualitative and quantitative data gleaned from these simulations would then be critically analysed in Chapter Six, offering insights into the training's effectiveness and areas for further improvement. The hands-on approach in both the training and simulations ensured that participants not only understood the concepts but could also apply them in practical situations, aligning with the study's objective to enhance the human defence against social engineering threats.

4 Cybersecurity Training Program Setup

The cybersecurity training program was strategically crafted with the following objectives and methodologies:

Training Objectives and Curriculum:

- To provide participants with comprehensive knowledge on identifying and mitigating social engineering threats.
- Topics ranged from foundational cybersecurity concepts to advanced countermeasures against sophisticated social engineering attacks.

Instructional Methods and Materials:

- Interactive and practical exercises analysis were utilized to cater to various learning styles.

Training Environment Configuration:

- The setup of the training was designed to facilitate an interactive and hands-on learning experience.

Adaptation for Diverse Participant Backgrounds:

- The program was tailored to accommodate the varying levels of prior knowledge among participants.
- Personalized guidance was provided, ensuring that each participant could effectively understand and apply the cybersecurity principles.

Program Content:

- **Introduction to Social Engineering**: The program started by covering social engineering tactics like phishing, baiting, and pretexting, providing participants with insights into current trends and techniques employed by cybercriminals.
- **Real-world Case Studies**: For more context, the program included analysis of real-world social engineering incidents. This segment helped participants understand the complexities and nuances of these attacks.
- **Identification and Response Techniques**: The program aimed to teach participants to recognize and respond to social engineering, addressing areas like identifying suspicious emails, understanding baiting psychology, and handling pretexting.
- **Hands-On Simulations**: To reinforce learning, the training included interactive simulations where participants practiced identifying and responding to mock social engineering scenarios.

- **Best Practices in Cyber Hygiene**: The program also covered fundamental cybersecurity practices, emphasizing the importance of maintaining robust personal and organizational cyber hygiene.

This training program was integral in equipping employees with the skills to recognize and counteract social engineering tactics. By emphasizing behavioural change and the psychological aspects of these threats, the training went beyond technical knowledge to foster a culture of security awareness. The interactive format of the program ensured an engaging and effective learning experience that was adaptable to the needs of all participants.

5 Data Collection Mechanisms

For the systematic collection of research data, the study employed the following mechanisms:

Tools and Software for Data Collection:

- Google Forms was utilized to deploy surveys assessing cybersecurity awareness among staff.
- Microsoft Excel was used for organizing and initial processing of survey data and simulated attack outcomes.

Configuration Steps for Tools:

- Surveys in Google Forms were configured to ensure relevance and ease of use for participants.
- Excel sheets were prepared with specific formulas and macros to facilitate efficient data analysis.

The data collection was designed to be robust and efficient, with clear steps for configuration to ensure the integrity and security of the data. Online tools provided the flexibility and scale required for the study. These mechanisms underpinned the reliability of the subsequent data analysis, providing a solid foundation for evaluating the effectiveness of the cybersecurity training program

6 Data Analysis Procedures

This section outlines the steps and methodologies used for the data analysis phase of the study:

Quantitative Data Analysis Procedures:

- Manual analysis due to the project's scope, with Excel aiding in data organization and preliminary evaluation.
- Statistical assessments involved computing averages, medians, modes, and measures of variability to uncover patterns and correlations.

Qualitative Analysis Procedures:

- Thematic analysis followed a six-phase process: data familiarization, initial coding, theme identification, review, definition, and compilation.
- Narrative data from mock cyber-attacks enriched the study, revealing behavioural insights complementing the quantitative data.

Triangulation Techniques:

- Cross-referencing survey results with observed behaviours in simulations to validate findings.
- Employing mixed-methods to enhance the depth and credibility of the analysis, ensuring robust and comprehensive conclusions.

The procedures adhered to rigorous academic standards, combining diverse data sets to provide a well-rounded understanding of cybersecurity training effectiveness and behavioural responses to social engineering threats. This methodical approach facilitated a nuanced interpretation of the complex interplay between knowledge, attitude, and actions in the cybersecurity domain.

7 Results Compilation

The compilation of results was a meticulous process aimed at ensuring the accuracy and reliability of the study's findings:

- ***Data Consolidation***: All quantitative and qualitative data were consolidated into a single repository for ease of analysis. Quantitative data from surveys were tabulated, while qualitative observations from simulations were transcribed and organized thematically.
- ***Verification Procedures***: Each data point underwent verification to confirm its validity. This involved cross-checking entries against source materials and double-checking numerical data for entry errors.

- ***Analytical Review***: The statistical analysis was reviewed for consistency in application and appropriateness of methods used. Thematic analysis of qualitative data was cross-examined by multiple reviewers to reduce the likelihood of bias.
- ***Results Triangulation***: Findings from different data sources were compared and contrasted to identify patterns and discrepancies, enhancing the reliability of the conclusions drawn.
- ***Drafting Preliminary Reports***: Initial reports were drafted, summarizing the findings from each data set. These reports were used as a foundation for the comprehensive final report.
- ***Peer Review***: Preliminary results were subjected to peer review within the research team to challenge and validate the findings.
- ***Final Compilation***: After rigorous reviews and validation, the final results were compiled, ensuring that they were presented in a clear, concise, and accurate manner for reporting in the study.

APPENDIX I

SURVEY QUESTIONS

1. **AGE?** *
   - Below 20
   - 20-29
   - 30-39
   - 40-49
   - 50 and above

2. **What is your Gender***
   - Male
   - Female

3. **What is your Occupation***
   - Your answer

4. **How many Years of Experience do you have in your field***
   - Less than 1 year
   - 1-4 years
   - 5-9 years
   - 10 years or more

5. **When was the last time you Received Cybersecurity Training?** *

- Less than 1 year
- 1-4 years
- 5-9 years
- 10 years or more

6. **How was the Training delivered** (if they received training)
   *
   - Workshop
   - Online Course
   - Seminar
   - Other (inferred, as there may be more types not listed in your data)

7. **How Frequent was the Training**
   *
   - Never
   - Annually
   - Biannually
   - More than twice a year

8. **Do you have any Knowledge of Baiting***
   - Yes
   - No
   - Uncertain

9. **Rate your Knowledge of Phishing***
   - 1
   - 2
   - 3
   - 4
   - 5
   - 6
   - 7
   - 8
   - 9
   - 10

10. **What are your Suggestions for Improvement on Cybersecurity Training***
    - Options also seem to be open-ended, allowing for a range of opinions and feedback.

11. **What are your Overall Thoughts on Cybersecurity Training***

- Options also seem to be open-ended, allowing for a range of opinions and feedback.

Link:https://docs.google.com/forms/d/e/1FAIpQLSdnfhFP6HfcBaKQ2Egdpp4fEBCt1d3z3IznqM7vdNhxHh5Oyw/formResponse