

Background

The **National Cyber Crime Reporting Portal** is a platform through which the citizens of India can report a cyber crime committed against them online.

This portal was launched on **30th August, 2019** by the Ministry of Home Affairs.

The Portal was launched along with the inauguration of the **Indian Cyber Crime Coordination Centre (I4C)** in New Delhi. The entire idea and scheme of launching and curbing the cyber crimes in India was divided into seven different parts.





HELPLINE NUMBER

1930

If you are a victim of Financial Cyber Fraud Dial Helpline Number 1930

Categories Of Cyber Crimes

- 1. Against People** - Includes Cyber Harassment And Stalking, Distribution Of Child Pornography, Credit Card Fraud, Human Trafficking, Spoofing, Identity Theft, Online Slander (False Statement About Someone).
- 2. Against Property** - Includes DDOS (Denial Of Service) Attacks, Hacking, Virus Transmission, Type Squatting, Computer Vandalism (Damage In Digital Form), Copyright Infringement, And IPR Violations.
- 3. Crimes Against Government** - Include Nation's Sovereignty (Power) And May Include Hacking, Accessing Confidential Information, Cyber Warfare, Cyber Terrorism, And Pirated Software.

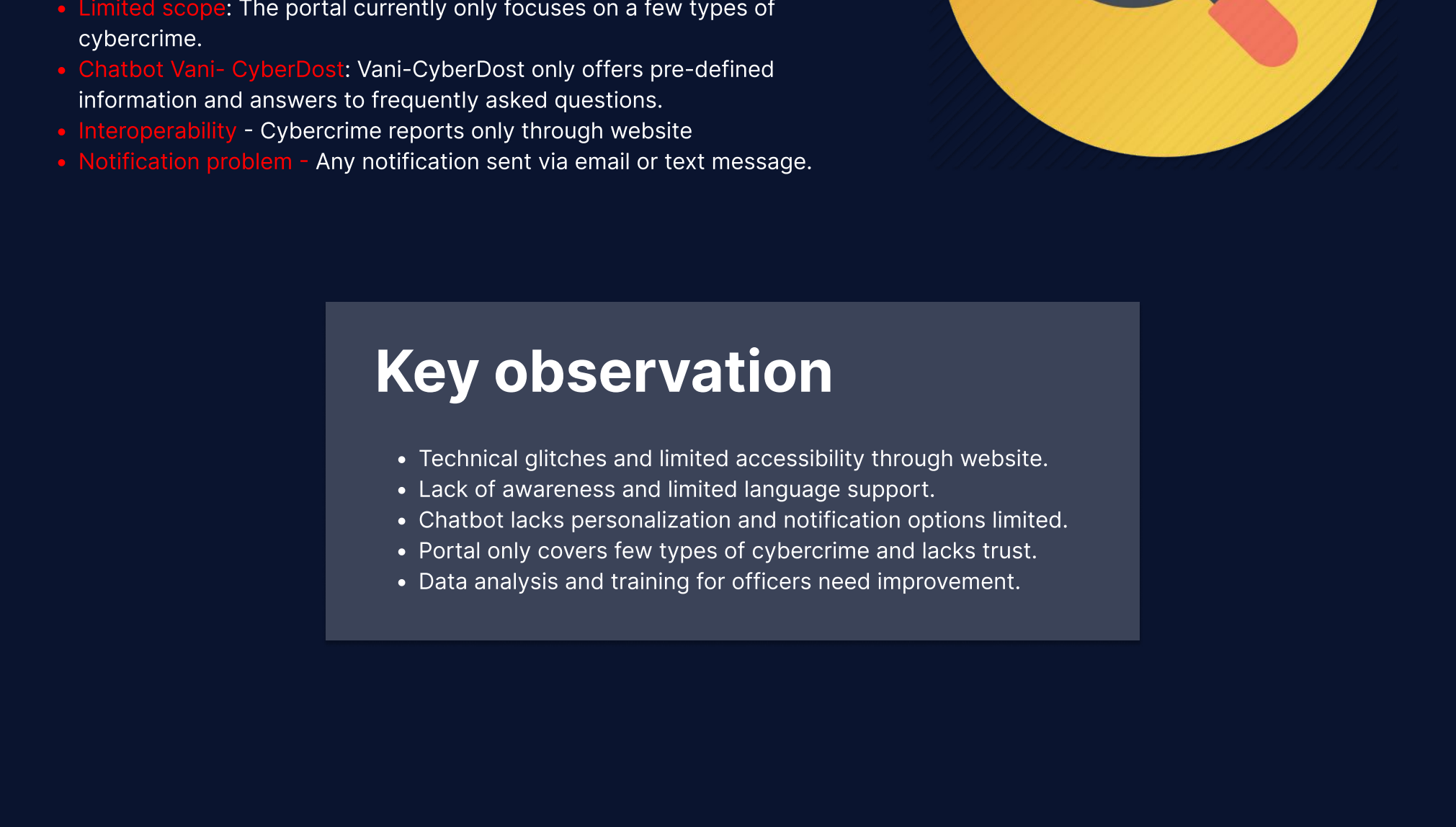
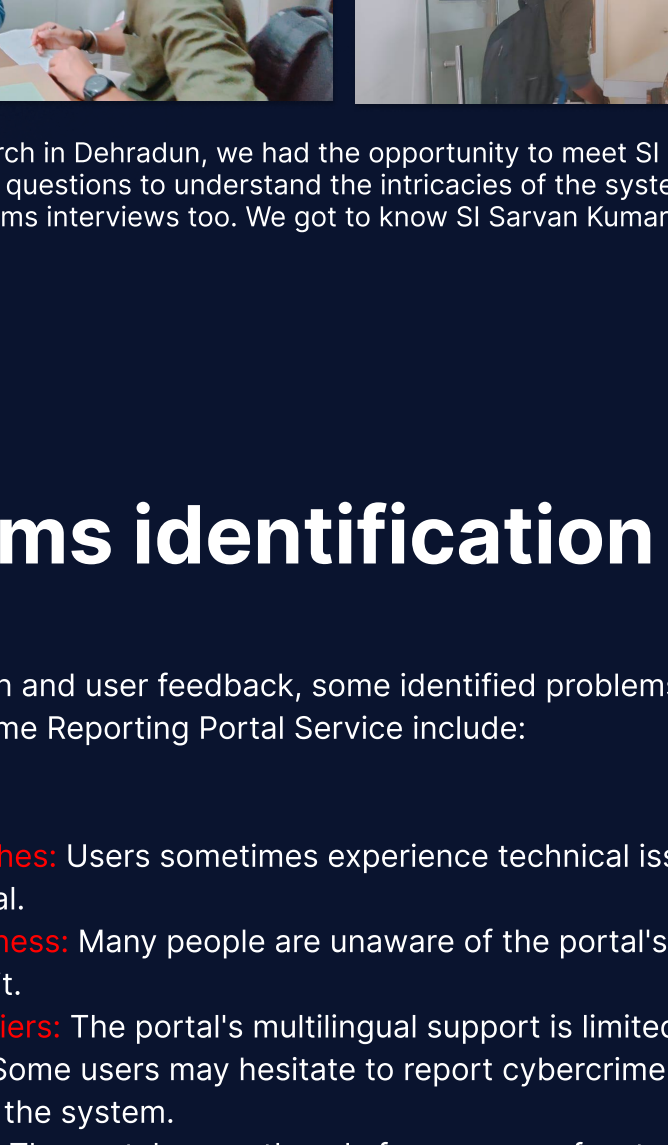


Types Of Crime Against People



System Visualization

How it works?



