CYBER SECURITY

UNIT - I

INTRODUCTION OF CYBERCRIME

K. BALAKRISHNA

B.TECH., MBA., M.TECH., DID., (PH.D)

TOPICS

1. Definition and Origins of the Word
2. Cybercrime and Information Security
3. Who are Cybercriminals?
4. Classifications of Cybercrimes
5. Cybercrime Era: Survival mantra for the Netizens

1. DEFINITION AND ORIGINS OF THE WORD

- The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.

- There're two sides to a coin. Internet also has it's own disadvantages. One is Cyber crime- illegal activity committed on the internet.

- *In 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.* ***This is the first recorded cyber crime!***

WHAT IS CYBERCRIME?

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.
- ***"Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them".***

Hence all criminal activities done using the medium of computers, the Internet, cyberspace and the WWW. Cybercrime can sometimes be called as *computer-related crime, computer crime, E-crime, Internet crime, High-tech crime*….

TYPES OF ATTACKS

Techno - crime : *Active attack*

- Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the *deletion, corruption, alteration, theft or copying of data on an organization's systems*.
- Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.

Techno – vandalism: *Passive attack*

- Techno Vandalism is a term used to describe *a hacker or cracker* who breaks into a computer system with the *sole intent of defacing and or destroying its contents*.
- Techno Vandals can deploy *'sniffers'* on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is! The best weapon against such attacks is a firewall which will hide and disguise your organization's presence on the Internet.

CYBER CRIMES IN INDIA

Total number of cyber crime cases recorded

2018	2019	2020
27248	44735	50035

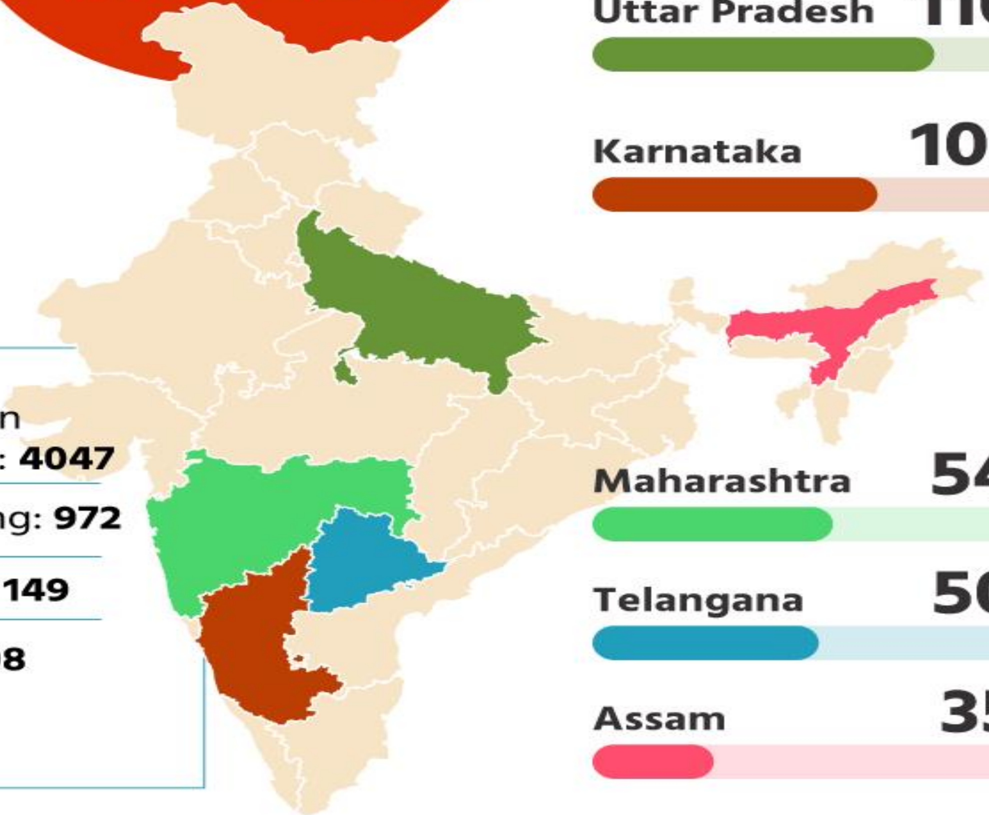
11.8% surge seen in 2020 as compared to previous year

