1. **Malicious:**- It has the capability to do something bad. It can be your finances,it can seal your money or anything else which is important for you. it can do something with data or files. It is not a nursery that will harm you. So it may be possible that you downloaded the malicious code from the internet but did not install it. So That means your computer has not been affected yet but there is malicious code in your computer.
2. **Phishing:-** Creating a duplicate or exact copy of a web page. For example creating a SBI login webpage and sending it to people to fill that and people filling that. So it's a kind of attack/hacking which is done to take credentials of a person by duplicating a webpage. There is many type of credential:
   1. You can stand behind him and see the credentials.
   2. Calling his mother or father and trying to get crediantle, etc.

Never do this because it is a cybercrime and you may go to jail for doing this.

1. **Social Engineering:** Social engineering done by taking information form you or from the internet or by talking to you personally. So basically means taking the information from you and using it for malicious purposes , financial purposes, etc.
2. **Spying:- spring is just a process to gain information, not hacking.** So gaining information is an important thing here. So spring can be a part of phishing. Ex: trying to see the keyboard while the other person is trying to stand behind the person. OR seeing information true to the camera that the password person is using.
3. **Ransomware:-** Ransomware is a kind of virus or you can call it a piece of software. Which **basically it locks all the files and makes it in an unreadable format.** So you cannot open that So **Ransome** basically means exchange of money. So applications ask you for a certain amount of money to open that. So you can pay them by throwing bitcoin or crypto. Paying money through bitcoin is very very hard but not impossible. So you have to pay Ransom whatever they are asking and then they unlock the information. But there is no guarantee that they will unlock you. So in future they can again come and ask you for money.

But government guidelines says that we should not pay ransom

amount and we should try to unlock by security expert.

1. **Key-Logging:**  Key-Logging is an activity of monitoring your key on your keyboard.
2. **Key-Logger:** key-logger is a software or a hardware that collects data and it genary used for hacking data. Ex: Let's say that you want to know your friend’s facebook password so you will go and you insert a usb kind of divide in his computer. Now whatever he does with his keyboard , it will be recorded inside that USB device. At that time if you use a mouse, or mouse activity, that also might be recorded. Same thing happened to the ATM machine ETC.
   1. To avoid this company has moved fast and is asking for 2-factor authentication or second time authentication password. 2-factor authentication passwords basically help you and ignore these things.
   2. Software is more harmful and it's easy to get.
3. **DDOS Attack(DoS-Denial of Services):** DDOS Attack done by either physical devices or most of the time it's done by computer. Whenever DDOS attract happens, it happens with a lot of devices and servers. And because of that your service goes down and its its tough to manage it.
   1. To stop this we use clouds. Cloud is a kind of system where thousands and thousands of servers are connected. So here you allowed to cloud that doesn’t matter what my site should not go down. Doesn’t matter how how money you have to pay. And India is avery very good init.
   2. It mostly happens in Gov. websites, e-commerce websites or it may happen with company websites as well. **Why do they do that?**
      1. Well they do that so they can control the website, or put their link and earn from it. OR they may give bad links or adult links to ruin the reputation.
4. **Cybercrime:** Cybercrime can be cattrise in many different ways.The very popular one is **“Trying to be someone else, which you are not.”**
   1. FOR EXAMPLE: you have created a fake facebook account and are talking to someone. That is cyber crime.
   2. Created a facebook account using anyone's name and asking money to their relatives. That is also a cyber crime.
   3. Or calling someone and saying that they have won 5 lakh rupees or a car. And then they say that they have to pay some amount to get the price. So these things come into a Cyber crime.
   4. One very very important thing is that people buy new numbers but they do not change/update the number on their facebook account. So what happens is that someone buys that number and tries to connect with accounts. So it should be very very important to change the number from the account as well.
5. **VPN(Virtual private Network):-** It's a kind of system where you can shift and use it. For ex: if any website is not opening from India but its opening in USA. so you can connect through the USA and see that website even if you are in india.
6. **Dark-Web**: The dark web refers **to encrypted online content that is not indexed by conventional search engines**. Sometimes, the dark web is also called the dark net. So if you want to know more about it, just go and search about it. But never ever buy anything from there, or never try to message them or never ever create an account there.
7. **Footprint:-** Footprint intrams of cyber security is basically an information which lists OR describes a person who has visited or gone through the website. For example: if you go to Amazon Website and open any product then your footprint is marked there, if you hit on another product it will open there. So this footprint can find what you like. And show you products related to that or it may show you ads related to that.
8. **FingerPrint:** Fingerprint and footprint are almost the same thing. So let's say you want to buy a gaming laptop. So they will use machine learning and show you all kinds of gaming laptops. So there will be gmail login, or subscribe, or a cookie which will tell information about you and then it shows you content/product related to that. And not only that website but it shows wherever you go. For ex: if you will go to read articles, or to read news, or to watch videos. The ads keep following you. And these all thing happen because of footprint/fingerprint.
   1. Wherever you go to facebook and like OR comment OR share. At the same time you live there. And if you observe then facebook keeps showing videos or memes related to that.
9. **Algorithm:** A set of steps which is very clearly written to do specific things. OR step by step to do things. Example: Opening a laptop, eating food. These things already know how to do and just follow that. And that is called an algorithm.