Cyber Security & Ethics

Subject Code:28573

Semester : 7th

Technology: Computer

Prepared By:
Md. Shakil Al Masum
Chief Instructor(Computer)
Barishal Polytechnic Institute

Chapter :01
Understand Cyber Security

Sl no	Topics
1.1	Define is Cyber Security
1.2	Classify Cyber Security
1.3	Describe the necessity & role of Cyber Security
1.4	Distinguish between information security & Cyber security
1.5	Describe & explain why information & cyber security are important to business & to society.
1.6	Explain Security, Identity, Authentication, Confidentiality, Integrity, Availability, Threat, Vulnerability, Risk & hazard.

Learning Objectives

After completed this session student will be able to-

- What is Cyber Security?
- Classify Cyber Security
- Describe the importance & role of cyber security
- Describe difference between information & cyber security
- Describe the importance of cyber security in business & society.
- Describe Security, Identity, Authentication, Confidentiality, Integrity, Availability, Threat, Vulnerability, Risk & hazard.

1.1 Define is Cyber Security

- **Definition**: **Cyber security** or information technology **security** are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Network **security** includes activities to protect the usability, reliability, integrity and safety of the network.

1.2 Classify Cyber Security

5 main types of cyber security:

1. Critical infrastructure security:

Common examples of critical infrastructure:

- electricity grid
- water purification
- traffic lights
- shopping centers
- hospitals

2. Application security:

Types of application security:

- antivirus programs
- firewalls
- encryption programs

3. Network security:

Common examples of network security implementation:

- extra logins
- new passwords
- application security
  - antivirus programs
  - antispyware software
  - encryption
  - firewalls
  - monitored internet access

4. Cloud security:

Cloud security is a software-based security tool that protects and monitors the data in your cloud resources. Cloud providers are constantly creating and implementing new security tools to help enterprise users better secure their data.

5. Internet of things (IoT) security:

IoT refers to a wide variety of critical and non-critical cyber physical systems, like appliances, sensors, televisions, wifi routers, printers, and security cameras.

1.3 Describe the necessity & role of Cyber Security

- **Three Principles of Cyber Security**

  There are at least three main principles behind cyber security: **confidentiality**, **integrity** and **availability**.

  1. Confidentiality involves any information that is sensitive and should only be shared with a limited number of people. If your credit card information, for example, was shared with a few criminals, your credit rating and your reputation could suffer very quickly.

  2. Integrity involves keeping information from being altered. When malware hits a hospital's computer systems, it can scramble patient records, lab results and can prevent staff from accessing a patient's allergy or drug information.

  3. Availability involves ensuring those who rely on accurate information are able to access it. Availability is often related to integrity, but can also involve things like a cyber attack preventing people from accessing specific computers, or from accessing the internet.

Why is Cyber Security Important?

- Cyber crime threatens national security as the internet becomes a favorite tool of international criminals, cyber crime perpetrated by organized crime networks has become a real threat to national & international.

Understanding the Role of Cyber Security :

Anything that relies on the internet for communication, or is connected to a computer or other smart device, can be affected by a breach in security. This includes:

- Communication systems, like email, phones and text messages
- Transportation systems, including traffic control, car engines, airplane navigation systems.
- Government databases, including Social Security numbers, licenses, tax records.
- Financial systems, including bank accounts, loans and paychecks.
- Medical systems, including equipment and medical records.
- Educational systems, including grades, report cards and research information.

