unicef
for every child

सत्यमेव जयते
Education Department
Government of Gujarat

CyberPeace
Foundation

Generic Cybercrimes

Standard Operating Procedures

September 2022

TABLE OF CONTENTS

1. INTRODUCTION TO CYBERCRIME

With development and dependence on technology and increased use of cyberspace over the years, particularly during the period of the pandemic, trends in cybercrimes have seen a significant increase. Cybercrimes encompass a broad range of criminal activities that range from financial fraud, sexual abuse to trafficking. Speaking at a conference organised by the Kerala Police in 2021[1], the then Chief of Defence Staff, General Bipin Rawat, citing the developing trends of cybercrimes, said that the current Information Technology Act 2000 is not equipped to consider new-age changes in the mode of functioning businesses and modus operandi of crime in cyberspace.

The National Crime Records Bureau (NCRB) Crime Report 2021 reports that a total of 52,974 cases were registered under Cyber Crimes among **States and Union Territories**, showing an increase of 5.9% in registration over 2020 (50,035 cases). Crime rate under this category increased from 3.7 in 2020 to 3.9 in 2021. During 2021, 60.8% of cyber-crime cases registered were for the motive of fraud (32,230 out of 52,974 cases) followed by sexual exploitation with 8.6% (4,555 cases) and Extortion with 5.4% (2,883 cases). In **Metropolitan cities** a total of 17,115 cases have been registered under Cyber Crimes, showing a decline of 8.3% over 2020 (18,657 cases). Cybercrime rate has declined from 16.4% in 2020 to 15.0% in 2021. Crime head-wise cases revealed that Computer Related Offences (section 66 of IT Act) (8,513 cases) formed the highest number of Cyber Crimes accounting for 49.7% during 2021.

[1] https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece

According to the Indian Computer Emergency Response Team (CERT-In, the nodal agency in India to deal with cyber security threats) the first two months of 2022 reported 2,12,485 incidents of cybercrimes as opposed to 2,08,456 incidents of cybercrime in all of 2018.

The following Standard Operating Procedures addresses generic cybercrimes, covering definitions, real-time examples, the process of redressal, relevant sections of law, best practices and case scenarios to facilitate filing and handling of cyber complaints. It also touches on basic procedures to be followed by law enforcement officers, from the filing of the First Information Report (FIR) to the stage of investigation.

2. DEFINING CYBER CRIME

Because of its developing nature, the term "cybercrime" has not been explicitly defined by law. However, it is widely understood to be *an* ***unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime***[2].

Cybercrimes are intended to cause harm to the victim, a vast majority of which are intended for financial gain. They can be targeted at either individuals or corporations. A vital aspect of cybercrime is its non-local character, posing challenges to law enforcement personnel world over.

In India, an aggrieved victim can use the National Cyber Crime Reporting Portal https://cybercrime.gov.in/ (official portal) to report any incident of cybercrime. Offences of financial cybercrime are covered under the Information Technology Act, 2000 (ITA) and additionally under the Indian Penal Code 1860 (IPC).

[2] https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

3. GENERIC CYBER CRIMES

Generic cybercrimes in this SOP are a reference to common forms of cybercrimes.

i. Hacking

[Generally Applicable Provisions under ITA Sec 43, 66]

Hacking refers to the act of gaining unauthorised access to data in a system or computer. With respect to cybercrimes, the cybercrime.gov.in portal provides for three types of hacking that one can complain against:

Hacking can be understood in the context of gaining unauthorised access to:

- Social media accounts – When a social media account is compromised and used by another without permission.
- Emails – If an email account has been compromised by someone without permission, sending unsolicited/spam emails with malware attached to it. Such malware, if opened, gets discretely downloaded and installed on the user's device. Personal information is then accessed and used for mala fide purposes.
- Unauthorised Access/Data Breach – When a computer, mobile website, server, etc., is being accessed without permission.
- Website-related/defacement – When an attack on a website changes the visual appearance of the site or webpage.

