Institute of Information Technology

Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

ICT-5418:
Cyber Crime and Cyber Terrorism

for

1st Semester of M.Sc in ICT

Lecture File: 01

Cyber Crimes: Violation of Cyber Security

Prepared by:

Professor K M Akkas Ali

akkas@juniv.edu akkas_khan@yahoo.com,

Institute of Information Technology (IIT)

Jahangirnagar University, Dhaka-1342

Recommended Books

Prepared by: K M Akkas Ali, Professor, IIT, JU

1. **Information Security: The Complete Reference** (2nd Edition)- Mark Rhodes-Ousley.
2. **Information Security Management: Concepts and Practice** (New York, McGraw-Hill, 2013).
3. **Cyber Security and Cyber War: What Everyone Needs to Know** (1st Edition, ISBN-13: 978-0199918119)- P.W. Singer, Allan Friedman.
4. **Cyber Security Basics: Protect Your Organization by Applying the Fundamentals** (1st Edition)- Don Franke.

Lecture File-01:
Cyber Crimes: Violation of Cyber Security

Prepared by: K M Akkas Ali, Professor, IIT, JU

Topic to be Discussed:

- Cyber Crimes
- Examples of Cyber Crime
- Nature of Cyber Crimes
- Reasons For Cyber Crimes
- Challenges of Cyber Crime
- Impact of Cyber Crime
- Categories of Cyber Crime
- Cyber Criminals

Introduction: Objective of the Lecture

- We are **living in the modern era run by** technology. Our daily life depends on it, live with it. So, nowadays the Internet is a common name known to everyone.
  - **People are using and depending on Internet more and more as it contains everything they need.**
  - **As Internet usage is increasing day by day, it makes the world small; people are coming closer.**
  - **Rapid technological growth and developments have provided vast areas of new opportunity and efficient sources for organizations of all sizes. So, the whole national security is heavily depending on technologies.**
  - **But these new technologies have also brought unprecedented threats with them- a cybercrime.**
- This lecture gives an overview of cyber crimes committed by cyber criminals.

Prepared by: K M Akkas Ali, Professor, IIT, JU

What is Cyber Crime?

- Development of IT has changed our societies, commerce and lifestyle.
  - **There are two sides to a coin- head and tail.**
  - **Similarly there are two sides of the Internet- Good side and Bad side.**
    - Bad side of the Internet creates considerable legal problems in many areas. One of the **major disadvantages of Internet is cyber crime** that can cause direct or indirect harm to whoever the victim is.
    - However, the largest threat of cybercrime is on the financial security of an individual as well as the government.

Prepared by: K M Akkas Ali, Professor, IIT, JU

What is Cyber Crime?

- A simple definition of cyber crime would be–
  - illegal activities committed primarily **through Internet contact**.
  - **unlawful acts** wherein the computer is either a **tool** or a **target** or **both**.
  - **any criminal act dealing with** computers and networks.
  - **any traditional crimes** conducted through the Internet.
- Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations.
  - **Cybercrime may be intended to harm someone's reputation, financial loss, physical harm, or even mental harm.**
  - **Committing cyber crime is a punishable offence by the information technology act.**

Prepared by: K M Akkas Ali, Professor, IIT, JU

What is Cyber Crime?

- Cyber crimes are committed to steal data, extort money, disrupt systems, or cause harm to individuals, organizations, or governments.
- Cyber crimes can target personal information, financial assets, national security, or even critical infrastructure.

"The modern thief can steal more with a computer than with a gun.

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

Prepared by: K M Akkas Ali, Professor, IIT, JU

Examples of Cyber Crime

Several examples of cyber crime:

- **Hacking** – It refers to unauthorized access to digital devices (like computers, smartphones, tablets, etc.) and networks systems to steal or manipulate data. [**N.B.** Hacking is not always a malicious act, but it can also be done for ethical reasons, such as trying to find software vulnerabilities so they can be fixed].
- **Phishing** – Fraudulent attempts to impersonate legitimate entities (e.g., banks, companies, or government agencies) to obtain sensitive information (e.g., passwords, credit card details, bank account details, social security numbers etc.) through fake emails or websites.
- **Malware Attacks** – Spreading viruses, ransomware, or spyware to damage or control devices.
- **Identity Theft** – Stealing someone's personal information to commit fraud.
- **Cyberbullying & Harassment** – Using digital platforms to threaten, blackmail, or humiliate individuals.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Examples of Cyber Crime

