

# Cyber security and types of cyber attacks

[Law](#), [Security](#)



## **Abstract**

Cyber security includes innovations, procedures and practices intended to ensure PCs, programs, systems and information from hacking, harm or unauthorized Access. Out in the open talk with different ideas, for example, privacy, data sharing, information Gathering, and surveillance. Cyber security comes into picture and additionally we experience cyber violations. To abstain from giving cybercriminals the activity, it is vital for those involved with the fight against cybercrime to attempt to envision qualitative and quantitative changes in its basic components with the goal that they can detail their strategies suitably. The significance of being familiar with the impacts of cyber crime keeping in mind the recent activities that have taken place and offering solutions to protect an individual and/or an organization from them is laid down in this paper. Types of cyber security and cyber attacks are listed in this paper. It explains the condition of cyber crimes and cyber security in India . A significance of Indian cyber laws is displayed in this paper too.

## **Introduction**

In today's world internet is most powerful thing. Without Internet our life will be nothing . Our Generation is growing very rapidly in terms of technology. These technologies are used in every sector of work such as business, education, shopping or banking transactions, almost everything is on the cyber space today. Since there is growth in IT sectors so cyber criminals are also there who are ready to steal your data through online database, hacking accounts, phishing etc. There are many Hackers who hack very big companies

such as LinkedIn, snapchat, myspace etc. And steal the data of many million users and sell it on darkweb. Business and government sectors have begun to focus effort on comprehensive cyber security solutions. With this effort has emerged a need for greater collaboration between research and industry fields. Cyber security plays an important role in the development of information technology as well as Internet services. Cybercrime is evolving at an astounding pace.

In information technology data protection or information security is one of the great challenges for the world. It is one of the serious issues in information industry. Internet is one of the important and very fast growing commodities for development of business as well as in different private and government organizations. It is being used as the largest communication and information exchange medium now. At the same time Internet is becoming an instrument of numerous types of cyber crimes.

It is being used to steal and manipulate the information of users. Important data is being stolen and personal as well as organizational threats are being imposed upon the users which are using Internet. Sensitive information, secret credentials and even the bank account details are being stolen these days with the use of Internet. Cyber security is becoming a serious issue for the complete world with intruders attacking people or organizations with the motive of getting access to their restricted content.[1-2]In today's time hackers hack the pc of the user and lock it and demands for the ransom if the user doesn't give the ransom the hacker will wipe the full data and many important folders. Also hacker can leak the data.

## **Types Of Cyber Security**

There are several types of computer securities that are completely based on protecting from different types of viruses, worms and Trojans[3]. The common types of computer security are as follows:

### **Network Security**

This is a common type of computer security which deals with securing the networks, that is from privately owned computer networks to the internet itself against different types of viruses and also many other forms of threats to keep the working of computer networking smooth. As the data is available to the admin person only but the hackers can hack the database using SQLi and get your user credentials and get your data and they have the full access of your network.

### **Data Security**

Another important form of the computer security is the data security. It is defined as the act of protecting the important data present on the computers from different types of threats through various software such as antivirus and firewalls. But sometimes the hacker encrypts the virus and the antivirus doesn't catch it. So this way hacker can get all your data and can control your whole pc.

### **System Security**

It mainly concerns about malicious programs that can disrupt and sometimes destroy the computer systems. These malicious programs can be viruses such as Love Bug, rabbits, Logic Bomb, Trojan horse and worms such as Morris Worm and, bugs. If the attacker succeeds in preventing computer

systems from operating smoothly, this can result in great financial losses for victims. Ransomware is a virus or malware which a hacker creates and bind into another application and send it to the user when the user opens the file. The virus executes and lock the computer with all data encrypted then the hacker demands the ransom from the victim. Until the victim gives the ransom the file is encrypted.

## **Types Of Cyber Attacks**

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. Researchers have studied and reported[4-6] various types and classes of cyber attacks.

### **Major types are as follows:**

#### 1. Ransomware

Ransomware is a type of malware that involves an attacker locking the victim's computer system files — typically through encryption — and demanding a payment to decrypt and unlock them.

#### 2. Malware

Malware refers to various forms of harmful software, such as viruses and ransomware. Once your computer is infected by the malware . it will have entire access of the pc. Since the hacker has the access he can get the whole data and can have your personal information such as credit card details

#### 3. Social Engineering

Social engineering is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

#### 4. Phishing

IN phishing attack an a hacker make a clone webpage og the any website and sends to the victim. By carelessness of the victim the victim puts the id and password in the webpage made by the hacker. Which is lookalike of the original webpage. So when the victim puts the id and password(credentials) the data directly goes to the hacker. In order to combat phishing attempts, understanding the importance of verifying email senders and links is essential.

#### 5. Denial of Service

In this, Hacker uses a system to overload a website or server to shut it down for as long as the hacker wants to. Through this the people will not get the content they want to from the website or server. If hacker is more careful and précised then they use DDOS attack to shut down a server or website . DDOS is known as Distributed Denial-of-Service Attack. In this the hacker uses more IP addresses and more computers to overload the website or server and shut it down.

#### 6. SQL Injection Attack

In hacking world its mainly known as SQLi attack which stands for structured programing language injection. Many servers and websites uses SQL to manage the data in their database. A SQL injection attack specifically targets this kind of server, using malicious code to get the

server. If the server stores username and password(credentials) and credit card details etc can be wasily accesible by the hacker. An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

## 7. Credential Reuse

Many users have same password for every website. Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matterhow tempting it may be to reuse credentials for your email, bank

## Conclusion

It can be concluded from this present study that with increasing rate of cyber crimes more detection techniques alongwith educating the users on being safe online needs to be established with complete guidance to know about the pros and cons of the web before entering it. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in enforcing " acceptable use" policy. Concrete measures must be found in order to track electronics evidence and preserve them so

that systems are better protected from cyber intrusions. To defend against cyber crimes, intrusion detection techniques should be designed, implemented, and administrated. The way to protect it for now is for everyone to be smart and to follow preventive measures. Individuals, institutions, and governments should all follow these measures.

## References:

1. Tonge A. M., Kasture S. S., Chaudhari S. R., Cyber security: challenges for society-literature review, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, 12(2), 67-75 (2013).
2. Stoll C., The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, New York: Pocket Books (1990).
3. <http://computernetworkingnotes.com/networksecurity-access-lists-standards-and-extended/typesof-attack.html>.
4. Homer J., Zhang S., Ou X., Schmidt D., Du Y., Rajagopalan S. R., and Singhal A.. Aggregating vulnerability metrics in enterprise networks using attack graphs, Journal of Computer Security, 21(4), 561-597 (2013)
5. Cerrudo C., An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks; retrieved from [https://ioactive.com/pdfs/IOActive\\_HackingCitiesPaper\\_CesarCerrudo.pdf](https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf), accessed on 30. 09. 2017
6. <https://searchsecurity.techtarget.com/definition/cybersecurity>
7. <https://www.rapid7.com/fundamentals/types-of-attacks/>