Can Smart Home Tech Be Remotely Hacked?

How many smart devices do you have in your home? According to research published in 2021, the average American household contains 25 intelligent items, including laptops, smartphones and other mobile tech. That is a significant jump from 2019, where the average home only had 11 smart devices.

These connected devices make our lives easier and more convenient. We can turn the lights on or off, adjust the thermostat, close the garage door or preheat the oven, all from smartphones.

However, another problem begins to emerge as we install more smart devices in our homes: cybersecurity. Each piece of smart technology relies on a wireless internet connection, and that comes with risks. Can smart home tech be remotely hacked? Is there a way to make these items safer from cybercriminals?

Types of Smart Home Tech

The term smart home is a blanket that includes any device networked with Wi-Fi and designed to make the homeowner’s life easier. Here are some of the most common ones and what they can do for you.

1. Virtual Assistants

Virtual assistants are the first thing most people think of when talking about smart homes. These devices tend to serve as a hub for the rest of the smart devices in the house, whether you have Alexa, Google, Siri or some home-brew assistant. You can access or control the rest of your smart home with something as simple as a voice command.

2. Thermostats

Traditional thermostats require manual control, while smart ones allow you to change your home’s temperature remotely. Bumping that temperature up when you’re not home during the day can save you up to 10% on your energy bills annually.

3. Garage Door Openers

Have you ever had to turn around and drive back home because you forgot to close the garage door – or worried that you had? Smart garage door openers allow you to be sure it’s closed or open it remotely if you need to let someone into your home when you’re away.

4. Appliances

Ovens, refrigerators, washing machines, coffee makers – if you can think of it, someone has probably added them to the Internet of Things. These devices are designed to make your life easier, but you’re also adding one more thing to your network. Ensure you’re making an informed decision about purchasing smart appliances.

5. Lightbulbs

LED lightbulbs are already replacing incandescent bulbs, offering a more energy-efficient alternative. Smart bulbs are the next step. You can control all the lights in your home from your smartphone or connect them to your virtual assistant and let Alexa or Siri control the lighting.

6. Power Strips and Plugs

We use so much electricity in our daily lives that it’s easy to take it for granted – at least until the electric bill comes in. Smart power strips and plugs in the wall make it easier to monitor your usage. Some even allow you to cut off power to appliances that might be draining too much electricity when they aren't in use. These power ghosts can drive up your utility bills.

7. Mattresses

Even mattresses come equipped with IoT sensors these days. Smart versions can help you sleep better by automatically regulating everything from temperature to firmness. Some even have massage or speaker features so you can listen to your favorite tracks and get a rubdown while you drift off to sleep.

DARKEST DAYS
HOW TO SURVIVE AN EMP ATTACK TO THE GRID
CLICK HERE
To get your copy of
Darkest Days and find out how
to survive when the lights go out!

Can Smart Home Tech Be Remotely Hacked?

With so much smart technology appearing in the average home, it's time to address the elephant in the room. Can this tech be remotely hacked?

The short answer is yes. In most cases, hackers aren't going to take control of your smart home to mess with your thermostat or flicker the lights when you're trying to sleep unless they're bored or testing the limits of their control. Instead, they work to access your network to utilize each device's processing power. They can then add those devices to a botnet, which they can use for concerted attacks on other networks. Your smart home tech becomes a zombie slave, part of a horde that cybercriminals can direct at will.

Do you remember when internet services stopped working on most of the internet for users in the United States and Europe in 2016? That was due to the Mirai Dyn botnet attack, one of the most significant hacks in recent memory. Information collected afterward defined millions of unique IP addresses involved in the attack. Each one was connected to a piece of hacked smart home tech.

Some devices, such as your virtual assistants, could be a lucrative target for hackers. Breaking into them could provide access to your Amazon or Google account, where criminals can steal other personal information such as email addresses or credit card numbers.

Off-brand tech is even more vulnerable to these hacks than the devices you might buy from Google, Apple or Amazon. These retail giants might have a bad reputation for what they do with the data they collect from users. Still, their software is some of the best in the industry – and it’s constantly updated when IT professionals or civilian bug reporters find a problem.

Off-brand smart tech software is often riddled with holes and backdoors, making it simple for savvy hackers to control even if you take steps to protect your network.

Protecting Your Smart Home Tech

Now you know it’s possible to hack smart home tech remotely. What steps can you take to protect yourself and your network from becoming part of the next botnet attack?

1. Secure Your Network

Start by securing your Wi-Fi network. Change the default password that came with the device, as well as the password that allows you to access the router directly. You might find that the username and password to get into the router are “admin” if you received your device from your internet service provider. Leaving these default passwords alone is like issuing an open invitation to hack your network.

Consider setting up a MAC address filter for your router for an additional layer of security. Each Wi-Fi-enabled device will have a unique one. Adding a MAC filter to your router means unauthorized users won’t be able to connect, even with the password.

2. Manage Your Account Passwords

Your Wi-Fi password isn’t the only piece of information you need to protect when it comes to keeping hackers out of your smart home network. Most devices require setting up an account with its associated companion app. Someone who gets your password will have access to your smart devices with no hacking required.

Don’t use the same password for everything. Instead, consider using a random generator to create a strong, unique password for each account. Use a password manager to help you securely track them all.

3. Change Default Device Passwords

Many smart home devices come equipped with default passwords. These can be handy when setting up your network, but they should be changed as soon as that’s finished. Some may be randomly generated, but manufacturers may use a list of default or admin passwords that enable them to access the device remotely if necessary. Every item they’ve ever sold could be vulnerable if these are leaked.

Change your default passwords. Use the same secure generator to create a new and unique one for each device.

4. Add Two-Factor Authentication

Provide an extra layer of security by adding two-factor authentication to your account. That makes it more difficult for hackers to find their way in. Authenticators generate a single-use code that is necessary to sign in. Hackers that manage to figure out your username and password won’t be able to get in without the authenticator linked to your account.

5. Don’t Access Your Network With Unsecured Wi-Fi

Public Wi-Fi is excellent in a pinch if you need to pull up a Google search or find directions, but it’s not secure. A savvy hacker could watch your every move if you access your home network via a public hotspot. Use your secure hotspot if you can’t avoid accessing your network while you’re away from home.

If connecting to public wireless networks is unavoidable, utilizing a virtual private network (VPN) can give you an extra layer of security. That will make it impossible for hackers to follow in your virtual footsteps.

Don’t Let This Discourage You

The idea of someone hacking your smart home tech is almost enough to scare us back to the Stone Age but don’t let it discourage you. There are so many benefits to installing smart home tech that they outweigh the risks. The key isn’t to keep smart tech out of your house – it’s to secure your network so trying to hack in isn’t worth the effort.

Protecting your home network from hackers is often as simple as changing the default passwords that come with your devices and keeping your system secure. Don’t use the same password for everything, and you should be golden. Hackers trying to create a botnet with smart home devices aren’t looking for a challenge. They’re looking for an easy way in. Deny them that and you’re safe as houses.