- **Financial Fraud** – It refers to deceptive practices aimed at illegally obtaining money, assets, or sensitive financial information through deceit, manipulation, or breach of trust. It can target individuals, businesses, banks, or governments, often exploiting legal loopholes, technology, or human vulnerabilities. **Examples**: Money theft, credit card fraud, or illegal transactions.
- **Cyber Terrorism** – Attacks on government or corporate systems to create fear or disruption.
- **Cyber Pornography** – It refers to the creation, distribution, or consumption of sexually explicit material (images, videos, texts, or live streams) through digital platforms.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Examples of Cyber Crime

- **Software and Media Piracy** – It refers to the unauthorized copying or stealing, distribution, or use of copyrighted digital content, including software programs, movies, music, games, e-books, and other intellectual property. It violates copyright laws, depriving creators and companies of rightful revenue.
- **Website Vandalism** – It refers to the deliberate act of defacing, replacing, altering, or damaging a website's content, design, or functionality without authorization, sometimes with offensive messages, propaganda, or disruptive code.
- **Spam Marketing** – It refers to the unethical practice of sending unsolicited, bulk messages—typically advertisements—to a large audience without their consent. These messages are often irrelevant, intrusive, and sent via email, SMS, social media, or comment sections, aiming to promote products, services, or scams.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Examples of Cyber Crime

- **Cyber-spying (or Cyber Espionage)** – It is the covert use of digital tools to secretly access, monitor, or steal sensitive data from individuals, organizations, or governments for political, economic, or military advantage.
- **Invasion of Privacy** – It refers to the unjust intrusion into an individual's personal life without consent, violating their right to keep certain matters confidential. It can occur through physical, digital, or surveillance means and is often legally actionable. **Examples**: A journalist publishing a celebrity's private health records. A coworker secretly recording conversations in a restroom. An ex-partner sharing intimate photos online without consent ("revenge porn").
- **Online Scam** – It is a fraudulent scheme conducted through the internet to deceive victims into losing money, personal data, or access to devices. Scammers use psychological manipulation (social engineering) and fake digital platforms to appear trustworthy while stealing from unsuspecting users. A WhatsApp message saying, "Your daughter is hurt—send $500 for surgery!" is a scam.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Offenses Categorized as Cyber Crime by UN

- The United Nations has categorized **five offenses** as cyber crime:

1. Unauthorized or illegal access to computer, computer system or computer network
2. Data interference, i.e. damage to computer data or programs
3. System interference i.e. sabotage to hinder the functioning of a computer system or network
4. Unauthorized or illegal interception of data
5. Computer espionage

Prepared by: K M Akkas Ali, Professor, IIT, JU

Nature of Cyber Crimes

Crime is a socially correlated phenomenon. Nature of cyber crime is far different from the nature of traditional crime happened in the real world.

- No matter how much we try, we cannot experience a society without crime.
- However with the time, nature of cyber crime changes in a given society.

Some natures of cyber crimes are:

1. Cyber crime cannot be segregated from a society. It depends upon the nature of a society. Complexity of the society determines the complexity of the cyber crime. It depends on-
   - the socio-economic and political structure of the society
   - the delinquent behavior in the society
   - the advancement of the technology which has produced new socio-economic and political problem in the society

Prepared by: K M Akkas Ali, Professor, IIT, JU

Nature of Cyber Crimes

2. Compared with the physical world, cyber world is borderless, that is, there is no jurisdictional boundaries. So, it is very difficult to control the cyber crime.

3. The cyber law applicable to a territory is not advanced enough to regulate the cyber crime as their nature is far different from the existing crime. Thus, the global dimension of cyber crime is made it difficult to handle and dealt with.

4. Modern technology has put an end to the barriers of time and space. So, cyber crimes can be committed unknowingly and far away from the victim without being physically present there.

