How to check if your WiFi owner is monitoring your activity?

Even if you're outside your home and workplace, it's important to stay connected. Still, if you connect to a network you don't control, it's also important to know who might be monitoring your online activity.

If someone manages a WiFi network, such as in a coffee shop or educational institution, they can potentially track and log what connected users do. This can include information like the websites you've visited or the specific web apps you've used.

Some network owners also use more advanced monitoring techniques to log users' connection times and how long they were online. If the websites you access don't use HTTPS, the Wi-Fi owner can even intercept unencrypted data like login details or messages.

In this guide, we'll discuss the ways that your activity can be tracked by Wi-Fi owners and why they might do this. We'll also cover some common methods to detect monitoring, as well as ways you can stay safe when using other wireless networks.

Why would a WiFi owner monitor activity?

There are several legitimate (and some not-so-legitimate) reasons for Wi-Fi owners to track what you do when connected to their network. These include:

Security purposes

Workplaces often employ staff to monitor network usage to protect the business from malware and data breaches e.g. from phishing scams. Many companies also monitor employee internet activity to make sure it is in line with their policies. For instance, a business may ban access to social media during certain hours.

Bandwidth management

Network administrators can use tools to detect if certain accounts or programs are consuming large amounts of bandwidth. They can then 'shape' this traffic i.e. by slowing it down to ensure that other users can access the network without excessive slowdown.

Parental controls

Parents and caregivers may use monitoring tools to check what their children are accessing online or to set limits on network usage e.g. only during certain hours.

Legal Requirements

Depending on the jurisdiction, owners of public WiFi networks may be required to log users' Internet activity for legal and regulatory reasons. For example, in Türkiye, ISPs and other telecoms organizations are required to log customers' Internet use. Some public WiFi networks even require users to provide a photo ID to connect.

Malicious Intent

Bad actors will sometimes deliberately set up 'Free WiFi' networks to encourage unsuspecting users to connect. They will then try to intercept sensitive information for criminal purposes e.g. to commit fraud. These types of fake public hotspots are known as 'honeypot' networks. While some people may set these up out of personal curiosity, this kind of monitoring is very dangerous as the WiFi owner can monitor all your traffic.

Signs that your WiFi activity might be monitored

The safest approach is to assume that unless you've set up the WiFi network yourself, the owner is monitoring you at all times. You can then take steps to protect your privacy.

However, there are also some telltale signs that the WiFi owner might be tracking your online habits:

Router logs show visited websites

If you can access the network router's interface, you may be able to check if it logs the domains to which users connect. Not all models support this. Of those that do, not all record identifiable information e.g. they may track bandwidth usage and IP addresses of domains to which users connect, but not the specific sites you've accessed. The only way to be sure is to log in to the router and inspect its records. See below for help with this.

Look for connected devices you don't recognize

Assuming that you're connecting to a private WiFi network, you can use certain network monitoring tools to scan for unfamiliar devices that may be monitoring your activity. If you're using public WiFI this is much harder to do, as anyone can connect at any time.

Slower than usual Internet speeds

Using monitoring software can slow down connected users' Internet connections. This means if traffic has suddenly become sluggish, the WiFi owner may be using monitoring tools. However, this can also be caused by other factors like too many devices being connected at once.

Frequent disconnections/interruptions

As with slower Internet speeds, device disconnections can have many causes like network issues. However, if it's happening all of a sudden it may be due to hackers. For example, 'de-authentication attacks' work by booting connected devices off a WiFi network. Bad actors then monitor the device reconnecting, either to try to capture the Wi-Fi password or to trick it into connecting to a fake 'evil twin' WiFi network.

Antivirus alerts for spyware or malware

If the WiFi owner requires users to install specialist software to access the network or can redirect users to domains containing malware, then your machine can become infected. This can be flagged by popular antivirus programs, so pay close attention to any alerts when connecting to a network you don't control.

Changes in browser settings or the homepage

Most WiFi networks will redirect users to a landing page when they first connect e.g. to agree to the Internet usage policy. However, this shouldn't change the homepage listed in your browser settings. If this, or any other settings, change without your input then the network may have compromised your browser.

Being redirected to other websites

If a WiFi owner has bad intentions, they can redirect DNS (Domain Name System) requests for malicious websites to domains they control instead. This is known as 'DNS hijacking'. Cybercriminals can also set up a malicious proxy server between their WiFi network and the Internet to redirect connection attempts to legitimate websites to domains containing harmful code.

