Wireless technology

It is a technology that allows the communication of distant entities without the use of wires or cables but using RF (radio frequency) as well as IR (infrared) waves.

RF is the frequency associated with radio wave propagation within the electromagnetic spectrum, and when it’s applied to an antenna, that creates an electromagnetic field which propagates through space. The AP (access point) is the cornerstone of wireless network that broadcasts a wireless signal for the computers -that are equipped with wireless network adapters which is often built in the computers or have an add-on adapter plugged into one of their expansion slots  
(USB port)- to detect and tune as well as it serves as a link to the wired network such as internet.

There are a lot of daily used examples on wireless technology like Wi-fi, radio, TV, radar and GPS, and 5G (fifth generation) is from the most important of them where it’s exponentially faster.

There are four types of wireless networks: wireless local area networks, wireless metropolitan area networks, wireless personal area networks and wireless wide area networks, each with its own function.

The reasons behind why wireless technology is now used on a large scale is that it’s a lot cheaper to install and maintain, is a lot faster, can be accessed anytime anywhere without carrying cables or wires which saves a lot of time and effort as well as it’s much more good in emergencies where it allows remote communication of help and support.

On the other hand, it has a lot of security threats such as raves dropping, man in he middle attack, IP and MAC addresses spoofing and denial of service (DoS) attach, and to secure wireless signals like WPA and WPA2, one must use strong security protocols. Alternatively, you can also use wireless intrusion prevention system to secure the wireless network.

One of the advantages of wireless technology is interference that can be minimized by relocating wireless networking hardware or specialized antennas, and its mainly sources are building materials like glass, concrete and metal that absorbs or reflects the radio waves, and devices like microwave ovens and cordless phones that operates in the same frequency range.

Data security on wireless networks mainly depends on encryption feature where you can protect your data and control access to network. Wireless network hardware supports several standard encryption schemes, but the most common are Wired Equivalent Privacy ([WEP](https://www.webopedia.com/definitions/wep/)), Wi-Fi Protected Access ([WPA](https://www.webopedia.com/definitions/wpa/)), and Wi-Fi Protected Access 2 ([WPA2](https://www.webopedia.com/definitions/wpa2/)).

Where WEP is the oldest and least secure encryption scheme. However, WPA and WPA2 are better and even better by using longer and more complex passwords.