CYBER SECURITY

Unit-1

Syllabus

INTRODUCTION TO CYBER CRIME : Cybercrime- Definition and Origins of the word Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens.

Cyber offenses: How Criminals Plan the Attacks, Social Engineering, Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector.

Cyber Security

Definition

Cyber Security is the practice of protecting systems, networks, and programs from digital attacks.

Protecting Digital Systems

“Cyber security is the protection of internet-connected systems, including hardware, software, and data, from cyber attacks”. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information.

Need for Cyber Security

We need cyber security to protect our private data, intellectual data, banking and financial data, national security, and sensitive data.

Cybercrime

Cybercrime is “unlawful acts wherein the computer is either a tool or target or both”.

Alternative Definitions of Cybercrime

Digital Technology

Cybercrime involves any criminal activity conducted using digital technology.

Targets and Tools

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Illegal Activity

Cybercrime is illegal activity involving computers, the internet, or network devices.

Financial Dishonesty

Any financial dishonesty that takes place in a computer environment.

Types of Attacks Prevalent in Cybercrime

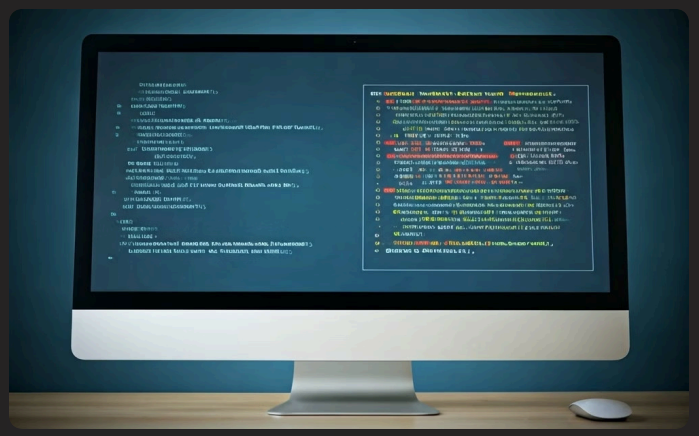
Techno-crime

The primary goal of techno-crime is typically financial gain, theft of information, or causing harm to individuals, organizations, or society. It is a premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. Example: Imagine someone hacks into a bank's computer system and steals money from people's accounts.

Techno-vandalism

Techno-vandalism is when someone uses technology to intentionally cause damage or disrupt systems, but not necessarily for financial gain.
Example: If someone spreads a computer virus that crashes other people's computers or websites just for fun or to cause trouble, that's techno-vandalism. They're not trying to steal anything, just to cause harm or disruption.

Difference b/w Cybercrime and Traditional Crime



Definition

Cybercrime committed using computers and the internet.

Traditional Crimes committed without the use of digital technology.

Tools Used

cybercrime :- Computers, smartphones, networks, and other digital devices.

Traditional crime :-Physical tools like weapons

Location

Cybercrime:-From any location with internet access.

Traditional crime:- Typically localized and requires physical presence.

Evidence Collection

Cybercrime:-Digital evidence like logs, IP addresses, and digital footprints.
Traditional Crime:-Physical evidence like fingerprints, DNA, and physical artifacts.

Examples

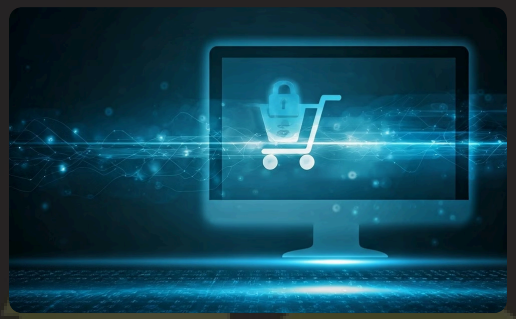
Cybercrime:-Hacking a company's database to steal sensitive information.

Traditional Crime:-Breaking into a house to steal valuables.

Classification Of Cyber Crime

Cybercrime Against Individuals

Cybercrime against individuals refers to criminal activities conducted using digital technologies that specifically target personal information, reputation, and personal safety of individuals.



Cybercrime Against Property

Cybercrime against property refers to illegal activities conducted via digital means that target an individual’s or organization’s property, including financial assets, intellectual property, and data.

