A Consumer Action Guide

# ‘Smart’ Homes

## Data privacy and security for your connected home

Home automation is changing the way we live, and the devices that make a “smart home” smart are becoming more commonplace, less expensive and easier to use. The “Internet of Things” (IoT) has brought us internet connectivity embedded in everyday objects that can talk to each other (and to you) through your home network. Many of us welcome the convenience and life enhancements offered by IoT devices but don’t understand fully how to protect our privacy and personal data when using them.

This guide will explain how smart homes work, what to be aware of when introducing smart devices to your home, what steps you can take to protect your data and your privacy, and where to learn more.

### What smart homes can do

A smart—or “connected”—home environment monitors, controls or automates household functions through devices connected to the internet and, in many cases, to each other. There are all sorts of things a smart home can do, including things like dimming the lights by voice command, setting the window blinds to open in the morning, starting the coffee maker just before you get out of bed, and watching a delivery being made to your home while you are away.

The types of things a smart home can do can be divided into three general categories:

**1) Monitor:** the ability to view the status of the home and its systems. Examples of monitoring include viewing or listening to activity (live or recorded), checking the temperature and making sure the door is locked.

**2) Control:** the ability to change the status of the home's systems. Examples of controlling include turning the thermostat up or down from afar or unlocking the door for a visitor.

**3) Automate:** the ability to program the home's systems to change automatically. An example of automation is setting the lights to go on and the heat to go up at the time you expect to get home from work.

## How smart homes work

Smart homes function by connecting on/off devices (electronics that can be switched on and off) to the internet and, in many cases, to each other. While this can be done with wires, it's most commonly done via your home's Wi-Fi network. Communication can go in all directions—from you to your smart devices, from the devices to you, and between devices.

The data being exchanged is stored in "the cloud"—a global network of servers—rather than on your computer's hard drive, in your smartphone's memory or on a personal server. Data stored in the cloud is accessible via the internet at any time and from any place you log in.

## Components of a smart home

Knowing what equipment and technology is needed to make a home smart highlights the many places in the network where your privacy and data need to be protected.

**Wi-Fi:** Wireless high-speed internet is essential because it allows devices throughout your home to communicate without direct cable connections. A Wi-Fi router attached to your internet modem (the device that brings internet service into your home) broadcasts the internet signal to all rooms.

**Smart devices:** There's a "smart" device for almost any function you can think of, including smart locks, doorbells, cameras, plugs (to give regular things, like a standard coffeemaker, smart functionality), lightbulbs, window shades, thermostats, appliances, speakers, televisions, smoke/carbon monoxide detectors, irrigation systems and water sensors.

**Hub:** A smart home hub is a device that helps all your devices talk to each other and to you, and it allows you to control all of them from a single app (software). However, a hub is not always essential; if your devices are compatible with each other (use the same communication "protocol"), and you don't mind controlling them from separate apps, you could forgo this component. (Learn more in PCMag's "What Is a Smart Home Hub (And Do You Need One?)": *https://www.pcmag.com/news/what-is-a-smart-home-hub-and-do-you-need-one*.)

**Apps:** Each device has an app (downloadable software) that enables you to control it from a smartphone, tablet or, in some cases, computer. If you use a hub, you can generally control everything through one app. Otherwise, you would use a separate app for each device (or for a suite of related devices from the same manufacturer).

**Smart speaker:** While not essential, a smart speaker (for example, Google Home or Amazon Echo) is a popular option because it allows you to control your home by voice through a digital assistant (for example, "OK, Google, wake me up at 6 a.m." or "Alexa, dim the lights").

## Privacy and security

The Internet of Things enables you to streamline daily life, and even to make your home safer and more efficient. But anytime you're connected to the internet, be aware of the potential privacy and security issues and take precautions.

In a smart home, your personal privacy and security could be at risk if your network can be breached by an intruder. For example, if your Wi-Fi network is not secured by a firewall and strong (non-default) password, someone could join it uninvited, potentially gaining access to your devices, including cameras, locks, baby monitors, your digital assistant, and other devices that can hear you, watch you and control the functions of your home. An intruder who can control your smart home could cause all kinds of trouble, from unlocking the doors (or locking you out) to turning on all the lights and appliances and overloading your circuits.

Your data privacy and security could be compromised if you share your home's data with another entity, either intentionally (for example, with the utility company that installed the smart meter that tracks your electricity usage) or unintentionally (for example, by using a device or an app that monitors your activity and shares it with third parties). Once your data leaves your home, it can be exposed through a breach of the company that has collected it, accessed by dishonest employees, or otherwise used in unwelcome or harmful ways. Cybercriminals who can hack into your home devices want your data because it can be used in many ways, from identity theft to harassment. Even something as seemingly useless as your smart thermostat data could tell a potential burglar when nobody is home.

There have been cases where a breached IoT device has been used to send thousands of spam emails, or recruited as a malicious "botnet," used to carry out a serious cyberattack (https://www.iotforall.com/iot-ddos-attack/).

