

Cybersecurity Suite – User Manual

1. Purpose of the Application

The Cybersecurity Suite integrates multiple tools, including a Password Strength Checker and a Malicious Email Scanner, into a single user-friendly interface. This manual guides users through the main window layout, usage, and troubleshooting.

2. Main Window Overview

When you run the toolkit, the main window appears. At the center of the window are four buttons:

- Password Checker
- Malicious Email Identifier
- Keylogger And Phishing Page Demo
- File Integrity Checker

Above the buttons, a label titled 'Select Tool' is prominently displayed.

3. Step-by-Step Usage Instructions

3.1 Using Password Checker

1. On the main window, click 'Password Checker'.
2. The password checker interface will load in the same window.
3. Enter your password into the input field.
4. Click 'Check Strength'.
5. A popup will display the password strength and recommendations.
6. Click the '← Back' button to return to the main menu.

3.2 Using Malicious Email Scanner

1. On the main window, click 'Malicious Email Scanner'.
2. The scanner interface will load in the same window.
3. Click 'Select Folder to Scan (.eml)'.
4. Choose a folder that contains .eml files. It will scan all mails inside folder.
5. The tool will display the analysis results in a scrollable text box.
6. Click the '← Back' button to return to the main menu.

3.3 Using File Integrity Checker

1. On the main window, click 'File Integrity Checker'.
2. The scanner interface will load in the same window.
3. Click 'Add Folder' to traverse through the folder which is been integrity checked.
4. Click 'Remove Selected' or 'clear all' to remove added folder/s.

5. Click 'Create Snapshot' to save baseline.
6. Click 'Verify integrity' to check integrity
7. Click the '← Back' button to return to the main menu.

3.4 Using Keylogger and Phishing Demo

1. On the main window, click 'Keylogger and Phishing Demo'.
2. The scanner interface will load in the same window.
3. Click on 'Start Demo' to get started.
4. Key logs will be saved in Logged file.
5. Click on Logged file to see the save logs.
6. Press key 'esc' to stop the keylogger.
7. Click the '← Back' button to return to the main menu.

4. Example Workflow

Imagine a user receives a suspicious email. They:

1. Launch the Cybersecurity Toolkit.
2. Click 'Malicious Email Scanner'.
3. Select a folder containing the .eml file.
4. Review the warnings about phishing content or attachments.
5. Return to the main window and choose 'Password Checker' to evaluate the strength of their email password.

5. Troubleshooting Tips

Issue	Solution
Error: Module not found	Verify that the module file names match (e.g., 'password_guiintegrated.py').
Buttons don't appear	Ensure all required .py files are in the same directory.
common_password.txt not found	Place the file in the same directory as the Python scripts.
.eml files not detected	Check file extensions and ensure the folder has valid .eml emails.
Back button not working	Make sure the `back_callback` is passed correctly in tool code.

6. Project Directory Structure

```
cybersecurity_suite/  
├── integrated_button_gui.py  
├── password_guiintegrated.py  
├── malicious_guiintegrated.py  
├── keylogger.py  
├── integritychecker_guiintegrated.py  
├── ph.html, style.css  
├── common_password.txt  
└── User_Manual.docx
```

7. Launching the Application

Open a terminal and run:

```
python gui.py
```