Cybercrime Against Organizations

Cybercrime against organizations involves illegal activities that target a company's digital assets, systems, and data, often leading to financial loss, reputational damage, and operational disruptions.

Cybercrime Against Society

Cybercrime against society refers to illegal activities conducted through digital means that impact the broader public or specific groups within society. For Example :Banned websites illegal materials are made available to the people through the internet.

CLASSIFICATION OF CYBER CRIME

Cybercrime Against Individuals

E-Mail Spoofing

When an email appears to be from one source but is actually sent from another, it's called spoofing. It's often used to deceive people into giving away personal information.

Spamming

Spam is the term for unsolicited bulk messages sent to many people, often through electronic messaging systems. It's a nuisance and can be used to spread malware or scams.

Cyber Defamation

Cyber defamation is when false and harmful information about someone is spread online, damaging their reputation. It can be done through websites, emails, or social media posts.

Cyber Stalking

Cyberstalking involves using the internet and other electronic means to harass, intimidate, or threaten someone, causing fear and distress. It can include sending threats, monitoring online activity, and spreading false information.

Cybercrime Against Property

Credit Card Frauds

Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.

Intellectual Property (IP) Crimes

Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.

Internet Time Theft

Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.

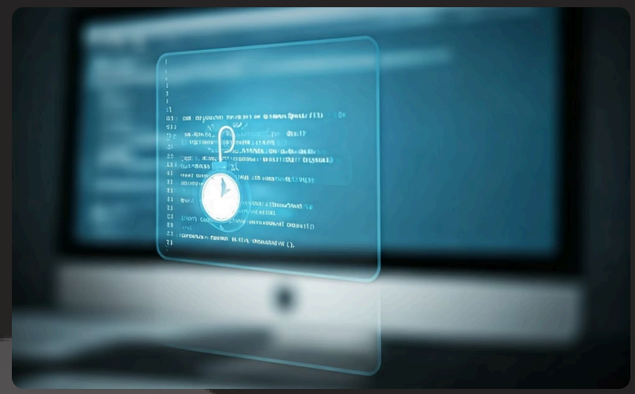
Cybercrime Against Organization

E-Mail bombing/Mail bombs

Sending a large number of emails to overwhelm the victim's email account or server.

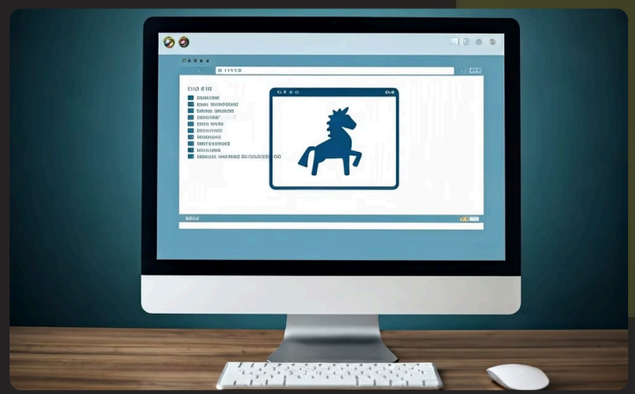
Salami Attack/Salami technique

Stealing small amounts of money from multiple accounts, adding up to a significant sum.



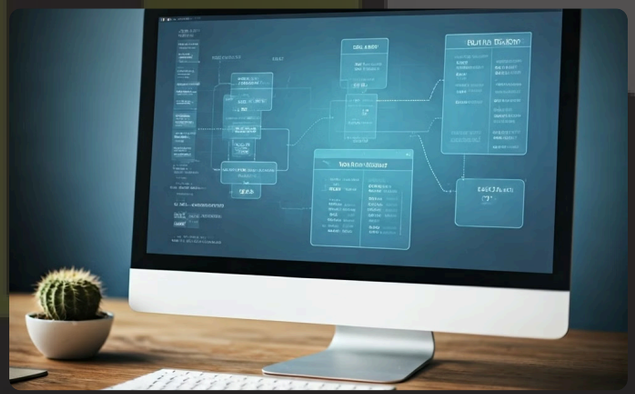
Logic Bomb

Malicious code that is activated under specific conditions, often after a period of time.



Trojan Horse

Malware disguised as legitimate software, granting unauthorized access to the computer.



Data Diddling

Altering data before it is processed by a computer, often for fraudulent purposes.

Cybercrime Against Society

Forgery

Currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners.

