

INTERNSHIP SYLLABUS

Cyber Security

A 90-hour field internship for undergraduate students, delivered in four stages: recorded lectures, an online assessment, geotagged field work, and a marked report. 6 modules, 4 of them in the field.

01	How the digital world works, and how it is attacked	CONCEPTUAL
02	Passwords, two-factor authentication, devices and accounts	FIELD
03	Safe digital payments and the anatomy of financial fraud	FIELD
04	Law, privacy, social media and reporting	CONCEPTUAL
05	Malware, backups and the small-business security checklist	FIELD
06	Running community cyber-awareness sessions	FIELD



EthnoMedico
— Agro Botanical Research Society

CYBER SECURITY

Part I: Programme document

1. Why this subject, why now

Almost every student in a Bihar college now carries a smartphone that holds a bank account, an Aadhaar-linked identity, a social life and a study life. The same is true of their parents, their village shopkeepers and their grandparents. The people who defraud them do not need to break into a computer. They need a phone call, a convincing message and a moment of panic.

The scale is documented. In a written reply to the Lok Sabha, the Ministry of Home Affairs reported that losses from cyber fraud complaints reached Rs 22,845.73 crore in 2024, against Rs 7,465.18 crore in 2023, with 36.37 lakh complaints received across the National Cyber Crime Reporting Portal and the 1930 helpline in 2024. The National Crime Records Bureau's Crime in India 2023 recorded more than 86,000 cyber crime cases, a rise of 31.2 per cent over 2022, driven mainly by cheating by personation. The Department of Telecommunications told the Rajya Sabha in February 2026 that citizens had filed 7.7 lakh reports of suspected fraud communication through the Chakshu facility, and that 39.43 lakh mobile connections had been disconnected on the basis of such inputs.

Behind these numbers are the cases every district knows: the OTP shared with a "bank officer", the UPI "collect request" that drained a savings account, the fake work-from-home job that asked for a registration fee, the video call from a "CBI officer" that ended in a "digital arrest", and the sextortion call that a young person was too ashamed to report.

Government has built a defence: the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs, the National Cyber Crime Reporting Portal at cybercrime.gov.in, the 1930 helpline, CERT-In's advisories and the Cyber Swachhta Kendra, the Sanchar Saathi portal, and now a data protection law in force. What is missing is the last mile: someone in every mohalla and every panchayat who understands these tools and can explain them in Magahi, Maithili, Bhojpuri or Hindi. This internship trains undergraduates from every stream to be that person, and gives them the evidence that they did it.

The subject is defensive throughout. Students learn how attacks work in order to recognise and prevent them. No offensive tooling, scanning or "ethical hacking" is taught or permitted.

2. Who it is for, and outcomes

Eligible streams: all undergraduate streams of the partner universities. No computer science background is assumed. A student needs a smartphone, a working data connection for the portal, and the willingness to talk to strangers respectfully.

Prerequisites: none.

Learning outcomes. On completing the internship, a student will be able to:

1. Describe how a phone, a network and a website exchange data, and where in that chain a fraud usually happens. (Understand)
2. Identify the common Indian fraud patterns (UPI and OTP fraud, phishing and vishing, fake job and investment offers, digital arrest, sextortion, SIM swap) from their warning signs. (Analyse)
3. Configure strong passwords, two-factor authentication, screen locks, app permissions and privacy settings on Android and on common Indian apps, for themselves and for others. (Apply)
4. Explain the citizen's rights and duties under the IT Act 2000 as amended, the DPDP Act 2023 and the Bharatiya Nyaya Sanhita provisions on cheating, in plain language. (Understand)
5. Guide a victim through reporting on the 1930 helpline, cybercrime.gov.in, Sanchar Saathi and the bank, within the time limits that protect the victim's money. (Apply)
6. Audit the basic security practices of a small business using a checklist, and recommend no-cost improvements. (Evaluate)
7. Design a local-language awareness message or poster, test it with the audience and revise it. (Create)
8. Plan, deliver and document a community cyber-safety session and write a structured report on it. (Create)



3. At a glance

MODULE	TITLE	TYPE	HOURS	FIELD TASK IN ONE LINE
1	How the digital world works, and how it is attacked	Conceptual	15	None (written reflection)
2	Passwords, two-factor authentication, devices and accounts	Field	15	Help five to eight elders or first-time users set up screen locks and 2FA and recognise scam calls, with consent
3	Safe digital payments and the anatomy of financial fraud	Field	15	Survey 25 traders and customers in a local market on digital-fraud experiences
4	Law, privacy, social media and reporting	Conceptual	15	None (written reflection)
5	Malware, backups and the small-business security checklist	Field	15	Checklist audit of a shop, cyber café or Common Service Centre, with the owner's consent
6	Running community cyber-awareness sessions	Field	15	Create and test a local-language poster or WhatsApp message, then run a session at a school, college or village

Total: 90 hours. Four field modules, two conceptual.

4. How the four stages apply to this subject

Stage 01 Learn. Each module has five to seven recorded lectures of 30 to 60 minutes, in Hindi with English technical terms on screen, plus written material in the portal. Lectures demonstrate settings on a real Android phone using screen recording, never on a live personal account. The portal tracks watch time; a lecture is complete at 80 per cent.

Stage 02 Test. One MCQ test per module, 20 questions, 30 minutes, single attempt, unlocked only when all lectures of the module are complete. Questions test recognition of fraud patterns and correct procedure, not memorised definitions.

Stage 03 Do. In Modules 2, 3, 5 and 6 the student goes to a real place, does the task, and uploads geotagged photographs of themselves doing it. Coordinates are checked against the assigned location. For this subject there is a rule that overrides everything else: a photograph must never show the contents of anyone's screen, a password, a PIN, an OTP, an Aadhaar number, a bank passbook, a card, a QR code that is linked to a real account, or a filled survey form with a name on it. Photographs show the student, the setting, the person being helped (with consent, from behind or side where possible), the checklist or poster, and the venue signboard.

Stage 04 Report. Each field module ends with a report of 800 to 1,200 words against the section prompts given in the module, marked on the rubric given there. Conceptual modules end with a 500-word written reflection.



5. Assessment and grading

COMPONENT	WEIGHT
Six module MCQ tests (average)	30
Field evidence, four field modules (5 each: location verified, evidence complete, safety and consent rules followed)	20
Four field module reports (7.5 each, on the module rubric)	30
Final report (Appendix A, marked on Appendix C)	20
Total	100

Grade bands: O (90 and above), A+ (80 to 89), A (70 to 79), B+ (60 to 69), B (50 to 59), C (40 to 49), F (below 40).

Passing standard: a minimum of 40 overall, every MCQ test attempted, every field Do stage verified, and no breach of the photograph rule. A single upload that shows a screen with personal data, a password or a PIN is removed and the Do stage is repeated; a second breach fails the module.

6. Field work: ethics, safety, permissions

Consent. Every person the student helps, surveys or photographs gives verbal consent after hearing, in their own language, who the student is, what the internship is, and that the photograph will be seen by the university and the Society. Minors are only involved in the Module 6 school session, with the head teacher's written permission and with no individual child identifiable in a photograph. Nobody is photographed against their will, and a refusal ends the interaction politely.

Never handle another person's credentials. The student guides; the owner types. The student never asks for, sees, writes down or photographs a password, PIN, OTP, CVV or Aadhaar number. If a person offers it, the student refuses and explains why the refusal is itself the lesson. The student never installs an app on someone else's phone from a link, and never uses a remote access app.

No scanning, no testing. The Module 5 audit is a conversation and a checklist. The student does not attempt to connect to the shop's Wi-Fi without permission, run any scanning tool, probe any device or "test" anyone's security. Doing so is an offence under the IT Act and results in immediate failure.

