# Access related crimes

This document is an extract from the book *Cyber Crime & Digital Evidence – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

Asian School of Cyber Laws

**www.asianlaws.org**

# 1. Access related crimes

According to section 2(1)(a) of the IT Act

*"**access**" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;*

[Note: The terms computer, computer system, computer network, logical, arithmetic, memory functions are discussed in detail in the ASCL publication titled "Fundamentals of Cyber Law".]

**Essentials of the term "access"**

1. Gaining entry into a computer, computer system or computer network

2. Instructing the logical, arithmetical, or memory function resources of a computer, computer system or computer network

3. Communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network

**Let us examine the essential elements**

**Grammatical variations** of access include terms such as accesses, accessed, accessing etc.

**Cognate expressions** are related words and phrases. Depending upon the situation, these could include "log on", "retrieve" etc.

**Gaining entry into** applies to physical access. The terms computer, computer system and computer network have been defined very widely under the IT Act. These terms may include the physical box (cabinet) in which a computer is housed. They may also include the physical room in which a computer network or super computer is housed.

**Illustration 1**
A massive super computer is housed in particular premises. Sameer breaks open the door and enters the premises. He has gained entry into the computer.

**Illustration 2**
A Government computer contains critical information in its hard disk. Sameer unscrews the cabinet of the computer in order to steal the hard disk. He has gained entry into the computer.

**Instructing** means "to give orders" or "to direct". Instructing is essentially a one way process which does not require two-way communication between the instructor and the instructed.

**Illustration 1**
A Government computer contains critical information. Sameer enters the room where the computer is located and keys in some commands into the keyboard. He does not realise that the keyboard is disconnected from the computer.

Here Sameer has **not instructed** the logical, arithmetic or memory functions of the computer.

**Illustration 2**
Sameer has set up his computer in such a way that he can remotely shut it down by sending an SMS. The process is as under:

1. He sends an SMS with the words "shutdown" to a particular service provider.

2. The service provider automatically forwards the contents of the SMS to Sameer's personal email address.

3. Sameer's computer is running an email client (e.g. MS Outlook) that is configured to automatically download emails from his account every 5 minutes.

4. The email client is also configured to run a file called "shutdown.bat" every time it downloads an email with the words "shutdown" in it.

5. This "shutdown.bat" files shuts down Sameer's computer within a few seconds.

6. This enables Sameer to shutdown his computer even when he is not in the same country.

This is an illustration of instructing the logical, arithmetic or memory functions of the computer.

**Communicating with** is essentially a two-way process that involves exchange of information.

**Illustration**

Sameer is a hacker attempting to steal some information from Sanya's computer. He first remotely scans Sanya's computer using specialised software. The software sends out queries to Sanya's computer which replies to the queries. As a result of this, Sameer obtains details of the operating system installed on Sanya's computer.

Sameer has communicated with Sanya's computer.

## 1.1 Unauthorized Access

According to section 43(a) of the IT Act

*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;*

*…….he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.*

The two concepts covered in this section are "accesses" and "secures access".

**Accesses** is a grammatical variation of the term access as discussed in the previous pages.

**Secures access** is a term that needs to be examined in depth. The term "secure" means "to make certain". The term "secures access" would mean "to make certain that access can be achieved as and when desired by the person seeking to access".

**Illustration**

Sanya is the network administrator of a Government department. She stores the passwords of the Government department main server in her personal laptop.

Sameer is Sanya's friend. Without Sanya's permission, he switches on her laptop and notes down the passwords of the Government department main server. He has accessed Sanya's laptop without her permission.

He has "secured access" to the Government server. Although he has not accessed the Government server, he has "secured" access to it. By obtaining the passwords, he has made certain that he can access the server as and when he desires.

This section covers incidents where the "permission" of the owner or other person in charge of the computer is not obtained. Permission is the "authorization granted to do something" e.g. Sanya permits Sameer to switch on her computer.

Permission can be **express** or **implied**. Permission can also be **complete** or **partial**.