Example:

A classroom platform, Seesaw, used by schools based out of Ohio, USA, was reportedly hacked, after some parents raised complaints of receiving messages with an explicit photo. The company said that the hackers didn't gain administrative access to Seesaw but instead breached individual user accounts by a 'credential stuff' attack. In such attacks

the hackers look through previous data breaches to identity combinations of usernames and passwords[3].

ii. Job Fraud

[Generally Applicable Provisions under ITA Sec 66B – 66D]

Job frauds refers to incidents that involve deceiving a person looking for employment by giving them false hope of employment or of earning high salaries or of extra income, in exchange for a fee.

Example:

The Enforcement Directorate seized ₹5.85 crore in raids on 12 Bangalore-based companies involved in a part-time job fraud case. The victims were mostly young people who were cheated by Chinese nationals through a mobile app called "Keepsharer," which promised them part time jobs and in exchange, collected money from them. The app sent advertisements through Whatsapp and Telegram via which they offered part-time job opportunities to people. The app was linked with an investment app and people were made to pay in order to register themselves on the app. They also raised funds by collecting money from the public as investment. The young victims were given the task of liking videos of celebrities and uploading them on social media. They were paid ₹20 on completion of the task, as promised. The amount was credited to their Keepsharer wallet. Eventually the app was deactivated from Playstore giving the victims no access to their Keepsharer wallets. The money was reportedly converted to cryptocurrency by the accused and transferred to their Chinese counterparts[4].

iii. Matrimonial fraud

[3] https://www.nbcnews.com/tech/security/popular-school-messaging-app-hacked-send-explicit-image-parents-rcna47687

[4] https://www.cnbctv18.com/india/ed-cracks-down-on-part-time-job-fraud-with-chinese-link-seizes-rs-585-crore-14860541.htm

[Generally Applicable Provisions under ITA Sec 66B – 66D]

Matrimonial frauds refer to instances where fake and misleading profiles are created on leading matrimonial websites to cheat people.

Example:

In June 2022, a native of Bihar was arrested in Noida for duping women on matrimonial sites[5]. The accused had a diploma in computer science. Three mobile phones and 16 debit and credit cards were recovered from his possession, while his account details showed transactions worth over ₹4 crore in four months. The accused served as the financier for a group of men from African countries who befriend women through matrimonial websites and would get them to transfer money on some pretext. One of the victims transferred over ₹60 lakhs to one of the men. One African national was also arrested from South Delhi in this regard and in his possession were many IDs including a forged FBI ID, seven mobile phones, forged bank letters, etc. Investigation revealed that once the women were befriended on the matrimonial websites with the promise of marriage, they would concoct a personal emergency situation and ask for large sums of money to be transferred to the account of an official either from the customs department or the RBI in the name of taxes or duties. The money went to various bank accounts managed by their Indian counterpart who would deduct 3% commission and give the rest of the amount to the foreign nationals. Over 300 women are suspected to be defrauded by this gang. A complaint was registered under IPC Section 420, 471, 120B and 34 along with provisions of the IT Act.

iv. Ransomware

[Generally Applicable Provisions under ITA Sec 43 and 66]

[5] https://www.hindustantimes.com/cities/noida-news/cyber-fraud-mastermind-held-in-greater-noida-for-duping-women-on-matrimonial-sites-101656268718510.html

Ransomware refers to cybercrimes in which malware locks data on a communication device, holding such data as hostage until a ransom, usually in the form of cryptocurrency, is paid.

Example:

A former Canadian government employee who turned into a ransomware hacker was sentenced to a 20 year prison term in USA[6]. He was an affiliate of a Russian-speaking ransomware gang that operated at the height of the Covid-19 pandemic. They hacked into computer systems of health districts, companies and schools and demanded ransom payments in exchange for returning the encrypted data. If the ransom demand was not met, their data was threatened to be posted on the dark web. They targeted over 400 victims around the world and collected nearly $40 million in ransom payments.

v. **Online Gambling**

[Generally Applicable Provisions under ITA Sec 66B – 66D]

Online gambling refers to illegal gambling done online, as a result of which monetary losses have occurred.

Example:

An accused, who was allegedly operating an online roulette gambling network in Maharashtra and cheated many people, was arrested[7]. The complaint was lodged by a local resident who claimed he was cheated of over ₹45 lakhs by the accused after downloading a gaming app on his mobile phone.

vi. **Sexting**

[Generally Applicable Provisions under ITA Sec 67, 67A, 67B]

[6] https://www.cbc.ca/news/canada/ottawa/ransomeware-hacker-vachon-desjardins-sentenced-1.6606274

[7] https://www.outlookindia.com/national/online-gambling-network-operator-arrested-in-nashik-news-192683

Sexting refers to the sending, receiving, or forwarding of sexually explicit messages, photographs or videos on any communication/digital device.