Safety. Field work is done in daylight, in public or semi-public spaces, with the location shared with a family member. Students go in pairs where possible. If a respondent becomes distressed while describing a fraud, the student stops the interview, offers the 1930 number and the portal address, and does not press. Students carry a college ID and a signed letter from the Society.

Who to inform before a visit. The principal or head teacher for a school or college session; the mukhiya or ward member for a village session; the owner for a shop, cyber café or CSC; the market association or the nearest thana where a market survey may draw a crowd. The Society's field coordinator is informed of every date and location in advance through the portal.



7. Final report format

The final report is 2,500 to 3,500 words following Appendix A. It has a cover page, a one-page summary, one section per field module (what was done, where, what was found, what changed), a section on the law and reporting pathway as the student would now explain it to a neighbour, a reflection on what the student would do differently, and an annexe with the four evidence checklists (Appendix B) signed by the student. Appendix C is the rubric.

8. Skills built and career pathways (India)

The internship builds skills that every employer now expects and that most graduates do not have evidence of: secure account and device management, the ability to explain risk to a non-technical audience, structured observation with a checklist, survey design and analysis, and written reporting.

Pathways in India that this internship opens or supports:

- **Banking and payments:** fraud awareness, customer protection and grievance roles at banks, small finance banks, payment companies and business correspondents, where knowledge of the RBI customer liability rules and the 1930 process is directly relevant.
- **Common Service Centres and Digital India roles:** Village Level Entrepreneurs and their staff, who already deliver digital services in every block of Bihar, need exactly this competency.
- **Government awareness programmes:** ISEA's Cyber Aware Digital Naagrik programme, state police awareness drives and school outreach recruit trained volunteers and master trainers.
- **Formal skilling:** the NSDC and IT-ITeS SSC (NASSCOM) qualification "Security Analyst" (NQR code QG-05-IT-01538-2023-V1.1-NASSCOM, NSQF Level 5) is a 480-hour programme whose first unit, "Contribute to managing information security", starts from the hygiene and policy awareness this internship teaches. Students from any stream can present this internship as relevant experience when applying.
- **Teaching and social work:** school teachers, anganwadi supervisors, NGO field staff and panchayat facilitators are all now expected to hold cyber-safety sessions.
- **Further study:** the NIST NICE Framework's work role categories, especially Oversight and Governance and Protection and Defense, show students that non-programming roles exist in cybersecurity: policy, awareness, compliance, investigation support.

9. Alignment: NEP 2020, UGC internship guidelines, NAAC criteria, SDGs

- **NEP 2020** calls for experiential learning, community engagement, digital literacy and skill-based education across disciplines. This internship delivers all four in one 90-hour unit and is designed for students of every stream, in line with the multidisciplinary intent of the policy.
- **UGC internship guidelines** under the National Higher Education Qualifications Framework and the Curriculum and Credit Framework for Undergraduate Programmes require a mandatory internship of 60 to 120 hours worth 2 to 4 credits. This 90-hour programme, with verifiable field evidence and a graded certificate, satisfies that requirement.
- **NAAC criteria:** Criterion 1 (curricular aspects: skill and field integration), Criterion 3 (research and extension: extension activities with community impact), Criterion 5 (student support and progression: career-relevant skills), and Criterion 7 (institutional values: outreach and inclusion).
- **SDGs:** SDG 4 (quality education, target 4.4 on relevant skills), SDG 8 (decent work), SDG 9 (target 9.c, access to ICT), SDG 10 (reduced inequalities, since fraud hits the poor and the elderly hardest) and SDG 16 (target 16.3, access to justice, through reporting pathways).

10. Benchmarks consulted

The module list and competencies were built against the following, and adapted as noted.

- **MeitY's Information Security Education and Awareness (ISEA) programme** (isea.gov.in, staysafeonline.in and infosecawareness.in, run by C-DAC Hyderabad). ISEA is in its third phase from October 2023 and runs the Cyber Aware Digital Naagrik mass awareness programme with role-based tracks for children, students, women, parents, teachers, senior citizens, government employees, NGOs, CSCs and MSMEs, in eleven Indian languages. Adapted: the audience-based structure of Modules 2 and 6, the use of ISEA's Hindi and other regional-language posters as starting material, and the "pledge" format for community sessions.
- **CERT-In Cyber Security Awareness Booklet for Digital Nagriks and Digital Enterprises** (National Cyber Security Awareness Month 2023, cert-in.org.in). Its chapters (phishing, vishing, malicious mobile applications, malware, social media frauds, attacks targeting senior citizens, children, women, persons with disability and organisations, password safety, basic hygiene, reporting to CERT-In and I4C) map almost one to one onto Modules 1, 2, 4 and 5. Adapted: the "key signs of malware" list and the safety tips per audience.
- **Cyber Swachhta Kendra** (csk.gov.in), the Botnet Cleaning and Malware Analysis Centre operated by CERT-In under Section 70B of the IT Act, with free bot removal tools from eScan, K7 and Quick Heal, and the M-Kavach 2, USB Pratirodh, AppSamvid and Browser JSGuard tools. Adapted: Module 5's "free tools first" approach for small businesses.
- **RBI's customer protection circular on limiting liability in unauthorised electronic banking transactions** (6 July 2017, RBI/2017-18/15) and RBI's 2025 announcement of the exclusive bank.in domain, with IDRBT as registrar, to cut phishing. NPCI's published UPI safety messages (never share UPI PIN, no PIN is needed to receive money, check the payee name). Adapted: Module 3's "three working days" reporting rule and the "receive money needs no PIN" teaching point.
- **NSDC and IT-ITeS SSC (NASSCOM) qualification file: Security Analyst**, NSQF Level 5, National Qualification Register (nqr.gov.in). Its National Occupational Standards SSC/N0901 to SSC/N0905 (managing information



security, coordinating incident response, configuring security devices, contributing to and supporting audits) are professional-level; this internship takes the entry-level awareness, policy and audit-support competencies only. Adapted: the checklist audit in Module 5 as a citizen-level version of "contribute to information security audits".

- **NIST NICE Workforce Framework for Cybersecurity** (NIST SP 800-181 Rev. 1; components on the NICE Framework Resource Center and NICCS). Its Task, Knowledge and Skill statements, and the work role categories Oversight and Governance, Design and Development, Implementation and Operation, Protection and Defense and Investigation. Adapted: the outcomes in Section 2 are written as knowledge and skill statements in the NICE style, and Section 8 uses the categories to show non-technical pathways.
- **UK NCSC Cyber Aware** (ncsc.gov.uk/cyberaware): six actions, namely a strong and separate email password, three random words for passwords, software updates, two-step verification, password managers and backups. **CISA Secure Our World** (cisa.gov/secure-our-world): strong passwords and a password manager, multifactor authentication, recognise and report phishing, update software. Adapted: the six NCSC actions and the four CISA steps were merged into the Module 2 "six habits" list and Indianised (Hindi passphrases, SMS OTP realities, shared family phones).
- **CompTIA IT Fundamentals (ITF+) FC0-U61 exam objectives**, Domain 6.0 Security (20 per cent of the exam): confidentiality, integrity and availability, device security, behavioural security, authentication and authorisation, password practices, encryption and business continuity. Adapted: the network and web basics in Module 1 and the "CIA triad" framing, taught at a non-technical depth.
- **I4C advisories** (i4c.mha.gov.in/advisories.aspx), including Digital Arrest based cybercrime in India (6 March 2025), Rise in Fake Captcha Filling Jobs cybercrime (8 April 2025), the fake job racket advisory (27 June 2024), and the 2021 and 2022 advisories on QR code tampering, fake customer care numbers, KBC lottery frauds, part-time job frauds, romance frauds and WhatsApp account hacking. Adapted: these are the case studies of Modules 1 and 3.

