What is Cyber Law?

Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system thet is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware. It covers many areas, such as access to and usage of the Internet, encompassing various subtopics as well as freedom of expression, and online privacy.

Cyber laws help to reduce or prevent people from cybercriminal activities on a large scale with the help of protecting information access from unauthorized people,

freedom of speech related to the use of the Internet, privacy, communications, email, websites, intellectual property, hardware and software, such as data storage devices. As Internet traffic is increasing rapidly day by day, that has led to a higher percentage of legal issues worldwide. Because cyber laws are different according to the country and jurisdiction, restitution ranges from fines to imprisonment, and enforcement is challenging.

Cyberlaw offers legal protections for people who are using the Internet as well as running an online business. It is most important for Internet users to know about the local area and cyber law of their country by which they could know what activities are legal or not on the network. Also, they can prevent ourselves from unauthorized activities.

The Computer Fraud and Abuse Act was the first cyber law, called CFFA, that was enacted in 1986. This law was helpful in preventing unauthorized access to computers. And it also provided a description of the stages of punishment for breaking that law or performing any illegal activity.

Why are cyber laws needed?

There are many security issues with using the Internet and also available different malicious people who try to unauthorized access your computer system to perform potential fraud. Therefore, similarly, any law, cyber law is created to protect online organizations and people on the

network from unauthorized access and malicious people. If someone does any illegal activity or breaks the cyber rule, it offers people or organizations to have that persons sentenced to punishment or take action against them.

What happens if anyone breaks a cyber law?

If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw he broke, where he lives, and where he broke the law. There are many situations like if you break the law on a website, your account will be banned or suspended and blocked your IP (Internet Protocol) address. Furthermore, if any person performs a very serious illegal activity, such as causing another person or company distress, hacking, attacking another person or website, advance action can be taken against that person.

Importance of Cyber Law

Cyber laws are formed to punish people who perform any illegal activities online. They are important to punish related to these types of issues such as online harassment, attacking another website or individual, data theft, disrupting the online workflow of any enterprise and other illegal activities.

If anyone breaks a cyber law, the action would be taken against that person on the basis of the type of cyberlaw

he broke, where he lives, and where he broke the law. It is most important to punish the criminals or to bring them to behind bars, as most of the cybercrimes cross the limit of crime that cannot be considered as a common crime.

These crimes may be very harmful for losing the reliability and confidentiality of personal information or a nation. Therefore, these issues must be handled according to the laws.

- When users apply transactions on the Internet, cyber law covers every transaction and protect them.
- It touches every reaction and action in cyberspace.
- It captures all activities on the Internet.

Areas involving in Cyber Laws

These laws deal with multiple activities and areas that occur online and serve several purposes. Some laws are formed to describe the policies for using the Internet and the computer in an organization, and some are formed to offer people security from unauthorized users and malicious activities. There are various broad categories that come under cyber laws; some are as follows:

Fraud

Cyber laws are formed to prevent financial crimes such as identity theft, credit card theft and other that occurring online. A person may face confederate or state criminal charges if he commits any type of identity theft. These

laws have explained strict policies to prosecute and defend against allegations of using the internet.

Copyrighting Issues

The Internet is the source that contains different types of data, which can be accessed anytime, anywhere. But it is the authority of anyone to copy the content of any other person. The strict rules are defined in the cyber laws if anyone goes against copyright that protects the creative work of individuals and companies.

Scam/ Treachery

There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual. Cyber laws offer many ways to protect people and prevent any identity theft and financial crimes that happen online.

Online Insults and Character Degradation

There are multiple online social media platforms that are the best resources to share your mind with anyone freely. But there are some rules in cyber laws if you speak and defaming someone online. Cyber laws address and deal with many issues, such as racism, online insults, gender targets to protect a person's reputation.

Online Harassment and Stalking

Harassment is a big issue in cyberspace, which is a violation of both criminal laws and civil. In cyber laws, there are some hard laws defined to prohibit these kinds of despicable crimes.

Data Protection

People using the internet depends on cyber laws and policies to protect their personal information. Companies or organizations are also relying on cyber laws to protect the data of their users as well as maintain the confidentiality of their data.

Contracts and Employment Law

When you are visiting a website, you click a button that gives a message to ask you to agree for terms and conditions; if you agree with it, that ensures you have used cyber law. For every website, there are terms and conditions available that are associated with privacy concerns.

