सत्यमेव जयते

ज्ञान-विज्ञान विमुक्तये

A Handbook on Basics of Cyber Hygiene for Higher Education Institutions

University Grants Commission
Ministry of Education
Government of India, New Delhi

October, 2024

Printed and Published by : Secretary, University Grants Commission,
Bahadur ShahZafar Marg,
New Delhi-110002

Contents

Disclaimer

- **For Figures and Tables:** The Majority of the figures used in the handbook have been pickedup from authenticated government websites such as the Ministry of Home Affairs (MHA), PIB check, @CyberDost, CDAC, ISEA Awareness portal, and so. The sources have been duly acknowledged throughout. For the rest of the images, details have been picked up from public domain and converted into visuals by Team IIPA.
- **For Examples and Case Stories:** The case stories or examples used in the handbook have been picked up from the legal domain. Care has been taken to mask all the identities. Further, these examples/case stories represented under various sections of a legal instrument(IT Act/IPC) are provided only for a general understanding of these sections. However,the reader should be aware that not just one but several sections could be simultaneouslyapplicable to these examples/case stories. Hence, one-on-one correspondence on cases is only indicative and not exhaustive.
- All the sources are mentioned in the 'Bibliography', which is provided at the end of the handbook.

FOREWORD

In recent times, Higher Education Institutions (HEIs) have been vulnerable to various kinds of cyber-attacks. The COVID-19 outbreak also put the HEI community 'online', particularly encompassing VCs, faculty, students, and support staff who needed to adjust comfortably and safely to the emerging demands of cyber security. Due to the lack of awareness of cybersecurity and trust in Cyberspace, HEIs have had some concerns towards the smooth transition to an 'online'mode of education. Therefore, it is imperative that creating awareness about Cyber threats and adherence to healthy Cyber hygiene practices will strengthen the cyber security ecosystem of HEIs.

The National Education Policy (NEP) 2020, which also promotes digitalization in education, identifies the need to leverage the use of technology in teaching while recognizing its potential risks and dangers. It has to be determined how the benefits of online/digital education can be reaped while addressing the concerns of the digital divide.

Our Higher Education Institutions must also come forward to develop good cyber hygiene habits and to address the new normal for cyber security. This will help the learners and organizations to reduce potential cyber risks with a security-centric approach and behavior.

To develop an ecosystem for cyber security in the cyberspace of HEIs, UGC has developed this "Handbook on Basics of Digital Hygiene for Higher Education". This will enable HEIs and their stakeholders to practice good cyber hygiene habits and to stay cyber secure. This document focuses on the key topics of cyber security, which help the learners to understand the basic concept of Cyber Hygiene, attacking vectors, preventive measures, tools to safeguard, the legal framework for cyber security, career opportunities, and ways for strengthening teachers, students and IT teams of Higher Education Institutions. HEIs must use sophisticated technologies/techniques to protect their assets and make their faculties and students digitally empowered andsecure.

I would like to acknowledge the valuable contribution of the Chairman of the Committee, Shri Abhishek Singh, Additional Secretary, Ministry of Electronics and Information Technology (MeitY); Shri Rajesh Kumar, CEO, Indian Cybercrime Coordination Centre (I4C); Shri Nishant Kumar, Director (NCFL & NCEMU), I4C; Prof. (Dr.) Charru Malhotra, Professor (e-Governance and ICT) at Indian Institute of Public Administration and all other members of the Committee in developing this document. I am also thankful to the UGC officials for providing their necessary support and relevant input.

I hope this handbook on digital hygiene will become a primer for administrators, teachers, and students in higher education across the country and help them achieve cyber empowerment.

Prof. M. Jagadesh Kumar
Chairman
University Grants Commission

October, 2024
New Delhi

LIST OF FIGURES

Chapter 1 Introduction

Chapter 2 Malware and Its Types

Chapter 3 Some Popular Types of Cyber Crimes

Chapter 4 A Ready Reckoner to Lodge Cyber Complaints and to Stay Cyber Safe

Chapter 5 Understanding the Institutional Framework of Cyber Security in India

Chapter 6 Glimpses into the Legal Framework for Cyber Security in India

Chapter 7 Strengthening Students, Teachers, and Institutions

LIST OF TABLES

Chapter 1: Introduction

1.1 Understanding Digital Hygiene

The term digital hygiene was first coined by Dr. Eduardo Gelbstein in 2006 in his book "Good Digital Hygiene." 'Digital Hygiene' is also called 'Cyber Hygiene. In this document, we shall primarily confine to the basic concepts related to digital hygiene.

Digital Hygiene can be defined as adhering to practices and behaviours that help keep the digital world safe and secure. They are basic and essential activities that keep digital devices free from any cyber threats or 'vulnerabilities.' It requires users to undertake some basic precautionary activities regularly or while connecting to cyberspace. These activities include regular updating and maintaining electronic devices, using passwords that follow security protocols, organizing the files stored on the device systematically, optimizing the device and software settings, and much more. These steps ensure greater safety for individuals and hence, for their organizations too.

The government of India has made several efforts to strengthen cyber hygiene. This includes the establishment of the Indian Computer Emergency Response Team (CERT-In), which is the national agency for incident response, including forecasting and mitigation for cybersecurity incidents. Its mandate includes monitoring and responding to cybersecurity incidents, issuing advisories and guidelines, and promoting best practices in cybersecurity. Cyber Swachhta Kendra (CSK) under CERT-In was established in collaboration with industry and academia to detect systems infected by bots. In collaboration with Internet Service Providers and Industry partners, it notifies the end users regarding the infection of their system and provides them assistance in cleaning their systems. CSK also aims to enhance common users' awareness of botnet and malware infections and measures to prevent them and secure their computers/systems/devices. The National Cyber Coordination Centre (NCCC) was set up to coordinate the intelligence-gathering activities of other agencies and monitor metadata for cyber threat detection. NCCC intends to help the country deal with malicious cyber activities by acting as the first layer for cyber threat monitoring and communicating with Government and private service providers

Additionally, the government has focused on real-time reporting of cybercrimes, capacity building of Law Enforcement Agencies (LEAs), and the implementation of the Crime and Criminal Tracking Network and System (CCTNS) in all police stations nationwide. The launch of 'CyTrain,' the world's largest cyber security training program, underscores India's commitment to equipping citizens with cyber awareness and skills. These initiatives collectively aim to fortify the nation's cyber infrastructure and enhance preparedness against evolving cyber threats.

Ministry of Electronics and Information Technology (MeitY), Govt. of India launched G20-Stay Safe Online Campaign in December 2022 to raise awareness among citizens to stay safe in the online world on the widespread use of social media platforms and rapid adoption of digital payments. Detailed information is available at www.staysafeonline.in.

This handbook aims to provide a deeper understanding of the significance of digital hygiene practices in safeguarding your online presence and fostering a safer digital environment for all. Through insights and guidance, it seeks to equip individuals with the knowledge and tools necessary to navigate the digital realm securely and responsibly.

Fig. 1.1 Digital Hygiene (Source: IIPA)

1.2 The Need for Digital Hygiene in the Education Sector

The COVID-19 outbreak resulted in an upsurge in the utilization of digital transformation in the education environment in most schools and universities. Increased focus on smart devices replaced conventional institutes with online classes. Digital transformation in the education sector consists of teaching-learning processes such as online learning video interaction, learning from augmented reality (AR)/virtual reality (VR), gamification, and exam portals. These new tools provide a platform for students and teachers to collaborate and conduct virtual sessions with the ability to record, share, learn, and evaluate sessions at their convenience.

These digital tools save time, overcome location, and provide the ability for faculty and studentsto teach and learn almost anywhere, anytime. Whiteboards and smartboards are becoming a norm to make the teaching-learning process truly interactive, particularly in the urban context. Some students and teachers now have access to smart mobile devices and related software and apps. The convenience of online courses and certifications, as well as the availability of large digital resources with micro-learning modules, have made them increasingly popular among students and educators worldwide as this model provides learners with various options at ease.

The trend of relying on digital technologies in the education sector will not slow down. Instead, it will further increase due to digitalization. Digitalization is the process of using new-age digital technologies such as artificial intelligence (AI), augmented reality (AR), virtual reality (VR), blockchain, and so on to maximize the use of the digital resources available. Applying new-age digital technologies also insists on modifying business models and eventually helps generate better value-producing opportunities.

It would, rather, transform further with the application of artificial intelligence and machine learning (ML) technologies. For instance, instead of providing a single curriculum for all students, educators will be aided by AI, using the same basic curriculum to give a wide range of hyper-personalized information tailored to each student's individual needs. Many tech companies are now focusing on the education industry, with purpose-built hardware, platforms, and digital tools to elevate the classroom learning experience. This trend of complete digital transformation in the education sector is also referred to as 'Edu-Tech.'

As per NCRB data, cybercrimes committed against children witnessed a sharp rise of more than 400 percent in 2020 from those committed in 2019[1]. A total of 842 instances of cybercrimes targeting kids were reported in 2020, while in comparison, a total of 164 cybercrimes against children were reported in 2019, 413 percent lower than those in 2020. This could also be attributed to the fact that children are now spending more time on the internet for educational and communication purposes and, hence, have become more vulnerable to cyber threats.

The rapid acceptance of Edu-tech insists that educators and students should now proactively adopt principles of digital hygiene. However, before proceeding to understand the various Do's and Don'ts of digital hygiene, elaborated in subsequent chapters, we shall understand some other related terms of digital hygiene. (We shall, henceforth, refer to all the associated stakeholders of the education system as only 'educators.')

1.3 Some Other Related Terms

1.3.1 Cyberspace

Cyberspace is a virtual environment of interconnected networks and digital systems to facilitate communication among various objects present in that network. Digital communication amongst these systems is undertaken using computer network connectivity, the internet, etc.

1.3.2 Surface Web

The Surface web, also called the White web, includes any public web content that is indexed by search engines. Web pages on the white web show up in the search results on sites like Google, Bing, and so on.

1.3.3 Deep Web

Deep Web is a part of the internet that isn't indexed by standard search engines such as Google Search, Bing Search, Yahoo Search, AOL Search, etc., and hence, is not accessible (Fig.1.2). For instance, privatenetworks used by select businesses, governments, and educational institutions to communicate and regulate aspects of their internal operations are on the deep web.

1.3.4 Dark Web[2]

The Dark Web is used to keep internet activity private and anonymous. It's a hidden collection of websites that can only be accessed with a specialized web browser, referred to as Tor, and it is not easily accessible through regular search engines like Google. It operates with layers of encryption, making it difficult to monitor. Because of its anonymity, the Dark Web has become a hotspot for illegal activities, including selling drugs, firearms, and stolen data. Criminals use it to trade goods without getting caught. The Dark Web poses a serious threat to national security because it enables illicit trading on a large scale.

[1] https://pib.gov.in/PressReleasePage.aspx?PRID=1806602
[2] https://iica.nic.in/images/FOIRNews/The-Dark-Web-Cyber-Terrorism-Arindam.pdf

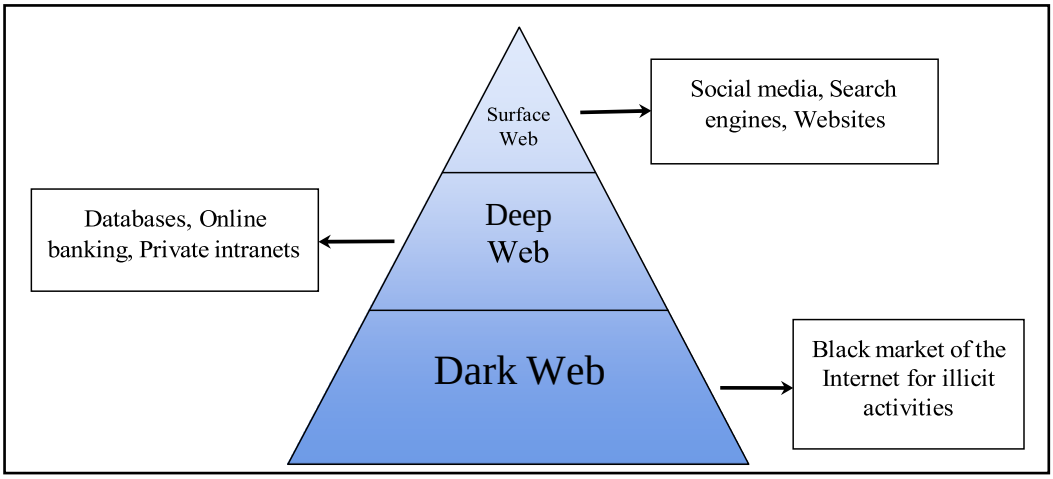


Fig. 1.2 Overview of Surface Web, Deep Web, and Dark Web (Source: IIPA)

1.3.5 Digital Footprints

Digital footprints refer to the information available in cyberspace or on digital devices due to the digital activities undertaken by an individual. These footprints are unique and traceable digital activities. Actions such as liking posts on social media, browsing internet content, leaving web cookies on visited websites, and more, all contribute to digital footprints. Implementing the "Right to be Forgotten" or "Right to be Erased" is challenging due to the presence of digital footprints in cyberspace. Digital footprints are also known as 'digital shadows' in literature.

1.3.6 Digital Inheritance

Digital inheritance is the process by which a person's digital assets, such as online accounts, files, and media, are transferred to specific individuals or beneficiaries after the person's death. It involves recognizing the existence of these digital assets and determining who has the right to access and use them after the individual passes away. This may include transferring access rights with beneficiaries and addressing the storage of these digital assets, which can be either on the deceased person's own devices or under the control of third-party service providers

1.3.7 Wire Frauds

Wire frauds are criminal acts or attempts to commit fraud with the aid of some form of electronic communication, e.g., telephone, internet, etc. Wire fraud may include a phone call, a fax, an email, a text, or social media messaging, among many other forms.

1.3.8 Cybercrime

The term "cybercrime" refers to criminal activities related to computers, information technology, the internet, and virtual reality. While there isn't a specific legal definition, it encompasses offences involving these technologies. Laws penalizing cybercrimes are found in various statutes and regulations, including the Information Technology Act, 2000 and the Indian Penal Code of 1860. Cybercrime involves any criminal activity conducted using computers, the internet, or other technology reconsigined by the Information Technology Act.

1.3.9 Data Breach

A data breach occurs when unauthorized individuals, including insiders or external attackers, access confidential or sensitive information stored in computer systems without proper authorization. This can involve medical records, financial data, personally identifiable information, and more. According to the Information Technology Act, 2000, specifically section 43A, if a body corporate possesses, handles, or deals with sensitive personal data or information and fails to implement and maintain reasonable security practices and procedures, they are held responsible. Additionally, provisions in the Information Technology (Amendment) Act, 2008 address the protection of critical information infrastructure, the privacy of information held in computer systems and networks, breach of confidentiality and privacy, and penalties for such breaches.

1.3.10 Data Recovery

Data recovery is the process of recovering data that has been lost, erased, corrupted, or rendered unavailable. The data is recovered from a backup copy kept in a different location. In case of data loss, the more current the backup copy is, the more completely the data can be restored. Successful data recovery requires a backup and restore plan that specifies data recovery objectives, usually as part of a larger data loss recovery plan.

1.3.11 Cybersecurity

Cybersecurity refers to the practice of safeguarding information, equipment, devices, computer systems, communication devices, and the data stored within them from unauthorized access, use, disclosure, disruption, modification, or destruction. In essence, it involves protecting networks, devices, and data from malicious activities or criminal exploitation while ensuring information confidentiality, integrity, and availability.

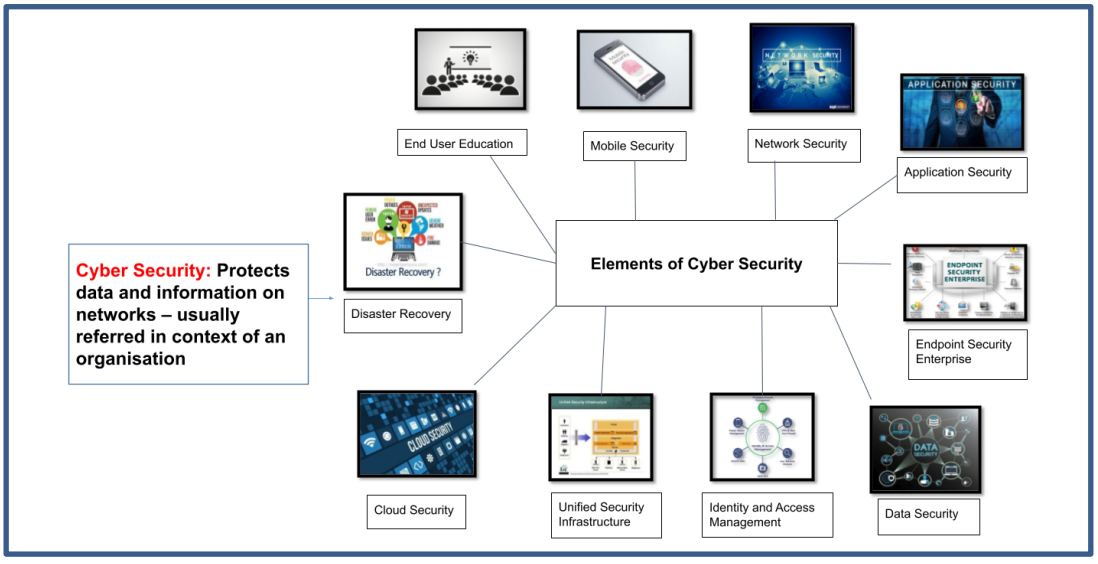


Fig. 1.3 Elements of Cybersecurity (Source: IIPA)

1.3.12 Information Security

Information encompasses various data types, including personal details, social media profiles, cell phone data, biometrics, and more. The practice of safeguarding this data against unauthorized access, use, disruption, disclosure, alteration, inspection, recording, or destruction

is termed as information security. Therefore, information security covers a broad spectrum of research fields, including cryptography, mobile computing, cyber forensics, and online social media, among others. Information security programs are constructed around three fundamental principles, commonly known as the CIA Triad:

- Confidentiality: Ensuring protection against unauthorized access to data and systems.
- Integrity: Ensuring protection against unauthorized changes or alterations to data.
- Availability: Ensuring access to authorized users as and when required.

1.3.13 Zero Trust Security

The Zero Trust Security model is based on three core aspects: verify every user, validate every device and transaction, and limit privileged access. In this, every identity is authenticated and authorized before access is granted. The core principle is "Never Trust, Always Verify."

1.3.14 Digital Forensics

Digital forensics is a term that combines elements of law and computer science to analyze data and secure data from computer systems, networks, wireless communications, and storage devices in a way that the information derived from them can be used as evidence in a court of law.

Digital forensics not only examines and interprets the motivation of the crime and reconstructs the evidence trail digitally but also identifies, collects, and analyzes the information found on computers, mobiles, and networks. They collect evidence of all types of crimes, such as murder, human trafficking, fraud, data theft, hacking attempts, drug dealing, or pedophiles.

Digital forensics makes it possible to recover even deleted e-mails and evidence after formatting the hard drive and investigating multiple users who have taken over the system.

Therefore, digital forensics techniques are useful in national security-related activities, including catching up with hardened criminals or pinning down deadly instances/criminals responsible for cyber espionage or cyber warfare.

1.4 Why Do People Fall Victim to Cyber Crimes?

It is almost an accepted fact that there are only two categories of entities in cyberspace. The first category of entities is 'who have already been hacked,' and the other category is of those 'who could be hacked.' Therefore, the biggest presumption that any entity can make in cyberspace is "I will never be hacked."

Individuals usually fall prey to cybercrimes, mainly for the following reasons:

- ***Ignorance*** – Ignoring current cybercrime trends can cause a person to become a victim. Hackers can spend months analyzing the loopholes in their victims' behavior and daily routine and then exploit them. The technique of studying and exploiting human behavior for cybercrime is also called the 'social engineering' technique. In this technique, the fraudsters usually use the digital users' ignorance and try to pick them up as a fraud.
- ***Trusting strangers*** – Cybercriminals employ strategies and present themselves as genuine to innocent victims. For example, hackers can have easy access to the company's networks by sending e-mails wherein they pose as co-workers. Unknowinglygullible individuals could trust such rogue individuals and, thus, end up providing sensitive information such as passwords and company credit card details to the hackers/rogue individuals. Cybercriminals can also create a sense of urgency and take advantage of theconfusion to deceive the victims into giving their sensitive financial /personal information.

- ***Underestimating the risk*** – In certain instances, victims become overconfident and end up underestimating the potential risks of revealing too much of their sensitive personal information in cyberspace. They, thus, end up sharing their passwords /OTP /Pins /CVV numbers with strangers or even with known ones.

1.5 Why Do People Commit to Cyber Crimes?

Similarly, individuals or groups of individuals commit cybercrimes primarily for the following reasons:

- ***Social Reasons***: The internet is being highly used for social abuse and harassment. Social abuse and harassment are defined as repeated and unsolicited behaviour by a threat vector through cyberspace with the intent to intimidate, humiliate, threaten, harass, or stalk the user. With the rapidly growing technology, internet users commit cybercrimes by engaging with users on various social media platforms. A number of cyberattacks are committed to directly or indirectly affect cyberspace users of diverse age groups.
- ***Financial Gains***: The threat actors utilize various techniques within cyberspace to facilitate their money-making efforts. Frauds are committed with the motive of gaining financial benefits. This occurs when someone steals one's money. This can be accomplished through various means, including identity theft and investment fraud.
- ***Cyber Espionage***: Cyber espionage is an intrusion to get secret information about an individual, an organization, or a nation. Cyber espionage is not an act of war but could be used as a tool to defeat the enemy state in a war. Some occurrences of cyber espionage could generate severe tensions between two nations and are therefore also frequently referred to as 'attacks.'

Based on this basic understanding of human behaviour and plausible reasons for becoming cyber-victims or cybercriminals, let us now try to understand the 'Threat Landscape'[3] of cybercrimes in the following section.

1.6 Threat Landscape of Cybercrimes

Threat Landscape would provide us with an overview of who could be potential 'Targets' of cybercrime. The victims of cyberattacks are generally individuals, organizations, or nations. Threat Landscape also explains who could be various kinds of perpetrators of cybercrime, also referred to as 'Threat Actors.' It then moves on to explain 'Motives' or reasons why threat actors commit a crime. Last but not least, the threat landscape also indicates what tools, referred to as 'Attack Vectors,' are used by criminals (threat actors) to initiate a cybercrime (Fig 1.4).

- **Targets:** The target/victim of any cybercrime could be an individual, an organization, or a nation.

- **Threat actors:** The threat actors could be several. These could be professional cybercriminals, malicious insiders, or hacker groups. Threat actors are constantly exploiting the 'bugs' in hardware/applications and weaknesses or vulnerabilities in humans/digital users.

  It is pertinent to note that in this handbook, the term 'threat-actors' has been referred to by several of its related terms, including 'fraudster,' 'scammer,' 'cybercriminal,' 'attacker,' 'hacker,' 'rogue actor' and so on. These references have been made according to the context.

[3] https://egyankosh.ac.in/bitstream/123456789/91742/1/Block-5.pdf

- **Motives/Reasons:** The motives for undertaking a cybercrime could be financial or for sheer amusement or to harass someone. Cyberattacks, generally, vary from an individual, organization, or nation by way of disruption of various services.
- **Attack Vectors:** Attack vectors are the paths or means by which an attacker gains unauthorised access to a computer system, network, or application to exploit vulnerabilities and carry out a cyber attack. Attack vectors can take various forms and exploit different weaknesses in a system's defenses.

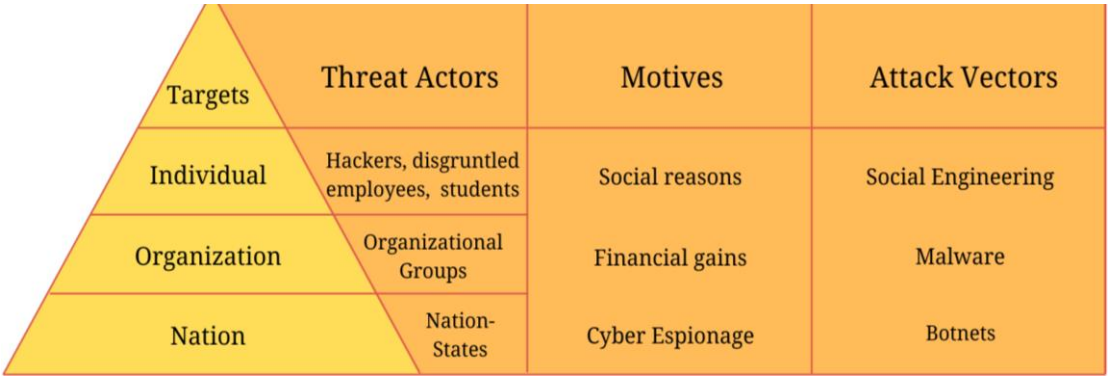


Fig. 1.4 Threat landscape (Source: IIPA)

1.7 Understanding Attack Vectors

Now, once we have understood some of the main reasons that threat actors commit or fall prey to a cybercrime along with essential aspects of the threat landscape, let us proceed to cover in detail some of the basic tools that threat actors employ to commit a cybercrime. These 'tools' are also called 'Attack Vectors'. Various kinds of popular attack vectors are explained in the following section.

1.7.1 Social Engineering

As already explained earlier, social engineering techniques refer to the soft techniques that usually include psychological manipulation of the victim by the threat actors. As indicated in the previous section, this manipulation could be done by calling them - pretending to be a potential job employer, or by sending an e-mail - pretending to be a co-worker. It can be undertaken through a voice call, video call, WhatsApp message, text message, or even an e-mail message to the potential victim in a manner to induce feelings of urgency, fear, or other comparable emotions. All such tricks could prompt the victim to reveal sensitive information. He/she could also be provoked to click a harmful link or open a malicious file. There are several social engineering toolkits that are freely available.

The Kali Linux operating system offers free social engineering toolkits like Maltego and Social Engineering Toolkit (SET).

1.7.2 Malware

Malware refers to programs such as viruses, worms, trojan horses, and rootkits that are designed to harm a computer/mobile/network device. Malware can get into the system in numerous ways, such as through opening e-mail attachments that contain malware, downloading infected files while data sharing, clicking on links in an instant messenger or chat rooms, or from active content applications on web pages (Since malware is quite relevant, we explain it in detail in the subsequent chapter).

1.7.3 Advanced Persistent Threats (APTs)[4]

An advanced persistent threat is a broad term to describe an attack in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network/network device to extract highly sensitive data. APTs are usually sponsored by nations or very large organizations. Businesses holding a large quantity of personally identifiable information are at high risk of beingtargeted by advanced persistent threats. They conduct research to identify previously unknown vulnerabilities and exploit those vulnerabilities to gain access to systems in an undetected manner.

For instance, Stuxnet, an APT, took down Iran's nuclear program. In 2010, U.S. and Israeli cyber forces attacked the Iranian nuclear program to slow down the country's ability to enrich uranium.

It is important to remember that this list of attack vectors explained herewith is not exhaustive. However, respecting the basic nature of this handbook, only some of the attack vectors have been covered.

1.8 Basics of Being Cyber Safe

Irrespective of the nature of the attack or attacker, one could always minimize the damages of cybercrime if the basic do's and don'ts, such as creating strong passwords, restricting access to personal information, respecting the privacy of others, and many more, are kept in mind (may refer Annexure at the end of the booklet).

Table 1.1 General Digital Hygiene Tips (Do's and Don'ts)

General Digital Hygiene Tips	
Do's	
1.	It is essential to adopt a rigorous "zero-trust" approach, which includes keeping theprivacy settings of all devices and apps stringent.
2.	Install all-important utilities on your digital devices, such as antivirus software, firewalls, and virtual private networks (VPN helps to camouflage real IP addresses).
3.	Procure all-important utilities from authorized sources or authorized app stores only.
4.	Use well-designed passwords for your accounts, different for each account, or use password managers.
5.	Alternatively, use hardware keys.
6.	Change all your passwords every month or use a password manager utility.
7.	Regularly update all your software.
8.	Switch off the Internet, Location, and Camera when not in use.
9.	Use only those trusted e-commerce websites that are accessible through HTTPS or padlock signs.
10.	Make sure that everything and everyone is verified before any access is granted to any information.

[4] https://informatics.nic.in/uploads/pdfs/fb12995f_36_37_tup_apt.pdf

General Digital Hygiene Tips	
Don'ts	
1.	Do not expose personal details such as DoB, Date of Graduation, Parents' Name onsocial media, or financial credentials such as PIN/CVV; hide them as much as possibleas these details could be easily manipulated for fabricating your identity by fraudstersor could lead to your login credentials.
2.	Do not react to spam e-mails or suspicious friend requests.
3.	Do not click on links that are accessible through unverified addresses.
4.	Do not install apps that come from unknown sources or are free.
5.	Do not fall for 'Free Offers' - if there is no/ less cost of the product,
6.	Do not grant unnecessary permissions to contacts/calendars/cameras to other apps that do not require it. For e.g., a cab-sharing app does not need to be given access to thecamera and so on.
7.	Do not click on the 'Remember Me' or 'Remember Password' options.
8.	Do not search for customer care numbers of your banks or utility service providersfrom your browsers; instead, go to the source website/correspondence flyers to look for the same.
9.	Do not undertake financial transactions in free Wi-Fi/public Wi-Fi zones.
10.	It is advised not to keep any sensitive photographs/videos, or any personal document in your mobile phone's storage. The personal documents may be Aadhaar cards, Voter IDs, PAN cards, Credit/Debit cards, private information on medical health, Income tax info., etc.
11.	Use of free internet in public places may be avoided, particularly for financial transactions, etc.
12.	There are issues particularly related to R&D Institutions, which may lead to data leakages, piracy issues, etc. The users must avoid the following: i. Open-source softwares freely available to convert doc to pdf, vice-versa, or to other formats, image resize, format converters jpg, jpeg, png, etc. ii. Online statistical/ mathematical tools, etc. iii. Many open-source software are available for free use and are downloaded by users. These may contain malicious codes (hidden segments) and could result in data theft. iv. Use of storage services provided by many private companies like Amazon, Google, Microsoft, IBM, etc. must be avoided.

However, this list of do's and don'ts is not exhaustive. We will uncover many more of these safetytips in the subsequent chapters.

1.9 Be Cautious and Follow Internet Ethics

Internet ethics are a set of moral principles that govern an individual or a group on acceptable behaviour while using digital devices. One should always be honest and respect the rights and privacy of others on the internet. Some of the basic rules that must be followed by an individual while using the internet include various caution points such as changing passwords regularly, never responding to unknown people on the internet, never sharing personal information with anyone, trusting information from genuine sources only, and much more (Fig. 1.5).

Fig. 1.5 Rules to follow, internet ethics (Source: ISEA Awareness portal)

Chapter 2: Malware and its Types

2.1 Understanding Basics of Malware

Malware refers to malicious apps that, upon installation, infect the victim's device with viruses or harmful scripts, etc. This could sabotage the smooth functioning of the device itself or collectuser information such as GPS coordinates, contact lists, and so on. This collected user information could be further shared with third parties who could misuse the same for their own/corporate gains.

For instance, Indian taxpayers were targeted by a malicious app impersonating 'ITR Mobile'. When unwittingly downloaded on the phone, the app requests permission to access Accessibility services. If granted, it could monitor and capture sensitive information such as banking details, PAN number, Aadhaar number, address, date of birth, mobile number, and email address. This allows hackers to steal login IDs and passwords for internet banking. The app then transmits these details to a third party, likely a fraudster, while displaying a fake update screen to deceive the user.

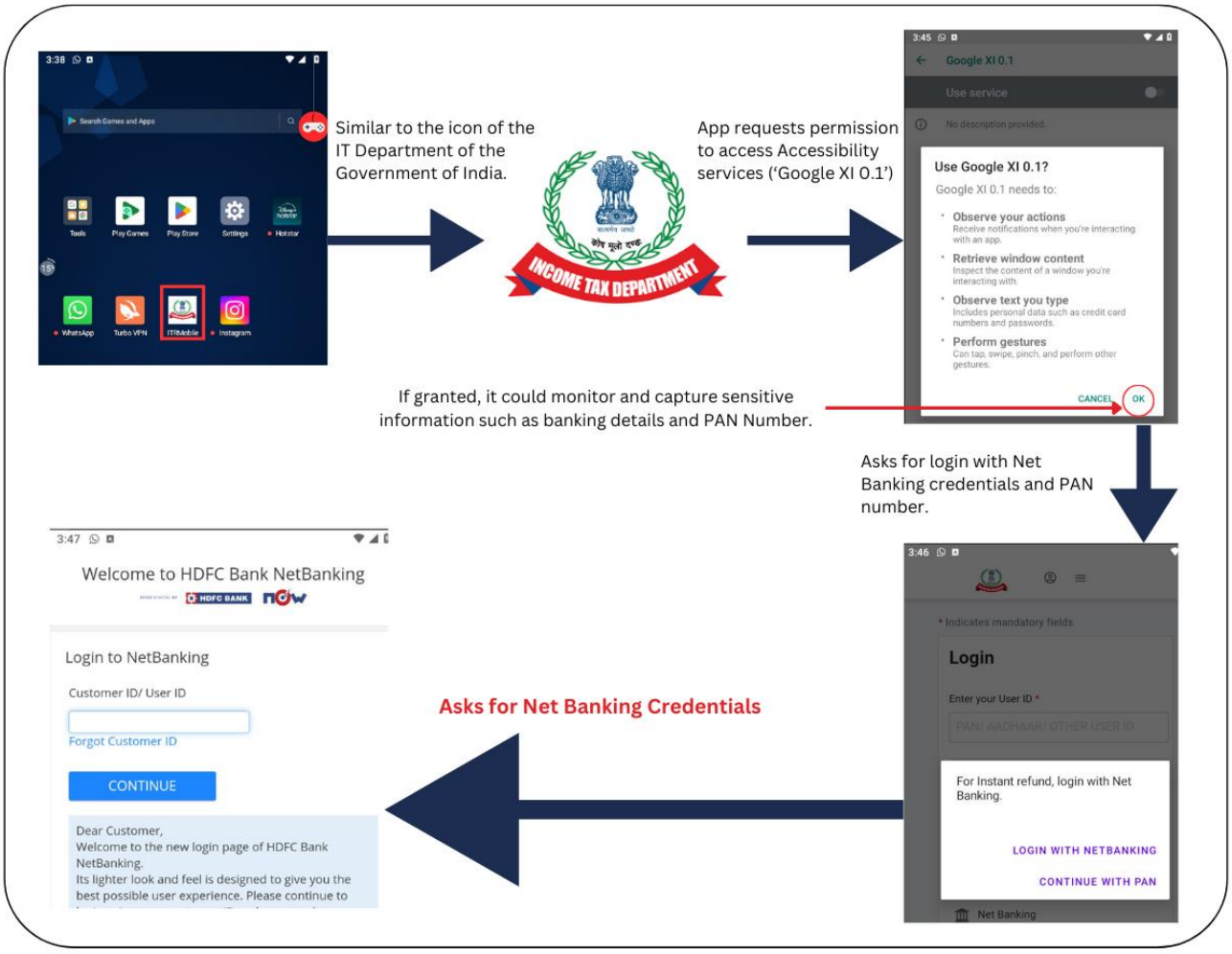


Fig. 2.1 A case of a malicious app

2.2 Types of Malware

2.2.1 Virus

A virus is a type of malware that duplicates itself by embedding its code into other programs. It spreads via infected websites, USB drives, and emails by attaching to legitimate files or data. The virus is triggered when the user opens the infected file or application. Once activated, it can delete or encrypt files, modify programs, or impair system functions.

