




Introduction to Cyber Security





Introduction and Definition

- **Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- It's also known as information technology security or electronic information security.
- The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- 
- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
 - **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
 - **Information security** protects the integrity and privacy of data, both in storage and in transit.
 - **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
 - **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
 - **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.




Types of cyber threats

- Cybercrime
- Cyber-attack
- Cyberterrorism



Types of cybercrime

- Hacking
- Unwarranted mass-surveillance
- Child pornography
- Child grooming
- Copyright infringement
- Money laundering
- Cyber-extortion
- Cyber-terrorism

- 
- **Hacking:** It is an illegal practice by which a hacker breaches the computer's security system of someone for personal interest.
 - **Unwarranted mass-surveillance:** Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.
 - **Child pornography:** It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.
 - **Child grooming:** It is the practice of establishing an emotional connection with a child especially for the purpose of child-trafficking and child prostitution.
 - **Copyright infringement:** If someone infringes someone's protected copyright without permission and publishes that with his own name, is known as copyright infringement.
 - **Money laundering:** Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.
 - **Cyber-extortion:** When a hacker hacks someone's email server, or computer system and demands money to reinstate the system, it is known as cyber-extortion.
 - **Cyber-terrorism:** Normally, when someone hacks government's security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.



Cybercrime and Information Security

- Security Architecture
- Network Diagram
- Security Assessment Procedure
- Security Policies
- Risk Management Policy
- Backup and Restore Procedures
- Disaster Recovery Plan
- Risk Assessment Procedures



Classification of Cybercrimes

- cyber crimes against individuals
- cyber crimes against organizations
- cyber crimes against society at large



Cyber crimes against individuals

- Cyberbullying
- Cyberstalking
- Cyber defamation
- Phishing
- Cyber fraud
- Cyber theft
- Spyware



Cyber crimes against organizations


- Attacks by virus
- Salami attack
 - Salami slicing
 - Penny shaving
- Web Jacking
- Denial of Service Attack
- Data diddling

Note: Any person convicted of a Salami attack shall be punished under **Section 66 IT Act** with imprisonment up to three years or a fine up to 5 lakhs or maybe both



Cyber crimes against society at large

- Cyber pornography
- Cyber terrorism
- Cyber Espionage



The legal perspectives - Indian perspective, Global perspective

- Information Technology Act, 2000 (IT Act)
- Indian Penal Code, 1860 (IPC)
- Information Technology Rules (IT Rules)
- Companies Act, 2013
- Cybersecurity Framework (NCFS)



Information Technology Act, 2000 (IT Act)

- Overview of the Act:
 - It is the first cyberlaw to be approved by the Indian Parliament. The Act defines the following as its object: The Act states that an acceptance of a contract may be expressed electronically unless otherwise agreed and that the same shall have legal validity and be enforceable. In addition, the Act is intended to achieve its objectives of promoting and developing an environment conducive to the implementation of electronic commerce.
- The important provisions of the Act: The IT Act is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cyber crimes. Following are the appropriate sections:
 - Section 43
 - Section 66
 - Section 66B
 - Section 66C
 - Section 66D
 - Section 66E
 - Section 66F
 - Section 67
- Reference: <https://blog.ipleaders.in/cyber-crime-laws-in-india/>



Importance of cyber crime laws

- An important goal of any cyber law is to prosecute those who undertake illegal activities using the internet. To effectively prosecute these types of crimes, such as cyber abuse, assaults on other websites or individuals, theft of records, disrupting every company's online workflow, and other criminal activities, significant efforts should be undertaken, and hence, which is where cyber laws come into the picture.
- In the cases involving a violation of cyber law, the action is taken against the individual on the basis of his location and how was he involved in that violation.
- Prosecuting or retracting hackers is the most important thing since most cyber crimes are beyond the reach of a felony, which is not a crime.
- The use of the internet is also associated with security concerns and there are even some malicious individuals who want to gain unauthorised access to the computer device and commit fraud using it in the future. Hence, all rules and cyber laws are designed to protect internet businesses and internet users from unwanted unauthorized access and malicious cyber-attacks. There are a variety of ways in which individuals or associations can take action against others who commit criminal acts or break cyber laws.



References for cyber crime laws:

- <https://probono-india.in/blog-detail.php?id=218>
- <https://www.appknox.com/blog/cybersecurity-laws-in-india>
- <https://www.meity.gov.in/content/cyber-laws>
- <https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/>
- <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- <https://www.clearias.com/cybercrime/>
- https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/#Relation_between_Cyber_Crime_and_Cyber_Security
- <https://digitalguardian.com/blog/what-cyber-security>
- <http://www.proind.in/blog/cyber-laws-in-india-and-information-technology-act-all-you-need-to-know/>
- <http://www.bhagininiveditacollege.in/pdf/2020/march/27/Dr%20Rachna%20Mahalwala%20-B.Com%201st%20year%20of%20Business%20Law%20Case%20Studies%20as%20Oper%20selected%20IT%20Act%20Sections%20Related%20to%20Offences.pdf>



