Cyber Security (CPE-411)

BTech. CSE

Department of Computer Science and Engineering

Punjabi University

Section B

Part-I

- The IT Act 2000
- Amendments IT Act 2008
- Sections IT Act: 43,65,66,67,68,69,70.
- Section relevant to cyber crime under IPC(Indian Penal Code).

Cyber Laws in India

- **Cyber Crime** is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India Penal Code, 1860. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. To put it in simple terms "*any offence or crime in which a computer is used is a cyber crime*".

ITA 2000

The Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself.

“ *To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “Electronic Commerce"*. The Information Technology Act, 2000, was thus passed and was made effective from 17 October 2000.

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

Amendment Act 2008 (ITAA-2008)

Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA

Some of the notable features of the ITAA

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

Section 43: Penalties and compensation for damage to computer,

Section 43 deals with penalties and compensation for damage to computer, computer system etc. This Section addresses the civil offence of theft of data. If any person without permission of the owner or any other person who is in-charge of a computer, accesses or downloads, copies or extracts any data or introduces any computer contaminant like virus or damages or disrupts any computer or denies access to a computer to an authorized user or tampers etc. He shall be liable to pay damages to the person so affected. Earlier in the ITA -2000 the maximum damages under this head was Rs.1 crore, which (the ceiling) was since removed in the ITAA 2008.

Writing a virus program or spreading a virus mail, a bot, a Trojan or any other malware in a computer network or causing a Denial of Service Attack in a server will all come under this Section and attract civil liability by way of compensation. Under this Section, words like Computer Virus, Compute Contaminant, Computer database and Source Code are all described and defined.

Section 65:
Tampering with computer source documents

Tampering with source documents is dealt with under this section. Concealing, destroying, altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years detention or two lakh rupees or with both. Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court (Bhim Sen Garg vs State of Rajasthan and others, 2006, Cri LJ, 3463, Raj 2411) attract punishment under this Section. Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc in any form.

Section 66:Hacking with computer system

Section 66: Computer related offences are dealt with under this Section. Data theft stated in Section 43 is referred to in this Section. Whereas it was a plain and simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Sec 66 and it was an offence.

Section 66A

Sending offensive messages thro communication service, causing annoyance etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. Punishment for these acts is imprisonment upto three years or fine.

66B: Receiving stolen computer or communication device

66C :Using password of another person

66B Dishonestly receiving stolen computer resource or communication device with punishment upto three years or one lakh rupees as fine or both.

66C Electronic signature or other identity theft like using others’ password or electronic signature etc. Punishment is three years imprisonment or fine of one lakh rupees or both.

66D: Cheating using computer resource
66E: Publishing private images of others

66D Cheating by personation using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.

66E Privacy violation – Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both.

66F Acts of cyberterrorism

66F Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or Trojan Horse or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. come under this Section. Punishment is life imprisonment.

Note: It may be observed that all acts under S.66 are cognizable and non-bailable offences.

Section 67

This section 67 deals with publishing or transmitting obscene material in electronic form. The earlier Section in ITA was later widened as per ITAA 2008 in which child pornography included. Publishing or transmitting obscene material in electronic form is dealt with here. shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

67A:Publishing images containing sexual acts
67B:Publishing child porn or predating children online

This section deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when combined with the material containing sexually explicit material attract penalty under this Section.

Section 67B :Child Pornography has been exclusively dealt with under this Section. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc or facilitating abusing children online or inducing children to online relationship with one or more children etc come under this Section.

Section 67C:Failure to maintain records

Section 67C fixes the responsibility to intermediaries (such as an ISP) that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment upto three years or fine.

Section 68: Failure/refusal to comply with orders

The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence. Imprisonment up to three years, or/and with fine up to ₹200,000

Section 69: Failure/refusal to decrypt data and 69A

Section 69: This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here.

Section 69A inserted in the ITAA, vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above.

Section 69B

Section 69B discusses the power to authorize to monitor and collect traffic data or information through any computer resource.