**Illustration 1**
Sanya is the network administrator of Noodle Ltd. The employment contract that she has signed with Noodle Ltd states that she is responsible for the "complete maintenance and security of the Noodle Ltd computer systems and networks".

Noodle Ltd has given her the **express permission** to access their systems.

This is also **complete permission**. As the network administrator Sanya would need complete access to all parts of the systems.

**Illustration 2**
Tanya is an employee of the marketing department of Noodle Ltd. All the marketing department employees have been allotted usernames and passwords which allows them to log into the Noodle Ltd main server.

Noodle Ltd has given Tanya the **implied permission** to access their systems. This is also a **partial permission**. As an employee of the marketing department, Tanya would need access only to that part of the system that contains information relevant to the marketing department.

This section also covers acts that **exceed permission**.

**Illustration**
Sameer is an employee of the finance department of Noodle Ltd. His username and password entitles him to access only limited information on the official Noodle server.

Tanya is the senior manager of the finance department. One day, while Tanya is abroad on official business, she calls up Sameer and gives him her username and password. She requests Sameer to retrieve some official documents from the Noodle server and email those documents to her. Sameer complies with her request.

Several days later, Sameer again uses Tanya's password to access the Noodle server. Now he has exceeded the scope of his permission. Tanya had given Sameer an implied permission to use her password only on one occasion.

The subsequent use of the password by Sameer is unauthorised and amounts to exceeding the scope of his permission.

The **penalty** provided for this section is compensation up to Rs 1 crore.

# Unauthorised Access (Summary)

| | |
|---|---|
| **Actions covered** | Accessing or securing access to a computer without adequate permission. |
| **Penalty** | Compensation up to **Rs 1 crore** |
| **Relevant authority** | Adjudicating Officer |
| **Appeal lies to** | Cyber Regulations Appellate Tribunal |
| **Investigation Authorities** | 1. Controller of Certifying Authorities (CCA)<br>2. Person authorised by CCA<br>3. Deputy Superintendent of Police authorised by Adjudicating Officer<br>4. CERT-IND official authorised by Adjudicating Officer<br>5. CCA official authorised by Adjudicating Officer |
| **Points to mention in complaint** | 1. Complainant details<br>2. Respondent details<br>3. Damages claimed<br>4. Fee details<br>5. Time of Contravention<br>6. Place of Contravention<br>7. Cause of action<br>8. Brief facts of the case |

## 1.2 Accessing Protected System

According to section 70 of the IT Act

*(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.*

*(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-Section (1).*

*(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this Section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.*

As per Executive order dated 12-9-2002, issued by Ministry of Communications &Information Technology details of every protected system should be provided to the Controller of Certifying Authorities.

**There are three elements to this section-**

1. Gazette notification for declaring protected system.
2. Government order authorizing persons to access protected systems.
3. Punishment for access to protected systems by unauthorised persons.

Let us discuss the relevant terms and issues in detail.

**Appropriate government** is determined as per Schedule VII of the Constitution of India.

Schedule VII of the Constitution of India contains 3 lists – Union, State and Concurrent. Parliament has the exclusive right to make laws on items covered in the Union List e.g. defence, Reserve Bank of India etc.

State Governments have the exclusive right to make laws on items covered in the State List e.g. police, prisons etc.

Parliament as well as the State Governments can make laws on matters in the Concurrent List e.g. forests, electricity etc.

**Illustration 1**
If the computer network of the Indian Army is to be declared as a protected system, the Central Government would be the appropriate Government.

**Illustration 2**
If the computer network of the Mumbai police is to be declared as a protected system, the Government of Maharashtra would be the appropriate Government.

**Illustration 3**
If the computer network of the Forest Department in Maharashtra is to be declared as a protected system, the Central Government as well as the Government of Maharashtra would be the appropriate Government.

