Cybersecurity Awareness Project: Phishing Simulation Bot

Objective

The purpose of this project is to simulate how phishing pages can collect personal information using modern web tools and bots. This project:

- Demonstrates a typical phishing attack pattern
- Gathers user device/browser information ethically
- Requests consent-based access to geolocation and webcam (simulated)
- Sends the collected data to a Telegram bot for demonstration

How It Works

- A user visits a fake "Secure Access" webpage
- The page collects:
  - Browser user agent
  - OS/platform
  - Language and timestamp
- With user consent, it also accesses:
  - Geolocation (via browser)
  - Webcam prompt (simulated)
- A Telegram bot receives this data instantly via API

Technologies Used

- Frontend: HTML, JavaScript
- Bot Integration: Telegram Bot API
- Hosting: GitHub Pages
- Optional Tools: Glitch, Netlify

Cybersecurity Awareness Project: Phishing Simulation Bot

Ethical Considerations

- All data collection is transparent and consent-based
- No personal data is stored or reused
- Webcam and geolocation features require explicit permission
- This simulation is built for educational purposes only

Learnings

- Understanding phishing tactics and how they exploit user trust
- Working with APIs and browser permissions
- How automation tools (bots) can be used ethically for awareness
- Hosting secure demo pages with GitHub Pages

Resources

- GitHub Repo: [your GitHub link]
- Live Demo: [your GitHub Pages link]