How to Secure your Wi-Fi at home and in your Business

Most households and companies go to great lengths to keep unauthorised users off their networks, but Wi-Fi access points and routers can provide hackers with a convenient way in.
That's because Wi-Fi signals are often broadcast beyond the walls of buildings and homes and out into the streets - an enticing invitation for hackers. No wonder that wardriving or drive by hacking is a favourite past time amongst cybercriminals.
Since many companies allow or even actively encourage employees to connect to the network using their own mobile devices - tablets and smartphones as well as laptops - it's not practical for most companies to switch off Wi-Fi access.

The same applies to home broadband users who might have guests coming over frequently. Instead, here are a few tips to make your wireless network more secure.

1. Use stronger encryption

Some Wi-Fi access points still offer the older WEP (Wired Equivalent Privacy) standard of protection, but it is fundamentally broken. That means that hackers can break in to a WEP-protected network using a hacking suite like Aircrack-ng in a matter of minutes.

So to keep out intruders, it's essential to use some variant of WPA (Wi-Fi Protected Access) protection, either WPA or the newer WPA2 standard (or WPA3 when it lands).
For smaller companies and households, it may be practical to use WPA with a pre-shared key. That means that all employees or family members use the same password to connect, and network security depends on them not sharing the password with outsiders.

It also means that the password should be changed every time an employee leaves the company.

Some Wi-Fi routers offer a feature called Wireless Protect Setup (WPS) which provided an easy way to connect devices to a WPA protected wireless network. However, this can be exploited by hackers to retrieve your WPA password, so it is important to disable WPS in the router's settings.

In larger organisations, it makes more sense to use WPA in enterprise mode, which allows each user to have their own username and password to connect to the Wi-Fi network.

This makes it much easier to manage when employees are leaving regularly, as you can simply disable ex-employees' accounts; but to use WPA in enterprise mode you have to run a server (known as a RADIUS server) which stores the login information for each employee.

2. Use a secure WPA password

Make sure that any password (or passphrase) that protects your Wi-Fi network is long and random so it can't be cracked by a determined hacker.

It is all too easy to set up any equipment with its default settings, especially as the default admin name and password are often printed on the router itself to allow quick access and setup. This means that hackers will try these to access your network. Changing both access name and password will make it more difficult for a criminal to gain access.

You can test the security of your WPA protected network (without revealing your password or passphrase) by using the CloudCracker service. You'll be asked to provide some data (the same data that a hacker could capture or "sniff" out of the air with a laptop from anywhere in range of your network) and the service will attempt to extract your password.

If the service is unsuccessful then a hacker is unlikely to be successful either. But if the service finds your password then you know that you need to choose a longer, more secure one.

Bear in mind that even WPA2 security standard is unlikely to resist a well organised and stubborn hacker or hacking group thanks to the KRACK Wi-Fiflaw that was discovered in October 2017.

3. Check for rogue Wi-Fi access points

Rogue access points present a huge security risk. These aren't your company's "official" Wi-Fi access points, but ones that have been brought in by employees (perhaps because they can't get a good Wi-Fi signal in their office) or conceivably by hackers who have entered your building and surreptitiously connected one to an Ethernet point and hidden it.

In either case, rogue access points present a risk because you have no control over them or how they are configured: for example, one could be set up to broadcast your SSID (the 32character identifier for a wireless network) and allow anyone to connect without providing a password.

To detect rogue access points you need to scan your offices and the area around it on a regular basis using a laptop of mobile device equipped with suitable software such as Vistumbler (a wireless network scanner) or airodump-ng. These programs allow the laptop to "sniff" the airwaves to detect any wireless traffic travelling to or from a rogue access point, and help you identify where they are located.

4. Provide a separate network for guests

If you want to allows visitors to use your Wi-Fi, it's sensible to offer a guest network. This means that they can connect to the internet without getting access to your company's or family's internal network. This is important both for security reasons, and also to prevent them inadvertently infecting your network with viruses or other malware.

One way to do this is by using a separate internet connection with its own wireless access point. In fact, this is rarely necessary as most business grade (and a lot of newer consumer) wireless routers have the capability of running two Wi-Fi networks at once - your main network, and another for guests (often with the SSID "Guest".)

It makes sense to turn on WPA protection on your guest network - rather than leave it open - for two important reasons. The first is to provide some level of control over who uses it: you can provide the password to guests on request, and as long as you change it frequently you can prevent the number of people who know the password growing too large.

But more importantly, this protects your guests from other people on the guest network who may try to snoop on their traffic. That's because even though they are using the same WPA password to access the network, each user's data is encrypted with a different "session key," which keeps it safe from other guests.

5. Hide your network name

Wi-Fi access points are usually configured by default to broadcast the name of your wireless network - known as the service set identifier, or SSID - to make it easy to find and connect to. But the SSID can be also be set to "hidden" so that you have to know the name of the network before you can connect to it.

Given that employees should know the name of your company Wi-Fi network (and the same goes for family members and friends in a households), it makes no sense to broadcast it so that anyone else who happens to be passing by can easily find it too.

It's important to note that hiding your SSID should never be the only measure you take to secure your Wi-Fi network, because hackers using Wi-Fi scanning tools like airodump-ng can still detect your network and its SSID even when it is set to "hidden."

But security is all about providing multiple layers of protection, and by hiding your SSID you may avoid attracting the attention of opportunistic hackers, so it is a simple measure that is worth taking.

6. Use a firewall

Hardware firewalls provide the first line of defence against attacks coming from outside of the network, and most routers have firewalls built into them, which check data coming into and going out and block any suspicious activity. The devices are usually set with reasonable defaults that ensure they do a decent job.

Most firewalls use packet filtering, which looks at the header of a packet to figure out its source and destination addresses. This information is compared to a set of predefined and/or user-created rules that govern whether the packet is legitimate or not, and thus whether it's to be allowed in or discarded.

Software firewalls usually run on the endpoint desktop or laptop, with the advantage of providing a better idea what network traffic is passing through the device. More than just which ports are being used and where data is going, it will know which applications are being used and can allow or block that program's ability to send and receive data.

If the software firewall isn't sure about a particular program it can ask the user what it should do before it blocks or allows traffic.

7. Enable MAC authentication for your users

You can limit who accesses your wireless network even further by only allowing certain devices to connect to it and barring the rest. Each wireless device will have a unique serial number known as a MAC address, and MAC authentication only allows access to the network from a set of addresses defined by the administrator.

This prevents unauthorised devices from accessing network resources and acts as an additional obstacle for hackers who might want to penetrate your network.

8. Use a VPN

A VPN or virtual private network will help you stay safe and secure online while above all keeping your private stuff private. They keep your data hidden from prying eyes one end to the other by encrypting it. In theory, hackers could penetrate your network and they'd still not be able to do any harm to your system assuming that a VPN is running permanently.

Reference:https://www.techradar.com/news/networking/wi-fi/five-tips-for-a-secure-wireless-network-1161225