All the acts, rules, regulations etc passed by the Central and State Government are notified in the **Official Gazette.** The Official Gazette in the electronic form is called the Electronic Gazette. A notification becomes effective on the date of its publication in the Gazette.

The Government **order** may specify the authorised persons by name or by designation (e.g. all officers of rank of Inspector and above deputed in a particular department).

The term "**securing access**" in this section is a grammatical variation of the term "secures access" as discussed earlier.

**Attempt to secure access** is a very wide term and can best be understood through the following illustrations.

**Illustration 1**
Sameer runs a password cracking software to crack the password of a protected system. Irrespective of whether he succeeds in cracking the password, he is guilty of attempting to secure access.

**Illustration 2**
Sameer runs automated denial of service software to bring down the firewall securing a protected system. Irrespective of whether he succeeds in bringing down the firewall, he is guilty of attempting to secure access.

**Illustration 3**
Sameer sends a Trojan by email to Pooja, who is the network administrator of a protected system. He plans to Trojanize Pooja's computer and thereby gain unauthorised access to the protected system. Irrespective of whether he succeeds in finally accessing the protected system, he is guilty of attempting to secure access.

The **punishment** provided for this section is rigorous or simple imprisonment of up to **10 years** and **fine**.

# Unauthorised Access to Protected System (Summary)

| | |
|---|---|
| **Actions covered** | Unauthorised access to protected system (or attempt thereof) |
| **Penalty** | Imprisonment up to **10 years** and **fine** (this may be rigorous or simple imprisonment i.e. with or without hard labour) |
| **Relevant authority** | Court of Session |
| **Appeal lies to** | High Court |
| **Investigation Authorities** | 1. Controller of Certifying Authorities (CCA)<br>2. Person authorised by CCA<br>3. Police Officer not below the rank of Deputy Superintendent |
| **Points to mention in complaint** | 1. Complainant details<br>2. Suspect details<br>3. Details of gazette notification and Government order<br>4. How and when the contravention was discovered and by whom<br>5. Other relevant information |

## Firos vs. State of Kerala

AIR2006Ker279, 2006(3)KLT210, 2007(34)PTC98(Ker)

**IN THE HIGH COURT OF KERALA**

W.A. No. 685 of 2004
Decided On: 24.05.2006

Appellants: **Firos**
**Vs.**
Respondent: **State of Kerala**

### Summary of the case

The Government of Kerala issued a notification u/s 70 of the Information Technology Act declaring the FRIENDS application software as a protected system.

The author of the application software filed a petition in the High Court against the said notification. He also challenged the constitutional validity of section 70 of the IT Act.

The Court upheld the validity of both, section 70 of the IT Act, as well as the notification issued by the Kerala Government.

### Background of the case

Government of Kerala, as part of IT implementation in Government departments, conceived a project idea of "FRIENDS" (Fast, Reliable, Instant, Efficient Network for Disbursement of Services).

The project envisaged development of a software for single window collection of bills payable to Government, local authorities, various statutory agencies, Government Corporations etc. towards tax, fees, charges for electricity, water, etc. A person by making a consolidated payment in a computer counter served through "FRIENDS" system could discharge all his liabilities due to the Government, local authorities and various agencies.

The work of developing the "FRIENDS" software was entrusted to Firos. The application-software "FRIENDS" was first established at Thiruvananthapuram, free of cost, and since the project was successful, the Government decided to set up the same in all other 13 district centres.

The Government of Kerala entered into a contract with Firos for setting up and commissioning "FRIENDS" software system in 13 centres all over Kerala for providing integrated services to the customers through a single window for a total consideration of Rs. 13 lakh. Firos set up FRIENDS service centres in all the 13 centres and they were paid the agreed remuneration.

A dispute arose between Firos and the Government with regard to Intellectual Property Rights (IPR) in the FRIENDS software.

The Government arranged to modify the FRIENDS software to suit its further requirements through another agency. Firos alleged violation of copyright and filed a criminal complaint against the Government. A counter case was filed by the Government against Firos.