5. The rapid evolution of internet technology has provided the scope for cyber criminals to commit their crime with least chance of detection or even without the risk of being caught.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Nature of Cyber Crimes

6. **Cybercrime is transnational in nature. So, geographical and political boundaries are rendered irrelevant in case of cybercrime.**

7. **The human society is become vulnerable to cyber crime due to more and more dependence on technology.**

Cyber crime becomes a global phenomenon.

- Understanding and regulation of cyber crime cannot be national but has to be international.
- We have to enact new laws and prepare preventive and defensive mechanism globally. Only then, we will be able to protect our society from cyber crime.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Causes that Raise Cyber Crimes/ Reasons For Cyber Crimes

- With the growing use of Internet, cyber crimes are also increasing day by day. Many people, organizations, countries have become victims of this crime.
- We could list the following reasons responsible directly or indirectly for the commission of cyber crimes.

1. **Doubling of computer power:**
   - More organizations depend on computer systems for critical operations
2. **Rapidly declining data storage costs:**
   - Organizations can easily maintain detailed databases on individuals
3. Networking advances and the Internet:
   - Copying data from one location to another and accessing personal data from remote locations is much easier
4. **Advances in data analysis techniques:**
   - Companies can analyze vast quantities of data gathered on individuals
5. **Loss of evidence:**
   - The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common and obvious problem.
6. **Easily Accessible:**
   - Using Internet is not a complex task. So, more people are using it and thereby causing more problems.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Causes that Raise Cyber Crimes/ Reasons For Cyber Crimes

7. Gaining Financial Benefit at Low Risk:

- Money is the major motivator for many cyber criminals. Especially because the dangers of criminality are less apparent when you are hiding behind the network.
- The perception of low risk and very high financial reward prompts many cyber criminals to engage in criminal activities.

8. Negligence

- It is very probable that while protecting the computer system, there might be any negligence, which is in turn provides a cyber criminal to gain access and control over the computer system.

9. Indefinite Legal Jurisdiction:

- Most Internet crimes are committed across international borders. The activities of law enforcement agencies are limited to the boundaries of legal jurisdiction. We have state law enforcement agencies, which can only operate within national borders, but they cannot easily cross international borders.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Cybercrime presents numerous challenges due to its evolving nature, advancement of technology, technical complexity, and global reach. Key challenges include:

Rapidy Evolving Tactics:

- Cybercriminals are rapidly using new technologies and tools to commit crimes. Law enforcement agencies often cannot keep up with this rapid change.
- New types of malware, ransomware, phishing techniques, etc. are constantly being invented, which are difficult to prevent.

Use of Global Networks:

- Cybercriminals use global networks, making it difficult to identify the source of the crime and take legal action.
- International cooperation becomes complicated due to differences in laws and policies across countries.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Inadequate Data Privacy and Security:

- The risk of personal and sensitive data being stolen or leaked has increased. Criminals use this data to cause financial losses or identity theft.
- Data protection policies are often inadequate or outdated, creating opportunities for committing cyber crimes.

Lack of Cyber Security Skills:

- Many organizations and individuals lack awareness and knowledge about cybersecurity. As a result, they easily beome victims to crimes like phishing, social engineering, etc.
- The lack of skilled cybersecurity professionals is also a major challenge.

Time-consuming and Expensive Recovery Process:

- Cybercrime causes huge financial losses to individuals, organizations, and governments. Ransomware, phishing, and other attacks cost billions of dollars.
- The recovery and recovery process is time-consuming and expensive.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

People are Unaware of Their Cyber Rights:

- Cybercrime usually happens to illiterate people around the world. Their governments take various steps to protect their cyber rights. But they are not aware of those rights.

Anonymity of the Criminals:

- Cybercriminals often use anonymity tools (e.g. Tor, VPN, or stolen identities) to hide their identities, which makes them difficult to identify.
- The use of cryptocurrencies also helps criminals hide their transactions.

Less Numbers of Case Registered:

- Every country in the world is facing the challenges of cybercrime. The rate of this crime is increasing day by day because many people do not even register cybercrime cases.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Limitations in Preventing Social Engineering:

- Cybercriminals often take advantage of human error or carelessness. They can use social engineering techniques to gain access to personal information.
- Preventing such attacks is difficult, as it relies on human behavior rather than direct technological vulnerabilities.

