

Topper Mantra Innovation Challenge (TMIC) 2026

Theme 6: Cyber Safety & Online Fraud

50 Core Hackathon Problem Statements | Classes 8–12

Readable handbook edition with bold section labels, objective bullets, and spacious formatting.

Contents

Segment A: Online Fraud Detection & Prevention

TMIC-CYB-001 - Phishing Link Detection Tool
TMIC-CYB-002 - Fake Payment Screenshot Detector
TMIC-CYB-003 - UPI Fraud Risk Alert System
TMIC-CYB-004 - Online Shopping Scam Detector
TMIC-CYB-005 - Fake Job Offer Verification Tool
TMIC-CYB-006 - Scholarship Fraud Verification System
TMIC-CYB-007 - Loan App Risk Checker
TMIC-CYB-008 - Fake Customer Care Number Detector
TMIC-CYB-009 - Fraud Message Pattern Detector
TMIC-CYB-010 - Online Fraud Risk Score for Common Users

Segment B: Identity, Privacy & Account Protection

TMIC-CYB-011 - Password Strength and Reuse Checker
TMIC-CYB-012 - Two-Factor Authentication Adoption Tool
TMIC-CYB-013 - Personal Data Exposure Checker
TMIC-CYB-014 - App Permission Risk Analyzer
TMIC-CYB-015 - Safe Login Alert System
TMIC-CYB-016 - Digital ID Misuse Prevention Tool
TMIC-CYB-017 - Privacy-Safe Form Filling Assistant
TMIC-CYB-018 - Social Media Privacy Audit Tool
TMIC-CYB-019 - Lost Phone Data Protection Guide
TMIC-CYB-020 - Family Account Safety Dashboard

Segment C: Cyberbullying, Digital Harassment & Online Abuse

TMIC-CYB-021 - Cyberbullying Evidence Capture Tool
TMIC-CYB-022 - Abusive Chat Warning System
TMIC-CYB-023 - Fake Profile and Impersonation Reporter
TMIC-CYB-024 - Image Misuse Alert and Response Tool
TMIC-CYB-025 - Anonymous Digital Harassment Reporting System
TMIC-CYB-026 - Online Gaming Safety System
TMIC-CYB-027 - Digital Consent Learning Simulator
TMIC-CYB-028 - Online Blackmail Emergency Pathway
TMIC-CYB-029 - Rumour and Fake Post Control Tool
TMIC-CYB-030 - Safe Peer Support for Online Abuse

Segment D: Financial Cyber Safety & Digital Payment Protection

TMIC-CYB-031 - OTP Scam Prevention System
TMIC-CYB-032 - QR Code Safety Checker
TMIC-CYB-033 - Screen-Sharing Scam Alert Tool
TMIC-CYB-034 - Digital Payment Receipt Verification

TMIC-CYB-035 - Elderly Digital Payment Safety Assistant
TMIC-CYB-036 - Small Business Cyber Fraud Shield
TMIC-CYB-037 - Bank Fraud Emergency Response Tool
TMIC-CYB-038 - Safe Online Donation Verification Tool
TMIC-CYB-039 - Subscription and Auto-Debit Tracker
TMIC-CYB-040 - Digital Transaction Risk Dashboard

Segment E: Cyber Awareness Infrastructure, School Systems & Community Protection

TMIC-CYB-041 - School Cyber Safety Help Desk
TMIC-CYB-042 - Cyber Safety Incident Tracker for Schools
TMIC-CYB-043 - Safe Internet Lab Monitoring System
TMIC-CYB-044 - Student Digital Footprint Cleaner
TMIC-CYB-045 - Cyber Safety Game for Rural Students
TMIC-CYB-046 - Local Language Cyber Fraud Assistant
TMIC-CYB-047 - Cybercrime Reporting Guide Tool
TMIC-CYB-048 - Cyber Safety Score for Students
TMIC-CYB-049 - Community Cyber Fraud Alert Network
TMIC-CYB-050 - Cyber Safe School Model

Segment A: Online Fraud Detection & Prevention

TMIC-CYB-001

Phishing Link Detection Tool

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to phishing link detection tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps students and citizens identify suspicious links, fake websites, malicious URLs, shortened links, and phishing pages before clicking.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for phishing link detection tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with phishing link detection tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Phishing • Link • Detection

TMIC-CYB-002

Fake Payment Screenshot Detector

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to fake payment screenshot detector are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps small shopkeepers, students, and local sellers verify whether a payment screenshot is genuine or fake before handing over products or services.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for fake payment screenshot detector. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with fake payment screenshot detector. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