The Government of Kerala issued a notification under Section 70 of the Information Technology Act declaring the FRIENDS software installed in the computer system and computer network established in all centres in Kerala as a protected system.

Firos filed a writ petition challenging section 70 of the IT Act.

**Issues raised by the Petitioner**

1. The Government of Kerala notification under section 70 of the IT Act is arbitrary, discriminatory and violates Article 19(1)(g) of the Constitution of India.

2. The Government of Kerala notification under section 70 of the IT Act is and was against the statutory right conferred under Section 17 of the Copyright Act.

3. Section 70 of the IT Act which confers the unfettered powers on the State Government to declare any computer system as a protected system is arbitrary and unconstitutional and inconsistent with Copyright Act.

4. Section 70 of the IT Act has to be declared illegal.

5. There is direct conflict between the provisions of Section 17 of the Copyright Act and Section 70 of the Information Technology Act. When there is conflict between two Acts, a harmonious construction has to be adopted.

**Conclusions of the court**

1. There is no conflict between the provisions of Copyright Act and Section 70 of IT Act.

2. Section 70 of the IT Act is not unconstitutional.

3. While interpreting section 70 of the IT Act, a harmonious construction with Copyright Act is needed.

4. Section 70 of the IT Act is not against but subject to the provisions of the Copyright Act.

5. Government cannot unilaterally declare any system as "protected" other than "Government work" falling under section 2(k) of the Copyright Act on which Govt.'s copyright is recognised under Section 17(d) of the said Act.

**Section 2(k) of the Copyright Act**

(k) 'Government work' means a work which is made or published by or under the direction or control of -

(i) the Government or any department of the Government;

(ii) any Legislature in India;

(iii) any Court, Tribunal or other judicial authority in India;

**Section 17(d) of the Copyright Act**

17. First owner of copyright:- Subject to the provisions of this Act, the author of a work shall be the owner of the copyright therein;

(d) in the case of a Government work, Government shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;

# 1.3 Hacking

According to section 66 of the IT Act

*(1)Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.*

*(2)Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.*

**There are 2 elements to this section-**

1. Intention to cause wrongful loss or damage
   **or**
   Knowledge of the likelihood of wrongful loss or damage

   **AND**

2. Destruction or deletion or alteration of information in a computer
   **or**
   diminishing value or utility of a computer resource
   **or**
   injuriously affecting a computer resource

Let us discuss the relevant terms and issues in detail.

**Loss** signifies detriment or disadvantage. Loss can be **temporary** or **permanent**. Loss can relate to something that the loser has currently or is likely to get in the future. This term is best understood through the following illustrations.

**Illustration 1**
Noodle Ltd runs a commercial email service. Sameer launches a denial of service attack on the Noodle website and brings it down for a few hours. Noodle's customers are disgruntled that they were unable to access their emails for a few hours and therefore leave the Noodle services.

Noodle has suffered a **loss of future revenue** that it could have earned from these customers. It has also suffered a **loss of goodwill and reputation**.

**Illustration 2**
Sameer is a graphics designer. He creates high resolution images and stores them on his computer. One of his employees deliberately deletes hundreds of these images. Sameer has suffered a **loss of data**.

If Sameer can recover the images using cyber forensics and data recovery technology, then he has suffered a **temporary loss** of data. If he cannot recover the data, then he has suffered a **permanent loss** of data.

**Wrongful loss** is the loss by unlawful means.

**Illustration 1**
Sanya has launched an innovative email service. Sameer gains unauthorised access to her source code, makes modifications to it and launches a rival email service causing loss to Sanya. **This is wrongful loss** as it is caused by unlawful means (unlawful access to the source code in this case).

**Illustration 2**
Sanya has launched an innovative email service. Sameer hires excellent programmers and develops and launches a better email service. This causes loss to Sanya. **This is NOT wrongful loss** as it is not caused by unlawful means.