IoT Device Vulnerabilities:

- As the number of IoT devices increases, so does the risk of cyberattacks. Many of them have weak security measures, making them easy targets for criminals.
- These devices are often connected to critical infrastructure, which poses a major security risk.

State-Sponsored Cybercrime:

- In some cases, cyberattacks are carried out for state or political purposes. Such attacks are highly planned and powerful, making them difficult to prevent.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Mostly Committed by Well Educated People:

- Committing cybercrime is not an easy task for everyone. The person who commits cybercrime is technically skilled. So, he knows how to commit the crime without getting caught by the authorities.

No Harsh Punishment:

- There is no strict punishment for every case of cybercrime. However, there are strict punishment and penalties in some cases, including cyber terrorism. As a result, many people are encouraged to commit cybercrimes due to lack of punishment.

Legal and Ethical Complexities:

- The legal framework (আইনী কাঠামো) for cybercrime is often inadequate or unclear. In many countries, laws related to cybercrime are still developing.
- From an ethical perspective, balancing personal privacy and security is a major challenge.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Increasing Threats of Cyber War:

- The potential for state or group conflict in cyberspace has increased more than ever. Critical infrastructure, such as power grids, banking systems, etc., could be targeted.

Complex Cyber Insurance Coverage:

- Cyber insurance is becoming increasingly important for organizations affected by cyber attacks. However, insurance coverage and liability are complex issues.

Lack of Global Cooperation:

- Efforts to combat cybercrime effectively are hampered by inconsistencies in information sharing and lack of international cooperation.

Emerging Technologies:

- The use of new technologies, including IoT, cloud computing, and AI, is creating new vulnerabilities and attacks that cybercriminals can exploit.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Insider Threats:

- Retaliatory or negligent actions performed by an employee within an organization can lead to significant breaches. These types of insider threats can be difficult to detect and prevent.

Lack of Cybersecurity Awareness:

- Many individuals and organizations lack awareness of cybersecurity best practices, leaving them vulnerable to social engineering, phishing, and other attacks.

No Jurisdictional Boundaries:

- Cybercrime has no jurisdictional boundaries. It often crosses international borders. The activities of law enforcement agencies are limited to the boundaries of legal jurisdiction. We have state law enforcement agencies, which can only operate within national borders, but they cannot easily cross international borders. So, jurisdiction, cooperation, and enforcement are complicated by differing laws and regulations across countries.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Challenges of Cyber Crime

Resource Constraints:

- Law enforcement agencies often face limited resources, expertise, and funding to combat sophisticated cyber threats effectively.

- The challenges of cybercrime are multifaceted and constantly evolving.
- Technological advancements, strengthening legal frameworks, raising awareness, and international cooperation are essential to address these challenges.
- Effective prevention against cybercrime is not possible without the combined efforts of individuals, institutions, and governments.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Impact Cyber Crime

- **Cyber crimes** are **offences** that are **committed against individuals or groups** with a criminal motive to intentionally **harm the reputation of the victim** or cause physical or mental loss, either directly or indirectly.
  - A report (**sponsored by McAfee**), published in 2014, estimated that the annual damage to the global economy was **$445 billion**.
    - Approximately **$1.5 billion** was lost in 2012 to **online credit and debit card fraud** in the US.
  - In 2018, a study by **Center for Strategic and International Studies (CSIS)**, in partnership with McAfee, concludes that close to $600 billion (**nearly 1% of global GDP**), is lost to cybercrime each year.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Impact Cyber Crime

The consequences of conducting a cyber crime can be catastrophic. For example,

- **Shutdown Business/ Operational Disruption:**
  - Entire IT system of a business may be shut down for several days or weeks due to a security breach, e.g., by **phishing** or **DoS** attack.

- **Loss of Confidential Data:**
  - Due to some cyber attacks, highly confidential and critical data may be compromised.

- **Financial Loss:**
  - Individuals and businesses can suffer significant financial loss because of cyber crime.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Impact Cyber Crime

- **Reputational Damage:**
  - Besides financial damage, organisation may suffer reputational damage also following cyber crime. The **damage to reputation making people hesitant** to share personal information, use their credit cards or shop at online store.
    - For example, consider a resort operator that relies heavily on its website to attract new customers, book reservations and maintain its brand.
    - If that site is hacked and infected with malicious links, it will be quarantined—placed in a "**sin bin**"—for a fairly long period by search engines, **making it harder for customers to find the website**.
    - Even after the operator resolves the hack, it could take months for the resort's virtual reputation to be restored.

