

WOLDIA UNIVERSITY SCHOOL OF COMPUTING INSTUTUTE TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

Assignment: **ethics**

**Team Member Name Id no**

## Tinsae abebe WDU1202005

1. Molalegn Edenshaw WDU1201525

## Olyad Husen WDU1200371

1. Tofik kedir WDU112792

## Tringo selima WDU1101354

Submitted to:Mr mezgebu

## March 07 2023

**Woldia, Amhara,Ethiopia**

# Contents

[Introduction 1](#_bookmark0)

1. [List and discuss the different types of computer crimes today.](#_bookmark1) [2](#_bookmark1)
   1. [The 3 Categories of computer crime](#_bookmark2) [2](#_bookmark2)
   2. [Types of computer crime](#_bookmark3) [3](#_bookmark3)
2. [Hacking and Cracking](#_bookmark4) [6](#_bookmark4)
   1. [Hacking](#_bookmark5) [6](#_bookmark5)
   2. [Cracking](#_bookmark6) [7](#_bookmark6)
      1. [Types of Cracking 7](#_bookmark7)
   3. [The difference between hacking and cracking](#_bookmark8) [8](#_bookmark8)
3. [What is encryption?](#_bookmark9) [10](#_bookmark9)
   1. [How Encryption Works](#_bookmark10) [11](#_bookmark10)
   2. [Types of Encryptions](#_bookmark11) [12](#_bookmark11)
   3. [The uses of Encryption](#_bookmark12) [13](#_bookmark12)
4. [Computer Security](#_bookmark13) [15](#_bookmark13)
   1. [Use of Computer Security](#_bookmark14) [15](#_bookmark14)
   2. [components of computer security](#_bookmark15) [17](#_bookmark15)
   3. [Types of Computer Security](#_bookmark16) [17](#_bookmark16)
5. [Software piracy](#_bookmark17) [18](#_bookmark17)
   1. [What are some legal consequences of software piracy?](#_bookmark18) [19](#_bookmark18)
   2. [Forms of Software piracy](#_bookmark19) [20](#_bookmark19)
6. [What is privacy](#_bookmark20) [21](#_bookmark20)
7. [Define cyber-crime, cyber terrorism, cyber terrorist](#_bookmark21) [22](#_bookmark21)
8. [Write down some of the Ethical and Unethical code of ethics in IT Areas ethical code of ethics](#_bookmark22)

[....................................................................................................................................................... 25](#_bookmark22)

* 1. [Ethical code of Conduct in IT](#_bookmark23) [25](#_bookmark23)
  2. [Unethical Codes of Conduct in IT:](#_bookmark24) [26](#_bookmark24)

[Conclusions](#_bookmark25) [28](#_bookmark25)

[Reference 29](#_bookmark26)

# Introduction

Ethics is the branch of philosophical study that focuses on ‘ethics’ is concerned with studying and/or building up a coherent set of ‘rules or principles by which people ought to live. Ethics is often used in connection with the activities of organizations and with professional codes of conduct. Sets of rules or guidelines stating how employees are expected to behave in their workplaces.

Ethics in IT refers to the study of moral principles and values that should guide the behavior of individuals and organizations involved in the creation, development, and use of information technology. The field of IT has revolutionized the way we live, work, and communicate, but it has also raised a number of ethical concerns related to privacy, security, intellectual property, accessibility, social impact, and environmental impact.

As the use of technology continues to grow and evolve, it is important to consider the social and ethical implications of our actions. This requires a commitment to ethical principles such as honesty, integrity, respect, and responsibility. It also requires staying informed about emerging ethical issues and engaging in ongoing education and training to ensure that we are able to make informed decisions and act in an ethical and responsible manner.

The study of ethics in IT is important for individuals and organizations involved in the creation, development, and use of technology, as it provides a framework for understanding and addressing ethical concerns related to the use of technology. By adhering to ethical principles and staying informed about emerging ethical issues, we can ensure that technology is used in a way that benefits society as a whole while minimizing potential harm.

# 1. List and discuss the different types of computer crimes today.

The growth and advances in digital technology creates a whole new platform for criminal activity. Since the advancement of technology, any crime that involves using a computer or network is generally referred to as a cybercrime or computer crime. The penalties differ for each crime, depending on whether they violated state or federal laws. In general, they include fines, imprisonment, probation, or all the above.

computer crime is the act of committing a crime using a computer, the internet, mobile device that is connected to the internet, and specialized software such as exploit kits and ransomware. Cybercrimes range from the theft of personal information such as bank accounts to the illegal distribution of content such as music and other material protected by copyright.

## The 3 Categories of computer crime

The major computer or cybercrimes that you hear about are often grouped into 3 types of cybercrime, including:

#### Individual

The first type of cybercrime is individual or personal cybercrime. These kinds of computer crime are committed against a single individual.

Examples of individual cybercrime include hacking an email account to steal a person's personal information, sending annoying spam emails to a person's email account, and using a person's webcam to spy on them.

#### Property

The second type of computer crime or cybercrime is property cybercrime. These types of computer crimes are committed against a person's property, including their computer, mobile device, and other connected devices.

Examples include ransomware, which is malicious software that steals a person's files and holds them hostage, demanding money in exchange for access to the files; stealing a person's identity and using it to commit other crimes; and disrupting a person's internet connection, such as by causing denial-of-service attacks.

#### Government

The third and final type of cybercrime is government cybercrime. These types of internet crimes are committed against a government, including the federal government, state governments, and local governments.

Examples of government cybercrime include planting malicious software on a government network to steal data or disrupt the network; stealing government data such as tax returns, which is a federal crime; and causing a denial-of-service attack on a government website, such as the IRS website.

