INDIAN CYBERSECURITY REPORT 2025

Citizen Awareness & K-12 Education Guide

Understanding Cyber Threats, Safety Measures & Protection Strategies

Dr. Bhavana Chibber

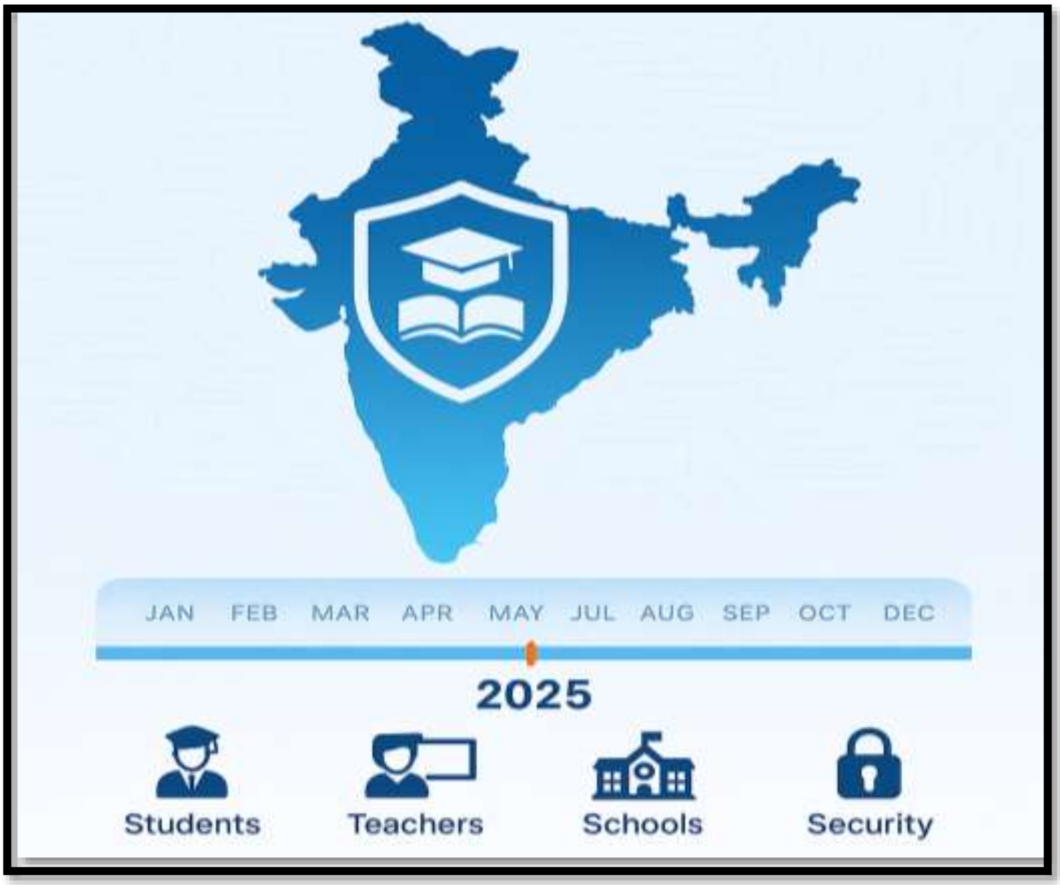
Principal | Author | Mentor | Researcher

Cybersecurity Expert & Awareness Advocate

□ CYBERSECURITY AWARENESS PROGRAMME □

Empowering Citizens & Young Learners Against Cyber Threats

December 2025



Gen AI image

DISCLAIMER & DATA SOURCES

About This Report

This report is an educational resource compiled by Dr. Bhavana Chibber for the purpose of cybersecurity awareness and public education. It synthesizes verified information from multiple authoritative sources to create a comprehensive guide for Indian citizens, families, and K-12 learners.