TMIC-CYB-003

UPI Fraud Risk Alert System

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to upi fraud risk alert system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that detects risky UPI payment situations such as unknown collect requests, fake refund links, QR fraud, screen-sharing scams, and suspicious payment instructions.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for upi fraud risk alert system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with upi fraud risk alert system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • UPI • Fraud • Risk

TMIC-CYB-004

Online Shopping Scam Detector

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to online shopping scam detector are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a system that helps users identify fake e-commerce websites, unrealistic offers, duplicate product pages, fake reviews, and unsafe payment links.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for online shopping scam detector. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with online shopping scam detector. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Online • Shopping • Scam

TMIC-CYB-005

Fake Job Offer Verification Tool

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to fake job offer verification tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps students and job seekers verify suspicious job offers, fake interview links, registration fee demands, forged offer letters, and fraudulent recruiter messages.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for fake job offer verification tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with fake job offer verification tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Fake • Job • Offer

TMIC-CYB-006

Scholarship Fraud Verification System

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to scholarship fraud verification system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps students verify whether a scholarship link, message, form, or application fee demand is genuine or fraudulent.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for scholarship fraud verification system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring,

educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with scholarship fraud verification system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Scholarship • Fraud • Verification

TMIC-CYB-007

Loan App Risk Checker

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to loan app risk checker are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a system that helps users identify risky instant loan apps based on permissions, reviews, hidden charges, data access, harassment reports, and suspicious behaviour.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for loan app risk checker. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with loan app risk checker. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Loan • App • Risk

TMIC-CYB-008

Fake Customer Care Number Detector

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to fake customer care number detector are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps citizens verify customer care numbers found on search engines, social media, posters, or messages before calling and sharing sensitive details.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for fake customer care number detector. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with fake customer care number detector. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Fake • Customer • Care

TMIC-CYB-009

Fraud Message Pattern Detector

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to fraud message pattern detector are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a system that identifies suspicious SMS, WhatsApp messages, emails, or social media messages based on urgency, fake rewards, OTP requests, links, and payment pressure.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.
- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for fraud message pattern detector. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with fraud message pattern detector. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Fraud • Message • Pattern

TMIC-CYB-010

Online Fraud Risk Score for Common Users

Theme: Cyber Safety & Online Fraud

Category: Online Fraud Detection & Prevention

Background: As digital services become part of daily life, risks linked to online fraud risk score for common users are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of online fraud detection & prevention and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a simple risk-scoring tool that tells users whether a digital interaction, message, link, call, or payment request is low-risk, suspicious, or high-risk.

Objectives:

- Help users identify fraud patterns before they take action.
- Reduce the risk of money loss, data theft, or account compromise.

- Make cyber warnings simple enough for everyday users and students.
- Promote timely verification before clicking, paying, or sharing details.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for online fraud risk score for common users. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with online fraud risk score for common users. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Online Fraud • Scam Detection • Online • Fraud • Risk

Segment B: Identity, Privacy & Account Protection

TMIC-CYB-011

Password Strength and Reuse Checker

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to password strength and reuse checker are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps students understand password strength, avoid reuse across accounts, and create stronger password habits without storing actual passwords.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for password strength and reuse checker. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with password strength and reuse checker. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Password • Strength • and

TMIC-CYB-012

Two-Factor Authentication Adoption Tool

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to two-factor authentication adoption tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that guides users to enable two-factor authentication on important accounts such as email, banking, social media, education portals, and cloud storage.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for two-factor authentication adoption tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with two-factor authentication adoption tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Two • Factor • Authentication

TMIC-CYB-013**Personal Data Exposure Checker**

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to personal data exposure checker are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps users identify what personal information they may be exposing online through profiles, forms, apps, public posts, or shared documents.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for personal data exposure checker. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with personal data exposure checker. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Personal • Data • Exposure

TMIC-CYB-014**App Permission Risk Analyzer**

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to app permission risk analyzer are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps users understand risky mobile app permissions such as contacts, camera, microphone, location, SMS, storage, and accessibility access.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for app permission risk analyzer. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with app permission risk analyzer. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • App • Permission • Risk

TMIC-CYB-015

Safe Login Alert System

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to safe login alert system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a system that helps users notice suspicious logins, unknown devices, new locations, password changes, or account recovery attempts.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for safe login alert system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with safe login alert system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Safe • Login • Alert