CYBER SECURITY

Part II: Modules



MODULE 1

How the digital world works, and how it is attacked

CONCEPTUAL

15 HOURS

Overview and learning outcomes

This module gives a non-technical student an accurate mental model of what happens when they tap "Pay" or open a link, and then walks through the fraud patterns that exploit that chain in India. By the end, the student can explain the CIA triad, read a URL, name the parts of a phone call scam, and describe eight Indian fraud patterns with their warning signs.

Hour allocation

Learn 12 hours (seven lectures, 5.5 hours; reading 6.5 hours). Test 1 hour. Written reflection 2 hours.

STAGE 01 · LEARN

LECTURES

1. **What security means: confidentiality, integrity, availability** (40 min). The CIA triad with Indian examples (a leaked Aadhaar scan, a changed bank IFSC on an invoice, a ransomware-locked hospital). Assets, threats, vulnerabilities and risk in plain words. Why "I have nothing to hide" is wrong: your account is a mule account waiting to happen. The attacker's economics: cheap, remote, repeatable.
2. **How a phone talks to the internet** (45 min). SIM, IMEI and the mobile network. IP addresses, DNS and what a URL is. What a browser does. HTTP versus HTTPS and what the padlock does and does not promise. Wi-Fi at home and in a cyber café. Why the mobile number is now the master key to identity in India.
- 3.

How the web and apps work (45 min). Client, server, request and response. Cookies and sessions: why "stay logged in" matters. App permissions on Android: what "accessibility", "SMS", "contacts" and "install unknown apps" actually grant. The Play Store, Play Protect and side-loaded APKs. Why the bank never needs you to install an app "for verification".

4. **Social engineering: the human exploit** (50 min). Authority, urgency, fear, greed and helpfulness as levers. The scam call script, step by step. Caller ID spoofing. Vishing, smishing and phishing. The "digital arrest": impersonation, intimidation, digital confinement and extortion, and the I4C statement that no such thing as a digital arrest exists in Indian law.
5. **Financial fraud patterns in India, part one** (50 min). OTP fraud, UPI collect-request fraud, fake customer-care numbers found through search engines, QR code tampering, KYC-update and electricity-bill SMS fraud, SIM swap. Warning signs of each. What the money trail looks like: mule accounts and the I4C Suspect Registry.
6. **Financial fraud patterns in India, part two** (50 min). Fake job offers and registration fees, task and captcha-filling scams, investment and trading groups on Telegram and WhatsApp, matrimonial and romance frauds, lottery and KBC frauds, loan-app harassment. Why students are targeted.
7. **Harm that is not about money** (40 min). Sextortion (the video call, the recording, the demand), morphed images, account takeover of WhatsApp and Instagram, cyberstalking, and impersonation profiles. The single rule: do not pay, do not delete evidence, report.

READING MATERIAL

- Section 1: Security vocabulary in Hindi and English, with the CIA triad and the risk equation. Draws on CompTIA ITF+ Domain 6.0 and the CERT-In awareness booklet.
- Section 2: Networks and the web for non-engineers, with a diagram of a UPI payment from tap to bank. Draws on NPCI's public UPI documentation.
- Section 3: A catalogue of twelve Indian fraud patterns, each with modus operandi, warning signs and the relevant I4C advisory, quoted with date.
-



Section 4: The I4C digital arrest advisory of 6 March 2025 in summary, and CERT-In's audience-specific tips for senior citizens, children, women and persons with disability.

- Section 5: Statistics with sources: the MHA's Lok Sabha figures for 2023 and 2024, NCRB Crime in India 2023, and the DoT's Chakshu figures.

STAGE 02 · TEST

Blueprint: 20 questions, 30 minutes, single attempt. Coverage: lectures 1 to 3 (7 questions), lecture 4 (4), lectures 5 and 6 (6), lecture 7 (3).

Sample MCQs (correct answer marked with an asterisk):

Q1 The padlock icon in a browser means:

- a. the website is honest
- b. the connection to the site is encrypted**
- c. the site is registered in India
- d. the site has no malware

Q2 A caller says he is from your bank and asks you to read out the OTP to "cancel a wrong transaction".

This is:

- a. standard bank procedure
- b. vishing**
- c. a KYC update
- d. a UPI mandate



Q3 To receive money through UPI you must:

- a. enter your UPI PIN
- b. scan the sender's QR code
- c. do nothing; no PIN is needed to receive money**
- d. share your OTP

Q4 Which permission lets a malicious app read your OTPs?

- a. Camera
- b. Location
- c. SMS**
- d. Bluetooth

Q5 "Digital arrest" is:

- a. a provision of the BNSS
- b. an I4C procedure
- c. a scam with no basis in Indian law**
- d. a court-ordered house arrest



Q6 A fake job offer usually reveals itself by:

- a. asking for an interview
- b. asking for a registration or training fee**
- c. sending an offer letter by email
- d. asking for a CV

Q7 Under the CIA triad, a hospital unable to open its patient records during a ransomware attack has lost:

- a. confidentiality
- b. integrity
- c. availability**
- d. authenticity

Q8 The mobile number is the master key to identity in India mainly because:

- a. it is printed on Aadhaar
- b. OTPs and account recovery flow through it**
- c. it is public
- d. it is linked to a PAN card



Q9 In a sextortion attempt the correct first response is:

- a. pay a small amount to make them go away
- b. delete the app and the chat
- c. do not pay, keep evidence, report
- d. confront the caller

Q10 A "mule account" is:

- a. a bank account used to receive and move stolen money
- b. a dormant account
- c. a joint account
- d. an account with a frozen balance

Glossary

CIA triad; vulnerability; social engineering; phishing; vishing; smishing; spoofing; mule account; side-loading; HTTPS; DNS; IMEI.

References

- Ministry of Home Affairs, Lok Sabha written reply on cyber fraud losses 2023 and 2024, as reported:
<https://www.angelone.in/news/market-updates/cyber-fraud-costs-indians-22-845-crore-in-2024-government>
- National Crime Records Bureau, Crime in India 2023: <https://www.ncrb.gov.in/>
- I4C advisories, including Digital Arrest based cybercrime in India (6 March 2025):
<https://i4c.mha.gov.in/advisories.aspx>
-



CERT-In, Cyber Security Awareness Booklet for Digital Nagriks and Digital Enterprises:

https://www.cert-in.org.in/PDF/CSA_Booklet.pdf

- CompTIA ITF+ FC0-U61 exam objectives, Domain 6.0 Security:

<https://www.certblaster.com/wp-content/uploads/2020/03/CompTIA-IT-Fundamentals-FC0-U61-Exam-Objectives.pdf>

- Chakshu facility statistics, Rajya Sabha reply, 5 February 2026:

<https://www.tribuneindia.com/news/chakshu/chakshu-facility-of-sanchar-saathi-enables-citizens-to-report-suspected-fraud>



MODULE 2

Passwords, two-factor authentication, devices and accounts

FIELD

15 HOURS

Overview and learning outcomes

The student learns the six habits that stop most everyday attacks, practises them on their own devices, and then helps five to eight elders or first-time smartphone users do the same. By the end, the student can set up a screen lock, a strong passphrase, 2FA on Google, WhatsApp and a bank app, review app permissions, and explain each step in the local language.

Hour allocation

Learn 6 hours (six lectures, 4 hours; reading 2 hours). Test 1 hour. Do 6 hours (preparation 1 hour, on site 4 hours, upload 1 hour). Report 2 hours.