Example:

A 22-year-old man was booked for blackmailing a 19-year-old girl after saving screenshots of WhatsApp video calls between them[8]. The accused had lured her and then involved her in sexting. The victim said she came in contact with the accused who resided in her neighbourhood. While they conversed, he recorded the video calls and pressured her to marry him, threatening to circulate the pictures online. A molestation and criminal intimidation case was filed against him under IPC.

vii. **Sextortion**

[Generally Applicable Provisions under ITA Sec 66E, 67, 67A, and 67B]

Sextortion refers to the act of extorting money or sexual favours from someone by threating to reveal evidence of their sexual activity.

Example:

The Bhopal cybercrime branch closed in on a sextortion racket being operated from Uttar Pradesh, Haryana and Rajasthan, arresting three persons in Rajasthan[9]. The accused impersonating a woman lured a Bhopal based civil servant aged 70 years with nude video calls and recorded his obscene videos to blackmail him. They threatened to share the video with his friends to blackmail him and extorted around ₹7 lakh from him. They blackmailed 27 other people in a period of six months and extorted ₹78 lakh from them. They used SIM cards and bank accounts in different states using forged IDs.

[8] https://timesofindia.indiatimes.com/city/bhopal/bhopal-19-year-old-lured-into-sexting-blackmailed/articleshow/83224721.cms

[9] https://timesofindia.indiatimes.com/city/bhopal/sextortion-gang-that-duped-retired-civil-servant-of-7l-busted/articleshow/92559318.cms

viii. **Misinformation/Disinformation**

Misinformation refers to false or inaccurate information, one which is deliberately intended to deceive, while disinformation refers to false information intended to mislead issued by a government organisation to a rival power or the media.

Example:

Mumbai police arrested two persons for spreading fake news against journalist Rana Ayyub[10]. They accused Ms. Ayyub of being aided by Pakistan and banned by Saudi Arabia and also made morphed anti-India tweets that expressed her hatred for India. The journalist started to receive rape and death threats online, after which she lodged a complaint with the cyber police in Mumbai. Four accused were identified and arrested in this case.

[10] https://indianexpress.com/article/cities/mumbai/two-more-arrested-for-spreading-fake-news-rana-ayyub-thanks-mumbai-police-7802899/

4. LEGAL PROVISIONS APPLICABLE TO GENERIC CYBERCRIMES

Generic cybercrimes, much like other cybercrimes, may involve elements of traditional crimes. They may include financial implications, crimes against women or children, offences against the State, offences relating to religion or offences affecting the human body/property, offences relating to documents, etc., as defined under the IPC and other relevant laws. The listed provisions of law are therefore not exhaustive, but only attempt to cover offences likely to arise from any kind of cybercrime.

It is important to note that the Information Technology Act, 2000, being a special Act, overrides the provisions of the IPC, when it comes to ***similar ingredients*** *under both legislations*[11].

Provisions under Information Technology Act, 2000 (ITA)	
43, 66	Damage to computer, computer systems, etc.
66B	Dishonestly receiving stolen computer resource or communication device
66C	Identity theft
66D	Cheating by personation

[11] Sharat Babu Digumati vs. Govt. of NCT of Delhi [AIR 2017 SC 150]; Gagan Harish Sharma vs. The State of Maharashtra [2019(3) Crimes 618(Bom.)].

66E	Violation of privacy
66F	Cyber terrorism
67	Publishing or transmitting obscene content in electronic form
67A	Publishing or transmitting of material containing sexually explicit act in electronic form
67B	Publishing or transmitting of material depicting children in sexually explicit act in electronic form
Financial Crimes / Property / Documents: Under Indian Penal Code, 1860 (IPC):	
118 & 119	Conceals design to commit offence (punishable with death or life imprisonment) using encryption.
378 & 379	Theft
383-389	Extortion
411	Dishonestly receiving stolen property
415	Cheating
419	Cheating by personation
420	Cheating and dishonestly inducing delivery of property
424	Dishonest/fraudulent removal/concealment of property

