Name:
Nikhil Kumar

Reg. No:
22BCY10158

Department:
SCAI

Course:
Computer Science and Engineering

Project Title

Phishing Simulation: How Hackers Steal Passwords and How to Stay Safe

---

Problem Statement / Use Case

Many people fall for fake emails or websites that look real. These tricks are called *phishing*, and they're a common way hackers steal usernames, passwords, or other personal information. Even trained employees can sometimes be fooled. This project will show how a phishing attack works by creating a fake login page that looks real. It will also teach how to spot these fake pages so that people don't fall for them in real life.

Project Objective(s)

- Show how easy it is to make a fake login page that looks like a real website.
- Demonstrate how hackers can collect usernames and passwords from people who are tricked.
- Teach people how to recognize phishing attacks by pointing out clues.
- Help improve cybersecurity habits through a simple and clear demo.

Tools and Technologies

Main Tools:

- **Kali Linux** – A special operating system used by security professionals.
- **Social Engineering Toolkit (SET)** – A tool that helps create fake websites for testing and learning purposes.

Other Tools (Optional):

- **Apache Server** – Used to host the fake website on the local network.
- **Wireshark** – Can be used to watch what data is sent over the network.
- **Python** – Can be used to write small scripts that save the collected usernames and passwords.

Methodology / Approach

1. **Install Kali Linux**: Use Kali Linux on a virtual machine or physical system.
2. **Launch SET Toolkit**: Open the Social Engineering Toolkit from Kali.
3. **Choose Website Cloner Option**: Select the option that copies a real website's login page (like Gmail or Facebook).
4. **Host the Fake Page**: Run a web server so that the fake page can be accessed on the network.
5. **Simulate Victim Login**: Ask someone to test the page by entering a fake username and password.
6. **Capture Credentials**: When the user submits the form, their details are stored by SET.
7. **Analyze the Data**: Show where the captured information is stored and explain how hackers use it.
8. **Raise Awareness**: Explain how to avoid these attacks—look at the website address, don't trust suspicious emails, and always check for HTTPS.

Innovation & Uniqueness

This project is special because it doesn’t just talk about phishing—it shows it in action. Many people don’t understand how easy it is to be tricked until they see it happen. This hands-on simulation helps people remember what to look out for. It’s an engaging and realistic way to teach a very important topic.

Relevance to Cybersecurity Field

- Helps understand how social engineering and phishing work in real life.
- Builds skills in ethical hacking, awareness training, and cyber defense.
- Shows why human behavior is important in cybersecurity.
- Matches topics taught in ethical hacking courses like CEH (Certified Ethical Hacker).

Expected Deliverables

- A working phishing page created using SET.
- A video or screenshots of the phishing attack in action.
- Logs showing where the captured credentials are saved.
- A simple training guide or presentation to explain phishing to others.
- A final report explaining how the attack was done, what was learned, and how to stay safe from it.