1.4 Distinguish between information security & Cyber security

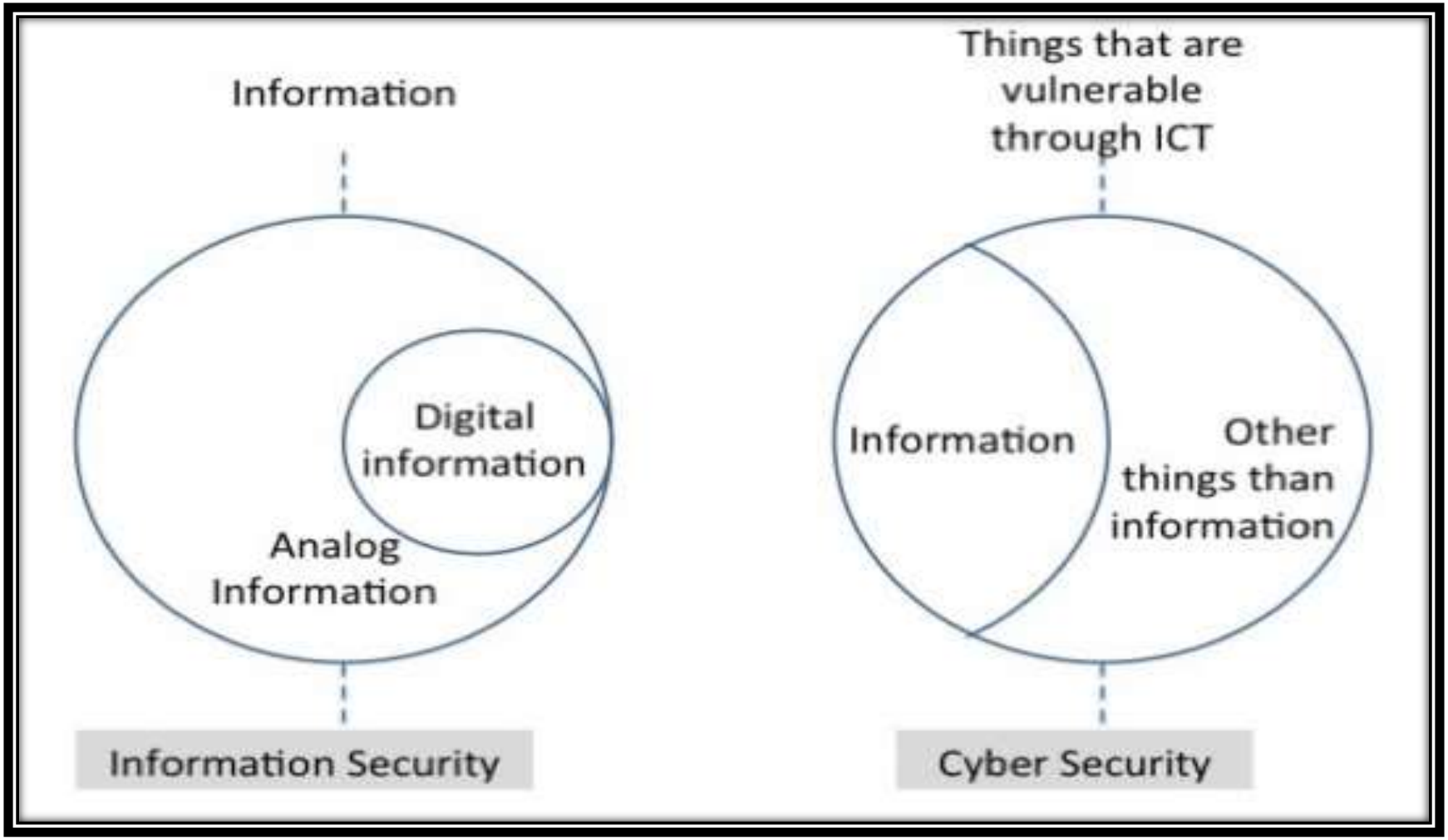


Fig: Information Security & Cyber Security

CYBER SECURITY

VERSUS

INFORMATION SECURITY

CYBER SECURITY	INFORMATION SECURITY
Cyber security deals with protecting your data and information that is in digital or electronic form.	Information security deals with safeguarding your information assets that are in both physical and digital format.
It protects data that exists in the cyber realm from unauthorized digital access.	It's all about protecting information and their confidentiality, integrity, and availability.
It deals with advanced persistent threats that are imminent.	It's the foundation of data security which means it's the first step.
It deals with cyber threats such as phishing, baiting, data breach, etc.	Ii deals with all sorts of threats to make sure proper security protocols are in place.

1.5 Describe & explain why information & cyber security are important to business & to society

- It is important to protect your business & to society against cyber security threats and make the most of the opportunities online.
- The online world offers businesses the potential for reaching a broader customer base, use international suppliers and sometimes even save on admin or supply costs. However, the world of online business can bring the potential for scams and security risks. A single successful attack could seriously damage your business and cause financial burden for you and your customers, as well as affect your business's reputation.
- It's a good idea to put an effective cyber security plan in place if your business accesses the internet or email to conduct business.

