Unit-1 Computer and Internet Crime

In this chapter we learn about

- ✓ Introduction to Professional Ethics and Human Values
- ✓ Why Professional Ethics
- ✓ Computer and Internet Crime
- ✓ Vulnerability.
- ✓ Different types of exploits and Security Policies
- ✓ Hacking and penalties of Hacking
- ✓ Recent Scandals and need for Ethics

What are Human Values???

It is a basic moral value one has to possess to live as a human being or citizen.

A value is defined as a principle that promotes well-being or prevents harm.

Values are our guidelines for our success—our paradigm about what is acceptable.

Evolution of Human Values:

The human values evolve because of the following factors:

1. The impact of norms of the society on the fulfillment of the individual's needs or desires.

2. Developed or modified by one's own awareness, choice, and judgment in fulfilling the needs.

3. By the teachings and practice of Preceptors (Gurus) or Saviors or religious leaders.

4. Fostered or modified by social leaders, rulers of kingdom, and by law (government)

Value Systems

Values are the unarticulated beliefs that form the foundation for ethical behavior, i.e. practices that are viewed by our society as correct behavior. As an Engineer, you should acknowledge the fundamental importance of the following values both for yourself and your profession:

Quality of life, Health, human potential, Empowerment, growth and excellence, Freedom and responsibility, Justice Dignity, integrity, worth and fundamental rights All-win attitudes and cooperation, Authenticity and openness Effectiveness, efficiency and alignment, Holistic, systemic view and affected parties orientation

Professional Ethics

Profession is a commitment to a designated and organized occupation by virtue of being an authority over a body of knowledge with requisite skills acquired through specialized training.

An occupation becomes a profession when a group of people sharing the same occupation work together in a morally acceptable way with members setting and following a certain ethics code.

A professional is a practitioner belonging to a specific profession.

Professional ethics, as opposed to personal values and morality, is a set of ethical standards and values a practicing engineer is required to follow.

It sets the standards for professional practice, and is only learned in a professional school or while practicing one's own profession.

(WHY PROFESSIONAL ETHICS?)

(a) To understand the moral values that ought to guide the profession,

(b) Resolve the moral issues in the profession, and

(c) Justify the moral judgment concerning the profession.

It is intended to develop a set of beliefs, attitudes, and habits that engineers should display concerning morality.

