

REPORT

ON

National Level Cyber Security Awareness Programme “Cyber Shield”

National Awareness Drive for Secure Digital Futures

REGISTRATION WINDOW	14 August 2026 to 15 September 2026
DURATION	33 days — self-paced online learning
MODE	Online (AACST Learning Hub, self-paced)
ACCESS	Learn 24×7, anytime and anywhere
FEE	Completely free — open to everyone
TOTAL LEARNERS	312 registered learners across 6 States

1. PROGRAMME OVERVIEW

Cyber Shield — National Awareness Drive for Secure Digital Futures was conceived by the Association of All Computer Science Teachers (AACST) as an open, self-paced national awareness initiative addressing the rapidly escalating landscape of cyber threats, online frauds and AI-enabled deception. Unlike a fixed-schedule webinar, the drive was delivered through the AACST Learning Hub as a self-paced online programme, allowing every learner to complete the modules 24×7 at a time and place of their own choosing. The drive remained open for registration from **14 August 2026 to 15 September 2026**, a continuous window of 33 days, offered entirely free of cost with no eligibility restriction of age, qualification or profession, and an e-certificate was awarded to every learner on successful completion.

312 LEARNERS REGISTERED	33 DAYS OF OPEN ACCESS	6 STATES & UTS REACHED	100% FREE OF COST
-----------------------------------	----------------------------------	----------------------------------	-----------------------------

2. ORGANISING BODY

ROLE	DETAILS
Organised by	Association of All Computer Science Teachers (AACST)
Patron, Mentor & Convener	Dr. Abha Khandelwal — Founder, AACST; Retd. HOD, Computer Science, Hislop College, Nagpur
President, AACST	Dr. S. B. Kishor — HOD, Computer Science, S. P. College, Chandrapur
Coordinator	Dr. Praveen Ghosekar — Secretary, AACST; HOD, Computer Science, J. M. Patel College, Bhandara
Resource Persons	Dr. Abha Khandelwal — Founder, AACST; Retd. HOD, Computer Science, Hislop College, Nagpur Dr. Praveen Ghosekar — Secretary, AACST; HOD, Computer Science, J. M. Patel College, Bhandara Dr. Shweta Shirpurkar — HOD, Computer Science, Mohta Science College, Nagpur

3. OBJECTIVES OF THE DRIVE

- To create nationwide awareness about cyber crimes, digital frauds and emerging online risks.
- To educate citizens on safe, responsible and ethical digital practices.
- To build recognition of AI-enabled threats such as deepfakes and voice cloning.
- To promote cyber hygiene, data protection and privacy awareness in everyday digital life.
- To make quality cyber-awareness education freely accessible, self-paced and barrier-free.
- To move towards a cyber-aware, resilient and digitally secure society.

4. CURRICULUM COVERED

The self-paced modules addressed the threat categories most frequently encountered by Indian citizens today, combining conceptual grounding with real-life case studies and practical countermeasures:

- Digital Arrest Frauds
- AI Voice Cloning & Deepfakes
- OTP & UPI Scams
- Identity Theft & Fake Profiles
- Social Engineering Attacks
- Cyberbullying & Online Fraud
- Digital Footprints & Privacy Protection
- Everyday Cyber Hygiene Practices

5. PARTICIPATION & OUTREACH ANALYSIS

A total of **312 registrations** were recorded during the 33-day window, representing **308 unique email addresses**. Registrations were received on **24 of the 33 days**, giving an overall average of **9.5 registrations per day** and **13.0 per active day**.

5.1 Daily Registration Trend

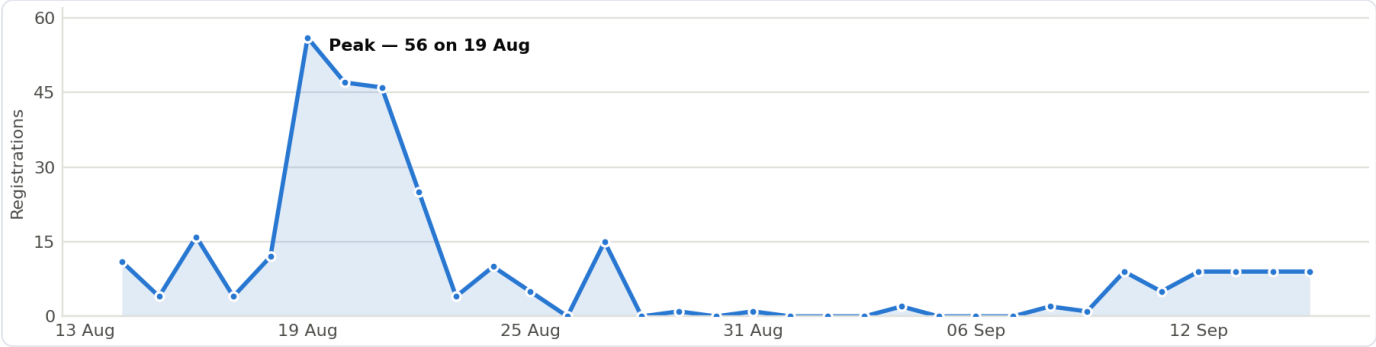


Figure 1 — Daily registrations, 14 August to 15 September 2026. Days with no registration are shown at zero.

