Cyber Garden v1.0

USER MANUAL

Social Engineering Defence Platform

Author: Chandu Dissanayake
8-9-2025

Table of Contents

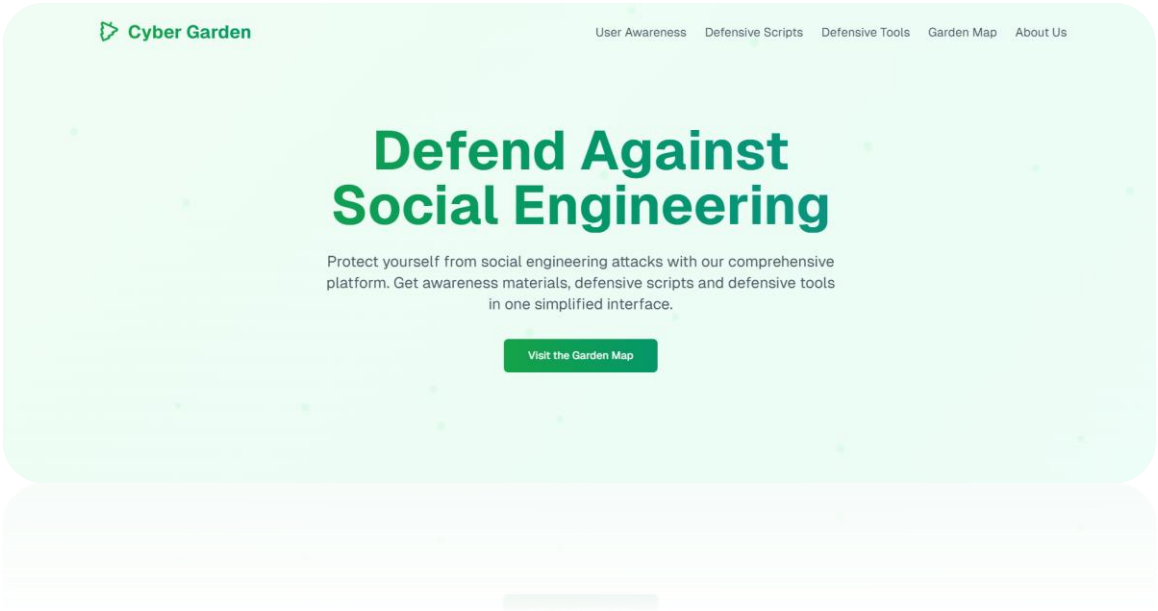
1. Introduction

Welcome to Cyber Garden, your comprehensive online platform designed to increase your awareness and defence against social engineering threats and cyberattacks. Cyber Garden provides educational sessions, defensive scripts, online analysis tools and interactive features to help you identify, analyze and mitigate common social engineering attacks effectively.

Purpose:

- Educate users on major social engineering threats.
- Provide easy-to-use defensive tools and scripts for personal or organizational cybersecurity.
- Enable safe and informed decision-making when encountering suspicious files, programs, or links.

This manual guides you step-by-step through using the Cyber Garden platform's key features so you can protect yourself confidently in today's digital environment.



2. User Awareness Section

The User Awareness section contains ten learning sessions designed to educate you on social engineering and its main threat categories. Each session explains the nature of the threat, its impacts and practical mitigation strategies. Below are the ten sessions.

1. Social Engineering (One foundational session explaining)
2. C2 Agents
3. Key Loggers
4. Bad USB Attacks
5. Macro Files
6. Phishing
7. Smishing
8. Vishing
9. Media Spying Agents
10. Location Spying Agents

Access and Navigation through User Awareness Sessions

Users are encouraged to view each awareness session sequentially as they are ordered on the platform. This ensures a progressive understanding of social engineering threats, from basic concepts to specific attack types.

Each session is designed to be concise and engaging, requiring no more than five minutes to complete. Users can read or watch the educational content provided within each session to gain a clear understanding of the threat it covers.

Within every session, key security tips and additional resources are available for further learning and practical guidance.

3. Defensive Scripts Section

To complement your awareness, Cyber Garden provides 10 defensive scripts to detect and respond to the threats described above.