Redirecting is sometimes done for legitimate reasons. For instance, when you first connect to public WiFi, most networks will redirect you to a 'captive portal' that asks you to agree to the terms and conditions before you can use the Internet.

Legal disclaimers or Terms of service

As we've learned, in most cases when you use public or corporate Wi-Fi you'll be asked to agree to their terms of service before you connect. Read through these carefully, as if your activity is being monitored this will likely be mentioned here.

Accessing router logs

If you have administrative access to the wireless network router, you can check its settings to see what activity is being monitored (if any).

However, we can't emphasize strongly enough that you should do this only with the permission of the network owner. Even if you feel they are threatening your online privacy, in most jurisdictions it's still illegal to access a network device without the owner's permission.

Assuming you have obtained permission, make sure your device is connected to the network in question then find your router's IP address. This is usually 192.168.1.1 or 192.168.0.1.

If you're unsure, the router IP is sometimes written on the device itself. Alternatively, check the manufacturer's website for the specific model to discover its IP address.

Once you've connected successfully, you'll next be asked to sign in to the router with your admin credentials. If you're not sure what these are, first check with the WiFi owner.

Failing this, read the manufacturer's online documentation to discover the default username and password. Once you're signed in, make sure to change the default password to something more secure using a reliable random password generator.

The next steps you take will depend entirely on your router model and the currently installed firmware. Popular options to check can include:

- System logs
- Traffic logs
- Security

Look for lists of connected websites and IP addresses. If you see these, you should also check for further data like MAC addresses (used to identify specific network devices) and/or the names of connected devices.

Remember, there are legitimate reasons to monitor network activity. The router may also not be recording information that can be used to identify your Internet usage, just lists of IP addresses/domains accessed by all users.

If you have time, check the router DNS settings to ensure that these are for a legitimate provider e.g. Google's DNS server addresses are 8.8.8.8 and 8.8.4.4.

Using network monitoring tools

In theory, utilities like Wireshark can be used for 'packet sniffing. I.e. to monitor all network traffic. In practice, unless you're a skilled network administrator then it's extremely difficult to filter specific traffic related to monitoring.

Still, even if you don't have this level of expertise there are some graphical, beginner-friendly scanning tools that you can use to detect all connected network devices and associated IP/MAC addresses like Angry IP Scanner.

If you see any devices you don't recognize, use your chosen tool to export the data so you can send it to the WiFi owner.

Running regular antivirus/antimalware scans is always a good idea, particularly so if you're connecting to a WiFI network you don't control. Update your software before running the scan so it can detect the latest threats.

Change your network profile

Most modern operating systems support different profiles depending on how much you trust the WiFi network to which you're connected.

For example, when you first connect to a network in Windows 11 your profile is set to 'public' by default. This makes it harder for other connected network devices to find yours. While this won't block all forms of monitoring, you should always use the 'public' profile where available, unless you need to communicate with other network devices e.g. for printer sharing.

Non-technical checks & considerations

Most corporate or public wireless hotspots have a 'Terms of Service' or 'Acceptable Use' policy. Make sure to read these carefully before you connect to check what you're allowed to do, and what activity they monitor.

Even if you're not authorized to access the network router, you can also use your eyes. If you see any unfamiliar devices connected to the router or your computer, disconnect from the network and speak to the WiFi owner about them before you proceed.

If it's safe and appropriate to do so, you can also ask the WiFi owner about any monitoring practices. Most network administrators are open about the activity they log, as it's done for legitimate purposes.

This is also a good time to do some online research about what data users typically share over wireless networks. For example, it's relatively easy for other users to see the IP and MAC address of your connected device. This information can be used to compose a 'digital footprint' of your online activities.

How to enhance your privacy on WiFi networks

As you'll see from our online guide to using public WiFi, our first advice to stay safe online is not to use it. These days, most people have access to mobile devices with 4G/5G connections and you can install eSIMs with a generous data allowance very inexpensively.

Most of these also support creating a wireless 'hotspot' to which you can connect your laptop or computer.

However, we understand that sometimes you may have no choice but to connect to a WiFi network you don't control. If you have to do this, some best practices include:

Use a secure web browser

Open-source privacy-focused web browsers like Brave and Pale Moon can offer excellent protection against tracking. This is because they contain code to block ads, as well as scripts that can gather data on your device.

