The crime that involves and uses computer devices and Internet, is known as cybercrime.

Cybercrime can be committed against an individual or a group; it can also be committed against government and private organizations. It may be intended to harm someone’s reputation, physical harm, or even mental harm.

Cybercrime can cause direct harm or indirect harm to whoever the victim is.

However, the largest threat of cybercrime is on the financial security of an individual as well as the government. Cybercrime causes loss of billions of USD every year let . us now discuss the major types of cybercrime −

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.

Cyber Security

Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.

Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access.

All sorts of data whether it is government, corporate, or personal need high security; however, some of the data, which belongs to the government defense system, banks, defense research and development organization, etc. are highly confidential and even small amount of negligence to these data may cause great damage to the whole nation. Therefore, such data need security at a very high level.

How to Secure Data?

Let us now discuss how to secure data. In order to make your security system strong, you need to pay attention to the following −

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

Once you have a complete blueprint of the points mentioned above, you can put better security system to your data and can also retrieve your data if something goes wrong.

