

Hacking & the Indian Law

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



www.asianlaws.org

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: <ol style="list-style-type: none"> 1. Destroying, deleting or altering data 2. Diminishing value / utility of computer 3. Injurious 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	<ol style="list-style-type: none"> 1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	<ol style="list-style-type: none"> 1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Damage suffered 5. Other relevant information



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