Enrolment rose sharply within the first week of promotion, peaking at **56 registrations on 19 August 2026** — the single highest day of the drive. The three-day period from 19 to 21 August alone accounted for 149 registrations, or 47.8% of the entire drive, indicating a strong and immediate response to the promotional campaign.

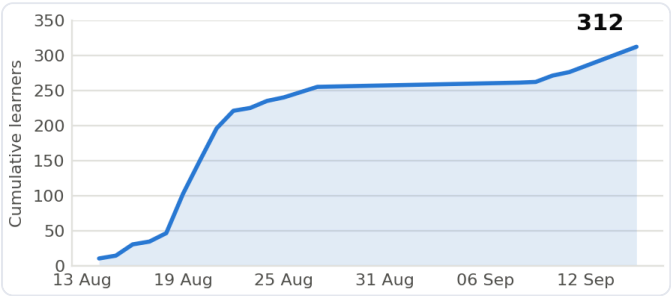


Figure 2 — Cumulative learner enrolment.

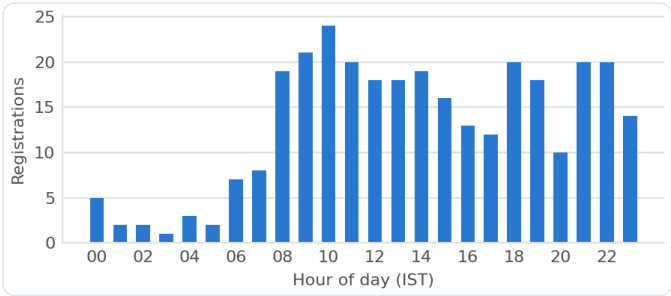


Figure 3 — Registrations by hour of day (IST).

Registrations were spread across the full day, with clear activity peaks in the mid-morning (09:00–12:00) and evening (18:00–23:00) periods. This distribution validates the self-paced, 24×7 design of the drive: learners engaged outside conventional programme hours, which a fixed-schedule webinar would not have accommodated.

5.2 Phase-wise Distribution

PHASE	PERIOD	LEARNERS	SHARE
Launch & peak uptake	14 Aug - 22 Aug 2026	221	70.8%
Sustained enrolment	23 Aug - 31 Aug 2026	36	11.5%
Closing surge	01 Sep - 15 Sep 2026	55	17.6%
Total		312	100.0%

5.3 State-wise Participation

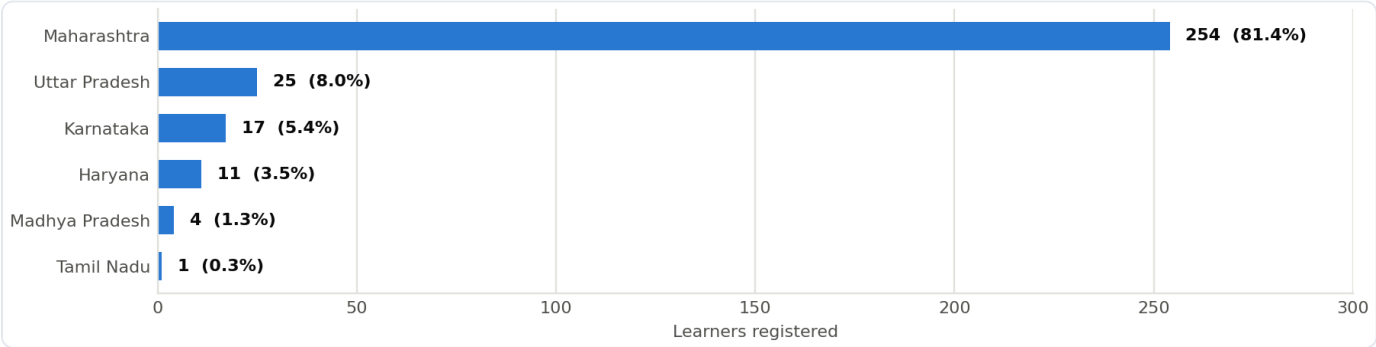


Figure 4 — Learners registered by State / Union Territory.

