Bank of Botetourt

August 2022

Yup, Hackers Can Attack Your Home Wi-Fi Network. Here's How to Protect It

The average US home now has more than 10 devices connected to the home Wi-Fi network. From laptops and tablets to phones, smartwatches and streaming devices, things add up quickly. And with so much data stored on those devices -- credit card numbers, bank records, login credentials and other personal and private information -- you want to make sure you're protecting yourself from hackers if your network is ever compromised.

Home network hacking does happen all too frequently. Internet crime cost people more than $6.9 billion in 2021, and while phishing and scams contributed to the losses, personal data breaches were also a significant factor. A secure home network will help reduce the risk of getting hacked and someone accessing your sensitive information. Not only that, it will keep away any unwanted or unauthorized users and devices that would slow down your connection or freeload on the internet service you pay for.

It's fairly simple to create and maintain a secure home Wi-Fi network. Below, you'll find 10 tips for securing your network. Some are more effective than others at keeping hackers and freeloaders at bay, but all are useful in their own way. Keep in mind that nothing can guarantee absolute security from hacking attempts, but these tips will definitely make it harder for anyone to compromise your network and data.

Place your router in a central location
Strong network security starts with a smart setup. If possible, place your router at the center of your home. Routers send wireless signals in all directions, so strategically placing your router in a central location will help keep your connection to the confines of your home. As a bonus, it will likely also make for the best connection quality.

Create a strong Wi-Fi password and change it often
This should go without saying, but I'm going to cover it still to emphasize its importance. Creating a unique password for your Wi-Fi network is essential to maintaining a secure connection. Avoid easily guessed passwords or phrases, such as someone's name, birthdays, phone numbers or other common information. While simple Wi-Fi passwords make them easy to remember, they also make it easy for others to figure them out. (Here's how to access your router settings to update your Wi-Fi password.)

Be sure to change your password every six months or so, or any time you think your network security may have been compromised.

Change the default router login credentials
Along the same lines of password-protecting your Wi-Fi network, you'll also want to keep anyone from being able to directly access your router settings. To do so, go ahead and change the admin name and password

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt
(540) 591-5000

for your router. You can log in to your router settings by typing its IP address into the URL bar, but most routers and providers have an app that lets you access the same settings and information.

Your router login credentials are separate from your Wi-Fi network name and password. If you aren't sure what the default is, you should be able to find it on the bottom of the router. Or, if it's been changed from the default somewhere along the way, again, here's how to access your router settings to update the username and password.

Turn on the firewall and Wi-Fi encryption
Most routers have a firewall to prevent outside hacking, as well as Wi-Fi encryption to keep anyone from eavesdropping on the data that's sent back and forth between your router and connected devices. Both are typically active by default, but you'll want to check to make sure they're on.
Now that you know how to log in to your router settings, check to make sure the firewall and Wi-Fi encryption are enabled. If they're off for whatever reason, go ahead and turn them on. Your network security will thank you.

Create a guest Wi-Fi network
"Can I get the Wi-Fi password?" is undoubtedly something all hosts have heard. Before sharing access to your main home network, consider creating a separate guest network for visitors. I'm not suggesting your guests are going to attempt anything nefarious with your main Wi-Fi connection, but their devices or anything they download while connected to your network could be infected with malware or viruses that target your network without them even knowing it.

A guest network is also ideal for your IoT devices, such as Wi-Fi cameras, thermostats and smart speakers -- devices that may not hold a lot of sensitive information and are perhaps more easily hackable than a smarter device such as a computer or phone.

Use a VPN
There are a few reasons to use a good VPN, and network security is definitely one of them. Among other things, a virtual private network hides your IP address and Wi-Fi activity, including browsing data.

VPNs are probably more useful when connected to a public network, but they can still add a level of security and privacy to your home network. Some VPNs are better than others, but like anything, you often get what you pay for. Free VPN services are available, but paying a little extra (seriously, just a few bucks per month) will deliver a much better, more secure service.

Keep your router and devices up to date
Software updates always seem to pop up when you need to get online most. While they can be annoying, there is a purpose to them and it often includes security updates. When companies become aware of potential or exposed security vulnerabilities, they release updates and patches to minimize or eliminate the risk. You want to download those.

Keeping your router and connected devices current on the latest updates will help ensure you have the best protection against known malware and hacking attempts. Set your router to automatically update in the admin settings, if possible, and periodically check to make sure your router is up to date.

Disable remote router access
Remote router access allows anyone not directly connected to your Wi-Fi network to access the router settings. Unless there's a need to access your router while away from home, to check or change the configuration of a child's connected device, for example, there should be no reason to have remote access enabled.

You can disable remote access under the router's admin settings. Unlike other security measures, disabled remote router access may not be the default.