2.2.2 Worm

A worm is a type of malware that replicates itself and propagates automatically across a network. It takes advantage of vulnerabilities in security software to steal sensitive data and install backdoors (which will be explained in the next section) that can be used to access the system, damage files, and cause other harm. Worms use up a lot of memory and take up a lot of bandwidth. As a result, servers, individual systems, and networks get overworked, go slow, and even crash in certain instances.

2.2.3 Trojan

A Trojan horse, commonly referred to as a 'Trojan,' is harmful software that disguises itself as legitimate but can take over a computer. Its purpose is to damage, disrupt, steal, or otherwise compromise data or networks. To deceive users, a Trojan presents itself as a genuine application or file. There is one unique feature of a Trojan. Viruses can execute and replicate, but a Trojan cannot do so.Trojans must be executed by the user, and this is the reason they are attached to an executable file.

For instance, a person downloaded an executable file thinking of installing it as a game, but with it, a Trojan has also been attached. Once the person runs that Exe file, along with the game, the Trojanalso gets installed on the device, and the attacker gets access to the device remotely.

2.2.4 Backdoor

A backdoor is a type of malicious software that grants unauthorized remote access to a device or program by exploiting system vulnerabilities and flaws. It operates stealthily in the background, keeping the victim unaware. With full control over the system, the attacker can perform harmful actions undetected. The system becomes susceptible to unauthorized file copying, modification, data theft, and many other things.

2.2.5 Rootkits

A rootkit is a type of software that enables hackers to access and control a device. While most rootkits target software and operating systems, some can also infect the hardware and firmware. Rootkits excel at concealing their presence, remaining hidden yet fully operational, allowing unauthorized access to the device. They enable hackers to carry out various malicious activities, such as stealing sensitive data and financial information, installing malware, or using the compromised device as part of a botnet (which will be explained in the next section) to send spam or engage in Distributed Denial of Service (DDoS) attacks.

2.2.6 Bots and Botnets

A bot is a software application designed to carry out automated, repetitive, and predefined tasks. Companies and individuals employ bots to do repetitive activities that humans would otherwise perform. When compared to human effort, bot tasks are usually simple and completed at a considerably faster rate. Bots can perform useful functions, such as providing customer support or indexing search engines. However, they can also be malicious, used to gain full control over an unauthorized device (Fig. 2.2).

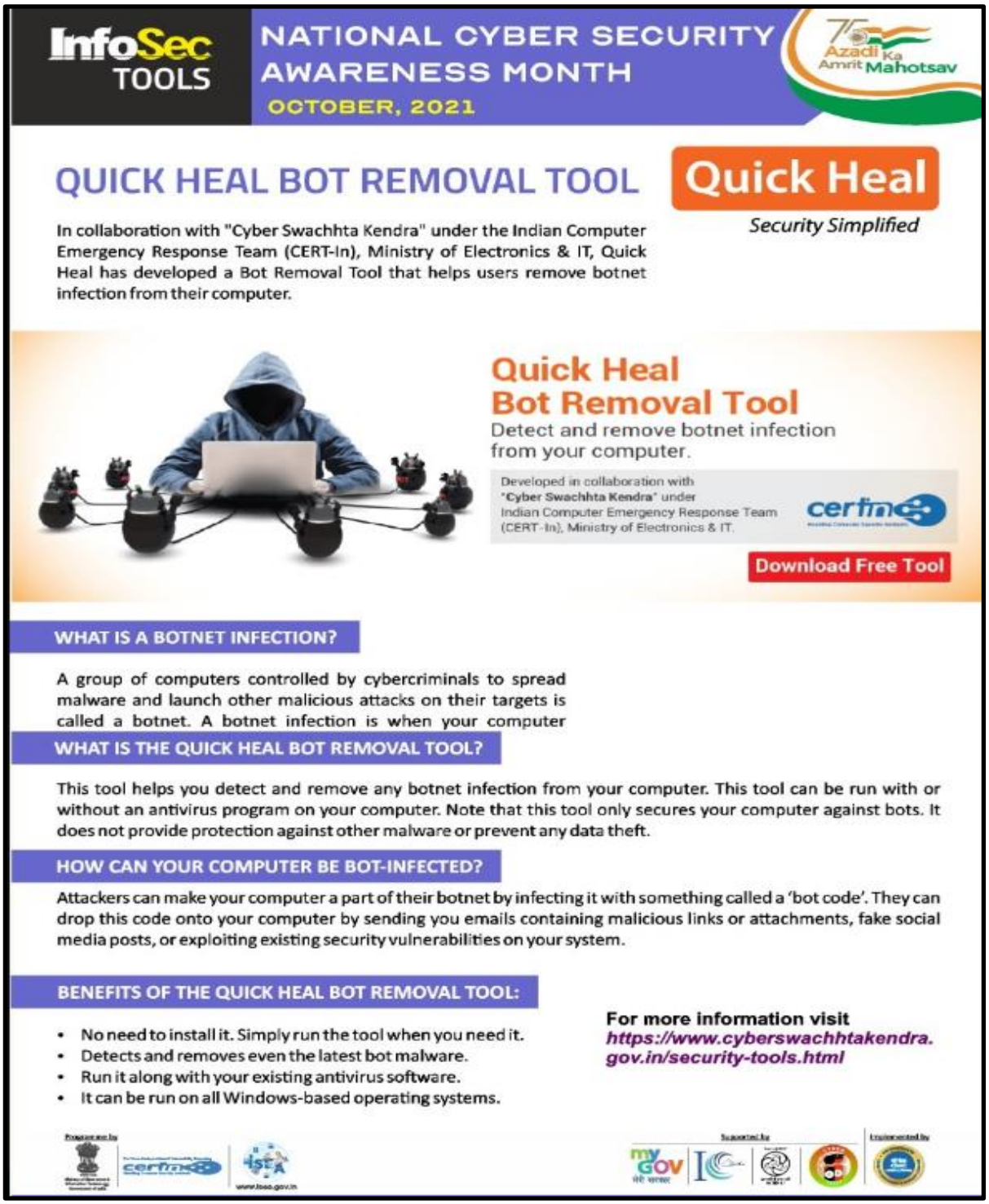


Fig. 2.2 Bots: Risks and Countermeasures (Source: ISEA Awareness portal)

A botnet is a collection of internet-connected devices that individually run one or more bots, frequently without the device owners' knowledge. Malware bots and internet bots can be programmed to breach user accounts, search the internet for contact information, transmit spam, and perform other malicious activities. Attackers may deploy harmful bots in a botnet to carry out these

activities and hide the source of the activity. Like any other malware, bots, and botnets are distributed and downloaded from social media or e-mail communications that provoke the victim to click a link. A bot might show up as a warning stating that the device will be infected with a virus if the user does not click on the connected link. By clicking the link, the user can infect the device with a virus that may damage the device in the following ways:

- **Unauthorized access** - Unauthorised Access refers to unauthorized attempts to bypass the security mechanisms of a computer/information system or network.
- **Data breach** - A data breach occurs when malicious insiders or external attackers gain unauthorized access to confidential or sensitive information, such as medical records, financial data, or personally identifiable information (PII).
- **IoT attacks** - IoT attacks include any cyberattacks that seek to gain access to (or control over) IoT devices with the intent to either cause harm to the devices or use them in attacks against other targets.

2.2.7 Advanced Persistent Threat

An advanced persistent threat (APT) is a broad term used todescribe an attack in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network/network device to extract highly sensitive data.

2.2.8 Ransomware

Ransomware is a form of crypto-virological malware that restricts access to a victim's personal data until a ransom is paid. While basic ransomware may only lock the system without harming files, more sophisticated versions employ a method known as cryptoviral extortion. This technique encrypts the victim's files, rendering them inaccessible, and requires a ransom payment for decryption.

Attackers might targetto lock systems or encrypt files of universities, government organizations, law firms, or other organizations with sensitive data and easy security systems.

2.2.9 Scareware

Scareware is a type of malicious software that deceives users into visiting fraudulent or malware-infected websites. Scareware may come in the form of pop-up ads that appear on the user's device screen. Scareware combines social engineering and fear tactics to force victims into purchasing and downloadingmalware. Usually, the alerts indicate that infected files have been discovered on the device, and to resolve the issue, the victim must purchase the software. However, no infected files exist, and the suggested software is most likely malware.

Fig. 2.3 Scareware: A fake alert to scare off the victim

2.2.10 Adware

Adware is malicious software that displays unwanted pop-up advertisements which can appear on a computer or mobile device. Such adware is usually downloaded along with software programs or apps from the internet. Free software which contains some advertisements may be annoying but is not illegal. However, even if a third-party program adds malicious ad software onto a user's device after obtaining the user's consent, it is illegal.

2.2.11 Keylogger

A keylogger is a type of malware that is especially challenging to detect. This software application tracks users' activities, providing hackers access to their personal information. By recording keystrokes, it can uncover passwords, credit card information, and frequently visited websites. The program installed on the computer captures every keystroke made by the user. The log file is then sent to a server, where fraudsters await its use. One can enable the task manager to detect if a keylogger is active, which could detect all active and unknown applications. One can also do a full malware scan displaying the complete list of detected threats.

2.3 Safety Tips to Prevent Malware

Such a long list of malware (which is still not exhaustive) could create unrest in the mind of any casual reader, too. However, as listed below, some basic tips[5] would go a long way to safeguard against major data/reputation loss.

Table 2.1 Safety Tips to Prevent Malware (Do's and Don'ts)

Safety Tips to Prevent Malware
Do's
1. Exert all caution in mind before opening e-mail attachments or images, particularly if the sender is unknown/unreliable.
2. Install anti-malware, antivirus software and applications only from authorized providers/ sources such as Play Store, App Store, or the company's official website.
3. Download files only from trusted sources. Avoid downloading attachments from unknown senders or clicking on suspicious links, even if they come from seemingly familiar sources.
4. Keep your operating system and software updated with the latest security patches. Most systems have built-in firewalls, so make sure they are enabled.
5. Regularly backing up your important files allows you to restore them in case of a malware attack.

[5] https://egyankosh.ac.in/bitstream/123456789/91742/1/Block-5.pdf

Safety Tips to Prevent Malware
Don'ts
1. Avoid logging into personal or professional accounts, such as email or banking, when connected to a public Wi-Fi network.
2. Don't open attachments from unknown senders or emails that appear suspicious.
3. Avoid visiting websites known for distributing malware, such as illegal downloading sites.
4. Security software is there to protect you, so don't disable it.
5. Pirated software often comes bundled with malware, so avoid using it. Stick to legitimate sources for your software.

2.4 How to Cure a Malware Infected Device

One could try the following checklist to de-infect the device.

1. If the slightest sign of infection (such as the device misbehaving, going slow, restarting repeatedly, etc.), one should first disinfect the device with an authentic antivirus.
2. Simultaneously, the victim could proceed to change all the passwords.
3. If a pop-up stays on the screen longer than usual, the browser can be closed bypressing Ctrl + Alt + Delete on the keyboard. Minor malware infection is usually resolved byrebooting the device.
4. As soon as there is any suspicion of infection, the victim should disconnect the device from the internet to avoid any further infection. This is very helpful in cases where the fraudster couldhave left a remote access trojan on the victim's device to reconnect it to his device remotely.
5. The last and the safest (but not the easiest) resort is to format the hard drive and install a clean operating system.
6. If the device is still malfunctioning, it would be most logical to take it to an authorized service provider or Cyber-Swachhta Kendra (https://www.csk.gov.in/about.html) of the Government of India or make use of the M-Kavach 2 mobile app (explained in detail in a later chapter).

The 'Cyber Swachhta Kendra' (CSK) is managed by the Indian Computer Emergency Response Team ("CERT-In") as part of the Government of India's Digital India program to detect and remove botnet infections across the country. (Fig. 2.4).

(Fig. 2.4 Home page of Cyber-Swachhta Kendras (https://www.csk.gov.in/about.html)

Chapter 3: Some Popular Types of Cyber Crimes

Now that our basics have been established, let us cover some of the more popular types of cybercrimes that have been trending in recent times.

3.1 Phishing[6]

A phishing attack is a tactic to deceive individuals into revealing confidential information through email, SMS, or WhatsApp.These sources usually contain a hyperlink text or a spurious link. When the victim unwittingly clicks on this link, he/she either downloads malware or unwittingly shares their sensitive personal details. It involves acquiring or attempting to obtain sensitive banking information, such as usernames, passwords, and credit card numbers. Phishing e-mails and SMS messages try to confuse the victim in several ways by sending messages that sound urgent. These messages may include alerts about unusual activity or attempted logins, requests to update payment information, and similar prompts. They might also ask users to verify personal details, send fraudulent invoices, require payment through a link, claim eligibility for a government refund, or offer coupons for free items.

3.1.1 E-mail Phishing

Email phishing seeks to obtain confidential information by sending messages that look like they come from a trusted source. This type of attack is not targeted and can be executed on a large scale.

The sender expects the user to click on the link given in the e-mail and share some personal details, intimidating them that their account is prone to unauthorized activity.

3.1.2 Spear Phishing/Whaling

Spear phishing entails sending emails or messages to specific individuals while pretending to be a trusted sender to convince them to share personal information or money or to compromise their digital devices. Unlike typical phishing attacks, spear phishing is highly focused and carefully researched, primarily aimed at business executives, public figures, and other high-value targets.

3.1.3 Vishing

Vishing, or voice phishing, occurs when a malicious caller impersonates a technical support or customer service representative, a government agency, or another organization to obtain sensitive information, such as banking or credit card details, via phone calls or voice messages (Fig. 3.1).

Any call from an unfamiliar number can pose a risk to the recipient, particularly those from phone numbers with two or three digits that start with the prefix "+."

3.1.4 Smishing

Smishing, often known as SMS phishing, is a cyberattack carried over mobile text messages. It occurs across various mobile text messaging platforms, including non-SMS channels such as data-based mobile messaging apps. Victims are tricked into providing crucial information to a fraudster through malware or fraudulent websites.

[6] https://incometaxindia.gov.in/pages/report-phishing.aspx

3.1.5 Pharming

Pharming is a deceptive cyber-attack that combines elements of farming and phishing. In this fraudulent scheme, cybercriminals install malicious code on a victim's computer or server, often through a bogus website. The victim is then directed to this fake website, where they may unwittingly provide personal information such as usernames and passwords. The attacker gains immediate access to this sensitive data. Pharming attacks exploit vulnerabilities in DNS (Domain Name System) servers, which are responsible for converting domain names into IP addresses. These attacks can occur by exploiting weaknesses in DNS server software or by altering the host's file on the victim's computer. Ultimately, cybercriminals intentionally redirect users to counterfeit versions of legitimate websites, aiming to steal their credentials.

Pharming is a cunning online trick. It's when illicit actors send real internet traffic to fake websites. These fake sites look real and try to steal important things like usernames, passwords, and bank details from people. Sometimes, they even put harmful software on your computer. One way they do this is called the 'Watering Hole Attack.' It's like waiting at a popular spot where lots of people go. These actors find out which websites a group of people often visit and put malicious content on those sites. When people from that group visit those sites, they get caught in the trap without knowing it. To do this trick, these actors first spy on what websites people like to visit. It's a cunning trick called 'social engineering' to figure out the best places to set up their trap.

Table 3.1 Safety Tips for Prevention from Phishing Attacks (Do's and Don'ts)

Safety Tips
Do's
1. Verify the sender's identity: Always verify the identity of the sender or caller before providing any personal or sensitive information.
2. Be cautious of links and attachments: Take care when clicking on links or downloading attachments from emails, SMS messages, or other sources, particularly if they seem suspicious or unexpected.
3. Use secure communication channels: Whenever possible, use secure communication channels, such as encrypted emails or secure messaging apps, to exchange sensitive information.
4. Enable security features: Enable security features such as email filters, spam detection, two-factor authentication, and encryption to enhance protection against cyber threats.
5. Stay informed and educate others: Keep up-to-date on the latest cybersecurity threats and online safety best practices. Share this knowledge with others in your household or organization to help them recognize and respond to potential threats effectively.

Safety Tips
Don'ts
1. Trust blindly: Avoid blindly trusting emails, phone calls, or messages from unknown or unverified sources, especially if they request personal or financial information or urge urgent action.
2. Provide personal information: Refrain from providing personal or sensitive information, such as passwords, Social Security numbers, or financial details, via email, phone, or other communication channels unless you can verify the legitimacy of the request.
3. Click on suspicious links: Avoid clicking on links or responding to messages that contain suspicious or unexpected content, as they could lead to phishing websites, malware infections, or other cyber threats.
4. Ignore security warnings: Take security warnings seriously, especially those issued by your web browser, email service provider, or antivirus software, and avoid ignoring or dismissing them without further investigation.
5. Neglect software updates: Regularly update your operating system, web browser, antivirus software, and other applications to patch security vulnerabilities and protect against known cyber threats.

3.2 Identity/Credential Theft

Identity theft is the act of obtaining some other person's personal information (PI), particularly personally identifiable information (PII), personal sensitive information (PSI), or personal confidential information (PCI) without their permission (Fig 3.1). Let us try to understand the difference between these similar and yet very different terms.

The term 'personal information' (PI) refers to a wide variety of information, including, but not limited to, one or more of the following categories (Table 3.1):

Table 3.2 Types of Personal Information (PI)

S.No.	Type of Personal Information (PI)
1.	Information or opinion about an individual's racial or ethnic origin
2.	Individual's political opinion
3.	Individual's religious beliefs
4.	Information or opinion about an individual's sexual orientation
5.	Criminal records
6.	Health information (medical records)
7.	Credit information
8.	Employee record information (subject to exemptions)
9.	Tax file number information
10.	Digital ID information (IP addresses, login IDs, passwords, cookie identifiers)

This personal information could have various aspects, which are identity-related, sensitive, and confidential.

- Personally identifiable information (PII) is any information that identifies or describes an individual. Identifying an individual could be as simple as a name or a number or include digital identifiers such as an IP address, cookie identifier, or login credentials.
- Personal sensitive information (PSI) would include information or opinions about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation, or criminal records. This definition varies from country to country.
- Confidential information is the information that the user decides to keep secret. For instance, if a user wants to keep her phone number a secret, then it is confidential; otherwise, it is not.Confidential information is also called 'classified information' because it is classified as confidential for some reasons only known to the user. Personal confidential information (PCI) may contain a person's phone number, address, bank account number, *Aadhaar* number, credit/debit card number, and passwords.

These discussions clearly reveal that personal information can lead to the disclosure of one's financial details, medical records, and other critical personal records. Therefore, it is crucial to keep personal information secure to prevent identity theft.

Identity theft occurs through access to social media accounts, personal documents, or skimming of credit/debit cards, and so on. Identity theft can be carried out by using various cybercrime techniques like social engineering, phishing attacks, and malware. Identity theft allows threat vectors to impersonate another individual to carry out various kinds of fraud, including identity fraud, financial fraud, social media crimes, and many others.

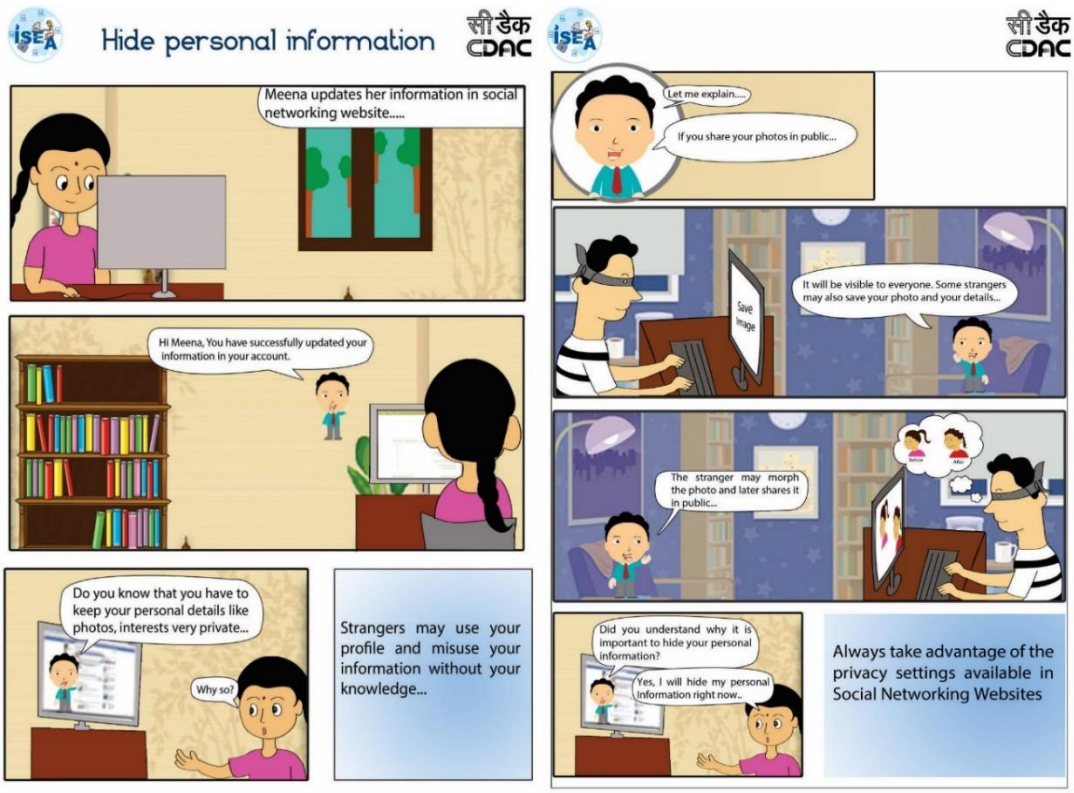


Fig. 3.1 Identity theft: The need to hide personal information (Source: CDAC)

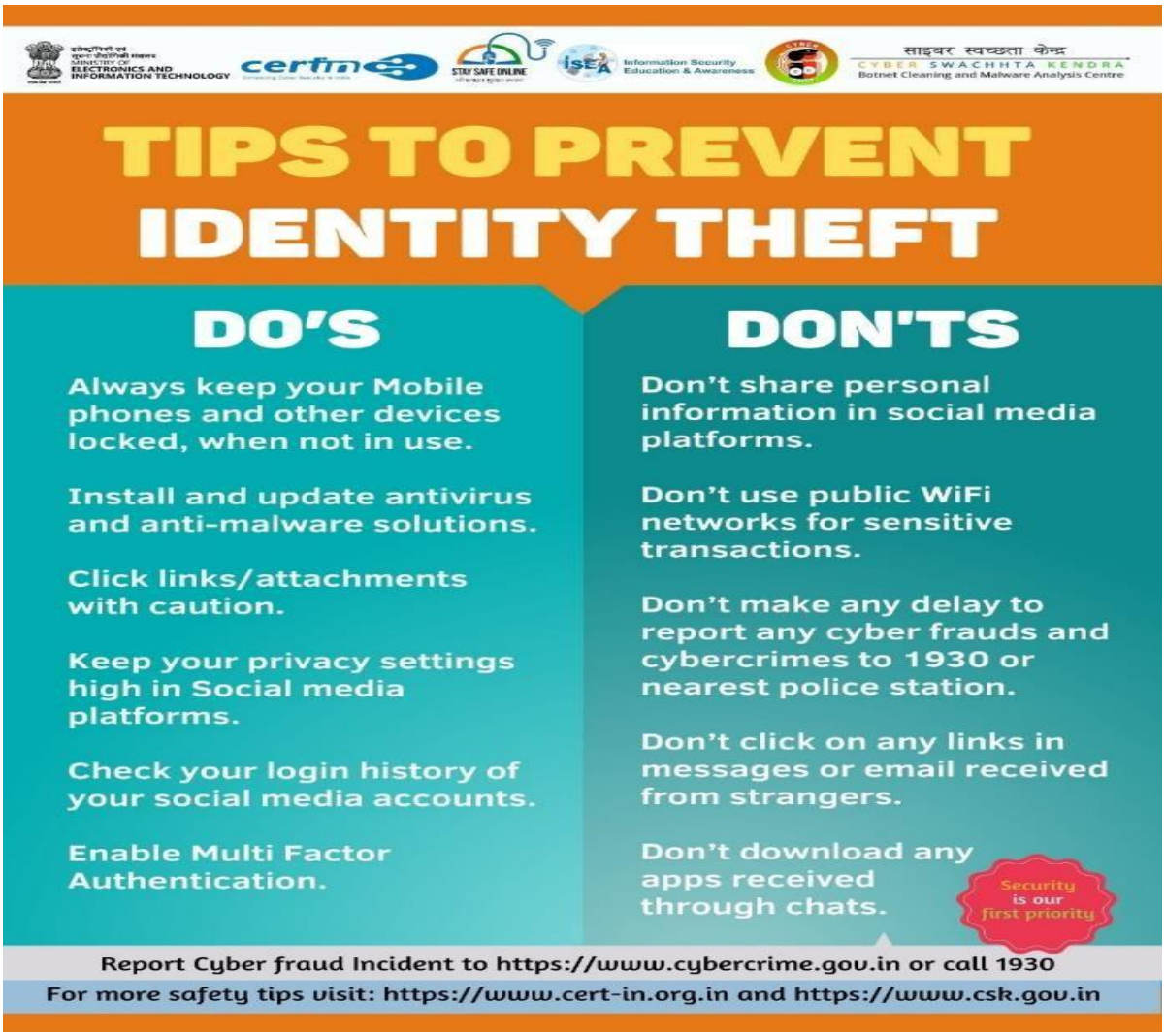


Fig 3.2 Tips to Prevent Identity Theft (Do's and Don'ts)

3.2.1 Shoulder Surfing

Shoulder surfing is done to obtain personal data such as PIN, passwords, and other sensitive information by secretly watching a target, usually over their shoulder. Thus, they observe the keystrokes or listen to sensitive information sent by the victim or by spying through overhead CCTV cameras, critically positioned over their keyboards, entering a pin at a cash machine/ATM, while filling a form, or while paying with a credit card. Shoulder surfing is an effective strategy for obtaining personal information, particularly in crowded areas where the victim is observed. Shoulder surfing also happens when the fraudsters install a reading device, such as a skim reader on an ATM to steal information.

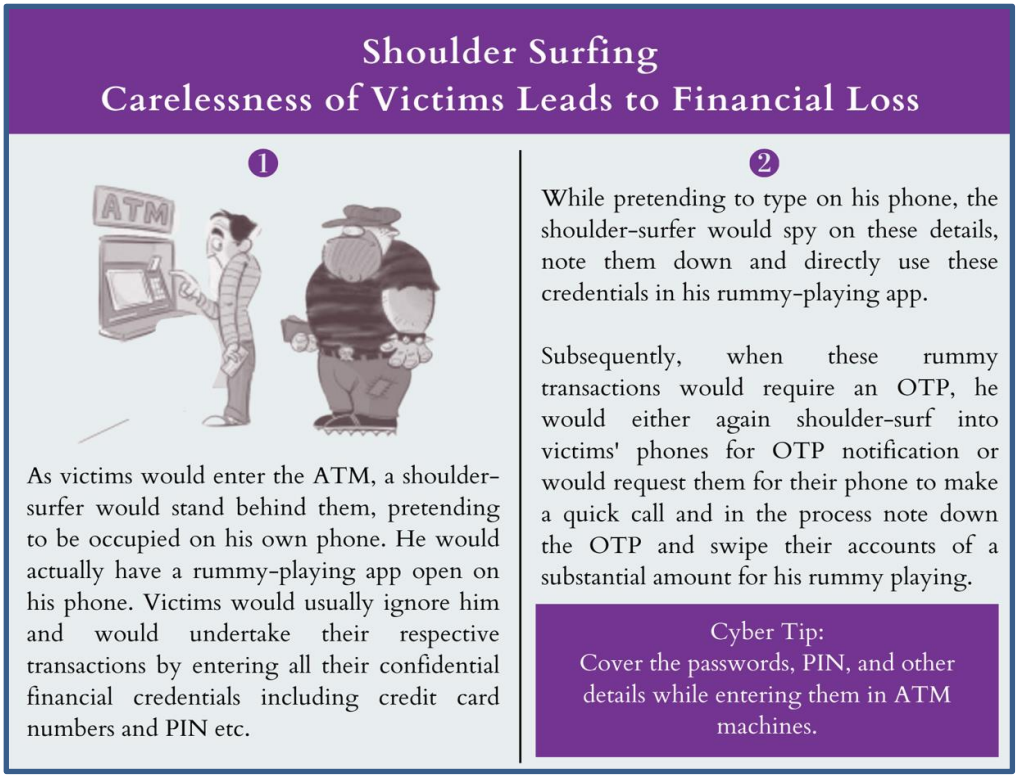


Fig. 3.3 Shoulder surfing: Carelessness of victims leads to financial loss (Source: IIPA)

Table 3.3 Safety Tips to Prevent Shoulder Surfing (Do's and Don'ts)

Safety Tips to Prevent Shoulder Surfing
Do's
1. Install a privacy filter that allows only the person sitting directly in front of the screen to seethe screen.
2. Use a password manager to create a strong password. It also consolidates all your passwords in one location.
3. Use biometric authentication as much as possible, such as - Facial recognition or fingerprint authentication, to minimize the need to input a PIN/password.
4. Pay attention to people standing close by in public places, especially when using ATMs, kiosks, or your phone for financial transactions.

Safety Tips to Prevent Shoulder Surfing
Don'ts
1. Don't leave the computer system unattended in any public space.
2. Avoid the temptation to write down your passwords on sticky notes or easily accessible locations.
3. Refrain from talking aloud about passwords, PINs, or other confidential details while in public areas.
4. Public computers may contain malware that can capture your keystrokes. Avoid using them for anything sensitive, like online banking.

3.2.2 Identity Frauds

Identity fraud happens when the stolen identity is used to commit various frauds, such as wrongfully gaining access to various resources, services, or goods.

Instances of such fraud include opening a bank account, obtaining credit cards, purchasing goods, applying for loans, committing offline crimes including murder, theft, etc., applying for jobs, or obtaining legal documents such as passports or licenses under a stolen identity.

3.2.3 Spoofing

Spoofing happens when threat actors attempt to conceal their true identities. They typically achieve this by impersonating a trusted partner or organization, misleading the recipient into believing the message is from someone else. Spoofing aims to unlawfully obtain sensitive information from the recipient, steal their login credentials (username and password), spread malware, and more.

For example, this can involve spoofing caller ID or the phone numbers displayed on incoming calls and text messages that appear to come from a targeted organization or individual.

3.2.4 Impersonation

Impersonation is a deceptive technique used to acquire basic credentials by posing as someone else. In this scheme, a malicious actor assumes the identity of another individual to illicitly access resources, credit, or privileges associated with that individual. While akin to spoofing, impersonation has distinct characteristics. Spoofing entails attempting to send communications from the exact user or company being targeted, whereas impersonation involves crafting communications that appear to be from the targeted user or company, though they originate from elsewhere.

Legally, "cheating by personation" occurs when an individual deceives others by assuming the identity of someone else, knowingly substituting one person for another, or misrepresenting themselves or another person as someone they are not. This offence applies regardless of whether the impersonated person is actual or fictitious.

Illustrations: (a) A deceives others by posing as a wealthy banker with the same name. This constitutes cheating by personation. (b) A deceives others by assuming the identity of B, a deceased individual. This also qualifies as cheating by personation.

3.2.4.1 Digital Arrest

'Digital Arrest Scam' is a latest modus operandi of cyber criminals where fraudsters impersonate police, CBI, or other government officials and falsely accuse victims of serious crimes, such as financial fraud, drug trafficking, or tax evasion. The aim of these criminals is to use fear and emotional pressure to extort money from their victims.

This scam typically starts with an unexpected phone call finally leading to a video call from someone posing as an official from a government agency. The criminals threaten immediate arrest to instill fear and compel the victim to act quickly. The victim is kept on the call for an extended period to prevent them from seeking help or verifying the information. Hence the name 'Digital Arrest'. The ultimate goal of the scam is to extort money from the victim.