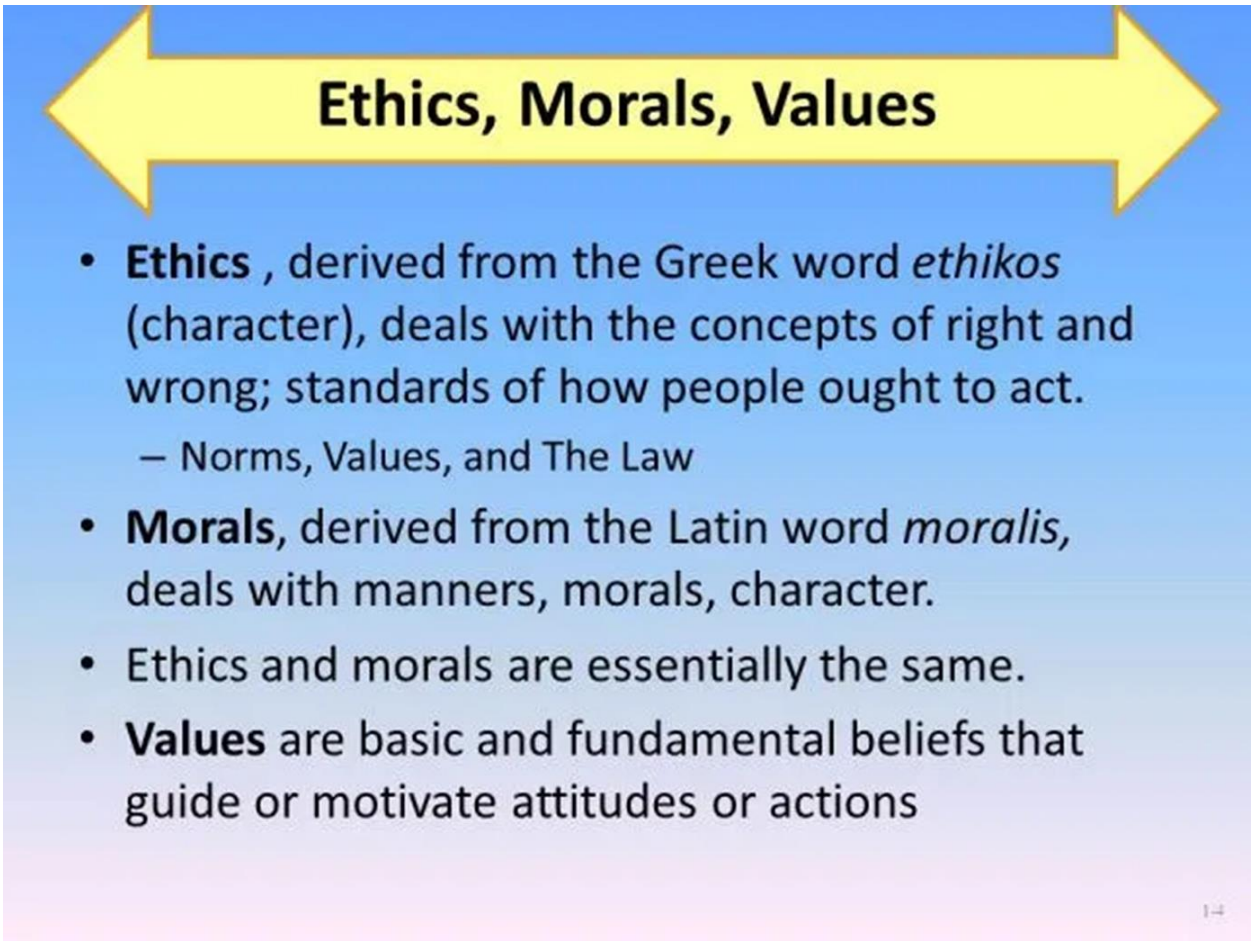
The prime objective is to increase one's ability to deal effectively with moral complexity in managerial practice.

Morals and Values

What are Morals?
Guiding principles that every human being should have.
It is knowledge of difference between right and wrong

What are Values??

Values are individual in nature. Values are "things that have an intrinsic worth in usefulness or importance to the possessor.



Computer Crimes

A computer crime is any unlawful activity that is done using a computer.

Computer Crimes are also called as Cyber Crimes.

The First Incident of Cyber Crime

The first major computer crimes came into being in the 1960's when a group of hackers emerged from Massachusetts Institute of Technology.

The first virus came into being in 1981. It was created on the Apple II operating software and was spread through floppy disk, containing the operating software.

Various types of Cyber Crimes are

1. Viruses and Worms

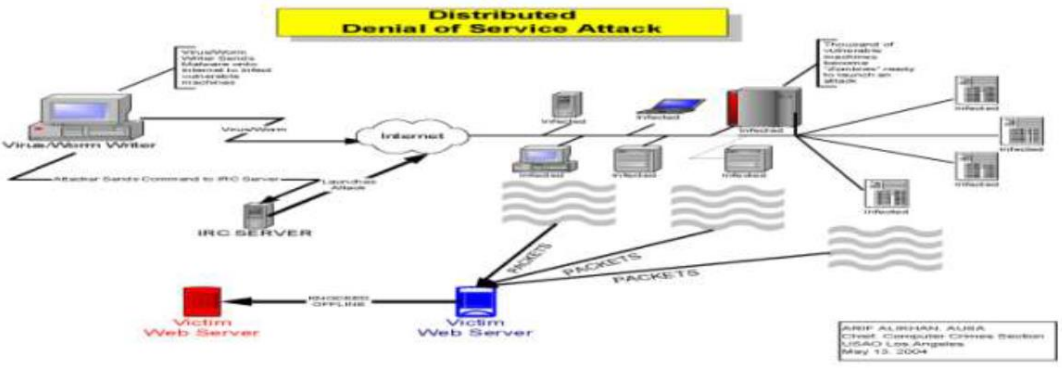
Viruses are programs that attach themselves to a computer or a file. They then circulate themselves to other files and to other computers on a network.

Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Examples of virus and worms are
Blaster, Slammer, Nimda, Code Red, ILOVEYOU. The Morris Worm, Elk Cloner.

2. Denial-of-Service-Attacks

These attacks occur when a person or a group of people try to prevent an internet site from functioning effectively either temporarily or on a long term basis.



3. Malware

Malware means malicious software. It is designed to secretly access an individual's computer without his/her permission. Most malware are software's created with the intent of stealing data. Using these software's, which are usually disguised as harmless pop-ups and such, information about the users is collected without their knowledge.

Hacking

Hacking is unauthorized access over a computer system, and it usually involves modifying computer hardware or software to accomplish a goal outside the creator's purpose.

5. Software Piracy

Unauthorized copying of purchased software is called software piracy. Making copies of the software for commercial distribution, or resale is illegal. However software piracy is still rampant around the globe, because it is almost impossible to put an end to it.

6. Fraud

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space.

Some of the cases of online fraud and cheating that have come to light are those relating to credit card crimes, bank fraud, contractual crimes, internet scams, identity theft, extortion etc.

7. Cyber stalking

Cyber stalking involves following a person's movements across the Internet by posting threatening messages on the bulletin boards frequented by the victim, entering the chat rooms frequented by the victim, and constantly bombarding the victim with emails.

8. Obscene or Offensive Content

Includes contents of websites that may be distasteful, obscene, or offensive in many ways. One of the major victims of this type of crime is child pornography.Child pornography includes sexual

images involving children under puberty, puberty, and post-puberty and computer generated images that appear to involve them in sexual acts.

9. Harassment

Any comment that may be considered degratory or offensive is considered harassment. Harassment via the internet occurs in chat rooms, social networking sites, and emails.

10. Trafficking

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms or weapons. These forms of trafficking are carried on under pseudonyms, encrypted emails, and other internet technology.

11. Computer Vandalism

Vandalism means deliberately destroying or damaging property of another. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer, or by physically damaging a computer or its peripherals.

12. Spam

The unwanted sending of bulk e-mail for commercial purposes is called spam. Although this is a relatively minor crime, recently new antispam laws have cropped up to restrict the sending of these e-mails.

Prevention of Computer Crime

Always use latest and updated antivirus software's to guard against virus attacks.

Avoid sending photographs online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

Web site owners should watch internet traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

Use a security program that gives control over the cookies and sends information back to the site, as leaving the cookies unguarded might prove fatal.

