Information Security

AIR UNIVERSITY

PROJECT PROPOSAL

GORUP MEMBERS:

MUHAMMAD BILAL - 241914

USAIDULLAH REHAN - 241815

AYAN HAMDANI - 241872

SYED SHADAN - 241911

isItSAFE

Anti-Deception Security Suite

Gorup Members

- Muhammad Bilal - **241914**
- Usaidullah Rehan - **241815**
- M. Ayan Hamdani - **241872**
- Syed Shadan Raza - **241911**

Project Overview

isItSAFE Toolkit is an integrated security application that focuses on identifying digital deception and protecting user privacy. The system consists of three independent yet complementary security modules:

- Fake Wi-Fi Access Point Detector
- Phishing / Fake Email Detector
- Image EXIF Metadata Cleaner

Objectives

- Our first module (**Fake Wi-fi AP Detector**) deals with mainly duplicate Wi-fi access points with similar names to the original Access point which then leads to **Evil Twin Attack**.
- The second module (**Fake Email Detector**) deals with most common type of cyber attack called **Phishing** which is old but still is mostly the trick used for attacking a firm.
- Third module (**Image EXIF Cleaner**) deals with most ignored security threat because most of the people while ignore this metadata attached to their shared images but this could be very important for a **Social Engineering Attack**

So, in total **isItSAFE** is about building a digital security bodyguard for people, not just networks. We are tackling the three sneakiest ways hackers trick users: by stopping them from falling for fake Wi-Fi hotspots and by automatically cleaning hidden details like location data from shared photos, cutting off the information hackers use to launch targeted attacks.

Our goal is to make people significantly harder targets by protecting them where they are most vulnerable: *in their decisions about who and what to trust online.*

Scope

In-Scope:

- Scanning and identifying suspicious Wi-Fi networks
- Phishing detection through text, sender info, and URL analysis
- Reading and removing EXIF metadata from image files
- Local execution on a user's computer

Out-of-Scope:

- Deep packet inspection or Wi-Fi packet capturing
- Email client integration (Gmail/Outlook API)
- Advanced AI-based phishing detection models
- Enterprise-level security features
- Advanced digital forensics

Tools & Technologies

Programming Language: **Python**

Libraries / Tools:

- **scapy** → Wi-Fi scanning
- **tkinter** → GUI development (**Optional**)
- **re, urllib, urlparse** → phishing detection
- **PIL (Pillow) / ExifTool** → metadata extraction & cleaning
- **Hashlib** → optional hashing
- **Wireshark** (optional for testing Wi-Fi scenarios)

Operating Systems: **Windows / Linux**

Methodology

- Phase 1: **Research** study fake Wi-Fi patterns, phishing indicators, and EXIF privacy issues.
- Phase 2: **Design** implementation plan like structure/intro on console.
- Phase 3: **Development** implement the three modules using Python scripts and libraries.
- Phase 4: **Testing** test Wi-Fi detection, phishing analysis, and EXIF cleaning on sample data.
- Phase 5: **Documentation & Presentation** prepare final report, screenshots, and PPT.

Deliverables

- Final Report
- Source Code
- Presentation Slides
- Demo Video (Optional)
- GUI Application (Optional)

Expected Outcomes

- ✓ Secure detection of fake Wi-Fi hotspots.
- ✓ Identification of phishing attempts.
- ✓ Safe sharing of images without metadata.
- ✓ User-friendly security toolkit.

References

- ✓ OWASP
- ✓ IEEE papers on phishing
- ✓ Scapy documentation
- ✓ Python Pillow documentation