## Types of computer crime

#### Hacking

The computer crime hacking refers to the practice of gaining unauthorized access to another person’s computer, database, or network where private information can be stored. It is a felony in the U.S. to hack a computer system, whether it is a single personal computer or an organizational computer network. However, not all types of “hacking” refer to crimes. Some organizations perform “Ethical hacking” on their own systems or with permission to explore the systems of others to look for vulnerabilities. This is treated differently than “malicious hacking,” the act of entering someone’s computer without their knowledge to take data or leave viruses.

Hacking involves gaining unauthorized access to a computer system or network. It can be done for various purposes such as stealing sensitive information, disrupting system operations, or installing malicious software.

Hacking is using technical skills or tools to exploit security vulnerabilities in a device, system or network to gain unauthorized access. This is usually the entry point to a range of other criminal activities that build on this initial intrusion. Although hackers can sometimes be described as “ethical” or “white hat” hackers, exposing vulnerabilities so that they can be fixed, hacking more frequently refers to cybercrimes. A common misconception is that hackers are lone individuals sneaking around inside systems, but hackers today often operate in cabals, trading knowledge and tools, working for themselves for financial gain or for state actors who use them for espionage as well. A successful intrusion may go undetected by the victim for a long time.

A significant recent example is the SolarWinds hack. SolarWinds is a cybersecurity company that provides remote administrative security services to a huge list of corporate and government clients. Hackers penetrated their defenses, then surreptitiously included malware in an update that SolarWinds pushed out to its customers. SolarWinds acknowledged that around 18,000 customers downloaded that update, making all of them potentially vulnerable.

#### Piracy

Piracy is a computer crime that occurs when a person distributes copyrighted material without gaining permission from the original owner. The shared material can be different types of media, including music, software, movies, images, and books. There are many sharing websites that practice internet piracy by offering free, downloadable versions of products. In many jurisdictions, it is only the sharing of materials that is illegal, and being in receipt may not be illegal. However, many peer-to-peer systems require users to share material with others as it is being downloaded, resulting in a form of collaborative piracy. The charges for piracy differ from case to case, so it is important to contact and attorney to assure that you are correctly informed about the laws regarding your specific situation.

#### Phishing

Phishing is a form of cybercrime in which someone uses the internet to try and trick someone else into giving them their login information, often using a fake website or email.

Phishing is an attack in which a seemingly genuine email or text message convinces someone to divulge sensitive account information without realizing it. The most common form is called “bulk phishing,” which targets many people simultaneously.

In this attack, criminals impersonate real banks, retailers, payment service providers and so on by designing emails and websites that look legitimate at a casual glance. A typical call to action might include a button labeled “verify your account information” that takes you to a fake site to input your credentials, or downloads malware that can harvest your account information without your knowledge.

#### Cyber Stalking/Harassment

Cyberstalking is often used to describe the act of stalking a person online, such as by repeatedly sending them unwanted messages or using the internet to track their location. The victim of cyber stalking is subjected to an excessive number of online messages, whether through social media, web forums, or email.

It is common for the perpetrator to have real world contact with the victim but use the internet to stalk them instead of stalking them in the physical sense. It could progress into traditional stalking if the perpetrator feels they need to make more of an impact on their victim’s lives

#### Identity theft

Identity theft in the world of computer crimes involves a form of hacking where the perpetrator accesses the victim’s sensitive information such as their Social Security Number (SSN), bank account information, or credit card numbers. They then use this information to spend their victim’s money for online shopping or simply to steal the money through fraudulent transfers.

#### Denial of Service (DoS)

Denial of service (DoS) cyberattacks are designed to make a website or other online service unavailable or unusable to other users. This is often accomplished by flooding a website with requests, causing it to slow down or crash.

Examples of denial of service cyberattacks include a person using a computer or a botnet to send a large number of requests to a website to overload its servers.

#### Copyright Infringement

Copyright infringement is stealing or sharing copyrighted materials without the owner's permission. The biggest example of copyright infringement is the act of sharing copyrighted music, videos, and other content through file-sharing sites.

Copyright infringement cybercrimes occur when someone illegally downloads copyrighted content, such as when someone uses a BitTorrent client to download music and movies illegally.

#### Child Pornography/Abuse

This cybercrime can involve the perpetrator looking to create or distribute sexual images of children. In some cases, the accused seeks out minors on the internet, whether that be via social media or chatrooms with the objective of producing child pornography. The government monitors a large amount of chat rooms in hopes to reduce and prevent this type of exploitation, and also maintains databases of existing child pornographic content that may be shared. Convictions for these charges typically mean long prison

sentences. It is important to contact an attorney in the case of any accusations of these crimes because the punishments are so severe.

# Hacking and Cracking

Hackers are specialized in building, and crackers in breaking. That is the fundamental difference between hacking as well as cracking concerning computer security. A lot of factors and various actors are involved in both. While some players act with malice, others don’t; some are equipped with the skills for putting your system down, and others are just looking for a loophole to make use of. Let’s explore the ways hacking is different from cracking.

## Hacking

Any attempt to intrude into a computer or a network without authorization is called hacking. This involves changing of system or security features in a bid to accomplish a goal that differs from the intended purpose of the system. It can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

An individual who involves themselves in hacking activities is known as a hacker, and some companies employ hackers as part of their support staff. These kinds of hackers use their skills to find flaws in the company security system, to prevent identity theft and other computer-related crimes against the company.

There are various kinds of hackers: the most common are white hats, black hats and grey hats.

* White hats hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organization.
* Black hat hackers hack to take control over the system for personal gains. They destroy, steal and even prevent authorized users from accessing the system, by finding loopholes and weaknesses in the system.
* Grey hat hackers comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system. They then notify the network system admin about the weaknesses discovered in the system.

## Cracking

Whereas hacking is the process of intruding computer systems without authorization in order to gain access to them, for good or bad purposes, cracking is the same practice though with criminal intention. However, cracking is generally less harmful than hacking.

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.