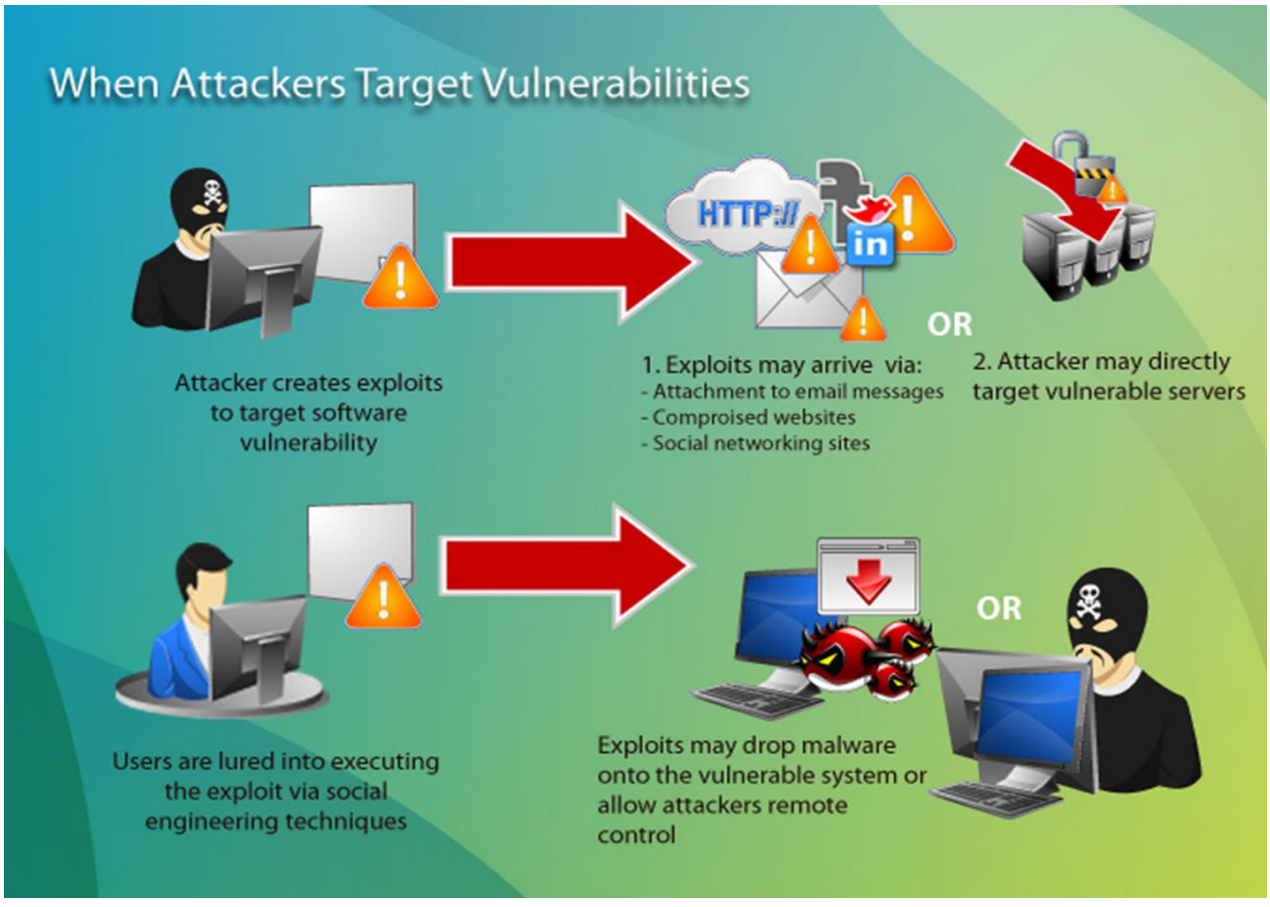
Vulnerability

Vulnerability refers to the inability to withstand the effects of a hostile environment.