**Damage** for the purposes of this section implies injury or deterioration caused by an unlawful act.

**Illustration 1**
Sameer picks up Sanya's laptop with the intention of stealing it. He then accidentally drops it on the floor, thereby destroying it. Sameer has caused damage.

**Illustration 2**
Sanya has left her laptop on a table. Someone drops water on the table and the water is about to touch the laptop. With the intention of saving the laptop from the water, Sameer picks it up from the table.

He then accidentally drops it on the floor, thereby destroying it. Sameer has not caused damage as per this section.

**Intent** means a fixed determination to act in a particular manner

**Illustration 1**
Sameer, a thief, picks up Sanya's laptop in order to steal it. The intent with which Sameer has picked up the laptop is to commit theft.

**Illustration 2**
Sanya has left her laptop on a table. Someone drops water on the table and the water is about to touch the laptop. In order to save the laptop from the water, Sameer picks it up from the table. The intent with which Sameer has picked up the laptop is to protect it from damage.

**To cause** means to make something happen. Cause can be direct or indirect.

**Illustration 1**
Sameer pressed the "delete" button on the keyboard causing the data to be deleted. Sameer's act of pressing the delete button is the **direct cause** of the data being deleted.

**Illustration 2**
Sameer accidentally sends a computer virus to Pooja by email. Pooja unwittingly downloads the virus. The virus spreads on her computer and overwrites a lot of data. Sameer's email was the **indirect cause** of the data loss.

The computer virus was the **direct cause** of the data loss.

**Knowingly** doing something implies consciously or wilfully doing something.

**Illustration 1**
Sameer downloaded software that enabled him to remotely shut down computers on the network. He felt that the software would be very useful and thus he installed it on many computers in his office.

He did not know that the software was in effect a Trojan that would compromise the security of his company. Here Sameer has not installed the Trojan knowingly.

**Illustration 2**
Sameer was very disgruntled with the fact that he was not promoted in his company. Out of anger he installed a Trojan on many computers in his office. Here Sameer has knowingly installed the Trojan.

**Likely to cause** means probable to cause. The term likely is usually used to mean "in all probability". This term has to be interpreted in light of the circumstances of each case.

**Illustration 1**
Sameer is working on a Windows computer. He downloads a virus that is known to damage Windows machines. The virus is **likely to cause** damage to his computer.

**Illustration 2**
Sameer is working on a Linux computer. He downloads a virus that is known to damage Windows machines. The virus is **not likely to cause** damage to his computer.

**Public** is a term that refers to "the people", "the general body of mankind", "the community at large", "a class of the community" etc. A thing is said to be public if it is owned by the public or if its uses are public.

**Illustration 1**
Sameer installs a keylogger on a cyber café computer. The keylogger would steal passwords of all the users of the cyber café computers. His act is such that it **affects the public**.

**Illustration 2**
Sameer launches a denial of service attack on the website of the Railways. This brings down the website and causes hardships to railway passengers looking to make online reservations or enquiries using the said website. His act is such that it **affects the public**.

**Illustration 3**

Sameer installs a keylogger on the computer used only by Pooja. The keylogger would steal passwords entered by Pooja using that computer. His act is such that it **does not affect the public**.

**Person** includes natural persons (such as men, women and children) as well as artificial persons (such as companies, societies etc).

**Information** includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.

Data is a formalised representation of information, knowledge, facts, concepts or instructions. Data undergoes processing by a computer. Data can be in electronic form (e.g. stored in a CD) or physical form (e.g. computer printouts).

Examples of data include computerised attendance records of a school, information in the RAM of a computer, printouts of a computerised accounting system etc.

**Microfilms** are processed sheets of plastic (similar to the commonly used photograph rolls) that carry images of documents. These images are usually about 25 times reduced from the original. The images cannot be viewed by the naked eye and special readers are used to project the images on a screen. They are most commonly used in libraries for transmission, storage, reading and printing of books.

