CYBER CRIMES – AN INDIAN PERSPECTIVE

Ms.Preeti Jain*

Introduction

Cyber Crime is any crime that involves a computer and a network. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

The different types of Internet crime vary in their design and how easily they are able to be committed. The typical crimes in criminal history are now being brought to a whole different level of innovation and ingenuity. Such new crimes devoted to the Internet are email "phishing", hijacking domain names, virus immistion, and cyber vandalism. A couple of these crimes are activities that have been exposed and introduced into the world. People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers. Other crimes such as email "phishing" are not as known to the public until an individual receives one of these fraudulent emails. These emails are cover faced by the illusion that the email is from your bank or another bank. When a person reads the email he/she is informed of a problem with he/she personal account or another individual wants to send the person some of their money and deposit it directly into their account. The email asks for your personal account information and when a person gives this information away, they are financing the work of a criminal.

* Company Secretary.

Cyber Laws

Since the first computer crime law, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the government has been trying to track down and stop online criminals. The FBI has tried many programs and investigations in order to deter Internet crime, like creating an online crime registry for employers (Metchik 29). The reality is that Internet criminals are rarely caught. One reason is that hackers will use one computer in one country to hack another computer in another country. Another eluding technique used is the changing of the emails, which are involved in virus attacks and "phishing" emails so that a pattern cannot be recognized. An individual can do their best to protect themselves simply by being cautious and careful. Internet users need to watch suspicious emails, use unique passwords, and run anti-virus and anti-spyware software. Do not open any email or run programs from unknown sources.

The Information Technology Act, 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000 / amendment thereof. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Some highlights of the Act are listed below:

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter-III of the Act details about Electronic Governance and

provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference. The said chapter also details the legal recognition of Digital Signatures.

Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter-IX of the said Act talks about penalties and adjudication for various contraventions. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000/- to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred.

Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences

include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Advantages of Cyber Laws

The IT Act, 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records/communications through digital signature.

From the perspective of e-commerce in India, the IT Act, 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital signatures have been given legal validity and sanction in the Act. The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The Act now allows Government to issue notification on the web thus heralding e-governance. The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government. The IT Act also

addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Under The IT Act, 2000, Cyber Crime is a collective term encompassing both 'Cyber Contraventions' and 'Cyber Offences'.

Cyber Contraventions (Chapter IX - Information Technology Act, 2000 / Amendment thereof)

This Chapter entails civil liability and the offender is liable to pay damages by way of compensation.

Unauthorised Access - Section 43 (a)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(a) accesses or secures access to such computer, computer system or computer network."

Illustration:

Priya is the network administrator of her organization. She stores the passwords of her organization's main server in her personal laptop.
Sahil is Priya's friend. Without Priya's permission, he switches on her laptop and notes down the passwords of her organization's main server. He has accessed Priya's laptop without her permission.

Copying Information – Section 43 (b)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer

network including information or data held or stored in any removable storage medium."

Illustration:

Priya has copied the original data from the computer at her workplace into her personal pen drive. She has copied the data.

Computer Contaminant or Virus – Section 43 (c)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network."

Illustrations:

The Melissa virus comes as an attachment to an email and named as "list.doc". When a victim clicks on the attachment, the virus seeks for the Microsoft Outlook address book to e-mail itself to the first 50 names on the list with a message "Here is that document you asked for…don't show anyone else.

Ashish installs a key logger on a cyber café computer. The key logger automatically records all text entered on the infected computer by users. Every evening at 5 pm the key logger transmits this recorded data to Ashish's email account. This is an example of a computer contaminant.

Damaging Computer – Section 43 (d)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network"

Illustrations:

1. Sonakshi deletes the database from the server of the company.

2. Amit picks up Shreya's laptop with the intention of stealing it. He then accidentally drops it on the floor, thereby destroying it. Amit has damaged Shreya's laptop.

Disrupting Computer Network – Section 43 (e)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(e) disrupts or causes disruption of any computer, computer system or computer network"

Illustrations:

An organization has a dozen computers connected to each other through a wireless access point. This access point creates a wireless network within the office. Balbir an employee deliberately switches off the access point. The computers are no longer in a network. Balbir has totally disrupted the organization network.

Denial of Access – Section 43 (f)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means"

Illustrations:

1. Mayank is the network administrator of the Mumbai office of a company. He is annoyed about his low salary and in rage disables the passwords of the other employees so they are unable to access the company servers. Mayank has totally denied access to the authorized employees.
2. Kunal has created a computer virus that opens up multiple program windows on a victim computer. This virus affects Raj's computer & opens up hundreds of program windows on his computer. This results in his computer becoming unusable. Kunal has caused total denial of access.

Facilitating Access – Section 43 (g)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder".

Illustration:

Chetan is planning to gain unauthorised access into the computer systems of HDFC Bank Ltd. Swati, the system administrator of Bank, is his good friend. She disables the Bank firewall at the time when Chetan is launching his attack. Swati has provided assistance to Chetan to facilitate his unlawful access.

Computer Fraud – Section 43 (h)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network."