Categories of Cybercrime

1. Crimes Against People
2. Crimes Against Property
3. Crimes Against Government



Types of Attack:

1. DoS and DDoS Attacks	11. Session Hijacking
2. MITM Attacks	12. Brute force attack
3. Phishing Attacks	13. Web Attacks
4. Whale-phishing Attacks	14. Insider Threats
5. Spear-phishing Attacks	15. Trojan Horses
6. Ransomware	16. Drive-by Attacks
7. Password Attack	17. XSS Attacks
8. SQL Injection Attack	18. Eavesdropping Attacks
9. URL Interpretation	19. Birthday Attack
10. DNS Spoofing	20. Malware Attack



Social Engineering

Examples:

1. Russian hacking group targets Ukraine with spear phishing
2. Deepfake Attack on UK Energy Company
3. Microsoft 365 phishing scam steals user credentials
4. Ransomware gang hijacks victim's email account



Cyber Stalking

- **Cyberstalking** is a type of cybercrime that uses the internet and technology to harass or stalk a person. It can be considered an extension of cyberbullying and in-person stalking. However, it takes the form of text messages, e-mails, social media posts, and other mediums and is often persistent, deliberate, and methodical.
- Cyberstalking is a type of cybercrime that uses the internet and technology to harass or stalk a person. It can be considered an extension of cyberbullying and in-person stalking. However, it takes the form of text messages, e-mails, social media posts, and other mediums and is often persistent, deliberate, and methodical.



Examples of cyber stalking

- Posting offensive, suggestive, or rude comments online
- Sending threatening, lewd, or offensive emails or messages to the victim
- Joining the same groups and forums as the victim
- Releasing the victim's confidential information online
- Tracking all online movements of the victim through tracking devices
- Using technology for blackmailing or threatening the victim
- Excessively tagging the victim in irrelevant posts
- Engaging with all online posts made by the victim
- Creating fake profiles on social media to follow the victim
- Posting or distributing real or fake photos of the victim
- Excessively sending explicit photos of themselves to the victim
- Making fake posts intended to shame the victim
- Repeatedly messaging the victim
- Hacking into the victim's online accounts
- Attempting to extort explicit photos of the victim
- Sending unwanted gifts or items to the victim



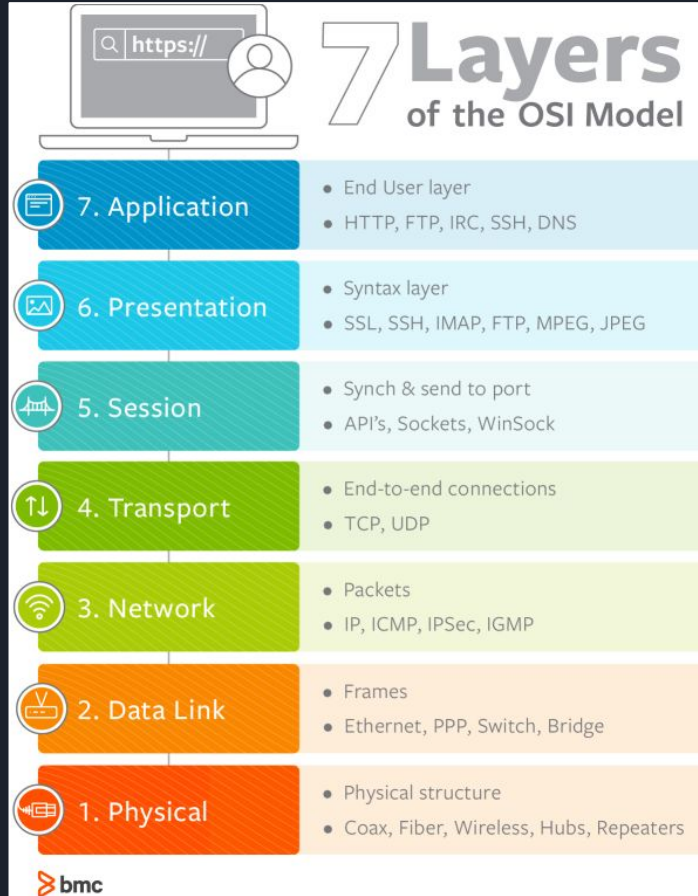
Consequences of Cyberstalking

- Cyberstalking is no different than stalking and leads to consequences that can be detrimental to the victims both physically and mentally.
- Victims who are harassed online experience fear, anger, confusion, and insomnia along with other health issues.
- Cyberstalking affects the overall well-being of victims.
- They often suffer from anxiety, distress, depression, PTSD, and suicidal ideation.