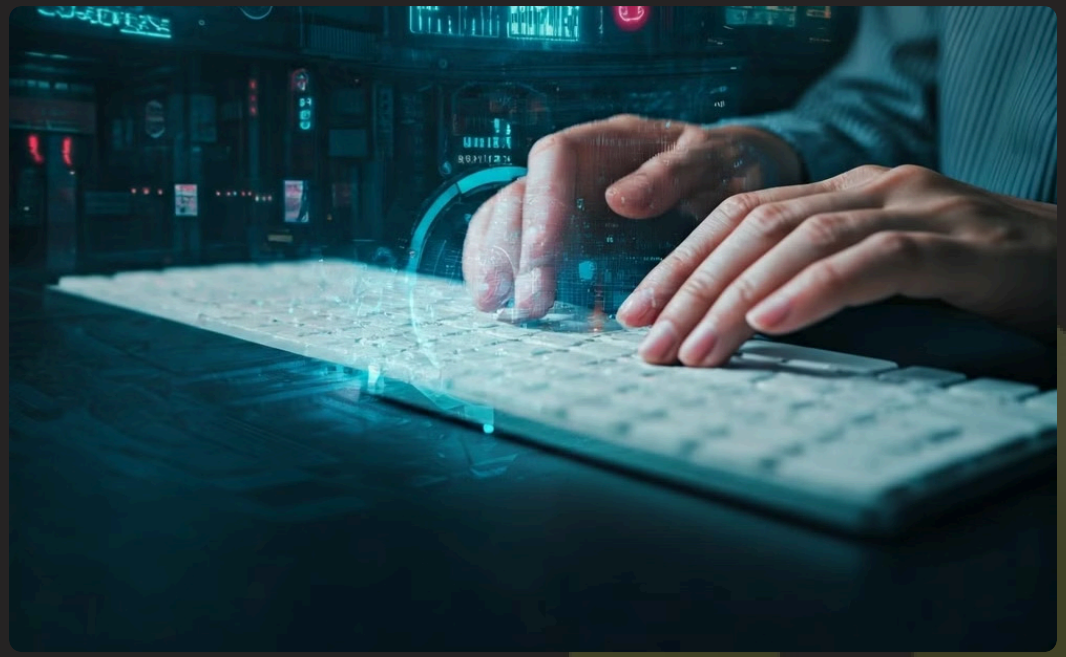
Cyberterrorism

It is defined as “any person, group or organization who, with terrorist intent, utilizes, accesses or aids in accessing a computer or computer network.

Web Jacking

Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). This crime involves “password sniffing”. The actual owner of the website no longer has any control over what appears on that website.

Origin of the Word "Cybercrime"



Cybernetics

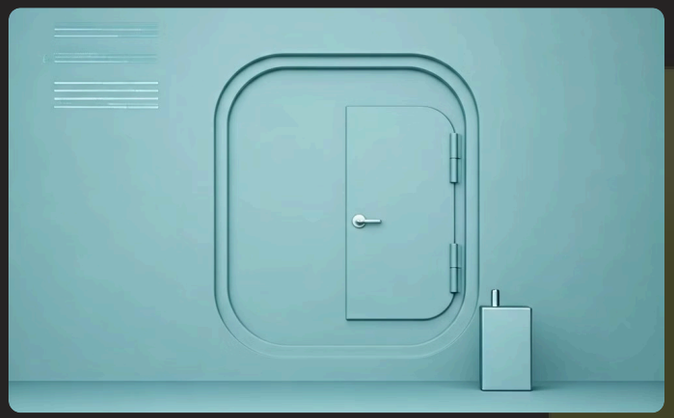
The term "cyber" is derived from "cybernetics," coined in 1948 by Norbert Wiener. It refers to the science of control and communication in animals, humans, and machines. The term "cyber" became associated with computers and networks in the 1980s, popularized by science fiction.

Crime

The word "crime" has ancient roots, originating from the Latin "crimen," meaning "accusation" or "charge." The term "cybercrime" emerged in the late 20th century as digital technology advanced, encompassing illegal activities conducted through computer networks.