STAGE 01 · LEARN

LECTURES

1. **The six habits** (35 min). Merged from NCSC Cyber Aware and CISA Secure Our World: strong and separate email password; long passphrases (three random Hindi or English words); 2FA everywhere it is offered; update software; back up; recognise and report phishing. Why email and the mobile number are the accounts to protect first.
2. **Passwords that work for real people** (40 min). Why "Ravi@123" fails and "neem chai kursi 47" works. Reuse and credential stuffing. Password managers, including the free one built into the phone's browser. What to do with a shared family phone. Writing passwords down safely versus unsafely.



3. **Two-factor authentication on Indian apps** (45 min). SMS OTP, authenticator apps and prompts. Setting up 2-Step Verification on a Google account, two-step verification on WhatsApp, and app lock on a UPI app. Recovery codes. Why an OTP is a one-time key that must never be spoken aloud. SIM swap and what "no network for hours" can mean.
4. **Device security on Android** (40 min). Screen lock, biometric, Find My Device, encryption by default, updates, Play Protect, removing unused apps, reviewing permissions, turning off "install unknown apps". Public charging and public Wi-Fi rules. What to do when a phone is lost or stolen: block the IMEI on CEIR through Sanchar Saathi.
5. **Accounts and recovery** (30 min). Recovery phone and email, checking active sessions, logging out of cyber-café computers, "Know your mobile connections" on Sanchar Saathi to find SIMs issued in your name.
6. **Teaching an elder** (30 min). Pace, patience, one change per visit, the owner always holds the phone, never touch their PIN, leave a one-page Hindi card behind. Role-play of a scam call so the person practises hanging up.

READING MATERIAL

- Section 1: The six habits with Hindi step-by-step cards for Google, WhatsApp, a UPI app and a bank app. Draws on NCSC Cyber Aware, CISA Secure Our World, CERT-In's password advisory CIAD-2022-0026 and the ISEA Cyber Varishth Naagrik material.
- Section 2: Sanchar Saathi services for citizens: Chakshu, CEIR and Know Your Mobile Connections.
- Section 3: The conversation script and consent wording for the field task, in Hindi.

STAGE 02 · TEST

Blueprint: 20 questions, 30 minutes. Lectures 1 and 2 (6), lecture 3 (6), lecture 4 (5), lectures 5 and 6 (3).

Sample MCQs:



Q1 The best of these passwords is:

- a. Patna@2024
- b. 12345678
- c. bansuri dhaan chhata 82**
- d. your mobile number

Q2 Two-factor authentication means:

- a. two passwords
- b. something you know plus something you have or are**
- c. two email accounts
- d. a longer PIN

Q3 If your phone suddenly has no network for hours and you did not change anything, you should suspect:

- a. a tower fault only
- b. SIM swap and call the operator and bank at once**
- c. nothing
- d. a software update



Q4 A lost phone's IMEI can be blocked through:

- a. cybercrime.gov.in
- b. CEIR on Sanchar Saathi**
- c. the Play Store
- d. UIDAI

Q5 Which account should get the strongest, most unique password first?

- a. Instagram
- b. primary email**
- c. a shopping app
- d. a game

Q6 "Install unknown apps" should be:

- a. on for all apps
- b. on for WhatsApp
- c. off, and turned on only knowingly and briefly**
- d. ignored



Q7 Recovery codes for 2FA should be:

- a. shared with a friend
- b. stored offline in a safe place** ●
- c. posted in a family group
- d. never generated

Q8 When helping an elder set up 2FA, the student should:

- a. type the PIN for them
- b. hold the phone
- c. let the owner hold the phone and type everything** ●
- d. photograph the settings for the report

Q9 Reusing one password on many sites is dangerous because of:

- a. phishing only
- b. credential stuffing after any one site leaks** ●
- c. slow logins
- d. nothing



Q10 Public charging points can be risky because:

- a. they charge slowly
- b. a cable can carry data as well as power**
- c. they are illegal
- d. they drain batteries

STAGE 03 · FIELD WORK

Do

The task. The student runs a "Digital Suraksha Sahayata" desk for one day, helping five to eight elders, women or first-time smartphone users in their own village, ward or college neighbourhood to set a screen lock, review app permissions, turn on two-step verification on WhatsApp and on the Google account, and practise refusing a scam call. Each person leaves with the one-page Hindi card.

Location and assignment. A panchayat bhawan, anganwadi centre, community hall, temple or mosque courtyard, college common room or a CSC, within the student's home district. The student proposes the location in the portal with the name of the person permitting it; the coordinator approves and pins the coordinates.

Steps on site.



1. Introduce yourself with your college ID and the Society letter; explain the internship and get verbal consent, including for photographs.
2. Ask what the person uses the phone for and what worries them. Listen first.
3. Guide the owner, who holds the phone throughout, through screen lock, permissions review, WhatsApp two-step verification and Google 2-Step Verification, one at a time. Skip any step the person does not want.
4. Role-play one scam call. The person practises saying "main bank jaakar poochhunga" and hanging up.
5. Hand over the card with 1930 and cybercrime.gov.in written large. Record only the person's first name, age band, and which steps were completed, in the log.

Evidence required. Six to ten geotagged photographs: the student at the venue with the signboard or a recognisable feature; the student sitting with a person being helped, phone screen turned away or off; the Hindi card in the student's hand; the log sheet with names covered; a group photograph if the participants agree. No photograph shows a screen, a document or a card belonging to a participant.

Safety and consent notes. Consent is per person, verbal, in the local language. Never touch a PIN or OTP. If someone reports an ongoing fraud, stop the setup, help them call 1930 on their own phone, and note it in the report without personal details.

STAGE 04 · REPORT

Section prompts (800 to 1,200 words): (1) Venue, permission and who came. (2) For each person, in an anonymised table: age band, main use of the phone, steps completed, steps refused and why. (3) The three most common misunderstandings you met and how you explained them. (4) What you could not solve and where you referred people. (5) What you would change in the Hindi card.

Rubric: Completeness of the anonymised log (5). Quality of explanation of the misunderstandings (6). Consent and no-credential rule visibly followed (4). Reflection on the card and method (3). Writing and structure (2). Total 20, scaled to 7.5.



Glossary

Passphrase; credential stuffing; two-factor authentication; authenticator app; recovery code; SIM swap; CEIR; Play Protect; app permission; screen lock; biometric.

References

- NCSC Cyber Aware: <https://www.ncsc.gov.uk/cyberaware/home>
- CISA Secure Our World: <https://www.cisa.gov/secure-our-world>
- Sanchar Saathi portal (Chakshu, CEIR, Know Your Mobile Connections): <https://sancharsaathi.gov.in/>
- ISEA Stay Safe Online, role-based material including Cyber Varishth Naagrik: <https://www.staysafeonline.in/>
- CERT-In advisory CIAD-2022-0026 on password management, listed in the CERT-In awareness booklet:
<https://www.cert-in.org.in/>

MODULE 3

Safe digital payments and the anatomy of financial fraud

FIELD

15 HOURS

Overview and learning outcomes

The student learns how UPI, cards, AePS and net banking are attacked and defended, the RBI rules that decide who bears a loss, and the exact steps and time limits for getting money back. The field task is a market survey of digital-fraud experience. By the end, the student can teach the "golden hour" reporting sequence and interpret a small survey.

Hour allocation

Learn 6 hours (six lectures, 4 hours; reading 2 hours). Test 1 hour. Do 6 hours (survey design 1 hour, on site 4 hours, data entry 1 hour). Report 2 hours.

