Cyber Challenge - Delhi Police

Organized by Delhi Police in collaboration with CyberPeace

November 28, 2024 – January 17, 2025

Introduction

Welcome to the Cyber Challenge – Delhi Police!

The Cyber Challenge organized by the Delhi Police in collaboration with CyberPeace aims to drive innovation in cybersecurity by addressing today's most pressing digital safety issues. This event calls upon developers, engineers, cybersecurity enthusiasts, and tech-savvy individuals to build practical, high-impact solutions for a safer digital space. Participants will tackle real-world problem statements directly impacting public safety and online security, with the opportunity to make meaningful contributions to digital well-being.

Objectives of the Cyber Challenge

Drive Innovation
Encourage participants to solve real-world cybersecurity issues.

Raise Awareness
Educate participants and the community about critical online safety concerns.

Enhance Public Safety
Create solutions that can improve digital security and protect vulnerable groups.

Foster Collaboration
Provide a platform for technologists to collaborate and create impactful solutions.

Join us in crafting a safer digital world through cutting-edge technology!

Competition Structure

The challenge is structured in three phases: Registration, Shortlisting, and a Grand Finale. Each phase is designed to encourage rigorous preparation and innovation, with finalists moving forward to a 36-hour intensive prototype development round.

Phase 1: Registration

Submission Requirements:

- Participants (individuals or teams of up to 3 members) must submit:
  - A brief writeup describing their proposed solution.
  - A PowerPoint presentation highlighting the solution's technology, impact, and feasibility.

Registration Process:

- Participants register online via our event portal.
- Submissions should clearly convey how their solution addresses one of the problem statements.

Phase 2: Shortlisting

Selection Process:

- The top 20 participants/teams will be shortlisted based on the quality of their writeup and PowerPoint presentation. Shortlisting criteria will include innovation, relevance to the problem statement, technical feasibility, and potential impact.
- Shortlisted participants will receive notification and an invitation to participate in the Grand Finale.

Phase 3: Grand Finale – 36-Hour Prototype Development

Format: Physical, In-Person Event

During the Grand Finale, shortlisted participants will have 36 hours to transform their proposed solutions into working prototypes. They will have access to mentors and necessary resources to assist in the development process. Teams are encouraged to focus on functionality, usability, and scalability within the time limit.

Evaluation and Judging

Judging Criteria

Innovation

Impact

Usability

Technical Feasibility

Presentation

Judging Panel

A panel of experts from cybersecurity, digital safety, and public safety fields will evaluate each prototype.

Awards Ceremony

Awards and Prizes

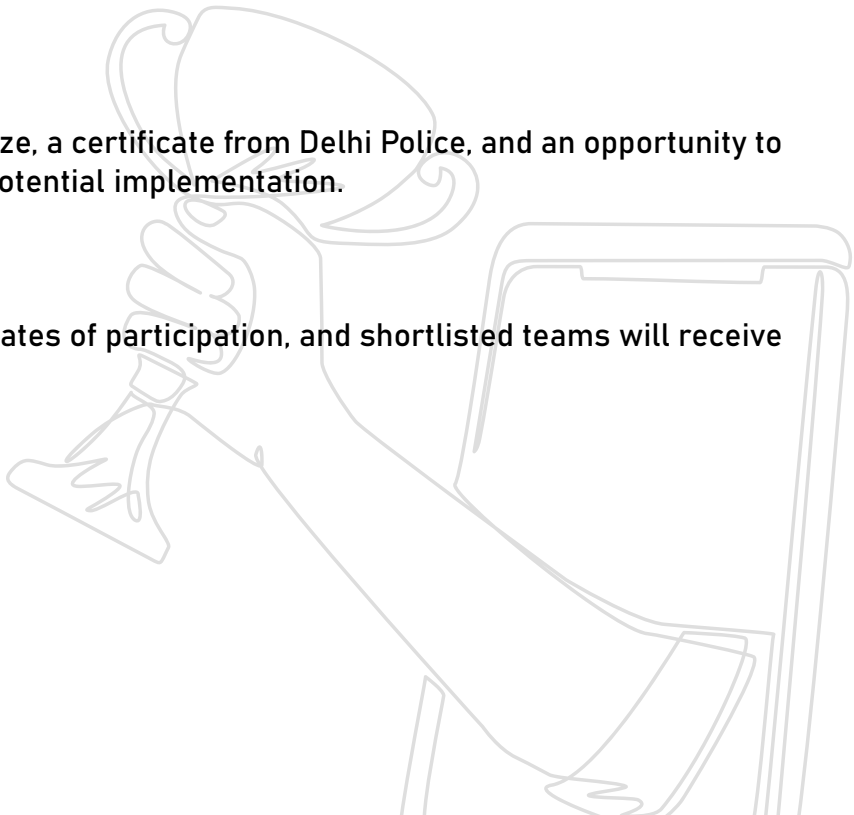
Top solutions will be awarded in the following categories:

- Best Overall Solution
- Most Innovative Solution
- Best Prototype Design
- Most Impactful Solution

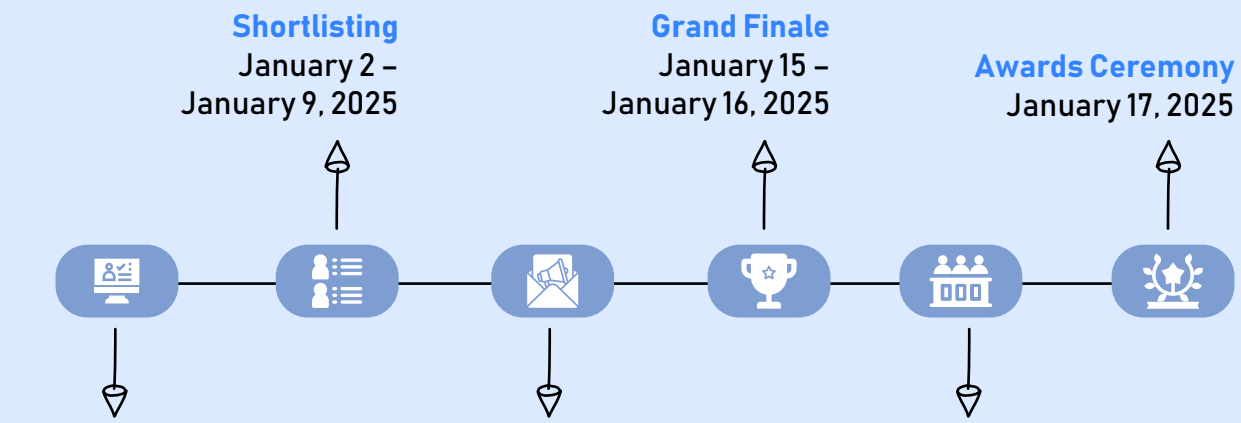
Each winner will receive a cash prize, a certificate from Delhi Police, and an opportunity to further develop their solution for potential implementation.

Participant Recognition

All participants will receive certificates of participation, and shortlisted teams will receive special recognition.



Timeline



Benefits of Participation

- **Learning and Skill Development:** Gain hands-on experience in cybersecurity, AI, and digital safety.
- **Networking Opportunities:** Connect with cybersecurity experts, industry leaders, and other participants.
- **Recognition and Awards:** Top solutions will receive awards and public recognition from Delhi Police.
- **Real-World Impact:** Your solution could potentially be implemented, contributing to safer digital environments.
- **Certificates and Prizes:** All participants will receive certificates, with top teams eligible for additional prizes.

Together, let's build a safer, more resilient internet for all.

Problem Statements

Counteracting Misinformation and Fake News

Problem Statement: The spread of fake news and misinformation, particularly through social media, has led to public unrest and misinformation. Participants need to develop tools and strategies to quickly identify, verify, and neutralize misleading information while ensuring the flow of accurate public safety communication.