Steps to keep your tech and business information & to society secure

- Back up data
- Secure your computer and devices
- Monitor and protect the use of computer equipment and systems
- Protect important information
- Manage administrative passwords
- Choose strong passwords
- Use spam filters
- Educate your staff to be safe online
- Put security measures in place

- Protect your customers
- Protect yourself
- Keep yourself informed about the latest cyber security risks

1.6 Explain Security, Identity, Authentication ,Confidentiality, Integrity, Availability,Threat , Vulnerability, Risk & hazard

- **Security**: Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.

- **Identity**: In *computer* technology, the unique name of a person, device, or the combination of both that is recognized by a system.

- **Authentication:**

Authentication is the process of verifying a principal's identity

- Who the person is
- Or, What the person is

Confidentiality: Information that is sensitive or confidential must remain so & should be accessible to authorized users only.

Integrity: Information must retain its integrity (original form) & not be altered or changed from its original state.

Availability: Information & systems must always be available to authorized users when needed.

- **Threat** : A **threat**, in the context of **computer security**, refers to anything that has the potential to cause serious harm to a **computer** system. A **threat** is something that may or may not happen, but has the potential to cause serious damage. **Threats** can lead to attacks on **computer** systems, networks and more.
- **Vulnerability:** 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.
- **Risk: Cyber risk** commonly refers to any **risk** of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. ... Deliberate and unauthorized breaches of security to gain access to information systems. Unintentional or accidental breaches of security.

Hazard:

- A hazard is any agent that can cause harm or damage to humans, property, or the environment. Risk is defined as the probability that exposure to a hazard will lead to a negative consequence, or more simply, a hazard poses no risk if there is no exposure to that hazard.

Ch:02
Understand Data & Evidence Recovery

Sl no	Topics Name
2.1	Define file recovery. Classify different procedures for file recovery.
2.2	Define data recovery & Forensic Tool kit(FTK)
2.3	Describe various types of Computer forensics tools
2.4	Discuss various Personal Identifiable Information
2.5	Discuss various types of E-mail threats.

Learning Objectives

After completed this session student will be able to-

- Describe file recovery & various procedures of file recovery
- Describe data recovery technique & forensic tool kit
- Describe PIB
- Describe about E-mail threat

2.1 Define file recovery. Classify different procedures for file recovery.

- **Define file recovery: File recovery** is the process of rebuilding or **recovering** lost **files** from a disk or hard drive that is no longer operational or was damaged from unnatural causes.

Classify different procedures for file recovery:

- Stellar Data Recovery for Mac: Data Recovery Utility for Mac Computers
- CDRoller: Recovers data from optical disc
- Data Recovery Wizard: by EaseUS. Microsoft Windows file recovery utility
- Disk Drill Basic: Data recovery application for Mac OS X and Windows
- dvdisaster: Generates error-correction data for optical disc
- GetDataBack: A Windows recovery program
- Hetman Partition Recovery: The complete data drive recovery solution
- IsoBuster: Recovers data from optical discs, USB sticks, Flash drives and Hard Drives

- Mac Data Recovery Guru: A Mac OS X data recovery program which works on USB sticks, optical media, and hard drives
- Norton Utilities: A suite of utilities that has a file recovery component
- Stellar Photo Recovery: Photo Recovery Utility for Mac & Windows Computers
- PhotoRec: advanced Multi-platform program with text-based user interface used to recover files
- Recover My Files: Proprietary evaluationware, Microsoft Windows 2000 & later, FAT, NTFS and HFS
- Recuva: Microsoft Windows 2000 & later, FAT and NTFS
- Stellar Data Recovery for Windows: Data Recovery Utility for Microsoft Windows
- TestDisk: Multi-platform. Recover files and lost partitions
- TotalRecovery: Microsoft Windows. Bootable backup and recover system
- TuneUp Utilities: Microsoft Windows XP & later. A suite of utilities that has a file recovery component

2.2 Define data recovery & Forensic Tool kit(FTK)

- ***Data recovery*** is the process of restoring *data* that has been lost, accidentally deleted, corrupted or made inaccessible. In enterprise IT, *data recovery* typically refers to the restoration of *data* to a desktop, laptop, server or external storage system from a backup.

