Securing Your Wireless Network

Today’s home network may include a wide range of wireless devices, from computers and phones, to IP Cameras, smart TVs and connected appliances. Taking basic steps to secure your home network will help protect your devices – and your information – from compromise.

- Understand How a Wireless Network Works
- Use Encryption on Your Wireless Network
- Limit Access to Your Network
- Secure Your Router
- Protect Your Network during Mobile Access

Understand How a Wireless Network Works

Going wireless generally requires connecting an internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any device within range can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network or access information on your device. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

Use Encryption on Your Wireless Network

Once you go wireless, you should encrypt the information you send over your wireless network, so that nearby attackers can’t eavesdrop on these communications. Encryption scrambles the information you send into a code so that it’s not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available for this purpose: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption.

WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only WEP encryption, which likely won't protect you from some common hacking programs. Consider buying a new router with WPA2 capability.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

Limit Access to Your Network

Allow only specific devices to access your wireless network. Every device that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

Secure Your Router

It's also important to protect your network from attacks over the internet by keeping your router secure. Your router directs traffic between your local network and the internet. So, it's your first line of defense for guarding against such attacks. If you don't take steps to secure your router, strangers could gain access to sensitive personal or financial information on your device. Strangers also could seize control of your router, to direct you to fraudulent websites.

Change the name of your router from the default. The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

Change your router's pre-set password(s). The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router, as its "administrator." Hackers know these default passwords, so change it to something only you know. The same goes for any default "user" passwords. Use long and complex passwords – think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters. Visit the company's website to learn how to change the password.

Turn off any "Remote Management" features. Some routers offer an option to allow remote access to your router's controls, such as to enable the manufacturer to provide technical support. Never leave this feature enabled. Hackers can use them to get into your home network.

Log out as Administrator: Once you've set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.

Keep your router up-to-date: To be secure and effective, the software that comes with your router needs occasional updates. Before you set up a new router and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.

And when you secure your router, don't forget to secure your computer too. Use the same basic computer security practices that you would for any computer connected to the internet. For example, use protections like antivirus, antispyware, and a firewall -- and keep these protections up-to-date.

Protect Your Network during Mobile Access

Apps now allow you to access your home network from a mobile device. Before you do, be sure that some security features are in place.

Use a strong password on any app that accesses your network. Log out of the app when you're not using it. That way, no one else can access the app if your phone is lost or stolen.

Password protect your phone or other mobile device. Even if your app has a strong password, it's best to protect your device with one, too.

\

Tips for Using Public Wi-Fi Networks

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but often they're not secure. If you connect to a Wi-Fi network, and send information through websites or mobile apps, it might be accessed by someone else.

To protect your information when using wireless hotspots, send information only to sites that are fully encrypted, and avoid using mobile apps that require personal or financial information.

How Encryption Works

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so it's not accessible to others. When you're using wireless networks, it's best to send personal information only if it's encrypted — either by an encrypted website or a secure Wi-Fi network. An encrypted website protects **only** the information you send **to and from that site**. A secure wireless network encrypts **all** the information you send using that network.

How to Tell If a Website is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server — a powerful computer that collects and delivers content. Many websites, like banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the start of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on **every** page you visit, not just when you sign in.

What About Mobile Apps?

Unlike websites, mobile apps don't have a visible indicator like **https**. Researchers have found that many mobile apps don't encrypt information

properly, so it’s a bad idea to use certain types of mobile apps on unsecured Wi-Fi. If you plan to use a mobile app to conduct sensitive transactions — like filing your taxes, shopping with a credit card, or accessing your bank account — use a secure wireless network or your phone’s data network (often referred to as 3G or 4G).
If you must use an unsecured wireless network for transactions, use the company’s mobile website — where you can check for the **https** at the start of the web address — rather than the company’s mobile app.

Don’t Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don’t** encrypt the information you send over the internet and **aren’t** secure. In fact, if a network doesn’t require a WPA or WPA2 password, it’s probably not secure.
If you use an unsecured network to log in to an unencrypted site — or a site that uses encryption only on the sign-in page — other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools — available for free online — make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people in your contact lists. In addition, a hacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

Protect Your Information When Using Public Wi-Fi

Here’s how you can protect your information when using Wi-Fi:

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you’re logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don’t stay permanently signed in to accounts. When you’ve finished using an account, log out.