If you get such suspicious call, report the number or source to 'Report & Check Suspect' section of cybercrime.gov.in

If you fall victim to this cybercrime report it by calling on 1930 or logging into cybercrime.gov.in

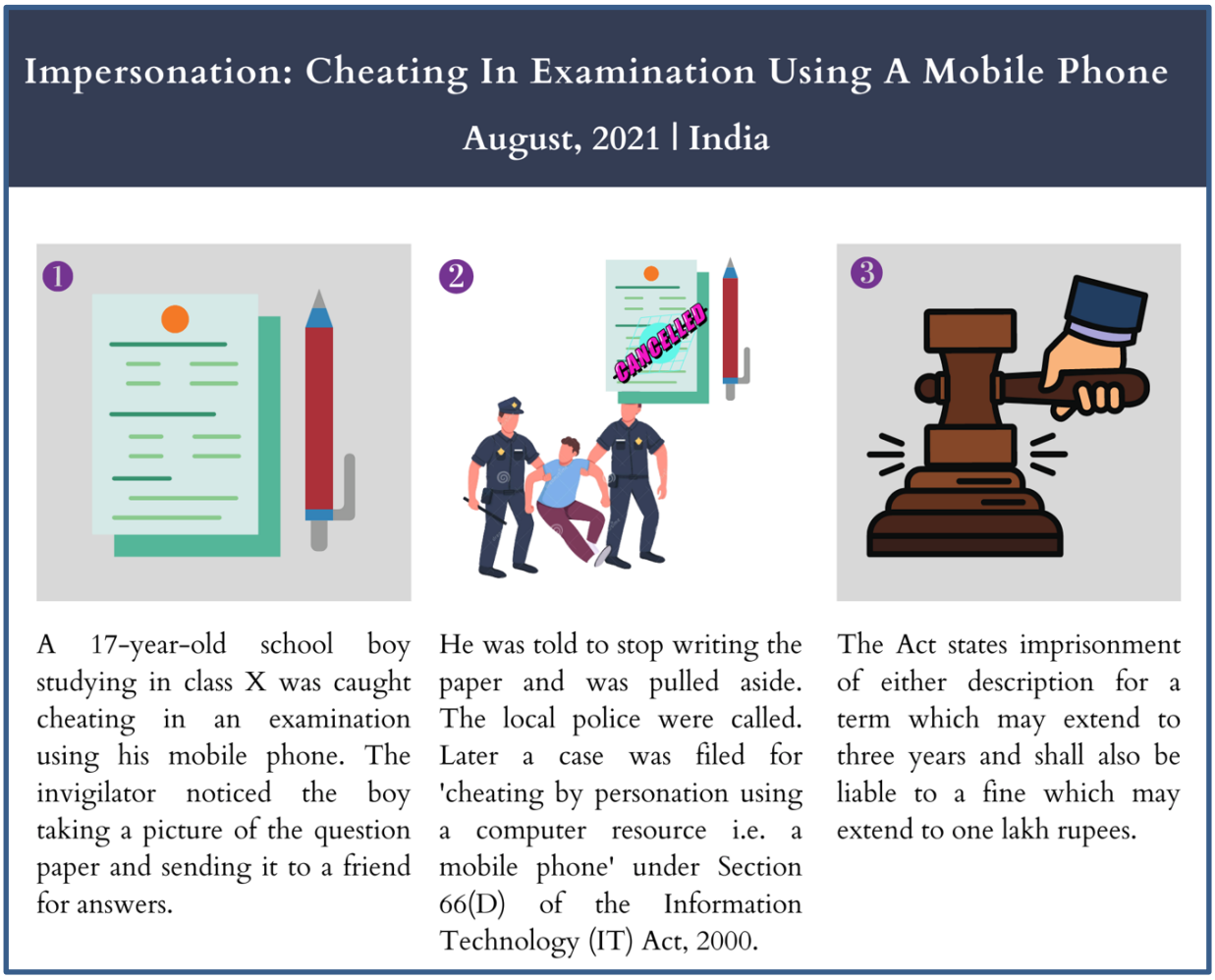


Fig. 3.4 Impersonation: Cheating in examination using a mobile phone (Source: IIPA)

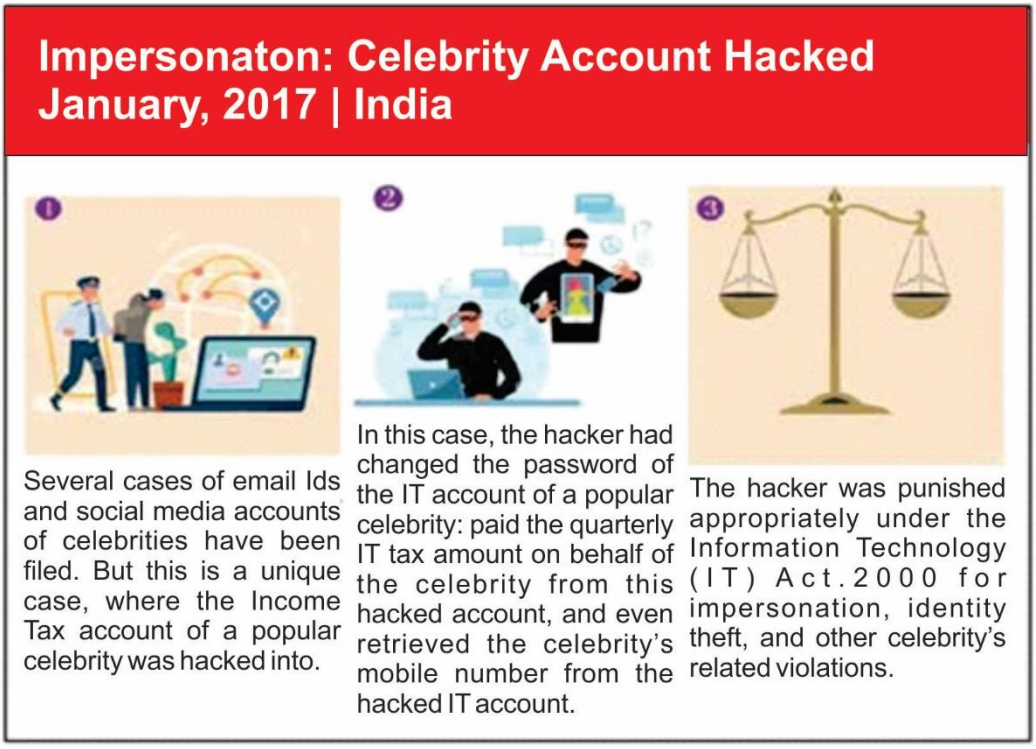


Fig. 3.5 Impersonation: Celebrity account hacked (Source: IIPA)

3.2.5 Application Frauds

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

Fig. 3.6 Application frauds: Accused procured 500 SIM cards using forged papers (Source: IIPA)

Table 3.4 Safety Tips to Prevent Shoulder Surfing (Do's and Don'ts)

Safety tips to Prevent Application Frauds
Do's
1. Monitor financial statements: Consistently review your bank statements, credit reports, and other financial accounts for unauthorized transactions or unusual activity.
2. Create strong passwords: Create robust and unique passwords for your online accounts, and activate two-factor authentication whenever possible to enhance security.
3. Verify sender's identity: Verify the identity of email senders or callers by asking for additional information or contacting the organization directly using verified contact details.
4. Be cautious of requests: Exercise caution with requests for personal information, financial transactions, or changes to account details, especially if they come from individuals claiming to be representatives of legitimate organizations or authorities.
5. Review application details: Thoroughly review the details of any applications for loans, credit cards, or other financial products before submitting them, ensuring accuracy and completeness.
6. Protect personal documents: Safeguard personal documents, such as identification cards, passports, and financial statements, to prevent unauthorized access or misuse by fraudsters.
7. Enable email authentication: Enable email authentication protocols such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to help detect and prevent email spoofing attacks.

Safety tips to Prevent Application Frauds
Don'ts
1. Share personal information: Avoid sharing sensitive personal information, such as Social Security numbers or bank account details, with unknown or untrusted individuals or organizations.
2. Click on suspicious links: Refrain from clicking on links in emails or messages that request personal information or direct you to unfamiliar websites, as they could be phishing attempts or malicious websites designed to steal your identity.
3. Trust caller ID or email addresses: Do not trust caller ID or email addresses alone, as they can be easily spoofed by attackers to appear as legitimate sources.
4. Blindly trust requests: Avoid blindly trusting requests for personal or financial information from unknown or unverified sources, as they could be impersonation attempts aimed at deceiving you into disclosing sensitive data.
5. Share confidential information: Refrain from sharing confidential or sensitive information with individuals or entities whose identities you cannot verify, especially if they request it via unsolicited emails, phone calls, or messages.
6. Provide false information: Avoid providing false or misleading information on applications for financial products, as this could constitute fraud and lead to legal consequences.
7. Fall for promises of easy credit: Be wary of offers for guaranteed approval or unusually low-interest rates, as they could be signs of fraudulent schemes aimed at luring unsuspecting individuals into application frauds.

3.3 Misinformation/Disinformation

Disinformation refers to the deliberate dissemination of misleading or biased information, often rooted in distorted narratives or facts, to serve a propaganda agenda. In contrast, misinformation is false information shared unintentionally, regardless of whether the intent is to deceive.

3.3.1 Fake Messages

Scammers often impersonate trusted individuals or institutions, crafting personalized messages to deceive their targets. To enhance the credibility of these messages, they frequently gather personal information from social media or compromised accounts*(Fig. 3.6)*.

The cybercrime unit of the Delhi Police has issued a warning regarding a potential scam where criminals are tricking unsuspecting users into verifying their phone numbers under the pretense of Know Your Customer (KYC) requirements. A tweet from the cybercrime unit indicates that scammers are sending fraudulent messages claiming that users' SIM cards will be deactivated if they fail to contact the phone numbers included in the message.

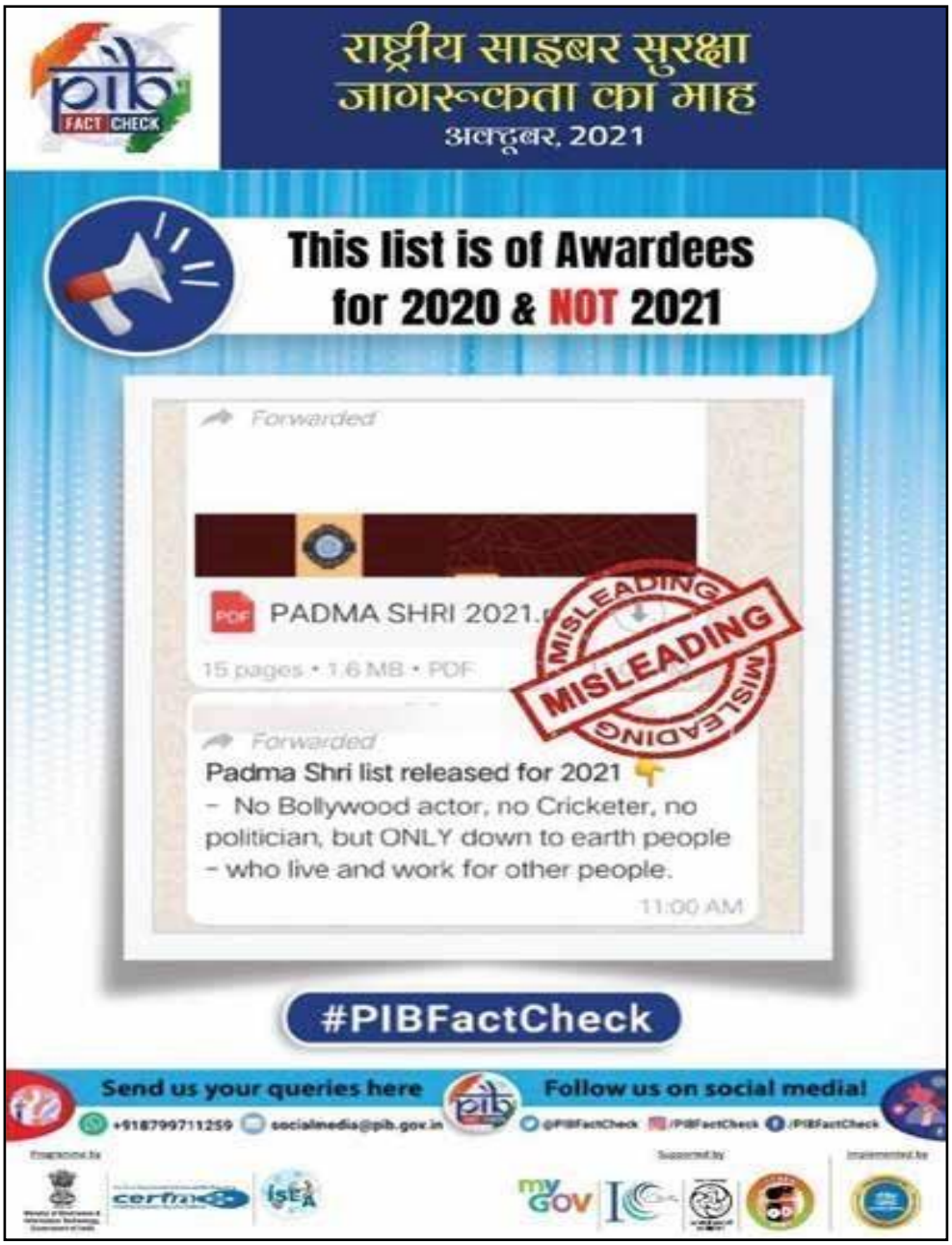


Fig. 3.7 An example of a fake message on WhatsApp (Source: PIB)

3.2.4 Fake News

Fake news refers to misinformation/ disinformation that is spread to mislead or deceive others.It can be spread through various digital platforms in the form of videos, audio, messages, or advertisements. Cyber fraudsters share such fake news to make money, promote ideas or beliefs about specific organizations or companies, trick or exploit people, promote personal opinions, etc.

Free recharge on COVID-19 vaccine - "As India commemorates the COVID-19 vaccination milestone, the government is granting three months of free recharge." the fake message stated. "Ifyou click the link below, your phone will be recharged. The offer is only available until December20." The viral message included a URL to take advantage of the deal. The fact-checking unit of thePress Information Bureau later confirmed that the government had not made such a declaration with a tweet, "Do not disclose or forward any of your personal information on any such bogus message's link."

Fig. 3.8 Fake news: Misinformation/disinformation by an online news channel (Source: IIPA)

Let us now understand how an internet user spots fake news *(Fig. 3.8)*:

- **Is there a bias?** - One can check for bias by evaluating the story to see if the author tried to get any information to tell their side of the story. This demonstrates their credibility and transparency in telling the story. One should search other media outlets to see what else is said about the story.

- **What is the date of the news?** - Some deceptive sites take stories or pictures from a few years ago and manipulate them to fit in a headline with recent events.

- **How did you come across it?** - One should identify whether the source of news is valid. It shouldn't come from people who just read the headline and share information. If it is a website, one should check the URL and look for inconsistencies such as spelling errors.

Fig. 3.9 Tips on How to Spot Fake News
(Source: https://repository.ifla.org/handle/123456789/167)

3.2.5 Deepfakes

Deepfakes are complex audio, video, or images that are created using artificial intelligence (AI) algorithms based on 'deep learning' techniques (refer to glossary to know what 'Deep learning' is). Deepfake audio, videos, and GIFs can rapidly disseminate false statements and actions to a worldwide audience, making it challenging to distinguish them from authentic information.[7]

In early 2020, a bank manager received a call from a man whose voice he recognized as the director of a company with whom he had spoken and worked before. He told the bank manager that his company was about to acquire, so he needed the bank to authorize some transfers of around INR 35 million. Believing everything was legitimate, the manager approved and initiated the transfer. What he didn't realise was that the transfer was going straight into the accounts of the criminals.

[7] https://egyankosh.ac.in/bitstream/123456789/91742/1/Block-5.pdf

3.2.6 Fake Websites

Scammers create fake websites that mimic well-known brands or mobile phone companies, promoting products at unusually low prices. They deceive unsuspecting customers into making online payments, only for the items never to arrive.

One tactic involves a false website offering a free high-value item with any purchase exceeding a certain amount. After the buyer completes the transaction, they receive a call from the website's supposed customer service, asking for a refundable fee for shipping, service, GST, and other costs related to the free item. This leads unsuspecting online shoppers to deposit thousands of rupees into the scammers' bank accounts.

Table 3.5 Safety Tips to Prevent Misinformation/Disinformation (Do's and Don'ts)

Safety Tips (Misinformation/Disinformation)
Do's
1. Check for spelling errors in the sender's address, the company's domain, or the URL, as well as grammatical mistakes in the main body of the email. Often, a popular website's name could be masqueraded by a name that sounds or appears similar.
2. Verify the authenticity of a message before sharing it on social media platforms.
3. Trust those news items that are from authorized or authenticated sources.

Safety Tips to Prevent Misinformation/Disinformation
Don'ts
1. Don't take phone calls or reply to messages from unknown sources.
2. Sharing something unverified can spread misinformation further. Take a moment to check before hitting that share button.

Fig. 3.10 Cyber Tip to Protect Oneself from Fake News (Source: MHA)

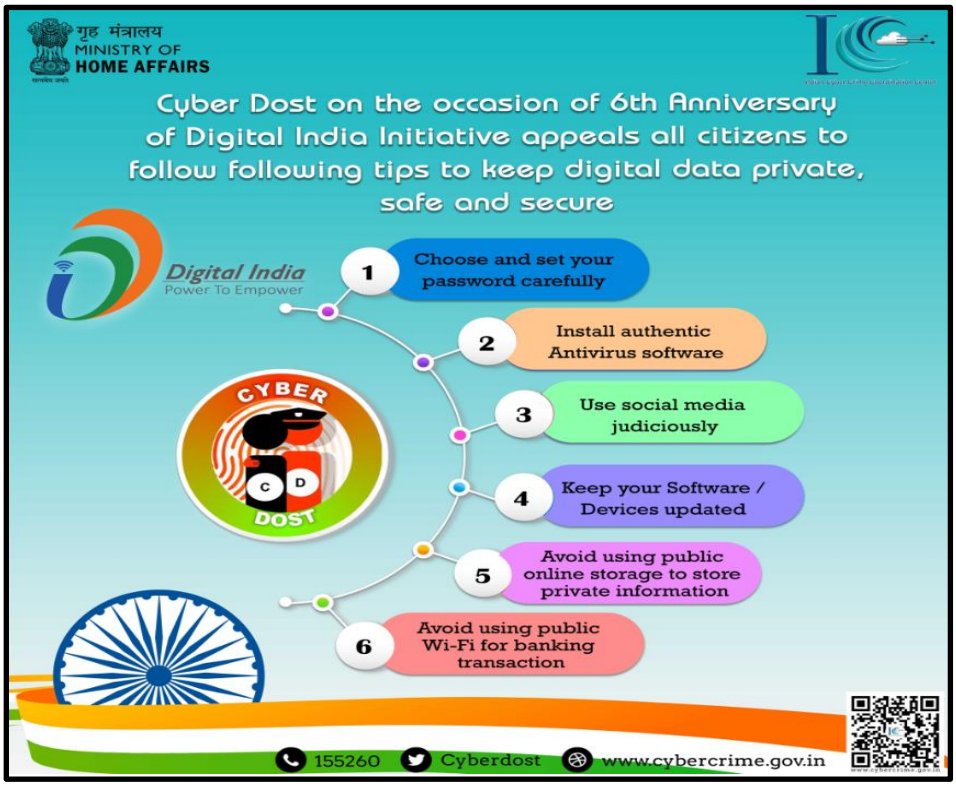


Fig. 3.11 Quick Tips to Keep Digital Data Private, Safe, and Secure (Source: MHA)

Fig. 3.12 Poster Warning People of 'Free Online Offers' (Source: ISEA Awareness portal)

3.4 Financial Frauds

3.4.1 Internet Banking-related Frauds

All banking services are now accessible online, including viewing account statements, transferring funds, requesting chequebooks, and issuing demand drafts, among others. As the number of services available online increases, the incidence of cyber fraud in the financial sector is also rising

3.4.2 UPI Frauds

Scammers often use a common tactic to deceive individuals by sending a payment request through their UPI app, making it easy for them to transfer funds. Once the payment request is accepted, the UPI app asks users for their PIN as the final step. If a person enters their UPI PIN, they risk losing all their money.

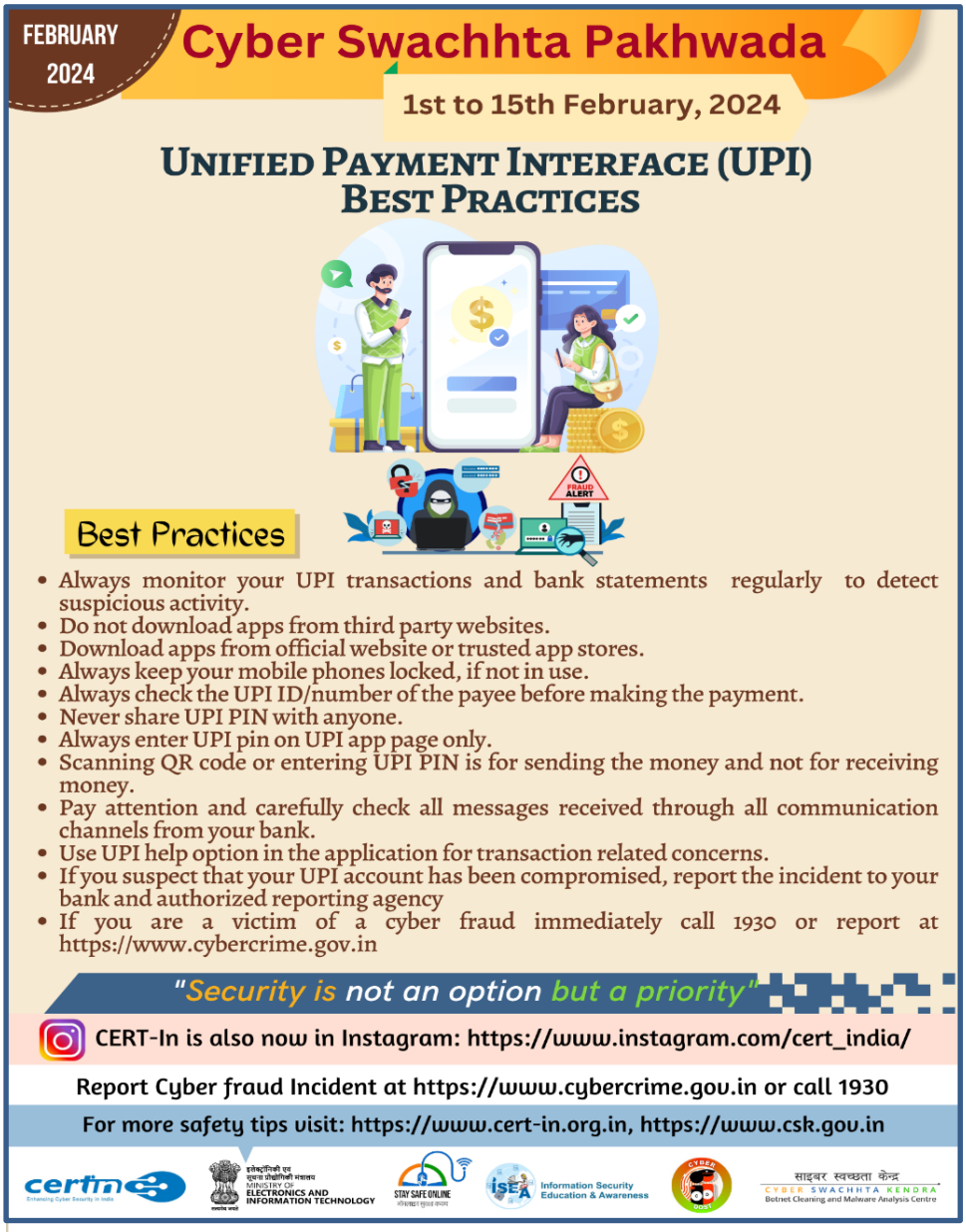


Fig 3.13 Best Practices for Unified Payment Interface (UPI)[8]

[8] https://www.csk.gov.in/tips/csp_12feb_1.png

3.4.3 OTP Frauds

Victims get SMS messages from fraudsters impersonating non-banking financial companies (NBFCs) offering loans or enhancement of credit limit and are asked to contact the fraudster's mobile number. When the victims call the number, the fraudsters ask them to fill out a few forms (even online) asking for financial details, etc. They also incite/convince them to share the OTP or PIN details, eventually resulting in a loss of money.

The OTP fraud can also happen after the person has been a victim of a social engineering attack where he/she is prompted to give their financial details to the attacker via email, and the attacker initiates a transaction from the victim's bank account details and further convinces the victim to share their OTP.

3.4.4 E-Wallet Frauds

The Reserve Bank of India has recently made KYC (Know Your Customer) mandatory for mobile wallet users, but fraudsters have exploited this requirement. Typically, a victim receives a text message stating that their e-wallet needs KYC verification and instructs them to call a provided phone number to check their e-wallet status. The scammers often request a nominal transfer (like INR 1) as part of the process. While the customer is entering their password or PIN for the transfer, the fraudsters gather information through various means, including a screen-sharing app that the victim unknowingly downloads. This gives the scammers access to the victim's wallet credentials. They can then transfer funds to other accounts using separate transactions, as the bank account is linked to the victim's phone.

Many network service providers are warning users not to fall for KYC-related messages, clarifying that they do not ask for personal information through calls or texts.

3.4.5 Credit/Debit Card Frauds

Fraud involving credit and debit cards is becoming increasingly common and continually evolving. Credit/debit card fraud refers to the unauthorized use of a card or similar payment method—such as automated clearing house (ACH) payments, exchange-traded funds (ETF), or recurring charges—to illegally acquire money or property. Scammers may either physically steal the cards or obtain card information through phishing links or card skimming techniques, subsequently using this information to make payments or withdraw funds from bank accounts.

3.4.6 QR Code-related Frauds[9]

Online transactions have become a new norm, particularly after the recent pandemic. However, one must be careful while carrying out transactions online. A quick response code, commonly known as a QR code, is a type of barcode that holds information horizontally and vertically. It has the account details embedded to transfer money to a particular account.

Cyber fraudsters impersonate potential customers and contact the person trying to sell a product on applications like OLX, Quikr, etc., and then agree to pay the price asked for the said well. The fraudsters claim that they can neither come to take the delivery physically nor can they pay in cash. Therefore, they need to make payments online. They then send a fake QR code to scan to receive money. However, once the seller scans the QR code, it gets debited from the seller's account instead of the amount being credited. The fraudsters can even access the seller's bank account and steal all the money through multiple transactions.

[9] https://www.cert- in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2017- 0055

3.4.7 E-Commerce Frauds

E-commerce frauds are financial cybercrime that involves illegal transactions performed on an e-Commerce platform by a fraudster. The fraudster would use stolen payment information for online transactions without the account owner's knowledge. It can be done by using either a false identity, stolen credit card, or fake card.

3.4.8 SIM Swap Frauds

SIM swap refers to the process of changing mobile SIM cards associated with registered phone numbers. A SIM swap scam, often called a port-out scam, involves tactics like SIM splitting and SIM jacking. When this occurs without the user's consent, it is typically for fraudulent purposes.

Fraudsters carry out this scam by obtaining a new SIM card from the telecom service provider linked to the victim's phone number. They may use various methods to achieve this, including gathering information from the victim's social media profiles (known as open-source intelligence or OSINT), phishing, or impersonating a telecom customer service representative. By posing as the user, they can easily obtain a new SIM card and deactivate the old one. Consequently, one-time passwords (OTPs) will no longer be sent to the original SIM, preventing the user from receiving alerts for any financial transactions related to their linked bank account. Instead, fraudsters receive OTPs and other notifications on the new SIM, allowing them to commit financial fraud against the victim's accounts.

Fig. 3.14 SIM Swap Frauds: A Businessman Loses INR 18 Lakhs (Source: IIPA)

3.4.9 SIM Cloning

This involves creating a duplicate SIM from the original using any software tool/ utility.It is more sophisticated than SIM swapping. It is done to access victims' International Mobile Subscriber Identity (IMSI) and encryption keys, which are used to identify and authenticate subscribers on mobile telephony. Cloning the SIM will enable the fraudster to take control and track, monitor, listen to calls, make calls, and send texts using the mobile number.

3.4.10 DEMAT/Depository Frauds

The safeguarding of shares and securities in India falls under the purview of two depositories, CDSL and NSDL. However, these depositories do not interact directly with Demat account holders. Instead, they provide Depository Participant (DP) licenses to stockbrokers and intermediaries, enabling customers to open Demat accounts. In cases of DEMAT or depository fraud, brokers have been known to transfer exchange-traded fund (ETF) units without the investors' consent, using them as collateral for margin funds in trades.

3.4.11 Cryptocurrency Frauds

Cryptocurrencies are anonymous digital tokens that can be traded for goods and services online. The rise of cryptocurrencies has led to the emergence of related sectors, such as cryptocurrency IRAs (individual retirement accounts) and digital wallet providers. However, due to their rapid transaction capabilities, portability, and global accessibility, cryptocurrencies can also be exploited for illegal activities like tax evasion, money laundering, and bribery. Fraudsters may attempt to manipulate cryptocurrency markets and similar derivative assets through tactics such as spoofing for improper market manipulation or engaging in crypto-jacking and giveaway scams.

- **Crypto-jacking** refers to a type of cybercrime in which hackers hijack individuals' electronic devices—such as computers, smartphones, tablets, and servers—to mine for bitcoin without their consent. This unauthorized mining process can significantly slow down the CPU performance of the affected devices and lead to increased electricity consumption while processing data**.**
- **Giveaway scams** are also common cryptocurrency cyberattacks. The hackers pretend to be well-known investors or even celebrities who offer assistance to tiny investors. When the victim transfers their cryptocurrency, however, instead of expanding their own investment, the money goes directly into the hands of the scammer.
- **Fake crypto wallets**: Fraudsters may also set up counterfeit crypto wallets, enabling them to steal funds from unsuspecting victims. They can create these fake wallets to deceive users, as well as establish fraudulent crypto exchanges to take money from clients.

Cryptocurrency frauds are usually done by the ‘pump and dump’ strategy where the value of an asset is ‘pumped’ dramatically through false and misleading statements, only to be ‘dumped’ afterwardas the price falls. This strategy is illegal as the dramatic ‘pump’ of the asset is often induced by a fraudster who has purchased the asset at a lower price.

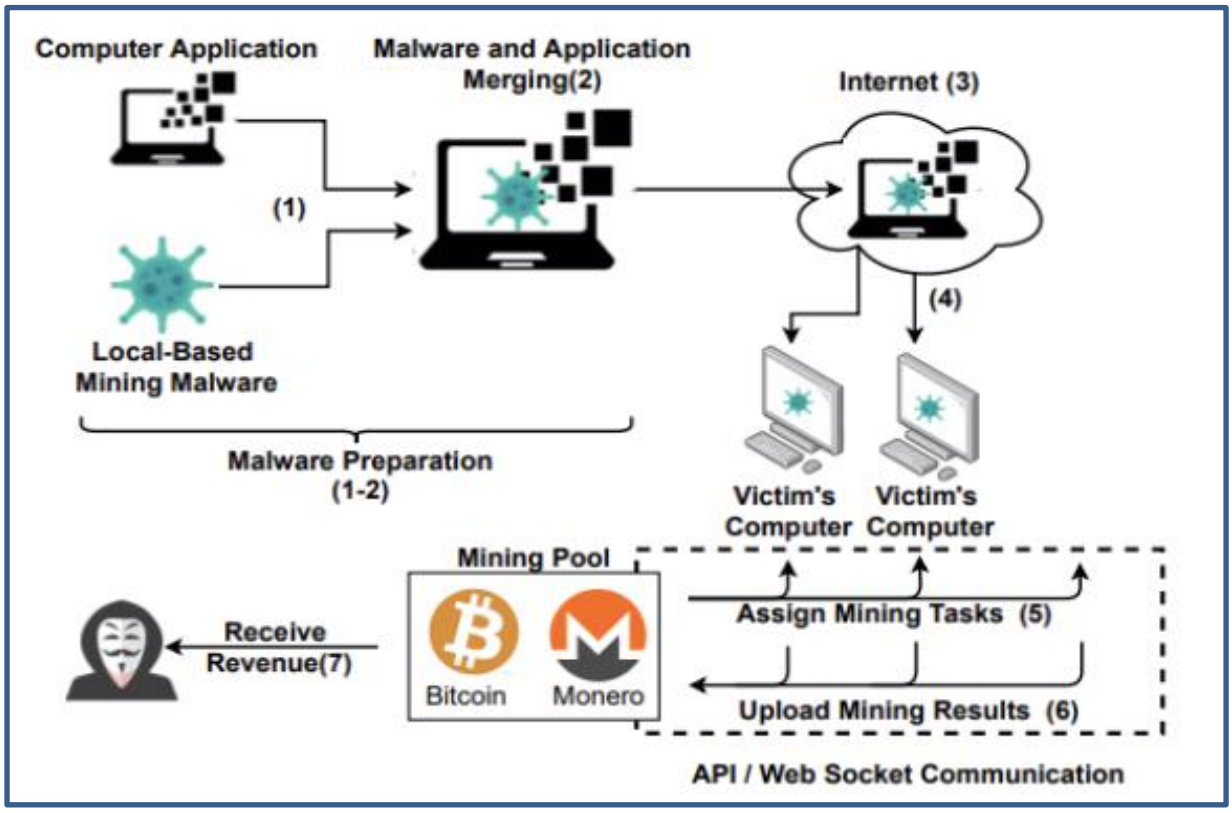


Fig. 3.15 Cryptocurrency Frauds (Source: SoK: Crypotjacking Malware – arXiv)

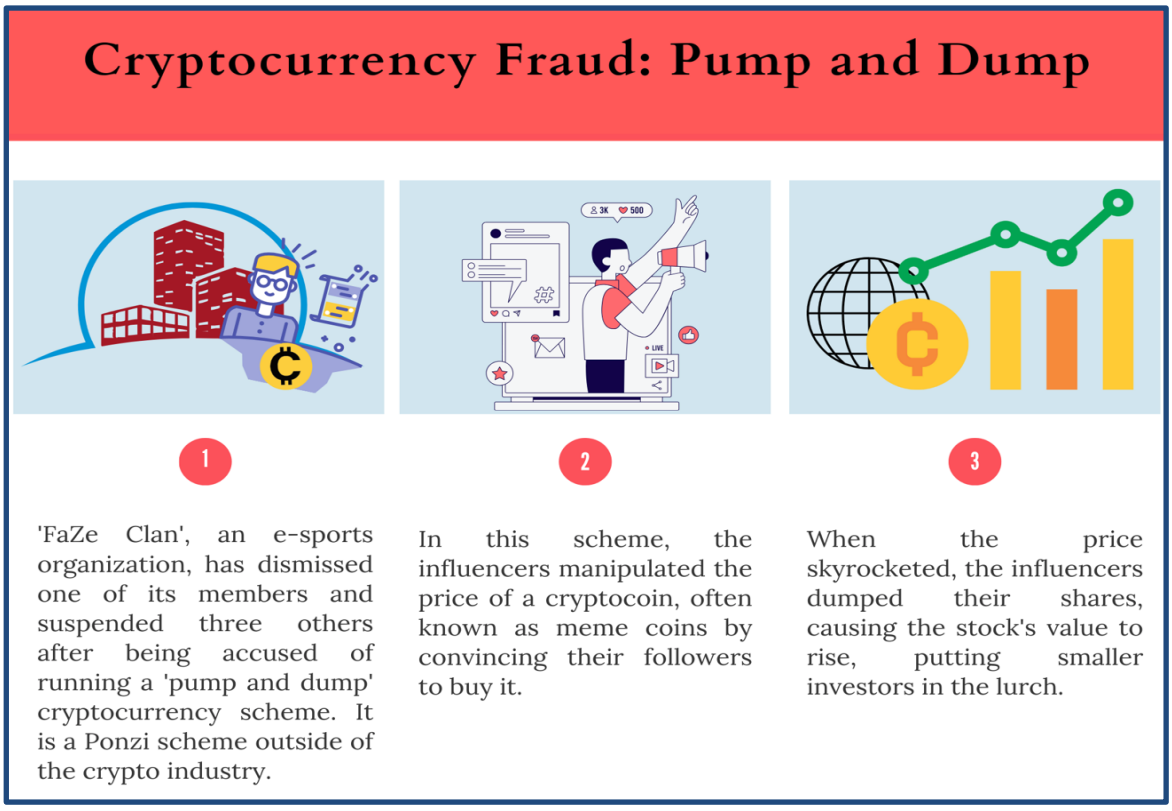


Fig. 3.16 Cryptocurrency frauds: jac and Dump (Source: IIPA)
(Source: https://www.semanticscholar.org/paper/SoK%3A-Cryptojacking-Malware)

3.4.12 Criminals Doing Frauds Exploiting 'Fear of Missing Out-FOMO'

The fear of missing out (FOMO) is related to the fear of missing out on a profitable investment. Some frauds are committed by triggering this type of fear. The fraudsters make bold claims about the high returns one might expect and time limits on the investment, thereby encouraging the victims to part with their money without thinking it through. Fraudsters exploit the rising popularity of digital assets like cryptocurrencies, bitcoins, initial coin offerings, etc., to trap innocent investors in scams, often leading to devastating losses. Given the rise in the price of some digital assets in recent years, some investors may have FOMO, thinking that they might miss an opportunity to become wealthy. FOMO is not the only thing that can influence one's financial decisions. Often social media, headlines, news, or advertisements can be misleading. If one makes an investment without evaluating the financial offer, one can end up losing a huge sum of money.

Fig. 3.17 A case study on the fear of missing out (FOMO) in online gaming (Source: IIPA)

For instance, the value of a crypto coin called Enzyme was falling in the crypto economy, but then something unusual happened. According to CoinGecko, the price of Enzyme, also known as Melon (MLN), jumped from INR 30 to INR 47 in just minutes, while daily trading volumes jumped from INR 3 million to over INR 100 million. It then dropped to INR 35 after a fewhours. The coin had just been 'pumped and dumped' as the scammers conspired to inflate the price to benefit quickly.

3.4.13 Side-Channel Attacks

Side-channel attacks aim to gather private information from a vulnerable system so that it may disrupt the system. For instance, such attacks could 'discover' the information leaks of a vulnerable system to 'break' into the cryptography of a system to disrupt it.

Since side-channel attacks rely on the relationship between leaked information and private data, such attacks could be prevented/minimised if the following points are taken care of:

1. One should try to eliminate or reduce the release of such information.
2. Given the relationship between the two, one should try to unrelate the leaked information to the private data through some kind of randomization of the cipher text that transforms the data in a way that can be undone after the cryptographic operationis completed.

Table 3.6 Safety Tips to Prevent Financial Frauds (Do's and Don'ts)

Safety Tips to Prevent Financial Frauds
Do's
1. Use an onscreen keyboard to enter the login credentials in banking portals.
2. Clear the browsing history from the web browser, especially when using public computers or cyber-cafes.[10]
3. Check the second-hand digital device for suspicious pre-installed apps before buying it.
4. Be aware of all offers that provide high returns in a limited time. They might be fake.

Safety Tips to Prevent Financial Frauds
Don'ts
1. Don't fall for high-profile testimonials - These scammers hire celebrities and social media influencers to promote their fake schemes. These actors try to portray everyday people and spread fake reviews.
2. Do not scan the QR code if you have to receive money.