A cracker is someone who breaks into a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. Crackers also act as Black Hats: by gaining access to the accounts of people maliciously and misusing this information across networks. They can steal credit card information, they can destroy important files, disclose crucial data and information or personal details and sell them for personal gains.

There are various types of crackers that include script kiddies, packet monkeys, skiddiest, lamers, warez d00dz, and wannabes. Some of the characteristics of crackers include:

* Less skilled and do not possess necessary in-depth knowledge about programming and codes.
* Always rely on the software tools created by others to carry out their operations.
* They only know the process of cracking the security networks and they lack the advanced knowledge.

#### Types of Cracking

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.

Password Cracking

Password cracking is the act of stealing people’s passwords from databases. But this is often more difficult than it sounds since most websites and services now encrypt their password databases using a one-way process called hashing.

Hashing cannot be reversed, so the cracker needs to:

1. Find and obtain the website’s hashes and the algorithms and processes used to create them (also known as the hash function).
2. Generate a password, apply the hash function, and see if it grants authentication. Because this process would be so time-consuming if done manually, crackers employ powerful software to automate the guesswork. The two most common methods of cracking a password are:

**Brute-forcing.** Brute-force cracking involves pumping out a massive amount of guessed characters until it gets a match to the hash algorithm. This also includes a dictionary attack which involves guessing the actual words used in the password.

* + **Rainbow table cracking.** A rainbow table is a table of precomputed hash chains. This helps crackers overcome difficulties in large password sets where brute- forcing is infeasible. Using the table, crackers use programs to try and determine a website's hash function.

#### Software cracking

Software cracking involves changing a program or piece of software. Usually, software cracking is done to remove paid software requirements or pop-up purchase reminders so that people can access the software for free. “Cracked” software is a paid program that has had its copy protections removed.

#### Network Cracking

Network cracking is the act of infiltrating a local area network (LAN). Sometimes referred to as web cracking or wired equivalent privacy (WEP) cracking, this usually involves accessing poorly secure networks. To illustrate how network cracks work, consider your home Wi-Fi system and all of the devices connected to it. These devices make up a wireless LAN that cracker can target. Wireless networks are favorable since a cracker doesn’t need a physical connection (like they would with a wired network). If your Wi-Fi network has no password protection, anyone could stand in its range and connect. But if it is password-protected, they will need to employ password cracking techniques to gain access. Once they have access, they can infiltrate any of your connected devices (known as computer cracking) and monitor your web traffic. With this ability, they can steal your data, access your accounts, or try to impersonate you.

## The difference between hacking and cracking

The fundamental difference between both is that while a hacker makes use of their in-depth knowledge of computer logic and code, a cracker seeks back doors in programs and uses these back doors for their

(cracker’s) maximum benefit. Hacking involves breaking into the security systems for the main objective of finding holes in the system and trying to rectify them, whereas cracking has to do with breaking into the security system for illegal and criminal purposes or for selfish reasons.

Also, one has more malicious intent than the other. Crackers tend to possess in-depth knowledge of code that is related to Python, Objective C (Mac), and .NET (Visual Basic, C++, C, C#), whereas hackers have extensive knowledge of various types of web code, such as MySQL, PHP, HTML, CSS, JavaScript, and Ajax. To understand the difference between hacking and cracking, you have to know what hacking is in the first place.

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. For example, many companies hire white hat hackers to check their security systems and make them as hack-proof as possible.

Cracking, on the other hand, is any kind of hacking that’s done for personal gain or other malicious reasons. Crackers, also referred to as black hat hackers, might take control over a system to destroy or steal information for profit, attempt to scam people, or just cause damage for the sake of it.

**Wrapping up**

Hacking involves making use of knowledge to only help strengthen the security of networks and systems while cracking will exploit knowledge for breaking the law. Though the 2 terms are interchangeably used, having outlined the differences between them above, you know better that they are not the same.

#### Ethical difference

Hackers are the good guys, white hats who break into networks to discover loopholes, and to restore the security of corrupted networks to build a secure system. They never do it illegally and always inform their hiring organization or individual of their actions. They're a great weapon in the hunting down and catching of crackers. Crackers, however, will break into the same system for personal, financial or any other kind of gain without the knowledge or permission of the system owners, for the purpose of engaging in illegal activities.

#### Skill difference

Hackers possess the ability to create programs and software tools; they're skilled in multiple codes and languages and have advanced knowledge of various select computer languages. Crackers, on the other hand, don't need to possess a deep well of knowledge, save for the one on how to actually break a system, and we don't normally see them being skilled enough to create their own programs. Even with so few crackers skilled enough to create tools and software to help them exploit the weaknesses they discover, we should never ignore their threat.

# What is encryption?

Encryption is the process of converting plain text or data into an unreadable format using a mathematical algorithm, known as a cipher. This is done to protect the confidentiality and privacy of the information being transmitted or stored. The process of encryption involves using a key, which is a unique code that is used to encrypt and decrypt the data.

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

When data is encrypted, it can only be read and understood by someone who has the key to decrypt it. This ensures that even if the encrypted data is intercepted by an unauthorized person, they will not be able to understand the content. Encryption is widely used to secure sensitive information such as financial transactions, personal data, and classified government documents. In computing, unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms, or ciphers.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a [key](https://www.techtarget.com/searchsecurity/definition/key), is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys

were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

## How Encryption Works

Encryption works by transforming plain text or data into an unreadable format using a mathematical algorithm, known as a cipher. The process of encryption involves using a key, which is a unique code that is used to encrypt and decrypt the data. Original information, or plain text, might be something as simple as "Hello, world!" As cipher text, this might appear as something confusing like 7\*#0+gvU2x—something seemingly random or unrelated to the original plaintext.

Encryption, however, is a logical process, whereby the party receiving the encrypted data—but also in possession of the key—can simply decrypt the data and turn it back into plaintext.