Information Security

Information security (InfoSec) refers to the processes and methodologies involved in protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It encompasses a wide range of practices and principles aimed at safeguarding data integrity, confidentiality, and availability. The CIA Triad is a fundamental concept in information security that stands for:

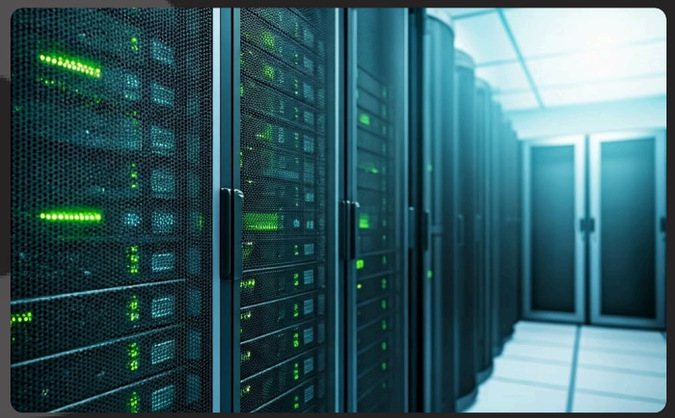


Confidentiality

Ensuring that information is accessible only to those authorized to have access. Techniques to maintain confidentiality include encryption, access controls, and authentication mechanisms.

Integrity

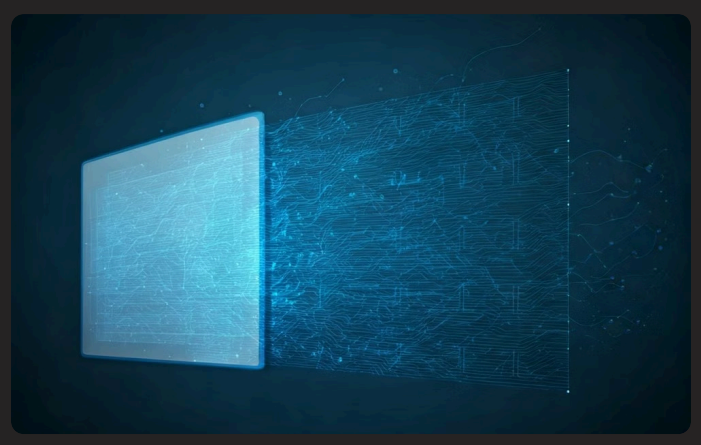
Ensuring the accuracy and completeness of information and processing methods. Measures to maintain integrity include checksums, hashing, and digital signatures, which help in detecting unauthorized alterations to data.



Availability

Ensuring that authorized users have access to information and associated assets when required. Strategies to ensure availability include implementing redundant systems, regular maintenance, and protection against denial-of-service (DoS) attacks.

Types of Information Security



Network Security

Protects the usability and integrity of network and data. This includes protecting the network from attacks such as distributed denial-of-service (DDoS) attacks and unauthorized access.

Application Security

Focuses on keeping software and devices free of threats. Security measures include code reviews, secure coding practices, and application firewalls.

Endpoint Security

Involves securing end-user devices such as computers, mobile devices, and tablets. This can include antivirus software, intrusion detection systems, and endpoint detection and response.

Data Security

Protects data in storage and in transit. Methods include encryption, masking, and tokenization to ensure data confidentiality and integrity.

Identity and Access Management (IAM)

Ensures that only authorized users have access to resources. This includes policies, processes, and technologies used to manage digital identities and control access to resources.

Cloud Security

Involves securing data, applications, and services hosted in the cloud. This includes ensuring compliance with regulatory requirements and protecting against data breaches and loss.

Information Security Governance

Encompasses the policies, procedures, and practices that ensure the effective and efficient use of information security within an organization. This includes risk management, compliance, and incident response planning.

Cryptography

The practice of securing information by transforming it into an unreadable format, only accessible by those possessing the decryption key. This ensures confidentiality and integrity of data.

Physical Security

Protects physical hardware and infrastructure from physical threats such as theft, vandalism, natural disasters, and unauthorized access.

Cybercriminals

Cybercriminals are individuals or groups who use computers and the internet to commit crimes. They use digital tools and systems to exploit weaknesses in the system to steal personal information, money, or sensitive data, or to disrupt services. Cybercriminals often aim to make a profit, but some may also be motivated by personal grudges, political reasons, or the challenge of breaking into secure systems. They can operate alone or as part of organized groups, and their actions can impact individuals, businesses, and governments. Examples of their activities include hacking into systems, spreading viruses, committing online fraud, and launching cyberattacks.

