**Eavesdropping attack** also referred to as sniffing or snooping attack is a major concern when comes to cyber security. Through these attacks, your information like passwords, card details, and other sensitive data is easily stolen while it is getting transferred from one device to another.

These kinds of attacks are most successful because they don't raise any kind of alert while the transmission is taking place because they take advantage of unsecured network communications to access data while it is being sent or received by its user. As Tom King, applications and security manager at 3i writes-

*Eavesdropping attacks are insidious because it's difficult to know they are occurring. Once connected to a network, users may unwittingly feed sensitive information — passwords, account numbers, surfing habits, or the content of email messages — to an attacker.*

Consider that you are a remote employee and you are transmitting some sensitive business information to your boss over the open network. At this point, a cyber attacker can silently intrude and place some software through which he can eavesdrop in the network pathway and capture all the important information. This is a classic example of an eavesdropping attack. These attacks can result in financial loss, identity theft or privacy loss, etc.

Eavesdropping Methods:

Attackers use various methods or techniques to listen in on conversations or to review network activity by using:

- Pickup devices pick up sounds or images, from the attached microphones and video cameras, and then the attackers can convert them into an electrical format to eavesdrop on targets. Attackers may also use mini amplifiers that help them in minimizing the background noise.
- A transmission link between a sender and the receiver would be tapped to eavesdrop. This can be done with the radiofrequency transmission or a wire, which can include active or unused telephone lines, electrical wires, or ungrounded electrical conduits. Some transmitters can operate continuously, but another approach can be remote activation.
- A listening post is when we put bugs on telephones to hear the conversations taking place. It uses triggers that records when a telephone is picked up to make or take a call and it is automatically turned off when the call ends. Secure areas where these recordings are monitored are known as listening posts. It can be anywhere, and they

have voice-activated equipment available to eavesdrop and record every activity.

- It is easier for attackers to gain unauthorized access to user accounts when weak passwords are used. It gives them a way to intrude into corporate systems and networks. Cyber attackers use these to their advantage and access confidential communication channels, intercepting activity, to listen in on conversations between colleagues to steal confidential business data.
- Users who connect to open networks that do not require any password and do not use encryption for the transmission of data provide an ideal situation for attackers for eavesdropping. Attackers can easily monitor user activity and listen to the communications that take place on the network.

Examples of Eavesdropping Attacks:

The attackers are usually looking for sensitive information that can be sold for criminal purposes that including call recordings, business strategies, and financial details. Some examples are :

- Spouse ware allows people to eavesdrop on their significant others by tracking their smartphone use or location details and keeping a check on all of their activities.
- Getting users' login credentials for hacking their Facebook accounts or email ids or stealing their card details when they are connected to public wi-fi networks like the ones that are freely available at railway stations or cafes etc.
- Smart voice recognition assistants like Amazon Alexa and Google Home are also vulnerable to eavesdropping because of their "always-on" mode which is a big threat to users' privacy.
- Wireshark was a sniffing program that caused Android smartphone users a lot of trouble back in 2011. In this attack authentication tokens were sent all over an unencrypted Wi-Fi network which resulted in Wireshark viewing, stealing, modify and even deleting all the confidential data.
- In 2015 even iOS suffered when over 25,000 iOS apps were vulnerable to eavesdropping attacks because of a bug in the open-source code library AFNetworking due to which HTTPS encryption could be taken down.

Eavesdropping Attack Prevention:

- Avoid using public Wi-fi networks.

- Use a virtual private network (VPN).
- Set strong passwords and change them frequently.
- Don’t repeat passwords for every site you register in.
- Protect your pc with antivirus and keep it updated.
- Use a personal firewall.
- Avoid clicking on shady or dodgy links.
- Make sure your phone is using the latest version available of its operating system.
- Download apps only from trusted sources like Android or Apple stores.
- Military-grade encryption is a great way to defend against an eavesdropping attack as it will take attackers around 500 billion years to decode i