Rate of cyber crime (incidents per lakh population)

2020	3.7%
2019	3.3%

Types of Crime reported

- Online banking fraud: **4047**
- OTP frauds: **1093**
- Credit/Debit card fraud: **1194**
- Cases related to ATM: **2160**
- Fake news on social media: **4047**
- Cyber stalking: **972**
- Fake profile: **149**
- Data theft: **98**



State wise reporting of cases:

Uttar Pradesh	11097
Karnataka	10741
Maharashtra	5496
Telangana	5024
Assam	3530

2. CYBERCRIME AND INFORMATION SECURITY

- Lack of information security gives rise to cybercrime!
- ***Cyber Security*** *means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.*

Challenges for securing data in business perspective:

- Cybercrimes occupy an important space in information security due to their impact.
- Most organizations do not incorporate the cost of the vast majority of computer security incidents into their accounting
- The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost
- Financial loses may not be detected by the victimized organization in case of Insider attacks such as leaking customer data.

3. WHO ARE CYBERCRIMINALS

Are those who conduct acts such as:

- *Child pornography*
- *Credit card fraud*
- *Cyberstalking*
- *Defaming another online*
- *Gaining unauthorized access to computer systems*
- *Ignoring copyrights*
- *Software licensing and trademark protection*
- *Overriding encryption to make illegal copies*
- *Software piracy*
- *Stealing another's identity to perform criminal acts*

CATEGORIZATION OF CYBERCRIMINALS

Type 1: Cybercriminals - Hungry for recognition:

- Hobby hackers
  - A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software.
- IT professional(social engineering):
  - Ethical hacker
- Politically motivated hackers :
  - Promotes the objectives of individuals, groups or nations supporting a variety of causes such as : Anti globalization, transnational conflicts and protest.
- Terrorist organizations
  - Cyber Terrorism
  - Use the internet attacks in terrorist activity
  - Large scale disruption of computer networks , personal computers attached to internet via viruses

CATEGORIZATION OF CYBERCRIMINALS

Type 2: Cybercriminals - Not interested in recognition!

- Psychological perverts
  - Express sexual desires, deviates from normal behavior
  - Poonam panday
- Financially motivated hackers
  - Make money from cyber attacks
  - Bots-for-hire : fraud through phishing, information theft, spam and extortion
- State-sponsored hacking
  - Hacktivists
  - Extremely professional groups working for governments
  - Have ability to worm into the networks of the media, major corporations, defense departments

CATEGORIZATION OF CYBERCRIMINALS

Type 3: Cybercriminals - the insiders

- Disgruntled former employees seeking revenge
- Competing companies using employees to gain economic advantage through damage and/ or theft.

Motives behind cybercrime:

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset
- Desire to sell network security services

4. CLASSIFICATION OF CYBERCRIMES

a. Cybercrime against an individual

b. Cybercrime against property

c. Cybercrime against organization

d. Cybercrime against Society

e. Crimes emanating from Usenet newsgroup

a. Cybercrime against an individual:

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- Password Sniffing

b. Cybercrime against property:

- Credit card frauds
- Intellectual property(IP) crimes
- Internet time theft

c. Cybercrime against organization:

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- E-Mail bombing/mail bombs
- Salami attack/ Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Industrial spying/ industrial espionage
- Computer network intrusions
- Software piracy

d. Cybercrime against Society:

- Forgery
- Cyber Terrorism
- Web jacking

e. Crimes emanating from Usenet newsgroup:

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are deceptive in another way
- Hence service at your own risk

HISTORY OF USENET GROUPS

- In 1979 it was developed by two graduate students from Duke University in North Carolina (UNC) as a network that allowed users to exchange quantities of information too large for mailboxes.
- Usenet was designed to facilitate textual exchanges between scholars.
- Slowly, the network structure adapted to allow the exchange of larger files such as videos or images.
- Usenet newsgroups constitute one of the largest source of child pornography available in cyberspace.
- This source useful for observing other types of criminal or particular activities: online interaction between pedophiles, adult pornographers and writers of pornographic stories.
- Usenet for sharing illegal content.

E-MAIL SPOOFING

- A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source. i.e., It is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency.

E-MAIL SPOOFING

- Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks.
- For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.
- The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.
- One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.