Types of Cybercriminals

Cybercriminals need recognition

Hobby Hackers: These hackers engage in hacking for fun and intellectual challenge. They enjoy exploring systems and learning about cybersecurity, often without malicious intent.

IT Professionals: Skilled individuals who might hack to demonstrate their abilities, gain recognition in the tech community, or improve their job prospects.

Politically Motivated Hackers: Also known as hacktivists, these hackers conduct attacks to promote political or social causes. They seek to draw attention to their message through their actions.

Terrorist Organizations: Groups that use hacking to further their extremist agendas. They seek recognition to spread fear, disrupt systems, and promote their ideologies.

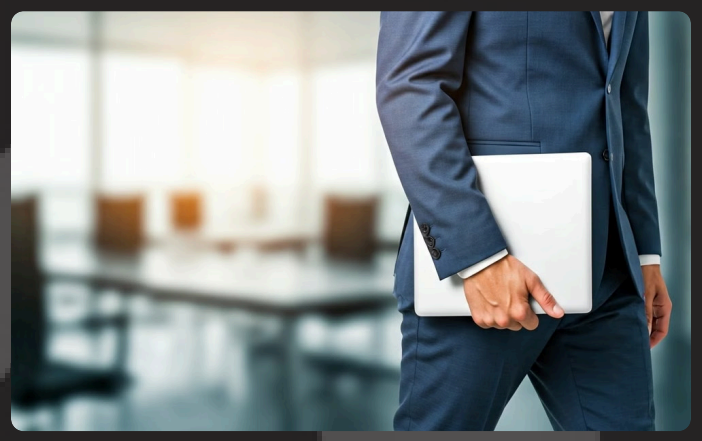
Cybercriminals driven by profit

Psychological Perverts: Cybercriminals who engage in deviant activities for personal gratification. This can include cyberstalking, online harassment, and other forms of digital abuse.

Motivated Hackers: These hackers are primarily driven by financial gain. They aim to steal money or valuable data while avoiding detection. Examples include identity thieves and financial loss.

State-Sponsored Hackers: Hackers working for government entities to conduct cyber warfare. Their actions are secretive and aim to serve national interests.

Organized Criminals: Groups that engage in hacking as part of broader criminal operations. They may run large-scale scams, ransomware attacks, or other illegal activities for profit.



Cybercriminals with insider access

Disgruntled/Dissatisfied Employees: Current or former employees who feel wronged by their employer and seek revenge. They may steal data or leak sensitive information.

Competitor Spies: Competitor Spies refers to individuals or groups who secretly gather information from within a company to help a competitor or to further their own criminal activities. They might be hired by rival businesses.

A Global Perspective on Cybercrime

Growing Threat

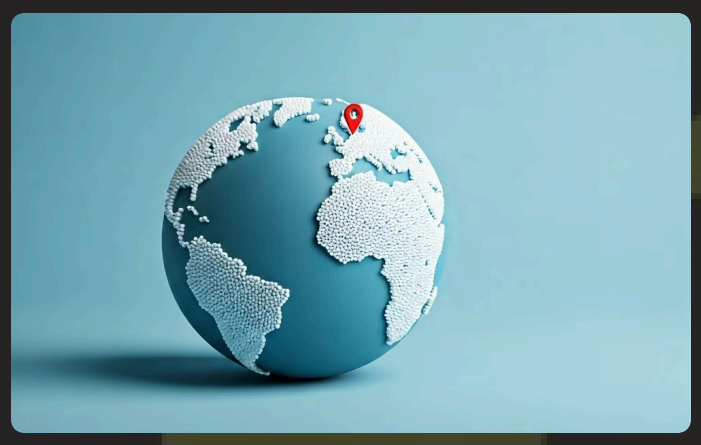
Cybercrime is increasing worldwide as more people and devices connect to the internet.

Economic Impact

It costs the global economy billions of dollars annually, including direct theft, recovery costs, and lost trust.

Privacy Concerns

Data breaches expose personal information, leading to identity theft and privacy violations.



Global Reach

Cybercriminals can target anyone, anywhere, making it a worldwide issue.

Regulation and Cooperation

Countries are creating laws to fight cybercrime, but effectiveness varies. International cooperation is crucial.