**Microfiche** is a type of microfilm containing several micro images.

**Illustration**

The following are information:

a. A photo of Priyanka Chopra stored on a DVD
b. A Shakira song stored on a CD
c. The ebook version of this book
d. A recording of a phone conversation

**Computer resource** includes computer, computer system, computer network, data, computer data base or software.

**Information residing in a computer resource** must be construed in a wide manner. It includes information that exists or is present in a computer resource temporarily or permanently. This is best discussed through the following illustrations.

**Illustration 1**
A personal computer has a BIOS chip that contains basic instructions needed to boot up a computer. These instructions are in the form of "information permanently residing" on the BIOS (which is a computer resource).

**Illustration 2**
Pooja is browsing a website. While she is viewing the website on her monitor, the information is cached in her computer in a folder specially reserved for temporary files.

Some of that information is also stored in the RAM of her computer. When the computer is shutdown, the information in the RAM is lost.

These are examples of information that is "temporarily residing" in a computer resource.

**Illustration 3**
Other illustrations of information residing in a computer resource are:

a. Music files stored in an iPod
b. Software installed on a computer
c. Ebook stored on a CD
d. Software installed in a cell phone
e. Software embedded in a microwave oven

**Destroys** means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

**Destroying information** also includes acts that render the information useless for the purpose for which it had been created.

**Illustration 1**
Noodle Ltd has created a vast database of customer details and buying habits.

The Noodle managers can query this database using a sophisticated "query management system".

Sameer has developed this unique and path breaking "query management system" entirely on his own. One day Sameer 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. Sameer has, in effect, also destroyed the information contained in the database.

**Deletes** in relation to electronic information means "to remove", "to erase", "to make invisible" etc. Such deletion can be temporary or permanent.

**Illustration 1**
Pooja has created a text file containing her resume. Sameer deletes the file from her computer. On deletion, the file gets automatically transferred to the "recycle bin" of Pooja's computer. Here Sameer has **temporarily deleted** the file.

Sameer empties the "recycle bin" of Pooja's computer. The file is still only **temporarily deleted** as it can be recovered using cyber forensics.

Sameer then uses specialised wiping software so that the file cannot be recovered using forensics. Now he has **permanently deleted** the file.

**Illustration 2**
Pooja is a novice computer user. She has created a text file containing her resume. Sameer changes the properties of the file and makes it a "hidden" file. Although the file still exists on Pooja's computer, she can no longer see it. Sameer has deleted the file.

**Alters**, in relation to electronic information, means "modifies", "changes", "makes different" etc. This modification or change could be in respect to size, properties, format, value, utility etc".

Alteration can be **permanent** or **temporary**. It can also be **reversible** or **irreversible**.

**Illustration 1**
Pooja has created a webpage for her client. A webpage is essentially an HTML (Hyper Text Markup Language) file. Sameer changes the file from HTML to text format. He has altered the file. This is a **reversible alteration**.

**Illustration 2**
Pooja has created a text file. Sameer changes the properties of the file and makes it a “hidden” file. The file retains its original content but it has been altered as its attributes have changed (it is now a hidden file). This is a **reversible alteration**.

**Illustration 3**
Pooja has created a text file named “pooja.txt”. Sameer changes the name of this file to “pooja1.txt”. Although the file retains its original content, it has been altered. This is a **reversible alteration**.

**Illustration 4**
Pooja is investigating Sameer’s computer for suspected cyber pornography. She seizes a word file that contains incriminating evidence against Sameer. As per procedure, she computes the hash value of the file and notes it in her report.

Sameer later manages to access the seized file and adds a “#” symbol to the contents of the file. The hash value of this altered file will be different from the hash value computed earlier by Pooja.

This is a **permanent irreversible alteration**. Even after the “#” symbol is removed, the hash value of the file will never be the same as the original computed by Pooja.

**Illustration 5**
Pooja is a graphics designer. She creates very high resolution images for her clients. A high resolution image can be magnified several times and still look clear.

Sameer is one of her employees. He changes some of the high resolution images into low resolution images. Although the low resolution images look the same as the high resolution ones, they cannot be magnified. The value and utility of the images has been reduced.