Overview

Nine defensive scripts are released corresponding to defend against the nine social engineering threats. An additional Process Terminator script is provided for easy termination of suspicious processes.

You may download:

- The entire script bundle at once via the "Script Bundle" option. [Recommended]
- Individual scripts one by one to suit your needs.

Navigation through Defensive Scripts Web Interface

On the left menu, select either Script Bundle or any individual script.

When selected, the right pane loads detailed information:

- Script name and description
- Key features
- Download links
    - ✓ Windows Edition
    - ✓ Linux/MacOS Edition
- Video Tutorial Access

Click the appropriate link to download.

- ✓ Windows Users: Windows Edition
- ✓ Linux Users: Linux/MacOS Edition
- ✓ Mac Users: Linux/MacOS Edition

After clicking the download link, you will be redirected to the MediaFire file download page. To download the script, please click the download icon on the MediaFire page. Then Zip file will be downloaded. Extract it and script folder will be there. You can find script files and ReadMe manual inside the folder.

Installation and Running Scripts

- **Windows:** Within script folder run .bat files as administrator (right-click → Run as administrator).
- **Linux/MacOS:** Make .sh scripts executable (chmod +x scriptname.sh) and run with sudo ./scriptname.sh from the terminal.

4. Defensive Script Execution and Guidance

DISCLAIMER

It is strongly recommended that users complete all relevant User Awareness sessions on the Cyber Garden platform before running any defensive scripts. These sessions provide essential knowledge about social engineering threats and include detailed tutorials on how each script operates.

Having a solid understanding ensures users know what actions the tools perform, minimizing the risk of unintended consequences. Running scripts without proper knowledge can be harmful. For example, terminating critical system processes by mistake using the Process Terminator script may cause system instability or corruption.

Users must exercise caution, verify any suspicious findings carefully and only take action when confident of the legitimacy of the detected processes or files.

ReadMe Manual (Windows Edition)

1. Run the script by .bat file.
2. Run the .bat file as administrator to provide higher privileges.
3. If there is any suspicious program, review that well. If it is unknown, terminate it, else keep it after confirming the legitimacy.

    - Option 1: [Recommended]
        - ✓ Note down the PID value which is related to the suspicious process from the script output.
        - ✓ Run the process terminator script which is from the Cyber Garden.
        - ✓ Simply, type the noted PID and continue.
        - ✓ Process will be terminated.

    - Option 2:
        - ✓ Note down the process name.
        - ✓ Then search task manager on your windows search bar.
        - ✓ Open the task manager.
        - ✓ Explore processes.
        - ✓ Find exact same process name that you marked as suspicious.
        - ✓ Right click on the process and end the task.
        - ✓ Process will be terminated.
4. If there is any malicious program, otherwise if it is well known or 100% verified, nothing to review, terminate it. [Follow the same instructions above to terminate.]

5. If there is any suspicious document, review that well. If it is unknown, delete it, else keep it after confirming the legitimacy.
    - ✓ Scan results of the relevant scripts will include file locations of suspicious or malicious files.
6. If there is any malicious document, otherwise if it is well known or 100% verified, nothing to review, delete it.
7. For the Bad USB detector, Run the script first and then plug in suspicious USB storage device.
8. Before run the Macro File Detector, make sure you have proper internet connection.
9. For the phishing analyzer, put your email file that means .eml into the Phishing Analyzer folder.
    - ✓ Download email from the mail application.
    - ✓ Put the .eml file into the Phishing Analyzer folder.
    - ✓ Run the script.
10. For the smishing analyzer put your suspicious message into message.txt inside the smishing analyzer folder.
11. For the vishing analyzer, provide accurate details and review the suspicious score and mitigation methods.
12. Find more information from the user manual on Cyber Garden official website.
13. Find user awareness sessions and video tutorials for the defensive scripts on Cyber Garden official website.
14. Stay tune with Cyber Garden.

ReadMe Manual (Linux/MacOS Edition)

1. Make the script executable using the following command:
    - ✓ chmod +x scriptname.sh
2. Run the script using sudo to provide elevated privileges:
    - ✓ sudo ./scriptname.sh
3. If there is any suspicious program, review it carefully. If it is unknown, terminate it. Otherwise, keep it after confirming the legitimacy.

