Learn how to take care of your smart home devices

Assign a name to your router.

Please don't use the name provided by the manufacturer; it could be used to identify the manufacturer or model. Give it an odd name that has nothing to do with you or your location. You must ensure that your identifier does not appear in the router name.

For wireless LAN, use a robust encryption mechanism.

We recommend using a strong encryption mechanism such as WPA2 in your router settings when setting up Wi-Fi network access. This keeps your network and communications secure.

Set up the guest network.

Make your Wi-Fi account password-protected. Visitors, friends, and family can log in to another network not connected to your **smart home devices**.

Replace the already provided username and password to something completely different.

Many Smart home devices come with a default password that may be known to cybercriminals. This gives you easy access to your Smart home devices and, in some cases, the data they contain. Are you thinking of buying a device that can't change the default password? Next, consider another possibility.

Use strong and unique passwords for Wi-Fi networks and device accounts.

Avoid using easy-to-guess phrases and passwords such as "password" and "123456". Instead, use letters, numbers, and symbols to create unique and complex passwords. It would help if you also considered using a password manager to improve security.

Double-check your device's settings.

Smart home devices may have privacy and security settings that are configured by default. You should change some default settings because they benefit the manufacturer more than you.

Turn off features you don't use.

A range of services, such as remote access, are commonly enabled by default on smart home devices. Make sure it's turned off if you don't need it.

Ensure that your software is up to date.

Please install any software updates that your smartphone maker offers you. This may be a fix for a security flaw. Mobile security is crucial because you can use your mobile device to connect to your smart home. The manufacturer of the IoT device may have also given updates. Alternatively, you may need to visit your website to see whether any changes have been made. Make sure to download and install the update on your device for added protection.

Look for existing Smart home devices on your home network.

It may be time to replace your aging security camera. Take a look at the new model to determine if it provides more security.

Complete the two authentication steps.

Malicious individuals can be kept out of your account with two-factor authentication (such as a one-time code delivered to your phone). Use two-factor authentication (or 2FA) if your smart device app supports it.

Stay away from public Wi-Fi networks.

Perhaps you want to manage your smart home equipment from a coffee using your mobile smartphone. Use a VPN if you're utilizing public Wi-Fi (which isn't always a good idea).

Beware of obstacles.

Make sure that a hardware failure does not cause a dangerous state of the device.
Undoubtedly, more Smart home devices are emerging and looking for a place in your home. Suppose they make your life more convenient-and happier-great. But don't forget to protect your smart homes and Smart home devices more and more.