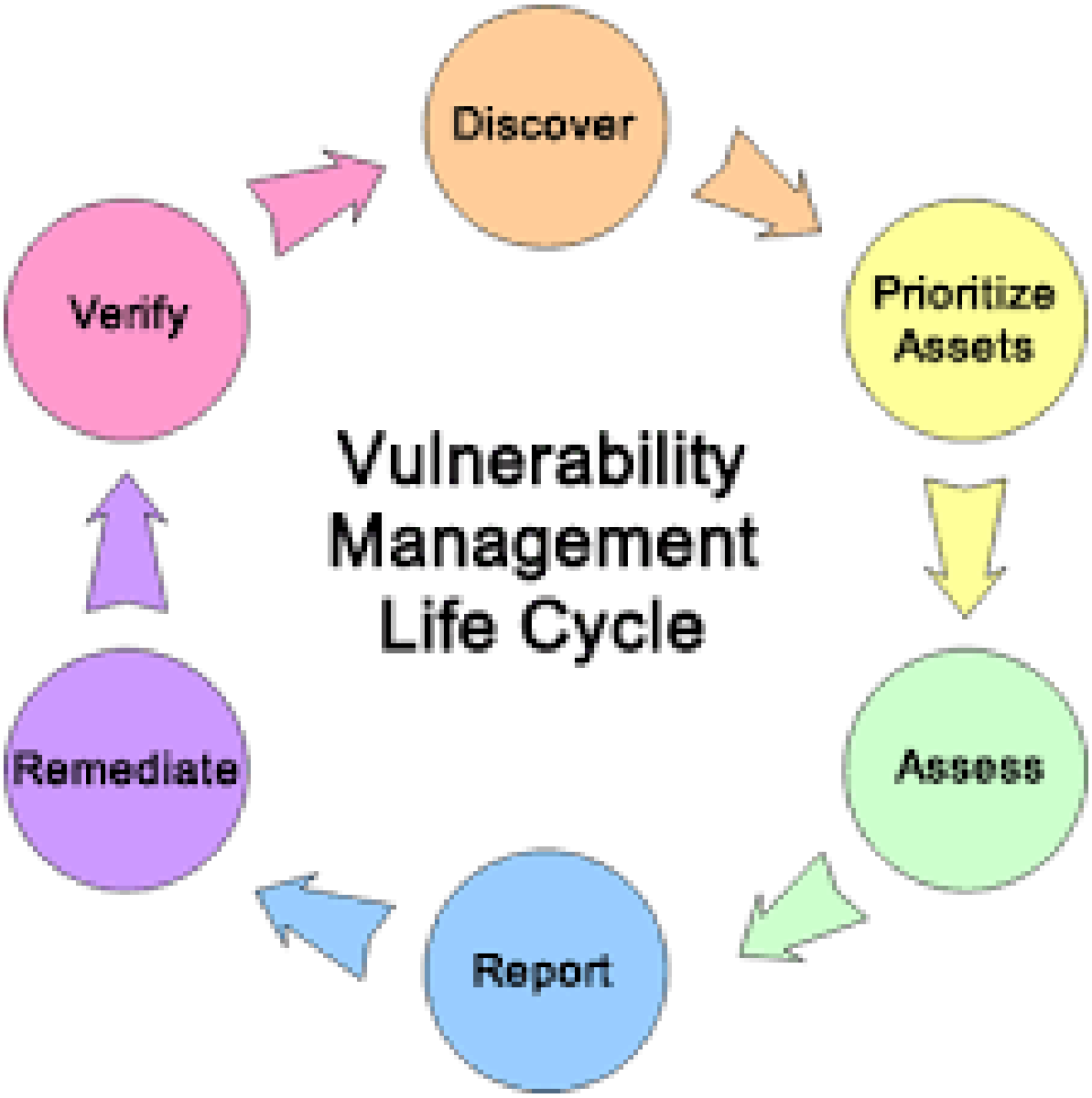
The discovery of system vulnerabilities within the software and operating system is inevitable within the information technology (IT) industry.

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack.

Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.
The Life Cycle of Vulnerability can be depicted as:



The Life Cycle of Vulnerability can be depicted as:



Hacking

Computer systems and the internet are characterized by anonymity. This haven of anonymity permits cybercrimes of various types.

Computer hacking is defined as the deliberate access or infiltration of a computer system or program without authorization. It is also the intentional access to a computer system or program exceeding authorized access.

A person commits a “computer crime” when he or she:

1. Accesses a computer system without authorization;

2. Accesses or uses a computer system to obtain unauthorized computer services (including computer access, data processing, and data storage);

3. Intentionally or recklessly disrupts, degrades, or causes disruption or degradation of computer services or denies or causes denial of computer services to an authorized user; or

4. Intentionally or recklessly tampers with, takes, transfers, conceals, alters, or damages any equipment used in a computer system.

It is also a computer crime to misuse computer system data.

The punishment for committing one of these computer crimes depends on the damage caused and risk of harm created.

What is unauthorized access or use?

UNAUTHORIZED USE OF COMPUTER OR COMPUTER NETWORK

It is a crime to use a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove, halt, or disable computer data, programs, or software;

2. Cause a computer to malfunction;

3. Alter or erase computer data, programs, or software;

4. Create or alter a financial instrument or an electronic funds transfer;

5. Cause physical injury to another's property;

6. Make or cause to be made an unauthorized copy of computer data, programs, or software residing in, communicated by, or produced by a computer or computer network;

Depending on the circumstances, a person who hacks into another's computer could be punished by a number of generally applicable crimes.

For example, if the hacking is done to take personal identifying information for certain purposes, it could be punishable as identity theft.

What is Ethical Hacking???

