Cybercrime in India

Jyoti Sharma*

Abstract

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Cybercriminals that target computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called a Denial-of-Service (DoS) attack.

Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.

Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

What is cybercrime?

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. Others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both -- i.e., target computers to infect them with a computer virus, which is then spread to other machines

**Legal Consultant, Haryana*