

FREQUENTLY ASKED QUESTIONS (FAQ)

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. Is watching Cyber Pornography a crime or not?

A. Watching cyber pornography in private area is not a crime. For more details, visit - <https://www.youtube.com/watch?v=D-yCtVWcjw8&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=2>

3. Is watching Child Pornography a crime or not?

A. Yes, watching child pornography is a crime. For more details, visit - <https://www.youtube.com/watch?v=D-yCtVWcjw8&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=2>

4. Where to report ATM fraud?

A. Report ATM fraud to nearest police station or online at national cybercrime reporting portal. For more details, visit- <https://www.youtube.com/watch?v=4-LvsFd8fQ&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=7>

5. Can feature (keypad) phone be also used for ATM fraud?

A. Yes, featured phone can also be used as a tool for ATM fraud. More details, visit - <https://www.youtube.com/watch?v=4-LvsFd8fQ&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=7>

6. What to do if a fake Facebook profile has been made?

A. Report to nearest police station. For more details, visit - https://www.youtube.com/watch?v=UnZAE_3TrRI&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=23

7. Can Whatsapp be hacked?

A. Yes, Whatsapp can be hacked. For more details, visit - <https://www.youtube.com/watch?v=KIYu2ijxZ3o&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=19>

8. What to report a stolen laptop/mobile?

A. Report to nearest police station. For more details, visit - <https://www.youtube.com/watch?v=VAzA4UV8p5Y&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=36>

9. What to do when someone blackmails me using nude video call?

A. Report to nearest police station. If the blackmailer asks for money, do not pay them. Paying money will make him/her continue to blackmail for larger amounts.

10. How to make strong passwords?

A. Strong passwords contains both uppercase and lowercase letters along with digits and special symbols like @, #, \$, %, &, <, >, etc. For more details, visit - <https://www.youtube.com/watch?v=VboU2XSpasQ&list=PL3qx8gT1WpLzQom-VzFxfVlvemZjKpx5N&index=31>

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. Is there any comprehensive law on Cybercrime today?

A. In India, we have IT Act which has sections which punish cyber criminals.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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

23. 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.

24. 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.

25. 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.

26. 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.

27. 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 read carefully while downloading content from unverified sources.
- Create strong passwords for any websites where personal information is stored.

27. What is Spam?

A. Spam means unrequested emails that you receive through commercial advertisers. These mails if responded to can sometimes lead to hackers having access to your computer/phone and your personal and confidential information stored in the device could be at risk.

28. How can I protect my banking information?

A. You can protect your banking information by taking the following preventive measures:

- Do not write down login and password information.
- Never provide your login information to anyone.
- Change your password at least once each quarter.
- Check your financial statements regularly, and report all suspicious activities.

29. How can I save myself from becoming a victim of fraud?

A. Keep the following in mind to save yourself from fraud:

- Be suspicious of any email, website, or person asking for financial information or passwords.
- Don't click on suspect links or open email attachments.
- Regularly change passwords.
- Review financial statements.
- Install updates offered by your operating system and software providers.
- Update antivirus regularly.

30. Is clicking and uploading nude pictures a cyber-crime?

A. Yes, it would amount to cybercrime. It is termed as "*voyeurism*" under section 345C of Indian Penal Code, 1860 and is punishable with imprisonment of 3 to 7 years.

31. Is it possible for hackers to access my computer's webcam?

A. Yes, they can. Each time you click away an update prompt, vulnerabilities in the apps you use expose your system to cyber-attacks. Cyber criminals take

advantage of these, make you navigate to fake websites, download malicious PDF documents or click on infected web banners on legitimate website.

32. What kind of passwords are more secure to protect my computer from hackers?

A. Complex, long passwords are better, but they're only useful in certain conditions. However, complex passwords are not enough to keep your profile protected. You need to:

- Manage passwords safely by using a password manager.
- Turn on 2-step authentication wherever it's available.
- Make sure the sensitive websites you visit (online banking, online shopping, etc.) use an encrypted connection.
- Keep your browser and software updated.

33. What can I do if I am a victim of online shopping fraud?

A. Gather all information you saved or printed when you were ordering and call the store's customer service department. Try to straighten things out directly. If the store refuses to consider your complaints, or temporizes, or doesn't answer the phone, you better talk to your credit card company or best file a complaint at the cyber cell.

34. Where can I file a cybercrime complaint?

A. The IT Act of India states that, when a cybercrime has been committed it shall have global jurisdiction. Hence, a complaint can be filed at any cyber cell situated in your city or elsewhere. It is advisable to always approach a cyber cell that is closer to your place for better access.