Challenges

Identifying attackers is difficult due to internet anonymity, and threats evolve quickly, making defense challenging.

Future Trends

Technologies like AI and the Internet of Things (IoT) present new security challenges, and cyber warfare is becoming more common.

Preventative Measures

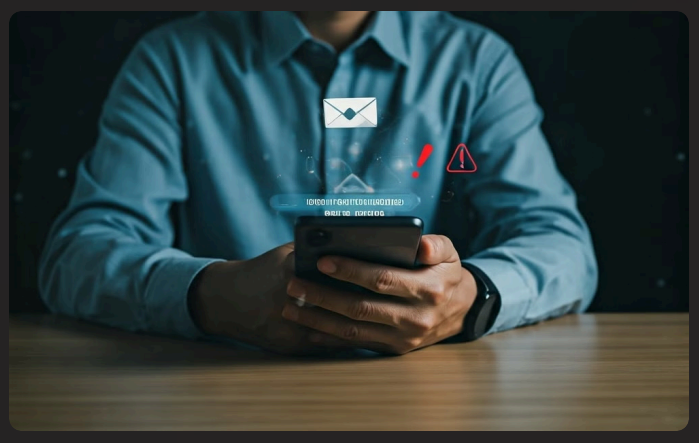
Educating users, using advanced security technologies, and having clear incident response plans are essential for combating cybercrime.

Conclusion

Cybercrime is a complex, evolving threat that requires coordinated global efforts and continuous improvement in cybersecurity measures. As technology continues to advance, staying ahead of cybercriminals will remain a significant challenge for the global community.

Cybercrime Era: Survival Mantra for the Netizens

Netizens = Net + Citizen. It refers to a citizen of internet. Netizen is someone who actively involved in online communities or the internet in general. The 5P Netizen Mantra for online security encompasses five key principles to help users stay safe and secure in the digital world: Precaution, Prevention, Protection, Preservation, and Perseverance.



Precaution

B**e cautious**: Always be mindful and alert when navigating the internet. Avoid clicking on unknown links or downloading files from untrusted sources.

Verify Sources: Ensure that websites and emails are legitimate before providing any personal or financial information.

Stay Informed: Keep yourself updated about common cyber threats and scams to recognize and avoid them.

Prevention

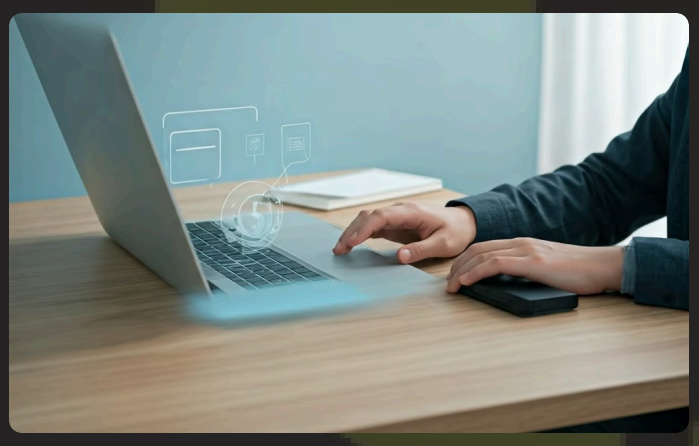
Use strong passwords: Use complex and unique passwords for different accounts to reduce the risk of unauthorized access.

Regular updates: Keep your operating system, software, and applications updated to patch vulnerabilities.

Avoid public Wi-Fi: Be cautious when using public Wi-Fi networks, as they are often insecure and can be exploited by cybercriminals.

Protection

Antivirus Software: Install and regularly update antivirus software to detect and remove malware. Firewalls: Use firewalls to block unauthorized access to your computer or network.



Preservation

Data Backup: Regularly back up your important data to an external drive or cloud storage to prevent loss in case of a cyber attack.

Secure Storage : Ensure that backups are stored securely and can be accessed only by authorized persons.

Perseverance

Continuous learning: Stay educated about the latest cybersecurity practices and threats.

Vigilance: Maintain a proactive approach to security by regularly reviewing and updating your security measures.

Adaptability: Be prepared to adapt and improve your security practices as new threats emerge.

Thank You For Visiting!

We're grateful for your interest in our services. Please connect with us on social media or check out our website for more information.



t.me/newbert7 Insta@newbert.in Website newbert.in