TMIC-CYB-016

Digital ID Misuse Prevention Tool

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to digital id misuse prevention tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy &

account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps users safely share Aadhaar, PAN, school ID, certificates, or personal documents using masking, watermarking, purpose tags, and expiry labels.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for digital id misuse prevention tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with digital id misuse prevention tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Digital • Misuse • Prevention

TMIC-CYB-017

Privacy-Safe Form Filling Assistant

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to privacy-safe form filling assistant are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that warns users when online forms ask for unnecessary sensitive information such as OTP, bank details, Aadhaar, passwords, or personal photos.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for privacy-safe form filling assistant. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with privacy-safe form filling assistant. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Privacy • Safe • Form

TMIC-CYB-018

Social Media Privacy Audit Tool

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to social media privacy audit tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps students review their social media privacy settings, public posts, tagged photos, visible personal details, and unknown followers.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for social media privacy audit tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with social media privacy audit tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Social • Media • Privacy

TMIC-CYB-019

Lost Phone Data Protection Guide

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to lost phone data protection guide are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a step-by-step emergency tool that helps users protect accounts, SIM, UPI, photos, email, and personal data when a phone is lost or stolen.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for lost phone data protection guide. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with lost phone data protection guide. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Lost • Phone • Data

TMIC-CYB-020

Family Account Safety Dashboard

Theme: Cyber Safety & Online Fraud

Category: Identity, Privacy & Account Protection

Background: As digital services become part of daily life, risks linked to family account safety dashboard are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of identity, privacy & account protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a privacy-respecting dashboard that helps families track whether important accounts have strong passwords, 2FA, backup contacts, and recovery options enabled.

Objectives:

- Strengthen user awareness of personal data and account security.
- Reduce risky digital habits such as weak passwords or oversharing.
- Support safer use of devices, apps, and online platforms.
- Encourage privacy-conscious behaviour without making tools complex.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for family account safety dashboard. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with family account safety dashboard. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Privacy • Account Security • Family • Account • Safety

Segment C: Cyberbullying, Digital Harassment & Online Abuse

TMIC-CYB-021

Cyberbullying Evidence Capture Tool

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to cyberbullying evidence capture tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a privacy-safe tool that helps students save screenshots, messages, usernames, dates, links, and incident notes for reporting cyberbullying or online abuse.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cyberbullying evidence capture tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cyberbullying evidence capture tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

TMIC-CYB-022

Abusive Chat Warning System

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to abusive chat warning system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that detects harmful patterns in online conversations such as threats, bullying, manipulation, blackmail, hate speech, and repeated harassment.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for abusive chat warning system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with abusive chat warning system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Abusive • Chat • Warning

TMIC-CYB-023

Fake Profile and Impersonation Reporter

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to fake profile and impersonation reporter are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps users identify and report fake profiles, impersonation accounts, copied photos, fake names, or identity misuse on social platforms.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for fake profile and impersonation reporter. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with fake profile and impersonation reporter. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Fake • Profile • and

TMIC-CYB-024

Image Misuse Alert and Response Tool

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to image misuse alert and response tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that guides users through immediate steps when personal photos, edited images, or private media are misused online.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for image misuse alert and response tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with image misuse alert and response tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Image • Misuse • Alert

TMIC-CYB-025

Anonymous Digital Harassment Reporting System

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to anonymous digital harassment reporting system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a school-level reporting system where students can safely report cyberbullying, online threats, fake rumours, or digital harassment without public exposure.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for anonymous digital harassment reporting system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling,

visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with anonymous digital harassment reporting system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Anonymous • Digital • Harassment

TMIC-CYB-026

Online Gaming Safety System

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to online gaming safety system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that protects students from abusive chats, stranger danger, gaming scams, pressure to share personal data, and toxic behaviour in gaming communities.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for online gaming safety system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with online gaming safety system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Online • Gaming • Safety

TMIC-CYB-027

Digital Consent Learning Simulator

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to digital consent learning simulator are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build an interactive simulator that teaches students about consent before sharing photos, screenshots, chats, videos, personal details, or private information.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for digital consent learning simulator. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with digital consent learning simulator. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Digital • Consent • Learning

TMIC-CYB-028

Online Blackmail Emergency Pathway

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to online blackmail emergency pathway are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a confidential tool that helps victims of online blackmail understand safe next steps, preserve evidence, contact trusted adults, and report the incident.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for online blackmail emergency pathway. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with online blackmail emergency pathway. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Online • Blackmail • Emergency

TMIC-CYB-029

Rumour and Fake Post Control Tool

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to rumour and fake post control tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps schools or communities verify viral claims, reduce panic, and stop the spread of fake rumours during sensitive incidents.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.

- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for rumour and fake post control tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with rumour and fake post control tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Rumour • and • Fake

TMIC-CYB-030

Safe Peer Support for Online Abuse

Theme: Cyber Safety & Online Fraud

Category: Cyberbullying, Digital Harassment & Online Abuse

Background: As digital services become part of daily life, risks linked to safe peer support for online abuse are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyberbullying, digital harassment & online abuse and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a guided peer-support model where students can help classmates facing cyberbullying while ensuring adult escalation for serious cases.

Objectives:

- Support safer reporting and evidence preservation for online abuse.
- Help students detect harmful digital behaviour early.
- Promote safe escalation to trusted adults or responsible authorities.
- Protect privacy and emotional wellbeing during incident response.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for safe peer support for online abuse. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with safe peer support for online abuse. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Cyberbullying • Online Safety • Safe • Peer • Support

Segment D: Financial Cyber Safety & Digital Payment Protection

TMIC-CYB-031

OTP Scam Prevention System

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to otp scam prevention system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that warns users when someone tries to trick them into sharing OTPs, PINs, CVV, passwords, or screen access during calls or chats.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for otp scam prevention system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with otp scam prevention system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • OTP • Scam • Prevention

TMIC-CYB-032**QR Code Safety Checker**

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to qr code safety checker are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps users check whether a QR code leads to a safe payment, fake link, malicious website, or unknown destination before scanning.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for qr code safety checker. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with qr code safety checker. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Code • Safety • Checker

TMIC-CYB-033**Screen-Sharing Scam Alert Tool**

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to screen-sharing scam alert tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that educates and warns users when screen-sharing apps are being used in risky financial situations, fake customer care calls, or refund scams.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for screen-sharing scam alert tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with screen-sharing scam alert tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Screen • Sharing • Scam

TMIC-CYB-034

Digital Payment Receipt Verification

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to digital payment receipt verification are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps small vendors verify payment success through transaction ID, timestamp, payer details, bank status, and official app confirmation.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for digital payment receipt verification. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with digital payment receipt verification. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Digital • Payment • Receipt

TMIC-CYB-035

Elderly Digital Payment Safety Assistant

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to elderly digital payment safety assistant are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial

cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a simplified safety assistant that helps elderly users make digital payments safely and avoid fraud calls, fake links, OTP sharing, and wrong transfers.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for elderly digital payment safety assistant. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with elderly digital payment safety assistant. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Elderly • Digital • Payment

TMIC-CYB-036

Small Business Cyber Fraud Shield

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to small business cyber fraud shield are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a cyber safety solution for small shops and local businesses to prevent fake payments, fake orders, refund scams, account takeover, and customer impersonation.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for small business cyber fraud shield. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with small business cyber fraud shield. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Small • Business • Cyber

TMIC-CYB-037

Bank Fraud Emergency Response Tool

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to bank fraud emergency response tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that guides users through immediate steps after suspected bank fraud, including blocking cards, freezing accounts, filing complaints, and saving evidence.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for bank fraud emergency response tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with bank fraud emergency response tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Bank • Fraud • Emergency

TMIC-CYB-038

Safe Online Donation Verification Tool

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to safe online donation verification tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps users verify donation requests, charity links, disaster relief funds, medical fundraising pages, and emotional scam campaigns.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for safe online donation verification tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with safe online donation verification tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Safe • Online • Donation

TMIC-CYB-039

Subscription and Auto-Debit Tracker

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to subscription and auto-debit tracker are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a system that helps users track hidden subscriptions, trial traps, auto-debits, recurring payments, and unwanted digital charges.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for subscription and auto-debit tracker. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with subscription and auto-debit tracker. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Subscription • and • Auto

TMIC-CYB-040

Digital Transaction Risk Dashboard

Theme: Cyber Safety & Online Fraud

Category: Financial Cyber Safety & Digital Payment Protection

Background: As digital services become part of daily life, risks linked to digital transaction risk dashboard are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of financial cyber safety & digital payment protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a dashboard that helps users review recent digital transactions, detect unusual activity, and identify possible fraud patterns early.