425	Mischief
463 - 474	Forgery
Crimes Against Women and Children	
Under Protection of Children from Sexual Offences Act, 2012 (POCSO)	
13 & 14	Using child for pornographic purposes
15	Storage of pornographic material involving child
16	Abetment of an offence
3&4	Penetrative sexual assault
5&6	Aggravated penetrative sexual assault
7&8	Sexual assault
9&10	Aggravated sexual assault
11&12	Sexual harassment
Under IPC	
292	Selling, letting to hire, distributing, publicly exhibiting, circulating, etc., of obscene materials
354	Assault or criminal force to woman with intent to outrage her modesty

354A	Sexual harassment
354C	Voyeurism
361-366	Kidnapping
370-374	Human trafficking
376 - -376AB	Rape
376-376E	Gang rape
383	Extortion
406	Criminal breach of trust
499 & 500	Defamation
506	Criminal intimidation
509	Word, gesture or act intended to insult modesty of a woman
Under Indecent Representation of Woman (Prohibition) Act, 1989 (IRWA)	
4 & 6	Prohibition of publication or sending by post of books, pamphlets, paper, slide, film, photograph, writing, drawing, etc., containing indecent representation of women.
Offences relating to Religion : Under IPC	
298	Uttering words, etc., with intent to hurt religious feelings

Others : Under IPC	
153	Wrongful provocation with intent to cause riot
499-500	Defamation
503	Criminal intimidation
505	Statements conducing to public mischief
120A- 120B	Criminal conspiracy

5. PROCESS OF REDRESSAL: REPORTING GENERIC CYBERCRIMES

Reporting on helpline

- A complainant can report cybercrimes on the designated helpline number 1930.
- Following which, the complainant will receive a system generated login ID/acknowledgement number through SMS/email, using which the complainant must mandatorily complete registration of complaint on the reporting portal http://www.cybercrime.gov.in within 24 hours.

Reporting Online

The https://cybercrime.gov.in/ portal facilitates a person to report the listed generic cybercrimes under the following categories in the "Report Other Cyber Crime" section.

Section	Category	Sub-category
Report Other Cyber Crimes	Online and Social Media Related Crime	Sexting
		Email Hacking
		Online Job Fraud
		Online Matrimonial fraud
		Profile Hacking
	Ransomware	Ransomware
	Hacking	Unauthorised Access / Data Breach

		Website Related / Defacement
	Online Gambling	Online gambling

Reporting Offline

Considering the challenges to access the internet for a significant percentage of the population in India, a complainant can file a written complaint in the nearest Cyber Cell or the nearest local police station. A cybercrime falls under global jurisdiction, meaning that a crime complaint can be made irrespective of the place where it was originally committed or where the victim is currently residing.

- Cybercrime complaints must be addressed to the Head of the nearest **Cybercrime Cell** and must contain the name, contact details and address of the complainant, along with necessary incidental details as mentioned in the above segment.
    - FIR in **local police station**: If a complainant does not have access to any of the cyber cells in India, they can file a First Information Report (FIR) at the nearest police station[12]. Every police station is mandated by Sec 154 Code of Criminal Procedure (CrPC) to record the information/complaint, irrespective of jurisdiction in which the crime was committed. If an FIR is not accepted by the local Police Station, the complainant can approach the **Commissioner or the Judicial Magistrate**.

The concerned police station will have the jurisdiction to register FIR under section 154(1)[13] read with section 156[14] of the CrPC and investigate.

[12] Police officer is duty-bound to register FIR on receiving information relating to the commission of a cognisable offence; Lalita Kumari vs. Govt. of UP & Ors, AIR 2014 SC 187:2013 (13)
Registration of Zero FIR is mandatory in cases where crime is not committed within the jurisdiction and the same has to be transferred to the concerned police station for further investigation where the offence has been committed; Kriti Vashisht vs State & Ors., CRL.M.C. 5933/2019, 11/2019