SPAMMING

- People who create electronic spam : **spammers**
- **Spam** is abuse of electronic messaging systems to send unsolicited bulk messages or mass e-mails such as chain letters indiscriminately.
- Spamming may be:
  - E-Mail Spam
  - Instant messaging spam
  - Usenet group spam
  - Web search engine spam
  - Spam in blogs, wiki spam
  - Online classified ads spam
  - Mobile phone messaging spam
  - Internet forum spam
  - Junk fax spam
  - Social networking spam

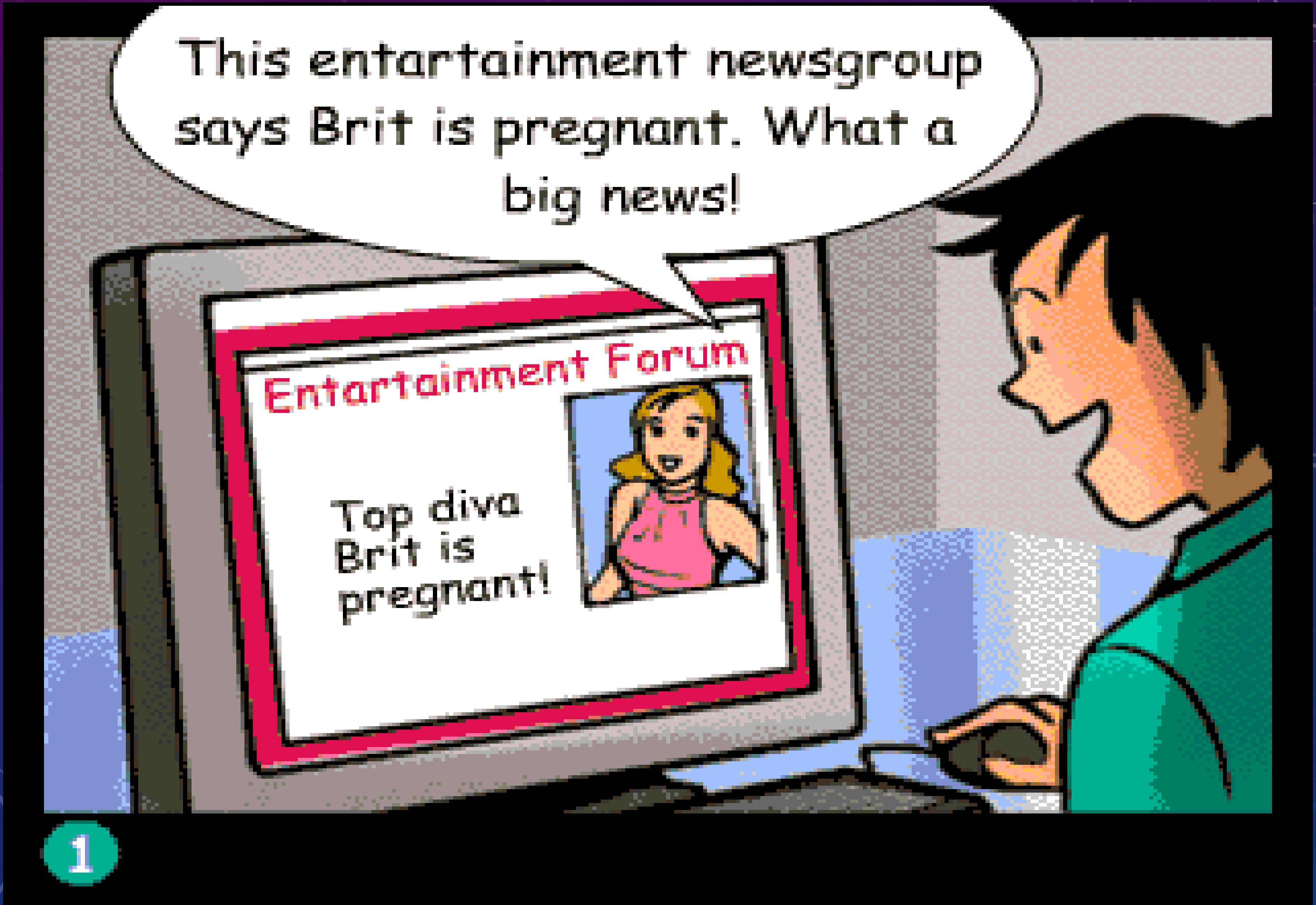
SPAMMING

- Spamming is difficult to control
- Advertisers have no operating costs beyond the management of their mailing lists
- It is difficult to hold senders accountable for their mass mailings
- Spammers are numerous

