CYBER CRIMES FAQS

1. What is Cybercrime?

A. Cybercrime refers to all the activities done with criminal intent in cyberspace. Because of the anonymous nature of the internet, miscreants engage in a variety of criminal activities. The field of cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with each passing day.

2. Do we have an exhaustive definition of Cybercrime?

A. No, unfortunately we don't have an exhaustive definition of cybercrime. However, any online activity which basically offends human sensibilities can be regarded as a cybercrime.

3. What are the various categories of Cybercrimes?

A. Cybercrimes can be basically divided into three major categories −

- Cybercrimes against persons,
- Cybercrimes against property, and
- Cybercrimes against Government.

4. Tell us more about Cybercrimes against persons.

A. Cybercrimes committed against persons include various crimes like transmission of child pornography, harassment using e-mails and cyber-stalking. Posting and distributing obscene material is one of the most important Cybercrimes known today.

5. Is Cyber harassment also a Cybercrime?

A. Cyber harassment is a distinct cybercrime. Various kinds of harassment does occur in cyberspace. Harassment can be sexual, racial, religious, or other. Cyber harassment as a crime also brings us to another related area of violation of privacy of netizens. Violation of privacy of online citizens is a Cybercrime of a grave nature.

6. What are Cybercrimes against property?

A. Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

7. Is hacking a Cybercrime?

A. Hacking is amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer system without your knowledge and has tampered with precious confidential data.

The bitter truth is that no computer system in the world is hacking proof. It is unanimously agreed that any system, however secure it might look, can be hacked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, and Amazon are a new category of Cybercrimes which are slowly emerging as being extremely dangerous.

Using one's own programming abilities to gain unauthorized access to a computer or network is a very serious crime. Similarly, the creation and dissemination of harmful computer programs which do irreparable damage to computer systems is another kind of Cybercrime.

8. What is Cybercrime against Government?

A. Cyber Terrorism is one distinct example of cybercrime against government. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual hacks into a government or military maintained website.

9. Is there any comprehensive law on Cybercrime today?

A. As of now, we don't have any comprehensive laws on cybercrime anywhere in the world. This is the reason that the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain. Cybercrimes fall into that grey area of Internet law which is neither fully nor partially covered by the existing laws. However, countries are taking crucial measures to establish stringent laws on cybercrime.

10. Is there any recent case which demonstrates the importance of having a cyber law on cybercrime within the national jurisdictions of countries?

A. The most recent case of the virus "I love you" demonstrates the need for having cyber laws concerning cybercrimes in different national jurisdictions. At the time of the web publication of this feature, Reuters has reported that "The Philippines has yet to arrest the suspected creator of the 'Love Bug' computer virus because it lacks laws that deal with computer crime, a senior police officer said". The fact of the matter is that there are no laws relating to cybercrime in the Philippines.

11. What is Vishing?

A. Vishing is the criminal practice of using social influence over the telephone system, most often using features facilitated by Voice over IP *VoIP*, to gain access to sensitive information such as credit card details from the public. The term is a combination of "Voice" and phishing.

12. What is Mail Fraud?

A. Mail fraud is an offense under United States federal law, which includes any scheme that attempts to unlawfully obtain money or valuables in which the postal system is used at any point in the commission of a criminal offense.

13. What is ID Spoofing?

A. It is the practice of using the telephone network to display a number on the recipient's Caller ID display which is not that of the actual originating station.

14. What is Cyber espionage?

A. It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods on the internet.

15. What is the meaning of Sabotage?

A. Sabotage literally means willful damage to any machinery or materials or disruption of work. In the context of cyberspace, it is a threat to the existence of computers and satellites used by military activities

16. Name the democratic country in which The Cyber Defamation law was first introduced.

A. South Korea is the first democratic country in which this law was introduced first.

17. What are Bots?

A. Bots are one of the most sophisticated types of crime-ware facing the internet today. Bots earn their unique name by performing a wide variety of automated tasks on behalf of the cyber criminals. They play a part in "denial of service" attack in internet.

18. What are Trojans and Spyware?

A. Trojans and spyware are the tools a cyber-criminal might use to obtain unauthorized access and steal information from a victim as part of an attack.

19. What are Phishing and Pharming?

A. Phishing and Pharming are the most common ways to perform identity theft which is a form of cyber-crime in which criminals use the internet to steal personal information from others.

20. Mention some tips to prevent cyber-crimes.

- Read the latest ways hackers create phishing scams to gain access to your personal information.
- Install a firewall on your computer to keep unwanted threats and attacks to a minimum.
- Use caution while opening emails and clicking links. You should tread carefully while downloading content from unverified sources.
- Create strong passwords for any websites where personal information is stored.