Illustration:

Rajni regularly uses her computer to log into her online banking account with State Bank of India. Sumit sends Rajni a phished email that appears to come from State Bank of India. The email contains a link to what appears to be a State Bank of India Webpage. Rajni enters her login details on this webpage. Now Sumit has obtained her login information. He then purchases some software online and uses Rajni's online bank account to pay for it. He will be liable under this section.

Hacking – Section 43 (i)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means."

Illustration:

A to Z Ltd. has created a vast database of customer details & buying habits. The managers can query this database using a sophisticated "query management system". Ravi has developed this unique and path breaking system entirely on his own. One day Ravi quits his job and takes the entire code of the "query management system" with him.

Now the information in the database is still intact but it is no longer usable for the purpose of predicting customer orders. Ravi, has in effect, also destroyed the information contained in the database.

Computer Source Code Theft – Section 43 (j)

"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, —
(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage."

Illustration:

1. Ajay has created a software program. The source code files of the program are contained in a folder on Ajay's laptop. Darsh deletes the folder. He has destroyed the source code.
2. Tarun is designing a software program. He draws out the flowchart depicting the outline of the functioning of the program. Vipul tears up the paper on which he has drawn the flowchart. Vipul has destroyed the source code.

Cyber Offences - (Chapter XI - Information Technology Act, 2000 / Amendment thereof)

This Chapter entails criminal prosecution and the offender is punishable with imprisonment term or fine or with both.

Tampering with Computer Source Documents - Section 65

"Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programming, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form."
Computer Source Code is the most important asset of software companies. "Computer Source Code" means the listing of programmes, computer commands, design and layout. This section encompasses knowledge or intention of the concealment, destruction, alteration of any Computer Source Code as the main ingredient. Computer source code is required to be kept or maintained by law for the time being in force. The offender shall be punishable with imprisonment up to three years and/or Fine up to Rs. 2 lakhs.

Hacking, Copying, Downloading etc. with Dishonest & Fraudulent Intention – Section 66

"If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-
a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code."

Any act referred to in Sec. 43, if done dishonestly or fraudulently will be covered u/s 66 ITA. The Act of Hacking is included. The offences under this section are cognizable and bailable. The words "dishonestly" or "fraudulently" shall have the meaning as defined u/s 24/25 IPC.

Punishment for Sending Offensive Messages through Communication Service etc. – Section 66A

"Any person who sends, by means of a computer resource or a communication device,-

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message."

Information includes voice besides text messages, images etc. Therefore, voice message is included. The terms "grossly offensive", "annoyance" or "inconvenience" are not defined and leaves scope for controversy.

- **Computer Resource - Section 2 (k)**
  "Computer Resource" means Computer, computer system, computer network, data, computer data base or software."

- **Communication Device - Section 2 (ha)**
  "Communication Device" means Cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image."

- **Information - Section 2 (v)**
  "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche."

Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device - Section 66B

"Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both."

This section makes the act of dishonestly receiving stolen computer resource or communication device as punishable. The punishment for receiving stolen property is dealt in Section 411 IPC. But if the stolen article is computer resource or communication device, the same would be dealt u/s 66B.

Punishment for Identity theft - Section 66C

"Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh"

Section 66C makes the identity theft as standalone crime. This section also covers password theft and the offence of phishing.

Punishment for Cheating by Personation by using Computer Resource - Section 66D

"Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees"

Cheating by impersonation in electronic realm is covered u/s 66D. This section also covers Phishing.

Punishment for Violation of Privacy - Section 66E

"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that

person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both".

- "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons.
- "capture" with respect to an image, means to videotape, photograph, film or record by any means.
- "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast.
- "publishes" means reproduction in the printed or electronic form and making it available for public.
- "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that-
  (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
  (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Punishment for Cyber Terrorism - Section 66F

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data

or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life."

Section 66F deals with Cyber Terrorism i.e. one who causes denial of access to computer resources, or has unauthorized access to a computer resource, or introduces a virus, with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in any section of the people is deemed to be committing cyber terrorism. The wordings of Section 66 F suggests that the use of the internet in an ancillary role in furtherance of terrorism ("ancillary cyber activities") for example; terrorist use of information technology to formulate plans, spread propaganda, support terrorist recruiting, raise funds, and communicate is not regarded as cyber terrorism. It is only when the destructive nature of the "act" itself is carried out via computers or other cyber/electronic means through techniques such as infected e-mail attachments. Delivery of the terrorist's message via the Internet does not constitute cyber terrorism.

Punishment for Publishing or Transmitting Obscene Material in Electronic Form - Section 67

"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to

five years and also with fine which may extend to ten lakh rupees".

As per Section 67, a material is obscene, if it is lascivious, appeals to prurient interest of a person and has the tendency to deprave and corrupt all those who are likely to read, see or hear the material via the net. This Section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or which is kept or used bona fide for religious purposes.

Punishment for Transmission of Material Containing Sexually Explicit Act etc. in Electronic Form - Section 67A

"Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used bona fide for religious purposes."

This Section covers "Sexually Explicit Content" transmitted in electronic form. The term "sexually explicit act or conduct" has not been defined.