What is Data Loss?

- Data has accidentally been erased or data control structures have been overwritten.
- Data has been corrupted or made inaccessible.
- Data is unable to be accessed from a previous functioning computer system or backup.

Common Computer Problems

- Computer won’t boot up
- Applications that are unable to run or load data
- Hard drive crashes
- Corrupt files or data
- Accidental reformatting of partitions
- Inaccessible drives and partitions
- Media surface contamination and damage

What Causes Data Loss?

- Sabotage
- Natural Disaster
- Hardware Error
- Virus Attack
- Human Error
  - Intentional deletion
  - Accidental overwriting of files
- Software Corruption

What Causes Data Loss?

Cause	Example	Percentage
Hardware & System Problems	Disk drive crashes, electrical outages or power surges, manufacturer defects.	45%
Human Errors	Accidental deletions, overwriting files, causing trauma to desktop or laptop.	33%
Software Corruption or Application Error	Application displays an error message when a document is opened. Installing or removing a program corrupts another.	12%
Computer Viruses	i.e.: MyDoom.A MyDoom.B W32.Welchia.Worm W32.Blaster.Worm W32.Spybot.Worm Downloader.Trojan W32.Swen.A@mm	6%
Natural Disasters	Fires, floods, lightning, earthquakes.	4%

Data Recovery Tips

• DO's	• DON'TS
– Backup your data frequently. – If you believe there is something wrong with your computer shut it down, do not continue to power up because you may do more damage. – If you here a clunk, clunk sound when you power up the drive, shut down! Do not panic nor turn the power button on and off. – Package the drive properly when you send it in to a data recovery specialist. You can cause additional damage to the hard drive if it is poorly packaged.	– Do not ever assume that data recovery is impossible; even in the worst cases, such as natural disasters data recovery specialists have been able to retrieve valuable data. – Never remove the cover from the hard drive; this will only cause further damage. – Do not rest your computer on a moveable object or piece of furniture. Shock and vibration can result in serious damage to the hard drive. – Do not subject the drive to extreme temperatures changes both hot and cold. – In the case where a drive has been exposed to water, fire or even smoke do not try to power up.

Forensic Tool Kit (FTK)

- **Forensic Toolkit**, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can, for example, locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption.

2.3 Describe various types of Computer Forensics Tools

Types of Computer Forensics Tools

❑ Hardware Forensic Tools:

- Range from single-purpose components to complete computer system & servers

❑ Software Forensic Tools:

Types

- Command line application
- GUI application

Types of Cyber Forensics

1. Law enforcement computer forensic
2. Computer evidence processing procedures
3. Preservation of evidence
4. Disk structure: evidence can reside at various levels within the structure of the disk.
5. Data encryption : should become familiar with different forms
6. Data compression
7. Erased files
8. Internet abuse identification & detection

2.4 Discuss various personal Identifiable information

What is PII?

- Personally Identifiable Information (PII) is any information, maintained by a company, which:
  - can be used to distinguish or trace an individual's identity
  - is linked or linkable to an individual
- Examples of PII:
  - Name, Address, SSN, Date of Birth, Phone Number
  - Device specific static identifier (e.g., IP Address, UDID, etc.)
  - Logs of user actions
  - Financial, Employment or Location data

2.5 Discuss various types of E-mail threats.

- Malware, short for malicious software, is frequently spread via e-**mail** on home networks. This type of security **threat** to home networks — and computers in general — may even appear to come from someone you know and trust. E-**mail** also has some original **threats** of its own, including spam, spoofing, and phishing attacks.

Fig: E-mail threats

Various Types Of Email Security Threats!