This protection is primarily designed to protect you from websites and advertisers snooping on your sensitive data, but can also be useful when you're on untrusted networks.

Use HTTPS

When you connect to a domain protected by HTTPS, then your browser can use its 'SSL Certificate' to negotiate a secure connection using TLS.

This will then encrypt traffic between your device and the site. This means, for example, that the WiFi owner could see that you have connected to a search engine like Google or Startpage but not the keywords you entered into the search bar.

All modern web browsers will use the HTTPS version of a website if it's available. However, if you're uncertain you can check the browser address bar to ensure the connection is secure.

If you're on an untrusted network and visit a site that doesn't use HTTPS, we recommend waiting until you're connected to your home network before proceeding.

Use Secure DNS

By default, most DNS queries are sent unencrypted. This means the first time that your device tries to connect to a domain it will send a 'query' to a dedicated DNS server to request its IP address.

If someone like your WiFi network owner is monitoring your connection, this means that they can log every site you visit.

Secure DNS resolves this by encrypting your DNS queries. Popular types include DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) which make it much harder for anyone to track which domains you're accessing.

Setting up DoH and DoT is fairly easy, as both standards are supported by popular DNS providers like Google and Cloudflare.

You can configure your device to use these instead of the DNS servers provided by your WiFi owner.

If you use a top-tier VPN service like hide.me, however, this step isn't necessary as the VPN client automatically sends all DNS queries to the VPN server.

Use two-factor authentication (2FA)

In a worst-case scenario, if the network owner is monitoring your connection they may be able to steal credentials for your online accounts.

You can mitigate this risk by using two-step verification. This means that when you sign in to your account for the first time from a new device you'll be asked to supply a special 6-digit code along with your password.

This code is generated using a dedicated app like Google Authenticator, so even if the WiFi owner steals your password they still won't be able to access your account.

Use a VPN

When you use a reliable VPN service your device establishes a secure connection to the VPN server.

This works differently from HTTPS, as while accessing websites secured with an SSL certificate can encrypt traffic between it and your device, the network owner can still see which sites you've visited.

However, with a VPN all traffic is encrypted before leaving your device. This means that not even the WiFi owner can see what sites you've accessed or which web apps you're using.

The best VPN services like hide.me come with additional security features like a kill switch, which blocks internet access unless you're connected to the VPN. This reduces the chance that the WiFi owner can monitor your activity if the VPN connection fails.

What to do if you suspect or confirm monitoring

Identify the network type

First, confirm whether this is a corporate network, public WiFi, or a private home network. Hotspots in business environments and public spaces are more likely to be monitored than private networks to optimize traffic and ensure no one is misusing the service.

Understand the potential reasons for monitoring

Once you understand the network type, you'll gain a better understanding of why the WiFI owner is monitoring users' activities. It may be for security reasons and/or to ensure compliance with local laws.

The owner may also monitor the network for personal reasons e.g. parents who want to ensure their children are only accessing appropriate content. If you suspect that the WiFi owner is tracking network activity for illegal purposes e.g. to steal sensitive information, contact a legal advisor for information on how to proceed.

Take steps to improve your privacy

The best way to protect yourself from network monitoring is not to connect to it. Instead, use a mobile data connection when you're away from trusted wireless networks in your home or workplace.

You can also follow the steps already outlined above, such as using a secure browser combined with a reliable VPN service to block malicious code and encrypt all your Internet traffic.

Review company or network policies

Generally speaking, employers have the right to monitor worker's Internet usage on their devices.

The situation becomes murkier if a company has BYOD (bring your own device) policies, or someone is working remotely as they may use their machine for both personal and business reasons.

The best solution to this is to carefully read all company and network usage policies when using business WiFi.

If you've been given a device to use for work purposes, use it only for that purpose. Keep a separate device for personal activities e.g. accessing your social media accounts.

This is particularly important if your company policy doesn't allow you to take steps to protect your privacy e.g. installing secure browsers or using a VPN.

If you suspect malicious monitoring or hacking

Disconnect from the network immediately

Save and close any running programs. Next, go to your device's network settings, and choose to either 'disconnect' from or 'forget' the target wireless network.

Run security scans on your devices

If this is a company device, submit it to your organization's IT department to check for unauthorized monitoring. If the device is yours, update your antivirus/antimalware software then run a full system scan.