Service Blueprint



Field Research

December 2023

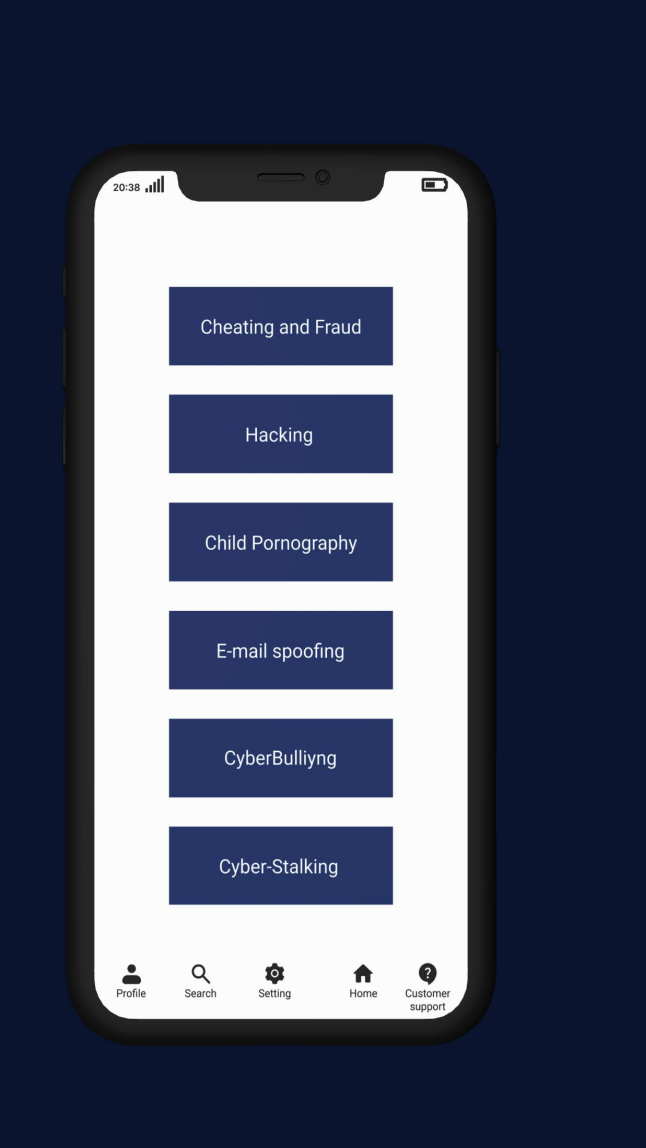


During our field research in Dehradun, we had the opportunity to meet SI Sarvan Kumar, an expert in cybercrime. We gained valuable insights from him, asking numerous questions to understand the intricacies of the system, including inquiries about blueprint, ecosystem and other relevant aspects. We took victims interviews too. We got to know SI Sarvan Kumar journey, which has inspired us in many ways.

Problems identification

Based on research and user feedback, some identified problems with the current Cyber Crime Reporting Portal Service include:

- Technical glitches:** Users sometimes experience technical issues while using the portal.
- Lack of awareness:** Many people are unaware of the portal's existence or how to use it.
- Language barriers:** The portal's multilingual support is limited.
- Lack of trust:** Some users may hesitate to report cybercrime due to lack of trust in the system.
- Limited scopes:** The portal currently only focuses on a few types of cybercrime.
- Chatbot Vani- CyberDost:** Vani-CyberDost only offers pre-defined information and answers to frequently asked questions.
- Interoperability** - Cybercrime reports only through website
- Notification problem** - Any notification sent via email or text message.



Key observation

- Technical glitches and limited accessibility through website.
- Lack of awareness and limited language support.
- Chatbot lacks personalization and notification options limited.
- Portal only covers few types of cybercrime and lacks trust.
- Data analysis and training for officers need improvement.

Modification



Benefits

- Enhanced Cultural Sensitivity
- Increased Public Awareness
- Improved Trust and Confidence

- For Victim**
- Reduced Stress and Anxiety
 - Improved Accessibility
 - Tailored Support
 - Clearer Communication
 - Enhanced Trust
- For Law Enforcement**
- More Efficient Case Management
 - Reduced Caseload
 - Improved Victim Engagement
- AI Chat bot**
- Automatically saves all chat history between victims and Vani-CyberDost
 - Enhanced Evidence Gathering
 - Improved Case Management

Benefits

Cyber Crime App:
Report anywhere, anytime. Get help faster, stay informed, and protect yourself.

Do Your Part
#BeCyberSmart

Thank you :)
Feedback Welcome