3.5 Man-in-the-Middle

Man-in-the-middle (MitM) attacks happen when an attacker intercepts communications between two parties by intruding and eavesdropping on their exchanges. In these attacks, the "targets" are typically an individual and a service. The attacker may remain undetected during the communication, secretly stealing credentials and modifying emails or other messages to facilitate cybercrime using the acquired information.

[10] https://egyankosh.ac.in/bitstream/123456789/91742/1/Block-5.pdf

3.5.1 Juice Jacking

A cyberattack in which an infected USB charging station is used to compromise linked devices is known as juice jacking. Juice jacking is a Man in the Middle (MitM) attack that targets hardware. In this technique, a mobile device's power is delivered over a USB cable that is also used to transfer data. The attacker uses a USB connection to load malware directly onto the charging station.In some cases, a connection cable is plugged in so that someone would come along and use the 'forgotten' cable. This usually happens at airports, shopping malls, and other public areas providing free mobile device charging stations.

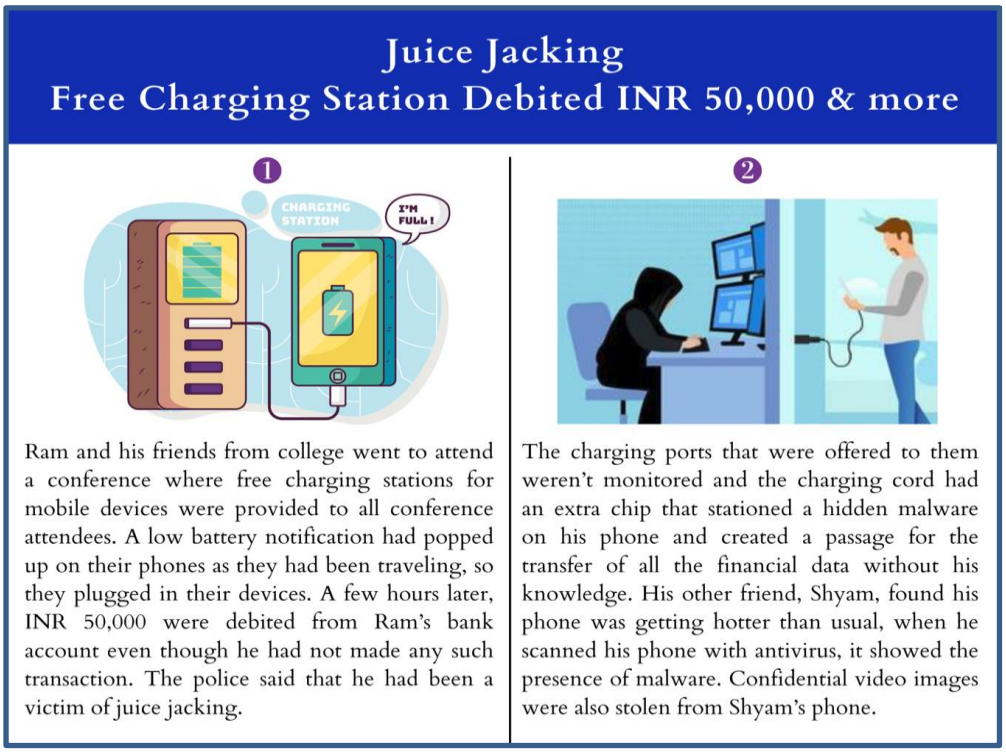


Fig. 3.18 Juice Jacking: Free Charging Station Debited INR 50,000 & More (Source: IIPA)

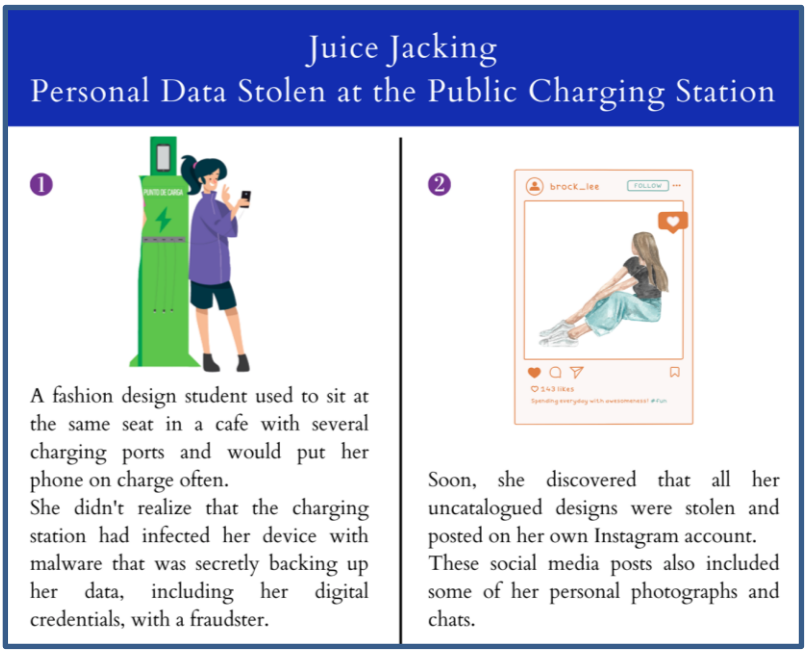


Fig. 3.19 Juice Jacking: Personal Data Stolen at the Public Charging Station (Source: IIPA)

Fig 3.20 Juice Jacking: Safety Tips[11]

3.6 Social Media Crimes

Across the globe, mobile devices dominate in terms of the total minutes spent online. Further, social media has rapidly grown, and its influence is increasing each day *(Fig. 3.19)*.

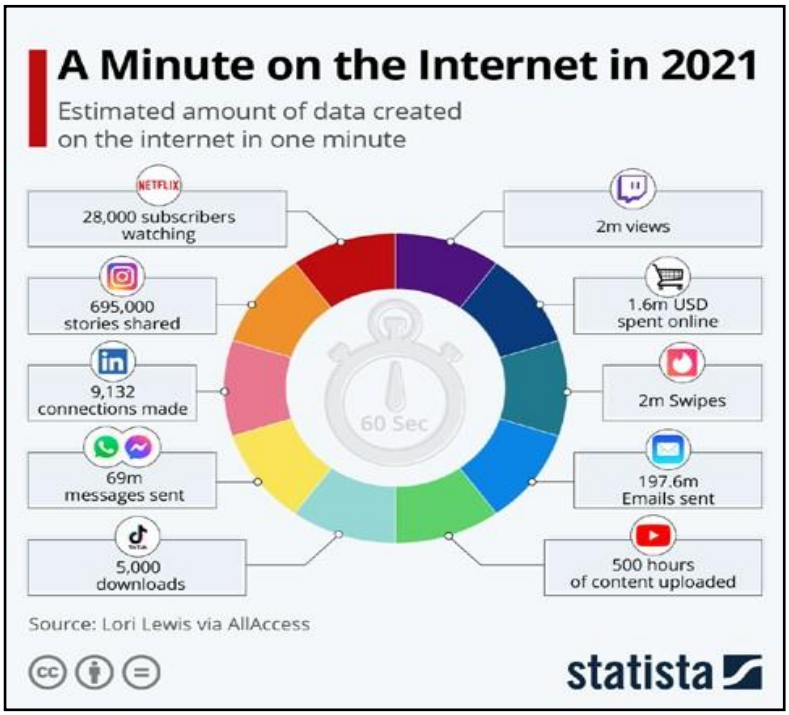


Fig. 3.21 Estimated Amount of Data Created on the Internet in One Minute (Source: Statista)

[11] https://www.csk.gov.in/tips/csp_5feb.jpg

However, social media, due to its excess popularity, has emerged as an extended hazard for depression, anxiety, loneliness, self-harm, or even suicidal thoughts. Sometimes, it promotes notions like inadequacy of life and experiences, fear of missing out –FOMO (covered in the previous section under 'financial frauds'), depression and anxiety, and defamation, which greatly impacts the mental health of the users.

'Cyber defamation' is a broad term that refers to any online or cyberspace act, deed, word, gesture, or thing that has the intention of defaming a person's reputation or goodwill so that others in the community - whether they are online or offline - will view them with disrespect, ridicule, hatred, disinterest, or with a negative quality. It can be committed via email, mailing lists, bulletin boards, the internet, discussion forums, and the World Wide Web.

3.6.1 Cyberstalking

A cyberstalker harasses or stalks victims through digital devices or the internet. This can involve using email, instant messaging, online messages, discussion forums, or other electronic communication methods. In many cases, the stalker remains unknown.[12]

3.6.2 Cyberbullying

Cyberbullying refers to bullying that occurs through digital technology, aimed at instilling confusion, fear, or shame in the victim. The bully posts unpleasant, damaging, or threatening information about the victim onsocial media or other platforms, such as blogs, gaming apps, etc.

Fig. 3.22 Tips on Cyberbullying for Young Children (Source: @CyberDost, MHA)

[12] https://egyankosh.ac.in/bitstream/123456789/91742/1/Block-5.pdf

3.6.3 Sexting

Sexting is the act of sending or sharing sexually provocative text messages and images, including nude or semi-nude photos, via digital devices. This can occur through hacking, where images are taken from the original recipient and shared without the sender's consent, or when a previously trusted individual misuses that trust. When such images are distributed without the victim's approval, sexting becomes problematic, and the victim is considered a target of cybercrime.

3.6.4 Honey Trapping[13]

Honey trapping is an act of using romantic or intimate relationships for interpersonal, political, or financial reasons to obtain sensitive information. It can compromise the safety of the individual and, sometimes, the nation's security as well. Attackers exploit the closeness of a relationship to manipulate or blackmail their victims. Today, this is mainly done through social media platforms, although the term was originally used in a non-digital context. One such concept is "pig butchering," where scammers use romantic relationships on dating apps and social media to entice individuals into investing in cryptocurrency and gold. This highlights how various types of fraud can be closely linked; for instance, social media scams can lead to cryptocurrency fraud and vice versa.

Fig. 3.23 Pig butchering crypto scam (Source: In shorts)

3.6.5 Sextortion

Sextortion is a cybercrime that occurs when a fraudster threatens a victim to share private and sensitive information, usually sexually explicit images, particularly to extort money or sexual favors from the victim. The fraudster may also threaten the victim to use information obtained from her/ his device that could harm the victim's friends or relatives, in case the victim doesn't comply with the demands of the fraudster.

Nowadays, sextortion email scams are also a common threat. These suspicious emails falsely claim to possess sexually explicit content related to the victim and demand ransom, usually in bitcoins.

[13] https://www.staysafeonline.in/concept/honey-trap

Fig. 3.24 Sextortion (Source: DCP Cybercrime)

3.6.6 Trolling

Trolling refers to the deliberate act of spreading hatred, discrimination, racism, or sexism through social media platforms or engaging in arguments with others online. This behavior incites personal disputes and controversy. In the early days of the internet, it was referred to as "flaming." Individuals troll on blog sites, social networks like Facebook, Instagram, and Twitter, news websites, discussion forums, game chats, and other platforms that allow them to publicly express negative comments about others.

Table 3.7 Safety Tips to Prevent Social Media Crimes (Do's and Don'ts)

Safety Tips to Prevent Social Media Crimes
Do's
1. Set social media profile privacy settings to the highest level of security.
2. Be very careful when sharing any personal information on social media.
3. Always remember to log out of apps and close the browser after each session.
4. Always put a profile guard on the profile display picture of social media accounts such as WhatsApp and Facebook, among others.

Safety Tips to Prevent Social Media Crimes
Don'ts
1. Don't give out social media login information to anyone.
2. Don't keep common passwords such as name, date of birth, or "1234" and so on.
3. Don't post any personal or sensitive information, such as bank details or passwords, on socialmedia sites.

Fig. 3.25 Cyber Tip to Stay Safe from Social Media Crimes (Source: @CyberDost, MHA)

3.7 Morphing[14]

Morphing is the technique of seamlessly transitioning from one image to another using online morphing tools. Typically, women are the primary targets of this practice. It involves downloading photos of individuals from various social media platforms using either fake or genuine profiles and then merging them with inappropriate content. The resulting altered images can be used for

[14] https://infosecawareness.in/concept/govt-employee/morphing

blackmail by threatening to release them to the public, putting pressure on the individuals or their families. Nowadays, deepfake technology is also being used to morph images and create fake videos of victims to deceive/harass their families.

3.7.1 Revenge Pornography

Revenge pornography poses a significant risk, driven by the intent to damage an individual's public reputation. The perpetrator may gain unauthorized access to the victim's account and exploit their identity to post explicit images. Alternatively, the attackers might pose as a sex worker to manipulate the victim into revealing their name, images, and other personal information, which could then be used to create a fraudulent public profile (Fig. 3.25). Revenge pornography leads to merciless trolling, cyberbullying, and other kinds ofsocial media humiliation.

Table 3.8 Safety Tips to Prevent Morphing (Do's and Don'ts)

Safety Tips to Prevent Morphing
Do's
1. Be cautious of making unknown people 'Friends.'
2. Remember that anything shared online will remain in cyberspace and could be misused anytime.

Safety Tips to Prevent Morphing
Don'ts
1. Avoid clicking on or sharing intimate photos or videos.
2. Refrain from pursuing relationships that pressurize you to share personal images or videos
3. Don't remain silent if you face threats or become a victim of cybercrime.

3.8 Grooming

Grooming is a kind of pedophile crime where the threat actor could win the trust of a child to engage in vulgar activities or to exploit them sexually. Attackers can create a counterfeit profile on any social media platform to portray themselves as someone younger or as a person familiar to the child. Young children between the ages of 13 and 15 are especially susceptible to being groomed or manipulated by adults they meet online.

3.9 Dangerous Game Challenges

Excessive video game playing is an activity that increases the risk of depression, anger, shyness, and anxiety, especially among young children and is, therefore, linked to the poorest long-term effects. Multiplayer video games such as BGMI, CODM, Free Fire, etc., increase the chances of violent behavior in the players, leading to changes in their actions. Cybercriminals may target in-game resources, fully developed game characters, paid game accounts, or linked credit card information. These assets can be compromised through phishing, password-stealing malware, or in-game scams.

Fig. 3.26 Do's and Don'ts on Online Gaming Safety for Children (Source: CDAC)

Table 3.9 Safety Tips to Prevent Dangerous Game Challenges (Do's and Don'ts)

Safety Tips to Prevent Dangerous Game Challenges
Do's
1. Turn off all notifications/pop-ups that lure for usually undesirable game offers.
2. Limit screen time.
3. Install parental control software.

Safety Tips to Prevent Dangerous Game Challenges
Don'ts
1. Don't make mobile phones/gaming apps a regular part of your routine, as it affects eyesight andfinancial health too.
2. Don't share personal sensitive information on gaming applications.

3.10 Remote Access Applications

Remote access applications are screening applications that have always been used by IT professionals to troubleshoot source codes, etc., during remote work. However, it is now also being used worldwide by fraudsters to connect to the digital devices of the victims to steal data and money. These applications are loaded into the victims' devices disguised as e-KYC frauds or under the pretext of updating SIM or ATM cards or through phishing links. Coaxed by fraudsters, victims unwittingly load these screen-sharing apps and end up granting fraudsters easy access. Remember never to share OTP or sensitive data on such apps.

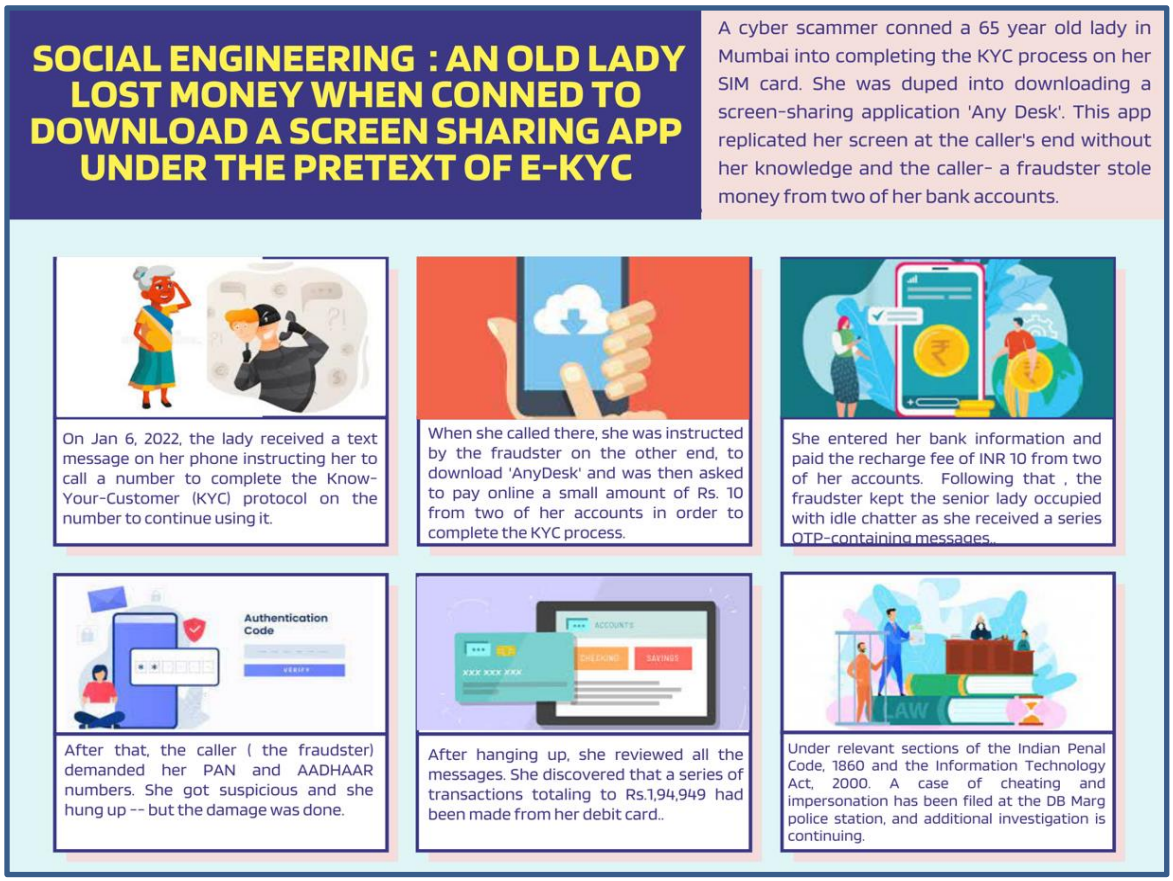


Fig. 3.27 A Case Study of Cybercrime through a Screen-sharing Application (Source: IIPA)

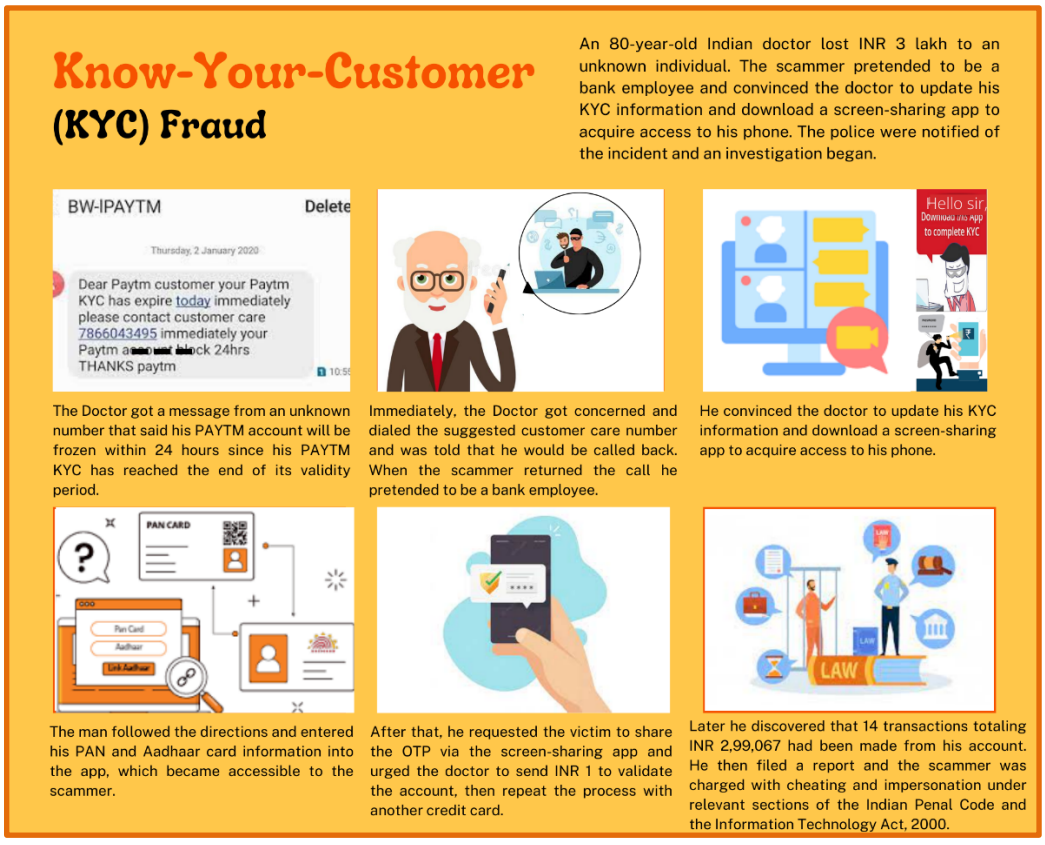


Fig. 3.28 A KYC Fraud using a Screen-sharing Application (Source: IIPA)

Table 3.10 Safety Tips to Prevent Cyber Crimes through Remote Access Applications (Do's and Don'ts)

Safety Tips to Prevent Cyber Crimes through Remote Access Applications
Do's
1. To restrict access, Invest money and time in installing secure/safe software, antivirus, firewall, and two-factor authentications.

Safety Tips to Prevent Cyber Crimes through Remote Access Applications
Don'ts
1. Never share your net banking password, One-Time Password (OTP), ATM or phone banking PIN, CVV number, or any other sensitive information with anyone, even if they claim to be a bank employee or representative. If someone asks for this information, notify your bank immediately.
2. Avoid saving banking or personal information in a browser or a payment site during purchases.

3.11 Matrimonial Frauds

Fraudsters create enticing online marriage profiles on matrimonial sites to befriend their victims. They build trust through emails, online chats, and phone calls, sometimes even using voice-changing apps to impersonate the victim's parents or guardians. Once they have fully gained the victim's trust, they propose marriage and pressure them to transfer money to their accounts, citing an emergency. After receiving the payments, the fraudsters vanish and move on to their next target.

3.12 Career frauds

Nowadays, many individuals seek job opportunities online. In cases of career-related fraud, scammers present fake job offers from well-known companies, claiming to hold senior positions there. They then request money transfers from victims under the guise of job registration fees. It can be challenging for people to determine the legitimacy of these offers, making them susceptible to falling for these fraudulent job schemes

Table 3.11 Safety Tips to Prevent Matrimonial and Career Frauds (Do's and Don'ts)

Safety Tips to Prevent Matrimonial and Career Frauds
Do's
1. Validate the social media profiles of the people who are offering marriage proposals/jobs from other sources too, such as Facebook or LinkedIn.

Safety Tips to Prevent Matrimonial and Career Frauds
Don'ts
1. Don't share personal/financial information with online friends or recruiters.
2. Don't accept job offers or marriage proposals online without validating the person's profile on various sources such as LinkedIn, Facebook, Twitter, etc.

Chapter 4: A Ready Reckoner to Lodge Cyber Complaints and to Stay Cyber Safe

4.1 Reporting a Cyber-Crime

In the face of adversity, it can be quite confusing for a victim to have easy access to various stepsto lodge an official cybercrime complaint. In India, there are several channels available to file a cybercrime complaint.

- The government of India has also provided cyber-cells in almost all the states (list availableat https://cyber crime.gov.in/Webform/Crime_NodalGrivanceList.aspx).
- One could also call the **National Helpline number '1930' (24*7)** for immediate reporting of Cyber Financial Frauds.
- The victim could lodge a cyber-complaint on the national portal "*cyber crime.gov.in*".
- The conventional measure is to report on the National Emergency Response number of '112'.
- The victim could also lodge the FIR with the local police station. The victim (or the well-wisher of the victim - who is lodging the complaint on behalf of the victim) must remember a zero FIR could be lodged from any police station. Usually, cybercrime is treated as a cognizable offence, whereby a police officer can be arrested without any arrest warrant.

In the next subsection, one shall also find a cue card of steps on how to do so. A summary of steps for filing online cyber-complaint is presented herewith (Fig 4.1).

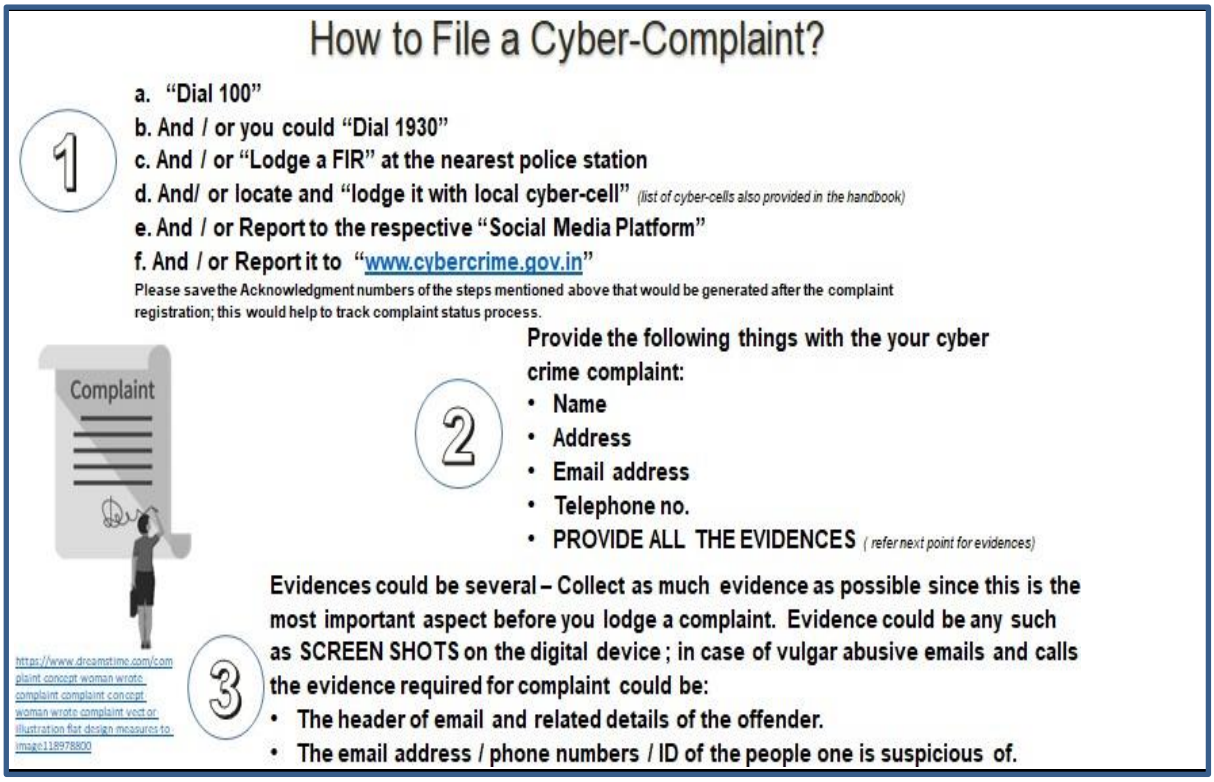


Fig 4.1 How to File a Cyber Crime Complaint (Source: IIPA)

4.1.1 Registering Complaints through an E-mail to State Cyber Nodal Officers

Apart from resorting to the channels mentioned above (Fig 4.1), a victim could also register a cyber-complaint by emailing the complaint directly to the designated Cyber Nodal Officerof the state. As already mentioned above, almost every state has local cyber cells monitored by Cyber Nodal Officers. A PDF file with the list of email IDs and contact numbers of the nodal officers is available in the 'Contact Us' section on the national cybercrime portal cybercrime.gov.in. The direct link to access the details of Cyber Nodal officers is https://cyber crime.gov.in/Webform/Crime_NodalGrivanceList.aspx. This link could be used to access the email of the respective Cyber Nodal Officer of the state to whom the cyber-complaintis to be addressed.

4.1.2 Registering Complaint by Women and Children Victims

Special helpline numbers and portals are available for women and children to lodge a cybercrime complaint, as summarized herewith.

i. Helpline and Portal for Women Victims -
   - Helpline numbers when the victim is a Woman: '1091' or '181'
   - Portal to lodge a complaint with the National Commission for Women (NCW): ncw. nic. in

ii. Helpline and Portal for Children Victims -
   - Helpline number when the Victim is a Child: '1098'
   - Helpline number by DCPCR (Delhi Commission for Protection of Child Rights) +91-9311551393

iii. Emergency Helpline number, in case of obscene calls/ online stalking - 1096/1090

iv. E-mail for women or children Victims: They could also email their cyber-complaint to an email address of the Ministry of Women and Child Development: mwcd@gov.in.
   - Cyber complaints by women/children victims could be lodged by their well-wishers. All such complaints could be "anonymous," too, and even these investigations could be undertaken anonymously, too, if requested.

4.1.3 Registering Complaint of Cyber-Financial Frauds

Special remedial measures are particularly available if financial fraud is committed (Fig 4.2).

1. The customer must file a complaint or **notify her bank regarding** the fraud throughthe bank's Customer Care Phone number, E-mail, or written complaint mentioningthe details of the fraud.
2. **The complaint or notification should be submitted within three days to ensure that the customer has no liability.**
3. It is also advisable **to file a police complaint** regarding financial fraud.
4. If the fraud is related to a credit/debit card, then the customer should contact the Bank's customer service and **get the card blocked immediately** to avoid any furthermisuse of the card.
5. The bank is required to reverse or refund the amount **within ten working days** from the date the customer notifies them, provided the customer has zero or limited liability.
6. If loss/fraud was due to the negligence of the customer, then the bank is not liable to provide any refund to the customer.

7. If the Customer is not satisfied with the resolution provided by the Bank, then shecan file a complaint with **RBI's banking ombudsman** (https://cms.rbi.org.in/cms/ IndexPage.aspx)

What to do if one is a Victim of a Financial Fraud

Apart from the steps already indicated (Fig 4.1), it is very relevant to Dial "1930" and lodge the complaint with the local cyber-cell.

1. If the fraud is related to a credit/debit card, Block the card and inform your bank.
2. Also Nofify the bank-branch of the fraud and save the registered complaint number.
3. The Complaint should be done to the bank within 3 days of the Crime being noticed, so that there is **Zero liability on part of the customer.**
4. The Bank has to reverse or refund the amount within 10 working days from the date of information/ complaint lodged by the Customer.
5. If the financial loss/fraud was due to the negligence of customer, then the bank is not liable to provide any refund to the customer.
6. if the customer is not satisfied with the resolution provided by the Bank, then she/he can file a complaint with RBI's banking ombudsman. (https://rbi.org.in/scripts/aboutusDisplay.aspx?pg=Banking ombudsmen.htm) or Call 14448 for grievance redressal.

The customer has zero liability in the case of a "third-party breach where the deficiency lies neither with the bank nor with the customer such as ***malware attack or large-scale hacking of the bank*** but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction"

Fig 4.2 Steps to Follow to File a Complaint, In Case of Financial Frauds (Source: IIPA)

4.1.4 Reporting to a Bank in Case of a Financial Fraud

Subject: Complaint against cybercrime and fraud with me

To: <ncrp.delhi@delhipolice.gov.in

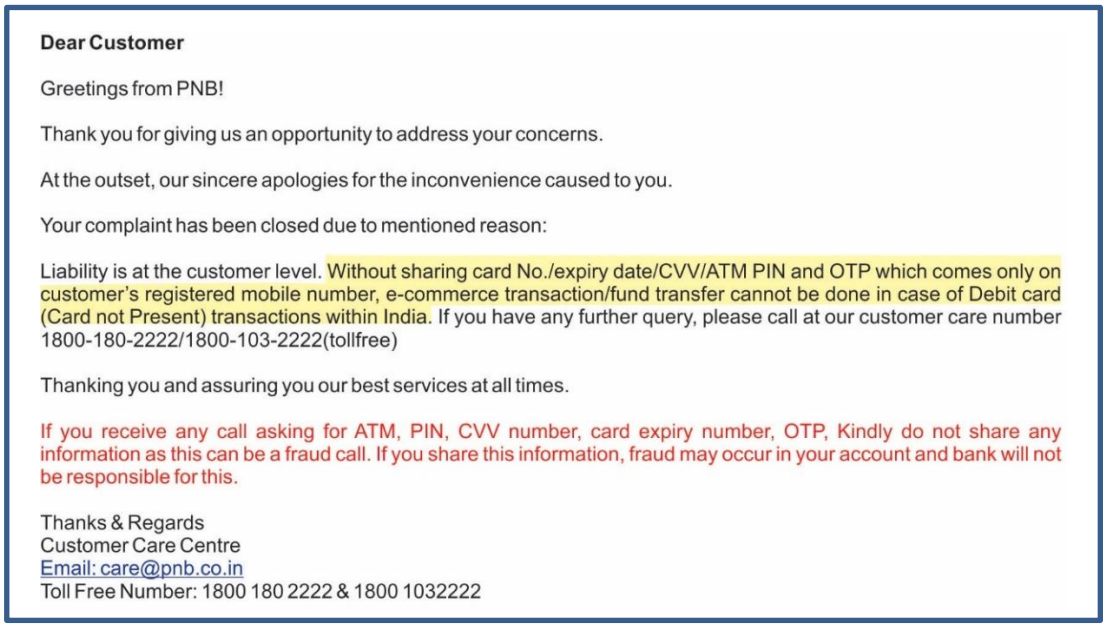
cc: <dcp.rohini@delhipolice.gov.in

Dear Sir

This is to inform you that today I received a call on behalf of NDPL from mobile number 919163712892. After that, I got a message that Rs.50,000/- were deducted from my account without my knowledge/consent. I did not make this transaction nor did I share any details of the card or account with anyone. I immediately called the customer care of the bank at about 7:00 pm and asked them to freeze my account which was done. My complaint number as per your customer service is A194218527.

However, since the last transaction of Rs.50,000/- was not made or authenticated by me.
I request you to revert that back to my account immediately and take the necessary action against the unauthorised transaction.

Fig. 4.3 An Example of Financial Fraud Complaint through E-mail



Dear Customer

Greetings from PNB!

Thank you for giving us an opportunity to address your concerns.

At the outset, our sincere apologies for the inconvenience caused to you.

