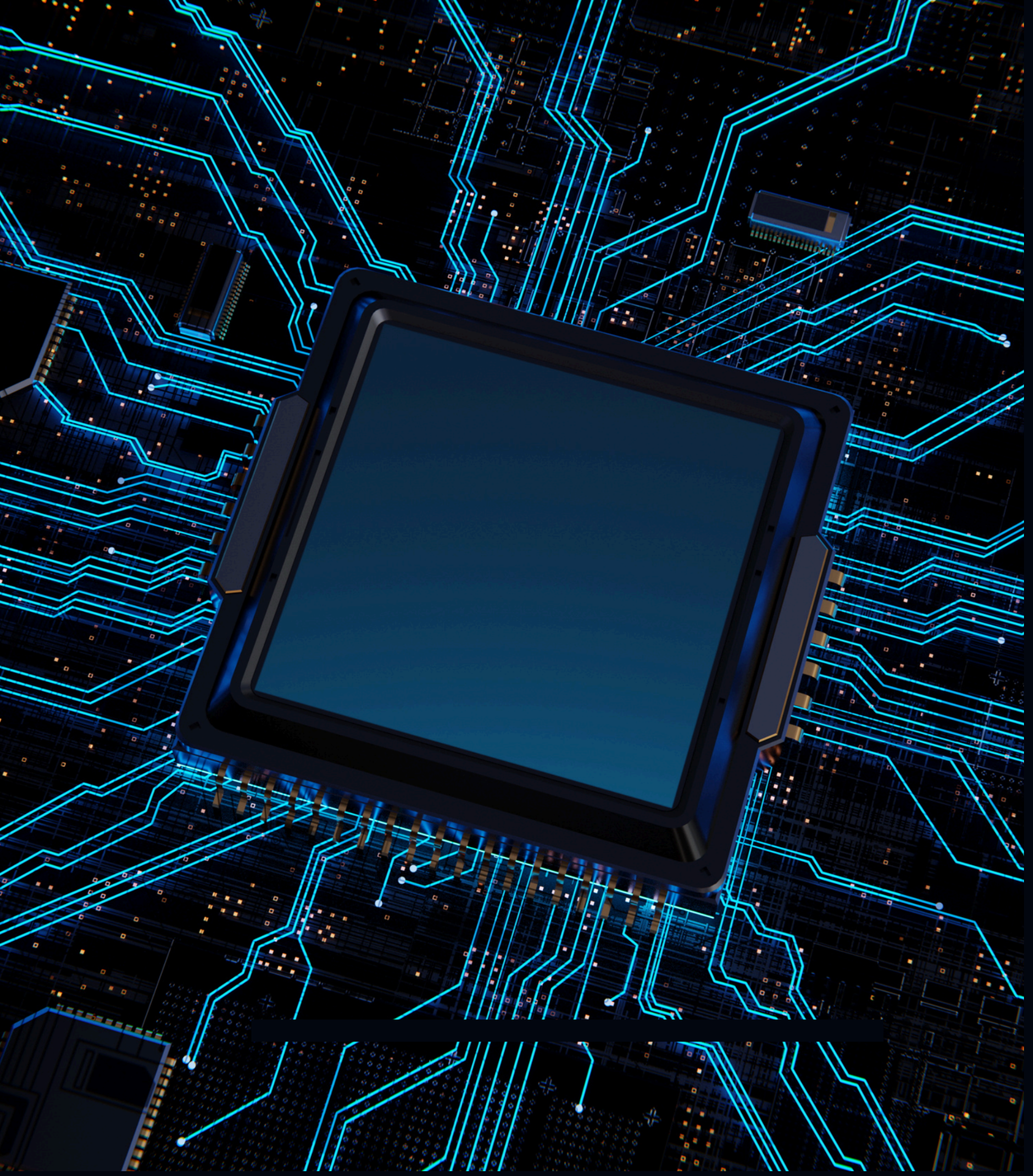
धर्मो रक्षति रक्षितः

Shielding Against Cyber Threats



PROJECT OVERVIEW

धर्मो रक्षति रक्षितः is an all-in-one cybersecurity toolkit designed to protect, analyze, and test the digital environment. It integrates essential tools including a keylogger, steganography, a password manager and generator, and a malware detection module. This suite is aimed at ethical hacking, digital forensics, and secure data management. Built using Python and modular design, it allows both beginners and professionals to explore multiple layers of cybersecurity in one environment.

CORE MODULES

Designed to teach, secure, and simulate real-world cyber environments.

EACH TOOL, ONE MISSION: TOTAL CONTROL OVER DIGITAL THREATS.