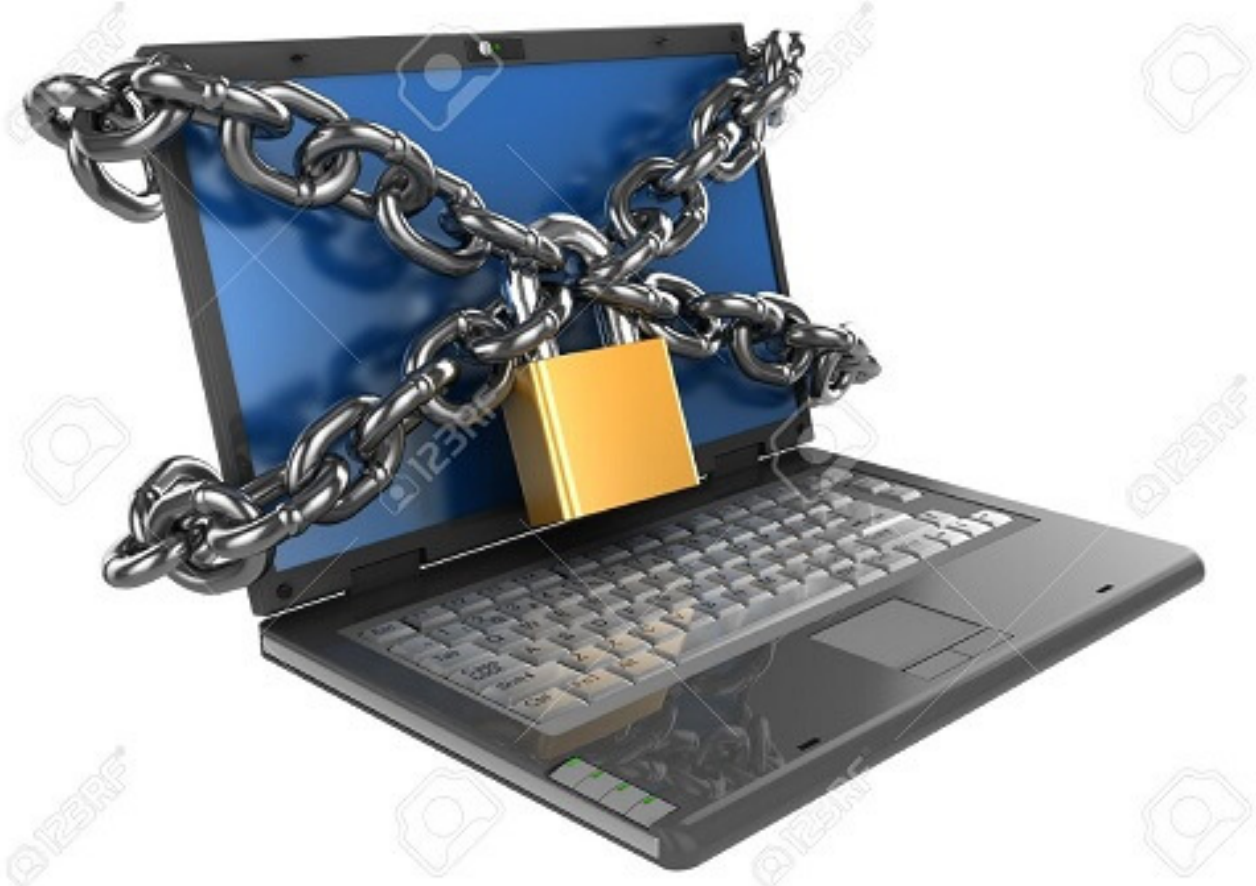
Trade Secrets

There are many organizations that are doing online businesses, which are often relying on cyber laws to protect their trade secrets. For example, online search engines like Google spend much time to develop the algorithms that generate a search result. They also spend lots of time developing other features such as intelligent assistance, flight search services, to name a few and

maps. Cyber laws help these organizations to perform legal action by describing necessary legal laws for protecting their trade secrets.

How to protect yourself on the Internet

Although the Internet is a resource that contains multiple different types of content, there are many hackers or unauthorized users that may be harmful to you in order to thief your personal information. Below are given all of the steps that may help you to keep your personal information and computers safe while using the Internet. All of the given steps or suggestions can be beneficial for all computer users, even if what type of computer, device, or operating system they are using.



Verify data is encrypted

When you are sending any confidential information, such as debit card numbers, credit card numbers, usernames, or passwords, send these types of information securely. In Internet browsers, look for a small lock (Internet browser security lock) to verify this; an icon will be shown in the right corner of the bottom of the browser address bar or browser Window. If you see the icon, it should be in a locked condition and not in an unlocked position. Also, make sure the URL starts with https (Hypertext Transfer Protocol Secure), as displaying in the below screenshot:

Internet Explorer secure address bar.

If the lock icon is in the locked position and data is intercepted, the data is encrypted that helps to keep secure your data and prevent others to understand it. The data can be read by anyone if the lock is in the unlocked position or no lock is visible because all information will be in the form of plain text. For example, an online forum is not secure, use a password, but you will not use the password with protected sites like an online banking website.

Use a safe password

Like online bank site or other websites that contain

confidential information, need to use very strong passwords, it is also recommended; you must use the different and strong password for all websites that require login id and password. You could use a password manager if you required help to remember your password.

