investopedia.com

What Is an Eavesdropping Attack?

Full Bio

4-5 minutos

What Is an Eavesdropping Attack?

An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device.

The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.

Key Takeaways

- An eavesdropping attack is the theft of information from a smartphone or other device while the user is sending or receiving data over a network.
- Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN).
- Avoiding public Wi-Fi networks and adopting strong passwords are other ways to prevent eavesdropping attacks.

Eavesdropping is a deceptively mild term. The attackers are usually after sensitive financial and business information that can be sold for criminal purposes. There also is a booming trade

in so-called spouseware, which allows people to eavesdrop on their loved ones by tracking their smartphone use.

Understanding the Eavesdropping Attack

An eavesdropping attack can be difficult to detect because the network transmissions will appear to be operating normally.

To be successful, an eavesdropping attack requires a weakened connection between a client and a server that the attacker can exploit to reroute network traffic. The attacker installs network monitoring software, the "sniffer," on a computer or a server to intercept data as it is transmitted.

Amazon Alexa and Google Home are vulnerable to eavesdropping, as are any internet-connected devices.

Any device in the network between the transmitting device and the receiving device is a point of weakness, as are the initial and terminal devices themselves.

How to Foil an Eavesdropping Attack

Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN).

Using a strong password and changing it frequently helps, too. And don't use the same password for every site you log onto.

Public Wi-Fi networks such as those that are available free in coffee shops and airports should be avoided, especially for sensitive transactions. They are easy targets for eavesdropping attacks. The passwords for these public networks are readily available, so an eavesdropper can simply log on and, using free software, monitor network activity and steal login credentials

along with any data that other users transmit over the network.

If your Facebook or email account has been hacked lately, this is probably how it happened.

Virtual Assistants Can Be Spied Upon

Virtual assistants such as Amazon's Alexa and Google Home also are vulnerable to eavesdropping and their "always-on" mode makes them difficult to monitor for security.

Some reported incidents that the companies did the snooping themselves appear to have been accidents caused by mistakes in speech recognition.

Avoid Dodgy Links

Another way to limit your vulnerability to an attack is to make sure your phone is running the most recent version available of its operating system. However, its availability is up to the phone vendor, who may or may not be efficient about offering the update.

Even if you do all of the above, you have to be careful from day to day. Avoid clicking on dodgy links. The sites they link to may install malware on your device. Download apps only from the official Android or Apple stores.