Keylogger

Captures keystrokes for monitoring and forensic investigation in a legal/controlled environment.

Steganography Tool

Conceals messages or files inside images to enable hidden communication.

Password Manager & Generator

Securely stores and creates strong, encrypted passwords for user safety.

Malware Detector

Scans for suspicious code signatures and known malware behaviors in files.

KEYLOGGER MODULE

Every keystroke tells a story — we just listen to it.

A Keylogger is a monitoring tool that records every keystroke made on a system's keyboard. It helps in activity analysis, security auditing, and user behavior tracking in a controlled or ethical hacking environment.

Why It's Used (Real-life Use Cases)

- Forensics: Used by cybersecurity professionals to analyze digital evidence during investigations.
- Parental Control / Internal Monitoring: Employers or parents may monitor systems to ensure safe and legal use.
- Ethical Hacking Labs: Security researchers test system vulnerabilities and data leakage points.
- It can violate privacy if misused or installed without consent.

Did you know?

A silent keylogger can record everything you type — without you ever noticing.

Tailored Solutions

A custom keystroke tracker for specific monitoring needs.

Proactive Monitoring

Stay ahead of threats — don't wait for them to strike.

STEGANOGRAPHY

Because the best secrets are the ones you never see.

Steganography is the art of hiding information in plain sight — like embedding secret messages inside images. This module allows users to conceal text data within image files, making it invisible to the naked eye but retrievable with the right key.
Unlike encryption, which scrambles the content, steganography hides its very existence, making it ideal for covert communication, secure data transfers, or digital forensics.

Why It's Used (Real-life Use Cases)

- Intelligence & Espionage: Agents may hide mission-critical data in seemingly normal files.
- Digital Forensics: Investigators may embed notes or case details inside media files during analysis.
- Private Communication: Journalists or whistleblowers use it to bypass surveillance and censorship.

Did you know?

A normal image even voice can secretly carry hidden messages using steganography.

Tailored Solutions

Not just hidden — customized, protected, and precise.

Proactive Monitoring

Stealth isn’t enough — awareness is the second layer of defense.

MALWARE DETECTOR

Spot the threat before it spreads.

Malware detection is the core defense mechanism of SHIELD — scanning, analyzing, and identifying malicious files or suspicious behavior in real-time. This module is designed to catch threats before they can execute, using signature checks, file behavior analysis, and extension monitoring.
Whether it's a virus, trojan, or a disguised payload, this tool inspects the system like a digital bloodhound.

Why It's Used (Real-life Use Cases)

- Corporate Security: Detects malicious attachments or scripts inside enterprise files.
- Pen-testing Labs: Helps ethical hackers identify potentially harmful files during vulnerability testing.
- Forensics & Law Enforcement: Used to examine seized digital evidence for embedded threats.

Did you know?

Over 300,000 new malware programs are created every day.

Tailored Solutions

Not every threat looks the same — not every solution should either.

Proactive Monitoring

Because real threats don’t wait — and neither do we.

PASSWORD MANAGER & GENERATOR

Secure, generate, and defend — all in one vault.

These module is a dual-purpose tool designed to both securely manage your passwords and detect weak or reused credentials. It stores login information in encrypted form, auto-generates strong passwords. Built for both convenience and safety, it minimizes the human risk in cybersecurity — no more using “123456” or writing passwords on sticky notes.

Why It's Used (Real-life Use Cases)

- Students & Individuals: Secure all account credentials with one master key.
- Offices & Teams: Generate and share encrypted passwords securely.
- Security Audits: Detect reused or weak passwords during internal reviews.

Did you know?

Most data breaches happen due to weak passwords.

Tailored Solutions

One vault — many ways to protect what matters.

Proactive Monitoring

Security that doesn’t sleep — always watching, always protecting.

THE CYBER AWARENESS CHALLENGE

The Cybersecurity Quiz module is designed to engage users, test their knowledge, and promote awareness of digital threats. With a mix of beginner to advanced questions, this interactive tool sharpens your understanding of real-world cyber attacks, safety practices, and digital hygiene.

Whether you're a student, enthusiast, or aspiring ethical hacker — it’s time to see how secure your mind really is.

Every right answer builds your firewall — one question at a time.

SECURITY AUTHENTICATION

- Safe & Encrypted Environment
- No Data Storage
- Educational & Ethical Use Only
- Secure Login System will be added soon
- Awareness-Focused Design
- No Hidden Trackers and malicious free

Built with security, transparency, and user privacy at its core — empowering users without compromising safety.

UNDER THE HOOD

-TECHSTACK USED

HTML

Structure of the web pages.