Your complaint has been closed due to mentioned reason:

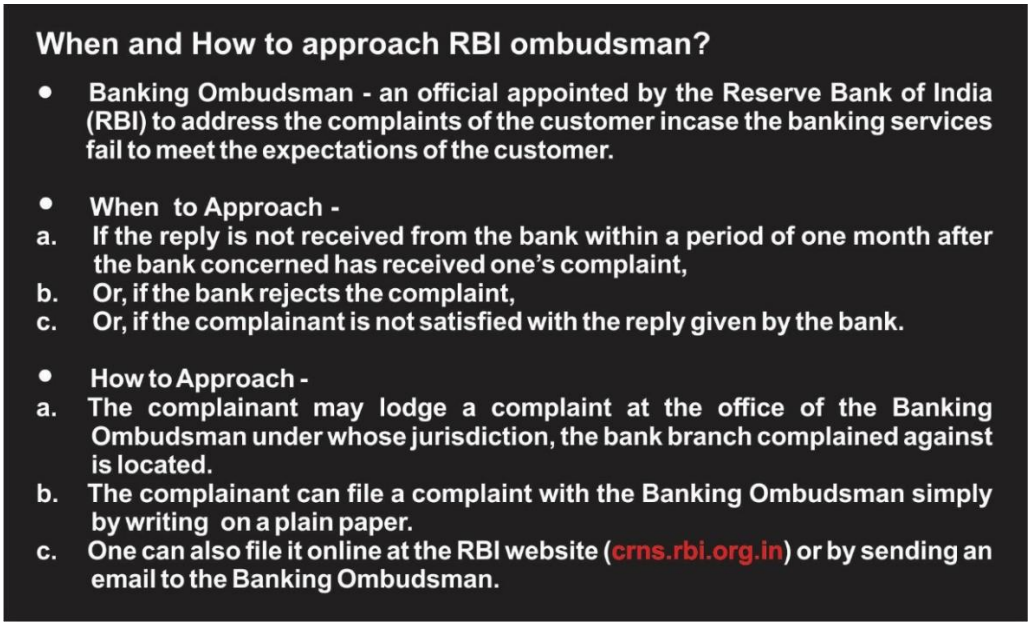
Liability is at the customer level. Without sharing card No./expiry date/CVV/ATM PIN and OTP which comes only on customer's registered mobile number, e-commerce transaction/fund transfer cannot be done in case of Debit card (Card not Present) transactions within India. If you have any further query, please call at our customer care number 1800-180-2222/1800-103-2222(tollfree)

Thanking you and assuring you our best services at all times.

If you receive any call asking for ATM, PIN, CVV number, card expiry number, OTP, Kindly do not share any information as this can be a fraud call. If you share this information, fraud may occur in your account and bank will not be responsible for this.

Thanks & Regards
Customer Care Centre
Email: care@pnb.co.in
Toll Free Number: 1800 180 2222 & 1800 1032222

Fig. 4.4 Banks Defeat the 'Zero Liability Policy' to the E-mail Complaints



When and How to approach RBI ombudsman?

- Banking Ombudsman - an official appointed by the Reserve Bank of India (RBI) to address the complaints of the customer incase the banking services fail to meet the expectations of the customer.

- When to Approach -

a. If the reply is not received from the bank within a period of one month after the bank concerned has received one's complaint,
b. Or, if the bank rejects the complaint,
c. Or, if the complainant is not satisfied with the reply given by the bank.

- How to Approach -

a. The complainant may lodge a complaint at the office of the Banking Ombudsman under whose jurisdiction, the bank branch complained against is located.
b. The complainant can file a complaint with the Banking Ombudsman simply by writing on a plain paper.
c. One can also file it online at the RBI website (crns.rbi.org.in) or by sending an email to the Banking Ombudsman.

Fig. 4.5 When and How to Approach an RBI Banking Ombudsman (Source: IIPA)

4.1.4.1 Measures to be taken when an individual loses their mobile phone:

1. Call the cell phone from a different device. One can also sound an alert by using the carrier's mobile app to override ringtone settings.
2. If the phone's text messages are enabled to appear on the lock or home screen, leave atext with contact information in case someone finds it.
3. Each phone has built-in security settings. One can monitor, ring, lock, or wipe thephone remotely using the 'find my phone' feature if it is enabled.
4. If a person is quite convinced that the phone has been stolen, one should wipe thedata from it remotely as quickly as possible to keep personal information safe.
5. If one cannot find the phone fast, use the 'find my phone' option on the phone to lockit remotely from anywhere. Also, just in case, change the passwords on all accounts, including financial accounts, emails, and social media.
6. Block the phone's IMEI by any of the following means:

To report a lost or stolen phone, follow these steps on the website: https://www.ceir.gov.in/:

File a Police Report: Ensure you keep a copy of the report

a. **Obtain a Duplicate SIM Card**: Contact your telecom service provider (e.g., Airtel, Jio, Vodafone/Idea, BSNL, MTNL) for a duplicate SIM for the lost number. This is necessary as you'll need it as your primary mobile number (where the OTP will be sent) when submitting your request to block the IMEI.

   Note: According to TRAI regulations, SMS functionality on reissued SIMs will be activated 24 hours after the SIM is activated.

b. **Prepare Required Documents**: Gather a copy of the police report and proof of your identity. You may also include the invoice from the mobile purchase.

c. **Fill Out the Request Registration Form**: Complete the form to block the IMEI of your lost or stolen phone and attach the necessary documents.

d. **Submit the Form**: After submission, you will receive a Request ID, which can be used to check the status of your request and to unblock the IMEI later.

e. **Contact Your Network Service Provider**: Contact your provider through their official customer service channels. They can disable the phone's service, making it inaccessible even if someone uses a new SIM card or changes operators.

f. **File a First Information Report (FIR)**: Report the incident at your nearest police station. This step is crucial, as it can help you contest any fraudulent charges made using your device, even if you do not recover the phone.

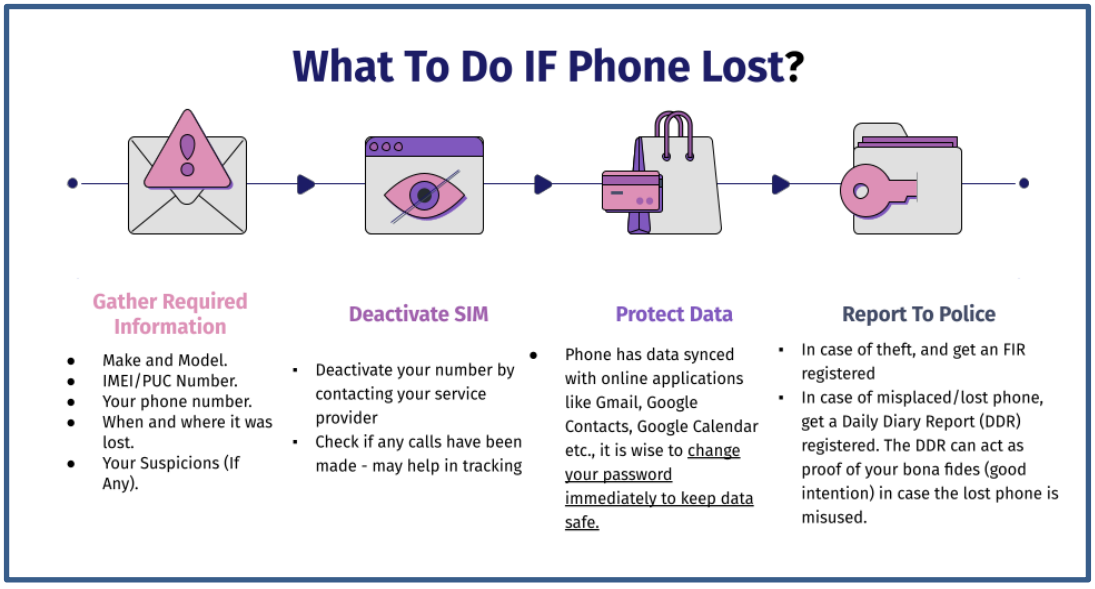


Fig. 4.6 Steps to Follow in Case of a Lost Mobile Phone (Source: IIPA)

4.1.5 Reporting Cyber Abuse on Social Media Platforms

As discussed in the previous chapter, social media users sometimes misuse the platforms to abuse, creating an inappropriate environment. A feature called 'Report or Mark as Spam' is available to users in such cases. This feature allows them to report channels,posts, profiles, comments, or other content if it violates the norms or harms another person'ssentiments (Fig. 4.7). The platform initiates appropriate action in accordance with EULA.

The government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021") on 25.02.2021, which was subsequently amended on 28.10.2022 and 6.4.2023. The IT Rules 2021 cast specific legal obligations on intermediaries, including social media intermediaries and platforms, to ensure their accountability towards safe & trusted Internet, including their expeditious action towards removal of prohibited misinformation and patently false information.

Reporting Cyber Abuse on Social Media Platforms, including Intermediary ("Intermediary" in the context of electronic records refers to any entity that handles, stores, transmits, or provides services related to such records on behalf of another. This encompasses telecom service providers, network service providers, internet service providers, web hosting companies, search engines, online payment platforms, auction websites, e-commerce marketplaces, and cyber cafes. Social media platforms can sometimes foster misuse and abuse, leading to an inappropriate environment. To counteract this, users are equipped with a 'Report or Mark as Spam' feature to report channels, posts, profiles, comments, or other content that breaches norms or harms sentiments. The platform will then take appropriate action in accordance with the End User License Agreement (EULA), along with applicable rules, regulations, privacy policies, and user agreements, all provided in a language chosen by the user.

Key Obligations for Intermediaries in Addressing Cyber Abuse:

a. Due Diligence by Intermediaries:

- Intermediaries are required to meet specific due diligence standards, particularly for social media and online gaming platforms.
- They must clearly display their rules, regulations, privacy policies, and user agreements in the user's chosen language.
- Users should be warned against hosting, displaying, uploading, modifying, or sharing prohibited content, such as unauthorized material, obscene or harassing content, and harmful content for children.
- Intermediaries are responsible for regularly updating users about these regulations.
- Upon becoming aware of illegal content, intermediaries must quickly remove or disable access to it, retain the relevant information for investigation, and assist authorized government agencies.

b. Other Obligations of Intermediaries:

- Maintain user data for a designated period after account cancellation or withdrawal.
- Implement appropriate security practices and procedures.
- Report cybersecurity incidents and share information with the Indian Computer Emergency Response Team.
- Ensure their services are accessible while upholding due diligence, privacy, and transparency.
- Before hosting or charging for online games, they must confirm registration with the relevant self-regulatory organization.
- Respect the constitutional rights granted to citizens.
- These provisions are designed to increase accountability and transparency in addressing cybercrime on social media and online gaming platforms.

c. Grievance Redressal Mechanism for Intermediaries:

Prominent Display of Grievance Officer Details:

- Intermediaries must prominently feature the name and contact details of the Grievance Officer on their website or mobile app, enabling users to report rule violations or other issues related to the intermediary's resources.

d. Handling of Complaints by Grievance Officer:

- The Grievance Officer must acknowledge complaints within twenty-four hours.
- Complaints must be resolved within fifteen days, except for specific cases related to removing certain types of content, which must be resolved within seventy-two hours.
- The Grievance Officer is responsible for receiving and acknowledging orders, notices, or directions from the Appropriate Government, competent authorities, or courts.

Within twenty-four hours of receiving a complaint regarding prima facie offensive content, the intermediary must take reasonable measures to remove or disable access to such content.

Reporting Cyber Crime Online

INSTAGRAM AND FACEBOOK	TWITTER	REPORTING TO UNICEF
Victims can **"Report"** individual comments and messages which violates the rules of Instagram and Facebook.	Victims can **"Report"** individual comments, messages and retweets which violates the rules of Twitter. Find policies under **ABOUT > HELP** section.	Victims can send an **anonymous report** to the UNICEF team, in case of a violating post, comment or story on Facebook or Instagram.
Users can find Facebook and Instagram policies under **ABOUT > HELP** section.	Twitter provides the option of '**Bystander reporting**', i.e., a user can report cyberbullying/ cyber harassment on behalf of another user as well.	The UNICEF team reviews these reports 24/7 around the world in **50+ languages**, if something is found abusive, it is removed immediately.

Fig. 4.7 Reporting Cyber Crime Online (Source: IIPA)

4.2 Lodging a Cyber Crime Complaint on the National Cyber-Crime Portal

As one can see from these discussions, the Government of India has provided numerous mechanisms to report a cyber-crime in India; however, it would be most prudent to file it on the web portal of cybercrime.gov.in, which is a centralized portal by the Government of India (GoI). A National Cybercrime portal has been established to integrate and centralize information related to all CyberCrime cases across India. This portal now saves the hassle of physically going to a police station. So,reporting the cyber-crime on this portal would be good enough. The status of the cybercrime report can also be tracked through the portal by providing the necessary information, such as the Acknowledgment number of the complaint and the registered phone number/login ID. While reporting a cybercrime on the portal "cyber crime.gov.in," there is an option to select the particularState/UT. If this option is exercised, then the complaint details will be automatically sent to theconcerned State Police. However, in case of any emergency or if an FIR has to be filed immediately,then the local Police Station can also be approached for the same.

a) To file a complaint on the centralized portal of the Government of India (cybercrime.gov.in), one can take cues from the steps mentioned below.

Step 1 - Open the web-portal https://cybercrime.gov.in/ (Fig. 4.8)

Step 2 - On the homepage of the portal, the victim would find multiple tabs to access. Next to the home tab, there are two other tabs, viz. Report Women/Child-Related Crime and Report Other Cyber Crime.

Step 3 - To report a women/child-related cybercrime, the victim can click on the 'Report Women/ Child-Related Crime' tab. Following this step, a drop-down menu with two options will appear.
- 'Report Anonymously' or 'Report & Track a Complaint.'

Step 4 - The victim can select the 'Report Anonymously' tab if the victim does not want toreveal her/his identity. The cybercrime report would be filed anonymously on the portal without any registration (i.e., without collecting the victim's personal information such as email ID, mobile number, etc.).

Step 5 - The victim has to then click on the 'File a complaint' tab followed by the 'I accept' tab to report a cybercrime. The victim must read all the conditions carefully and then accept them.

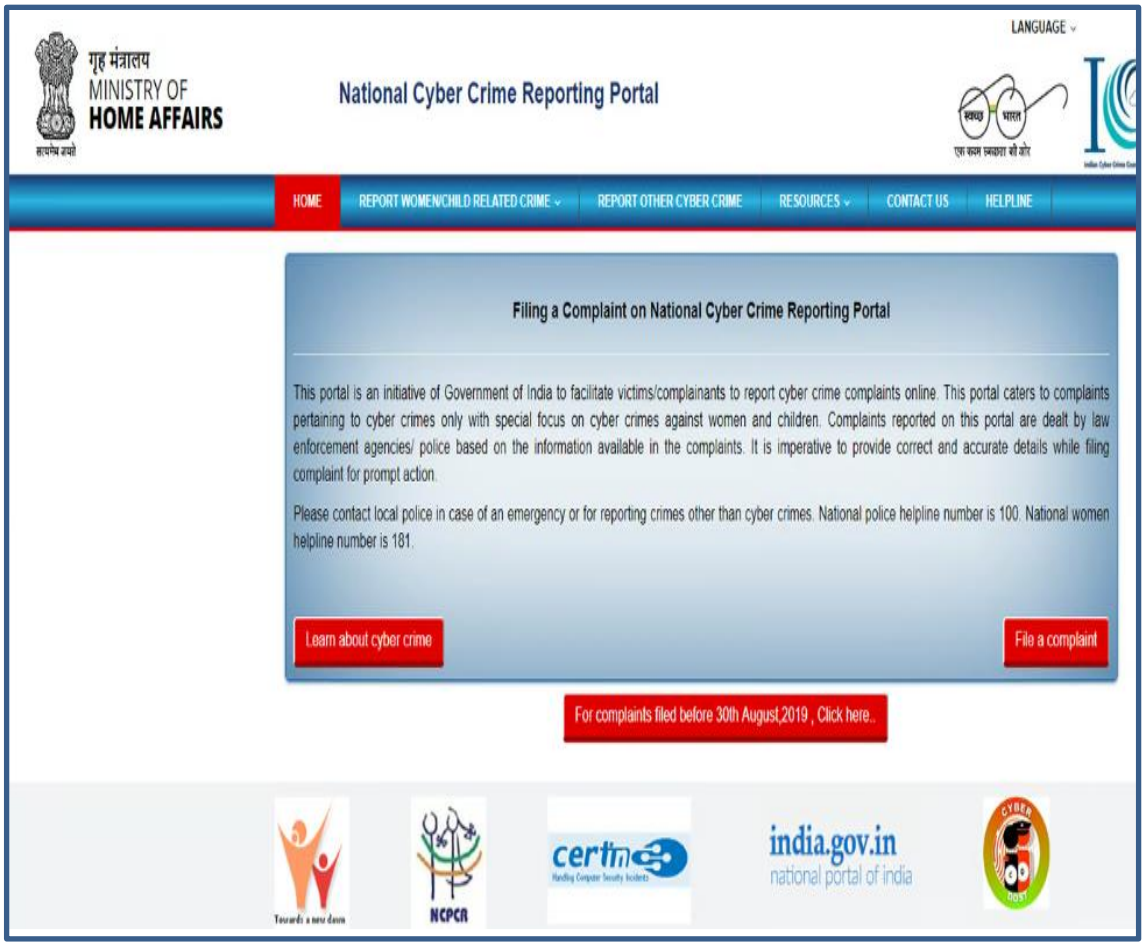


Fig. 4.8 Portal for Filing a Complaint (Source: National Cyber Crime Reporting Portal)

Step 6 - Fill in the complaint and incident details as asked in the following form. Once the form is completed, the victim has to click on the 'Save & Next' tab to move to the next part of the report.

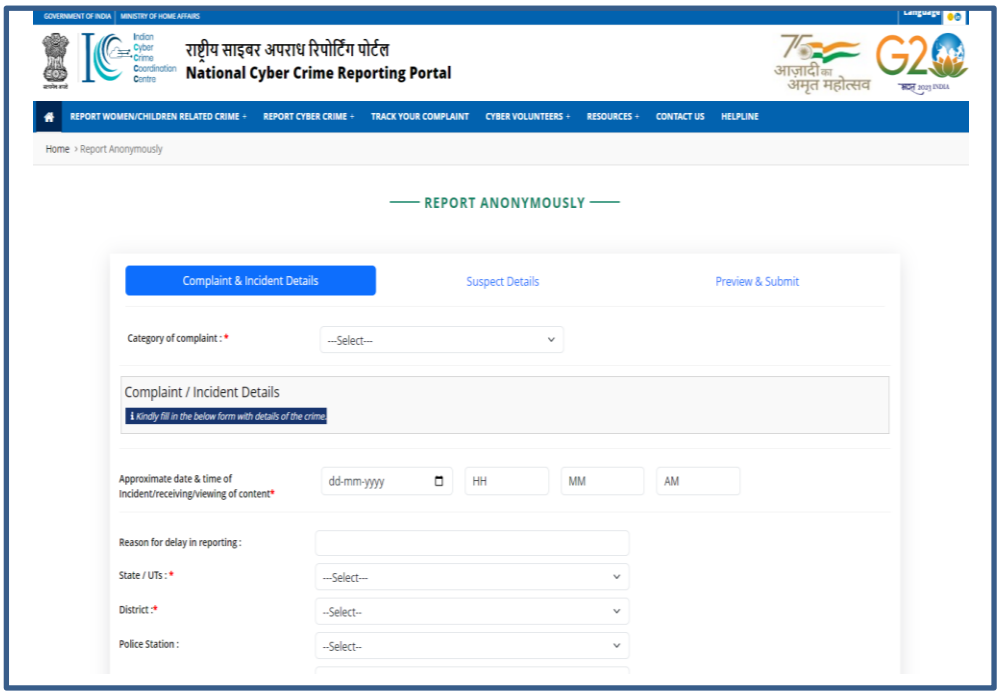


Fig.4.9 Cyber Crime Complaint Form to Report Anonymously(Source: National Cyber Crime Reporting Portal)

Step 7 - These details would be followed by the suspect details, if any. After clicking on the 'Save & Next' tab, the victim can preview the form and re-check all the details entered in the report.

Step 8 - Finally, the victim has to submit the report by clicking the 'Submit' tab on the screen.

Step 9 - However, if the victim selects the 'Report & Track' tab, a box to enter the citizen login details appears on the screen where the victim would be asked to fill in the state in which the crime occurred along with personal information such as a login ID (same as the email ID of the victim) and mobile number of the victim.

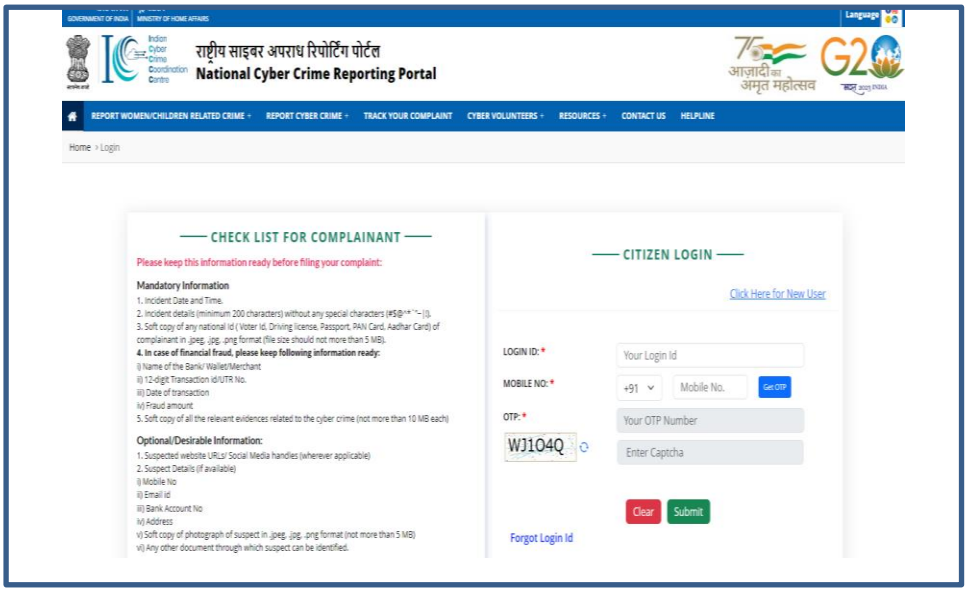


Fig. 4.10 Registering a New User on the National Cyber Crime Reporting Portal

Step 10 - The victim would receive an OTP on the registered mobile number and then, the victim can report the crime on the portal. After successfully logging in, the victim can choose the respective area of cybercrime and register a complaint.

Step 11 - The victim would be asked to fill in the relevant details of the cyber-crime.

Step 12 - However, if the victim selects the 'Report Other Cybercrimes' tab on the homepage, the victim will directly reach the page with the 'File a Complaint' tab. From here onwards, the victim must follow the same steps as above in the 'Report Anonymously' tab.

b) Tracking the Complaint Status on the National Cyber-Crime Portal

Step 1 - As soon as the victim has registered a complaint on the cybercrime portal, the victim will receive an acknowledgment number on the login ID and the registered mobile number to track the status of the complaint. All further communication regarding the investigation will be done through the victim's registered mobile number/login ID.

Step 2 - The victim would click on the 'Report and Track' tab to check the status of the cyber complaint. The complaint status can be tracked through the given acknowledgment number and an OTP that would be generated as the victim enters the portal.

Step 3 - The victim would enter the login ID, the mobile number, the OTP, and the captcha. As the victim clicks on the 'Submit' tab, the victim would receive the following screen with the status of the complaint updated by the police and the date on which the action was taken (Fig. 4.11).

Fig. 4.11 To track the complaint status (Source: National Cyber Crime Reporting Portal)

4.3 To Register Complaint if an Organization's Website is Hacked

In the cyber domain, identifying the individual responsible for the website hacking can be a challenging task, as many hackers conceal their tracks by using a VPN, Proxy, or Tor network, or sometimes the attack may be launched from another compromised machine. However, the IP Address from where the hack was perpetuated can be identified by analyzing the Web server logs and its configuration files, Logs of perimeter devices like Firewall, IPS/IDS, Network devices,

Application logs, Operating System Logs, User Activity Logs, etc. This information can be further used by Law Enforcement Agencies (LEA) to investigate further and identify the suspect.

The case can be reported to –

- **Indian Cybercrime Coordination Centre (I4C) -** To report a website hacking incident to I4C, India's central cybercrime agency established by MHA, the complaint can be reregistered at cybercrime.gov.in with sufficient evidence of the complaint for swift action. Accuracy is crucial for I4C's specialized teams to respond promptly, enhancing national-level coordination against cyber threats.
- **Cybersecurity Govt. Agencies ("CERT-In"/NCIIPC/NIC-CERT) -** The complaint of website hacking of a government organization should also be made to "CERT-In" (incident@cert-in.org.in) and National Critical Information Infrastructure Protection Centre (NCIIPC) (ir@nciipc.gov.in) if the site or its infrastructure or data has been officially notified as aCritical Infrastructure. If the site is hosted in NIC's Data Centre, then it should be reported to NIC-CERT (incident@nic-cert.nic.in).
- **Local Police Station** - A formal complaint can be submitted to the local SHO, along with screenshots of defaced websites and whatever technical/ related details are available.
- **CBI** - CBI should also be reported for the central government website. An email can be sent to (speou9del@cbi.gov.in) detailing the case along with the related artifacts/evidence/ screenshots. However, we still need to check whether there are any regulatory requirements for reporting a hacking incident to CBI.

Organizational Support for Incident Reporting and Support ("CERT-In"/NCIIPC)

a. "CERT-In" and NCIIPC can help in the analysis of logs/firewall/IP to know who hacked the website. They are well equipped with state-of-the-art tools for the same. They also have a cyber forensic wing for further analysis.

b. However, the organization must share all logs (Web server logs/firewall/IDS/IP routers and switches), the network diagrammatic scheme, and the website setup.

c. Once the incident is registered; an incident number will be generated and shared.

d. Once the incident gets resolved, the enquiring agency ("CERT-In"/NCIIPC) will ***provide the Root Cause Analysis (RCA)*** and close the case.
("CERT-In" toll-free number: 1800-11-4949; email: incident@cert-in.org)

4.4 Preventive Measures

"It is better to be safe than sorry" - runs an old adage. By taking some basic precautions, it would always be wiser to safeguard the endpoints - the digital devices in the users' hands. Some of the very popular preventive measures are safeguarding digital devices by installing anti-virus software (preferably more than one), installing firewalls, and so on.

4.4.1 Install Antivirus Software

Antivirus software is a type of application that is meant to prevent, detect, and eradicate malware attacks on individual computing devices, networks, and information technology systems. Antivirus software, which was initially meant to identify and remove viruses from computers, can now guard digital devices against a wide range of threats, including keyloggers, browser hijackers, trojan horses, worms, rootkits, spyware, adware, botnets, ransomware, and many more.

An antivirus software typically initiates a scan when a new device is started or plugged into the main system. Some antivirus software does this automatically in the background, while others warn users of infestations and prompt them to delete the files. Antivirus software is typically granted privileged access to the whole system to undertake all these activities. As a result, antivirus software in itself is also a frequent target for attackers. Hence, it is absolutely necessary to get reputed and

reliable antivirus software and update it regularly from its official site as the company comes out with patches against the latest discovered vulnerabilities. For the same reasons, many cyber experts insist on loading more than one anti-virus software on your device so that if one fails, the other one is still there to protect the device.

4.4.2 Install a Firewall

When the user's device, particularly a PC, is accessible through an internet connection or Wi-Fi network, it is prone to a cyber threat. However, one could restrict outside access to one's computer with a firewall. A firewall is a network security mechanism that monitors all incoming and outgoing traffic and allows, rejects, or drops that specific traffic depending on a predetermined set of security rules. The firewall checks network traffic against the rule set defined in its table. Firewalls are typically configured to block data from unknown or suspicious locations, such as certain IP

Addresses or certain devices/ports while allowing the authorized devices to get connected to the protected device/network.

Hardware firewalls come as separate devices. In an in-home/small office environment, routers from certain vendors could also include some of the relevant firewall features. In the software version, the majority of the firewalls come pre-configured to block malicious traffic.

In a similar context, a virtual private network (VPN) is another commonly used tool. It is a service that enables the user to maintain privacy online. A VPN creates a private channel for data and communications while the user utilizes public networks, establishing a secure, encrypted connection between the digital device and the internet.

Digital device users may also require a copy protection device (explained in the *Glossary*). A hardware key, also called a "dongle," is a type of software copy protection device that can be plugged into the USB port of a digital device. The application scans for a key as soon as the device is switched on, and it only activates if the key has the right code. A hardware key is used mostly with high-priced software. Since hardware keys are hard to replicate, they offer very effective copy protection.

However, a word of caution - Firewalls do not guarantee that malware will not attack the computer. It only protects against malware.

Therefore, to assure full protection the user must install a firewall in conjunction with other antivirus software to stay completely safeguarded.

4.4.3 Create Strong Passwords

Passwords are essential 'locks' to safeguard a user's social media account, bank login, Wi-Fi access, and so on. Passwords act as a deterrent against cyber attackers who may try to gain unauthorized access to the accounts or devices to steal the data. Therefore, storing all the passwords in a secure place is very important. For the same reason, one should have a very strong password that should be difficult to crack and update frequently.

1. **Characteristics of Weak Passwords:**
   i. Passwords that contain fewer than ten characters.
   ii. Passwords that are dictionary words (in any language).
   iii. Passwords that are common terms, including names of family members, pets, friends, colleagues, or characters from movies, novels, or comics, as well as computer-related terminology and names of websites, companies, or software.
   iv. Passwords that include birthdays or other personal details, such as addresses and phone numbers.
   v. Patterns of letters or numbers, like "123456," "aaaaa," "qwerty," "asdfg," or "zxcvb."

2. Tips for Creating Strong Passwords:

i. A robust password should incorporate letters, numbers, special characters, and uppercase letters. One effective method is to substitute letters with numbers and symbols, such as changing "i" to "!", "o" to "0," and "s" to "$." For example, the simple term "Microsoft" can be transformed into the much more secure "M!cr0$0ft."

ii. Password length is crucial; longer passwords are more difficult to crack.

iii. Consider using a memorable sentence and taking the first letter of each word to create a complex password that is easy to remember.

For instance, the sentence "My Name is Dinesh Anandan, and I was born on 1 January 1986!" can generate the password "MNiDAaIwbo1J1986!", which is lengthy, includes numbers, special characters, and uppercase letters, making it both memorable and unlikely to appear in a dictionary.

If one tends to forget passwords for different accounts, using a password manager to remember them is better. These password managers are readymade apps/utilities to create, manage, and store passwords. Many popular service providers have proprietary password managers that help generate strong, unique passwords for all accounts, such as bank accounts,social media, etc.

Benefits of using a password manager

1. The user would no longer need to remember all the passwords.
2. Password managers can generate safe passwords for the user automatically.
3. Password managers can warn the user about a phishing website.
4. Password managers are time savers.
5. Password managers can sync across many operating systems. They aid in the protectionof user identity.

If a task involves sharing passwords, such as when sending a password for an encrypted file attached to an email, it should be communicated through a separate channel, like a phone call or SMS.

Table 4.1 Tips for Creating Strong Passwords (Do's and Don'ts)

Tips to Create Strong Passwords
Do's
1. Create a strong password with at least ten characters, incorporating a mix of letters, numbers, and symbols.
2. Change all the passwords of email, computer, etc., periodically, at least once every month.
3. Treat passwords as sensitive information.
4. Use unique passwords for each login account. Sharing passwords across multiple accounts increases the risk of exposure if any site is compromised.
5. When you need to share passwords, such as for an encrypted file sent via email, do so through a different channel, like a phone call or SMS.
6. Avoid clicking at the prompt of the "Remember Password" feature whenever it is promptedby various browsers/apps.

Tips to Create Strong Passwords
Don'ts
1. Do not save passwords in browsers in an easily readable format, nor write them down on devices, whiteboards, office notice boards, or any other places where unauthorized individuals could find them. If you need to share passwords, use a separate method of communication, such as a phone call or SMS.

Fig. 4.12 Tips to Protect Password

4.4.4 Switch-On Incognito Mode

All major online browsers have a function that allows the user to open a private browsing window that deletes the browsing history when closed. It's known as "Incognito Mode," "Private Browsing," or "InPrivate Browsing," depending on the browser being used. When a user browses privately in Incognito mode, Chrome doesn't save the browsing history, cookies, site data, or information entered online.

How to go to Incognito mode while browsing -

1. Open Chrome on your computer.
2. Click "More" in the top right corner, then select "New Incognito Window."
3. A new window appears. In the top corner, check for the Incognito icon.

OR

Users can also use a keyboard shortcut to open an Incognito window -

1. Windows, Linux, or Chrome OS: Press Ctrl + Shift + n.
2. Mac: Press ⌘ + Shift + n.

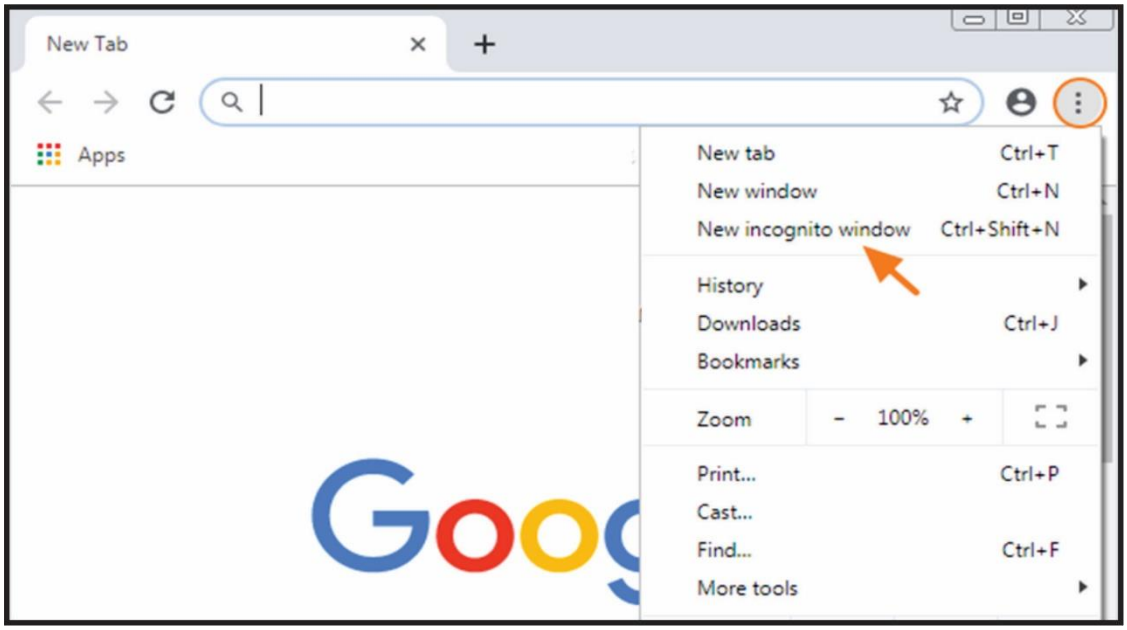


Fig. 4.13 How to Switch on the Incognito Mode

After selecting the "New incognito window" option, one can see in Fig. 4.13 that one will get the black screen and clearly see the incognito sign " ".Refer to the following Fig. 4.14.