Under this ITAA Section, the nominated Government official will be able to listen in to all phone calls, read the SMSs and emails, and monitor the websites that one visited, subject to adherence to the prescribed procedures and without a warrant from a magistrate's order.

The Government represented by the Indian Computer Emergency Response Team, (the National Nodal Agency, as nominated in Section 70B of ITAA) has very rarely exercised.

Section 70B: Securing access or attempting to secure access to a protected system

The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence. Imprisonment up to ten years, or/and with fine.

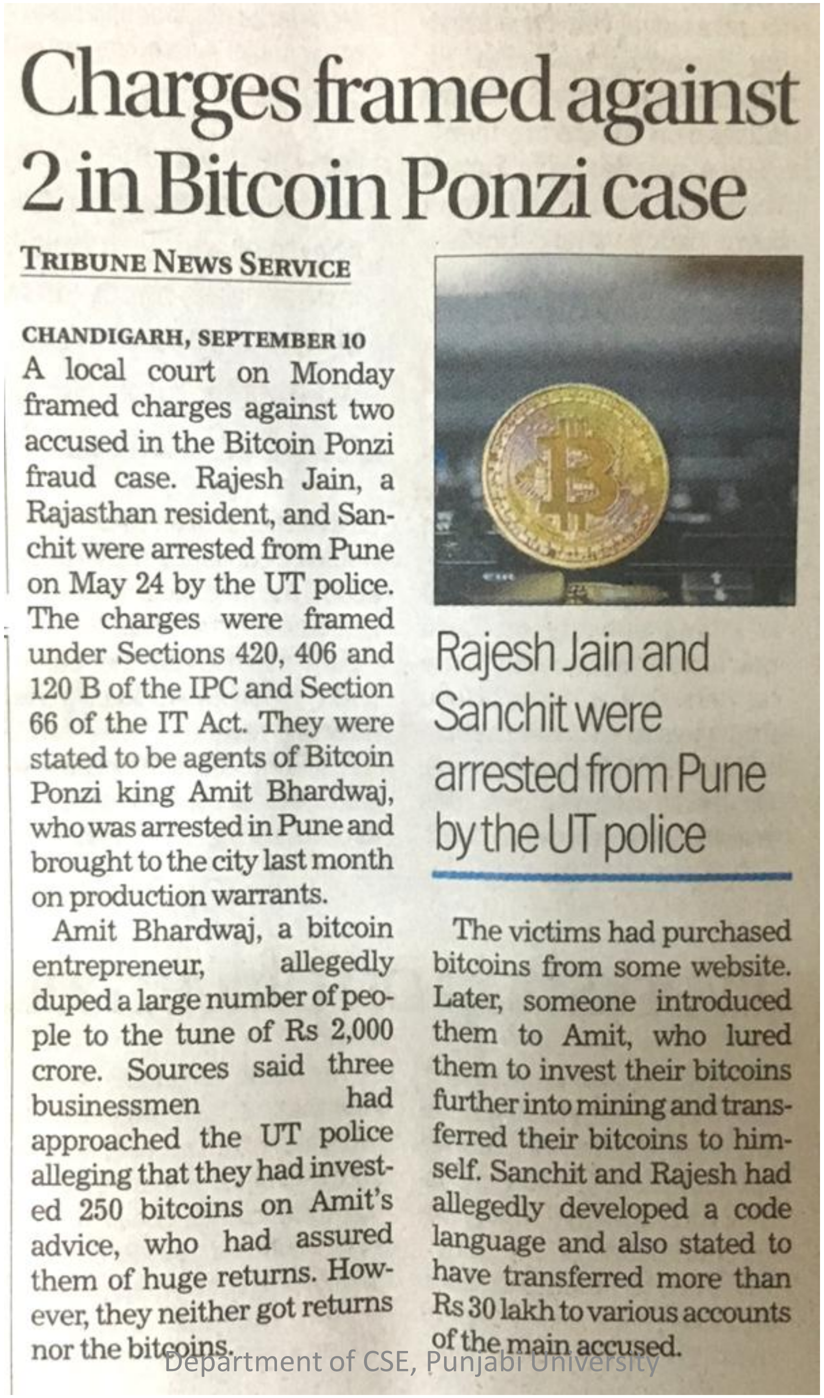
Section relevant to cyber crime under IPC(Indian Penal Code).

ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word ‘electronic’ thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (eg 192, 204,463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records.

Section relevant to cyber crime under IPC(Indian Penal Code).

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Tribune 10 Sept. 2018



Charges framed against 2 in Bitcoin Ponzi case

TRIBUNE NEWS SERVICE

CHANDIGARH, SEPTEMBER 10

A local court on Monday framed charges against two accused in the Bitcoin Ponzi fraud case. Rajesh Jain, a Rajasthan resident, and Sanchit were arrested from Pune on May 24 by the UT police. The charges were framed under Sections 420, 406 and 120 B of the IPC and Section 66 of the IT Act. They were stated to be agents of Bitcoin Ponzi king Amit Bhardwaj, who was arrested in Pune and brought to the city last month on production warrants.

Amit Bhardwaj, a bitcoin entrepreneur, allegedly duped a large number of people to the tune of Rs 2,000 crore. Sources said three businessmen had approached the UT police alleging that they had invested 250 bitcoins on Amit's advice, who had assured them of huge returns. However, they neither got returns nor the bitcoins.

Rajesh Jain and Sanchit were arrested from Pune by the UT police

The victims had purchased bitcoins from some website. Later, someone introduced them to Amit, who lured them to invest their bitcoins further into mining and transferred their bitcoins to himself. Sanchit and Rajesh had allegedly developed a code language and also stated to have transferred more than Rs 30 lakh to various accounts of the main accused.

Case Study

Lottery Fraud and Cyber Squatter

Most of the times we receive electronic mails information that we are going to win or we won a prize in a lottery. To receive lottery money the recipients of letters or e-mails naturally sent their reply. As they will send reply again they will receive another e-mail asking information about bank accounts, mode of transactions they prefer and other confidential information. They do charge money as processing fee before that fund transfer. But that prize in lottery to recipient’s accounts never happened and on the other hand his confidential information, bank accounts etc. may be misused or abused for commission of other crimes.

HSBC, Bangalore Cyber Fraud Case

The accused who was a resident of Bangalore joined HSBC on 12th December 2005 producing forged certificates. He had links with terrorist groups and the underworld groups. He was arrested on charges of data theft and cyber fraud. He committed data theft to illegally transfer money from account of a multinational and the UK based Bank’s customers. HSBC Electronic Data Processing India Pvt. Ltd., Bangalore was the Bank’s BPO arm. They had lodged a complaint with the Cyber Crime Police Station (CCPS) against that cyber fraud. The crime was so dangerous in nature that the HSBC’s technical team from Hyderabad as well as Interpol section of police department became involved to investigate and control it.