#	STATE / UNION TERRITORY	LEARNERS	SHARE
1	Maharashtra	254	81.4%
2	Uttar Pradesh	25	8.0%
3	Karnataka	17	5.4%
4	Haryana	11	3.5%
5	Madhya Pradesh	4	1.3%
6	Tamil Nadu	1	0.3%
Total		312	100.0%

Participation was drawn from **six States**, led by Maharashtra with 254 learners (81.4%), followed by Uttar Pradesh (25), Karnataka (17), Haryana (11), Madhya Pradesh (4) and Tamil Nadu (1). The concentration in Maharashtra reflects AACST's established institutional network in the region, while enrolments from five further States confirm that the drive achieved genuine cross-regional reach.

6. KEY HIGHLIGHTS

- 312 learners enrolled in a completely free, open-to-all national drive.
- Sustained 33-day access window with no fixed timing constraint.
- Peak single-day enrolment of 56 learners on 19 August 2026.
- Reach extended across six States, from Maharashtra to Tamil Nadu.
- Coverage of contemporary AI-driven threats including deepfakes and voice cloning.
- E-certification awarded on successful completion, at no cost to the learner.

7. LEARNING OUTCOMES

On completion of the drive, learners were able to:

- Recognise the principal categories of cyber threat and digital fraud in circulation today.
- Identify and resist online scams, including OTP, UPI and digital-arrest frauds.
- Detect AI-generated deception such as deepfake video and cloned voice calls.
- Apply practical safe-digital-practice habits in daily personal and professional use.
- Protect personal, financial and health data against unauthorised access.
- Understand and manage their own digital footprint and privacy exposure.

8. CERTIFICATION

An e-certificate was awarded to every learner who successfully completed the drive. In keeping with the instruction published on the programme flyer and brochure, learners were advised at the point of registration to enter their login name exactly as they wished it to appear on the certificate, which ensured accuracy of records and minimised post-issue correction requests.

9. OBSERVATIONS & RECOMMENDATIONS

Observation. Nearly half of all registrations (47.8%) arrived in a three-day burst immediately following the promotional push, after which daily enrolment declined steeply before recovering modestly in the closing fortnight.

- **Stagger promotion.** A second and third promotional wave, scheduled mid-window, would sustain enrolment through the quieter period observed between 23 August and 09 September.
- **Broaden geographic outreach.** With 81.4% of learners from a single State, targeted outreach to teacher associations and institutions in under-represented States would materially widen national coverage.
- **Engage institutions directly.** Only two registrations used an institutional email domain; the remainder were personal accounts. Partnering with colleges for cohort-level enrolment would raise both volume and completion rates.

- **Validate email at entry.** The register contains four duplicate addresses and at least one mistyped domain. A simple format check and confirmation step at registration would protect certificate delivery.
- **Retain the self-paced format.** The spread of registration activity across all hours confirms that flexible access materially widened participation.
- **Capture richer learner data.** Recording city, age band and occupation at registration would enable finer demographic reporting in future drives.

10. CONCLUSION

The Cyber Shield National Awareness Drive achieved its objective of delivering free, accessible and practically useful cyber-security awareness to citizens across India. Over a 33-day window it brought 312 learners from six States into structured engagement with the most pressing digital threats of the present moment — digital arrest frauds, UPI and OTP scams, identity theft and AI-enabled deception — without financial, scheduling or eligibility barriers of any kind. The drive demonstrates that a self-paced, zero-cost, openly accessible model can carry cyber awareness well beyond the conventional academic audience, and stands as a meaningful step towards AACST’s continuing mission of building a cyber-aware, responsible and digitally secure society.

ANNEXURE — DAY-WISE REGISTRATION RECORD

Days on which no registration was received are omitted from the table below.

DATE	LEARNERS	DATE	LEARNERS	DATE	LEARNERS
14 Aug	11	22 Aug	25	08 Sep	2
15 Aug	4	23 Aug	4	09 Sep	1
16 Aug	16	24 Aug	10	10 Sep	9
17 Aug	4	25 Aug	5	11 Sep	5
18 Aug	12	27 Aug	15	12 Sep	9
19 Aug	56	29 Aug	1	13 Sep	9
20 Aug	47	31 Aug	1	14 Sep	9
21 Aug	46	04 Sep	2	15 Sep	9

11. GLIMPSES

A visual record of the Cyber Shield National Awareness Drive — campaign outreach, learning modules and learner participation.

CYBER SHIELD

National Awareness Drive for Secure Digital Futures
(14 August 2026 — 15 September 2026)

Deepfake Voice Scam — AI voice cloning case study

Victim Profile — who cyber fraud targets

Cyber SMART — safe practices for young users

Digital Footprints — a permanent trail

Case Studies on Digital & Cyber Frauds

Expert session in progress for participants

Empowering Minds. Securing Digital Futures.

aacst.org

Expert sessions of the Cyber Shield drive — deepfake voice-cloning case study, victim profiling, safe-practice guidance for young users, digital footprints, and real-world cyber-fraud case studies.

HOSTED ON
AACST Learning Hub — programsandevents.aacst.org

PREPARED BY
AACST Editorial Team