5 Ways to secure Wi-Fi Networks

Wi-Fi or wireless networks are great for home and small business users, allowing to use multiple internet capable devices on one shared connection. But wireless networks can be subject to vulnerability#, malicious eavesdropping##, hacking###, and freeloaders####. The security protocol used to protect the vast majority of wifi connections has been broken, potentially, if you don't use proper protection when you set up a network. Hackers can easily intercept wireless network traffic over open air connections and extract information like passwords and credit card numbers, bank accounts, etc. Wi-Fi is one entry-point hacker can use to get into your network without setting foot inside your building because wireless is much more open to eavesdroppers than wired networks, which means you have to be more diligent about security.

Vulnerability

The vulnerability#, dubbed "KRACKs" (Key Reinstallation AttaCKs), is actually a group of multiple vulnerabilities that when successfully exploited, could allow attackers to intercept and steal data transmitted across a Wi-Fi network. Digital personal information that is transmitted over the Internet or stored on your connected devices — such as your driver's license number, Social Security number, credit card numbers, and more — could be vulnerable. All of this personal information can be used toward committing identity theft, such as accessing your bank or investment accounts without your knowledge.In Wi-Fi network attackers can manipulate web pages, turning them into fake websites to collect your information or to install malware on your devices.

Eavesdropping

Eavesdropping## is the unauthorized real-time interception of private communication, such as a phone call, instant message, videoconference or fax transmission. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside. The security layer that protects Wi-Fi networks has been cracked by hackers, potentially allowing them to listen to your communications on devices connected to the internet,

Hacking

Hacking### a cybercrime means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network.

Freeloaders

Freeloaders#### are unauthorized users jumping on your Wi-Fi connection. Freeloaders will not only consume your bandwidth but can also wreak havoc on your network and use your connection to perform illegal activities.

Importance of Network security

A hacker is an individual who uses a computer, networking or other skills to overcome a technical problem. The term hacker may refer to anyone with technical skills, but it often refers to a person who uses his or her abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example, steal information to hurt people via identity theft, damage or bring down systems and, often, hold those systems hostage to collect the ransom

What is Wi-Fi

Before we talk about wifi network security and vulnerability attacks, let us know what is Wi-Fi, which I have already discussed in my previous post, "What is wifi and how it works".WLAN (IEEE 802.11x) protocol links two or more devices over a short distance, using spread spectrum signals. (Spread spectrum is a technique used for transmitting radio or telecommunications signals. The term refers to the practice of spreading the transmitted signal to occupy the frequency spectrum available for transmission).To establish a wifi network, we need one wireless access point and one wireless adopter in the device. Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it. Please understand the difference between router and access point. The router acts as a hub that sets up a local area network and manages all of the devices and communication in it. Wireless routers function as a basic access point. An access point, on the other hand, is a sub-device within the local area network that provides another location for devices to connect from and enables more devices to be on the network. So access point enables to connect more devices. A router act as an access point but Access point cannot work as a router.

Wifi Network security

Here we will discuss the wireless Network security (Wireless Security) which is under the head of Network (Wired and wireless Network) cybersecurity Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. The core area is the prevention of unauthorized access or damage to computers or data using wireless networks.

1. WPA/WPA2

Wi-Fi is one entry-point which hacker can use to get into the network. The wireless networks don't have built-in security mechanisms. Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default. This security is achieved by WPA /WPA2

–what is WPA/WPA2-WPA stands for Wi-Fi Protected Access, and is a security technology for Wi-Fi networks. It was developed to overcome the weaknesses of WEP (Wired Equivalent Privacy), WPA provides strong encryption by use of either of two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also includes built-in authentication support. Later on, it was found TKIP has some security holes so WPA2 was developed with strong wireless encryption and does not allow the use of an

algorithm called Temporal Key Integrity Protocol (TKIP). Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is a new wireless security protocol in which only authorised users can access a wireless device, with features supporting stronger cryptography (e.g. Advanced Encryption Standard or AES), stronger authentication control (e.g. Extensible Authentication Protocol or EAP), key management, replay attack protection, and data integrity. Wi-Fi certified product has had to use WPA2 since 2006 and is based on the IEEE 802.11i technology standard for data encryption. WPA2 has Advanced Encryption Standard(AES) for security.Also, WPA2 requires to enter a longer password than WPA requires. Only WPA2 should be active in the router as WPA sometimes interfere with WPA2 and WEP make it easier for hackers to break into the network. You can check the security of your router at secure.com
Both versions of Wi-Fi Protected Access (WPA/WPA2) can be implemented in either of two modes: Personal mode and enterprise mode

2.WPA/.WPA2 in Personal mode

When enabling the Personal mode—technically called the Pre-shared Key (PSK) method—of WPA or WPA2 security, you create one unique global password. Everyone enters this same password before connecting to the wireless network. This mode is appropriate for most home networks—but not business networks. A unique encryption passphrase* is defined on the wireless router and any other access points (APs). The passphrase must be entered by users when connecting to the Wi-Fi network. This passphrase is saved on the device.
A passphrase* is a string of words that must be used to gain access to a computer system or service. The passphrase is the latest trending buzz online nowadays.
A password, a secret word or phrase that must be used to gain admission to a place,.is typically composed of not more than 10 letters or symbols, or a combination of both. It could be a string of random symbols such as “A@ew#qS” or just a word like “Ohmygod”, or a combination of both such as “hel@py#u!”.
A passphrase can also contain symbols, words, numbers and does not have to be a proper sentence or grammatically correct but uses spaces and can be much longer than the password. For example “Work hard to help self @99” is a passphrase. A Passphrases is easier to remember and are next to impossible to crack. Major OS and applications support passphrase. It should be least more than 14 characters long for better security

3.WPA/WPA2 in Enterprise Mode

WPA2 Enterprise uses IEEE 802.1X, which offers enterprise-grade authentication. In this setup, there is no shared passphrase. The Enterprise mode of WPA or WPA2 security, however, enables to assign users a unique username and password to log into the Wi-Fi, if you implement the popular PEAP method.PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections.PEAP is designed to provide more secure authentication for 802.11 WLANs).In this way, it authenticates every user individually. The

encryption keys for the network aren’t saved on computers or devices. Users never deal with the actual encryption keys. They are securely created and assigned per user session in the background after a user presents their login credentials. This prevents people from recovering the network key from computers.This technique prevents hackers from performing dictionary-based attacks

4. Use an inconspicuous network name (SSID) & Password

When you turn on your device’s Wi-Fi capabilities, You look at some of the names of your neighbors’ connections. In this way, you will find some are using the name of their organization or the family’s name, or even just the default SSID used by the router. If you are using your home address, or some date of birth, family name, then you are broadcasting yourself to intrusion. The name should be difficult and should not reveal any of your identity. Think of your wireless network name almost as if it were a password. The more unique it is, the better. The password of Wi-Fi (SSID) should be Random, Complex and long. The network password can be up to 63 characters long so feel free to be creative with your password.Now a days use passphrase

5.Physical Security

Most of the access points (router) have a reset button, which is used when you forget SSID name and password. This button brings all setting to default one. If there is no physical security of access point, anyone can reset and use the wifi network to their advantage. By securely mounting network equipment, such as access points, in a less accessible location with strong physical security controls, the risk can be minimized.