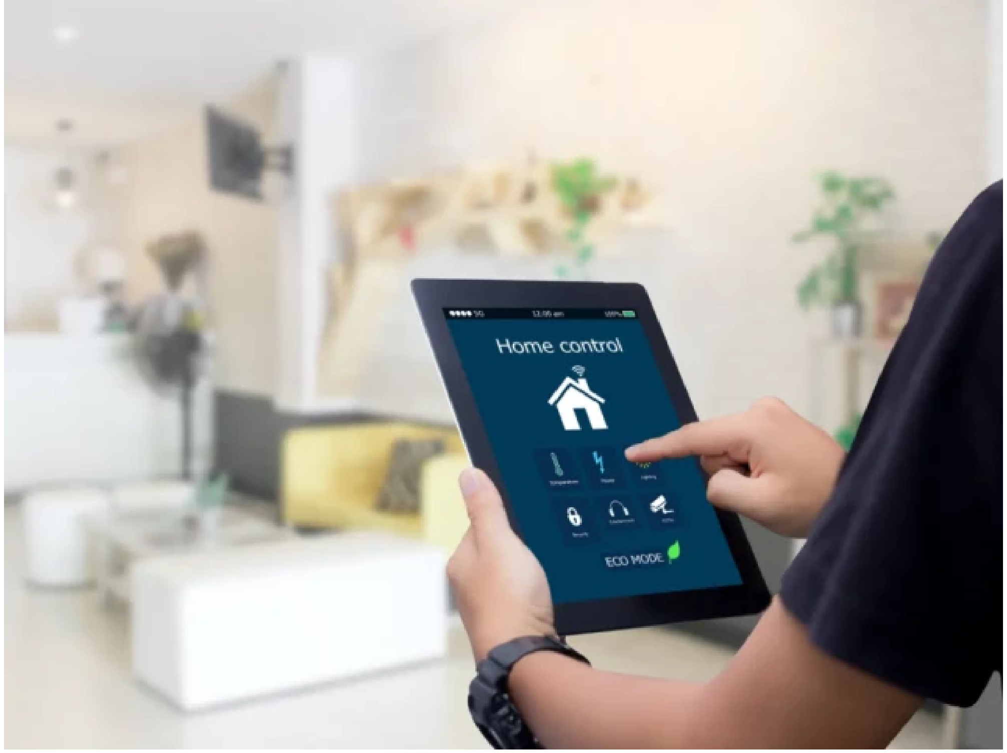
7 Essential Smart Home Security Tips For Securing Your Smart Home

Updated on 3rd Nov 2021 12:08 in General, IoT, Smart

Without a doubt, having a connected home not only simplifies your life but also makes it more efficient. Thanks to advancements in technology, homeowners can use IoT (Internet of Things) to turn an ordinary house into a smart home. As of November 2020, there are more than 48 million smart homes in the U.S., with millions of others in other parts of the world. These numbers can only grow as more people adopt smart living, with an estimate of more than 77 million smart homes in the U.S. by 2025.



The exponential growth of the number of smart homes comes with security concerns, especially cybersecurity risks. There has been an increasing concern over the security of a smart home, with cases of identity theft, digital privacy, and data breaches on the rise. Smart homes make use of smart devices connected through the internet. These can include kitchen appliances, entertainment, household appliances, personal gadgets, light bulbs, and home security systems. With these devices, you can automatically turn lights on and off without being home, open or close doors, and even schedule alerts for reminders.

While smart home devices deliver a sense of comfort and security, is it possible to use them risk-free? Here is everything you need to know about securing your smart home and smart devices.

Smart home device security risks

Exploitation of passwords

While millions of people may own intelligent homes, only a tiny fraction of these owners take password protection seriously. More often than not, people use weak passwords for their smart home hub, which connects all the smart devices in the home.

This security lapse makes it easy for a hacker to gain access to all the devices in your home if they hack into the smart home hub. Once hacked, the attacker can take control of all the devices in your home, using this opportunity to wreak havoc in your home.

Tracking

While most people trust their smart home devices to keep their information secure, a simple hack can give hackers access to your location information down to the street name and house number. This is usually done through phishing attempts where a hacker sends a malicious link to a user on the smart home network. Clicking on the malicious link compromises the entire smart home network.

Home intrusion

Hackers can exploit security devices like surveillance cameras and smart door locks to gain access to your home. Most hackers take advantage of security loopholes like the lack of data encryption for smart doorbells, making them an easy target.

Suppose there are security loopholes in your security devices. In that case, hackers can exploit this vulnerability to disable cameras, unlock your doors and burglarize your home, or even lock you out of your own home.

Using unsecured IoT devices

Sometimes, smart home devices are rushed to the market by companies trying to remain relevant without ensuring security concerns about the device have been addressed. Unfortunately, using a smart device with security vulnerabilities from the manufacturer opens your home network to many security issues, including hacking and malware deployment. In most cases, cheap devices are also the ones that have the highest risk of having security issues out of the box. This is because security testing adds to the cost of the device and, as such, is usually lackluster or straight up non-existent.