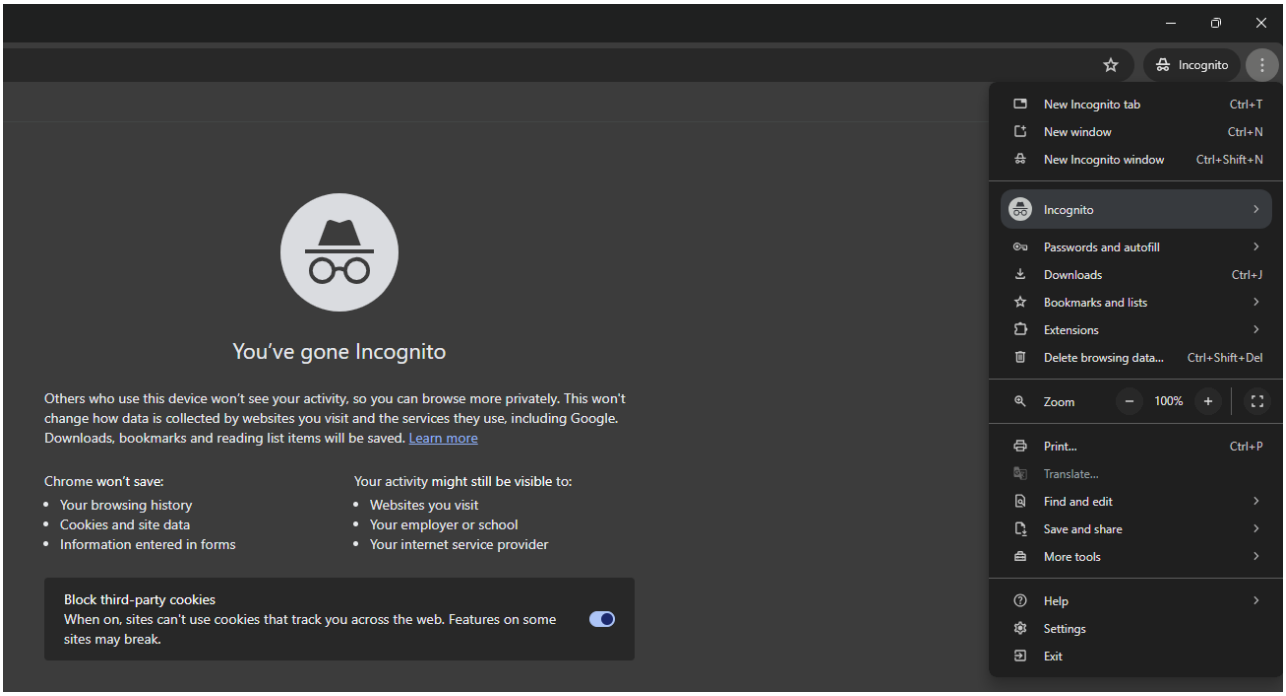


Fig.4.14 Device Screen, as the User Switches on the Incognito Mode

Following are a few advantages of using private/Incognito mode while browsing the Internet:

- **Deletes cookies:** Cookies are commonly used to provide users with a more targeted and customized browsing experience. Cookie Service providers, track these cookies and compileusers' online behavior and preferences to personalize the browsing activity. However, if thesecookies get hacked and land up with rogue actors, these could be misused to hack into theuser's personal information.

  Therefore, a user should ideally browse in Incognito mode. When a user logs out with Incognito Mode enabled, the browser will automatically remove these cookies, keeping the personal settings hidden from these service providers/web portals.

- **Keep browsing history private:** If a person needs to check their email or shop online on a public computer, there's a possibility that the device would save the browser history. This implies that the next person who logs on to the same device can also see all of thewebsites visited by the previous user and even get into them using their credentials.
- Incognito Mode prevents this kind of undesirable 'visibility' of browsing history by removing any temporary browser data as soon as the person logs out.
- **Enables multiple sessions:** It allows people to log into multiple accounts at the same time. For example, a person may use an Incognito window to log into the work account while using a regular window to stay in their account.

4.4.5 Employ Two-Factor Authentication

Two-factor authentication (2FA), sometimes also called 'two-step verification' or 'dual-factor authentication,' is a safety method wherein users get authentication elements to verify their identity before gaining access to an app, account, or email.

First-factor authentication is the password of the account. The second authentication could either be the user's mobile number or a biometric factor, such as a fingerprint or face scan. Two-factor authentication provides a further layer of safety to the authentication techniqueby making it more difficult for attackers to get access to a person's gadgets or online assets. Onlineservice providers are also increasing the usage of 2FA to guard their users' credentials against beingutilized by hackers who breach databases to get their users' passwords. So, if there is 2FA,these passwords could never be used singularly.

Apart from these basic preventive measures of browsing in Incognito mode, or always employing 2FA and adopting the practice of buying anti-malware software or firewalls from authorized vendors, one should specifically be very alert while securing one's e-commerce usage or safeguarding their mobile devices with extra caution. The following sections shall cover these aspects too.

4.5 Securing E-Commerce Usage

With the advent of the internet and online shopping, it has now become necessary to ensure that e-commerce transactions are safe and secure for all stakeholders involved. E-commerce security refers to the practices that provide secure online transactions. Some of the important aspects that could be kept in mind by the end-users are:

Table 4.2 Tips to Secure e-Commerce Usage (Do's and Don'ts)

Tips to Secure e-Commerce Usage
Do's
1. Check that the e-commerce website starts with HTTPS and displays a green padlock icon https:// to the left of the website's URL.
2. Shop only on genuine and trustworthy websites with contact details, such as email, phone number, or chat, available on them.
3. Create a separate e-mail address for online buying to prevent harmful emails, spam of sales promotions, or misleading offers.
4. Check the seller's reputation and credibility before making online payments.

Tips to Secure e-Commerce Usage
Don'ts
1. Do not blindly trust reviews. Sometimes the reviews too are fabricated by the e-commerce vendors themselves.
2. Do not fall for the "cheapest deals," especially if those are offered by relatively unknown vendors/sites. Always remember, there are no "free lunches," "amazing deals," or "freebies"in the e-commerce world.
3. Do not use or trust the customer care numbers provided on Google with personal information. These are often fake customer care numbers.
4. Do not save personal information, particularly financial details, on the e-commerce web portals.

Ways to Check if a website is Legit or Not

1. Do check validity by reviews, feedback from people, and the traffic on the website.
2. Do you Prefer a website with the connection type 'HTTPS,' particularly for the payment page?
3. Do check for a green padlock icon on the left corner beside the URL.
4. Evaluate website URLs ('http' or 'https').
5. Do not visit websites like '.biz' and 'info.'
6. Do check for spelling, like the name of the website, common spelling mistakes, use of dashes and similar symbols or similar-looking names but not the same name, and giving away of the fake e-commerce website.
7. Do not give personal details on ads or forms that request personal information.
8. Do not undertake financial transactions that do not display proper contact information.

Table 4.3 Tips to check if a website is legit or not.

Check if a website is legit or not
1. Check validity - by reviews, feedback from people, and the traffic on the website
2. Check for the green padlock icon on the left corner beside the URL.
3. Check for spelling in the domain name of the website, common spelling mistakes such as the use of dashes and similar symbols or similar-looking names, and giving away a fake e-commerce website.

4.6 Securing Digital Devices

Table 4.4 Tips to Secure Digital Devices

Tips to Secure Digital Devices
1. Turn on automatic updates in device settings so that apps are updated regularly.
2. Use a lock-screen application, biometric, or a password/PIN, particularly for mobile devices, as itcontains all the personal information, including contacts, financial information, GPS, and so on.
3. Close the webcam and computer audio when not in use.
4. Delete all Wi-Fi networks/Apps from the device that are no longer in use.
5. Switch off the Wi-Fi hotspot whenever it is not required.
6. Make it secure by enabling authentication for Wi-Fi hotspots and also restrict the number of users who can connect to this Wi-Fi hotspot.
7. Turn off location and internet while not in use.
8. Take a backup of the device data regularly.
9. Clear browsing history from time to time to prevent the misuse of personal information and to also help applications run better.

Tips to Secure Digital Devices
Don'ts
1. Do not use a USB or other external device owned by some other person.
2. Do not switch on your GPS/location settings when in public places or in sensitive settings.

4.7 Secure Internet Browsing

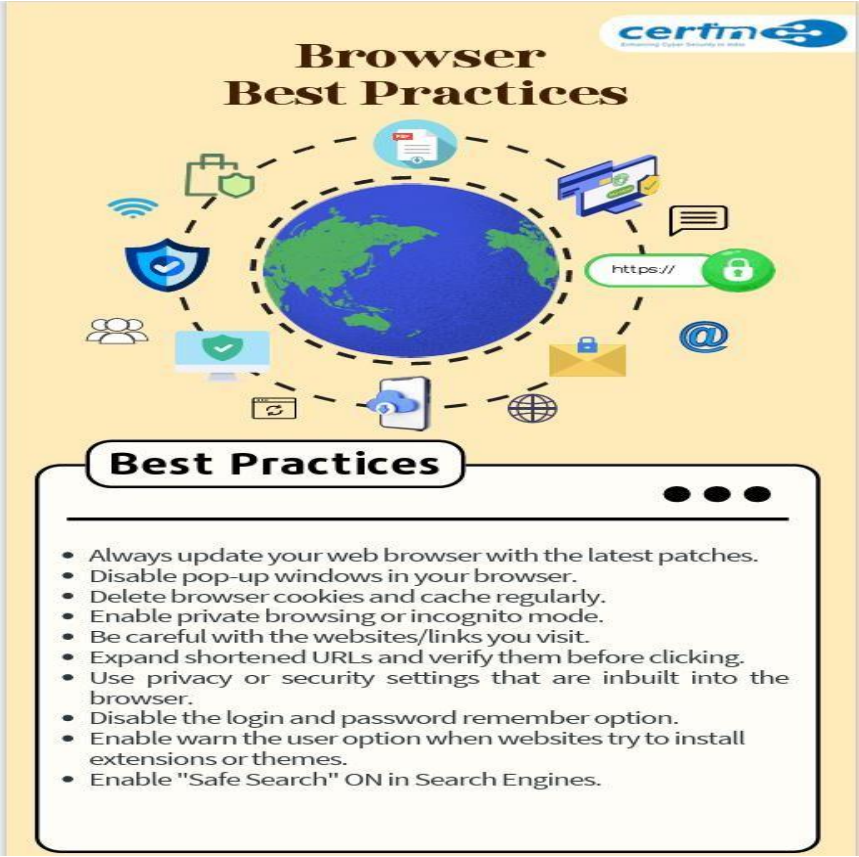


Fig 4.15 Browser Best Practices[15]

4.8 Some other Tools to Safeguard the Data ----(the associated sub-sections mentioned below it are unrelated or please consider point 10 of comments on digital hygiene handbook)

4.8.1 DigiLocker

One of the main projects of the Government of India under its prestigious Digital India program is the provision of a "Digital Locker," also popularly called "DigiLocker." DigiLocker is a cloud-based document storing solution for all by the Government of India.

Benefits of DigiLocker

It ensures that the user can access the documents anytime, anywhere. This is practical and time-saving.

1. It eliminates the use/circulation of fake documents, as originals are accessible onlythrough the individual's secured and authorized Digilocker account.
2. It even cuts down on government agencies' administrative costs by reducing theirreliance on paper.
3. The most essential aspect is that because papers are issued directly by registered issuers, DigiLocker makes it easy to verify their validity.

[15] https://www.cert-in.org.in/PDF/ISA_Booklet.pdf

Fig. 4.16 Homepage of the DigiLocker Website (Source: DigiLocker Website)

How to Use DigiLocker

Each citizen can use a cloud space of up to 1 GB to store their documents on DigiLocker.

Step 1: To avail yourself of DigiLocker's services, visit the official website at https://digilocker.gov.in/. Alternatively, you can download the DigiLocker mobile application from your device's App Store or Play Store.

Step 2: The user will be directed to the DigiLocker homepage. To proceed, they should click the "Sign Up" tab located in the top right corner of the screen.

Step 3: You will be redirected to an account creation page. The user would be asked to enter the following information - full name of the user, date of birth, mobile number, and email ID.

Step 4: The user will be asked to enter a preferred six-digit security PIN and click the 'Submit' tab.

Step 5: You will receive an OTP on the provided mobile number. Enter the OTP and click on the 'Submit' tab.

Step 6: To access a broader range of documents and services, verify your identity through Aadhaar-based authentication. Enter your Aadhaar number and click 'Update'.

Step 7: You will receive an OTP on the mobile number linked to your Aadhaar. Enter the OTP and click on the 'Submit' tab.

Step 8: You will be asked to create a username. Enter the username and click the 'Submit' tab again. Your DigiLocker account is now ready to be used.

Step 9: To get and import your digital documents, sign in to your DigiLocker account using either the registered mobile number or the UID number along with the six-digit security PIN and confirm with the OTP.

Step 10: Click on the 'Search Documents' icon after signing in. You will see different organizations under various categories.

Step 11: To get or import the documents, click on the respective organization tabs from which you are searching for your document and provide the required details to import your document into the "Issued Documents" section.

Step 12: Once the document is imported into the "Issued Documents" section, you can access it anytime, anywhere. DigiLocker 'Issued Documents' are considered as valid as original documents under the IT Act, 2000.

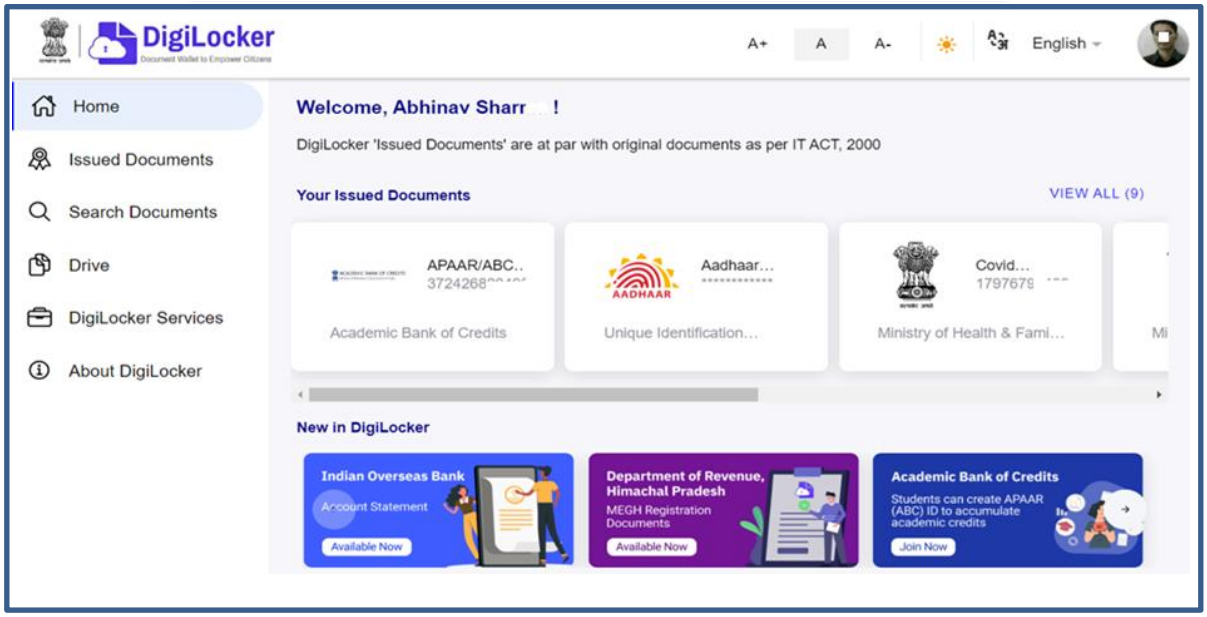


Fig. 4.17 DigiLocker Screen to Upload Documents Online (Source: DigiLocker Website)

Now, almost all the academic institutions and education boards issue the mark sheets of the students only in the Digilocker account of the students. The option of directly receiving certificates in the DigiLocker of the student is indeed a good alternative to the alternative of physically carrying hard-copy/paper-based certificates for the students.

However, students could also upload a scanned version of spurious certificates in their own DigiLocker accounts, particularly in those instances where the certification year is much prior to thetime of introduction of a DigiLocker facility by the education boards.

Therefore, to ensure the complete validity of certificates, a more secure option for education boards is to provide 'blockchain-based' certificates, which we will learn about in the next section.

4.8.2 Blockchain

A blockchain is a digital, tamper-proof, decentralized ledger that records transactions almost instantly and monitors assets within a virtual network. An asset can be tangible (a house, car, cash, land) or intangible(intellectual property, branding). Virtually anything that has any value attached to it can be trackedand traded on a blockchain network. Each transaction will be entered into the ledger, providing a continual control system regarding manipulation, mistakes, and data integrity.

Features of Blockchain Technology

- **Near-real time:** Blockchain provides near-real-time settlement of recorded transactions, eliminating friction and lowering risk.
- **No middleman:** Instead of faith, blockchain technology is based on cryptographic evidence allowing any two parties to interact directly with one other without the use of a middleman.
- **Distributed ledger:** The peer-to-peer distributed network keeps a public history of transactions. The blockchain is made publicly available and widely accessible. Only the evidenceof the transaction's existence is generally preserved by the blockchain, not the identities of the parties or the transaction data.
- **Irreversibility & Immutability:** The blockchain maintains a precise and verifiable record of every single transaction that has ever occurred. This prevents previous blocks from being changed, preventing duplicate spending, fraud, abuse, and transaction manipulation.
- **Smart Contracts:** Stored procedures that run on a Blockchain to perform predefined business processes and complete a commercially/legally enforceable transaction without the requirement for a middleman.

Due to several such advantages of blockchain, some teaching and training institutes have started issuing completion certificates on the blockchain. Such certificates are not just in soft copy but are also duly certified and tamper-proof. It leaves no scope for "fake degrees" or "fake mark sheets" and could be easily validated by job-providing agencies.

4.8.3 Parental Controls

With the ease of access, the internet exposes kids to various threats like identity theft, cyberbullying, social media scams, and malicious content. That is why parental control has become an essential requirement to protect children.

Parental controls are features or software allowing parents to monitor and restrict their child's online activities. A wide variety of programs/utilities do such things as block andfilter websites and content, record their activities, limit their time online, and view their browsing history and communications.

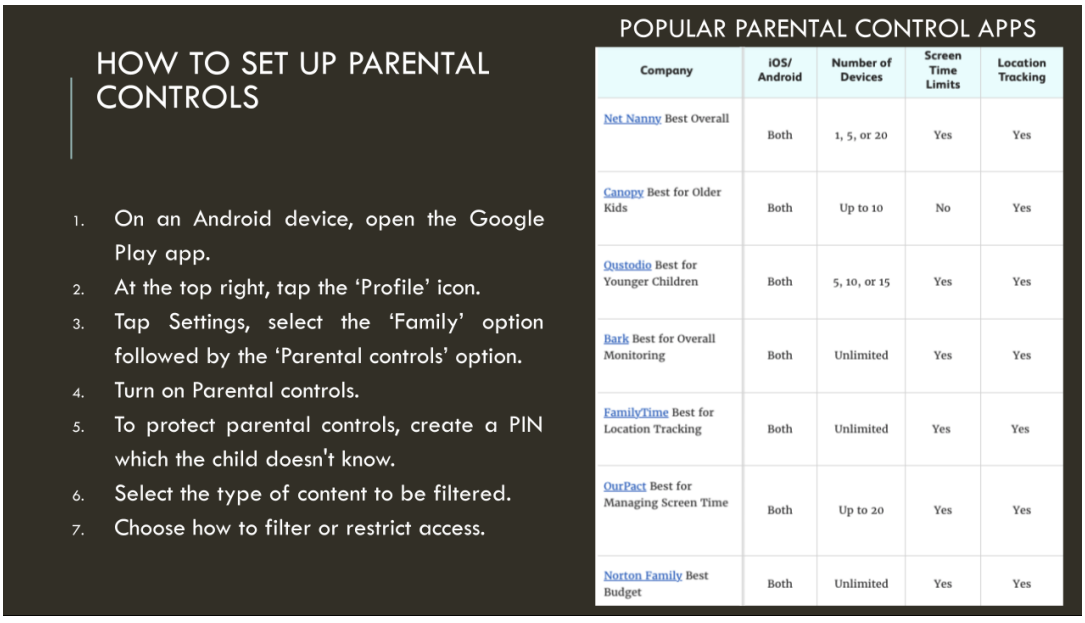


Fig. 4.18 Steps to set up parental controls and popular parental control apps (Source: IIPA)

Chapter 5: Understanding the Institutional Framework of Cyber Security in India

On June 29, 2021, India was ranked the tenth best country in the world in the 'Global Cybersecurity Index' (GCI) 2020 (International Telecommunication Union- ITU, 2020). This tenth rank is a significant leap of thirty-seven places from India's previous GCI rank in the year 2018. This ranks India 4th in the Asia Pacific region. GCI Index particularly measures a country's commitment towards its cyber security preparedness on five fronts viz legal, technical, organizational, capacity development, and cooperation. Undoubtedly, the Government of India (GoI) has undertaken some good initiatives in all these five aspects, particularly in institutionalizing several cybersecurity-related organizations. Some of these cyber-security-related organizations directly report to the Ministry of Electronics & Information Technology (MeitY), and others are attached to the Ministry of Home Affairs (MHA) and the Ministry of Defence. In this chapter, we shall delineate only a handful of them that are more relevant to the context of this handbook.

5.1 Organizations working under PMO

5.1.1 National Security Council Secretariat (NSCS)

National Security Council Secretariat (NSCS) of India is an executive government agency tasked with advising the Prime Minister's Office on national security and strategic interest matters. The appointment of the National Cyber Security Coordinator (NCSC) under the NSCS is responsible for the formulation of policies and strategies for cyber security, including their compliance and implementation. The NCSC also coordinates and consults with various Indian stakeholders and agencies handling cyber-related activities to evaluate and analyze the progress of incident reports. The NCSC also engages with private industry to form policies that will govern the scope of public-private partnerships in the field of cybersecurity.

The NCSC is an authority in India that provides an overarching view of the existing and emerging cyber security risks by advising and ensuring the implementation of action plans for cyber security by nodal agencies. The NCSC under the NSCS is also mandated to suggest positions in International Forums on internet governance and cyber security issues. The office of the NCSC also undertakes R&D projects to build capabilities and capacities in cyber, including the conduct of National-level cyber exercises.

5.1.2 National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Critical Information Infrastructure Protection Centre (NCIIPC) is an entity of the Government of India that was established under Section 70A of the IT Act, 2000 (amended in 2008) as the National Nodal Agency to protect Critical Information Infrastructure. The goal is to provide a safe, secure, and reliable information infrastructure for the nation's critical sectors.

5.2 Ministry of Electronics and Information Technology (MeitY)

The Ministry of Electronics and Information Technology (MeitY) aims to drive India's e-development as a catalyst for transforming the nation into a developed society. Its mission focuses on promoting e-governance to empower citizens, fostering inclusive and sustainable growth in the Electronics, IT, and ITeS sectors, and enhancing India's influence in Internet

Governance. This includes a multifaceted strategy that emphasizes human resource development, research and innovation, improving efficiency through digital services, and ensuring a secure cyberspace. One of its key goals is to safeguard India's cyberspace.

MeitY oversees important legislation such as the Information Technology Act 2000 (amended in 2008), the Digital Personal Data Protection Act 2023, and the National Cyber Security Policy 2013, among other IT-related laws. Below are some key cybersecurity organizations operating under MeitY (listed in a particular order).

5.2.1 "CERT-In" (Indian Computer Emergency Response Team)

The Indian Computer Emergency Response Team (CERT-In) is a statutory organisation under the Ministry of Electronics and Information Technology, Government of India. CERT-In has been designated under Section 70B of the Information Technology Act, 2000, to serve as the national agency to respond to computer security incidents as they arise.

The "Cyber Swachhta Kendra" is a project of the Indian Computer Emergency Response Team ("CERT-In"), which works as a Botnet Cleaning and Malware Analysis Centre. CSK provides free desktop and mobile security solutions through collaboration with Industry partners to detect and remove Botnet infections. Cyber Swachhta Kendra's website also provides awareness material to educate the public about the importance of protecting their data on computers, mobile phones, home routers, and other devices. M-Kavach 2, a comprehensive mobile device security solution developed by CDAC to address emerging threats related to Android-based mobile devices, is also available on the Cyber Swachhta Kendra website. The major emphasis of M-Kavach is on advising the users against security misconfigurations, detection of hidden/ banned apps, and scanning the device for potentially malicious apps installed on the user's mobile device.

Figure 5.1 Cyber Swachhta Kendra-Security Tools

Fig. 5.2 Homepage of the M-Kavach 2 App (Source: CDAC)

5.2.2 The National Cyber Coordination Centre (NCCC)

The government has set up the National Cyber Coordination Centre (NCCC) to generate macroscopic views of the country's cyber security threats. The Centre will scan the country's cyberspace at the metadata level and generate near real-time situational awareness. NCCC is a multi-stakeholder body and is being implemented by the Indian Computer Emergency Response Team (CERT-In) at the Ministry of Electronics and Information Technology (MeitY).

5.2.3 Standardization Testing and Quality Certification (STQC)

STQC Directorate is an attached office of the Ministry of Electronics and Information Technology (MeitY), Government of India, established in 1980. STQC Directorate has established a network of fifteen testing and calibration laboratories in the country, including the North-Eastern region. STQC laboratories offer quality assurance services in the field of electronics and information technology, including e-Governance applications as per national/ international standards/ best practices, and obtained many national and international accreditations/ recognitions.

5.2.4 Centre for Development of Advanced Computing (CDAC)

The Ministry of Electronics and Information Technology's (MeitY) Centre for Development of Advanced Computing (C-DAC) is the ministry's primary research and development Centre

For IT, electronics, and related fields. C-DAC has been conducting research and development in many sub-areas within the Cyber Security sector. C-DAC's thematic areas of current focus include (a) High-Performance Computing/ Supercomputing and Grid Computing, (b) Indian Language Technologies, (c) Cyber Security, (d) Professional Electronics covering VLSI Technologies, Power Systems Technologies, Intelligent Transport Systems, (e) Health Informatics, (f) Software Technologies covering Free & Open Source Technologies and E-Governance Applications, and (g) Education Technologies covering e-learning and intelligent Class Rooms. In each of these areas, it has achieved notable outcomes in innovation, system design and development, research publications, and implementation.

5.2.5 Controller of Certifying Authorities (CCA):

The Central Government has appointed the Controller of Certifying Authorities (CCA) under section 17 of the IT Act. The CCA's office was established on November 1, 2000, with the goal of promoting E-Commerce and E-Governance through the widespread use of digital signatures. Under section 18(b) of the IT Act, the CCA has set up the Root Certifying Authority of India (RCAI) to digitally sign the public keys of Certifying Authorities (CAs) across the country. The RCAI operates in accordance with the standards established by the Act. The CCA uses its private key to certify the public keys of CAs, allowing users in cyberspace to verify that a licensed CA issued a certificate. Additionally, the CCA maintains a Repository of Digital Certificates, which includes all certificates issued to CAs in India.

5.3 Ministry of Home Affairs (MHA)

The Ministry of Home Affairs (MHA) oversees the country's cybersecurity and information security. The cyber and information security in the country is primarily undertaken through its Cyber and Information Security (C&IS) Division (https://www.mha.gov.in/division_of_mha/cyber-and- information-security-cis-division). The division is responsible for Cyber Security, Cyber Crime, implementation of the National Information Security Policy and Guidelines (NISPG), working of National Intelligence Grid (NATGRID) - which is the integrated intelligence master database structure for counter-terrorism purposes, and many more such related issues. There are four wings /desks in this division.

i. The "coordination wing" investigates all coordination matters, including RTI applications and annual reports.

ii. The second wing, called the "cyber-crime wing," deals with all matters related to cyber-crime complaints, its best practices, etc.

iii. The third wing of this division, the "information security," deals with information security-related matters, including capacity building of its officials.

iv. The fourth wing/desk, called the "monitoring unit," investigates the policy of lawful interception and coordinates with MeitY to block websites and much more.

5.3.1 Indian Cyber Crime Coordination Centre (I4C) :

The Indian Cyber Crime Coordination Centre (I4C) was established on October 5, 2018, as part of the Central Sector Scheme within the Cyber and Information Security Division of the Ministry of Home Affairs. Its main goal is to create a national-level coordination center to tackle all issues related to cybercrime in the country. I4C focuses on strengthening the capabilities of Law Enforcement Agencies (LEAs) and enhancing cooperation among different agencies and law enforcement bodies. The headquarters of I4C in New Delhi was inaugurated and dedicated to the nation on January 10, 2020. As of July 1, 2024, I4C has been recognized as an attached office under the Ministry of Home Affairs. The Indian Cyber

Crime Coordination Centre comprises several components, which are detailed as follows:

1. **National Cybercrime Reporting Portal (NCRP)** allows Indian citizens to report all types of cybercrime. It was officially dedicated to the nation by the Hon'ble Home Minister of India on January 20, 2020.
2. **National Cybercrime Threat Analytics Unit (NCTAU**) facilitates collaboration among law enforcement agencies, private sector, academia, and research organizations to analyze cybercrime information. It collects data from open sources, the National Cybercrime Reporting Portal, CERT-In, and other agencies, analyzes it, and shares actionable insights with relevant authorities to inform their responses and strategies.
3. **National Cybercrime Ecosystem Management Unit (NCEMU**) is working to build a stronger national cybersecurity framework by bringing together government agencies, industry leaders, and academic experts. By promoting collaboration and a multi-stakeholder approach, the NCEMU is dedicated to creating an effective ecosystem for addressing and neutralizing cyber threats.
4. **Joint Cybercrime Coordination Teams (JCCT)** facilitate coordination between law enforcement agencies across states and UTs by sharing information such as names, contact details, and case specifics of cyber criminals. The JCCT enhances interstate cybercrime investigations through operational collaboration and an integrated platform, ensuring effective coordination and efficient handling of complex, multi-state cybercrime cases.
5. **National Cybercrime Forensic Laboratory (NCFL)** in New Delhi provides advanced forensic analysis of digital evidence to support law enforcement investigations. Utilizing the latest technology, the NCFL keeps pace with evolving cybercrime techniques to ensure thorough analysis and accurate results in solving cases.
6. **National Cybercrime Training Centre (NCTC)** standardizes training for cybercrime prevention, containment, and investigation. It focuses on building the capacity of law enforcement agencies, public prosecutors, and judges in handling cybercrime.
7. **National Cybercrime Research and Innovation Centre (NCR&IC)** tracks emerging technologies and predicts potential vulnerabilities exploited by cyber criminals. It builds strategic partnerships with academia, industry, and intergovernmental organizations to advance research and innovation in cybercrime prevention and response.
8. **Cyber Fraud Mitigation Centre (CFMC)** established at 14C with representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and States/UTs Law Enforcement Agency will work together for immediate action and seamless cooperation to tackle online financial crimes. CFMC will serve as an example of "Cooperative Federalism" in law enforcement.

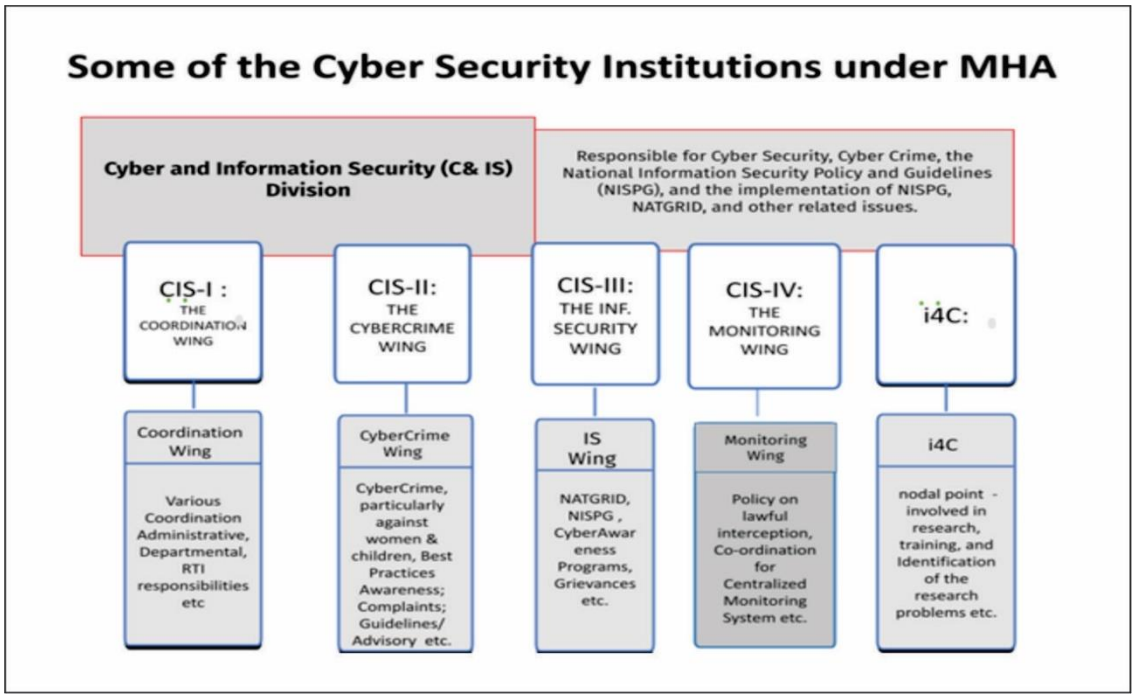


Fig. 5.3 Some of the Cybersecurity Institutions under MHA (Source: IIPA)

5.4 State Cyber-Crime Cells

Apart from these organizations, India currently has cyber crime cells in almost all states of the country (https://cyber crime.gov.in/Webform/Crime_NodalGrivanceList.aspx), which were also already mentioned in the previous chapter (How to file a cyber-complaint on National crime portal). The state cybercrime cells, managed by cyber nodal officers, provide an effective response mechanism at the state level in case of cybercrime. An individual can visit a cybercrime cell in their city to register and file a written complaint and take action against cybercrime. Some of these state cybercrime cells are quite vibrant in related activities. For instance, The Delhi Police's Cyber Crime Cell is a specialized division that investigates all complex and sensitive cyber incidents, particularly those involving women and children as victims. The Delhi Police's CyPAD (Cyber Prevention & Awareness Detection) unit (http://cybercelldelhi.in/about-us.html) is also a part of Delhi's cybercrime cell. It also has a Cyber Lab with 'National Cyber Forensics Lab' (NCFL)with all the related forensics capabilities.

Chapter 6: Glimpses into the Legal Framework for Cyber Security in India

A cybercriminal is prosecuted under the Information Technology (IT) Act, 2000, and the Bhartiya Nyaya Sanhita, 2023 (earlier Indian Penal Code, 1870). We shall have a brief glimpse into each in this chapter.

Disclaimer: The cases cited under each act are given to support the general understanding of the acts. However, the reader should be aware that one case is not restricted to one particular act. Hence, one-on-one correspondence on cases is not exhaustive. This has been done only to strengthen the basic concepts of the reader.

6.1 Information Technology Act 2000 (Amended in 2008)

The Indian Parliament introduced the Information Technology Act, 2000 (IT Act) on October 17, 2000. This law is one of India's key legislations addressing cybercrime and e-commerce issues, and it is enforced by the Ministry of Elecronics and Information Technology (MeitY). Due to the rapid increase in computer and internet usage, the government has amended the IT Act multiple times to tackle the evolving nature of cybercrimes. The Information Technology Amendment Act, 2008 (IT Act 2008) introduced significant changes to the original IT Act 2000.

Some of the relevant IT Act 2000 sections comprise the following:

- **Section 43**: This section pertains to penalties and compensation for causing damage to a computer or computer system. It applies when someone manipulates or tampers with a computer, system, or its services, resulting in unauthorized use. The individual responsible is required to compensate the affected party for the damages caused.
- **Section 65**: This section addresses the intentional concealment, destruction, or alteration of any computer source code used in a computer, program, system, or network, especially when such source code is legally required to be maintained. Anyone guilty of this act can face imprisonment of up to three years, a fine of up to two lakh rupees, or both.
- ***Bomb Hoax Email Case****: In 2009, a 15-year-old boy was arrested by the Cybercrime Investigation Cell (CCIC) of the city's crime branch for allegedly sending a false bomb threat email to a private news channel. The email claimed that five bombs had been planted in Mumbai, daring the police to locate them. The police immediately alerted and traced the email's origin through the Internet Protocol (IP) address.*
- **Section 66 -** Defines offenses such as hacking with intent to cause damage or disruption and unlawful access to computer systems or networks and provides penalties for the aforementioned offenses, including imprisonment and fines.
- **Section 66B**: This section outlines the penalties for individuals who knowingly receive or possess stolen computer resources or communication devices. If a person is found to have obtained or retained such stolen items with the awareness or reasonable belief that they were stolen, they may face imprisonment for up to three years, a fine of up to one lakh rupees, or both.