For decades, attackers have tried by brute force—essentially, by trying over and over again—to figure out such keys. Cybercriminals increasingly have access to stronger computing power such that sometimes, when vulnerabilities exist, they are able to gain access.

Data needs to be encrypted when it is in two different states: "at rest," when it is stored, such as in a database; or "in transit," while it is being accessed or transmitted between parties.

An encryption algorithm is a mathematical formula used to transform plaintext (data) into ciphertext. An algorithm will use the key to alter the data in a predictable way. Even though the encrypted data appears to be random, it can actually be turned back into plaintext by using the key again. Some commonly used encryption algorithms include Blowfish, Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), RC5, RC6, Data Encryption Standard (DES), and Twofish.

Encryption has evolved over time, from a protocol that was used only by governments for top-secret operations to an everyday must-have for organizations to ensure the security and privacy of their data.

example of how encryption works:

* + 1. Alice wants to send a message to Bob securely. She uses an encryption algorithm and a secret key to encrypt the message.
    2. The encrypted message is sent over an insecure channel, such as the internet.
    3. Bob receives the encrypted message and uses the same encryption algorithm and secret key to decrypt the message.
    4. Once the message is decrypted, Bob can read the original plain text message.

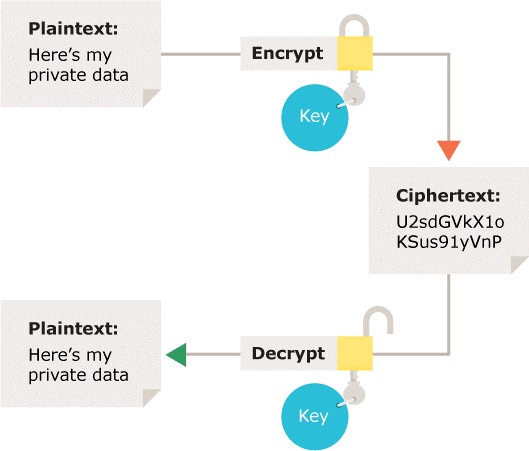
## Types of Encryptions

There are many different types of encryptions, each with its own benefit and use case.

#### symmetric encryption

In this simple encryption method, only one secret key is used to both cipher and decipher information. In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

While the oldest and best-known encryption technique, the main drawback is that both parties need to have the key used to encrypt the data before they can decrypt it. Symmetric encryption algorithms include AES-128, AES-192, and AES-256. Because it is less complex and executes faster, symmetric encryption is the preferred method for transmitting data in bulk.



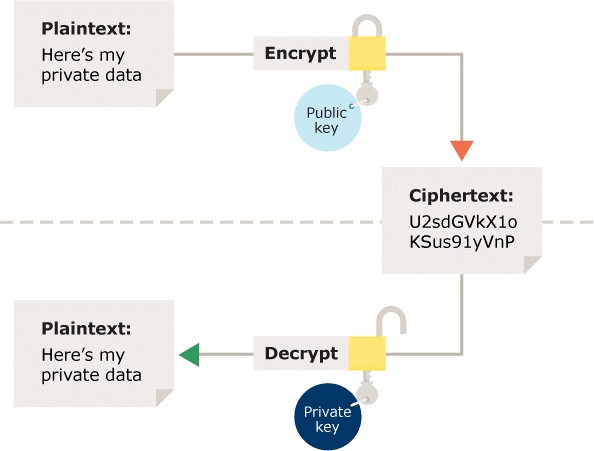
*Figure 1 Symmetric encryption – Using the same key for encryption and decryption*

#### asymmetric encryption

Also known as public key cryptography, asymmetric encryption is a relatively new method that uses two different but related keys to encrypt and decrypt data. Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key. One key is secret and one key is public. The public key is used to encrypt data, and the private key is used to decrypt (and vice versa). Security of the public key is not needed because it is publicly available and can be shared over the internet.

Asymmetric encryption presents a much stronger option for ensuring the security of information transmitted over the internet. Websites are secured using Secure Socket Layer (SSL) or Transport Layer Security (TLS) certificates. A query to a web server sends back a copy of the digital certificate, and a public key can be extracted from that certificate, while the private key stays private.

The private key is kept secret by the owner and the public key is either shared amongst authorized recipients or made available to the public at large . Data encrypted with the recipient’s public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorized or unlawful access to the data.



*Figure 2: Asymmetric encryption – Using a different key for the encryption and decryption process.*

## The uses of Encryption

Encryption has become an enormous asset to organizations, allowing them to confidently offer a more secure experience for employees, customers, and other stakeholders.

**Privacy and Security**

Encryption can prevent data breaches. Even if an attacker maliciously gains access to a network, if a device is encrypted, the device will still be secure, rendering attempts by the attacker to consume the data useless. Encryption ensures no one can read communications or data except the intended recipient or data owner. This prevents attackers from intercepting and accessing sensitive data.

**Regulations**

Encrypting data allows organizations to protect data and maintain privacy in accordance with industry regulations and government policy. Many industries, especially those in financial services and healthcare, have explicit rules on data protection.

**Secure Internet Browsing**

Encryption also keeps users safe while browsing the internet. Earlier in the internet's history, attackers found ways to steal unencrypted information sent between users and web services over the Hypertext Transfer Protocol (HTTP). The standard to encrypt web content by running HTTP over the Secure Socket Layer protocol emerged, soon to be replaced with the Transport Layer Security protocol, enabling enterprises, publishers, and e-commerce providers to offer a secure experience for users.

With encryption, users feel safer entering personal information into webpages and carrying out financial or e-commerce transactions.

**Encryption Keeps Sensitive Data Safe**

Encryption will continue to be a core security feature in everything from video chats to e-commerce to social media. Basically, if it can be shared or stored, it will be encrypted. Both organizations and individual users would benefit from keeping on top of encryption standards to ensure that both their personal and professional data is safe from misuse or compromise.