STAGE 01 · LEARN

LECTURES

- 1. How UPI, cards and AePS actually work** (45 min). The VPA, the PIN, the collect request, the QR code, the merchant and the bank. Cards and the CVV. Aadhaar-enabled Payment System at a business correspondent and why biometric lock on the myAadhaar portal matters in rural Bihar. What "additional factor of authentication" means.
- 2. Fraud on payments, pattern by pattern** (50 min). Collect-request fraud ("accept to receive refund"), QR code swap at a shop, fake customer-care numbers, screen-sharing apps, remote access apps, fake payment



screenshots shown to shopkeepers, AePS withdrawal without the customer's knowledge, fake bank.in look-alikes.

3. **Who bears the loss: the RBI rules** (40 min). The RBI circular of 6 July 2017: zero liability if the bank is at fault or if a third-party breach is reported within three working days; limited liability of Rs 5,000, Rs 10,000 or Rs 25,000 by account type for reports within four to seven working days; the bank's board policy beyond that. Grievance escalation: bank, then the RBI Integrated Ombudsman Scheme through cms.rbi.org.in. Why the bank.in domain migration helps.
4. **The golden hour** (40 min). Call 1930 immediately; the Citizen Financial Cyber Fraud Reporting and Management System relays the complaint to banks and wallets so the money can be held. File on cybercrime.gov.in with the transaction reference. Inform the bank in writing. Change passwords, block cards. Keep every screenshot. What the acknowledgement number is for.
5. **Talking to traders** (30 min). The Bakhtiyarpur bazaar as a case: who takes UPI, who was cheated, who stopped using it out of fear. Survey ethics, sampling in a market, asking about money without embarrassment, closing with the 1930 card.
6. **Reading a small survey** (35 min). Tally sheets, simple percentages, a two-way table (age band by fraud experience), what 25 responses can and cannot tell you.

READING MATERIAL

- Section 1: UPI, cards and AePS explained with diagrams. Draws on NPCI's public UPI material and UIDAI's biometric lock service.
- Section 2: The RBI 2017 customer protection circular, tabulated; the RBI Integrated Ombudsman Scheme 2021 in brief; RBI's bank.in and fin.in domain announcement of 2025.
- Section 3: The golden hour sequence as a one-page Hindi card; the I4C Suspect Repository ("Report and Check Suspect") on cybercrime.gov.in.
- Section 4: The survey instrument (twelve questions), consent script and tally sheet.



Blueprint: 20 questions, 30 minutes. Lectures 1 and 2 (8), lecture 3 (5), lecture 4 (4), lectures 5 and 6 (3).

Sample MCQs:

Q1 A message says "Accept this collect request to receive your refund of Rs 4,999". Accepting it will:

- a. credit your account
- b. debit your account**
- c. do nothing
- d. verify your KYC

Q2 Under the RBI 2017 circular, a customer who reports a third-party fraud within three working days of the bank's alert has:

- a. full liability
- b. zero liability**
- c. liability of Rs 10,000
- d. liability decided by the police

Q3 The first call after discovering a fraudulent transaction should be to:

- a. 100
- b. 1930**
- c. 112
- d. the local thana



Q4 AePS fraud can be reduced by:

- a. sharing Aadhaar only on WhatsApp
- b. locking biometrics on the myAadhaar portal**
- c. deleting Aadhaar
- d. using a different bank

Q5 A "fake payment screenshot" scam targets:

- a. the customer
- b. the shopkeeper**
- c. the bank
- d. NPCI

Q6 Complaints unresolved by a bank can be escalated to:

- a. the Data Protection Board
- b. the RBI Integrated Ombudsman**
- c. CERT-In
- d. TRAI



Q7 The bank.in domain exists so that:

- a. banks pay lower fees
- b. customers can recognise genuine bank websites**
- c. UPI works faster
- d. foreign banks are excluded

Q8 Remote access apps requested by a "customer care" caller are used to:

- a. speed up refunds
- b. see and control your phone**
- c. install updates
- d. verify Aadhaar

Q9 The 1930 helpline replaced which earlier number?

- a. 100
- b. 155260**
- c. 1800-11-4949
- d. 1091



Q10 A two-way table in the survey is used to:

- a. compute averages
- b. compare fraud experience across groups such as age bands**
- c. list respondents
- d. rank shops

STAGE 03 · FIELD WORK

Do

The task. A survey of 25 respondents, traders and customers mixed, in a local market on digital-payment use and fraud experience, followed by handing each respondent the golden-hour card. No names, phone numbers or account details are collected.

Location and assignment. A weekly haat, a bazaar street, a bus-stand market or a block-level market in the student's home district. Proposed by the student, approved by the coordinator, coordinates pinned.

Steps on site. (1) Inform the market association or nearest shop owners' group and the nearest thana if the market is large. (2) Approach every third shop or stall to reduce selection bias; approach customers waiting at counters. (3) Read the consent script; take verbal consent. (4) Ask the twelve questions and tally. (5) Give the 1930 card and answer questions. (6) If someone describes a live fraud, help them call 1930 on their own phone.

Evidence required. Six to ten geotagged photographs: the student in the market with a recognisable landmark; the student in conversation with a respondent (side or back view, no face if they prefer); the blank survey sheet and tally sheet in hand; the stack of golden-hour cards; a wide shot of the market. No filled survey sheet with any identifying detail, no shop's QR code standee, no phone screen.

Safety and consent notes. Daylight only, in pairs where possible. If a crowd gathers, pause. Never ask for an account number, a UPI ID or a screenshot. Do not photograph any respondent under 18.

STAGE 04 · REPORT

Section prompts (800 to 1,200 words): (1) Market, date, permissions, sampling method. (2) Results table: respondents by trader or customer, age band, payment modes used, fraud attempted, fraud succeeded, reported or not, and why not. (3) Two findings that surprised you, with numbers. (4) What respondents did not know about 1930 and the RBI rules. (5) Limits of your survey.

Rubric: Sampling and consent described honestly (4). Results table complete and correctly tallied (6). Interpretation with numbers, not impressions (5). Limits stated (3). Writing and structure (2). Total 20, scaled to 7.5.

Glossary

VPA; collect request; AePS; business correspondent; additional factor of authentication; zero liability; limited liability; CFCFRMS; golden hour; ombudsman; mule account; suspect repository.

References

- RBI, Customer Protection: Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, 6 July 2017: https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11040
- RBI Complaint Management System (Integrated Ombudsman Scheme): <https://cms.rbi.org.in/>
- RBI exclusive bank.in domain announcement, as reported:
<https://www.business-standard.com/finance/personal-finance/rbi-to-introduce-bank-in-and-fin-in-domains-to-enhance-pay>
- NPCI UPI safety tips, as reported:
<https://www.business-standard.com/finance/personal-finance/passwords-to-vigilance-npci-shares-5-tips-for-safe-digital-tra>
- National Cyber Crime Reporting Portal and Report and Check Suspect: <https://cybercrime.gov.in/>
- UIDAI myAadhaar services, including biometric lock: <https://myaadhaar.uidai.gov.in/>
- I4C, Cybercriminals Tampering with QR Codes (26 April 2022) and Fake Customer Care Numbers (21 March 2022):
<https://i4c.mha.gov.in/advisories.aspx>

MODULE 4

Law, privacy, social media and reporting

CONCEPTUAL

15 HOURS

Overview and learning outcomes

The student learns the legal architecture a citizen needs: the IT Act 2000 as amended in 2008, the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita provisions that matter for cyber fraud, the Digital Personal Data Protection Act 2023 and Rules 2025, and the full reporting map. Social media safety and sextortion response are taught here because the law and the reporting route are the answer to both.

Hour allocation

Learn 12 hours (seven lectures, 5.5 hours; reading 6.5 hours). Test 1 hour. Written reflection 2 hours.

