National College of Ireland

Configuration Manual

MSc Research Project
MSc Cybersecurity

Shona Susan Shaji
Student ID: 23291257

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shona Susan Shaji		
Student ID:	23291257		
Programme:	MSc Cybersecurity	**Year:**	2024-2025
Module:	MSc Practicum		
Lecturer:	Mark Monaghan		
Submission Due Date:	15th September2025		
Project Title:	Mitigating Ai Driven Cyber Deception: Theoretical Modelling of Social Engineering Tactics and Human Vulnerability		
Word Count:	1000	**Page Count:**	

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: Shona Susan Shaji

Date: 15/09/2025

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

Shona Susan Shaji

Student ID: 23291257

Project Title: Mitigating AI-Driven Cyber Deception: Theoretical Modelling of Social Engineering Tactics and Human Vulnerability
Environment: Local Python environment (no server or XAMPP required)

1. System Requirements

Minimum Hardware

- RAM: 4 GB
- Disk Space: ~100 MB
- OS: Windows 10 or later (macOS/Linux also supported)

Software Requirements

- Python 3.10 or above
- pip (Python package manager)
- PowerShell or Terminal

2. Folder Structure

```
AI_Phishing_Simulator/
│
├── main.py                    → Main program file
├── messages.py                → Predefined phishing message database
├── scoring.py                 → Deception scoring using enhanced logic
│
├── theories.py                → Logic to map psychological theories
├── logger.py                  → Logs results into text and JSON
├── chart.py                   → Generates visual bar chart from results
│
├── output/                    → Output folder
│   ├── result.txt             → Human-readable logs
│   └── result. Json            → Data used for visualizations
│
└── README.md                  → Overview and instructions
```

3. Installation Steps

Step 1: Install Python

Download and install Python 3.10+ from:
https://www.python.org/downloads/

During install, tick the checkbox for "Add Python to PATH".

Step 2: Install Required Libraries

Open PowerShell or Terminal in the project folder, then run:

```
pip install matplotlib
```

That's all. No extra libraries are needed.

4. How to Run the Program

Option A: Using Predefined AI Phishing Messages
In the terminal, navigate to the project folder:

```
cd Desktop\AI_Phishing_Simulator
python main.py
```

You'll be prompted:

```
=== AI-Phishing Simulation ===
1. Run Predefined AI Phishing Messages
2. Analyse Your Own Suspicious Message
3.Exit
```

Type `1` and press Enter to run examples built into the tool.

Option B: Analyze Your Own Suspicious Message
Launch `main.py` the same way and choose `2`.
Paste any phishing-style message (email, SMS, etc.), and the tool will analyse:

- Detected psychological triggers
- Deception score (0–100)
- Activated Theories

The program will now continuously prompt the menu to choose from until you choose option 3 (Exit)

5. How to View the Chart (Optional)

Once some messages are analyzed, run this in terminal:

```
python chart.py
```

This displays a bar chart showing deception scores for each analyzed message.

6. Output Files

Located in the `output/` folder:

- `result.txt` → Human-readable analysis logs
- `result. Json` → Raw score + theory data for charts

7. Troubleshooting

Issue	Solution
Python not recognized	Ensure Python is added to system PATH
No chart displayed	Run `pip install matplotlib`
Empty result output	Ensure message input is not blank
Encoding error (rare)	Change terminal encoding: `chcp 65001` in PowerShell

8. Result Example

```
Paste the suspicious message here:
> We've detected unusual sign-in attempts on your profile. To protect your
data, confirm your identity now.

Custom Message:
We've detected unusual sign-in attempts on your profile. To protect your
data, confirm your identity now.
Psychological Triggers: authority, personalisation, phishing pattern
Deception Score: 70/100
 High deception risk. Likely to trigger fast emotional response (System 1
thinking).
 Activated Theories:
   - Affective Priming (strong emotional influence)
   - Trust Calibration (misplaced trust in appearance)
   - Actor-Network Theory (AI-human interaction)
   - Actor-Network Theory (AI-human interaction)
------------------------------------------------------------
1. Run Predefined AI Phishing Messages
2. Analyze Your Own Suspicious Message
3. Exit

Choose an option (1, 2, or 3 / q to quit): 3
Goodbye!
```

9. License & Acknowledgements

This is a student academic research prototype built using basic Python tools.
It does not collect or send data and is safe for educational purposes.