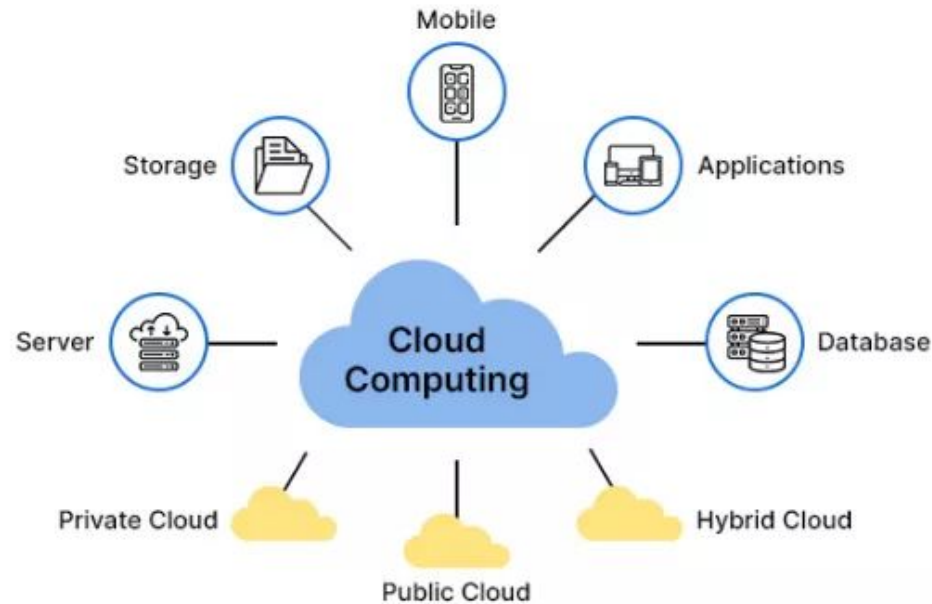


Types of Cyberstalking

- **Catfishing:** The creation of fake profiles or copying of existing ones on social media to approach victims.
- **Monitoring check-ins on social media:** Keeping an eye on the activities of a victim on social media to accurately gauge their behavior pattern.
- **Spying via Google Maps and Google Street View:** Using Street View to spy on a victim and find their location from posts or photos on social media.
- **Hijacking webcam:** Webcams can be hijacked by introducing malware-infected files into the victim's computer.
- **Installing stalkerware:** Stalkerware tracks the location, enables access to texts and browsing history, makes audio recordings, etc., without the victim's knowledge.
- **Tracking location with geotags:** Digital pictures mostly have geotagged with the time and location of the picture if it is in the metadata format, which makes it easier for stalkers to access that information by using special apps.



Cloud Computing and cybercrime





On-Premises



IaaS

Infrastructure as a Service



PaaS

Platform as a Service



SaaS

Software as a Service

Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking




What Does Anonymizer Mean?

An anonymizer is a proxy server that makes Internet activity untraceable. An anonymizer protects personally identifying information by hiding private information on the user's behalf.



What is a cloud attack?

- Any cyber attack that targets off-site service platforms that offer storage, computing, or hosting services via their cloud infrastructure can be classified as a cloud cyber attack. This can include attacks on service platforms that utilise service delivery models like **SaaS**, **IaaS**, and **PaaS**.



What are the largest cloud attacks in recent years?

- CAM4—2020
- Advanced Info Service (AIS)—2020
- Keepnet Labs—2020
- Microsoft—2019



CAM4—2020

- CAM4 is an adult live streaming website that fell victim to a cloud cyber attack in March 2020 that exposed 10.8 billion sensitive entries amounting to 7 TB of data.
- The leaked database included location details, email addresses, IP addresses, payment logs, usernames and more.



Advanced Info Service (AIS)—2020

- The AIS data breach was discovered by cybersecurity researcher Justin Paine when browsing BinaryEdge and Shodan.
- According to Paine, the leaked database included 8.3 billion network flow logs and DNS query logs of AUN customers of the Thailand-based telecommunications company.



Keepnet Labs—2020

- One of the more ironic cloud data breaches of 2020, the Keepnet Labs data breach involved a leaky Elasticsearch database that contained entries that were previously exposed by various data breaches across the globe.
- The database included two data collections containing 5 billion and 15 million entries respectively.



Microsoft—2019

- On January 22, 2020, Microsoft announced that one of their cloud databases was breached back in December 2019, resulting in the exposure of 250 million entries, including email addresses, IP addresses, and support case details.
- According to the computing giant, the cause of this data breach was a misconfigured network server that was hosting the critical information.
- While this is not the biggest, it was one of the most shocking cyber attacks due to the high-profile nature of the target.



The causes of cloud computing cyber attacks

- Misconfiguration
- Compromised user accounts
- API vulnerability
- Malicious insider activity



10 Most Common Types of Attacks on Cloud Computing

- Cloud malware injection attacks
- Abuse of cloud services
- Denial of service attacks
- Side channel attacks
- Wrapping attacks
- Man-in-the-cloud attacks
- Insider attacks
- Account or service hijacking
- Advanced persistent threats (APTs)
- New attacks: Spectre and Meltdown



References:

<https://www.ibm.com/topics/cloud-computing>

<https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-computing>

<https://www.investopedia.com/terms/c/cloud-computing.asp>

<https://cloud.google.com/learn/what-is-cloud-computing>