[13] Information in cognisable cases

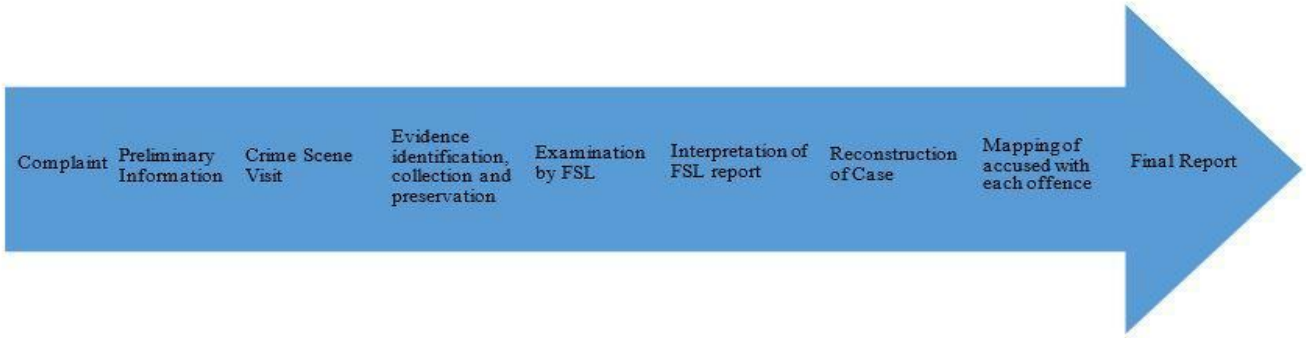
[14] Power to investigate cognisable cases

6. INVESTIGATIVE PROCEDURES

Every complaint of a cybercrime received by the local police station either directly through a complaint or through assignment, must be thoroughly investigated. **Sec. 78 ITA** empowers a Police Officer, not below the rank of Inspector, to investigate offences under the ITA. **Sec. 80 ITA** grants any Police Officer not below the rank of Inspector to enter any public place, search and arrest without warrant any person who is reasonably suspected of having committed or of committing or about to commit an offence under the ITA.

Before classifying an act as a cybercrime, the Investigation Officer (IO) must collect necessary information from complainants/victims to fully understand the scope of the incident and its possible outcomes, the various aspects of the crime, its location and circumstances. It is recommended that the IO consults with the Cybercrime cell before issuing an FIR to determine the provisions of law, especially under the ITA.

A brief workflow [15] of a cybercrime investigation is indicated in the flowchart below:



[15] Police Force Training on Cyber Frauds, by Shri .Kapil Garg, State Crime Records Bureau, Rajasthan Police

Preliminary Investigation[16]

All cyber cells or local police stations that receive or are assigned a complaint of cyber bullying/cyber stalking must take due cognisance of such complaints without dismissing them. The Investigating Officer (IO) must initiate a preliminary inquiry. Some pertinent questions to ask the victim/complainant for the listed generic cybercrimes include:

i. Detailed description of the incident – details of platform where the incident took place, time of occurrence, frequency of harassment, etc.
ii. Details of suspect, if known, and relationship with the victim, if any
iii. Details of money trails/ transactions if any, details of recipient.
iv. Associated phone numbers and Call Details Records (CDR) of the same.
v. Do the details in hand point to other crimes?
vi. Was there any negligence by the victim?
vii. If the crime was carried out on a website / application, who are the developers of such applications? Who provides support and maintenance? Who are the administrators? What measures are taken to ensure user safety?
viii. If there is explicit content in question, is the content still continuing to be circulated online? Is there a requirement to initiate proceedings to take down the material immediately and into consideration for evidence?

The IO must initiate procedures[17] to take down the objectionable content from said websites/ apps, by issuing letters to concerned website/Social networking platforms/ Apps to remove such content immediately along with furnishing detailed information on the upload of the said content on their platform.

[16] Investigative Manual on Cyber Harassment Cases, by Bureau of Police Research and Development
[17] SOP for Investigation of Objectionable Viral Pictures / Videos on various Social Networking Platforms - http://odishapolicecidcb.gov.in/sites/default/files/SOP_0.pdf

Additionally, media correspondents may be requested to not circulate the objectionable content on their platforms.