There are many other uses of encryption. These include:

* Encrypting data stored on a laptop hard disk. This is important as a laptop might contain sensitive information and could be easily stolen. If the hard disk is encrypted, the information will be unreadable unless the thief also has the key. In this situation it is usually a username and password.
* When sending sensitive information, such as passwords or credit card details, over the internet. When a website uses the HTTPS protocol information being transferred is encrypted. This means that if the connection is intercepted, the information will be unreadable.
* Encrypting a document, such as a spreadsheet, using software tools, before sending it to a colleague via the internet, for security purposes.
* Encrypting satellite TV transmissions to prevent users who do not subscribe from watching TV shows.

# Computer Security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Computer security refers to the protection of a computer's hardware and the data that it holds. Computer security can be implemented using passwords, encryption, and firewalls, and denying physical access to a computer's location.

Computer security is the protection that is set up for computer systems and keeps critical information from unauthorized access, theft, or misuse. There are various practices in place that are widely in use, mainly for the protection of computer systems and networks and preventing potential malicious activities. While computer hardware is secured in the same way that sensitive equipment such as lockers and doors are protected, critical information and system access and authorization, on the other hand, are protected through complex security tactics and practices

Computer security refers to the process of protecting computer systems and networks from unauthorized access, theft, damage, or disruption. Computer security involves a wide range of measures, including hardware, software, and procedural safeguards, to ensure the confidentiality, integrity, and availability of data and resources.

computer security is an ongoing process that requires constant vigilance and adaptation to new threats and risks. By implementing a comprehensive security strategy that includes access control, network security, encryption, backup and recovery, patch management, training and awareness, risk assessment, incident response, compliance, threat intelligence, and physical security, organizations can protect their computer systems and data from a wide range of security threats.

## Use of Computer Security

If a computer security system is not put in place until a problem arises, it could lead to major issues and concerns, and it will be too late to resolve them. Especially in a data-driven world, it is imperative to keep all kinds of information from malicious hackers and prevent vital information from falling into the wrong hands for misuse. Computer security helps keep valuable information protected and maintain the health

of a computer with no disruptive behavior in its performance caused by viruses and malware. The other use of computer security include:

#### Data Protection:

One of the primary advantages of computer security is that it protects sensitive data from unauthorized access, theft, or damage. This includes personal data, financial data, confidential business data, and other types of sensitive information.

#### Business Continuity:

Computer security measures such as backup and recovery ensure that critical systems and data can be restored in the event of a disaster, such as a natural disaster, cyber-attack, or hardware failure. This helps to ensure business continuity and minimize downtime.

#### Regulatory Compliance:

Many industries are subject to government regulations and industry standards regarding data privacy and security. Implementing computer security measures can help organizations comply with these regulations and avoid costly penalties.

#### Reputation Management:

Data breaches and other security incidents can damage an organization's reputation and erode customer trust. Computer security measures can help to prevent these incidents and demonstrate a commitment to data privacy and security, enhancing the organization's reputation.

#### Cost Savings:

While implementing computer security measures requires an investment of time and resources, it can ultimately save money by reducing the risk of security incidents, minimizing downtime, and avoiding costly penalties for noncompliance.

Overall, computer security is a complex and ever-evolving field that requires ongoing attention and investment to stay ahead of emerging threats and risks. By implementing a comprehensive security strategy that includes multi-factor authentication, vulnerability scanning, penetration testing, SIEM, cloud security, and mobile device security, organizations can protect their computer systems and data from a wide range of security threats. computer security is essential for protecting sensitive data, ensuring business money. By implementing comprehensive security measures, organizations can reduce their risk of security incidents and protect their valuable data and resource

## components of computer security:

**Access Control**: Access control is the process of limiting access to computer systems and resources to authorized users only. This is typically accomplished through the use of passwords, encryption, biometric authentication, and other techniques.

**Network Security**: Network security involves protecting computer networks from unauthorized access, theft, or damage. This is typically accomplished through the use of firewalls, intrusion detection systems, and other security measures.

**Encryption**: Encryption is the process of converting plain text or data into an unreadable format using a mathematical algorithm, known as a cipher. Encryption is used to protect sensitive data such as financial data, personal information, and confidential business data.

**Backup and Recovery:** Backup and recovery is the process of creating backups of important data and systems and developing plans for restoring them in the event of a disaster, such as a natural disaster, cyber- attack, or hardware failure.

**Patch Management**: Patch management involves regularly updating software and operating systems to address security vulnerabilities and prevent unauthorized access or damage to the system.

**Training and Awareness:** Computer security also involves educating users about best practices for protecting computer systems and data. This includes training users on how to create strong passwords, avoid phishing scams, and report security incidents.

## Types of Computer Security

Here are a few types of computer security tactics that are used widely for the protection of software, hardware, electronic data, and network in computer systems.

#### Application Security

Application security is the introduction of security features in applications during their development process. This actively helps prevent potential cyber threats such as data breaches, denial-of-service attacks (DoS), SQL injection, and many others. Some examples of application security tools are antivirus software, firewalls, web application firewalls, encryption, etc.

#### Information Security

If you are worried about the unauthorized use of your computer system or breach of its confidentiality, availability, and integrity, you may employ information security. Information security is a set of practices that aim to protect the confidentiality, integrity, and availability (known as the CIA triad) of data from unauthorized access and misuse.

#### Network Security

Network security is any activity that aims to protect the integrity and usability of a network and data. It consists of both hardware and software technologies that are specifically designed to prevent unauthorized intrusion into computer systems and networks.

#### Endpoint Security

End-users are increasingly becoming the biggest security risk unintentionally. With no-fault from their end, exempting the lack of awareness, the virtual gates of an organization are open to hackers and attacks. Most of the end-users are unaware of the ICT policy, and therefore, it is imperative that the users who handle sensitive information on a regular basis understand and be knowledgeable about all comprehensive security policies, protocols, and procedures.