Objectives:

- Reduce common financial fraud risks during digital transactions.
- Help users verify payments, requests, and payment channels safely.
- Protect vulnerable groups such as small vendors and elderly users.
- Promote faster response when suspicious financial activity occurs.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for digital transaction risk dashboard. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with digital transaction risk dashboard. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: Digital Payments • Financial Safety • Digital • Transaction • Risk

Segment E: Cyber Awareness Infrastructure, School Systems & Community Protection

TMIC-CYB-041

School Cyber Safety Help Desk

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to school cyber safety help desk are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a school-level cyber help desk system where students can report suspicious links, cyberbullying, fake profiles, account issues, online fraud, or digital safety concerns.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for school cyber safety help desk. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with school cyber safety help desk. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • School • Cyber • Safety

TMIC-CYB-042

Cyber Safety Incident Tracker for Schools

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to cyber safety incident tracker for schools are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a privacy-safe tracker that helps schools understand common cyber safety incidents among students without exposing individual identities.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cyber safety incident tracker for schools. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cyber safety incident tracker for schools. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Cyber • Safety • Incident

TMIC-CYB-043

Safe Internet Lab Monitoring System

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to safe internet lab monitoring system are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a solution that helps schools manage safe internet use in computer labs by tracking unsafe websites, suspicious downloads, harmful searches, and misuse of school devices.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for safe internet lab monitoring system. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with safe internet lab monitoring system. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Safe • Internet • Lab

TMIC-CYB-044

Student Digital Footprint Cleaner

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to student digital footprint cleaner are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps students identify risky public posts, overshared personal details, old embarrassing content, and privacy mistakes in their digital footprint.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for student digital footprint cleaner. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with student digital footprint cleaner. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Student • Digital • Footprint

TMIC-CYB-045

Cyber Safety Game for Rural Students

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to cyber safety game for rural students are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a game-based solution that teaches cyber safety concepts such as phishing, OTP fraud, fake links, online privacy, and safe payments in simple language.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cyber safety game for rural students. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cyber safety game for rural students. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Cyber • Safety • Game

TMIC-CYB-046

Local Language Cyber Fraud Assistant

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to local language cyber fraud assistant are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a multilingual assistant that explains cyber fraud warnings, reporting steps, helpline numbers, evidence preservation, and safe digital behaviour in local language.

Objectives:

- Build cyber safety support systems at school and community level.

- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for local language cyber fraud assistant. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with local language cyber fraud assistant. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Local • Language • Cyber

TMIC-CYB-047

Cybercrime Reporting Guide Tool

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to cybercrime reporting guide tool are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a tool that helps users understand where and how to report cybercrime, what evidence to save, what details to include, and how to track complaint status.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cybercrime reporting guide tool. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cybercrime reporting guide tool. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Cybercrime • Reporting • Guide

TMIC-CYB-048

Cyber Safety Score for Students

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to cyber safety score for students are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a self-assessment tool that gives students a cyber safety score based on password habits, privacy settings, app permissions, payment safety, and online behaviour.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cyber safety score for students. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cyber safety score for students. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Cyber • Safety • Score

TMIC-CYB-049

Community Cyber Fraud Alert Network

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to community cyber fraud alert network are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a community-level alert system where verified cyber fraud patterns, scam messages, fake links, and risky phone numbers can be shared responsibly.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for community cyber fraud alert network. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with community cyber fraud alert network. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Community • Cyber • Fraud

TMIC-CYB-050

Cyber Safe School Model

Theme: Cyber Safety & Online Fraud

Category: Cyber Awareness Infrastructure, School Systems & Community Protection

Background: As digital services become part of daily life, risks linked to cyber safe school model are increasing for students, families, and ordinary users. Many people act quickly online without clear verification, which can lead to fraud, privacy loss, harassment, or account compromise. This challenge sits within the broader area of cyber awareness infrastructure, school systems & community protection and asks participants to create a practical, user-friendly solution that can work in real-life settings, including school and community contexts.

Problem Statement: Build a complete model for a cyber-safe school that includes reporting support, awareness tools, account protection, payment safety, device safety, incident tracking, and parent-student guidance.

Objectives:

- Build cyber safety support systems at school and community level.
- Make reporting, guidance, and awareness more structured and accessible.
- Help institutions understand common cyber safety gaps and patterns.
- Promote safer digital ecosystems for students, teachers, and families.

Scope of Innovation: Participants may build a mobile app, web tool, browser extension, chatbot, dashboard, simulator, alert system, learning module, decision-support tool, or low-cost hybrid model for cyber safe school model. The solution may use pattern recognition, checklists, structured workflows, privacy-safe data handling, visual scoring, educational interaction, or escalation pathways. Designs should be simple, practical, and suitable for users with varying digital literacy levels.

Expected Impact: A strong solution should make users safer, more confident, and better prepared while dealing with cyber safe school model. It should reduce avoidable mistakes, support early action, and create measurable improvement in cyber safety awareness and response quality.

Challenge Tags: School Cyber Safety • Community Protection • Cyber • Safe • School