Data Sources & Attribution

All statistics, incidents, and case studies in this report are sourced from:

- **Government Sources:** Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY), National Cyber Crime Reporting Portal (NCRP), Indian Cyber Crime Coordination Centre (I4C)
- **Industry Reports:** Seqrite India Cyber Threat Report 2025, Data Security Council of India (DSCI), Acronis Cyberthreats Report H1 2025, CloudSEK Research, Rubrik Zero Labs
- **Verified News Sources:** The Economic Times, Bloomberg, Reuters, Press Trust of India, The Times of India, and other credible media outlets
- **Judicial & Legal Records:** Supreme Court of India proceedings, Government advisories, Official notifications
- **Academic & Research Sources:** Cybersecurity research papers, forensic case studies, threat intelligence reports

Scope & Limitations

- This report covers cybersecurity incidents and trends from January to November 2025
- All financial figures are based on reported cases; actual losses may be higher due to underreporting
- Case studies are real but some victim identities are protected as per media reports
- The cyber threat landscape evolves rapidly; readers should check official sources for latest updates

Copyright & Usage

© 2025 Dr. Bhavana Chibber - Cybersecurity Awareness Programme. This report may be freely shared for educational and non-commercial purposes with proper attribution. Schools, institutions, and community organizations are encouraged to use this material for awareness training.

Contact for Verification

For source verification, fact-checking inquiries, or to report updates, please contact Dr. Bhavana Chibber through official channels. All claims in this report can be cross-referenced with the cited sources.

MESSAGE FROM CURATOR

My Mission & Approach

Dear Fellow Citizens, Educators, and Young Learners,

As a cybersecurity expert who has dedicated my career to protecting our digital society, I have witnessed the devastating impact of cybercrimes on ordinary Indians. But I have also seen the transformative power of education. When people understand the threats, they can protect themselves. When children learn cyber hygiene early, they become digital citizens who navigate the online world safely.

This report represents more than statistics and case studies. It embodies my commitment to making cybersecurity accessible to everyone, from senior citizens who may be intimidated by technology to young students who are digital natives but lack awareness of dangers.

My Educational Philosophy

As a Principal, Author, Mentor, and Researcher, my approach is built on three pillars:

- **Simplification Without Dumbing Down:** Cybersecurity is complex, but everyone deserves to understand it. I break down technical jargon into relatable scenarios without losing accuracy.
- **Empowerment Through Knowledge:** Fear paralyzes; knowledge empowers. I focus on practical actions people can take immediately, building confidence in their ability to stay safe.
- **Age-Appropriate Learning:** A 70-year-old grandmother needs different guidance than a 12-year-old student. This report addresses all age groups with targeted advice.

Why I Focus on K-12 Education

Children today are born into a digital world. By age 10, many have smartphones. By 12, they're on social media. By 15, they're conducting financial transactions. Yet, cybersecurity education in schools remains minimal or absent.

I believe that ***cybersecurity literacy should be as fundamental as reading, writing, and arithmetic.*** When we teach children to look both ways before crossing the road, we're teaching physical safety. We must teach them to verify before clicking links, that's digital safety.

Young learners are not just vulnerable targets; they're also the solution. A cybersecurity-aware teenager can protect their entire family. A student who learns safe practices today becomes a responsible digital citizen tomorrow and a cybersecurity professional the day after.

What Makes My Approach Different

- **Real Stories, Real Impact:** I share actual case studies because stories resonate more than statistics. When students hear about an 86-year-old losing ₹20 crore, they remember to warn their grandparents.
- **Hands-On Learning:** In my workshops, students don't just listen, they practice. They create strong passwords, enable two-factor authentication, spot phishing emails.
- **Community Multiplication:** Every person I train becomes an ambassador. One aware student educates their family. One trained teacher impacts hundreds of children annually.
- **Continuous Evolution:** Cyber threats change daily. My programme updates regularly, ensuring learners get current, relevant information.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY: 2025 THREAT LANDSCAPE