- **Section 66C**: This section addresses penalties for identity theft. Anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other unique identification feature is subject to imprisonment of either description for up to three years and may also face a fine of up to INR 1,00,000.
- **Section 66D**: This section deals with penalties for cheating by impersonation using computer resources. Any person who, through any communication device or computer resource, deceives by impersonation can be imprisoned for up to three years and may also be liable to a fine of up to INR 1,00,000.
- **Section 66E**: This section addresses offenses related to violating an individual's privacy, which is considered a punishable crime.

  Example: In an infamous case, a pornographic MMS was filmed on the premises of a prominent institution and shared externally, tarnishing the university's reputation. Media reports suggested that the two accused students initially attempted to extort money from the victim but, after failing, distributed the video via mobile phones and the internet, even selling it as a CD in the illicit market.

- **Section 66F**: This section covers cyberterrorism, specifically large-scale disruptions to computer networks connected to the Internet. It includes activities such as cyberattacks using viruses, worms, phishing, malicious software, hardware strategies, programming scripts, and other related tools.
- **Section 67**: This section deals with penalties for publishing or transmitting obscene material electronically. It punishes individuals who publish, transmit, or cause to be published any lascivious content, appeals to prurient interests, or whose impact is likely to corrupt or deprave those who may access, read, or view it, taking all relevant circumstances into account.

  Harassment via Fake Social Media and Email Accounts*: A woman became the target of harassment through numerous fake social media posts and a barrage of emails sent from a fraudulent account created by the perpetrator using her name. These false postings led to a series of distressing phone calls to the victim. After the woman filed a complaint, the police apprehended the accused. Investigations revealed that the offender, a family friend, had been interested in marrying the victim. Upon her refusal, he began to harass her online.*
  Verdict*: The court found the offender guilty and sentenced him under Sections 469, 509 of the Indian Penal Code (IPC), and Section 67 of the Information Technology Act, 2000.*
  Under Section 469 IPC*, the offender received two years of rigorous imprisonment and a fine of INR 500.*
  Under Section 509 IPC*, the sentence included one year of imprisonment and a fine of INR 500.*
  Under Section 67 of the IT Act 2000*, the offender was sentenced to two years of imprisonment and a fine of INR 4000.*

All the sentences were supposed to run simultaneously. The offender settled the fine and was taken to Chennai's Central Prison.

- **Section 67A**: This section provides penalties for publishing or transmitting material containing sexually explicit acts or conduct in electronic form. For a first conviction, the offender can face up to five years in prison and a fine of up to ten lakh rupees. For subsequent convictions, the prison term can extend to seven years, with the same fine limit.

- **Section 67B**: This provision addresses the publication or transmission of content depicting children engaged in sexually explicit acts or behavior. It encompasses various activities such as creating, collecting, seeking, viewing, downloading, advertising, promoting, sharing, or distributing such content. The penalties for violations are stringent, with specific terms and conditions detailed further within the section.
- **Section 69**: This section grants authority to issue directives for the interception, monitoring, or decryption of any information transmitted through a computer resource.
- **Section 69A**: Under Section 69A of the IT Act, the Central Government or its authorized officials can block public access to any online information if it's necessary for national security, public order, or preventing crime. The decision must be documented in writing. Specific procedures and safeguards for implementing such blocking will be prescribed. Intermediaries who do not comply with these orders can face up to seven years in prison and fines.
- **Section 70**: This section addresses unauthorized access to protected systems. It states that if a person, without proper authorization, accesses or attempts to access a computer resource that is protected by security measures, they can be penalized. The penalties include imprisonment for up to three years, a fine of up to five lakh rupees, or both. This section aims to protect systems from unauthorized access and ensure compliance with security measures.
- **Section 71**: If someone makes false statements or hides important information to obtain a license or electronic signature certificate, they can face up to two years in prison, a fine of up to one lakh rupees, or both.
- **Section 72**: If a person accesses and discloses confidential electronic records or information without consent, they can be punished with up to two years in prison, a fine of up to one lakh rupees, or both.
- **Section 73**: This section deals with penalties for sending offensive or false electronic communications. If someone sends or causes to be sent any message or information that is offensive, false, or meant to harm, they can be punished with imprisonment for up to three years, a fine of up to five lakh rupees, or both.
- **Section 74**: This section pertains to the misuse of digital signatures. It makes it illegal to knowingly use or create fraudulent electronic signatures or certificates intending to deceive. The penalties for such offenses include imprisonment for up to seven years, a fine, or both.

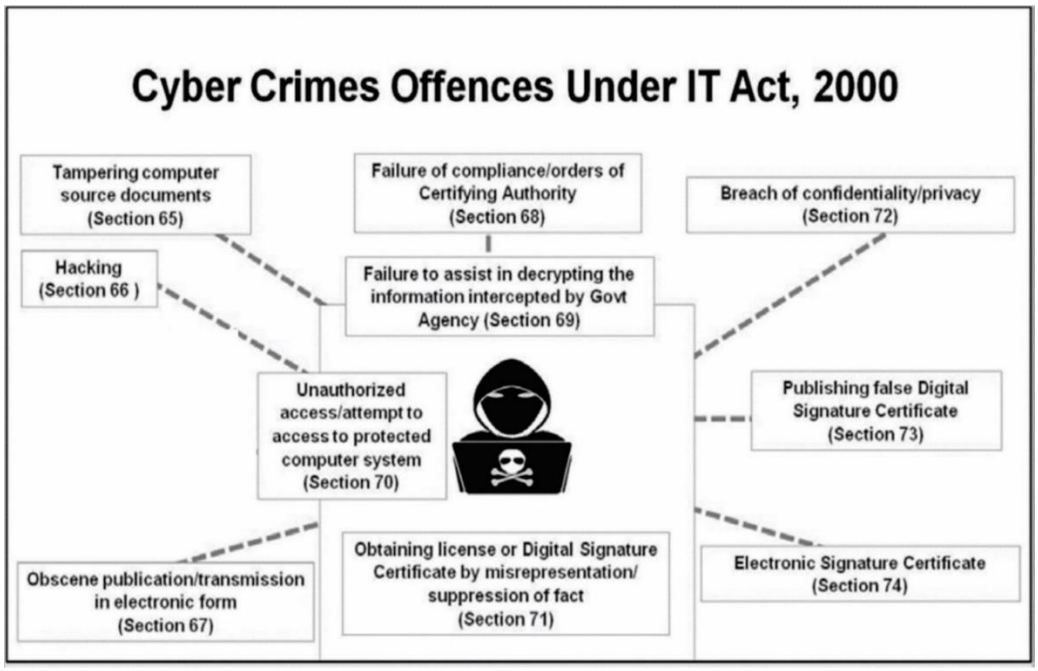


Fig. 6.1 Cyber Crime offences under IT Act, 2000 (Source: IIPA)

6.2 Indian Penal Code (IPC), 1860

The Bhartiya Nyaya Sanhita, 2023 (earlier Indian Penal Code) codifies criminal offences and guides cybercrime. The acts coveredby the Information Technology Act of 2000 are based on the offences codified under the Bhartiya Nyaya Sanhita, 2023 (earlier Indian Penal Code) related to computer and internet use. To make the punishment severe for the offender, Legal Enforcement Agencies use parts of the Bhartiya Nyaya Sanhita, 2023 (earlier Indian Penal Code) and the Information Technology Act of 2000.

The tabular representation (Table 6.1 and Table 6.2) will adequately highlight the comparison between erstwhile offences under IPC and present Offences under BNS that apply to cyber-crimes.

Table 6.1: Sectionwise Comparison between Offence under IPC(Erstwhile) and Offence under BNS (Present)

Offences under IPC	Offences under BNS
Offences by/against public servant (Section 167,172,173,175)	Offences by/against public servant (Section 201, 206, 207, 210)
False electronic evidence (Section 193)	False electronic evidence (Section 229)
Destruction of electronic evidence (Section – 204,477)	Destruction of electronic evidence (Section –241, 343)
Counterfeiting Property Mark (Section- 183,482,483,484,485)	Counterfeiting Property Mark (Section- 218, 345(3),347(1),347(2),348)
Cheating (415, 420)	Cheating (318(1), 318(4))
Forgery (Section- 463,465,466,468,469,471,474,476,477)	Forgery (Sections 304, 377, 379, 380, 382, 383, 385, 388, 389, 391, 392, 357)
Tampering (Section 489)	Tampering (Section 498)
Criminal Breach of Trust (Section – 405,406, 408,409)	Criminal Breach of Trust (Section – 316, 317, 319, 320)
Counterfeiting Currency /Stamps (Section -489 & 489E)	Counterfeiting Currency /Stamps (499 to 503)

Table 6.2: Comparison between Offence under IPC(Erstwhile) and Offence under BNS(Present) based on provisions

Provision	Description	IPC Section	BNS 2023 Provision	Comparison
Defamation	Defines defamation and prescribes punishment for it.	Section 500	BNS 2023 Section 106	BNS Section 106 addresses defamation with potentially updated definitions or penalties.
Sedition	Defines sedition and prescribes punishment for disaffection against the government.	Section 124A	BNS 2023 Section 132	BNS Section 132 may modernize or alter the scope and penalties related to sedition.
Insulting Modesty	Deals with acts intended to insult or offend the modesty of a woman.	Section 509	BNS 2023 Section 137	BNS Section 137 may include updated definitions or increased penalties for offenses related to modesty.
Public Mischief	Addresses statements or rumors that could cause public alarm or mischief.	Section 505	BNS 2023 Section 145	BNS Section 145 may refine the scope of public mischief and address new forms of misinformation.
Criminal Intimidation	Covers intimidation with threats to cause harm or injury.	Section 506	BNS 2023 Section 124	BNS Section 124 might update definitions and the scope of criminal intimidation and threats.

Cybercriminals are prosecuted under the Information Technology (IT) Act, 2000, and the Bhartiya Nyaya Sanhita, 2023 (Indian Penal Code). We shall have a brief glimpse into each in this chapter.

Disclaimer: The cases cited under each act are given to support the general understanding of the acts. However, the reader should know that one case is not restricted to one particular act. Hence, one-on-one correspondence on cases is not exhaustive. This has been done only to strengthen the basic concepts of the reader.

6.3 National Cyber Security Policy, 2013

The National Cyber Security Policy was unveiled by the Ministry of Electronics and Information Technology (MeitY) in July 2013, aiming to establish a secure and resilient cyberspace for individuals, businesses, and the government. Its mission focuses on safeguarding information and infrastructure within cyberspace, enhancing capabilities to prevent and respond to cyber threats, mitigating vulnerabilities, and minimizing the impact of cyber incidents. This is achieved through a blend of institutional frameworks, personnel, processes, technology, and collaborative efforts. The policy aims to foster a secure cyber environment and assurance framework, promote open standards, strengthen regulatory measures, manage vulnerabilities, protect e-governance services, and advance research and development in cybersecurity alongside human resources development.

6.4 Directions relating to information security practices issued by CERT-In, MeitY

The Internet in India is rapidly expanding, with projections indicating that over 1.2 billion Indians will gain access in the coming years, utilizing it for business, education, finance, and

various other applications, including digital government services. While this growth has spurred innovation, it has also led to increased cybercrimes, user risks, and challenges to online safety. The Government of India aims to ensure that users experience a Safe & Trusted Internet.

As part of this initiative, Cyber Security Directions were introduced to enhance online safety and trust for users. On April 28, 2022, CERT-In issued these directions under sub-section (6) of section 70B of the Information Technology Act, 2000, which is overseen by MeitY. The goal is to clarify for various stakeholders how to achieve compliance and promote an open, safe, trusted, and accountable Internet across the country.

These directions aim to bolster online safety and cyber security, ensuring a secure online environment. They apply to service providers, intermediaries, data centers, corporations, and government entities, outlining requirements such as synchronizing ICT system clocks, reporting cyber incidents to CERT-In, maintaining ICT system logs, and ensuring subscriber information and KYC records registration. Specifically, this applies to Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers, Virtual Private Network (VPN) Service providers, virtual asset service providers, virtual asset exchange providers, and custodian wallet providers. It is important to note that these Cyber Security Directions of April 28, 2022, do not pertain to individual citizens.

6.4.1 Guidelines on information security practices for Government entities" issued by CERT-In, MeitY

These guidelines are designed to establish a prioritized baseline for cyber security measures and controls within government and affiliated organizations. They aim to assist security teams in implementing essential controls and procedures to safeguard their cyber infrastructure against significant threats. Additionally, these guidelines serve as foundational documents for administration and audit teams (including internal, external, and third-party auditors) to assess an organization's security posture in relation to cyber security baseline requirements.
The guidelines encompass best practices categorized into various security domains, including Network Security, Application Security, Data Security, Auditing, and third-party outsourcing. Issued by the Indian Computer Emergency Response Team (CERT-In), these guidelines relate to information security practices, procedures, prevention, and response and apply to all Ministries, Departments, Secretariats, and Offices listed in the First Schedule of the Government of India (Allocation of Business) Rules, 1961, along with their attached and subordinate offices, as well as all government institutions, public sector enterprises, and other government agencies under their administrative oversight.

Discover essential guidelines on information security practices tailored for government entities here[16]: https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

6.5 National Information Security Policy and Guidelines (NISPG), MHA

MHA (Ministry of Home Affairs) has been given the task of coordinating and managing public and private sector information security activities. It developed a National Information Security Policy and Guidelines (NISPG)[17] in 2013, which established information handling processes and provided security guidelines for classified information assets. This policy proposed that each government organization shall establish a security division responsible for planning, implementing, and overseeing all activities related to information security. The Information security wing of the Cyber and Information Security divisionof MHA will be responsible for risk analysis- based on threat and risk assessments emerging from technology adoption.

[16] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[17] https://surveyofindia.gov.in/pages/national-information-security-policy-and-guidelines

There are nine critical domains for implementing a sound information security program. These nine domains work together to establish a foundation for a strong information security program. These domains are:

1. **Personal Cyber-security:** Personal cyber-security refers to ongoing efforts to secure individual users' accounts and devices against cyber-attacks. This is done by inculcating basic Do's and Don'ts of Digital Hygiene.
2. **Physical Security:** It is defined as the protection of persons, hardware, software, networks, and data from physical events that might cause catastrophic losses to an organization, including fire, natural catastrophes, theft, damage, or terrorism. Access control, Surveillance, and Testing are the three basic components of the physical security architecture.
3. **Identity and Access Management (IAM):** It identifies and authorizes users across the organization.

   Privileged Access Management (PAM): PAM serves as a subset of IAM and focuses on privileged users who need permission to access more sensitive data.

   For instance, PAM maintains privileged account credentials (such as passwords) in a special-purpose, highly secure password vault.
4. **Network Security:** Network security can be referred to as the measures adopted by an organization to safeguard its computer network and data by utilising appropriate technologies and tools such as Firewall, Network Segmentation, Remote Access VPN,E-mail Security, Sandboxing and so on.
5. **Application Security:** This refers to the security measures used at the application level to protect data or code inside the app from being stolen or hijacked throughout application development and design and after deployment.
6. **Data Security:** It protects digital information against corruption, theft, or illegal access over its entire life cycle. It includes hardware, software, storage devices, user devices, access and administrative controls, and organisational rules and procedures.
7. **Information Security (InfoSec):** It aims to protect and transit data sent across thenetwork via terminals. It is concerned with the confidentiality, integrity, and availability (CIA) of information assets of an organization. Examples of Information Security include Procedural Controls, Access Controls, Technical Controls, Compliance Controls, etc.
8. **Threat and Vulnerability Management:** The technique of finding, categorising, remediating, and managing flaws in an IT environment is known as threat and vulnerability management. It covers vulnerability detection, reporting, prioritisation, and response inthe network. With these insights, one can address security gaps before they cause a breach.
9. **Security Incident Management:** The process of recognizing, monitoring, documenting, and evaluating security risks or occurrences in real-time is known as security incident management. An active threat, an attempted incursion, policybreaches, and a data leak are all examples of security incidents.

Chapter 7: Strengthening Students, Teachers, and Institutions

7.1 Career in Cyber Security

As technology progresses and becomes more and more interconnected, our world becomes more prone to cybercrime. This can be seen in the massive rise in online criminal behavior around the country and in the world. Thus, there is an immediate need for professionals in Cybersecurity and Digital Forensics. Some of the job profiles that are important to protect the present digital spacesare:

1. **Intelligence Analysts:** They work in the field, interrogate witnesses, perform research,conduct searches, and also coordinate with law enforcement/intelligence organizationsto identify and mitigate security concerns.
2. **Cyber Forensic Experts:** They collect and analyse potential evidence, such as deleted, encrypted, or corrupted data, during an investigation.
3. **Cybercrime Investigators:** They collect evidence from digital systems that can be utilised in the prosecution of internet-based or cyberspace illegal activities.

   While a computer forensics investigator possesses and employs many of the same abilities, a cybercrime investigator is primarily focused on and competent at investigating crimes that use the internet as the major attack vector.
4. **Cyber-security Instructors:** They are responsible for devising and implementing effective teaching/training tactics to educate learners/employees on cyber-security skills.
5. **Technology Analysts:** They communicate with the stakeholders to understand their technical needs and design efficient technology systems to meet these needs. They arealso responsible for the smooth and consistent functioning of information technology systems.
6. **Risk and Compliance Managers/Analysts:** They are in charge of liaising with relevant regulatory agencies to ensure adherence to risk and compliance reportingrequirements, as well as plan and execute the internal audit programmes for compliance obligations. Usually, a risk and compliance analyst supports the manager in discharging these activities.
7. **Application Security Professionals:** They advise and validate the secure design and development of IT applications, including updates to existing ones. They also identifysystem and application vulnerabilities and information security threats.
8. **Cyber-security Researchers:** They specialise in the design, development, integration, and deployment of cutting-edge tools, techniques, and systems to safeguard cyberoperations.
9. **Red Team Professionals:** The colors red, blue, and purple represent diverse cyber security tactics as well as highly experienced teams. These teams are in charge of defending the organization's assets from unknown attacks.

   Red team raises the heat and shows businesses where their assets might be compromised. This could be done by simulating an assault in controlled, natural surroundings - analogous to doing regular fire drills. It then relays results back to the firm so thatfirms may reinforce their cyber security and seek to invest in their defensive system through offensive measures. The red team is, therefore, responsible for identifying weak areas in a company's security and delivering a report of flaws.

The blue team is composed of security experts who possess an in-depth understanding of the organization. Their primary responsibility is safeguarding the organization's vital assets from various threats. The blue team begins by collecting data, identifying what requires protection, and conducting a risk assessment to achieve this.

On the other hand, the purple team represents a collaborative security approach where the red and blue teams work together closely. This teamwork enhances cyber capabilities by fostering continuous feedback and facilitating team knowledge transfer.The purple team can help security teams improve the effectiveness of vulnerabilitydetection, threat hunting, and network monitoring by accurately simulating common threat scenarios and facilitating the creation of new techniques designed to preventand detect new types of threats.

Apart from the job profiles discussed above, there are various other career development options in the field of cybersecurity. Cybersecurity is an ever-evolving vast domain with various key areas interconnected in one way or the other. Some of these key areas have been identified as governance, risk assessment, career development, security operation, security architecture, threat intelligence, and many more (Fig. 7.1).

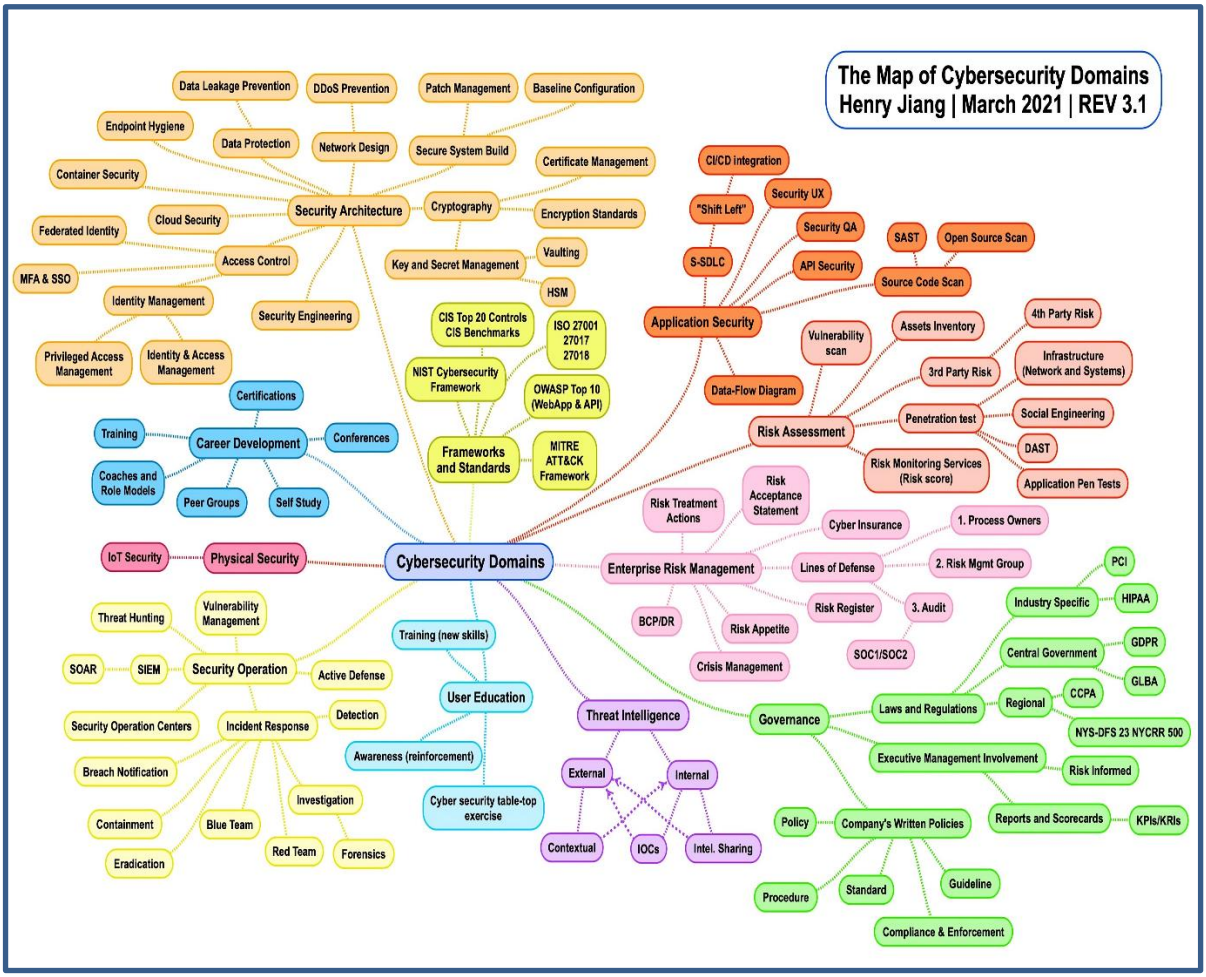


Fig. 7.1 Mapping of Cybersecurity Domains (Source: Henry Jiang on LinkedIn)

7.2 Certifications and Other

The CCISO certificate is the highest achievement offered to chief information security officers (CISOs). OSCP (Offensive Security Certified Professional), SANS Technology Institute, ISFCE

(International Society of Forensic Computer Examiners), IACIS (The International Association of Computer Investigative Specialists), GIAC (Global Information Assurance Certification), CISSP (Certified Information Systems Security Professional), and (ISC)2 (International Information Systems Security Certification) are among the organization unauthorized that provide related professional training and certifications.

Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI) CompTIA Security+, Cisco Certified Network Associate (CCNA), CompTIA Network+, Certified Network Defender (CND), Certified Penetration Testing Engineer (CPTE), Certified Forensic Examiner (CFE), Certified Cyber Forensics Professional (CCFP), EnCase Certified Examiner (EnCE), Certified Incident Handler (GCIH), Certified Cyber Investigator (CCI).

7.3 Massive Open Online Courses (MOOCs)

National Cybercrime Training Centre (CyTrain) aims to build the capacities of individuals through the provision of certain MOOCs focused on combating cybercrimes, impact containment, and investigations. This is a virtual training Centre by the National Crime Records Bureau (NCRB). The intended trainees are officers of all ranks, including senior officers from States/Union Territories as well as from Central Police Organizations/Central Armed Police Forces. Some of these MOOCs are listed below (can be accessed through this link https://cytrain.ncrb.gov.in/course/):

7.3.1 Common Cyber Crime Course

7.3.2 Cybercrime Awareness for Police Officers

7.3.3 Cybercrime Investigation: Case Studies

7.3.4 Cybercrime Investigation: Hands-on Approach

7.3.5 Judiciary/Prosecution Track

7.3.6 Investigation Track

7.4 Strengthening Teachers and IT Teams of Higher Education Institutions (HEIs)

Let us now understand clearly the changing roles and responsibilities of educators in the present context when digital tools and Edu-tech are becoming a norm. Since the technical components of conducting a virtual class are far more complex than conducting a session offline, the educator has to take on the role of a tech specialist, facilitator, and content designer. Fordoing so, some of the tips are:

- **Aa a Tech-Designer:** Be Aware of Basics of Digital Hygiene - The educator must always be on guard against various cyber threats that can occur during onlineclasses, such as violation of the classroom by unauthorized entrants or invasion of the privacy of students or educators, etc.
- **As a Facilitator:** Use Mixed-Media and Varied Communication Techniques -The learning pace for students could vary; there could be fast learners, and there couldbe slow learners in an online class. To ensure proper learning by all levels of students,the educator must rely on different assessment formats in her online classroom.

  For instance, there could be a combination of strategies such as insistence on personal video introductions, parallel quizzing and queries in chat rooms, expectations of prompt responses to inquiries, short online quizzing in between the sessions, and unexpected/random requeststo the students to switch on videos. All these techniques would ensure proper uptake of learning in digital mode and isolate the possibility of unexpected intrusions of rogue actors in the digital classrooms.

- **As a Content Designer:** Select Digital Tools Appropriately - The educator must be capable of selecting digital tools that are:
  a. appropriate for the respective learning objective
  b. could also be easily accessed and understood by students
  c. could help assess the knowledge and skills of students. To do so, educators must be well-exposed to the use of AI/data analytics to properly evaluate the learning pace of their students.

Such threats could be avoided/minimized if an online educator takes the following basic principles of digital hygiene (apart from generic Do's and Don'ts that have already been discussed in this handbook):

Table 7.1 Safety Tips to be Followed by Educators for Conducting Online Classes (Do's and Don'ts)

Safety Tips to be Followed by Educators for Conducting Online Classes
Do's
Do establish certain norms for online classes. For instance, educators must insist on the use of web cameras in online classes, employ follow-up emails, and conduct extensive discussion forums and chat rooms, apart from conducting online classes.
Do circulate the list of protocols of Do's (For instance, 'Do switch on your camera, when requested') and Don'ts (For instance, 'Don't take screenshots'; 'Don't use undesirable words', etc.) that must be followed by each and every student while attending the online class.
Ensure the provision of a 'waiting room' while creating links for online classes.
Create a unique classroom URL and secure its access with a strong password.
Do insist that the students must not reveal their personal information to anyone until it has been completely verified that everyone who is in the online class has permission to be there.
Don'ts
Do not send classroom invites to unregistered email IDs/ phone numbers of students. Right at the outset, of course, these student details must be taken up and verified by the educator.
Do not publish the classroom details, including names of the speakers, students, or related URLs or passwords, on any public forum such as WhatsApp groups. Instead, this information could be shared in closed email groups.
Do not let the students inside the online classroom without verifying their email IDs.

Considering the present scenario, online classes are an inevitable means to deliver knowledge, which demands a great deal of time on the Internet. Thus, it is of utmost importance to make the students and educators aware of the possible scammers performing phishing activities and creating fake websites. Another noteworthy aspect is that an individual's privacy should not be compromised at any cost and financial information should not be easily accessible.

As already discussed in the first chapter, with the prevailing trend in Edu-Tech, the technical componentsof conducting a virtual class are far more complex than conducting a session offline.

7.5 Some of the R&D, Capacity Building and Awareness Initiatives by the Government of India

MeitY, MHA and DST (Department of Science and Technology) undertake several R&D and related academic initiatives in the cyber-security domain, as listed herewith:

7.5.1 Information Security Education and Awareness (ISEA) under MeitY

In 2014, MeitY approved a program named "Information Security Education and Awareness (ISEA) Phase II," which aims to build capacity in the area of information security by creating the right kind of qualified human resources to meet the ever-evolving challenges in this area through learning (formal and non-formal courses), training of government officials, and public awareness campaigns.

The Information Security Education and Awareness (ISEA) Project by MeitY is aimed at capacity building in the area of information security for the development of human resources in this area. The project is implemented through a network of 52 institutions, comprising premier academic institutions such as IITs, NITs, Govt. Engineering Colleges, select C-DAC & NIELIT centres and Technical Universities. The ISEA initiative focuses on promoting education (formal and non-formal courses), training government personnel, students, faculty, and school teachers; and educating the general public at large about cyber hygiene and cyber security through awareness workshops, outreach activities, multilingual awareness material in the form of handbooks, posters, short-videos, etc. disseminated through print, electronic and social media and through ISEA awareness portal www.infosecawareness.in. More details about the ISEA program are available on https://www.isea.gov.in/

7.5.2 Centre for Development of Advanced Computing (C-DAC) under MeitY

The Ministry of Electronics and Information Technology's (MeitY) Centre for Development of Advanced Computing (C-DAC) is the ministry's primary research and development Centre for IT, electronics, and related fields. C-DAC has been conducting research and development in many sub-areas within the Cyber Security sector.

7.5.3 Cyber Surakshit Bharat Programme by MeitY

Cyber Surakshit Bharat program is an initiative of the Ministry of Electronics and Information Technology (MeitY) with the National e-Governance Division (NeGD) as the implementing agency to strengthen the Indian cyber security ecosystem. The purpose of the program is to spread awareness, build capacity, and enable government departments to take steps that need to be taken to create a resilient IT setup.

The "Cyber Surakshit Bharat" (CSB) program was initiated in partnership with an industry consortium in Public-Private Partnership (PPP) with the objective of educating & enabling the Chief Information Security Officers (CISOs) & broader IT community of Central/State Government banks and PSUs to address the challenges of cyber security. The technical contents of the training were developed after intense discussion with industry consortium and knowledge partners.

Fig 7.2: Logo of Cyber Surakshit Bharat

7.5.4 CyberDost by MHA

Various social media handles titled "CyberDost" have been created, to spread cybercrime awareness amongst the masses. @CyberDost aims to educate people by regularly creating videos/GIFs that give cyberc rime and cyber safety tips. This handle is designed to enhance people's basic understanding of cyberc rimes and the precautions that should betaken to prevent them.

7.5.5 Cyber Volunteers program by MHA

The Cyber Crime Volunteers Programme, devised by I4C, seeks to bring together individuals who are ardent supporters of national service under one umbrella initiative. The primary objective of this endeavor is to involve citizens in the collaborative struggle against cybercrime on a national scale.

Those who possess good intentions are urged to participate in the Cyber Crime Volunteer Program by designating themselves as flaggers of illicit content. This position is responsible for assisting law enforcement agencies in identifying, reporting, and removing illicit or unlawful online content.
Additionally, volunteers interested in other activities supporting the fight against cybercrime are cordially invited to apply. Submissions of applications for participation should be addressed to the State Nodal, who will maintain communication with the applicants as required.
The Cyber Crime Volunteer Program offers individuals a valuable opportunity to contribute to combating online criminal activities. Volunteers can play a crucial role in creating a safer digital environment for all users by joining this initiative.

7.5.6 Cyber Commandos program by I4C, MHA

Indian Cyber Crime Coordination Centre (I4C) is taking significant strides in bolstering India's cyber defense capabilities through the establishment of Cyber Commandos. The concept of Cyber Commandos was first introduced during the DGPs/IGPs Conference held in the month of January 2023, The Hon'ble Prime Minister recommended that a Special Wing of suitably

trained 'Cyber Commandos' should be established to counter threats of cyber security from the cyberspace. Hon'ble Prime Minister reiterated in the DGP/IGP conference held in January 2024 that the cyber commando force should be created without any delay. These commandos will undergo rigorous residential training, equipping them with the skills to respond to cyber threats effectively. The training will be conducted in collaboration with top institutions. Cyber Commandos are conceived to a part of a National Level Force who will be stationed in States/UTs/Headquarters and work for their parent organization. They are expected to be assigned roles according to the expertise they have developed during training in Digital forensics, Incident Response, and Securing ICT Infrastructure.

Significance of Cyber Commandos:

By creating a specialized force, India aims to enhance its ability to combat cybercrime significantly.
Cyber Commandos will respond to threats and proactively identify and mitigate potential vulnerabilities.
The initiative will foster a pool of highly skilled cybersecurity professionals.

7.5.7 Some Other Related Initiatives by the Department of Science and Technology(DST)

The Department of Science and Technology (DST) under the Ministry of Science and Technology is also doing research in the cyber security domain. DSTs attempt to define a national R&D agenda that is required to enable the country to get ahead of adversaries and produce the technologies. Broad research areas include information security, digital services, and the protection of digital services.The details are available at http://dst.gov.in/basic-research-cyber-security.

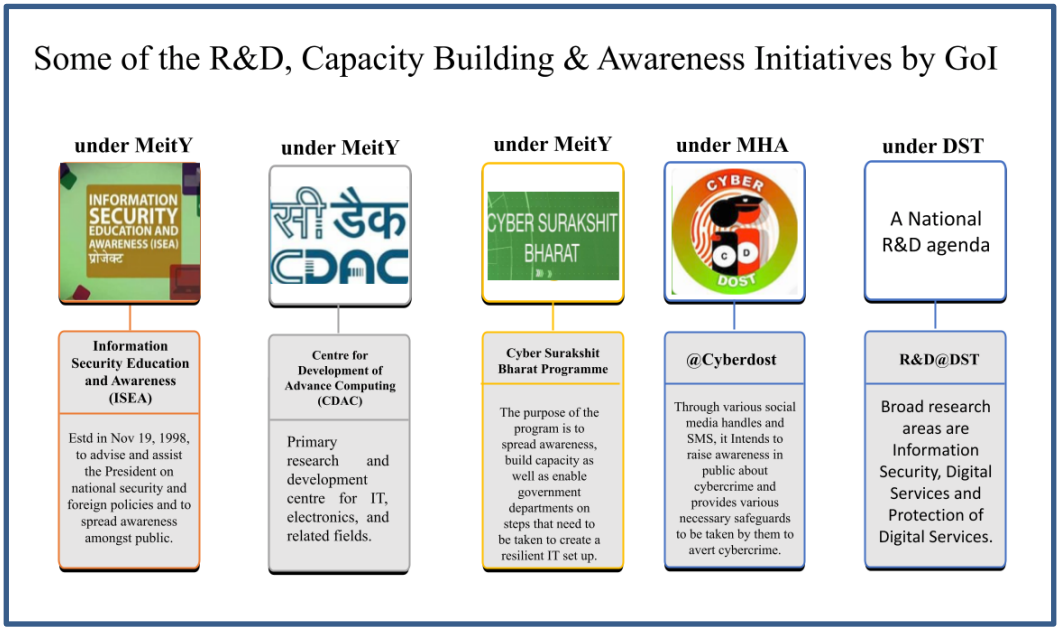


Fig.7.2 Some of the Capacity Building & Awareness Initiatives by GoI (Source: IIPA)

Extract CSB Logo from https://www.meity.gov.in/writereaddata/files/Cyber%20Surakshit%20Brochure_.pdf

7.5.8 National and State Level Initiatives under MHA's Scheme of 'Cybercrime Prevention against Women and Children (CPWC)'

From 2018 onwards, under the CPWC scheme of MHA, several initiatives have been undertaken to strengthen the cyber posture of the masses, particularly women and children. Some

of the related national and state-level advents under CPWC are summarized herewith:

7.5.8.1 The National Commission for Protection of Child Rights (NCPCR) has developed a special toolkit for cybercrimes against children.