#### Internet Security

Internet security is one of the most important types of computer security that come with a set of rules and protocols that focus on specific threats and activities that happen online. It provides protection against hacking, DoS attacks, computer viruses, and malware.

# Software piracy

Software piracy is the unauthorized use, reproduction, or distribution of software. This can include downloading software from the internet without paying for it, sharing software with others illegally, or using counterfeit or unlicensed software.

Software piracy is the unauthorized use or distribution of copyrighted software. This can take many forms, such as copying software from one computer to another, downloading software from the internet without paying for it, or selling unauthorized copies of software.

Software piracy is a significant problem that can have both financial and legal consequences for individuals and businesses. Piracy can lead to lost revenue for software developers and publishers, as well

as reduced investment in new software development. It can also lead to security risks, as pirated software may contain viruses or other malware.

Software piracy is a serious issue that can have significant financial and legal consequences for both individuals and companies. Piracy can lead to lost revenue for software developers and publishers, as well as reduced investment in new software development. It can also lead to security risks, as pirated software may contain viruses or other malware.

Many countries have laws that prohibit software piracy, and companies often take legal action against individuals or organizations engaged in piracy. To combat piracy, software developers and publishers may use digital rights management (DRM) technologies to prevent unauthorized use or distribution of their software, or offer subscription-based or cloud-based services that make it more difficult to pirate their software.

It is important for individuals and businesses to use software legally and ethically, and to report instances of software piracy to the appropriate authorities. By doing so, we can help to support the development of innovative software solutions and protect against the risks associated with piracy.

## What are some legal consequences of software piracy?

The legal consequences of software piracy can vary depending on the country and the severity of the offense. In general, software piracy can result in civil and criminal penalties, including fines, imprisonment, and seizure of equipment used in the piracy.

The consequences of software piracy can be significant. In addition to legal consequences, such as fines and imprisonment, software piracy can also have financial consequences. Piracy can lead to lost revenue for software developers and publishers, which can reduce their ability to invest in new software development. It can also harm the broader economy by reducing employment opportunities and innovation.

In many countries, software piracy is a violation of copyright law, which can result in civil lawsuits filed by the software developer or publisher. In some cases, these lawsuits can result in significant financial damages, which can be many times the cost of the pirated software.

In addition to civil penalties, some countries also have criminal penalties for software piracy. Criminal penalties can include fines and imprisonment, and can be particularly severe in cases of large-scale piracy or commercial piracy.

In some cases, individuals or organizations engaged in software piracy may also be subject to seizure of equipment used in the piracy, such as computers or servers. This can have significant financial and operational consequences for businesses engaged in piracy.

Overall, the legal consequences of software piracy can be severe, and it is important for individuals and organizations to take steps to ensure that they are using software legally and ethically.

## Forms of Software piracy

1. **Counterfeiting**: This involves copying software and selling it as a legitimate product.
2. **Softlifting**: This is when an individual or organization installs a single licensed copy of software on multiple computers without authorization.
3. **Internet piracy**: This involves illegally downloading or sharing software over the internet.
4. **End-user piracy:** This is when an individual or organization makes unauthorized copies of software for personal or business use.
5. **Hard-disk loading**: This is when a computer seller installs pirated software onto a computer system before selling it.

Software piracy can have a significant impact on the software industry, as well as on the broader economy. According to some estimates, software piracy costs the industry billions of dollars each year in lost revenue. This can have a ripple effect on the economy, as reduced revenue can lead to reduced investment in new software development, which can in turn reduce employment opportunities and innovation.

In addition to the financial impact of software piracy, there are also security risks associated with using pirated software. Pirated software may contain viruses or other malware, which can lead to data loss, system crashes, and other problems. In some cases, pirated software may also contain backdoors or other vulnerabilities that can be exploited by hackers.

To combat software piracy, many countries have laws that prohibit the unauthorized use, reproduction, or distribution of software. Companies may also take legal action against individuals or organizations

engaged in piracy, which can result in significant fines and other penalties. In addition, software developers and publishers may use digital rights management (DRM) technologies to prevent unauthorized use or distribution of their software, or offer subscription-based or cloud-based services that make it more difficult to pirate their software.

Ultimately, it is important for individuals and businesses to use software legally and ethically. By doing so, we can help to support the development of innovative software solutions and protect against the risks associated with piracy.

# What is privacy

Privacy refers to the ability of individuals to control the collection, use, and disclosure of their personal information. It is the right to be left alone and to have control over one's personal data.

Privacy is a fundamental human right that is recognized in many international human rights treaties and national constitutions. It is closely related to other rights, such as freedom of expression, association, and assembly. The right to privacy protects individuals' personal autonomy and dignity, and enables them to make personal choices without fear of surveillance, intrusion, or discrimination.

Privacy is a complex issue that is impacted by many factors, such as technology, culture, and social norms. In recent years, advances in technology, such as the growth of the internet and the rise of social media, have created new challenges for privacy.

In the digital age, privacy has become a complex issue, as individuals' personal information is often collected, stored, and shared by companies and governments. This has led to concerns about data breaches, identity theft, and other privacy violations. In some cases, individuals may not even be aware that their personal information is being collected or used.

To protect privacy, many countries have laws and regulations that govern the collection, use, and disclosure of personal information. For example, the GDPR in the European Union provides individuals with certain rights, such as the right to access, correct, and delete their personal data, and requires companies to obtain explicit consent before collecting and using personal data.

In addition to legal protections, individuals can also take steps to protect their privacy, such as using strong passwords, avoiding sharing personal information on social media, and using encryption and other security tools to protect their data.

Privacy can be divided into different categories, such as physical privacy, which involves the right to be free from physical surveillance and intrusion into one's personal space, and informational privacy, which involves the right to control the collection, use, and disclosure of personal information.

In today's digital age, privacy has become an increasingly important issue, as individuals' personal information is often collected, stored, and shared by companies and governments. This has led to concerns about data breaches, identity theft, and other privacy violations.