Keep your software and operating system up-to-date

To protect yourself on the Internet, it is better to update your software installed on your computer and operating system regularly. It is necessary because many updates are released by the developers of the operating system that are related to computer security-related issues. Therefore, you should update your system when the latest updates are released.

When available always enable two-factor authentication

You can use the two-factor authentication feature to make more secure your accounts, like Gmail or others that require a login and contain your private data. It offers advanced protection by adding an additional step in verifying you at the time of login. If you enable two-factor authentication and the service does not verify your computer or other devices after authenticating your password, it sends a text message with a verification code on your cell phone. It includes more powerful security; for example, if someone knows your password of any account

and tries to access your account, but he does not have your phone, he cannot access your account even with a valid password.

Always be cautious of e-mail links and attachments

The email attachments and hyperlinks sent through email are the most common resources to spread viruses and malware. It is recommended to always be extremely cautious to open any attachments and hyperlinks, which you have received through email from others, even if they have sent by friend or family.

Be aware of phishing scams

There are many phishing scams and techniques that can be more harmful in respect to losing your secret information. Therefore, it is necessary to familiarize yourself with these types of techniques. Hackers mainly target websites that need a login, such as PayPal, eBay, Amazon, online banking sites, and other popular sites.

E-mail is not encrypted

If you send any confidential information through email, it can be read or understood by unauthorized users as email is not encrypted. Therefore, confidential data like debit card information, credit card information, password and more should not be transmitted over e-mail.

Use an alternative browser

For protecting your systems, Internet browsers also play an important role. For example, earlier versions of Internet Explorer are not more secure. If you are using a lass secure browser in terms of your browser like Internet Explorer, you should switch to another browser like *Mozilla Firefox* or *Google Chrome*. Also, if you are using Microsoft Windows 10 operating system on your computer and want to stay to use a Microsoft Internet browser, you can switch to the Microsoft Edge rather than Internet Explorer that is more secure in terms of protecting your systems.

Use caution when accepting or agreeing to prompts

When you are indicated to install an add-on or any program, before clicking on the Ok button, you need to read and understand the agreement carefully. If you do not understand the agreement or feel it is not necessary to install, you should not install this kind of program, cancel or close the window, which may be harmful for you.

Also, when you are installing an add-on or any program, you need to care about any check box that asks if this third-party program will be ok to install. These often cause more issues and leave these boxes unchecked because these are never required.

Be cautious where you are logging in from

Business

If you are working in any organization, your place of work can monitor your computer by installing key loggers or use other methods. In this case, someone can collect usernames and passwords and read these logs if he has access to this information. It can be more harmful to lose your personal information. Additionally, if your computer is shared with other co-workers, do not store any passwords in your browser.

Wireless network

When you are using a wireless network, you must be careful that all the information sent from your computer and to your computer can be read and intercepted by any unauthorized person. You can log in to the network securely with the help of using WPA or WEP and prevent losing your secret information. Furthermore, make sure the network is secure if it is a home wireless network.

Friend's house

Sometimes, you may use your friend's computer and log in to your account on that computer, which may not be fully secure. Intentionally or unintentionally, you can enter your username and password on your friend's computer or the computer with whom you are not familiar. Finally, never save the password information on your friend's

computer browser when you are logging into any site on a friend's computer.

Always think before you share something

There are many social media sites, such as Instagram, Facebook, that enable you to make online friends and connect with them. The networking sites are also the best place to share your personal information with your friends, family or others. When you share something on social networking sites or the Internet, make sure you are not sending any information that can be harmful to you if everyone sees it. The sent information on the social network or the Internet should be public. Also, make sure you are sharing such something that will not offend anyone or embarrass you, and you must not be uploaded on the Internet.

Update Internet browser plugins

You should update Internet browser plugins or install the latest plugins to protect yourself while online on the computer. Due to browser plugins like Adobe Flash, attackers may find some easiness or security vulnerabilities to hack any system. Therefore, you need to check out regularly that all your installed Internet plug-ins are up-to-date.

Be aware of those around you

If you are working on the computer at any public area, school, library and more, make sure anyone is not looking at your screen, as there will be many people around you. On the other hand, it can be cautious if anyone is looking at your system screen that is called shoulder surfing. If you are required to system screen private, you can use a privacy filter for the display.

Secure saved passwords

There are many users that are habitual to save login information and password on the system, but it can be insecure. Therefore, make sure you are storing your personal details, such as credit card detail and account passwords, in a secure area. It is recommended for everyone to use a password manager to save your passwords.

A password manager is a software that holds all securely encrypts and login information, and password protects that information. If you save a password in a browser and anyone has access to your Internet browser, the password information may be seen by that person. For instance, in the Firefox Internet browser, anyone can see all stored passwords if you do not set up a master password.

Do not always trust what you read online

You should be aware about that it is possible for anyone to publish a website on the Internet. There are various

creators who may have intention for creating a site only for malicious purposes. For instance, a website can be created to gain unauthorized access and spread fear, lies, or malware.