Search engine spamming:

- Alteration or creation of a document with the intent to deceive an electronic catalog or a filing system
- some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- Remedy: permanently exclude from the search index

CYBER DEFAMATION


This entartainment newsgroup says Brit is pregnant. What a big news!
Entartainment Forum
Top diva Brit is pregnant!
1

CYBER DEFAMATION

Cyber defamation, also known as online defamation, is when someone is falsely accused of something online. Cyber defamation is the use of the internet or a computer to damage another person's reputation or diminish one's own reputation in the eyes of others.

Hey, I read on wikipedia that your mom —
Funny, 'cause the version I read had your mom's photo.

- Example: someone publishes defamatory matter about someone on a website or sends an E-mail containing defamatory information to all friends of that person.

CYBER DEFAMATION

It may amount to defamation when-

- If imputation to a deceased person would harm the reputation of that person, and is intended to be hurtful to the feelings of his family or other near relatives.
- An imputation is made concerning a company or an association or collection of people as such.
- An imputation in the form of an alternative or expressed ironically.
- An imputation that directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

CYBER DEFAMATION

Types of defamation:

- Libel : written defamation
- Slander: oral defamation
- The plaintiff must have to show that the defamatory statements were unlawful and would indeed injure the person's or organization's reputation.
- When failed to prove, the person who made the allegations may still be held responsible for defamation.

INTERNET TIME THEFT

- Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.
- The person get access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means and uses the internet without the other person’s knowledge.
- This theft can be identified when Internet time is recharged often, despite infrequent usage.
- This comes under “identity theft”.

SALAMI ATTACK/ SALAMI TECHNIQUE

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed.

- An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

Examples:

- Small “shavings” for Big gains!
- The petrol pump fraud

DATA DIDDLING

- Data diddling involves changing data input in a computer. In other words, information is changed from the way it should be entered by a person typing in the data.
- Usually, a virus that changes data or a programmer of the database or application has pre-programmed it to be changed.
- For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.
- To deal with this type of crime, a company must implement policies and internal controls.
- This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

Ex: Electricity board in India have been victims to data diddling programs inserted when private parties computerized their systems.

FORGERY

- The act of forging something, especially the unlawful act of counterfeiting a document or object for the purposes of fraud or deception.
- Something that has been forged, especially a document that has been copied or remade to look like the original.
- Counterfeit currency notes, postage, revenue stamps, mark sheets, etc., can be forged using sophisticated computers, printers and scanners.

Real life case:

- **Stamp Paper Scam – a racket that flourished on loopholes in the system**
- Abdul Karim Telgi, the mastermind of the multi-crore counterfeiting, printed fake stamp papers worth thousands of crores of rupees using printing machines purchased illegally with the help of some conniving officials of the Central Govt.'s Security Printing Press (India Security Press) located in Nasik. These fake stamp papers penetrated in more than 12 states through a widespread network of vendors who sold the counterfeits without any fear and earned hefty commissions.
- **Amount swindled** Rs. 172 crores
- Telgi is in jail serving his 13 plus 10 years term

WEB JACKING

- This term is derived from the term hi jacking.
- In these kinds of offences the hacker gains access and control over the web site of another.
- He may even change the information on the site.
- The first stage of this crime involves “password sniffing”.
- The actual owner of the website does not have any more control over what appears on that website
- This may be done for fulfilling political objectives or for money.

Real Life Examples:

- Recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein.
- Further the site of Bombay crime branch was also web jacked.
- Another case of web jacking is that of the ‘gold fish’ case. In this case the site was hacked and the information pertaining to gold fish was changed.

INDUSTRIAL SPYING/ INDUSTRIAL ESPIONAGE

- Industrial espionage is the covert and sometimes illegal practice of investigating competitors to gain a business advantage. The target of investigation might be a trade secret such as a proprietary product specification or formula, or information about business plans.
- In many cases, industrial spies are simply seeking any data that their organization can exploit to its advantage.