Enhancing Women's Safety through Predictive Analytics

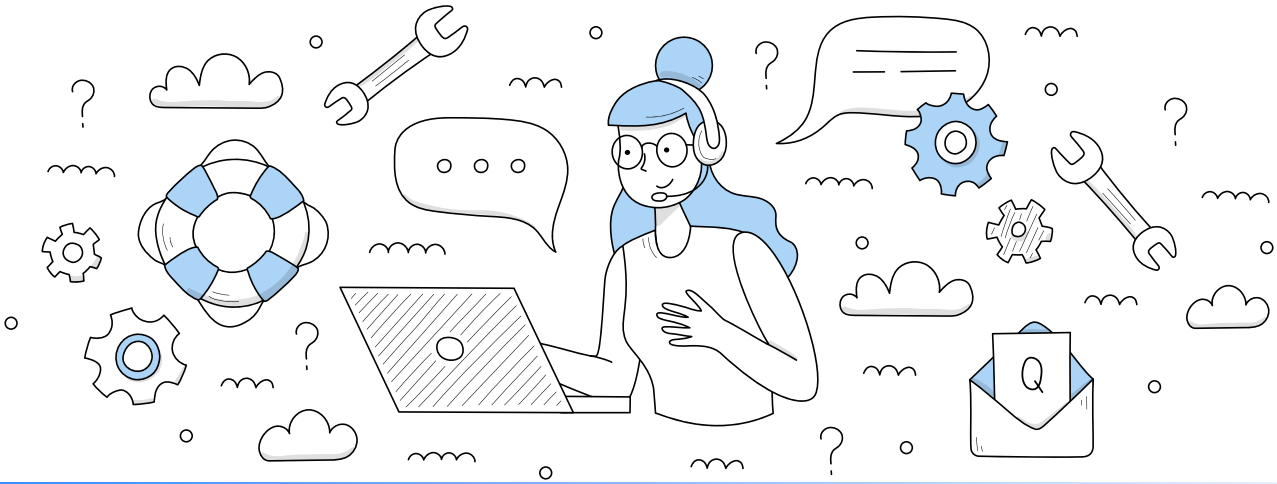
Problem Statement: Develop a predictive analytics tool that utilizes data from various social media platforms, public security cameras, and historical crime data to identify potential threats to women's safety in specified areas. This software tool should also recommend preventive actions and alert local law enforcement and community safety groups in real-time.

Social Media Monitoring of Juvenile Gang Activity

Problem Statement: Design an ethical social media monitoring system that can detect signs of gang activity and radicalization among juveniles. The system should use natural language processing to analyze posts, detect patterns, and alert authorities about potential gang recruitment or radical behavior, facilitating early intervention.

Combating the Challenge of Digital Arrest Scam

Problem Statement: The phenomenon of "digital arrests," where fraudsters impersonate law enforcement officials to coerce victims into transferring funds under false legal threats, has surged across India. These scams exploit the victims' fear of legal repercussions, involving sophisticated deceit with fake identities, forged documents, and manipulated video calls resembling police environments. The rapid escalation in these cases has led to significant financial and emotional distress among the public, prompting urgent calls for effective interventions. The tool can offer solutions for prevention anlaytics based detections, pattern analysis etc.



Challenge

Develop an integrated cybersecurity solution that:

Educates the Public: Implements a widespread digital literacy and public awareness campaign that educates citizens on recognizing and responding to digital arrest scams. This campaign should use various media platforms to reach a broad audience and include real-time alerts about ongoing scam tactics.

Authenticates Official Communications: Creates a secure, easy-to-use portal or mobile application that helps citizens verify the authenticity of communications purportedly from law enforcement or other government agencies.

Supports Victims: Establishes a rapid response system for victims to report incidents and receive immediate help. This system should coordinate with banking institutions, telecom companies, and law enforcement to quickly freeze fraudulent transactions and trace the source of the scam.

Legal and Technical Framework Enhancement: Proposes changes to existing laws to include specific provisions against digital arrest scams, enhancing penalties and defining clear procedural guidelines for digital communication by law enforcement.

Innovative Technology Utilization: Leverages AI and machine learning to detect patterns indicative of scams and preemptively block communications from known fraudulent sources.

Partners

National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Follow us

@GlobalCyberChallenge

@GlobalCyberChallenge

@icyberchallenge

Registration begins on
November 28th, 2024

Scan the QR Code or Follow the link for Registrations

https://cyberchallenge.in/