    - Option 1: [Recommended]
        - ✓ Note down the PID value which is related to the suspicious process from the script output.
        - ✓ Run the process terminator script which is from the Cyber Garden.
        - ✓ Simply, type the noted PID and continue.
        - ✓ Process will be terminated.

    - Option 2:
        - ✓ Note down the process name.
        - ✓ Open the terminal and run: ps aux | grep processname
        - ✓ Identify the correct process and run: sudo kill -9 PID
        - ✓ Process will be terminated.

4. If there is any malicious program, or if it is well known or confirmed as harmful, terminate it immediately. [Follow the same instructions above to terminate.]
5. If there is any suspicious document, review it carefully. If it is unknown, delete it. Otherwise, keep it after confirming the legitimacy.
    - ✓ Scan results of the relevant scripts will include file paths of suspicious or malicious files.
6. If there is any malicious document, or if it is verified as dangerous, delete it immediately.
7. For the Bad USB detector, run the script first and then plug in the suspicious USB storage device.
8. Before running the Macro File Detector, make sure you have a proper internet connection.
9. For the phishing analyzer, place your email file (.eml) into the Phishing Analyzer folder.
    - ✓ Download the email from your mail client.
    - ✓ Place the .eml file inside the Phishing Analyzer folder.
    - ✓ Run the script.
10. For the smishing analyzer, put your suspicious message into a file named message.txt inside the Smishing Analyzer folder.
11. For the vishing analyzer, provide accurate call details and review the suspicious score and mitigation methods shown by the script.

12. Find more information in the user manual available on the official Cyber Garden website.
13. Visit the Cyber Garden website for user awareness sessions and video tutorials for the defensive scripts.
14. Stay tuned with Cyber Garden.

5. Defensive Tools Section

Cyber Garden offers three online defensive tools to analyze suspicious URLs and links, which are common in social engineering attacks.

Tools Overview

- **Suspicious Link Detector:** Analyzes URL patterns and assigns a suspicious score. A score above 40% indicates a significant risk, avoid visiting.
- **Suspicious Zone Detector:** Visits the URL to detect cookie hijacking, hidden forms and checks for security headers. Providing a suspicious score above 40% is dangerous.
- **Suspicious Endpoint Detector:** Checks if the link is a file download and rates the risk of malicious downloads. Suspicious score above 40% means avoid visiting.

Access and Navigation through User Awareness Sessions

- Enter the suspicious link in the input box for each tool.
- If you have a suspicious link, first enter it into the Suspicious Link Detector and note the suspicious score.
- Next, enter the same link into the Suspicious Zone Detector and record its suspicious score.
- Then, input the link into the Suspicious Endpoint Detector and note the score.
- If the suspicious scores from these tools are below 40%, the site is generally considered safe to visit.
- Even if the scores are lower or borderline, avoid entering any personal or sensitive information on the site.
- If the site appears to be a well-known login page, do not enter credentials directly. Instead, search for the official login page through a trusted search engine like Google to avoid cloned or phishing pages designed to steal your information.

6. Garden Map and Chatbot

The Garden Map is an interactive visualization of social engineering concepts, representing threats as components of a garden to simplify understanding.

Use the Garden Wizard chatbot for any clarifications or to ask questions about social engineering and defence methods.

The chatbot can guide you through unclear points and help you navigate the platform.

7. Summary of Use Flow

Learn: Start with User Awareness sessions to understand threats.

Analyze: Use Defensive Tools to check suspicious links encountered in emails, messages, or websites.

Detect: Download and run Defensive Scripts corresponding to threats you want to scan for on your system.

Respond: If malicious or suspicious programs/files are found, use the Process Terminator script or manual methods to terminate or delete them.

Explore: Use Garden Map and Chatbot for further learning and support.

8. Support and Updates

Visit the Cyber Garden official website regularly for updated sessions, tools, scripts and tutorials.

Video tutorials accompany each defensive script to guide you through setup and usage.

Contact support via the website for technical help or feedback.

Stay tuned for future enhancements and new threat coverage.

Thank you for using Cyber Garden. Stay safe, aware and secure.

[END]