- **Compromising Online Banking Transactions:**
  - Phishing emails (purportedly came from friends, or even from bank) seduce individual into clicking on infected links or attachments containing malware, which have the effect of compromising online banking transactions.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Impact Cyber Crime

- **Loss of Personal or National Security and Reputation:**
  - Cyber crime may threaten a person or a nation's security and reputation.
- **Loosing Control of Websites:**
  - Hacking website of a company lead to divulge confidential data and may lose control of the site. Propaganda can be spread and **ransom money** can be extracted by the hackers.
- **Loss of Company Assets:**
  - Bank account numbers and passwords stolen during a breach can cause theft of account funds which could cause a business to lose its working capital.
    - **Proprietary information**, such as **product designs**, **customer records**, **company strategies** **or** **employee information**, **is often compromised or stolen outright**. All of these assets have incalculable value to a business, and thus can inflict crippling losses.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Impact Cyber Crime

- **Legal Consequences:**
  - Victims of cyber crimes often have to resort to cyber courts to recover their data and bring the perpetrators to justice. In this case, a considerable amount of money has to be spent to fight the case.

- **Psychological Impact:**
  - The mental health of the victim of cyberbullying or harassment can be damaged.

- **National Security Threat:**
  - National security can be at risk if the systems of government or important organizations are compromised.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Crime

- Cyber crime refers to all activities done with criminal intent in cyberspace.
  - It can be classified into various categories based on several criteria.

Category A:

- Cyber crime can be classified into **two categories** based on the fact whether the computer is either a tool or a target:
  - Computer Assisted Cyber Crimes
  - Computer Oriented Cyber Crimes

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Crime

Category B:

- Cyber crime can be classified basically into **three major categories** based on entities against which it is performed:
  - Cyber Crimes Against Persons:
  - Cyber Crimes Against Property:
  - Cyber Crimes Against Government:

Category C:

- An arbitrary taxonomy of cyber crimes:
  - Classic cyber crimes
  - Internet fraud
  - Content/substance-oriented online crimes

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Crime

Category A:

- **Computer Assisted Cyber Crimes:**
  - Computer is instrumental in committing the crime.
  - **Examples:**
    - Selling nonexistent, defective, substandard or counterfeit goods
    - Selling obscene and prohibited sexual representations.
    - Theft of credit card, bank fraud, fake stock shares
    - Intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Crime

Category A:....

- **Computer Oriented Cyber Crimes:**
  - Computer is the target of the crime.
    - **Malicious Software:**
      - viruses
    - **Worm:**
      - Self-replicating programs spread autonomously without a carrier. Ex. Via mail, scanning remote systems
    - **Trojan:**
      - installed during downloading some program as a background activity causing irreparable damage.
    - **Spyware:**
      - parasitic software that "spies" on your computer which can capture information like Web browsing habits, e-mail messages, usernames and passwords, credit card information etc.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Category B:

Prepared by: K M Akkas Ali, Professor, IIT, JU

1. Cyber Crimes Against Persons:

- Here individuals are the target of the crime.
- It involves the actions that are taken to theft personal information and to harm an individual by making misuse of that information.
- Different types of cyber crimes against individual are:
  - Transmission of child-pornography
  - Harassment of any person (such as sending defaming e-mail)
  - Posting and distributing obscene material
    - Example: A minor girl in Khulna was lured to a private place through cyber chat by a man, who, along with his friends, attempted to gang-rape her. As some passersby heard her cry, she was rescued

Category B: ...

2. Cyber Crimes Against Property:

- It involves the taking of property or money and does not include a threat of force or use of force against the victim.
- Here properties of individual or organization are the target of the crime.
- Different types of cyber crimes against property are:
  - Unauthorized computer trespassing through cyberspace
  - Computer vandalism
  - Transmission of harmful programs
  - Unauthorized possession of computerized information
  - Destruction of other's property through internet
    - Example: A Mumbai-based engineering company lost a say and much money in the business when the rival company stole the technical database from their computers with the help of a corporate cyber spy.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Category B:...