≈ 34.27%

CSS

Styling and layout and responsiveness.

≈ 27.02%

PYTHON

Core logic for tools like keylogger, steganography, malware detection, and password management.

≈ 23.78%

JAVASCRIPT

Interactivity and dynamic behavior.

≈ 14.94%

MODERN INFORMATION

PROTECT FROM HACKERS

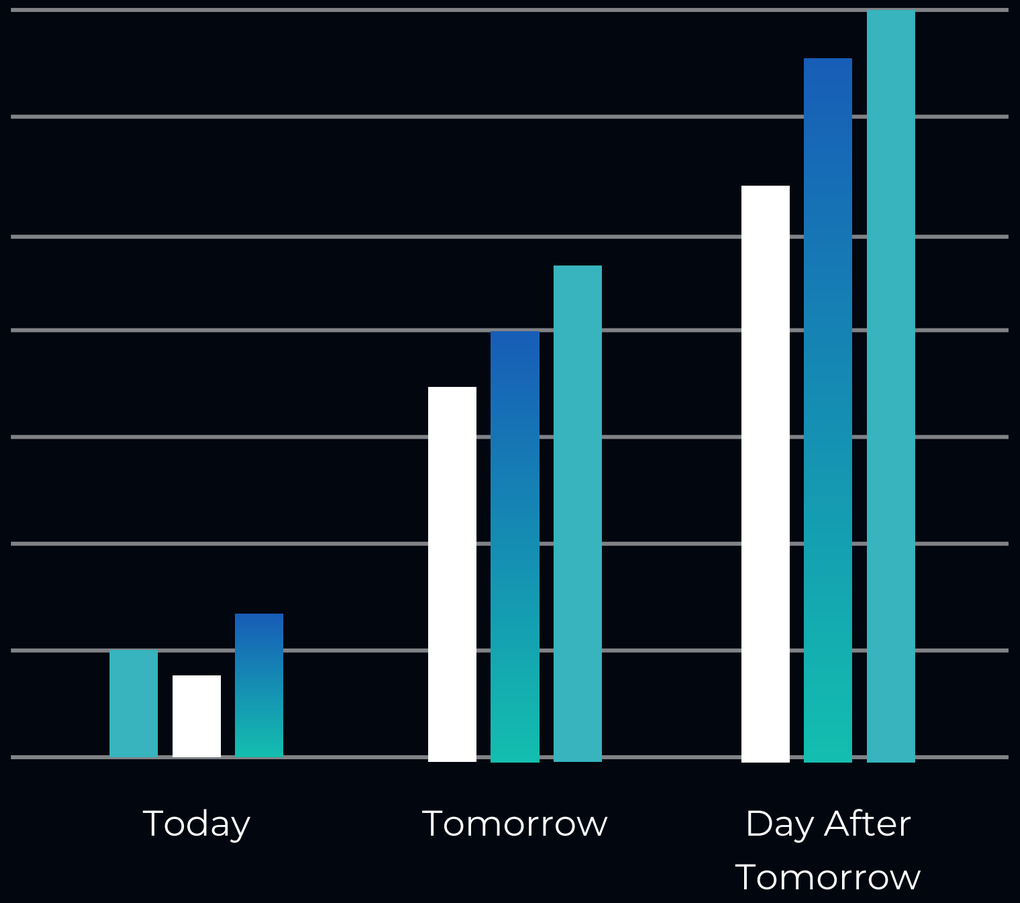
- Disable Auto-Download in Messaging Apps
- Avoid Clicking Suspicious Links
- Enable Two-Factor Authentication (2FA)
- Avoid Public Wi-Fi for Sensitive Transactions
- Never Install Unknown APKs or Software
- Check App Permissions

OUTCOME

Cyber Threat Awareness

Learning Through Interaction

Motivation to Practice Safe Digital Habits



WHERE WE ARE HEADED NEXT

Innovation doesn't stop here.

Integration of AI-Powered Threat Detection.

Expanding boundaries, enhancing security.

Multi-Factor Authentication (MFA).

From private roots to public power.

Open Source : Currently private, but planning to go public for community contributions.

From Project to Product

One idea. One vision. Global impact.

OUR AMAZING TEAM

Anshika
JavaScript & Support Developer

Ayush Rathore
Lead developer & Cybersecurity Enthusiasts

Devansh Gupta
Web Designer & Cyber Ethusiasts

Anurag Singh
Currently not joined

THANKS FOR JOINING THE CYBER MISSION

We appreciate your time and attention.
This project is not just a toolkit — it's a mission to raise awareness, strengthen defenses, and build a safer digital world.

Together, we can turn ideas into innovations and challenges into change.