Punishment for Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, etc. in Electronic Form - Section 67B

"Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
(d) facilitates abusing children online or
(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years."

The section 67B deals with child pornography. This section makes even the recording in electronic form of any sexually explicit act with children shall be punishable under this section. Even if one is found to be engaged in online relationship with sexual overtone that may offend a reasonable adult on the computer resource

would be punishable under this section. The expression "May offend a reasonable adult" is subject to judicial scrutiny and interpretation and leaves scope for misuse and controversy.

Other Important Provisions

Power to Issue Directions for Blocking for Public Access of any Information through any Computer Resource – Section 69A

"(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub- section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."

Government gets power to issue directions for blocking for public access of any information through any computer resource. Directions can be issued in the interest of Sovereignty & integrity of India, Defence of India, Security of the State, Friendly relations with foreign States or Public order or Preventing commission of cognizable offence relating to above. An intermediary who fails to comply with directions in this regard shall be punished with imprisonment upto 7 years with fine.

Information Technology (Procedures and Safeguards for Blocking of Access of Information by Public) Rules, 2009 notified lays down the procedures, guidelines for blocking of the website empowering the designated officer who would act on the complaint made by nodal officer of Govt. Deptt. or Competent Court. For cyber security, Government may order any intermediary to allow access

to any computer resources and violation results in imprisonment upto 3 years with fine.

Punishment for Disclosure of Information in Breach of Lawful Contract – Section 72A

"Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both."

This Section deals with Data base security & privacy. A person including an intermediary is held liable if he discloses "personal information" which he accessed while providing services under a contract. The liability arises if the disclosure was made with an intention to cause or knowing that he is likely to cause wrongful loss or wrongful gain to a person.

Offences with Three Years Imprisonment to be Cognizable - Section 77B

"Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable."

Offence	Cognizable or non cognizable	Bailable or Non-bailable
Imprisonment less than 3 years	Non Cognizable	Bailable
Imp. of three years	Cognizable	Bailable
Imp. of more than 3 years	Cognizable	Non-Bailable

Protection Tips

Mentioned below are the some protection tips which may help in minimizing cyber risks:

Tips for Safe Computing

1. Use licensed operating system and other software on your computer. Using pirated software, besides being a crime, exposes you to cyber attacks. This is because you will be unable to get the regular security updates from the software manufacturer. Such updates are critical for protecting your system from cyber attacks.
2. Use a good anti-virus software. There are many free as well as commercial anti-virus software available. Ensure that the "automatic update" feature of the anti-virus software is always on. An anti-virus software loses effectiveness if it is not regularly updated.
3. Enable the auto-update feature in the operating system as well as all installed software.
4. Turn on the firewall in the operating system.
5. Use full disk encryption if your computer contains sensitive information.
6. Remember to backup your data regularly on multiple pen drives.
7. Think before you click on links or attachments - Do you need to? Is it trusted? If you are suspicious about an email attachment, you can open it in gmail using the "View as HTML" option. You can also use a sand-box utility (e.g. from www.sandboxie.com) to open the file in an isolated environment so that it cannot contaminate the rest of your hard disk.
8. Think before you download a files or program from the Internet - Do you need it? Is it trusted?
9. Remember, your computer contains a lot of personal information. Keep it safe and secure.
10. Keep good passwords. A good password is one that is not guessable even by someone who knows you very well. Make sure your password is "nonguessable" and difficult to "crack" - e.g. T!t1kSh@ instead of titiksha.
11. Maintain a regular backup of all names and email addresses in your contact list so that if your email account is hacked, you can notify your contacts not to act upon any emails sent from the hacked account.

12. Unless you trust a site, don't give your address, password, or credit card information.
13. Remember, if your computer is hacked, it can be misused for -
    i. Sending spam and phishing and fraud emails
    ii. Distribute pirated music, movies, software etc
    iii. Distribute pornography
    iv. Hack into other computers

Tips for Safe Online Banking

1. Connect to your bank using a device that has the latest and updated security software, web browser and operating system.
2. Logout immediately after you have completed your transactions.
3. If you are connected to a public wifi, don't access your bank account.
4. Never click on a link in an email to visit your bank's site. Always type the url in the browser address bar.
5. Never disclose your password or PIN to anyone, not even to a genuine bank employee.
6. Take a print-out of the transaction confirmation. Store this print-out till you cross check that transaction in your monthly statement.

Tips for Securing Your Mobile Device

1. Mobile devices (smart phones, tablets, iPads etc.) are computers with software that must be regularly updated. If needed, synch them with a "clean" computer. Make sure your mobile devices have the latest security software, web browser and operating system. Keep these updated.
2. Use strong passcodes to lock your mobile devices.
3. Understand what data (location, access to your social networks) will be accessed by an app before you install it.
4. Consider disabling the geo-tagging feature on your phone.
5. If you are connected to a public Wifi, don't access sites where you need to enter your password, credit card information etc.
6. While banking and shopping online, ensure the sites are https or shttp.
7. Remember, your mobile device contains a lot of personal information. Keep it safe and secure.