- Do not use the same password on different websites. It could give someone who gains access to **one**of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn't automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can get a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees. What's more, VPN options are available for mobile devices; they can encrypt information you send through mobile apps.
- Some Wi-Fi networks use encryption: WEP and WPA are common, but they might not protect you against all hacking programs. WPA2 is the strongest.
- Installing browser add-ons or plug-ins can help. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites — look for **https** in the URL to know a site is secure.
- Take steps to secure your home wireless network.

Virtual Private Network (VPN) apps

You probably know by now that using your mobile device on the public Wi-Fi network of your local coffee shop or airport poses some risk. Public networks are not very secure – or, well, private – which makes it easy for others to intercept your data. So, what can you do to keep your mobile data private and secure while out and about? Some consumers have started using Virtual Private Network (VPN) apps to shield the information on their mobile devices from prying eyes on public networks. Before you download a VPN app, you should know that there are benefits and risks.

- VPN app basics
- Before you download a VPN app

VPN app basics

How do VPN apps work? When you use a VPN app, data sent from your phone – be it your browsing data or the apps you are using – is routed through servers located elsewhere. A VPN app can make traffic from your phone to a website you visit appear to come from a server operated by the VPN provider, rather than directly from your phone. Some VPN apps also encrypt the data sent between your phone and the VPN server. So, for example, say you are using a public Wi-Fi network that isn't secure – such as a network that allows anyone to use it, even if they don't have a password. Other people on the same network can see your traffic. But when you use a VPN app that encrypts the data, anyone monitoring your network connection only sees gibberish – even if the particular site you are visiting doesn't itself employ encryption.

Why would someone use a VPN app? VPN apps tout a variety of uses. Not only do some VPN apps promise to keep your information secure on public networks, but some also claim they will keep your information private from advertisers and other third parties. And because VPN apps route your traffic through another network, they can make it appear as if your traffic is coming from somewhere else. This is similar to how a company might use a VPN to allow employees to use their work computer as if they were on the company's network, even while they're on the road.

What are some privacy and data security concerns about using a VPN app? First, you should be aware that when you use a VPN app, you are giving the app permission to intercept all of your internet traffic. You don’t want to grant such permission lightly. Also, a group of technical researchers who studied almost 300 VPN apps found (link is external) potential privacy and security risks with some VPN apps. According to the study, for example, some VPN apps did not use encryption; some requested sensitive, and possibly unexpected, privileges; and some shared data with third parties for purposes such as injecting or serving ads, or analyzing the data to see how people are using a particular site or service. Given these findings and the considerable trust you must place in a VPN app with your traffic, here are some things to consider before you download a VPN app.

Before you download a VPN app

- **Research the VPN app before you use it.** You are trusting a VPN with potentially all of your traffic. Before you download a VPN app, learn as much about the app as you can. Look up outside reviews from sources you respect. You can also look at screenshots, the app’s description, its content rating, and user reviews, and can do some online research on the developer. The fact that an app promises security or privacy does not necessarily make it trustworthy.
- **Carefully review the permissions the app requests.** Apps will present the permissions they request on their app store page, during installation, or at the time they use the permission. It’s useful information that tells you what types of information the app will access on your device in addition to your internet traffic. If an app requests particularly sensitive permissions (reading text messages, for example), consider whether the permission makes sense given the app’s purpose and whether you trust the app developer with that access.
- **Know that not all VPN apps actually encrypt your information.** Some VPN apps use protocols that do not encrypt your traffic, or encrypt only some of your traffic. Outside reviews from sources you respect might provide more information about a particular app’s use of encryption.
- **A VPN app generally isn’t going to make you entirely anonymous.** Instead, the app will typically obscure the content of your traffic from your internet service provider or public Wi-Fi provider, shifting trust from those networks to the VPN app provider.

In addition, sites you visit may be able to determine that you are using a VPN app, and can still use any identifying information you directly share with them (for example, filling out a form with your email address) to track you.

- **VPN apps may share your information with third parties.** Many VPN apps are free because they sell advertising within the app, or because they share your information with (or redirect your traffic through) third parties. If you are using the VPN app to keep your traffic private, make sure you review the VPN app’s terms and conditions and its privacy policy to determine if it shares information with third parties such as advertisers, and if so, what information it shares.