Generic Cybercrime	**Pertinent questions to ask**	**Potential Evidence**
Hacking	● What kind of content has been compromised ● Is the hacker known to the victim? Is there a potential reason for the hacking? ● Was there any personal / identifiable / banking details available in the hacked device/website/profile? ● Are there any competing businesses or individuals to consider for investigation?	Money Transactions, IP addresses, Copies of communication (if any), Associated numbers, etc.
Job Fraud	● What kind of job was offered to the victim, promised remuneration and details of the company? ● What was promised in exchange for the guaranteed job? ● Did the portal show partnerships/tie-ups with other companies?	Registration details, if available of the entities in question; Money transaction details and associated bank accounts, UPIs, payment gateway details, etc.; Associated phone numbers.
Matrimonial Fraud	● What details of the suspect were revealed to the victim? ● Details of conversations and monetary promises made, if any.	Legitimacy of the website and registration details Details of due process followed to vet registration of customers

	● Pictures/videos, and other details shared with the suspect	
Ransomware	● What efforts were made to contain the incident? What SOP did the organisation have in place in events of hacking and ransomware? ● Are there any individual or business rivals that need to be investigated? ● Details of ransom sought for and details of payment methods asked.	Images of systems affected for forensic analysis, firewall logs, copy/photo of ransom note, ransomware variant (if known), any email addresses or URL, etc, provided by the attacker for communication, payment methods required by the attacker.
Online Gambling	Where did the complainant find the illegal online gambling portal – app/website/messages?	Screenshots of SMSs, emails, links, websites, social media handles, messenger apps, etc., received/seen by the complainant including date and time of such receipt.
Sexting	● Any known reasons for the attack/harassment and details of the same. ● When and where the harassment began – online and offline? ● Details of all communication between the victim and the suspect,	Screenshots, copies of messages with sender details.

	copies/screenshots of such correspondence.	
Sextortion	• Any known reasons for the attack/harassment and details of the same. • When and where the harassment began – online and offline? Details of all communication between the victim and the suspect, copies/screenshots of such correspondence.	Screenshots, copies of messages with sender details, details of transactions, receiving bank/UPI/wallet details.
Misinformation/ Disinformation	On what platform was the information viewed / disseminated?	Copies / screenshots of the content; details of handles that posted the content; URL/website/App details.

Crime Scene Investigation

Where the scene involves electronic sources of digital evidence, the following serve as sources of digital evidence[18]:

Computer Processing Unit (CPU)	Containing digital devices with all the files and folders stored including deleted files and information.

[18] Standard Operating Procedures, Digital Evidence related to Crimes Against Women and Children, Kerala Police : https://keralapolice.gov.in/storage/pages/custom/ckFiles/file/7GafuMCjLbFgjBNh8aXz8WhLv2Zqtfczvbi7Uv6m.pdf

Display Monitor screens (if switched on)	All graphics and files that are open and visible on screen can be noted as electronic evidence.
Smart Cards, Dongles and Biometric Scanners	Provides information on users, level of success, configurations and permissions.
Answering Machines	Access to voice messages with date and time information, last phone number called, memos, names, caller identification information, deleted messages, etc.
Digital Cameras	Access to images, videos, sounds, removable cartridges, time and date stamps.
Handheld devices such as personal digital assistants, electronic organisers, smart phones	Access to information pertaining to addresses, appointments, calendars, documents, emails, messages, passwords, etc.
Hard drives	To access all stored information from the system
Local Area Network (LAN) Card or Network Interface Card (NIC)	To gain access to Media Access Control (MAC).
Modems, Routers, Hubs and Switches	To gain information related to IP addresses, etc.
Servers	To access information like logins, emails exchanged, contents downloaded, pages accessed, etc.
Network cables and connectors	To trace back to their respective computers and to identify types of devices that are connected to the computers

Pagers	To gain address information, text messages, phone numbers
Printers	To access information like number of prints last printed, usage logs, time and date stamps, network identity information, finger prints.
Removable storage media and devices	To access stored files
Scanners	To gain access to previously scanned material
Telephones	If possible, to gain access to phone numbers, messages, passwords, caller identification information, recorded voice messages
Copiers	To gain access to physical and electronic documents, user usage logos, time and data stamps
CD & DVD Drives	To access stored files or data
Credit Card Skimmers	Magnetic stripe contains cardholder's information which include expiration date, user's address, credit card numbers and usernames
Digital Watches	Latest digital watches can contain all information available on smartphones that it has been synced with
Fax Machine	To access relevant documents, phone numbers, logs, etc.
Global Positioning System (GPS)	Provides travel logs, home locations, previous destinations, way point coordinators, way point name, etc.
Keyboards and mouse	To examine for fingerprints