- **Threat** 1: Ransomware
- **Threat** 2: Phishing
- **Threat** 3: Spear Phishing
- **Threat** 4: Spoofing
- **Threat** 5: Whaling

Ch: 03
Understand Cyber Crimes

SL no	Topics
3.1	Define Cyber Crime
3.2	Discuss Various types of Cyber crimes cyber bullying,cyber extortion, phishing, Identity Thefts, Scamming, Cyber Laundering, DDos attack etc
3.3	Define Malware . Describe various types of Malware.
3.4	Describe various types of cyber crimes such as Hacking, Cracking, Virus Attacks, Pornography, Software piracy.
3.5	Define Intellectual property.
3.6	Describe Tracking, Ip Tracking, E-mail recovery, Encryption & Decryption methods
3.7	Describe Password Cracking

Learning Objectives

After completed this session student will be able to-

- Describe Cyber Cyber crimes cyber bullying,cyber extortion, phishing, Identity Thefts, Scamming, Cyber Laundering, DDos attack etc
- Describe various types of Malware.
- Describe various types of cyber crimes such as Hacking, Cracking, Virus Attacks, Pornography, Software piracy.
- Define Intellectual property.
- Describe Tracking, Ip Tracking, E-mail recovery, Encryption & Decryption methods
- Describe Password Cracking