Kolkata Cyber Fraud Case

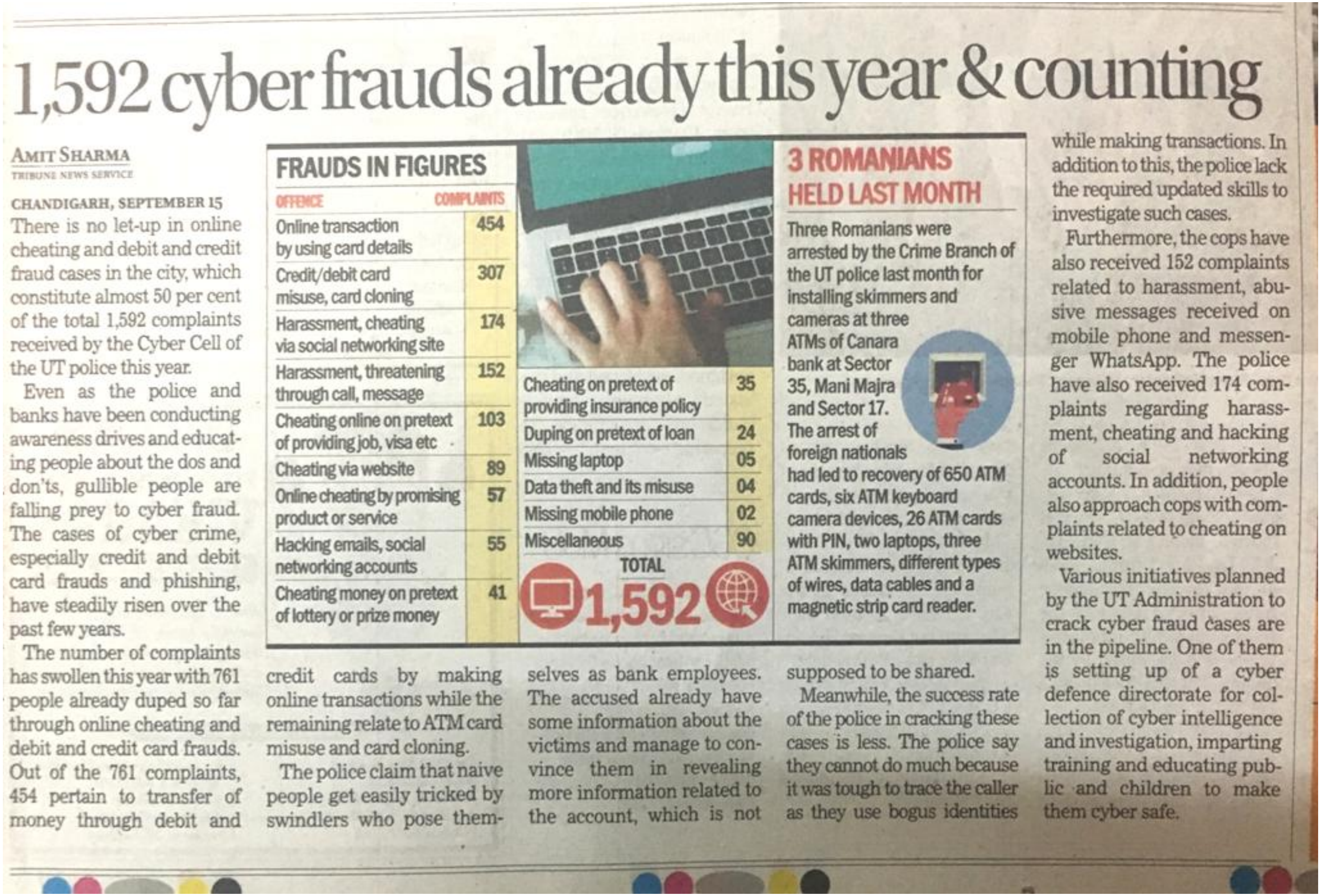
Sulagna Roy, a 23 years old NIFT educated call centre employee committed cyber fraud through calcuttaweb.com. Her nature of work was selling dish TV to US client. During her work she collected credit card information of those clients and then started purchasing more than 52 items worth Rs. 1.8 lakh ($,4,000) by using laptop internet and cyber cafes internet, these items were including jewellery, sarees, chocolate, air-conditioner etc. The calcuttaweb.com provided details of purchases to Detective Department and CID at Kolkata. She only earned Rs. 8,000 monthly but was buying that valuable thing. She was arrested and charged with fraud and cheating. She confessed that she did it for fun but not to commit any intentional crime.

Need of Ethical hacking

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call Ethical Hacking.

The need for more effective information security practices is increasingly evident with each security breach reported in the media. When adopting new technologies like cloud computing, virtualization, or IT outsourcing, enterprises are facing imminent security threats and must adjust their security processes, policies, and architectures accordingly.