STAGE 01 · LEARN

LECTURES

- 1. The IT Act 2000 and the 2008 amendment** (50 min). Section 43 (unauthorised access, damage, civil compensation), 43A (failure to protect data), 66 (computer-related offences), 66B (receiving stolen computer resource), 66C (identity theft: misuse of password or unique identifier), 66D (cheating by personation using a computer resource), 66E (violation of privacy: capturing or publishing private images), 67, 67A and 67B (obscene and sexually explicit material, and material involving children), 70B (CERT-In), 72A (disclosure in breach of lawful contract), 79 (intermediary safe harbour). Section 66A struck down in 2015.
- 2. The new criminal codes** (35 min). BNS Section 318 (cheating, replacing IPC 415 to 420) and Section 319 (cheating by personation), in force from 1 July 2024. BNSS Section 173: Zero FIR at any police station regardless



of jurisdiction, and electronic information of an offence. POCSO Act 2012 where a child is involved. What this means for a student helping a victim.

3. **DPDP Act 2023 and Rules 2025** (50 min). Assent 11 August 2023; Rules notified 14 November 2025 with an eighteen-month phased commencement. Data Principal, Data Fiduciary, Consent Manager. The seven principles. Rights: consent and withdrawal, access, correction, erasure, nomination, grievance redressal, with a ninety-day response duty. Verifiable parental consent for children. Breach notification to affected individuals in plain language. The Data Protection Board of India, digital and four-member, with appeals to TDSAT. Penalties up to Rs 250 crore for failing to keep reasonable security safeguards.
4. **Privacy in practice** (40 min). What a data fiduciary is in daily life: the shop that scans your Aadhaar, the app that wants your contacts, the coaching centre that keeps your marksheet. Data minimisation as a personal habit: share a masked Aadhaar, refuse unnecessary KYC, read the permission prompt.
5. **Social media safety** (45 min). Privacy settings on WhatsApp, Instagram and Facebook; who sees your profile photo and status; location in photographs; fake verification badges; impersonation profiles; account takeover through OTP; reporting inside each platform; platform grievance officers under the IT Rules 2021. Digital footprint and future employers.
6. **Sextortion, morphing and harassment: the response** (40 min). The pattern; why victims pay; the rule: do not pay, do not delete, screenshot everything, block, report on cybercrime.gov.in under the women and children category (which allows anonymous reporting) and to the platform; Sections 66E, 67, 67A, 67B and BNS provisions; support for a friend who is a victim; the school and family conversation.
7. **The reporting map** (40 min). 1930 for financial fraud; cybercrime.gov.in for everything, with the acknowledgement number; Chakshu on Sanchar Saathi for suspected fraud calls and messages; CEIR for a lost phone; the district cyber police station or cyber cell and the Zero FIR; the bank and the RBI Ombudsman; CERT-In for incidents affecting systems (incident@cert-in.org.in, 1800-11-4949); the platform's grievance officer; the Data Protection Board for personal data breaches. Which one first, and what to carry.

READING MATERIAL

—



- Section 1: Plain-language digest of IT Act sections 43 to 79 as listed, with one Indian example per section. Draws on the Act as amended, available on India Code.
- Section 2: BNS 318 and 319, BNSS 173, POCSO 2012, in brief.
- Section 3: The DPDP Act and Rules, drawing on the PIB explainer of 17 November 2025 and MeitY's Rules.
- Section 4: Privacy settings checklists for WhatsApp, Instagram and Facebook, in Hindi.
- Section 5: The reporting map as a one-page flowchart.

STAGE 02 · TEST

Blueprint: 20 questions, 30 minutes. Lecture 1 (5), lecture 2 (3), lectures 3 and 4 (5), lectures 5 and 6 (4), lecture 7 (3).

Sample MCQs:

Q1 Using someone else's password or OTP fraudulently is an offence under IT Act Section:

- a. 43A
- b. 66C**
- c. 67
- d. 79

Q2 Cheating by pretending to be a bank officer on a phone call is covered by IT Act Section 66D and BNS

Section:

- a. 173
- b. 318
- c. 319**
- d. 66E



Q3 A Zero FIR can be filed:

- a. only at the cyber police station
- b. at any police station regardless of jurisdiction** 
- c. only online
- d. only for financial fraud

Q4 Under the DPDP Act, the individual whose data is processed is the:

- a. Data Fiduciary
- b. Data Principal** 
- c. Consent Manager
- d. Data Processor

Q5 The highest penalty under the DPDP Act, for failing to keep reasonable security safeguards, is up to:

- a. Rs 50 crore
- b. Rs 200 crore
- c. Rs 250 crore** 
- d. Rs 500 crore



Q6 Processing a child's personal data requires:

- a. school permission
- b. verifiable parental or guardian consent**
- c. nothing
- d. Aadhaar

Q7 A victim of sextortion should first:

- a. pay once
- b. delete the account
- c. stop contact, keep evidence, report**
- d. share the video with friends for advice

Q8 Suspected fraud calls and SMS that caused no loss are reported on:

- a. 1930
- b. Chakshu on Sanchar Saathi**
- c. CERT-In
- d. TDSAT



Q9 Appeals from the Data Protection Board go to:

- a. the High Court
- b. TDSAT**
- c. CERT-In
- d. the RBI

Q10 IT Act Section 66A is:

- a. in force
- b. struck down by the Supreme Court in 2015**
- c. about child abuse material
- d. about CERT-In

Glossary

Data Principal; Data Fiduciary; Consent Manager; verifiable parental consent; Zero FIR; cheating by personation; intermediary; grievance officer; safe harbour; sextortion; morphing; digital footprint.

References

- Information Technology Act 2000 as amended, India Code: <https://www.indiacode.nic.in/>
- Digital Personal Data Protection Act 2023 and Rules 2025, PIB explainer, 17 November 2025:
<https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>
- Bharatiya Nyaya Sanhita 2023, Sections 318 and 319, overview:
<https://www.azbpartners.com/bank/overview-of-the-bharatiya-nyaya-sanhita-2023-penal-code/>
-



Bharatiya Nagarik Suraksha Sanhita 2023, Section 173:

https://en.wikipedia.org/wiki/Bharatiya_Nagarik_Suraksha_Sanhita

- National Cyber Crime Reporting Portal: <https://cybercrime.gov.in/>
- Sanchar Saathi, Suspected Fraud Communication (Chakshu): <https://www.sancharsaathi.gov.in/sfc/>
- CERT-In incident reporting: <https://www.cert-in.org.in/>
- Indian Cyber Crime Coordination Centre: <https://i4c.mha.gov.in/about.aspx>



MODULE 5

Malware, backups and the small-business security checklist

FIELD

15 HOURS

Overview and learning outcomes

The student learns what malware is, how it arrives on a phone or a shop computer, how to recognise infection, what the free Cyber Swachhta Kendra tools do, and how backups turn a disaster into an inconvenience. The field task is a consented checklist audit of a small business. By the end the student can complete the checklist, explain each item and recommend no-cost fixes.

Hour allocation

Learn 6 hours (six lectures, 4 hours; reading 2 hours). Test 1 hour. Do 6 hours (preparation 1 hour, on site 3 hours, write-up 2 hours). Report 2 hours.

STAGE 01 · LEARN

LECTURES

- 1. Malware for non-engineers** (40 min). Virus, worm, trojan, spyware, banking trojan, ransomware, adware.
How it arrives: APK from a link, pirated software on a USB, a cracked Tally or Photoshop, a malicious browser extension, a fake "update". CERT-In's key signs of infection: pop-ups, apps opening on their own, storage vanishing, redirecting browser, messages sent without you, antivirus disabled.
- 2. Cyber Swachhta Kendra and free tools** (35 min). What the Botnet Cleaning and Malware Analysis Centre is, operated by CERT-In under Section 70B. Free bot removal tools (eScan, K7, Quick Heal), M-Kavach 2 for Android, USB Pratirodh, AppSamvid, Browser JSGuard. Built-in defences: Play Protect, Windows Defender, updates.