In the investigation of a physical crime scene[19]:

[19] Cyber Crime Investigation Manual by Data Security Council of India, Nasscom and Deloitte India

a. A preliminary review of the scene of offence is recommended. This can be the home of an individual, a cyber café, the premises of companies/organisations, etc. The scene must be surveyed meticulously to understand the local situation, circumstances, and technical details of systems or networks at the scene of the crime.
b. The scene must be secured and every individual present at the scene must be made note of.
c. All potential evidence like passwords, documents, slips, account details, notes, etc., must be seized.
d. Electronic/digital evidence is fragile and can be easily altered or tampered with. Due care must be taken while seizing any perishable evidence. Help of an experienced technical or forensic personnel must be sought.
e. Due care must be taken in containing the incident or offence in order to minimise the damage, prevent any further damage or to avoid any alteration of the evidence.
f. Proper identification and protection of the place of occurrence and an 'as and where is' description of such place must be recorded.
g. Due procedures regarding collection of evidence when system is switched on or when the system is switched off, must be followed, thereafter, proper packaging and preservation of electronic evidence and devices must be adhered to.
h. Forensic Duplication of electronic evidence must be carefully done and proper chain of custody must be recorded.
i. Statements of witnesses must be recorded.
j. Evidence must be classified.
k. A seizure memo or panchanama must be drawn up under Sec.165 CrPC read with Sec.80 ITA. A technical expert who can properly identify the equipment and sound advice to the IO should accompany the search and seizure. The panchanama must record timezone/system time along with the system's hash value and serial number. If a system is off, it should not be switched on. Photographs of the device must be taken.
l. Proper chain of custody must be maintained and recorded.

Evidence collected should be produced immediately before the concerned court, where orders to hand over digital evidence to forensic experts must be obtained.

6.3 Cyber Forensics

Once evidence has been collected and properly preserved, the IO must proceed to hand over digital evidence to forensic experts/Forensic Science Laboratory (FSL), in order to extract evidence from digital devices without altering the authenticity of the original evidence object. This practice would efficiently recover data including files that have been deleted and also provide a timeline of events based on times associated with the files.

6.4 Preparing Final Report[20]

a. All information shared by the complainant while registering the FIR and investigation must be included while drawing up the Final Report (Chargesheet).
b. Documents proving chain of custody of digital evidence to be attached with the Final Report.
c. Forensic report received from experts/FSL to be attached with the Final Report.
d. Information about place of occurrence and process followed to analyse the available evidence must be detailed.
e. An analysis of the available evidence and mapping of the offences to the accused must be detailed to complete the Final Report.

[20] Cyber Crime Investigation Manual by Data Security Council of India, Nasscom and Deloitte India

7. BEST PRACTICES

i. Working in collaboration

a. Working in collaboration with organisations using a multi-disciplinary, multi-agency approach, is a recommended best practice in cases of child abuse.

b. In cases where child sexual abuse is identified and rescue of victims are involved, it is essential to work in collaboration with units specialised in child care and protection – this can include Special Juvenile Police Units(SJPUs) and local NGOs.

ii. Victim-centric approach

a. Where it is essential to interact with a minor victim, it is essential to follow safeguards laid down under the POCSO Act. Section 24 and 26 POCSO, mandates the following:

- The statement of the child must be recorded at the place of residence or the place of choice for the child and preferably by a woman police officer not below the rank of a sub-inspector.
- Statement must be recorded in the presence of the parents of the child or any person in whom the child has trust or confidence.
- Assistance of a special educator must be sought if the child suffers from a mental or physical disability.
- The officials shall not be in uniform while recording such statement.
- The child shall not at any point come in contact with the accused.
- The child shall not be detained in the police station in the night for any reason
- The identity of the child must be protected from the public media unless directed by the Special Court in the interest of the child.

iii. Evidence Seizure and Collection

a. Digital Evidence is highly volatile in nature. Therefore, it is particularly important to handle the collection, sealing and preservation of such perishable information with utmost care.

b. To prevent any questions on authenticity of the evidence during trial, the Investigative Officer must take care to prepare and maintain chain of custody throughout the course of investigation.