The year 2025 marked a watershed moment in India's cybersecurity history. With 369 million malware detections, ₹22,812 crore in financial losses, and cyber warfare becoming reality during the May geopolitical crisis, the digital threat landscape evolved beyond anything previously experienced. India witnessed unprecedented cyber threats in 2025, with over 369 million malware detections, averaging 702 potential security threats every minute. This report synthesizes verified data from government sources, industry reports, and credible media to provide a comprehensive overview of the cybersecurity landscape. For educators, this year demonstrated unequivocally that cybersecurity literacy is not optional, it is as fundamental as mathematics, science, and language education.

2025 At A Glance: Critical Statistics

Metric	2025 Data
Total Malware Detections	369 Million (11 per second)
Financial Losses	₹22,812 Crore (~$2.7 Billion)
India's Global Ranking	#2 Most Targeted Nation
Most Attacked Sector	Healthcare (21.82%)
AI-Generated Phishing	82.6% of campaigns
Education Sector Impact	~16% of all attacks

Source: DSCI-Seqrite India Cyber Threat Report 2025, GIREM-Tekion State of AI-Powered Cybercrime Report 2025, CERT-In data

Month-wise Cybersecurity Incident Report – 2025

National Executive Summary

The year 2025 marked a critical period for India’s cybersecurity landscape, witnessing a sharp escalation in cyberattacks, financial frauds, regulatory reforms, and national security incidents. The country experienced large-scale data breaches in the healthcare, fintech, and mobility sectors, along with coordinated nation-state cyber campaigns linked to geopolitical tensions. Digital arrest scams emerged as one of the most financially damaging threats, prompting interventions from the Supreme Court, CBI, and multiple ministries. Meanwhile, India strengthened its cyber governance through new CERT-In guidelines, cybersecurity budget allocations, stricter SIM authentication rules, and institutional restructuring under the National Security Council Secretariat. Law enforcement agencies across states demonstrated enhanced operational capabilities through large-scale arrests and recovery of fraud proceeds. Overall, 2025 reflected both the growing sophistication of cyber threats and the parallel strengthening of India’s cyber defense ecosystem.

January 2025

In January 2025, a Pakistan-backed spear-phishing campaign targeted DRDO researchers in Delhi using malware-infected PDFs, which was successfully blocked. At the same time, the Pakistan-linked APT36 espionage group attempted to deploy Crimson RAT malware using lures related to the Pahalgam attack. The Indian Cybercrime Coordination Centre ordered the removal of apps violating IT laws for failing to share hoax threat data. Additionally, the government released Draft Digital Personal Data Protection Rules to operationalize the

DPDPA framework.

Sources:
https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

https://practiceguides.chambers.com/practice-guides/cybersecurity-2025/india/trends-and-developments

February 2025

In February 2025, health insurer Niva Bupa investigated a potential customer data breach in Gurugram. Gurugram Police arrested 27 individuals linked to a multi-crore cyber fraud operation. Across India, digital arrest scams caused losses of ₹26 billion by the end of the month, with impersonation tactics escalating rapidly.

Sources:
https://63sats.com/blog/global-cyber-pulse-25-february-2025

https://www.bloomberg.com/features/2025-india-digital-scams/

March 2025

In March 2025, I4C issued a nationwide advisory warning citizens about the sharp rise in digital arrest fraud complaints reported through the NCRP portal. A CloudSEK report further projected that Indian entities could lose ₹20,000 crore to cybercrime in 2025, with the BFSI sector alone accounting for ₹8,200 crore in losses.

Sources:
https://cybercrime.gov.in/pdf/Advisories/ADVISORYTAU-ADV-003DigitalArrest06.03.2025.pdf

https://m.economictimes.com/industry/banking/finance/indian-entities-may-lose-rs-20000-cr-to-cyber-crimes-in-2025-cloudsek-report/articleshow/118651127.cms

April 2025

In April 2025, Nippon Life India Asset Management detected a cyberattack on its IT infrastructure that disrupted operations without a data breach. During the same period, Angel One faced potential data leakage caused by an AWS cloud misconfiguration, highlighting risks in cloud security management.