Change passwords for important accounts

If you followed our advice (above) to use 2FA for your accounts, then even if the password is compromised bad actors still won't be able to log in.

Nevertheless, this is a good time to check that you use strong, unique passwords for all your important accounts. We recommend using an open-source password manager like Bitwarden to do this, as it can automatically generate high-entropy passphrases for each account.

Report to the relevant authorities (if necessary)

If you suspect that someone has accessed your device illegally then you can report the incident to the appropriate law enforcement body e.g. IC3 handles cybercrime reports in the USA.

Make sure to gather as much information as possible when preparing your report. If the network is a public hotspot or owned by a business make sure to include a copy of its 'acceptable use' policy detailing what monitoring (if any) is authorized.

If you have access to the network router, try to export and download relevant logs. Law enforcement can also assist you with creating a copy of your device's network logs.

If possible, don't use your device until you've spoken with the authorities, as they may want to preserve any evidence.

Stay vigilant about your online activity

In this guide, we've covered some common signs of WiFi owner monitoring including slow performance and random disconnects.

While these can be caused by other network issues, you should always check carefully for signs that your online activity is being tracked.

If you're unsure, it's safest to assume that WiFi owners are monitoring your Internet usage. That's why it's so important to take proactive steps to protect your online privacy, such as using a reliable VPN service to encrypt your web traffic.

Naturally, the spread of wireless networks makes it very easy to connect to the Internet from any location.

However, you need to balance this convenience with security. You can never be sure who's watching.

FAQ

Can a WiFi owner see my activity even if I use Incognito mode?

Yes. Incognito or 'private browsing' mode can only prevent your browsing data from being saved to your device. The WiFi owner can still see the sites your device connects to and other web data using information like the router logs unless you take extra precautions.

Does clearing my browser history stop the WiFi owner from seeing it?

No. Clearing your browser history only removes data about your browsing history from your device's internal storage. It doesn't affect the router or network logs.

Can a WiFi owner see what I do in apps?

WiFi owners can analyze your traffic patterns and DNS requests to detect whether you're using specific apps. However, most modern apps use HTTPS to connect to the provider's servers. This means, for instance, that while a WiFi owner could see you've used the Netflix mobile app they couldn't track the specific shows you watched.

Can WiFi owners steal my passwords or other credentials?

Almost all modern websites use SSL/TLS to secure logins. This means that while the WiFi owner may see that you've accessed a particular website e.g. your online bank, they won't be able to see the username and passwords you've entered. For extra security, set up 2FA (two-factor authentication). That way, even if your password is compromised, bad actors won't be able to sign in from a new device without a code generated by an authenticator app.

The WiFi owner says I have to install software to use their network. What should I do?

Many legitimate organizations like schools and businesses require users to install specialist software before using their wireless network. These can be used to block malicious/inappropriate content, as well as monitor web activity.

If you're required to do this, we recommend installing the software on a device you only use for school/work purposes.

If you need to carry out personal activities e.g. checking your Facebook account, use a different device - ideally with a mobile data connection.

If the owner of a public WiFi hotspot is asking you to install software, we recommend using a different network instead.

What's the difference between WiFi monitoring and ISP monitoring?

WiFi monitoring is done by the owner of a local network e.g. in a coffee shop. Your Internet Service Provider (ISP) can also see and log your Internet activity as it passes through its infrastructure. Your WiFi owner may be monitoring you, even if your ISP isn't and vice versa.

Is it legal for WiFi owners to monitor my activity?

In many cases, yes. In most jurisdictions, this is allowed on corporate and public WiFi networks, so long as the terms of service clearly explain that web activity may be monitored.

However, if someone creates a fake 'honeypot' hotspot or gathers network data for malicious purposes this would be illegal in most countries.

Certain jurisdictions have data protection laws, such as the EU's GDPR that require any data collected to be relevant, necessary, and deleted in a timely fashion. This means WiFi owners could get into trouble if they gather more data than is necessary, or retain it for too long.

How does a VPN protect me from WiFi owner monitoring?

When you use a trustworthy VPN service your device establishes a secure connection to the VPN server.

Even if the WiFi owner is monitoring your traffic, all they'll see is encrypted data packets. This makes it almost impossible for them to work out which sites you're accessing or apps you're using.

The best VPN services like hide.me also process DNS requests, so network owners can't track the sites you visit by forcing you to use their own DNS servers.