3. **Backups: the 3-2-1 idea, simplified** (35 min). Two copies at least, one of them somewhere else. Phone backup to Google, photos, WhatsApp chats; a shop's Tally or billing data to a pen drive kept at home and to a free cloud drive. Testing a restore. Ransomware becomes an inconvenience if the backup is current.
4. **The small-business threat model** (45 min). A kirana with a UPI QR standee, a cyber café with ten shared PCs, a CSC handling Aadhaar and pension work, a coaching centre with student records. Threats: QR swap, fake payment screenshots, shared admin passwords, browsers that remember customers' passwords, pirated OS with no updates, no logout, data of customers left on desktops, staff phones with remote-access apps. Obligations under the DPDP Act for anyone holding customer data.
5. **The checklist and how to use it** (40 min). The 25-item checklist across five headings: devices and updates, accounts and passwords, payments, customer data and privacy, backups and recovery. How to ask each item as a question, not an accusation. Scoring. What "no-cost fix" means for each item.
6. **Writing a recommendation the owner will act on** (25 min). One page, three actions, in Hindi, ordered by risk. Follow-up visit.

READING MATERIAL

- Section 1: Malware types and signs. Draws on CERT-In's awareness booklet and CSK alerts.
- Section 2: CSK tool guide with download steps from csk.gov.in.
- Section 3: The 25-item checklist with Hindi phrasing and scoring guide.
- Section 4: DPDP obligations for small businesses in one page.

STAGE 02 · TEST

Blueprint: 20 questions, 30 minutes. Lectures 1 and 2 (7), lecture 3 (4), lecture 4 (5), lectures 5 and 6 (4).

Sample MCQs:



Q1 Cyber Swachhta Kendra is operated by:

- a. I4C
- b. CERT-In**
- c. NPCI
- d. UIDAI

Q2 Which is not a sign of malware listed by CERT-In?

- a. frequent pop-ups
- b. apps opening by themselves
- c. faster performance**
- d. antivirus disabled on its own

Q3 The most common way ransomware becomes a minor problem rather than a disaster is:

- a. paying quickly
- b. a current tested backup**
- c. a stronger password
- d. an antivirus



Q4 A pirated operating system is risky mainly because:

- a. it is slower
- b. it gets no security updates**
- c. it uses more storage
- d. it cannot run Tally

Q5 In the audit, the student may:

- a. connect to the shop Wi-Fi and scan it
- b. plug in a pen drive to check for viruses
- c. ask questions and observe with consent**
- d. reset a device

Q6 A cyber café browser that remembers customers' passwords is a problem of:

- a. availability
- b. confidentiality**
- c. integrity
- d. performance



Q7 "Two copies, one somewhere else" describes:

- a. 2FA
- b. a backup rule**
- c. RAID
- d. encryption

Q8 M-Kavach 2 is:

- a. a UPI app
- b. a free mobile security application listed by CSK**
- c. a government ID app
- d. a browser

Q9 A shop that keeps customers' Aadhaar photocopies in an unlocked drawer is failing which DPDP principle?

- a. purpose limitation only
- b. security safeguards**
- c. consent only
- d. none

Q10 The recommendation note should contain:

- a. all 25 items
- b. three prioritised no-cost actions**
- c. a product to buy
- d. a scan report

STAGE 03 · FIELD WORK**Do**

The task. With the owner's consent, the student completes the 25-item checklist for one small business, discusses each item, and leaves a one-page prioritised recommendation in Hindi. A follow-up visit or call after one week records what changed.

Location and assignment. A kirana or general store that takes UPI, a mobile repair or recharge shop, a cyber café, a Common Service Centre, a small coaching centre or a pharmacy, in the student's home district. Proposed, approved and pinned as before.

Steps on site. (1) Introduce yourself; explain that this is a conversation and a checklist, not a test, and that nothing will be touched or connected. Get verbal consent, including for photographs. (2) Walk through the five headings, asking and observing. The owner or staff demonstrate; the student does not operate any device. (3) Score the checklist. (4) Explain the three highest-risk findings and the free fixes, including CSK tools where relevant. (5) Leave the recommendation note. (6) Arrange the follow-up.

Evidence required. Six to ten geotagged photographs: the student at the shop front with the signboard; the student with the owner (consented) at the counter; the checklist on the clipboard, filled in but with the shop name covered; the recommendation note in hand; a general photograph of the premises showing no screens, no QR standees and no documents. No photograph shows a monitor, a phone screen, a bill, a register, a QR code or a customer.

Safety and consent notes. No scanning, connecting, plugging in or installing under any circumstance. If the owner asks the student to "fix" something, the student explains the steps and the owner does them. If the student finds evidence of a crime in progress, they do not investigate; they advise reporting and leave.

STAGE 04 · REPORT

Section prompts (800 to 1,200 words): (1) Business type, consent, how the audit was conducted. (2) Checklist scores by heading, with the three highest risks explained. (3) The recommendation note, reproduced. (4) What the owner said, what the owner changed at follow-up, and why some things did not change. (5) What in the checklist did not fit this kind of business.

Rubric: Checklist complete and scoring justified (6). Risks prioritised correctly with no-cost fixes (5). Consent and no-touch rule visibly followed (4). Follow-up recorded honestly (3). Writing and structure (2). Total 20, scaled to 7.5.

Glossary

Malware; trojan; ransomware; spyware; botnet; Cyber Swachhta Kendra; Play Protect; backup; restore; threat model; checklist audit; no-cost fix.

References

- Cyber Swachhta Kendra: <https://www.csk.gov.in/> and FAQ <https://www.csk.gov.in/faq.html>
- CERT-In, Cyber Security Awareness Booklet (malware signs, security tools):
https://www.cert-in.org.in/PDF/CSA_Booklet.pdf
- Common Service Centres, CSC e-Governance Services India Ltd: <https://www.csc.gov.in/>
- I4C, Banking Trojans stealing confidential information (21 April 2022) and malicious browser extensions (30 August 2022): <https://i4c.mha.gov.in/advisories.aspx>
- PIB explainer on DPDP obligations of Data Fiduciaries:
<https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>

MODULE 6

Running community cyber-awareness sessions

FIELD

15 HOURS

Overview and learning outcomes

The student turns everything learned into a session for other people: a local-language poster or WhatsApp message tested with the audience, and a 45-minute session at a school, college or village with permission. By the end the student can plan a session for a specific audience, run it with participation rather than lecture, measure whether anything was learned, and document it.

Hour allocation

Learn 6 hours (five lectures, 3.5 hours; reading 2.5 hours). Test 1 hour. Do 6 hours (design and testing 2 hours, session 2 hours, documentation 2 hours). Report 2 hours.

STAGE 01 · LEARN

LECTURES

1. **Who is in the room** (40 min). Class 9 students, first-year undergraduates, a self-help group of women, a panchayat gathering, senior citizens: what each fears, what each already knows, what each will actually change. ISEA's role-based approach as a model. Choosing three messages, not thirty.
2. **Messages that survive in Hindi, Magahi, Maithili and Bhojpuri** (45 min). Short verbs, real names, no jargon. "OTP kisi ko na batayein" versus "share nahi karna chahiye". The rule of one image, one line, one number. Adapting ISEA and CERT-In posters. The WhatsApp forward: 60 words, one action, 1930 at the end, no link.
3. **Testing before telling** (35 min). Show the poster to five people from the target group; ask what it means and what they would do; revise. A three-question before-and-after quiz to measure learning.