One of the biggest challenges to privacy in the digital age is the collection and use of personal data by companies and governments. Personal data can include a wide range of information, such as names, addresses, phone numbers, email addresses, social security numbers, and more. This data can be used for a variety of purposes, such as marketing, research, and law enforcement.

privacy is an important right that can help individuals to maintain control over their personal information and protect themselves against the risks associated with its misuse. As technology continues to advance, it will be important for individuals and society as a whole to continue to address and adapt to new challenges to privacy.

# Define cyber-crime, cyber terrorism, cyber terrorist

Cybercrime refers to criminal activities that are carried out using computers, networks, or the internet. Cybercriminals use technology to commit crimes such as identity theft, fraud, hacking, and cyberstalking.

Cybercrime is a type of crime that involves the use of computers, networks, and the internet to commit illegal activities. Cybercriminals may use various techniques to exploit vulnerabilities in computer systems, steal personal or sensitive information, disrupt computer networks, or launch attacks on individuals, organizations, or governments. Examples of cybercrime include hacking, phishing, identity theft, cyberstalking, cyberbullying, ransomware attacks, and distributed denial-of-service (DDoS) attacks. Cybercrime is a growing concern worldwide, as the increasing dependence on technology has made individuals and organizations more vulnerable to these types of attacks.

Cybercrime can have serious consequences, both for individuals and for organizations. It can result in financial losses, damage to reputations, and even physical harm in some cases. As a result, it is important for individuals and organizations to take steps to protect themselves from cyber threats, such as using strong passwords, keeping software up-to-date, and using antivirus software and firewalls.

Cyber terrorism is a form of terrorism that involves the use of technology to carry out attacks. Cyber terrorists may use tactics such as hacking, denial-of-service attacks, and the spread of malware to disrupt computer systems, cause damage, or steal information. The goal of cyber terrorism is typically to cause fear, panic, and economic damage.

Cyber terrorism refers to the use of technology and the internet to carry out terrorist activities. It involves the use of cyberspace to plan, coordinate, and execute attacks on computer systems, networks, and critical infrastructure, with the aim of causing widespread disruption, destruction, or fear.

Cyber terrorism is a growing concern for governments and organizations around the world, as the increasing dependence on technology has made individuals and societies more vulnerable to these types of attacks.

Cyber terrorism can take many forms, including hacking into government or corporate networks to steal sensitive information, launching distributed denial-of-service (DDoS) attacks on critical infrastructure such as power grids or financial systems, and using social media or other online platforms to spread propaganda or incite violence.

The potential consequences of cyber terrorism are significant. An attack on critical infrastructure, such as a power grid or transportation system, could have serious economic and social consequences. An attack on a financial system could cause widespread financial instability. An attack on a government or military network could compromise national security.

Governments and organizations around the world are taking steps to prevent and respond to cyber terrorism. This includes investing in cybersecurity measures, developing emergency response plans, and increasing collaboration and information sharing between countries and organizations to better detect and prevent cyber-attacks.

cyber terrorism is a complex and evolving threat that requires ongoing efforts from governments, organizations, and individuals to prevent and mitigate its impact.

#### challenges of Cyber terrorism

One of the challenges of dealing with cyber terrorism is the difficulty in identifying and apprehending perpetrators. Cyber terrorists can operate from anywhere in the world and may use techniques to conceal

their true identities and locations. This makes it difficult for law enforcement agencies to track them down and bring them to justice.

Another challenge is the constantly evolving nature of cyber threats. Cyber terrorists are constantly developing new techniques and tools to carry out attacks, and it can be difficult for governments and organizations to keep up with these evolving threats.

To address these challenges, governments and organizations are taking a multi-faceted approach to preventing and responding to cyber terrorism. This includes investing in cybersecurity infrastructure and capabilities, developing emergency response plans, and increasing collaboration and information sharing between countries and organizations.

In addition, there is a growing emphasis on the importance of public awareness and education about cyber threats. This includes educating individuals and businesses on how to better protect themselves from cyber-attacks, and encouraging them to report suspicious activity to law enforcement agencies.

#### characteristics of cyber terrorism

One of the key characteristics of cyber terrorism is that it is often carried out by non-state actors, such as terrorist groups, rather than by governments. This makes it difficult for governments to respond to cyber terrorism in the same way that they would respond to a traditional military attack.

Cyber terrorism can also have significant economic consequences. For example, a successful attack on a financial institution could result in the theft of millions of dollars or cause widespread financial instability. An attack on critical infrastructure, such as a power grid or transportation system, could disrupt essential services and have a significant impact on the economy.

To prevent and respond to cyber terrorism, governments and organizations are investing in a range of cybersecurity measures. This includes developing advanced technologies and tools to detect and prevent attacks, as well as investing in the training and development of cybersecurity professionals.

A cyber terrorist is an individual or group that carries out cyber terrorism. Cyber terrorists may be motivated by political, ideological, or financial reasons, and they may target a variety of organizations, including governments, businesses, and individuals.

A cyber terrorist is an individual or a group that uses technology and the internet to carry out terrorist activities. Cyber terrorism involves the use of cyberspace to plan, coordinate, and execute attacks on

computer systems, networks, and critical infrastructure, with the aim of causing widespread disruption, destruction, or fear.

A cyber terrorist could use a range of techniques to carry out their attacks, including hacking into government or corporate networks to steal sensitive information, launching distributed denial-of-service (DDoS) attacks on critical infrastructure such as power grids or financial systems, or using social media or other online platforms to spread propaganda or incite violence.

The motivations of cyber terrorists can vary, but they are typically driven by political or ideological goals rather than financial gain. Cyber terrorists may seek to advance a particular political or ideological agenda, or to create fear and chaos in order to undermine social or political stability.