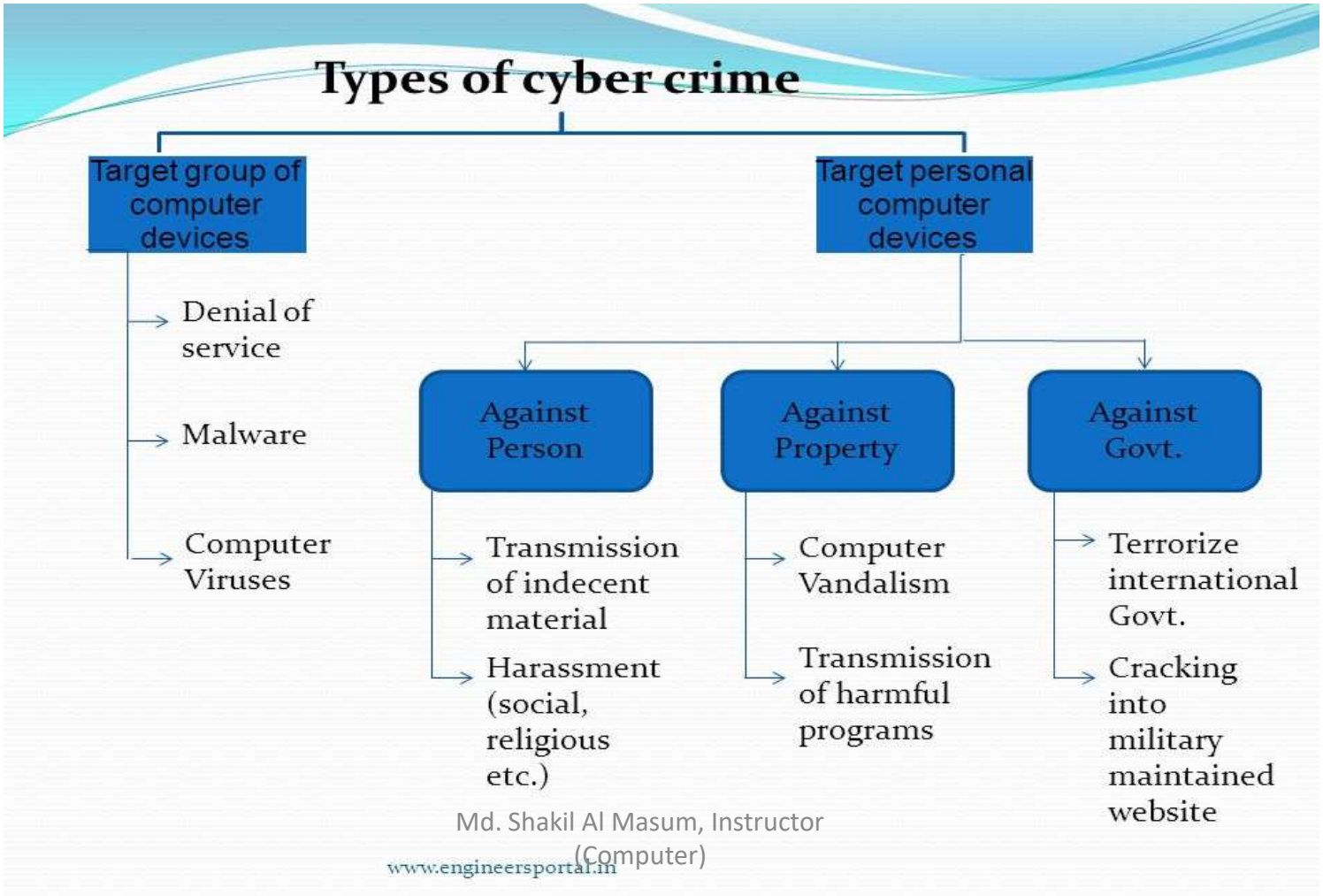
3.1 Define Cyber Crime

- **Cybercrime** is defined as a **crime** in which a computer is the object of the **crime** (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate **crimes**). **Criminals can** also use computers for communication and document or data storage.

- Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

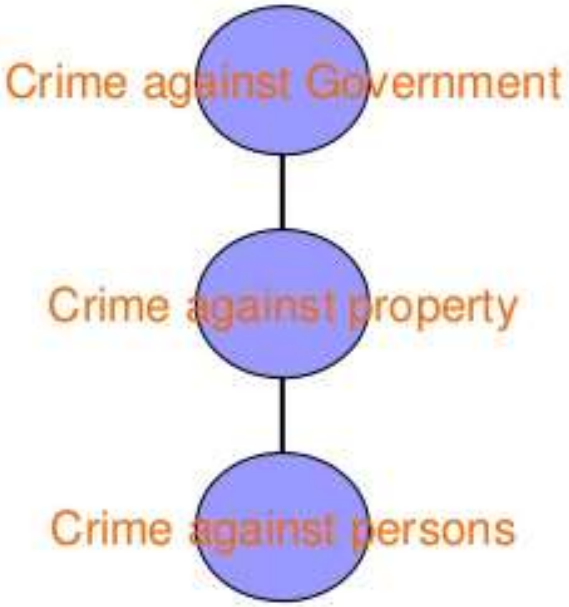
3.2 Discuss Various types of Cyber crimes, cyber bullying,cyber extortion, phishing, Identity Thefts, Scamming, Cyber Laundering, DDos attack etc

Types of Cyber Crime:

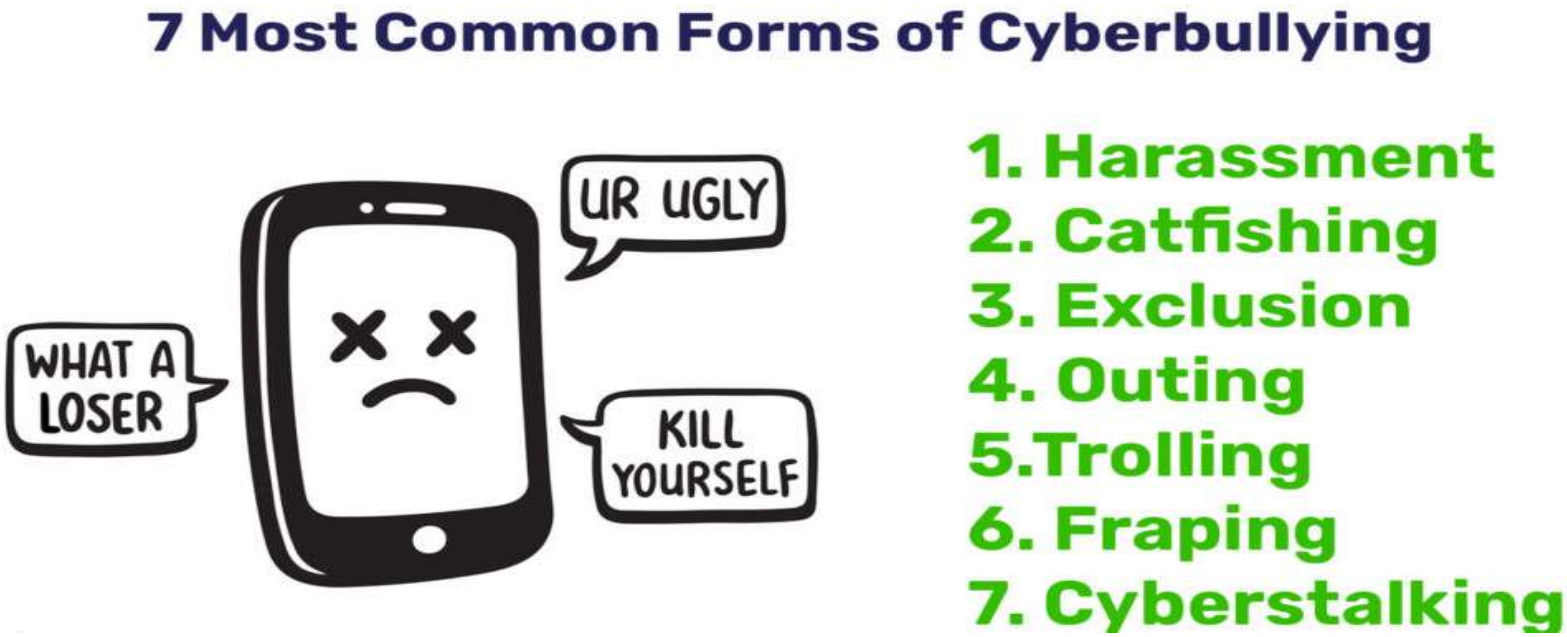


Types of Cyber crimes

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phising
- Cyber terrorism



Cyber-bullying :The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.



- ***Cyberextortion*** is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

- Common types of **extortion** include blackmail, protection schemes, and certain types of hacking. **Extortion** is not a black and white action, and many state laws differ on key aspects of an act of **extortion**. For **example**, is a frivolous lawsuit a form of **extortion**?

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message

• 5 Categories of Phishing

Based on the phishing channel, the types of phishing attacks can be classified into the following categories:

1. Vishing

- Vishing refers to phishing done over phone calls. Since voice is used for this type of phishing, it is called vishing → voice + phishing = vishing.
- Considering the ease and enormity of data available in social networks, it is no surprise that phishers communicate confidently over a call in the name of friends, relatives or any related brand, without raising any suspicion.

2. Smishing

- SMS phishing or SMiShing is one of the easiest types of phishing attacks.
- The user is targeted by using SMS alerts.
- In SMiShing, users may receive a fake DM or fake order detail with a cancellation link.
- The link would actually be a fake page designed to gather personal details.

3. Search Engine Phishing

- Search engine phishing is the type of phishing that refers to the creation of a fake webpage for targeting specific keywords and waiting for the searcher to land on the fake webpage.
- Once a searcher clicks on the page link, s/he will never recognize that s/he is hooked until it is too late.

4. Spear Phishing

- Unlike traditional phishing – which involves sending emails to millions of unknown users – spear phishing is typically targeted in nature, and the emails are carefully designed to target a particular user.
- These attacks have a greater risk because phishers do a complete social profile research about the user and their organization – through their social media profile and company website.
- Out of the different types of phishing attacks, **Spear phishing is the most commonly used type of phishing attack** – on individual users as well as organizations.
- **5. Whaling**
- Whaling is not very different from spear phishing, but the targeted group becomes more specific and confined in this type of phishing attack.

- ***Identity theft***, also known as *identity fraud*, is a crime in which an imposter obtains key pieces of personally identifiable information, such as Social Security or driver's license numbers, in order to impersonate someone else.
  - Financial Identity Theft. ...
  - Driver's License Identity Theft. ...
  - Criminal Identity Theft. ...
  - Social Security Identity Theft. ...
  - Medical Identity Theft. ...
  - Insurance Identity Theft. ...
  - Child Identity Theft. ...
  - Synthetic Identity Theft.

- ***Spamming*** is abuse of electronic messaging systems for sending restricted bulk messages using a computer or a cellular phone. ... SMS Phishing also known as Smishing is normally carried out through send malicious SMS to mobile phone users.

- **cyber-laundering** is the same as the conventional money **laundering** practice which consists of three stages: Placement, placing dirty money into a legal financial system. Layering, transferring or changing the form of money through complex transactions to obscure the origin of funds.

DDos Attack:

- Distributed *DoS attack*. A distributed denial-of-service (*DDoS*) *attack* occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an *attack* is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

3.3 Define Malware . Describe various types of Malware.

- **Malware**: *Malware*, or malicious software, is any program or file that is harmful to a computer user. Types of *malware* can include computer viruses, worms, Trojan horses and spyware.