7.5.8.2 States/UTs have been given substantial grants to set up Cyber Forensic Training Labs and hire Cyber Forensic Consultants to run the labs in their respective states.

7.5.8.3 States/UTs have also been given funding to train police officers, prosecutors, and judicial officers under the CPWC scheme.

7.5.8.4 Funds have also been earmarked to facilitate cybercrime awareness and R&D by establishing a Centre of Excellence (CoE) on research and development activities related to cybercrime prevention and control.

7.5.8.5 Several courses have been designed for law enforcement agencies on 'Cybercrime Investigation,' particularly for North Eastern states.

7.6 Cyber Crisis Management Plan (CCMP) for Organisations

For combating cyber-attacks at the organizational level, the Government of India has developed an almost exhaustive template of a Cyber Crisis Management Plan (CCMP), which could be implemented by all Central Government Ministries/Departments, State Governments, and their entities, and critical sectors. A Cyber Crisis Management Plan (CCMP) is a plan that provides a strategic framework & guides actions to prepare for, respond to, and coordinate recovery from a cyber crisis. Each organization has to develop one CCMP plan, as it helps the organization to put in place mechanisms to effectively deal with cyber security crises and be able to pinpoint responsibilities and accountabilities right down to the individual level.

7.7 Suggested Cyber Policy Guidelines for HEIs

Policies that clearly define what should be done and what should not be done while executing specific tasks can help minimize the risk of cyber threats. Various federal rules require HEIs to guarantee the privacy, security, and confidentiality of personally identifiable information (PII) and/ or information security. These federal rules could be summarised as the following:

7.7.1 The Family Educational Rights and Privacy Act (FERPA) prohibits educational institutions from revealing student PII or education information without written consent.

7.7.2 The Federal Information Security Modernization Act of 2014 (FISMA 2014) mandates federal data security.

7.7.3 The Gramm-Leach-Bliley Act (GLBA) requires financial institutions, including colleges and universities, to protect customer personal information (PII).

7.7.4 The Higher Education Act (HEA) requires HEIs with Title IV programs to have information security policies, controls, monitoring, and management procedures.

7.7.5 Enrolment Agreement with the Student Aid Internet Gateway (SAIG) requires HEIs with Title IV programs to preserve all Federal Student Aid applicant information.

When developing cybersecurity plans, policies, and procedures, HEIs must keep these federal regulations in mind, as well as state and local laws related to managing information security in the academic setting.

7.8 How to Stay Cyber-Safe: Recommended Resources

In today's digitally interconnected world, the threat of cyber-attacks looms large, posing significant risks to individuals and organizations alike. To mitigate these risks and empower people with the knowledge and tools to safeguard themselves against cyber threats, we have compiled a curated selection of awareness booklets. These booklets serve as comprehensive guides, covering common cyber-attacks and best practices that users can implement to enhance their cybersecurity posture. By familiarising yourself with these resources and adopting the recommended measures, you can actively fortify your collective defences against cyber threats.

- Cyber security Awareness Booklet for Digital Nagriks and Digital Enterprises https://www.cert-in.org.in/PDF/CSA_Booklet.pdf
- Internet Safety Awareness Booklet for Digital Nagriks and Digital Enterprises https://www.cert-in.org.in/PDF/ISA_Booklet.pdf
- https://www.cybercrime.gov.in/UploadMedia/CyberSafetyEng.pdf
- https://www.cybercrime.gov.in/UploadMedia/TSWSW-HandbookforTacklingCyberCrimes.pdf
- https://www.cybercrime.gov.in/pdf/Final_English_Manual_Basic.pdf
- https://www.cybercrime.gov.in/pdf/Safe%20Use%20of%20social%20Media%20Platform%20Brochure%20final.pdf
- https://rbi.org.in/commonman/Upload/english/Content/PDFs/English%20BEAWARE.pdf

The Final Remark

We hope that this handbook has been helpful to its readers. It intends to contribute to the basic understanding of digital hygiene concepts to various HEI stakeholders. However, the readers would appreciate that this domain is always in flux. Therefore, it is also an individual’s responsibilityto keep scanning this ever-evolving ecosystem and keep refurbishing their knowledge and skills tostay cybersafe. The handbook strives to merely initiate this journey for its readers.

REFERENCES

1. https://blog.online.colostate.edu/blog/online-teaching/redefining-teaching-the-five-roles- of-the-online-instructor/
2. https://www.dqindia.com/big-leap-blackboard-smartboard/
3. https://blog.sanako.com/virtual-classroom-security-threats-and-how-to-address-them
4. https://panoply.io/analytics-stack-guide/data-profiling-best-practices/
5. https://www.kaspersky.com/resource-center/threats/deep-web
6. https://www.tylercybersecurity.com/blog/cyberattacks-101-man-in-the-middle
7. https://guides.lib.uw.edu/c.php?g=345925&p=7772376
8. https://www.cyber crimechambers.com/
9. https://www.geeksforgeeks.org/what-is-information-security/
10. http://rmias.cardiff.ac.uk/
11. https://cyber crime.gov.in/
12. https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html
13. http://www.cybercelldelhi.in/Fakeshoppingsite.html
14. https://gadgets.ndtv.com/how-to/features/online-payment-frauds-upi-apps-e-wallets-how- to-avoid-steps-guide-2384538
15. https://www.hdfcbank.com/personal/useful-links/security/beware-of-fraud/sim-swap
16. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/credit-card-fraud
17. https://www.financialexpress.com/money/5-strategies-to-safeguard-against-demat- account-frauds/1721683
18. https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/
19. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-2.2.1
20. https://www.kaspersky.com/blog/online-gamer-threats/4474/
21. http://www.cybercelldelhi.in/mobileapprelatedcrimes.html
22. https://www.endnowfoundation.org/detect_matrimony_frauds-php/
23. https://economictimes.indiatimes.com/tech/internet/making-payments-online-follow- these-10-steps-to-keep-your-money-safe/articleshow/60840679.cms
24. https://www.npci.org.in/what-we-do/aeps/product-overview
25. https://www.getastra.com/blog/knowledge-base/ecommerce-security/
26. https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221
27. https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices
28. MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF (defense. gov)
29. https://opensource.com/resources/linux
30. https://www.linux.com/what-is-linux/

31. https://www.javatpoint.com/advantages-of-linux
32. https://www.meity.gov.in/content/icert
33. http://www.isea.gov.in/
34. https://nciipc.gov.in/index.html
35. https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division
36. http://cwprs.gov.in/WriteReadData/file/cyberdost/cyberdost_twitter_mha.pdf
37. https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/ Details-about-CCPWC-Cyber crime Prevention-against-Women-and-Children-Scheme
38. http://www.cybercelldelhi.in/
39. https://www.cdac.in/index.aspx?id=cyber_security
40. https://www.drishtiias.com/daily-updates/daily-news-analysis/new-facility-to-tackle- cyber-crimes
41. https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-cyber crimes
42. https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-2020
43. https://www.myadvo.in/blog/how-to-file-a-cyber-crime-complaint-with-cyber-cell-in- India/
44. https://www.researchtrend.net/ijet/pdf/70-S-806.pdf
45. https://startsmarter.co.uk/the-advantages-and-disadvantages-of-digitalisation/
46. https://www.fortinet.com/resources/cyberglossary/worm-virus
47. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
48. https://study.com/academy/lesson/what-is-a-backdoor-virus-definition-removal-example.html
49. https://www.kaspersky.com/resource-center/definitions/what-is-rootkit
50. https://www.pandasecurity.com/en/mediacenter/mobile-news/funeral-directors/
51. https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/malware-vs-viruses.html
52. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-spoofing/
53. http://www.cybercelldelhi.in/socialmediacrimes.html
54. https://www.asurion.com/connect/tech-tips/what-to-do-when-your-phone-is-lost-or-stolen/
55. http://www.isea.gov.in/
56. https://cytrain.ncrb.gov.in/course/
57. https://www.careers360.com/courses-certifications/articles/top-universities-in-india-offering-cyber-security-courses
58. https://rems.ed.gov/docs/CybersecurityC.pdf
59. http://faridkotpolice.in/guidlines.pdf
60. https://cybersecurityguide.org/careers/chief-information-security-officer/
61. https://ciso.eccouncil.org/cciso-certification/
62. https://www.infosectrain.com/courses/cciso-certification-online-training/
63. https://www.the420.in/step-by-step-guide-how-to-file-cyber crime-complaint-online-in-India/

64. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep- fake-voice- tech-to-steal-millions/?sh=462e58e47559 as accessed on 11-02-2022.
65. https://www.pngitem.com/middle/TiTxxi_thief-robber-png-criminal-clipart-transparent-png/
66. https://www.kaspersky.com/resource-center/definitions/cookies
67. https://www.mooc.org/
68. https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain
69. https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2017-0121. pdf
70. https://www.dailypioneer.com/2020/columnists/now--digital-distancing.html
71. https://cdac.in/index.aspx?id=cs_eps_mkavach
72. https://digitalindia.gov.in/content/mkavach
73. https://tech.hindustan g20.com/how-to/how-to-use-DigiLocker-app-keep-all-documents- on-your-phone-at-all-times-71644991202025.html
74. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
75. https://www.DigiLocker.info/view-certificates-DigiLocker-app-link/
76. https://www.pcmag.com/encyclopedia/term/hardware-key
77. https://www.cert- in.org.in/PDF/CSA_Booklet.pdf
78. https://www.cert- in.org.in/PDF/ISA_Booklet.pdf

Glossary of Terms

Artificial Intelligence: Artificial Intelligence (AI) is the ability of a computer or a robot controlled by a computer to do tasks that are usually done by humans because they require human intelligence and discernment.

Backup: In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after an event of data loss.

Bandwidth: In computing, bandwidth is the maximum rate of data transfer across a given path.

Big Data: Big Data refers to extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

Biometrics: In information technology, biometrics usually refers to automated technologies for authenticating and verifying human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements (NIST, 2015).

Bots: A bot is a computer program that performs automatic, repetitive, and pre-defined activities. Bots are designed to mimic or replace human behavior.

Browsing history: Browsing history refers to the list of web pages where a user has visited, as well as associated with metadata such as page title and time of visit.

CIA Triad: Information security programs are built around three principles, referred to as the CIA Triad - Confidentiality, Integrity, and Availability, where:

1. Confidentiality entails not disclosing information to unauthorized individuals,entities, or processes;
2. Integrity involves ensuring the accuracy and completeness of data; and
3. Availability indicates the availability of information when it is required.

Cognizable offences: It means those offences where a police officer could arrest without warrant. Cognizable offences are usually serious in nature.

Content Delivery Network: A Content Delivery Network (CDN) is a geographically distributed network of servers and their data centres that help in content distribution to users with minimal delay.

Copy Protection Device: A copy protection device makes use of technological tools to prevent the users from copying data from secured digital devices.

Crack-software: The password, product key, license key illegally used for unauthorized usage are known as crack of the software. A software where certain features have been disabled such as copy-protection features, adware, etc., to pirate it (RBI).

Cryptocurrency: A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. For example, bitcoin, Litecoin, Ethereum, etc.

Cryptography: Cryptography is the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use or prevent their undetected modification (NIST, 2015)

Cyberbullying: Cyberbullying is bullying through digital technology where unpleasant, damaging, and wrong content about someone else can be sent, posted, or shared.

Cyber Espionage: Cyber espionage is an act of intrusion that can give the desired information.

Cyberspace: According to the National Institute of Standards and Technology (NIST, 2015), cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberstalking: Cyberstalking is a crime when a victim is harassed by the attacker utilizing e-mail, Instant Messaging (IM), internet messages, discussion groups, etc., to communicate electronically with the victim.

Cyberwar: Cyberwar refers to the actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption (Clarke and Knake, 2010).

Data accessibility: Data access refers to a user's ability to access or retrieve data stored within a database or other repository.

Data Breach: A data breach occurs when malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information, or personally identifiable information.

Data profiling: Data profiling is the process of reviewing source data, understanding structure, content, interrelationships, and identifying potential for data projects.

Data Diddling: Data diddling is a type of cybercrime in which data is altered as it is entered intoa computer system, most often by a data entry clerk or a computer virus.

Decryption: The conversion of encrypted data into its original form is called Decryption.

Deepfakes: Deepfakes is a new and complex type of audio, video, or image disinformation that is typically used for malicious purposes. They can quickly spread fraudulent words and actions to a global audience, and they can be difficult to tell apart from genuine information.

Demat Account: Demat Account is short for dematerialization account and makes the process of holding investments like shares, bonds, government securities, mutual funds, and insurance easier, eliminating the hassles of physical handling and maintenance of paper shares and related documents.

Denial of Service (DOS): Denial of service (DoS) is a type of cyberattack designed to disable, shut down or disrupt a network, website, or service. Typically, malware is used to interrupt or inhibit the normal flow of data into and out of a system to render the target useless or inaccessible for a certain period.

De-parameterization: De-parameterization is protecting an organization's systems and data on multiple levels by using a mixture of encryption, secure computer protocols, secure computer

systems, and data-level authentication, rather than the reliance of an organization on its network boundary to the Internet.

Digital currency: Digital currency is a form of currency that is available only in digital or electronic form. It is also called digital money, electronic money, or electronic currency.

Digitalization: Digitalization is the use of emerging technologies/ new age technologies (NATs) such as Artificial Intelligence, Machine Learning, the Internet of Things, etc. to modify a business model and generate new revenue and value-producing opportunities.

Distributed Denial-of-Service (DDoS): It is a type of cybercrime when an intruder strikes a server with internet traffic to restrict people from accessing linked websites and online services.

Distributed network: A distributed network is a type of computer network that is spread over different networks. This provides a single data communication network, which can be managed jointly or separately by each network

Domain name: A domain name is an easy-to-remember name that's associated with a physical IP address on the Internet. For instance, the domain name google.com might translate to the physical address *198.102.434.8*.

E-commerce: The term electronic commerce (e-commerce) refers to a business model that allows companies and individuals to buy and sell goods and services over the Internet.

Encryption: Encryption is the process of encoding a document or data so that only individuals with access to a secret key, password, or token can open and decrypt (make readable) the information.

Extranet: An extranet is a controlled private network that allows access to partners, vendors, and suppliers or an authorized set of customers, normally to a subset of the information accessible from an organization's intranet.

Financial Frauds: Financial frauds occur when someone steals one's money or else harms one's financial health by deceitful, dishonest, or unlawful tactics. This can be accomplished through a variety of means, including identity theft and investment frauds.

Firewall: A firewall is an inter-network gateway that restricts data communication traffic to and from one of the connected networks and thus protects that network's system resources against threats from the other network (NIST, 2015).

Hacker: Unauthorized user who attempts to or gains access to an information system.

Hacking: Hacking is the activity of using a computer to access information stored on another computer system without permission, or to spread a computer virus (Cambridge Dictionary).

Hoax email: An email hoax is a scam that is distributed in email form. It is designed to deceive and defraud email recipients, often for monetary gain. Hoaxes are emails typically arriving in chain letter fashion that often describe impossible events, highly damaging malware.

Identity/Credential Theft: Identity theft is the obtaining of some other person's personal information without their permission. Personal information may contain a person's name, phone number, address, bank account number, Aadhaar number, credit/debit card number, passwords among other things.

Impersonation: Impersonation is used as a technique where basic credentials are stolen. The threat actor or bad actor pretends to be someone else by adopting that person's identity to get access to resources, credit, or other benefits in that person's name and fame.

Information Assets: An information asset is a collection of data that is defined and managed as

a single unit, allowing it to be easily understood, shared, safeguarded, and exploited. A contact database is an excellent example of a single information asset.

Information security: Information security refers to the safeguarding of data and information systems against unauthorised access, use, disclosure, intrusion, manipulation and destruction to maintain confidentiality, integrity, and availability. Cybersecurity is a specific type of information security that refers to the ways in which organizations protect digital information, such as networks, programs, devices, servers, and other digital assets.

Inspection: Inspection refers to the examination of an information system to determine compliance with security policy, procedures, and practices (NIST, 2015).

Intranet: An intranet is a computer network for sharing information, easier communication, collaboration tools, operational systems, and other computing services within an organisation, usually to the exclusion of access by outsiders.

Intrusion: Intrusion involves stealing valuable resources and jeopardising the security of systems, networks, devices, or data, as the case may be.

IoT Attacks: IOT attacks include any cyberattacks that seek to gain access to (or control over) IOT devices with the intent to either cause harm to the devices or use them in attacks against other targets.

Keylogger: Keyloggers are activity-monitoring software programs that give hackers access to the user's personal data such as passwords, credit card numbers, or the web pages they visit, by logging the keyboard strokes.

Law Enforcement Agency (LEA): A law enforcement agency (LEA) is any government agency responsible for the enforcement of the laws.

Law Enforcement Cyber Centre (LECC): These centres are designed to assist the police, patrol officers, digital forensic investigators, prosecutors, and detectives who are investigating and preventing crimes that involve technology.

Logic Bombs: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Machine Learning: Machine learning is a subset of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.

Man-in-the-Middle: Man-in-the-Middle (MitM) attacks happen when an intruder intercepts on interactions between two parties. These attacks give intruders the chance to intrude and overhear on the communication or data transfer between the two targets and to alter the traffic that is flowing between them.

Margin funds: Margin funds refer to a short-term loan facility that investors use to make up for any shortcomings that they encounter, while trading or when purchasing stocks, at a predeterminedrate of interest.

Misinformation/Disinformation: Misinformation is simply false information that is disseminated, whether or not the purpose is to deceive, whereas disinformation is intentionally misleading or biased information that is based on distorted narratives or facts to achieve propaganda.

Massive Open Online Courses (MOOCs): MOOCs are free online courses available for anyone to enroll. Due to the recent pandemic, MOOCs have become quite common among learners, as they are quite affordable and flexible in nature. They are an easy way to acquire new skills, advance career opportunities and deliver quality educational experiences at large.

Morphing: Morphing is the process of smoothly transitioning from one image to another without any changes using online morphing tools.

Multi-Factor Authentication (MFA): An authentication system that requires more than one distinct authentication factor for successful authentication (NIST, 2015).

National Nodal Agency: National Nodal Agency has been set up for all measures to protect the nation's critical information infrastructure.

NATGRID: The National Intelligence Grid (NATGRID) is an integrated intelligence master database structure under the Ministry of Home Affairs, Government of India. It was created with the purpose of counter-terrorism and connects the databases of various core security agencies around the country and can be accessed by these agencies around the clock.

Nodes: A node is a basic unit of a data structure, such as a linked list or tree data structure. Nodes contain data and also may link to other nodes.

Open-source Intelligence (OSINT): Open-source intelligence is the collection and analysis of data gathered from open sources to produce actionable intelligence such as social media profiles, etc.

Outsourcing: Outsourcing is a business practice in which a company hires a third party to perform tasks, handle operations or provide services for the company.

Phishing: A phishing attack is a means of tricking people into disclosing confidential information by answering an email. It involves obtaining or attempting to gain specific banking information (e.g. username, password, credit card numbers, etc.).

Pig butchering: Pig butchering is a crypto cybercrime where fraudsters use romance on dating apps and social media platforms to lure people in cryptocurrency and gold investments.

Remote access control: Remote access control refers to the ability to monitor and control access to a computer or network (such as a home computer or office network computer) anywhere and anytime.

Rootkits: A rootkit is a kind of software that allows hackers to gain access to and command over a computer.

Server: A server is a computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

Skimming: Skimming is an illegal practice used by identity thieves to capture credit card information from a cardholder surreptitiously. Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.

Social Engineering: Social engineering assaults usually include psychological manipulation to persuade unaware users. It involves sending an email or other message to a target that elicits feelings of urgency, fear, or other comparable emotions, prompting the victim to reveal sensitive information, click a harmful link, or open a malicious file.

Spam: Spam is any kind of unwanted, unsolicited digital message that is sent out in bulk. Usually, spam is sent through email, but it can also be sent through text messages, phone calls, or social media.

Spoofing: Spoofing occurs when cyber threat actors try to hide their true identities by faking the sender of a message to regularly fool the recipient into thinking it came from someone else.

Spyware: Spyware is defined as malicious software designed to enter a computer device, gather data about the person, and forward it to a third party without consent.

SSL Certificates: An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.

Supply-chain attack: A supply chain attack is an attack that allows the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products), or services at any point during the life cycle (NIST, 2015).

Trojan: A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet can take control of the computer.

Unauthorized access: Unauthorized access refers to the unauthorized attempts to bypass the security mechanisms of a computer/information system or network.

Worm: A worm virus is a harmful program that duplicates itself and spreads through a network automatically. The worm virus exploits flaws in the security software to steal important information, install backdoors that can be exploited to access the system, corrupt files, and perform other types of harm.

Zero-FIR: Zero-FIR implies rights of the citizens to file a complaint at any police station, which means even if the incident of crime has taken place outside the jurisdiction of the police station, it is bound to register a Zero FIR.

Abbreviations Used

ABBREVIATIONS USED	FULL FORMS
ACH	Automated Clearing House
AePS	Aadhaar Enabled Payment System
ATM	Automated Teller Machine
CD	Compact Disc
CDSL	Central Depository Services Limited
CISO	Chief Information Security Officer
CPU	Central Processing Unit
CSK	Cyber Swachhta Kendras
CVV	Card Verification Value
CyTrain	National Cybercrime Training Centre
DDoS	Distributed Denial of Service
DEMAT	Dematerialisation account
EFT	Electronic Funds Transfer
ETF	Exchange-Traded Fund
GPS	Global Positioning System
GST	Goods and Services Tax
HEI	Higher Education Institution
HTTPS	Hypertext Transfer Protocol Secure
IMSI	International Mobile Subscriber Identity
IRAs	Individual Retirement Accounts
IT	Information Technology
KYC	Know Your Customer
LEA	Law Enforcement Agency
LECC	Law Enforcement Cyber Centre
MMS	Multimedia Messaging Service
MOOCs	Massive Open Online Courses
NATGRID	National Intelligence Grid
NBFC	Non-Banking Financial Company
NISPG	National Information Security Policy and Guidelines
NIST	National Institute of Standards and Technology
NSDL	National Securities Depositories Limited
OLX	On-Line Exchange
OTP	One-Time Password
PCs	Personal Computers
PDF	Portable Document Format
PII	Personally Identifiable Information
PIN	Personal Identification Number
PoS	Point of Sale
SIM Card	Subscriber Identity Module Card
SMS	Short Message Service
UPI	Unified Payments Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus

Annexure

Summarizing the List of Do's and Don'ts for an Individual to Stay Cybersafe

It is quite evident from this handbook that technological adoption and the rise of internet users in the country over the last decade have resulted in an increase in the number of cybercrimes. Therefore, to prevent a cybercrime or to at least minimize its damages, a compiled list of Do's and Don'ts has been again summarized herewith. All the important precautions to be taken care of have been listed as Do's and important considerations to be avoided are listed as Don'ts. The listing herewith is in no specific order. Hoping the readers find these checklists not just handy but useful too.

A Checklist of Do's to Stay Cyber Safe

Safety Tips to Prevent Malware
Do's
1. Exert all caution in mind before opening email attachments or images, particularly if the sender is unknown/unreliable.
2. Install anti-malware, anti-virus software, and applications only from authorized providers/ sources such as Play Store, App Store, or the company's official website.

Safety Tips to Prevent Shoulder Surfing
Do's
3. Install a privacy filter that allows only the person sitting directly in front of the screen to see the screen.
4. Use a password manager to generate a strong password. It also collects all passwords in one place.
5. Use biometric authentication as much as possible such as - Facial recognition or fingerprint authentication so that the need to input a PIN/password is minimized.

Safety Tips (Misinformation/Disinformation)
Do's
6. Look for spelling mistakes in the sender's address/company's domain/URL and for grammatical mistakes in the main email body. Often popular websites' names could be masqueraded by names that sound or appear similar.
7. Double-check the authenticity of a message before forwarding it to social media platforms.
8. Trust those news items that are from authorized or authenticated sources.

Safety Tips to Prevent Financial Frauds
Do's
9. Use an on-screen keyboard to enter the login credentials in banking portals.
10. Remove the browsing history from the web browser particularly while using public computer devices/cyber-cafes.
11. Check the second-hand digital device for any suspicious pre-installed apps, before buying it.
12. Be aware of all offers that provide high returns in a limited time. They might be fake.

Safety Tips to Prevent Juice Jacking
Do's
13. Prefer to carry a power bank every time.
14. Charge digital devices before carrying them.

Safety Tips to Prevent Social Media Crimes
Do's
15. Keep social media profiles' privacy settings as strict as possible.
16. Exercise extreme caution when sharing any personal information on social media.
17. Always remember to log out of apps and close the browser, after each session.
18. Always put a profile guard on the profile display picture of social media accounts such as WhatsApp, Facebook among others.

Safety Tips to Prevent Morphing
Do's
19. Be cautious of making unknown people as 'Friends'.
20. Do remember that anything shared online will remain in cyberspace and could be misused anytime.

Safety Tips to Prevent Dangerous Game Challenges
Do's
21. Turn off all notifications/pop-ups that lure for usually undesirable game offers.
22. Limit screen time.
23. Install parental control software.

Safety Tips to Prevent Cyber Crimes through Remote Access Applications
Do's
24. Invest money and time in installing secure/safe software, antivirus, firewall, and two-factor authentications to restrict access.

Safety Tips to Prevent Matrimonial and Career Frauds
Do's
25. Validate the social media profiles of the people who are offering marriage proposals/jobs, from other sources too such as Facebook or LinkedIn.

Safety Tips to Create Strong Passwords
Do's
26. Create a strong password with a minimum length of ideally 10 characters and a mix of alphabets, numbers, and characters.
27. Change all the passwords of email, computer, etc. periodically, a minimum of once every month.
28. Treat passwords as sensitive information.
29. Create different passwords for each log-in account. Using the same password for more than one account risks multiple exposures if any website used by the user is hacked.
30. If your work requires you to communicate passwords, such as while sending a password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.
31. Avoid clicking at the prompt of the "Remember Password" feature whenever it is prompted by various browsers/apps.

Safety Tips to Secure e-Commerce Usage
Do's
32. Check that the e-commerce website starts with HTTPS and displays a green pad-lock icon to the left of the website's URL.
33. Shop only on websites that are genuine and trustworthy and have contact details email, phone no. or chat available on it.
34. Create a separate email address for online buying to prevent harmful emails, spam of sales promotions, or misleading offers.
35. Check the seller's reputation and credibility before making online payments.

Safety tips to Secure Digital Devices
Do's
36. Turn on automatic updates in device settings so that apps are updated regularly.
37. Use a lock-screen application, biometric, or a password/PIN particularly for mobile devices as it contains all the personal information, including contacts, financial in-formation, GPS, and so on.
38. Close the webcam and computer audio when not in use.
39. Delete all Wi-Fi networks/Apps from the device that are no longer in use.
40. Switch off the Wi-Fi hotspot whenever it is not required.
41. Make it secure by enabling authentication for Wi-Fi hotspots and also restrict the number of users who can connect to this Wi-Fi hotspot.
42. Turn off location and internet while not in use.
43. Take a backup of the device data regularly.
44. Clear browsing history from time to time to prevent the misuse of personal in-formation and to also help applications run better.

Safety Tips to Secure Internet Browsing
Do's
45. Keep checking the content that is being accessed or downloaded.
46. Download all the software/apps from a reliable and trusted source only.
47. Double-check the sender's identities, before opening any email or clicking a link.

Check if a website is legit or not
Do's
48. Check validity - by reviews, feedback from people, and the traffic on the website
49. Check for the green padlock icon on the left corner beside the URL.
50. Check for spellings in the domain name of the website, common spelling mistakes such as the use of dashes and similar symbols or similar-looking names, and giving away a fake e-commerce website.

General Digital Hygiene Tips
Do's
51. Do adopt a tight "zero-trust" strategy, which involves maintaining strict privacy settings on all devices and apps.
52. Install all-important utilities on your digital devices such as anti-virus software, firewalls, and virtual private network (VPN helps to camouflage real IP addresses).
53. Procure all-important utilities from authorized sources or authorized app stores only.
54. Use well-designed passwords for your accounts; different for each account; or use password managers.
55. Alternatively, use hardware keys.
56. Change all your passwords every month or use a password manager utility.
57. Regularly update all your software.
58. Switch off Internet, Location, and Camera when not in use.
59. Use only those trusted e-commerce websites that are accessible through HTTPS or padlock signs.
60. Do make sure that everything and everyone is verified before any access is granted to any information.

A Checklist of Don'ts to Stay Cyber Safe

Safety Tips to Prevent Malware
Don'ts
1. Don't sign in to personal or professional accounts such as email or banking while using a public Wi-Fi network.

Safety Tips to Prevent Shoulder Surfing
Don'ts
2. Don't leave the computer system unattended in any public space.
3. Don't click links from untrusted sources, they could be malware and be used to steal data while using a public Wi-Fi network.

Safety Tips to Prevent Misinformation/Disinformation
Don'ts
4. Don't take phone calls or reply to messages from unknown sources.

Safety Tips to Prevent Financial Frauds
Don'ts
5. Don't fall for high-profile testimonials - These scammers hire celebrities and social media influencers to promote their fake schemes. These actors try to portray everyday people and spread fake reviews.

Safety Tips to Prevent Juice Jacking
Don'ts
6. Don't leave phones unlocked in public spaces.
7. Don't ignore any prompt messages displayed on the device screen if connected to a public power outlet, read them carefully and understand its implications.

Safety Tips to Prevent Social Media Crimes
Don'ts
8. Don't give out social media login information to anyone.
9. Don't keep common passwords such as name, date of birth, or "1234" and so on.
10. Don't post any personal or sensitive information such as bank details, or passwords on social media sites.

Safety Tips to Prevent Morphing
Don'ts
11. Don't click or share intimate pictures or videos.
12. Don't pursue or engage in relationships that pressurize sharing of personal pictures or videos.
13. Don't suffer in silence, in case of any threats or if the person is victimized by any cybercrime.

Safety Tips to Prevent Dangerous Game Challenges
Don'ts
14. Don't make mobile phones/gaming apps a regular part of routine as it affects eyesight and financial health too.
15. Don't share personal sensitive information on gaming applications.

Safety Tips to Prevent Cyber Crimes through Remote Access Applications
Don'ts
16. Don't give the net-banking password, One-Time Password (OTP), ATM or phone banking PIN, CVV number, or other sensitive information to anyone, even if they pretend to be a bank employee or representative, and notify the bank immediately if this happens.
17. Don't save banking/personal information in a browser or on a payment site while making a purchase.

Safety Tips to Prevent Matrimonial and Career Frauds
Don'ts
18. Don't share personal/financial information with online friends or recruiters.
19. Don't accept job offers or marriage proposals online without validating the person's profile on various sources such as LinkedIn, Facebook, Twitter, etc.

Tips to tighten the passwords
Don'ts
20. Don't store your passwords in readable form on your devices, whiteboard, office notice boards, or in any other location where unauthorized persons might discover or use them. If your work requires you to communicate passwords, such as while sending a password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.

Tips to Secure e-Commerce Usage
Don'ts
21. Do not blindly trust reviews. Sometimes the reviews too are fabricated by the e-commerce vendors themselves.
22. Do not fall for the "cheapest deals", especially if those are offered by relatively unknown vendors/sites. Always remember, there are no "free-lunches" or "amazing deals" or freebies" in the e-commerce world.
23. Do not use or trust the customer care numbers provided on Google with personal information. These are often fake customer care numbers.
24. Do not save personal information, particularly financial details on the e-commerce web portals.

Securing Digital Devices
Don'ts
25. Do not use a USB or other external device, owned by some other person.
26. Do not switch on your GPS/location settings when in public places or in sensitive settings.

Securing Internet Browsing
Don'ts
27. Do not save official data on the cloud or on devices that are continuously connected to the internet.
28. Do not use services that demand location or ask for the upload of photos with GPS coordinates.
29. Do not download free software or apps as they could infect the devices to 'steal' personal information

General Digital Hygiene Tips
Don'ts
30. Do not expose personal details such as DoB, Date of Graduation, Parents' Name on social media, or financial credentials such as PIN/CVV; hide them as much as possible as these details could be easily manipulated for fabricating your identity by fraudsters or could lead to your login credentials.
31. Do not react to spam emails or suspicious friend requests.
32. Do not click on links that are accessible through unverified addresses.
33. Do not install apps that come from unknown sources or are free.
34. Do not fall for "free offers" - if there is no/ less cost of the product then you could become the product.
35. Do not grant unnecessary permissions to contacts/calendar/camera to other apps that do not require it. For E.g. a cab-sharing app does not need to be given access to the camera and so on.
36. Do not click on the "Remember Me" or "Remember Password" options.
37. Do not search for customer care numbers of your banks or utility service providers from your browsers; instead, go to the source website/correspondence flyers to look for the same.
38. Do not undertake financial transactions in free-Wifi/public Wi-Fi zones.

Acknowledgements

UGC acknowledges the contribution of the following Expert Committee in providing their valuable inputs for the "Handbook on Basics of Digital Hygiene for Higher Education Institutions".

1.	Shri Abhishek Singh, IAS Additional Secretary, Ministry of Electronics and Information Technology (MeitY)	Chairman
2.	Shri Sanjay Sahay IPS (Retd.) Former (ADGP) IT, Cyber Security & Emerging Technologies Expert Bengaluru	Member
3.	Prof. (Dr.) N. K. Chaudhary Dean & Professor, School of Cyber Security & Digital Forensics, National Forensic Sciences University (NFSU), Gujarat	Member
4.	Dr. Ananthalakshmi Ammal R Former Senior Director and Group Head, Cyber Security Group, CDAC, Thiruvananthapuram	Member
5.	Prof. Charru Malhotra (PhD, IIT-D) Professor (e-Governance and ICT) at Indian Institute of Public Administration (IIPA), New Delhi	Member
6.	Prof. Atul Pandey Professor-Cyber Law Chairperson Rajiv Gandhi National Cyber Law Centre, NLIU, Bhopal	Special Invitee
7.	Dr. Diksha Rajput Deputy Secretary	UGC

University Grants Commission also appreciates the efforts made by Shri Rajesh Kumar, CEO, Indian Cybercrime Coordination Centre (I4C); Shri Nishant Kumar, Director, I4C; Shri Deepak Virmani, Director (Coordination), I4C; Shri Gaurav Gupta, Additional Director (Scientist E, Cyber Crime Awareness & Digital Forensics), MeitY; Shri. Rajnish Kumar, COO and Director(CB & Finance), NeGD; Shri Vinod Kumar Chouhan, Scientist 'E', Cyber Security Division, MeitY; Shri Abhay Garg, Scientist 'B', Cyber Security Division, MeitY; Shri Gaurav Atrey, Assistant Manager, Digital Indian Corporation, MeitY; Ms. Ishika Bansal, Research Officer, IIPA; Ms. Rachita Garg (Independent Cyber Lawyer) and supported by Shri Hitesh Manik, Section Officer, UGC; Dr. Neelam Kumari, former Consultant, UGC; Dr. Prachi Jain Aggarwal, Young Professional, UGC; and Shri Suresh Chandra, Clerical Assistant, UGC, in bringing out this document.

Prof. Manish R Joshi
Secretary
University Grants Commission

October, 2024

KEYWORDS

D

E

F

G

H

I

J

K

M

O

P

R

S

V

W

Z