# Write down some of the Ethical and Unethical code of ethics in IT Areas ethical code of ethics

### Ethical code of Conduct in IT:

1. Respect for privacy: IT professionals should respect the privacy of individuals and ensure that personal information is protected and used only for the intended purpose.
2. Honesty: IT professionals should be honest and transparent in their dealings with clients, colleagues, and other stakeholders.
3. Professionalism: IT professionals should maintain a high level of professionalism in their work, including being responsive to client needs, meeting deadlines, and providing high-quality work.
4. Confidentiality: IT professionals should maintain the confidentiality of sensitive or confidential information, and should not disclose such information without appropriate authorization.
5. Respect for intellectual property: IT professionals should respect the intellectual property rights of others, including copyrights, trademarks, and patents.
6. Transparency: IT professionals should be transparent in their processes, decision-making, and communication with clients and stakeholders.
7. Responsibility: IT professionals should take responsibility for their work, be accountable for their actions, and strive to deliver projects that are of high quality and meet client expectations.
8. Continuous learning: IT professionals should engage in continuous learning and professional development to stay up-to-date with technology advancements, industry standards, and best practices.
9. Collaboration: IT professionals should cultivate a culture of collaboration, teamwork, and mutual respect, and work towards achieving shared goals and objectives.
10. Social responsibility: IT professionals should recognize their role in society and work towards the betterment of society, including contributing to initiatives that promote sustainability, social justice, and equal access to technology.

### Unethical Codes of Conduct in IT:

1. **Plagiarism**: IT professionals should not engage in plagiarism, which involves taking credit for someone else's work without permission or attribution.
2. **Misuse of technology**: IT professionals should not use technology to engage in illegal or unethical activities, such as hacking, cyber stalking, or identity theft.
3. **Discrimination**: IT professionals should not engage in discrimination based on race, gender, age, religion, or other factors.
4. **Breach of confidentiality**: IT professionals should not disclose sensitive or confidential information without appropriate authorization, and should take steps to ensure that such information is protected from unauthorized access.
5. **Conflict of interest**: IT professionals should avoid conflicts of interest, such as accepting work from clients that may compromise their objectivity or integrity.
6. **Malware creation and distribution**: IT professionals should not create or distribute malware, which can cause harm to individuals, organizations, and society at large.
7. **Extortion**: IT professionals should not engage in extortion or blackmail, which involves threatening individuals or organizations with harm if they do not comply with demands.
8. **Insider trading**: IT professionals should not engage in insider trading, which involves using confidential information to make personal financial gains.
9. **Placing personal interests above clients**: IT professionals should not prioritize their personal interests over those of their clients, as this can lead to conflicts of interest, breaches of confidentiality, and poor- quality work.
10. **Discriminatory algorithms**: IT professionals should be aware of the potential for bias and discrimination in the algorithms they develop and ensure that they are fair, unbiased, and do not perpetuate discriminatory practices.

Adhering to ethical codes of conduct is critical in the IT industry, as it helps to promote trust, integrity, and accountability among IT professionals and stakeholders. By following ethical principles, IT professionals can help to ensure that technology is used for the betterment of society and that it does not cause harm or perpetuate unethical practices.

Overall, IT professionals are expected to adhere to a high standard of ethical conduct in their work, and to act with honesty, integrity, and professionalism at all times. By following ethical codes of conduct, IT professionals can build trust with clients, colleagues, and other stakeholders, and contribute to the overall success and reputation of the IT industry.

# Conclusions

The growth and advances in digital technology creates a whole new platform for criminal activity. Since the advancement of technology, any crime that involves using a computer or network is generally referred to as a cybercrime or computer crime.

hacking and cracking are two terms that are often used interchangeably, but they refer to two very different activities. Hacking refers to the act of using one's knowledge of computer systems to access and modify them in a legitimate and ethical manner, such as identifying and fixing security vulnerabilities. On the other hand, cracking refers to the act of using one's knowledge of computer systems to illegally gain unauthorized access or control of them, such as stealing sensitive data or disrupting computer networks.

Encryption is used in a wide range of applications, including online transactions, communication, and data storage. It is particularly important for protecting sensitive information such as financial data, medical records, and personal information.

computer security is an ongoing process that requires a comprehensive approach to protect computer systems and data from a wide range of threats. By implementing strong security measures, staying informed about emerging threats, and prioritizing computer security as a key aspect of risk management, individuals and organizations can help to prevent cyber-attacks and protect sensitive information.

In general, individuals and organizations in the IT industry should prioritize ethical conduct and adhere to established codes of conduct in order to promote trust, credibility, and responsible behavior. By doing so, they can help to ensure that technology is used in a way that benefits society as a whole while minimizing potential harm.

# Reference

https://[www.britannica.com/technology/computer-security](http://www.britannica.com/technology/computer-security) https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537 https://us.norton.com/blog/privacy/what-is-encryption https://[www.fortinet.com/resources/cyberglossary/encryption](http://www.fortinet.com/resources/cyberglossary/encryption) https://[www.ibm.com/topics/encryption](http://www.ibm.com/topics/encryption)

https://[www.cloudflare.com/learning/ssl/what-is-encryption/](http://www.cloudflare.com/learning/ssl/what-is-encryption/) https://[www.formpl.us/blog/workplace-ethics](http://www.formpl.us/blog/workplace-ethics) https://poe.com/Sage https://[www.slideshare.net/lineking/key-distribution](http://www.slideshare.net/lineking/key-distribution) https://[www.edureka.co/blog/what-is-computer-security/](http://www.edureka.co/blog/what-is-computer-security/)

https://[www.edureka.co/blog/cybersecurity-fundamentals-introduction-to-cybersecurity/](http://www.edureka.co/blog/cybersecurity-fundamentals-introduction-to-cybersecurity/) https://[www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html](http://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html) https://[www.computerhope.com/jargon/c/computer-security.html](http://www.computerhope.com/jargon/c/computer-security.html)