This is an example of **permanent and irreversible alteration**.

**Value** implies monetary worth.

**Illustration**
Pooja is a graphics designer. She buys a sophisticated computer for Rs 2 lakh. The value of the computer is Rs 2 lakh. She purchases one license of specialised graphics software for Rs 50,000 and installs the software on her computer. The value of the computer is now Rs 2.5 lakh.

She then hires a specialist to configure her computer for optimal performance. The specialist charges her Rs 10,000 for his services. The value of the computer is now Rs 2.6 lakh.

**Utility** means “usefulness”.

**Illustration 1**
The utility of a high resolution image lies in its ability to be magnified several times. This enables the image to be used for various purposes such as on a website, in a printed catalogue, on a large hoarding etc.

**Illustration 2**
The utility of anti-virus software is its ability to detect computer viruses and other malicious code.

**Illustration 3**
The utility of a sophisticated computer is its ability to render high resolution graphics files in a very short time.

**Diminish** means “reduce” or “lessen”,

**Illustration**
A computer worm replicates itself and thereby hogs up system resources such as hard disk space, bandwidth etc. This can diminish the performance and speed of the computer network.

**Diminishes value** means “reduces the monetary worth”.

**Illustration**
Pooja is a graphics designer. She creates very high resolution images for her clients. A high resolution image can be magnified several times and still look clear. She can sell each image for around Rs 5000.

Sameer is one of her employees. He changes some of the high resolution images into low resolution images. Although the low resolution images look the same as the high resolution ones, they cannot be magnified. Now she cannot sell an image for more than Rs 400. Sameer has thus diminished the value of the images.

**Diminishes utility** means “reduces the usefulness”.

**Illustration**
Pooja has purchased a very sophisticated computer that has 2 GB RAM. This enables the computer to render a large image file in 3 seconds. Sameer steals 1 GB RAM from the computer. Now the computer takes more than 5 seconds to render the image file. Sameer’s act of stealing the RAM has diminished the utility of Pooja’s computer.

**Affects** means “influences” or “produces a change in”.

**Illustration**
A computer virus changes the data stored in a computer. The virus affects the data.

**Injurious** means “harmful”, “hurtful”, or “detrimental”.

**Illustration**
A computer virus is injurious to the data stored in a computer.

**Affects injuriously** means produces a "harmful or detrimental change".

**Illustration 1**
Placing a powerful magnet close to a floppy disk causes permanent and irreversible damage to the disk. We can say that the magnet affects the disk injuriously.

**Illustration 2**
Dropping a laptop on the floor can affect it injuriously.

**Illustration 3**
Dropping water on a laptop can affect it injuriously.

As we can see, the term hacking has been given a very wide definition under the Indian law. To better understand the scope of "hacking" under the Indian law let us consider some illustrations of acts that would be covered by "hacking".

**Illustration 1**
A disgruntled employee of a small Indian bank placed a powerful magnet near the banks' main server. Over a few weeks, the bank lost vital data relating to its customer's accounts.

**Illustration 2**
Mahesh Mhatre and Anand Khare (alias Dr Neukar) were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell. They had allegedly used password cracking software to crack the FTP password for the police website. They then replaced the homepage of the website with pornographic content.

**Illustration 3**
A computer network was used for receipt and accounting of electricity bills by the New Delhi Municipal Council. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

**Illustration 4**
A keyboard operator processing orders at an Oakland USA department store changed some delivery addresses and diverted several thousand dollars worth of store goods into the hands of accomplices.

**Illustration 5**
A ticket clerk at the Arizona Veterans' Memorial Coliseum in USA issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

**Illustration 6**
The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US $ 10 billion.

**Illustration 7**
Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

**Illustration 8**
A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these 'friends' managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom.

Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. A year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

**Illustration 9**

The network administrator in a global bank received a beautifully packed CD ROM containing "security updates" from the company that developed the operating system that ran his bank's servers. He installed the "updates" which in reality was Trojanized software. Huge amounts of confidential data were stolen from the bank's systems.