Sources:
https://www.eimt.edu.eu/25-major-cyber-attacks-in-india-threats-and-strategies

May 2025

May 2025 saw a massive coordinated cyberattack campaign following Operation Sindoor, with over 1.5 million attacks on Indian digital infrastructure. Star Health suffered a catastrophic data breach involving 7.24 TB of data affecting 31 million customers. Authorities dismantled a Pakistan-linked cyber fraud gang in Bihar and busted a major Telangana-based cybercrime network operating investment, trading, and job scams.
Sources:https://eventussecurity.com/cybersecurity/india/cyber-attacks/

June 2025

In June 2025, Zoomcar confirmed a data breach impacting 8.4 million users. Hyderabad Cyber Crime Police arrested 25 fraudsters across seven states and recovered over ₹4 crore. A ransomware attack on a Lucknow-based advertising firm encrypted its systems but operations were restored using backups.

Sources:
https://www.cm-alliance.com/cybersecurity-blog/major-cyber-attacks-ransomware-attacks-and-data-breaches-of-june-2025
https://www.thehindu.com/news/national/telangana/hyderabad-cyber-crime-unit-makes-25-arrests-in-june-recovers-over-4-crore-from-online-fraudsters/article69796504.ece
https://www.linkedin.com/posts/aikha_cybersecurity-india-databreach-activity-7348783024597028865-oecS

July 2025

In July 2025, the Lazarus Group hacked WazirX cryptocurrency exchange via smart contract vulnerabilities. ICICI Bank’s vendor portal was infected with credential-harvesting malware. CERT-In announced new cybersecurity guidelines, and the National Cybersecurity Policy 2025 entered formal review.

Sources:
https://eventussecurity.com/cybersecurity/india/cyber-attacks/
https://eventussecurity.com/cybersecurity/india/cyber-attacks/
https://strobes.co/blog/new-cert-in-guidelines-2025-what-every-security-team-needs-to-act-on-now/
https://www.cybersecurityinstitute.in/blog/indian-governments-new-cybersecurity-policy-explained-simply

August 2025

By August 2025, cybercrime cases crossed 12 lakh nationwide, with Maharashtra and Uttar Pradesh worst affected. Telangana reported a decline in cyber fraud losses to ₹681 crore due to public awareness campaigns.

Sources:
https://www.indiatoday.in/india/story/over-12-lakh-cybercrimes-have-already-been-reported-in-india-up-to-june-30-this-year-with-maharashtra-being-the-worst-affected-2764903-2025-08-01
https://timesofindia.indiatimes.com/business/cybersecurity/telangana-sees-cyber-fraud-dip-losses-down-to-rs-681-crore-cyber-bureau-attributes-fall-to-increased-public-awareness/articleshow/123276106.cms

September 2025

In September 2025, amendments to the Allocation of Business Rules clarified cybersecurity responsibilities across ministries and designated the NSCS as the nodal coordinating authority.

Source:
https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

October 2025

October 2025 witnessed major cybercrime crackdowns and new national cybersecurity reforms. Hyderabad Cyber Crime Police arrested 55 individuals across eight states and refunded ₹62 lakh to victims. Delhi residents lost nearly ₹1,000 crore to scams involving investment frauds, digital arrests, and spoofed boss scams. The Union Budget 2025–26 allocated ₹782 crore for cybersecurity projects, SIM blockage, and IMEI deactivation for fraud control. The government also introduced the Promotion and Regulation of Online Gaming Bill 2025.