Real Life Cases:

- A Chinese Trojan horse email campaign targeted some 140 senior Israeli defense corporation employees (2013) involved in highly classified, sensitive security projects. The email was made to appear as if it came from a known German company that regularly works with the Israeli defense industry.
- However, it turned out to contain a Trojan horse, which, according to the report, attempted to funnel information from the recipients' computers. The Trojan horse was noticed by computer defense systems and shut down.
- The defense establishment then realized how many Israelis received the email, and reportedly tracked the malicious program down to Chinese defense industries.The incident led security companies to reiterate to employees computer security guidelines.

HACKING

Every act committed towards breaking into a computer and/ or network is called hacking.

Purpose of hacking:

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

HACKING

- *Hacking* is any technical effort to manipulate the normal behavior of network connections and connected systems.
- A *hacker* is any person engaged in hacking.
- The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems.
- M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking.
- The so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.
- Later, outside of M.I.T., others began applying the term to less honorable pursuits. For example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally.
- As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

HACKING VS. CRACKING

- Hacking is the act of compromising digital devices to gain unauthorized access. Although the media commonly uses the term “hacking” to refer to illegal activities, people in the hacking community generally consider themselves the good guys, while crackers are the bad guys.
- This is because, in the hacking community, the goal of hacking is to improve or alter security systems and programs.
- Cracking is a technique that is used to break into computer software, systems, or networks with malicious intent. In the same way that a bank robber might crack a safe, a “cracker” breaks into a digital device or program.
- There are several types of cracking, and crackers employ many different techniques to break into computer systems and software. However, the three most common forms of cracking are password cracking, software cracking, and web cracking.

Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have advanced knowledge of computers OS and programming languages.	They may or may not be skilled, some crackers just know a few tricks to steal data.
They work in an organization to help protect their data and give them expertise in internet security.	These are the person from which hackers protect organizations.
Hackers share the knowledge and never damages the data.	If they found any loophole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benefit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for their cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as their motive is to stay anonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers.

TYPES OF MODERN HACKERS

- **Hackers fall into three general categories: black hat hackers, white hat hackers, and gray hat hackers.** Although hackers are often associated with exploiting vulnerabilities to gain unauthorized access to computers, systems, or networks, not all hacking is malicious or illegal. In its purest sense, hacking is simply the application of computer skills to solve a particular problem.

Black hat hackers:

- Black hat hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it, often by implanting a virus or other type of malware such as a trojan.

White hat hackers:

- White hat hackers are ethical security hackers who identify and fix vulnerabilities. Hacking into systems with the permission of the organizations they hack into, white hat hackers try to uncover system weaknesses in order to fix them and help strengthen a system’s overall security.

TYPES OF MODERN HACKERS

Gray hat hackers:

- Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don't have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But gray hat hackers may demand payment in exchange for providing full details of what they uncovered.

Other types of hackers:

Although nearly all hackers fall into one of the three categories (black hat, white hat, or gray hat), there are other types and sub-types of hackers.

- **Green hat hackers:** Green hat hackers are "green" in the sense that they're inexperienced and may lack the technical skills of more experienced hackers. Green hats may rely on phishing and other social engineering techniques to bypass security systems.
- **Blue hat hackers:** Blue hat hackers are white hat hackers who are actually employed by an organization to help improve their security systems by conducting penetration tests.
- **Red hat hackers:** Also known as vigilante hackers, red hat hackers are motivated by a desire to fight back against black hat hackers, but they do this by infiltrating black hat communities on the dark web and launching hacking attacks against their networks and devices.

REAL LIFE CASE : DEC 2009
NASA SITE HACKED VIA SQL INJECTION

- Two NASA sites recently were hacked by an individual wanting to demonstrate that the sites are susceptible to SQL injection.
- The websites for NASA's Instrument Systems and Technology Division and Software Engineering Division were accessed by a researcher, who posted to his blog screen shots taken during the hack.
- The researcher, using the alias "c0de.breaker," used SQL injection to hijack the sites.
- SQL injection is an attack process where a hacker adds additional SQL code commands to a page request and the web server then tries to execute those commands within the backend database
- The NASA hack yielded the credentials of some 25 administrator accounts.
- The researcher also gained access to a web portal used for managing and editing those websites.
- In this particular case, the researcher found the vulnerabilities, made NASA aware of them, then published findings after the websites had been fixed.
- An attacker, however, could have tried to use that web server as an entry point into other systems NASA might control or edit the content of the sites and use them for drive-by downloads.