The **punishment** provided for hacking is imprisonment up to 3 years and / or fine up to Rs 2 lakh.

# Hacking with Computer System (Summary)

| | |
|---|---|
| **Actions covered** | Following acts done with knowledge / intent to cause wrongful loss / damage:<br>1. Destroying, deleting or altering data<br>2. Diminishing value / utility of computer<br>3. Injuriously affecting computer |
| **Penalty** | Imprisonment up to **3 years** and / or fine up to **Rs 2 lakh** |
| **Relevant authority** | Judicial Magistrate First Class |
| **Appeal lies to** | Court of Session |
| **Investigation Authorities** | 1. Controller of Certifying Authorities (CCA)<br>2. Person authorised by CCA<br>3. Police Officer not below the rank of Deputy Superintendent |
| **Points to mention in complaint** | 1. Complainant details<br>2. Suspect details<br>3. How and when the contravention was discovered and by whom<br>4. Damage suffered<br>5. Other relevant information |

# 1.4 Assisting Unauthorized Access

According to section 43(g) of the IT Act

*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) 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;*

*…….he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.*

The essential element of this section is that assistance is provided for obtaining access to a computer in contravention of the IT Act and its allied laws.

A person who obtains access to a computer in contravention of the IT Act would be liable under the relevant sections (e.g. 43(a) or 66 or 70 etc). What this section specifically covers is providing assistance to such a person. Such assistance must facilitate the unlawful access.

**Assistance** is the act of helping or aiding.

**Facilitate** means "to make easier" or "to make less difficult" or to "assist in the progress of".

Let us consider some illustrations to understand this concept.

**Illustration 1**

Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Aditi, the manager of Noodle, hands over a list of passwords to Sameer. Using these passwords, Sameer gains the unlawful access. Aditi has provided assistance to Sameer to facilitate his unlawful access.

**Illustration 2**

Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She is monitoring the Intrusion Detection System (IDS) of Noodle at the time when Sameer is launching his attack.

The IDS detects the attack and gives a warning. Priyanka deliberately ignores the warning and does not use any measures to stop the attack.

Priyanka has provided assistance to Sameer to facilitate his unlawful access.

**Illustration 3**
Sameer is planning to gain unauthorised access into the computer systems of Noodle Bank Ltd. Priyanka, the network security administrator of Noodle, is his good friend. She disables the Noodle firewall at the time when Sameer is launching his attack.

Priyanka has provided assistance to Sameer to facilitate his unlawful access.

The **penalty** provided for this section is compensation up to **Rs 1 crore**.

# Assisting unlawful access (Summary)

| | |
|---|---|
| **Actions covered** | Providing assistance to facilitate unlawful access to a computer |
| **Penalty** | Compensation up to **Rs 1 crore** |
| **Relevant authority** | Adjudicating Officer |
| **Appeal lies to** | Cyber Regulations Appellate Tribunal |
| **Investigation Authorities** | 1. Controller of Certifying Authorities (CCA)<br>2. Person authorised by CCA<br>3. Deputy Superintendent of Police authorised by Adjudicating Officer<br>4. CERT-IND official authorised by Adjudicating Officer<br>5. CCA official authorised by Adjudicating Officer |
| **Points to mention in complaint** | 1. Complainant details<br>2. Respondent details<br>3. Damages claimed<br>4. Fee details<br>5. Time of Contravention<br>6. Place of Contravention<br>7. Cause of action<br>8. Brief facts of the case |


www.asianlaws.org

**Head Office**

6th Floor, Pride Senate,

Behind Indiabulls Mega Store,

Senapati Bapat Road,

Pune - 411016.

India

**Contact Numbers**

+91-20-25667148

+91-20-40033365

+91-20-64000000

+91-20-64006464

**Email:** info@asianlaws.org

**URL:** www.asianlaws.org