A major regulatory update this month was the Telecommunications (Telecom Cyber Security) Amendment Rules, 2025, notified on October 22. These rules introduced the Mobile Number Verification (MNV) Platform for validating mobile numbers used in digital services such as banking and e-commerce. The rules mandated IMEI scrubbing, continuous cybersecurity hardening, and placed compliance obligations on Telecom Identifier User Entities to prevent unauthorized access and cyber fraud.

Sources:
https://www.thehindu.com/news/national/telangana/in-cyber-crime-arrests-across-8-states-62-lakh-refunded-to-victims-in-october/article70252485.ece
https://www.tribuneindia.com/news/delhi/delhiites-lose-rs-1000-crore-to-cyber-frauds-in-2025/
https://etedge-insights.com/technology/cyber-security/the-future-of-cybersecurity-is-india-ready-to-protect-its-digital-future/

November 2025

November 2025 saw major cyber fraud busts alongside significant data protection regulatory advances. Police in Puducherry arrested engineering students running a ₹90-crore investment scam, and Hyderabad Police conducted multiple out-of-state arrests connected to digital arrest, trading, and investment scams.

A landmark development this month was the notification of the Digital Personal Data Protection (DPDP) Rules 2025 on November 14. The rules operationalize the 2023 DPDP Act and mandate data minimization, explicit consent for processing, a 72-hour data breach reporting requirement, and a phased implementation timeline. The rules also formalize the establishment of the Data Protection Board, introduce Consent Manager registration requirements, and set compliance deadlines ranging from 12 to 18 months.

Sources:
https://www.ndtv.com/topic/cyber-crime-in-india
https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf
https://www.reuters.com/sustainability/boards-policy-regulation/india-strengthens-privacy-law-with-new-data-collection-rules-2025-11-14/
https://www.india-briefing.com/news/dpdp-rules-2025-india-data-protection-law-compliance-40769.html/

December 2025 (up to 6th)

In early December 2025, the Supreme Court ordered a nationwide CBI probe into digital arrest scams and questioned the RBI on AI-based account freezing. The Telecom Ministry mandated the Sanchar Saathi app on smartphones. Updated TCS Amendment Rules enforced continuous SIM authentication and automatic messaging app logouts.

Sources:

https://kashmirobserver.net/2025/12/01/sc-orders-cbi-probe-nationwide-into-digital-arrest-cases/
https://www.theguardian.com/technology/2025/dec/01/india-phone-sanchar-saathi-app-cybersecurity
https://www.india-briefing.com/news/india-tcs-rules-2025-sim-verification-messaging-apps-41022.html/

K-12 CYBERSECURITY EDUCATION FRAMEWORK

Methodology for Grooming Young Digital Citizens

Why K-12 Cybersecurity Education Matters

Children are growing up in a world where cyber threats are as real as physical dangers. Yet, while we teach them to look both ways before crossing the street, we often fail to teach them to verify before clicking links. My K-12 framework addresses this critical gap by building cybersecurity awareness from kindergarten through high school.

Age-Appropriate Learning Pathways

Stage 1: Foundation Years (Kindergarten - Grade 2, Ages 5-7)

Learning Objective: Build basic digital awareness and introduce concept of online safety through play

Core Concepts	Teaching Methods	Activities
• Personal information is private • Screen time limits • Ask before clicking • Stranger danger online	• Storytelling with cyber heroes • Animated videos • Role-play scenarios • Coloring books	• Create a 'Cyber Safety Superhero' character • Make posters: What is private • Practice asking permission

□ Teaching Tip for Grades K-2:

Use the 'Traffic Light' Rule:
Green = Safe websites (educational games approved by parents),
Yellow = Ask First (new games or websites),
Red = Never Go (pop-ups, ads, stranger messages). Make colorful traffic light posters for the classroom.