Verify connected devices
Frequently inspect the devices that are connected to your network and verify that you know what they are. If anything on there looks suspicious, disconnect it and change your Wi-Fi password. You'll have to reconnect all your previously connected devices after changing your password, but any users or devices that are not authorized to use your network will get the boot.

Some devices, especially obscure IoT ones, may have some odd default names of random numbers and letters that you don't immediately recognize. If you come across something like that when scrutinizing your connected devices, go ahead and disconnect it. Later on, when you can't start your robot vacuum cleaner from your phone, you'll know that's what it was.

Upgrade to a WPA3 router
WPA3 is the latest security protocol for routers. All new routers should come equipped with WPA3, so if you buy a new router, you should have nothing to worry about there. However, many people rent their routers directly from the provider, which may not include the most up-to-date equipment.

If your router was made before 2018 it's possible that you have a WPA2 device, which lacks the same level of security protocols as newer, WPA3 devices. A quick search of your device's model should tell you when it came out and any specific features such as whether it has WPA2 or WPA3. If you've got a router with WPA2, call your provider and negotiate for a better, more recent router.

Network security is not a guarantee
Again, even with the most recent and effective methods of protecting your home network, security is never going to be 100% certain. As long as there is the internet, hackers and cybercriminals will find ways to exploit it. But with the tips above, hopefully you can better keep your network secure from anyone trying to use your connection or access your data.

Source: CNET, David Anders, July 1, 2022 7:46 a.m. PT, First published on June 10, 2022 at 1:56 p.m. PT.

How to Stop Oversharing on Social Media

Social media is a crucial part of many people's lives, but oversharing online has significant consequences.

From sharing your birthday celebration pictures on social media to posting every single thing that happened that year, you might be oversharing on social media without even realizing it.

While there's nothing wrong with sharing big achievements with your friends, too much information can invite unwelcome attention. Moreover, there's something to be said about a private life being a happy life.

So, what is oversharing on social media—and why do many people do it? Most importantly, how can you stop this issue from ruining your life? Let's find out.

Why Oversharing Online Can Be Damaging

If you share a picture, a video, thoughts, or opinions every few hours, the chances are you don't really care much about the content of that post. However, it may result in unhealthy outcomes in the long run.

Let's understand it this way. Everything you share online stays there forever. Even if you delete it, someone must have seen it, who can take a screenshot or simply talk about it to others.

These things may result in judgmental behavior, a recruiter holding up to contact you, or someone exploiting and taking advantage of the information you share about the minors in your family.

How to Tell When Your Sharing Has Become Oversharing

Several signs could point to you oversharing. Below, you'll find some of the most common things to look out for.

- You post pictures or videos every second hour without analyzing them.
- You share your intimate moments with loved ones, even though it's healthier to live in the moment with them and put the camera away.
- You treat social media as your online diary and share every moment of your day.
- You order food or shop just to get to post their pictures online.
- Your mood and feeling of self-worth have started to rely on the number of likes and comments.

How Can You Stop Oversharing on Social Media?

1. Avoid Posting When You're Angry
When you angrily post online, you could face significant consequences. An aggressive or offensive tweet might get you fired, and you might begin to lose real-life friends if you regularly post vulgar content because you're unhappy.

2. Choose Your Content Wisely
Whether you post once a month or daily, scrutinize your content before you share it with the world. Make sure the background of your pictures and videos doesn't reveal any private information.

You should also keep in mind to never share your routine or places you visit regularly on specific occasions. Moreover, you should never share your current location or check-ins when you're still there.

When you post pictures of your or someone else's kids, make sure that people can't get information you might not want them to know. If you show the logo of the school they go to or name the park where they play every evening, others with malicious intentions might take advantage.

3. Think Ahead of Time
Ask yourself when you post: can it affect me in the future in any way? This is one of the easiest ways to determine whether you should publish this picture or video or not. If the answer is yes, and the consequences are potentially large, it's better to refrain from sharing.

4. Separate Your Personal and Professional Audiences
Something that's okay to share with your family and friends might be oversharing with your colleagues and professional network. So, create separate groups of people or keep different professional and personal profiles altogether. It allows you to share appropriate stuff that's suitable for each of your viewers.

5. Avoid Sharing Everything on Your Online Journal
Before you try to document your life online on Facebook, Instagram, Twitter, or any other social platform, take a moment to think about what to share.

6. Keep Track of Your Social Media Usage
The less time you'll spend on these platforms, the less itch you'll have to contribute to it. Apps like Social Fever can help you keep track of the time you spend on these websites, and you can take action from there accordingly.

Oversharing on Social Media Is Never Good
Social media platforms are a great way to express yourself, but that doesn't mean it cannot get dangerous. So, it's important to understand your boundaries and know when to stop. You must keep a balance between what you let people in on and what you keep to yourself.

Source: MUO, Sadaf Tanzeem, January 6, 2022