ONLINE FRAUDS

- Fraud that is committed using the internet is “online fraud.” Online fraud can involve financial fraud and identity theft.
- Online fraud comes in many forms.
  - viruses that attack computers with the goal of retrieving personal information, to email schemes that lure victims into wiring money to fraudulent sources,
  - “phishing” emails that purport to be from official entities (such as banks or the Internal Revenue Service) that solicit personal information from victims to be used to commit identity theft,
  - to fraud on online auction sites (such as Ebay) where perpetrators sell fictional goods.
  - E-Mail spoofing to make the user to enter the personal information : financial fraud
  - Illegal intrusion: log-in to a computer illegally by having previously obtained actual password. Creates a new identity fooling the computer that the hacker is the genuine operator. Hacker commits innumerable number of frauds.

PORNOGRAPHIC OFFENSES: CHILD PORNOGRAPHY

Means any visual depiction, including but not limited to the following:

1. Any photograph that ca be considered obscene and/ or unsuitable for the age of child viewer.
2. Film ,video, picture;
3. Obscene Computer generated image or picture

HOW DO THEY OPERATE

1. Pedophiles use false identity to trap the children/teenagers
2. Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
3. Befriend the child/teen.
4. Extract personal information from the child/teen by winning his confidence.
5. Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address as well.
6. Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
7. Extract personal information from child/teen
8. At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

SOFTWARE PIRACY

- Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- End-user copying
- Hard disk loading with illicit means
- Counterfeiting
- Illegal downloads from internet

Buying Pirated software have a lot to lose:

- Getting untested software that may have been copied thousands of times.
- Potentially contain hard-ware infecting viruses
- No technical support in case of software failure
- No warranty protection
- No legal right to use the product

COMPUTER SABOTAGE

- Computer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracies through viruses, worms, logic bombs.

Chernobyl virus

- The Chernobyl virus is a computer virus with a potentially devastating payload that destroys all computer data when an infected file is executed.,

Y2K virus

- **Y2K bug,** also called Year 2000 bug or Millennium Bug, a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000.

E-MAIL BOMBING/MAIL BOMBS

- In Internet usage, an *email bomb* is a form of net abuse consisting of sending huge volumes of *email* to an address in an attempt to overflow the mailbox or overwhelm the server where the *email* address is hosted in a denial-of-service attack.
- Construct a computer to repeatedly send E-mail to a specified person's E-mail address.
- Can overwhelm the recipient's personal account and potentially shut down the entire system.

COMPUTER NETWORK INTRUSIONS

- An intrusion to computer network from any where in the world and steal data, plant viruses, create backdoors, insert trojan horse or change passwords and user names.
- An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

PASSWORD SNIFFING

- Password sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site.
- Through sniffers installed, anyone can impersonate an authorized user and login to access restricted documents.

CREDIT CARD FRAUDS

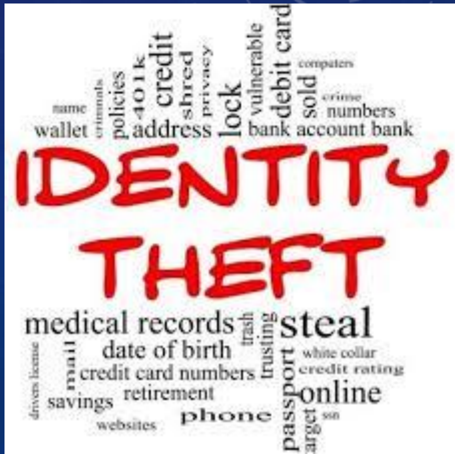
- **Credit card fraud** is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.
- Credit card fraud is also an adjunct to identity theft.

IDENTITY THEFT

- Identity theft is a fraud involving another person's identity for an illicit purpose.
- The criminal uses someone else's identity for his/ her own illegal purposes.
- Phishing and identity theft are related offenses.