3. Cyber Crimes Against Government:

- Here target is the government.
- This is the least common cybercrime, but is the most serious offense.
- A crime against the government is also known as cyber terrorism.
- Different types of cyber crimes against government are:
  - Threaten the international governments
  - Terrorize the citizen of a country
  - Cracking on defense and government sites
  - Intra-bank transfer of funds for terrorist activities
  - Espionage
  - Inciting riot
- This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Crime

Category C:

1. Classic Cyber Crimes:

- Focus is on the hardware/network itself.
  - Theft of services
  - Computer intrusion
  - Computer Viruses, Worms, Trojan Horses, Spyware
  - Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

2. Internet Fraud:

- Crime on deception.
  - Internet auction fraud
  - PPC (Pay-Per-Click) click fraud
  - Phishing and Money laundering

3. Content/Substance-Oriented Online Crimes:

- These crimes are based on online materials.
  - Spam
  - Child pornography and Illegal obscenity
  - Warez
  - Online gambling

Prepared by: K M Akkas Ali, Professor, IIT, JU

Cyber Criminals

- Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.
  - A cybercriminal may use computer expertise, knowledge of human behavior, and a variety of tools and services to achieve his or her goal.
- The kinds of crimes a cybercriminal may be involved in can include hacking, identity theft, online scams and fraud, creating and disseminating malware, or attacks on computer systems and sites.

Cyber Criminals

- Cyber criminals commit illegal activities online for a wide variety of reasons, ranging from altruistic intentions, personal glory, revenge, espionage, and/or financial gain. The major reasons cyber criminals commit crimes are for money, sex, or power.
  - The way that cybercriminals choose a target depends on their motivation.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Criminals

1. Children and Adolescents (between the age group of 6 – 18 years):

- The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things.
- Other reason may be to prove themselves to be outstanding amongst other children in their group.
- Further the reasons may be for psychological event. e.g. the Bal Bharati case in Delhi was the outcome of harassment of the delinquent by his friends.
  - A 16-year-old boy was arrested in April 2001 on the charge of creating a pornographic website containing obscene comments about some women teachers and girls of his school, **Air Force Bal Bharati in Delhi**. When he was released on bail, the school refused to take him back.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Criminals

2. Organized Hackers:

- These kinds of hackers are mostly organized together to fulfill certain objective. The reason may be to fulfill their political bias, fundamentalism, etc.
- The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfill their political objectives..

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Criminals

3. Professional Hackers Vs. Crackers (Black Hat Hacker):

- The term 'hacker' broadly relates to theft of valuable data for personal gain or criminal objective.
  - When the same individual hacks with the intention to protect the IT infrastructure and to serve the purpose of owners, with permission from the organization, they become a professional hacker. It is when the job of hacking is objectivated for ethical reasons.
- A professional hacker (also called **ethical hacker,** penetration tester or **white hat hacker**) is a skilled individual hired by an organization to test effectiveness of its IT infrastructure.
- Professional hackers find vulnerabilities in computer systems and fix them. They help their clients in protecting and defending their systems from being hacked by malicious attackers. The knowledge they possess about programming, various computer languages, code and general computer security is advanced and used for morally good purposes.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Criminals

- A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system.
- They look for backdoors in programs and systems, exploit those backdoors, and steal private information for use in a malicious way.
  - A hacker might discover holes within systems and the reasons for such holes. He (or she) constantly seeks further knowledge, freely share what they have discovered, and never intentionally damage data. But a cracker is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get reliable and valuable information.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Categories of Cyber Criminals

4. Discontented Employees:

- This group includes those people who have been either sacked by their employer or are dissatisfied with their employer.
- To avenge, they normally hack the system of their employee.

Prepared by: K M Akkas Ali, Professor, IIT, JU

Discussion Points

- Cyber Crimes
- Examples of Cyber Crime
- Nature of Cyber Crimes
- Reasons For Cyber Crimes
- Challenges of Cyber Crime
- Impact of Cyber Crime
- Categories of Cyber Crime
- Cyber Criminals

Prepared by: K M Akkas Ali, Professor, IIT, JU

Have a question?

Thank you…