1,592 cyber frauds already this year & counting

AMIT SHARMA
TRIBUNE NEWS SERVICE

CHANDIGARH, SEPTEMBER 15

There is no let-up in online cheating and debit and credit fraud cases in the city, which constitute almost 50 per cent of the total 1,592 complaints received by the Cyber Cell of the UT police this year.

Even as the police and banks have been conducting awareness drives and educating people about the dos and don'ts, gullible people are falling prey to cyber fraud. The cases of cyber crime, especially credit and debit card frauds and phishing, have steadily risen over the past few years.

The number of complaints has swollen this year with 761 people already duped so far through online cheating and debit and credit card frauds. Out of the 761 complaints, 454 pertain to transfer of money through debit and credit cards by making online transactions while the remaining relate to ATM card misuse and card cloning.

The police claim that naive people get easily tricked by swindlers who pose themselves as bank employees. The accused already have some information about the victims and manage to convince them in revealing more information related to the account, which is not supposed to be shared.

Meanwhile, the success rate of the police in cracking these cases is less. The police say they cannot do much because it was tough to trace the caller as they use bogus identities while making transactions. In addition to this, the police lack the required updated skills to investigate such cases.

Furthermore, the cops have also received 152 complaints related to harassment, abusive messages received on mobile phone and messenger WhatsApp. The police have also received 174 complaints regarding harassment, cheating and hacking of social networking accounts. In addition, people also approach cops with complaints related to cheating on websites.

Various initiatives planned by the UT Administration to crack cyber fraud cases are in the pipeline. One of them is setting up of a cyber defence directorate for collection of cyber intelligence and investigation, imparting training and educating public and children to make them cyber safe.

FRAUDS IN FIGURES

OFFENCE	COMPLAINTS
Online transaction by using card details	454
Credit/debit card misuse, card cloning	307
Harassment, cheating via social networking site	174
Harassment, threatening through call, message	152
Cheating online on pretext of providing job, visa etc	103
Cheating via website	89
Online cheating by promising product or service	57
Hacking emails, social networking accounts	55
Cheating money on pretext of lottery or prize money	41
Cheating on pretext of providing insurance policy	35
Duping on pretext of loan	24
Missing laptop	05
Data theft and its misuse	04
Missing mobile phone	02
Miscellaneous	90

TOTAL
1,592

3 ROMANIANS HELD LAST MONTH

Three Romanians were arrested by the Crime Branch of the UT police last month for installing skimmers and cameras at three ATMs of Canara bank at Sector 35, Mani Majra and Sector 17. The arrest of foreign nationals had led to recovery of 650 ATM cards, six ATM keyboard camera devices, 26 ATM cards with PIN, two laptops, three ATM skimmers, different types of wires, data cables and a magnetic strip card reader.

Penetration Testing

Penetration Testing is a method that many companies follow in order to minimize their security breaches. This is a controlled way of hiring a professional who will try to hack your system and show you the loopholes that you should fix.

Penetration testing is conducted by professional ethical hackers who mainly use commercial, open-source tools, automate tools and manual checks. There are no restrictions; the most important objective here is to uncover as many security flaws as possible.

Ethical Hacking Steps

Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose and NMAP.

Ethical Hacking Steps

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Ethical Hacking Steps

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Network Mapper (NMAP)

NMAP stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts. Network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets to determine:

- what hosts are available on the network,
- what services those hosts are offering,
- what operating systems they are running on,
- what type of firewalls are in use, and other such characteristics.

NMAP runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

Nmap (Version 7.60) scripts can now perform brute force SSH password cracking, query servers about what auth methods and public keys they accept, and even log in using known or discovered credentials to execute arbitrary commands. We're including four scripts to start out with, and it opens the door to many more future capabilities.

Metasploit

Metasploit is one of the most powerful exploit tools. As an Ethical Hacker, you will be using “Kali Linux Distribution” which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X. Matasploit can be used either with command prompt or with Web UI. To open in Kali, go to Applications -> Exploitation Tools -> metasploit.