These are the different types of malware and explaining how to recognize them:

- Virus
- Worm
- Trojan
- Ransomware
- Adware
- Spyware
- File-less malware
- The hybrid attack

3.4 Describe various types of cyber crimes such as Hacking, Cracking, Virus Attacks, Pornography, Software piracy.

- *Hacking* generally refers to unauthorized intrusion into a computer or a network. The person engaged in *hacking* activities is known as a *hacker*. This *hacker* may alter system or security features to accomplish a goal that differs from the original purpose of the system.

- The term "**cracking**" means trying to get into **computer** systems in order to steal, corrupt, or illegitimately view data. The popular press refers to such activities as hacking, but hackers see themselves as expert, elite programmers and maintain that such illegitimate activity should be called "**cracking**."

- ***Virus / worm attacks*** *Viruses* are programs that attach themselves to a *computer* or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a *computer*, either by altering or deleting it. Worms, unlike *viruses* do not need the host to attach themselves to.

- **Cyberpornography** is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyberpornography is a criminal offense, classified as causing harm to persons.

- **Software piracy** is the illegal copying, distribution, or use of **software**. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business **Software** Alliance (BSA), about 36% of all **software** in current use is stolen.

3.5 **Define Intellectual property.**

- **Intellectual property** (IP) is a category of **property** that includes intangible creations of the human intellect. There are many types of **intellectual property**, and some countries recognize more than others. The most well-known types are copyrights, patents, trademarks, and trade secrets.

Fig: Intellectual Property

3.6 Describe Tracking, Ip Tracking, E-mail recovery, Encryption & Decryption methods

- **Tracking:** *Tracking* is a term that defines the synchronized movement of an on-screen pointer or cursor with that of an input device such as a mouse.
- **Ip tracking:** software that converts an **IP** address into a hostname and provides location and other information.
- **A *recovery* phone number or *email* :**address helps you reset your password if: You forget your password. Someone else is using your account. You're locked out of your account for another reason.

Encryption :

- In cryptography, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. **Encryption** does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

Decryption:

- Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data manually or unencrypting the data using the proper codes or keys.

3.7 Describe Password Cracking

- Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it's an art of obtaining the correct password that gives access to a system protected by an authentication method.

- Password cracking employs a number of techniques to achieve its goals. The cracking process can involve either comparing stored passwords against word list or use algorithms to generate passwords that match.

What is password strength?

- **Password strength is the measure of a password's efficiency to resist password cracking attacks**. The strength of a password is determined by;
- **Length**: the number of characters the password contains.
- **Complexity**: does it use a combination of letters, numbers, and symbol?
- **Unpredictability**: is it something that can be guessed easily by an attacker?

Password cracking techniques

- There are a number of **techniques that can be used to crack passwords**. We will describe the most commonly used ones below;
- **Dictionary attack**– This method involves the use of a wordlist to compare against user passwords.
- **Brute force attack**– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@$$word using the brute force attack.

- **Rainbow table attack**– This method uses pre-computed hashes. Let's assume that we have a database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found, then we have the password.
- **Guess**– As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.

- **Spidering**– Most organizations use passwords that contain company information. This information can be found on company websites, social media such as facebook, twitter, etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

Password cracking tool

- **These are software programs that are used to crack user passwords**. We already looked at a similar tool in the above example on password strengths. The website www.md5this.com uses a rainbow table to crack passwords. We will now look at some of the commonly used tools .
- **John the Ripper**
- John the Ripper uses the command prompt to crack passwords. This makes it suitable for advanced users who are comfortable working with commands. It uses to wordlist to crack passwords. The program is free, but the word list has to be bought. It has free alternative word lists that you can use. Visit the product website http://www.openwall.com/john/ for more information and how to use it.

Cain & Abel

- Cain & Abel runs on windows. It is used to recover passwords for user accounts, recovery of Microsoft Access passwords; networking sniffing, etc.

Ophcrack

- Ophcrack is a cross-platform Windows password cracker that uses rainbow tables to crack passwords. It runs on Windows, Linux and Mac OS. It also has a module for brute force attacks among other features. Visit the product website http://ophcrack.sourceforge.net/ for more information and how to use it.