

## **VIII Module: Pen Testing and Cyberlaw**

**Penetration Testing using Metasploit and Metasploitable Cyberlaw Section under IT act 2000-43, 65, 66A, 66B, 66C, 66D, 66E, 66F, 67A, 67B, 71, 72, 73 and 74, Penalty and preventive measures to be taken for the crime associated with each case if any and real life cybercrime cases under each section.**

**Section :43 : Penalty and Compensation for damage to computer, computer system, data, etc**

**Example : Mphasis BPO Fraud: 2005**

In December 2004, four call centre employees, working at an outsourcing facility operated by Mphasis

in India, obtained PIN codes from four customers of Mphasis' client, Citi Group. These employees

were not authorized to obtain the PINs. In association with others, the call centre employees opened

new accounts at Indian banks using false identities. Within two months, they used the PINs and

account information gleaned during their employment at Mphasis to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw

cash from the falsified accounts, \$426,000 was stolen; the amount recovered was \$230,000.

Verdict: Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.

**Section 65 : Tampering with computer source documents**

**Section 65 and 43(d) of the IT. Act covers the offence of data diddling.**

**Example :**

In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores.

These were allegedly prepared using Desk Top Publishing Systems.

**Example :**

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totaling several billion rupees.

**Section 66A : Punishment for offensive messages****Example :**

Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint

about tarnishing her image in the social networking site Orkut.

Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted

on the profile. The profile had been sketched in such a way that it drew lewd comments from many

who visited her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

**Example:**

The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer. The lawyer took exception to a community called 'We

hate India', owned by someone who identified himself as Miroslav Stankovic. The community

featured a picture of the Indian flag being burnt.

**Example**

Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Profane names were posted on the profile. The matter came to light after the girl's family started receiving lewd/coarse calls referring to Orkut.

**Example:**

In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too

late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five

bombs in Mumbai; you have two hours to find it.” The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

### **Section 66C - Punishment for identity theft**

#### **Example:**

The CEO of an identity theft protection company, Lifelock, Todd Davis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a \$500 cash advance loan.

#### **Example:**

Li Ming, a graduate student at West Chester University of Pennsylvania faked his own death, complete with a forged obituary in his local paper. Nine months later, Li attempted to obtain a new driver's

license with the intention of applying for new credit cards eventually.

### **Section 66D - Punishment for cheating by impersonation by using computer resource**

#### **Example:**

A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly

induces Z to let him have on credit goods online for which he does not mean to pay. A cheats.

#### **Example :**

A branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days

### **Section 66E - Punishment for violation of privacy**

#### **Example:**

Jawaharlal Nehru University MMS scandal In a severe shock to the prestigious and renowned institute - Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus

and transmitted outside the university.

Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

**Example:**

Nagpur Congress leader's son MMS scandal

On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts.

According to

the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

**Section-66F Cyber Terrorism**

**Example:**

In 1997, 35 computer specialists used hacking tools freely available on 1 ,900 web sites to shut down large segments of the US power grid. They also silenced the command and control system of the Pacific Command in Honolulu.

**Example:**

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-

week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists

against a country's computer systems.

**Example:**

In 1994, a 16-year-old English boy took down some 100 U.S. defense systems.