Stage 2: Building Blocks (Grades 3-5, Ages 8-10)

Learning Objective: Develop critical thinking about online content and understand basic password security

Core Concepts	Teaching Methods	Activities
• Strong passwords • Identifying fake news • Cyberbullying awareness	• Interactive quizzes • Group discussions • Real-world examples • Hands-on practice	• Password strength contest • Spot the fake news game

Core Concepts	Teaching Methods	Activities
• Digital footprint basics		• Create digital citizenship poster • Practice saying 'no' to strangers online

□ Teaching Tip for Grades 3-5:

The 'Passphrase Power' Exercise: Instead of teaching complex passwords like 'P@ssw0rd!', teach passphrases. Example: 'MyDogRockyLoves2PlayFootball!' - Easy to remember, hard to crack. Have students create their own using favorite things, then test strength using visual meters.

Stage 3: Critical Awareness (Grades 6-8, Ages 11-13)

Learning Objective: Understand cyber threats, social media safety, and responsible digital citizenship

Core Concepts	Teaching Methods	Activities
• Phishing recognition • Social media privacy • Two-factor authentication • Malware awareness • Online reputation management	• Case study analysis • Simulated phishing exercises • Peer education projects • Guest speakers (cyber experts)	• Spot the phishing email challenge • Privacy settings audit on own social media • Create awareness videos for younger students • Cybersecurity club formation

□ Teaching Tip for Grades 6-8:

The 'Phishing Lab' Exercise: Create fake phishing emails (clearly marked as educational) and have students analyze them. What makes it suspicious? Check sender email, hover over links without clicking, look for urgency tactics, check for spelling errors. Then, students create their own 'awareness phishing email' to teach family members. This transforms them from potential victims to cyber defenders.

Stage 4: Advanced Digital Citizenship (Grades 9-12, Ages 14-18)

Learning Objective: Master cybersecurity fundamentals, explore career pathways, become community cyber ambassadors

Core Concepts	Teaching Methods	Activities
• Encryption basics • VPN usage • Ethical hacking intro • Financial cybersecurity • Cyber law awareness • AI threats understanding	• Technical workshops • Capture The Flag competitions • Industry internships • Research projects • Career counseling sessions	• Set up secure home network • Conduct security audit for family • Lead awareness campaign in community

Core Concepts	Teaching Methods	Activities
		• Participate in cybersecurity olympiads • Mentor younger students

□ Dr. Chibber's Teaching Tip for Grades 9-12:

The 'Family Cyber Guardian' Project: Each high school student becomes the cybersecurity consultant for their family. They conduct a complete security audit: check all devices, update passwords, enable 2FA, install antivirus, train family members on scams. They submit a report documenting what they found and fixed. This project has real-world impact—many students have prevented their families from falling victim to scams.

Implementation Guide for Teachers & Schools

Monthly Cyber Awareness Calendar

Integrate cybersecurity education throughout the academic year:

- **August - Digital Citizenship Month:** Start year with basic online safety rules
- **September - Password Power:** School-wide password strength challenge
- **October - Cyberbullying Awareness:** Coincide with national anti-bullying campaigns
- **November - Phishing Prevention:** Teach email and message safety
- **December - Safe Online Shopping:** Holiday season scam awareness
- **January - Privacy Settings:** New year, new privacy check
- **February - Data Protection Day (Jan 28):** Celebrate with awareness activities
- **March - Social Media Safety:** Review what to share, what to keep private
- **April - Malware Awareness:** Teach about viruses, trojans, ransomware

Classroom Resources & Tools

- **Free Educational Platforms:** Common Sense Media, Google's Be Internet Awesome, Cybersmart India
- **Simulation Tools:** Phishing awareness platforms, password strength checkers
- **Hands-On Activities:** Cybersecurity board games, coding projects, awareness poster contests
- **Assessment Methods:** Quizzes, practical demonstrations, project-based learning

Parent Engagement Strategies

Cybersecurity education works best when reinforced at home:

- **Parent Workshops:** Quarterly sessions on monitoring children's online activity
- **Family Homework:** Students teach parents what they learned in class
- **Newsletter Tips:** Monthly cyber safety tips in school communications
- **Parent-Child Contracts:** Collaborative agreements on screen time and online behavior

Few Success Stories

Case Study 1: The Student Who Saved Her Grandmother

After attending my Grade 7 workshop, 12-year-old Priya recognized a digital arrest scam call targeting her 68-year-old grandmother. She immediately disconnected the call, explained it was a scam, and helped her grandmother report it to cyber police. The scammers were demanding ₹5 lakh. Priya's knowledge saved her family from financial ruin.