4. **Running the session** (50 min). A 45-minute plan: two minutes of a real local story, a live scam-call role-play with a volunteer, three messages, the reporting map on one chart, a pledge, questions. Managing a classroom, a courtyard and a panchayat bhawan. What to do when someone discloses a fraud in front of others.
5. **Permissions, safeguarding and documentation** (30 min). The head teacher's written permission and the no-identifiable-child photograph rule. The mukhiya's permission. Attendance count, not names. Handing the reporting card to every participant. Recording the before-and-after scores.

READING MATERIAL

- Section 1: Session plans for five audiences, each with three messages and a role-play script.
- Section 2: Template posters in Hindi from ISEA Stay Safe Online and CERT-In, with guidance on adaptation and attribution.
- Section 3: The before-and-after quiz and attendance sheet.
- Section 4: A one-page reporting map chart for display.

STAGE 02 · TEST

Blueprint: 20 questions, 30 minutes. Lectures 1 and 2 (8), lecture 3 (4), lecture 4 (5), lecture 5 (3).

Sample MCQs:

Q1 The best number of key messages for a 45-minute community session is:

- a. one
- b. three**
- c. ten
- d. as many as possible



Q2 A WhatsApp awareness message should end with:

- a. a link to a website
- b. the 1930 number and one action**
- c. the student's phone number
- d. a warning about the law

Q3 Testing a poster before the session means:

- a. checking spelling
- b. showing it to members of the target group and revising**
- c. printing it in colour
- d. posting it online

Q4 For a school session, photographs may show:

- a. children's faces if the teacher agrees
- b. the student presenting, with no identifiable child**
- c. the attendance register
- d. a child's phone



Q5 The most effective element of a session, according to the module, is:

- a. a lecture on the IT Act
- b. a live scam-call role-play**
- c. a slide show
- d. a quiz

Q6 If a participant discloses a fraud during the session, the student should:

- a. ask for details in front of everyone
- b. speak privately afterwards and give the 1930 number**
- c. ignore it
- d. post it in the WhatsApp group

Q7 Learning from the session is measured by:

- a. attendance
- b. the before-and-after quiz**
- c. applause
- d. the number of photographs

Q8 Permission for a village session comes from:

- a. the district magistrate
- b. the mukhiya or ward member**
- c. the police station only
- d. no one

Q9 "OTP kisi ko na batayein" is preferred over a longer sentence because:

- a. it is shorter and commands one action**
- b. it is grammatically formal
- c. it uses English
- d. it is a legal phrase

Q10 The attendance sheet should record:

- a. names and phone numbers
- b. a count and age bands**
- c. Aadhaar numbers
- d. signatures with addresses

STAGE 03 · FIELD WORK

Do

The task. The student designs one poster or one WhatsApp message in the local language, tests it with five members of the target group and revises it, then delivers a 45-minute session to at least 20 participants at a school, college or village with permission, using the before-and-after quiz.



Location and assignment. A government or private school (classes 9 to 12), the student's own or a nearby college, a panchayat bhawan or self-help group meeting, an anganwadi centre's mothers' meeting, in the student's home district. Proposed with the permitting person's name, approved and pinned.

Steps on site. (1) Confirm the permission in writing or by a message from the head teacher or mukhiya. (2) Set up the chart and posters. (3) Run the three-question before quiz by show of hands, counted. (4) Deliver the plan: story, role-play, three messages, reporting map, pledge, questions. (5) Run the after quiz. (6) Hand out the reporting card. (7) Record the count and scores.

Evidence required. Eight to twelve geotagged photographs: the venue signboard with the student; the tested poster or printed message with the student; the session in progress from the back of the room, showing the student and the chart, with no identifiable child and no participant's phone; the pledge moment; the head teacher or mukhiya with the student if they agree; the tally of the before-and-after quiz on paper. No participant's face in a school setting; no attendance sheet with names.

Safety and consent notes. Written permission for schools; no session with children without a teacher present throughout; no individual conversation with a child alone. Adults consent verbally to group photographs. Do not collect contact details to "add to a group". Attribute any adapted poster to ISEA or CERT-In.

STAGE 04 · REPORT

Section prompts (800 to 1,200 words): (1) Audience, venue, permission, attendance. (2) The message or poster: first draft, what the five testers said, the revision, with both versions reproduced. (3) The session as it actually ran, including what went wrong. (4) Before-and-after quiz results with a short interpretation. (5) What you would do differently for this audience next time.

Rubric: Evidence of testing and revision (6). Session plan followed and adapted sensibly (5). Quiz results recorded and interpreted (4). Permission and safeguarding rules visibly followed (3). Writing and structure (2). Total 20, scaled to 7.5.

Glossary



Target audience; key message; role-play; pledge; before-and-after quiz; safeguarding; attribution; local language adaptation; reporting map; facilitation.

References

- ISEA Stay Safe Online, posters, handbooks and pledge: <https://www.staysafeonline.in/>
- ISEA Information Security Awareness portal, audience sections and handbooks:
<https://www.infosecawareness.in/>
- ISEA programme, Cyber Aware Digital Naagrik: <https://isea.gov.in/about/>
- CERT-In awareness booklet, audience-specific tips: https://www.cert-in.org.in/PDF/CSA_Booklet.pdf
- CISA Secure Our World partner resources (session format ideas):
<https://www.cisa.gov/secure-our-world/partner-resources>

CYBER SECURITY

Appendix

A. Final report template

1. **Cover page:** student name, roll number, college, university, district, dates of field work, internship subject.
2. **Summary** (one page): what was done in the four field modules, the four locations, the total number of people reached, the three most important things learned.
3. **Module 2: Digital Suraksha Sahayata:** venue, people helped (anonymised table), misunderstandings met, referrals made.
4. **Module 3: Market survey:** market, sampling, results table, two findings with numbers, limits.
5. **Module 5: Small-business audit:** business type, checklist scores by heading, recommendation note, follow-up outcome.
6. **Module 6: Community session:** audience, message tested and revised (both versions), session narrative, quiz results.
7. **The law and the reporting map as I would explain it to a neighbour** (400 to 600 words, in Hindi or English).
8. **Reflection:** what I would do differently; what I now do differently on my own phone.
9. **Annexe:** the four signed field evidence checklists (Appendix B); the recommendation note and poster as images.

Length 2,500 to 3,500 words excluding annexe.

B. Field evidence checklist

For each field module, the student ticks and signs:

- Location proposed, approved and coordinates matched.
- Permission obtained from the named person (head teacher, mukhiya, owner, market association) and recorded.
- Verbal consent taken from every person helped, surveyed or photographed, in their language.
- No photograph shows a screen, password, PIN, OTP, Aadhaar number, card, QR code, bill, register, filled form or identifiable child.
- No credential of any other person was seen, typed, written or photographed by the student.
- No device belonging to another person was operated, connected to, scanned or had anything installed by the student.
- Required number of geotagged photographs uploaded, each showing the student on site.
- Anonymised log or tally sheet uploaded with names covered.
- Reporting card (1930, cybercrime.gov.in) handed to every participant.
- Any disclosure of an ongoing fraud handled by referral, not investigation, and noted without personal details.



C. Rubric for the final report

CRITERION	MARKS
Accuracy: every legal, procedural and institutional statement is correct and current (IT Act sections, DPDP, 1930, RBI liability rules, Sanchar Saathi)	5
Evidence: each module section is grounded in the student's own data, tables and photographs, honestly reported including failures	5
Analysis: findings are interpreted with numbers and compared across modules; limits are stated	4
Communication: the "explain to a neighbour" section is plain, correct and usable in the local language	3
Ethics and safety: consent, no-credential and photograph rules are documented and visibly followed	2
Structure and writing: follows the template, within length, clear	1
Total	20