Ethical hacking is a branch of study where computer security experts (ethical hackers/white hat hackers) find the vulnerabilities and weaknesses of a system with the permission of the owner of the system who is responsible for fixing of vulnerability.

So it can be called a good hacking which finds out any probable way to hack the system and fixes it before it is hacked by black hat hackers.

Ethical hacking is also known as penetration testing, intrusion testing, or red teaming but it is not only limited to penetration testing.

If hacking is offensive, ethical hacking is defensive.

Need of Ethical Hacking

India is ranked third among countries which are facing highest number of cyber threats as per security software firm Symantec. The same research also ranked second in terms of targeted attacks.

Incidents of Hacking

There have been numerous hacking attacks on Indian government websites where state government websites or defense websites have been hacked.

Principal Controller of defense accounts website was hacked due to which defense officials could not access their salary information.

The government, to reduce hacking of precise work, has agreed to the proposal of DEITY, which is the department of information and technology to stop using popular email ids for official purpose and has sanctioned a budget of Rs. 100 cores to safeguard the data.

In the infamous case of Amit Tiwari, who was a global hacker, he has hacked more than 950 accounts since 2003 and was caught by the police only in 2014. This shows the lack of evidence and the difficulty in arresting a hacker.

Some of the real scandals or data breaches in Computer Industry

Marriott International

Date: 2014-18

Impact: 500 million customers

Details: In November 2018, Marriott International announced that cyber thieves had stolen data on approximately 500 million customers.

The breach actually occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

Adult Friend Finder

Date: October 2016

Impact: More than 412.2 million accounts

Details: The FriendFinder Network, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached sometime in mid-October 2016. Hackers collected 20 years of data on six databases that included names, email addresses and passwords.

eBay

Date: May 2014

Impact: 145 million users compromised

Details: The online auction giant reported a cyberattack in May 2014 that it said exposed names, addresses, dates of birth and encrypted passwords of all of its 145 million users.

The company said hackers got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database.

Uber

Date: Late 2016

Impact: Personal information of 57 million Uber users and 600,000 drivers exposed.

The company learned in late 2016 that two hackers were able to get names, email addresses, and mobile phone numbers of 57 users of the Uber app. They also got the driver license numbers of 600,000 Uber drivers.

No other data such as credit card or Social Security numbers were stolen. The hackers were able to access Uber's GitHub account, where they found username and password credentials to Uber's AWS account. Those credentials should never have been on GitHub.

Data breaches/Hacks in India

The Big Phone Hack

The recent WhatsApp breach targeting dissident Indians with spyware underlines the possibility of a wider vulnerability.

Late in the evening on October 28, 2019, Delhi-based freelance journalist Rajeev Sharma received a phone call. The caller identified himself as John Hilton, a researcher from CitizenLab, a Canada-based Internet Research agency. Sharma was warned that his phone had been under surveillance for two weeks until May 2019. He was not alone. It turns out that the phones of

several dozen Indian journalists, lawyers and activists were hacked using an invasive Israeli-developed malware.

LinkedIn was hacked in the year 2016 and some 6.5 million accounts are said to have been affected. However, four years later, in May 2016, the company said that many more users were affected by the breach.

In September 2016, email and password data of 68 million **Dropbox users** was found selling on the darknet marketplace. The dataset was claimed to be part of a 2012 hacking attack. The company sent out emails to affected users asking them to reset their passwords. According to Motherboard website, in all the details of 68,680,741 accounts was stolen.

Facebook is facing one of the biggest scandals in its history. The company is under fire for 'improperly sharing' user's personal data with a UK-based company called Cambridge Analytica. The data is said to have been used later to influence US election results.

In the year 2018, **Facebook** claimed that in all some 87 million users have been affected by the data breach. As for India, as per the social networking company, the figures stand at approximately 562,120 people.

Restaurant app **Zomato** suffered a major security breach in May 2017 when data of some 17 million users was stolen.

Hackeread.com claimed that a user by the name of "nclay" claimed to have hacked Zomato and was offering data of some 17 million registered Zomato users on darkweb marketplace.

Zomato had acknowledged the hacking attack, however, claimed that no payment information or credit card data was stolen/leaked.