c. Where necessary, if the investigating officer lacks specialised training in handling evidence, the help and expertise of a technical personnel or a digital forensic expert must be sought.

d. It would be a good practice to concur with the cyber cell at the stage of FIR and while preparing the Final Report to know what provisions of law would be appropriate to include.

iv. Trainings on handling evidence

a. Officers authorised to handle investigation in cybercrime cases must be subject to periodic training on investigative methods- identification, collection, preservation and presentation of digital evidence in cybercrimes.

v. Knowledge sharing

a. It is vital to keep abreast of trends, modus operandi of cybercrimes in the country and across the globe.

b. It is a recommended practice to involve expert private agencies in the training of law enforcement officers and to exchange information on trends and modus operandi of cybercrimes.

9. FREQUENTLY ASKED QUESTIONS (FAQs)

1. **What kinds of cybercrimes can be reported on the government portal?**

   Crimes related to women/Child and other cybercrimes such as mobile crimes, online and social media crimes, online financial fraud, ransomware, hacking, cryptocurrency crimes and online cyber trafficking.

2. **What kind of information should be provided to report a complaint?**

   A complainant is required to register himself using a valid name and number, following which an OTP will be sent for verification. Once registered, a complaint can be filed by selecting the appropriate category and sub-category.

   Any evidence pertinent to the complaint placed is relevant to the investigation – credit card receipts, bank statements, envelopes if received, online money transfer receipts, copy of email, URL of webpage, screenshot of suspect's mobile number, video, images, and other documents.

3. **Is there an action for false complaints?**

   Providing false complaints could make the complainant liable to penal action under IPC.

4. **How can a complaint check the status of his complaints?**

   Once a complaint is placed online, the complainant will receive an acknowledgment number which can be used to track the progress of the complaint.

   If the complaint has been filed in the Local Police Station or Cyber Cell, the Investigation Officer in charge of the case must provide updates to the complainant on the status of the case.

5. **Can a complaint be filed by a victim who has been victimised by a foreign national/company or by a foreigner who has been victimised by an individual or company in India?**

   Yes, one may file a complaint related to all types of cybercrimes on the portal, regardless of residence or citizenship.

6. **How can a person keep themselves safe online?**

   Some of the recommended ways a person can exercise vigilance online are:

   - Always review websites before browsing. While downloading apps, make sure they are downloaded from recognised portals. Never download DMZ or APK files from websites, social or messaging platforms.
   - Always use updated versions of software and systems
   - Install trusted Anti-Virus software on devices.
   - Always choose robust passwords that are changed frequently and do not save them online.
   - Do not share any financial information online.
   - Do not respond to calls that ask for sensitive information.
   - It would be a good and safe practice to set withdrawal limits on cards and accounts.
   - Keep your financial statements safely.
   - Always keeps PINs a secret.

7. **What precautionary measures can one take while making online payments?**

   While making payments online, the following precautionary methods are advised:

   - While making payments, look for a secure payment option with Pad Lock symbol. Never share OTP/PIN numbers in any form with the buyer or seller or make any payments while on call. If a payment link appears suspicious, do not click or fill out any information on such links.
   - Never scan QR codes especially where the party forcefully asks to scan a code or asks to approve a small payment in order to process a bigger one.

- While using Internet Banking Services, always keep login credentials a secret. Activate alerts on registered mobile numbers to monitor any suspicious activity. It is a good practice to monitor bank account activities frequently. Always disable the auto-fill option on the browser used. Remember to log out from account when done with net banking facilities instead of directly closing the browser.

8. **Are there any precautionary measures one can take on a matrimonial website?**

   Dating and Matrimonial websites have now become a popular way of finding a match. However, much like every other platform in cyberspace, it comes with the risk of being victimised by fraud. One could consider the following precautions while using these platforms:

   - Use verified websites, talk to people who have used the platform before, to check its reliability.
   - Use a separate email ID to log on to these platforms and avoid sharing any personal and identifiable data.
   - If matched with another individual, always do an end-to-end background check of the individual. As relevant questions to know the person better and to detect any inconsistencies on his/her part.
   - Keep close friends/family aware of such interactions.
   - If choosing to meet the person offline, always choose to meet in public places.
   - Never share private and sensitive photographs/videos.
   - Do not entertain any requests for money.