Case Study 2: The High School Cybersecurity Club

A Delhi school implemented my Grade 9-12 curriculum and formed a Cybersecurity Club. Twenty students became certified Cyber Ambassadors. They conducted 40+ awareness sessions reaching 2,000+ community members. Three students went on to win national cybersecurity competitions. Five are now pursuing cybersecurity engineering degrees.

Case Study 3: The Primary School Digital Citizenship Program

A Mumbai school integrated my K-2 framework. Within one semester, 95% of students could identify what information is private, 87% asked parents before clicking links, and cyberbullying incidents dropped by 60%. Parents reported children teaching them about password safety.

CITIZEN PROTECTION GUIDE

Digital Arrest Scam - Complete Awareness

Based on verified reports from Supreme Court proceedings and government data, digital arrest scams have claimed ₹3,000 crore from Indian citizens in 2025. Understanding this scam is critical for everyone.

SCAMMERS SAY	THE TRUTH
Police will call you for video investigation	**NO agency EVER conducts phone/video investigations**
Digital arrest is legal procedure	**NO such legal concept exists in India**
Transfer money to prove innocence	**NO government EVER asks for money transfers**
Your Aadhaar/documents used in crime	**If true, police visit in person with warrant**

IMMEDIATE ACTION IF CONTACTED

- **DISCONNECT IMMEDIATELY:** Hang up. Do not engage.
- **DO NOT TRANSFER MONEY:** Under ANY circumstance
- **Call Helpline 1930:** National Cybercrime Helpline immediately
- **Tell Family:** Warn others, especially elderly
- **Report Online:** Visit www.cybercrime.gov.in

Emergency Helplines & Resources

Purpose	Contact	Available
Cybercrime Reporting	**1930**	24x7
Online Complaint Portal	cybercrime.gov.in	24x7
Child Safety	**1098**	24x7
Women Helpline	**181**	24x7

CONCLUSION - BUILDING A CYBER-SAFE INDIA

As we've journeyed through the cybersecurity landscape of 2025, one truth emerges clearly, knowledge is our most powerful defense. From the 369 million malware detections to the ₹20,000 crore stolen from citizens, the threats are real and growing. But so is our collective capacity to protect ourselves.

The Power of K-12 Education

By integrating cybersecurity education from kindergarten through high school, we're not just teaching children to be safe—we're cultivating a generation of digital citizens who will build a safer India. Every student who learns to spot a phishing email becomes a protector for their entire family. Every teenager who understands AI threats becomes an ambassador for their community.

My Commitment Continues

As a Principal, Author, Mentor, and Researcher, I remain committed to reaching every corner of India with cybersecurity awareness. This report is freely available for schools, institutions, community organizations, and individuals. Use it, share it, teach from it.

Call to Action

- **Educators:** Implement the K-12 framework in your schools
- **Parents:** Reinforce cyber safety lessons at home
- **Students:** Become cyber ambassadors for your families and communities
- **Citizens:** Share this knowledge, especially with vulnerable populations
- **Organizations:** Support cybersecurity awareness programs

My Promise to You

I promise to make cybersecurity education accessible, actionable, and anxiety-free. Whether you're a parent wanting to protect your child, a teacher seeking curriculum resources, or a young student curious about staying safe online, this report is for you.

Together, we can build a generation of cyber-aware Indians who use technology confidently and safely.

With dedication to your digital safety!

Together, We Build A Cyber-Safe India

End of Report