Examples:

- Fraudulently obtaining credit
- Stealing money from victim's bank account
- Using victim's credit card number
- Establishing accounts with utility companies
- Renting an apartment
- Filing bankruptcy using the victim's name



REAL LIFE CASES

- **Dr. Gerald Barnes**
  Gerald Barnbaum lost his pharmacist license after committing Medicaid fraud. He stole the identity of Dr. Gerald Barnes and practiced medicine under his name. A type 1 diabetic died under his care. "Dr. Barnes" even worked as a staff physician for a center that gave exams to FBI agents. He's currently serving hard time.
- **Andrea Harris-Frazier**
  Margot Somerville lost her wallet on a trolley. Two years later she was arrested. Andrea Harris-Frazier had defrauded several banks—using Somerville's identity—out of tens of thousands of dollars. The real crook was caught.
- **Abraham Abdallah**
  A busboy named Abraham Abdallah got into the bank accounts of Steven Spielberg and other famous people after tricking his victims via computer, getting sufficient data to fake being their financial advisors—then calling their banks…and you know the rest.

CYBERCRIME: THE LEGAL PERSPECTIVE

- Cybercrime possess a mammoth challenge
- Computer crime: Criminal Justice Resource Manual(1979)
  - Any illegal act for which knowledge of computer technology is essential for a successful prosecution.
- International legal aspects of computer crimes were studied in 1983
  - Encompasses any illegal act for which the knowledge of computer technology is essential for its prepetration

CYBERCRIME: THE LEGAL PERSPECTIVE

- The network context of cyber crime make it one of the most globalized offenses of the present and most modernized threats of the future.
- Solution:
  - Divide information system into segments bordered by state boundaries.
    - Not possible and unrealistic because of globalization
  - Or incorporate the legal system into an integrated entity obliterating these state boundaries.

CYBERCRIME: INDIAN PERSPECTIVE

- India has the fourth highest number of internet users in the world.
- 45 million internet users in India
- 37% - in cyber cafes
- 57% are between 18 and 35 years
- The Information Technology (IT) Act, 2000, specifies the acts which are punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T.
- 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year (2006)
- Thereby reporting an increase of 52.8% in 2007 over 2006.
- 22.3% cases (49out of 217 cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2004-2007

SL. NO.	Crime Heads	Cases Registered				% Variation in 2007 over 2006	Persons Arrested				% Variation in 2007 over 2006
		2004	2005	2006	2007		2004	2005	2006	2007	
1	Tampering computer source documents	2	10	10	11	10.0	0	10	8	2	-75
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	14	33	25	30	20.0	31	27	34	25	26.5
	ii)Hacking	12	41	34	46	35.3	1	14	29	23	-20.7
3	Obscene publication/transmission in electronic form	34	88	69	99	43.5	21	125	81	86	6.2
4	Failure										
	i) Of compliance/orders of Certifying Authority	0	1	0	2	-	0	0	0	1	-
	ii) To assist in decrypting the information intercepted by Govt. Agency	0	0	0	2	-	0	0	0	0	-
5	Un-authorised access/attempt to access to protected computer system	0	0	0	4	-	0	0	0	0	-
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	0	0	0	11	-	0	0	0	11	-
7	Publishing false Digital Signature Certificate	0	0	0	0	-	0	0	0	0	-
8	Fraud Digital Signature Certificate	0	1	1	3	200.0	0	3	0	3	-
9	Breach of confidentiality/privacy	6	3	3	9	200.0	7	13	2	3	50.0
10	Other	0	0	0	0	-	0	0	0	0	-
	Total	**68**	**179**	**142**	**217**	**52.8**	**60**	**192**	**154**	**154**	**0.0**

INCIDENCE OF CYBER CRIMES IN CITIES

- 17 out of 35 mega cities did not report any case of Cyber Crime i.e, neither under the IT Act nor under IPC Sections) during the year 2007.
- 17 mega cities have reported 118 cases under IT Act and 7 megacities reported 180 cases under various section of IPC.
- There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006),
- and an increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various section of IPC
- Bengaluru (40), Pune (14) and Delhi (10) cities have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act.

5. CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

The term “Netizen” was coined by Michael Hauben. Quite simply, “Netizens” are the Internet users. Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms).

The 5P Netizen mantra for online security is:

a. Precaution

b. Prevention

c. Protection

d. Preservation

e. Perseverance

5. CYBERCRIME ERA:
SURVIVAL MANTRA FOR THE NETIZENS

- For ensuring cyber safety, the motto for the “Netizen” should be “Stranger is Danger!”
- NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyber labs across major cities in India. More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced.
- Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes.
- However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals.
- The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.