Distributed Denial of Service (DDoS) and Permanent denial of Service (PDoS)

A DDoS attack is used to render a network of machine resources unavailable to the user by disrupting service to the internet temporarily or indefinitely. DDoS attacks are on the rise in smart homes because of the lack of proper security protocols for IoT devices.

Also referred to as phlashing, a PDoS attack is a type of cyberattack that causes damage to a device, sometimes beyond the point of repair, forcing the owner to replace the device or reinstall hardware. For example, BrickerBot is a common PDoS attack used to exploit IoT home devices with weak security passwords.

How to secure smart home devices

The best way to secure your smart home is to secure your smart devices. In many cases, they are directly responsible for the security of your home, such as the case with a smart lock or smart alarm system. You can imagine that all your security will be pretty useless if an attacker manages to get into your network!

Reinforce your Wi-Fi password security

Using a secure password for your Wi-Fi is the most basic form of internet security. If you use a weak password for your Wi-Fi network, you should consider changing it to something harder to crack. The best password should be at least eight characters long with numbers, letters, and special symbols. Having a strong Wi-Fi password will ensure every device connected to the Wi-Fi network is protected. There are, unfortunately, still ways for your network to be hacked, as discussed here. As such, it's essential to keep in mind that the security provided by Wi-Fi is limited.

Keep your IoT devices software updated

Whenever a smart device software manufacturer notices a flaw in the software, they develop a security patch to counter the vulnerability. This patch is made available in the form of a software update sent out to device owners to install. Failing to update the device with the latest software opens it up to possible attacks by hackers taking advantage of the security flaw.

To ensure your devices are always updated, you can set them to automatically install updates whenever they are available. However, consider manual software updates for smart devices critical to your home security like doorbells, security locks, and cameras.

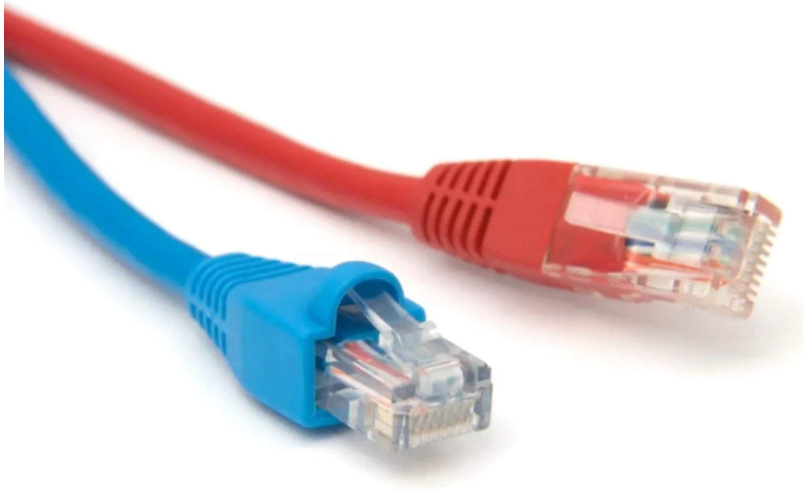
Securing your router

Even as you improve your Wi-Fi password, the router is a critical access point you need to protect. When your router is not secured, it is still possible for a hacker to access your network.

To ensure your router is protected, you need to change the username and password from the default to something more secure. When securing your router, you should also use WPA2 encryption.

An additional benefit of securing your router is the convenience of improving security for all connected devices. According to ExpressVPN, your smart devices will benefit from an added layer of protection by installing a VPN for your router.

Host your IoT devices on a separate network



Most modern routers allow the user to create guest networks. You should use this feature to create a separate network for your IoT devices. This ensures you can pump the security on the guest network while ensuring the security of your primary network in case of a hack. It's also good practice to only hand out the credentials to your guest network whenever a friend comes over, as this protects you from any malware they may have and them from anything on your network.

Your personal devices can connect to the main network while the guest network is set up for smart home devices. This is so important because anything connected to your network can see all data going by. As a result, you want to keep devices that use your network for less sensitive data away from the ones that have your personal information.

Disable unused features

The beauty of owning smart home devices is the ability to control them from anywhere. While this is convenient, it also presents an easy to exploit entry option for hackers. As a rule of thumb, always disable unused IoT features to minimize possible access points for hackers. These include unused Bluetooth connections, unrequired remote access, and voice control. Even if the potential exploit sounds impossible to pull off, it is still good practice to disable them. Just think, no one can exploit a feature if you don't even have it enabled.

Bottom line

When you have smart home devices, the key to ensuring protection is by taking the security of your home into your hands. Implementing the security options in this post will go a long way in protecting your IoT devices and home from cybersecurity threats that could happen to anyone. Remember, it only takes one rogue device or unprotected entry-point to cause many problems for your smart home. With great power comes great responsibility, and this holds true for the luxury of advanced home control via voice, remote location, and automation. Don't even risk letting this great power fall into the hands of a bad actor; harden your security before you need it.

Other Posts

11 Awesome Smart Home Features That You Want in Your Home

The 15 (Hidden) Hazards of Smart Home DIY You Need to Know