## Smart home 'best practices'

By following experts' recommendations for online safety, and taking advantage of the many tools and controls offered by devices and apps, it's possible to reduce the possibility of intruders accessing your smart home network.

**Secure your Wi-Fi network.** Protecting your wireless network is like locking your front door: It's the first line of defense against intruders. Make sure the encryption feature on your router is turned on and, if you have a choice, use the stronger WPA2 (or WPA3, if available) encryption instead of the older and weaker WEP (https://bit.ly/2K5qlu2).

Don't name your network(s) something revealing (such as your address or name). Ideally, set your Wi-Fi router so that your network name (technically, its SSID, or "service set identifier") is hidden (not visible in the list of nearby Wi-Fi networks). There's typically a way to do this under the router Settings—for example, by changing "Visibility Status" to "Invisible" or by selecting "Enable Hidden Wireless."

Create separate Wi-Fi networks—one for your computer and mobile devices and another one for your home automation—and use a different password for each. That way, if your IoT network is compromised, your computer and mobile

devices are still protected. (If your router allows more than two networks, set up a third for visitors, including contractors, so that they don't have access to your devices.) (Learn more about boosting router security from Consumer Reports [https://www.consumerreports.org/digital-security/ways-to-boost-router-security/] and Wired [https://www.wired.com/story/secure-your-wi-fi-router/]. Learn more about setting up separate Wi-Fi networks from PCMag [https://www.pcmag.com/how-to/10-ways-to-set-up-your-wi-fi-for-guests].)

**Password-protect your devices and apps.** Start by changing the default password on the router and your other IoT devices, since cybercriminals often already know the default passwords. And since your smartphone functions as the universal remote control for your connected home, be sure it requires a passcode, touch ID or facial recognition to start and "wake up." Make sure your passwords are strong (in other words, long and randomized). (Google [https://support.google.com/accounts/answer/32040?hl=en] and CNET [https://www.cnet.com/how-to/strong-passwords-9-rules-to-help-you-make-and-remember-your-login-credentials/] offer tips for creating and managing passwords.) Consider using a password manager so that you can use strong passwords and not worry about forgetting them. (If you use a password manager, take special care to choose a strong "master" password.)

**Choose devices that meet high security standards.** Make sure that the home automation and security devices you purchase and integrate meet secure transmission protocols, like Z-Wave or Zigbee. This is generally the case with most well-established brands, but might not be the case for cheaper or off-brand devices. As is often true, price shouldn't be your most important criteria. Check the packaging or the manufacturer's website to find out which protocol the device uses. Consider replacing older models with newer ones that offer stronger security. (Learn more about home automation protocols at https://www.safewise.com/blog/zigbee-vs-zwave-review/ and https://theiotpad.com/tips/home-automation-protocols.) When considering a particular device, "google" it to compare how it rates on a variety of reviewers' lists and to compare features, prices, pros and cons, etc. (See the "Learn more" section for websites that provide tech product reviews.)

**Update your firmware and software.** Firmware is the software that makes your devices (router, hub, etc.) work. There are different ways of updating firmware; you may have to access the device's Settings menu, a "native" app (installed directly on the device), or visit the manufacturer's Support page. (Get tips for updating router firmware: https://www.lifewire.com/how-to-upgrade-your-wireless-routers-firmware-2487671.) Software refers to the apps and programs that help you control your home automation. Updating regularly (manually, or by enabling auto-updates) will ensure that you have the latest security patches against vulnerabilities that have been discovered, and may even add entirely new security measures that make your IoT devices even safer. Replace devices that are no longer supported by the manufacturer; otherwise, security flaws will remain.

**Vet your apps.** Whether considering a device with its own (proprietary) app or shopping around for a third-party app, "google" the app's name to make sure users are satisfied with its functionality as well as the level of privacy and security it offers. To control what an app collects and shares, check the settings in the app itself (as opposed to the device settings) and adjust them to achieve the level of privacy that you want. If the app wants to collect more personal data than you are comfortable with and doesn't allow you to adjust the settings or opt out, don't download it. Only download apps from a reputable source (such as the Apple App Store or Google Play).

**Customize dashboards, tools and controls.** Take advantage of any opportunities offered on the device maker's website or in your apps to review and fine-tune your settings for optimal security and privacy. If two-factor authentication is an option (requiring a verification code or fingerprint in addition to username and password), consider using it. Review and understand the permissions you are giving the app when you download it; often, the default is to allow more of your data to be collected and shared.

**Require a PIN for purchases.** If you've entered

## ‘Smart TV’ security

Today’s televisions have built-in features that give them “smart” functionality, including cameras that enable facial recognition and microphones that enable voice control. Like other internet-connected devices, smart TVs can compromise your privacy and data security if you don’t take precautions.

For example, both the television manufacturer and the developers of video streaming and other apps on your TV gather information about you to do things like provide programming suggestions and to help marketers target their ads.

At the same time, a smart TV can sometimes provide a “back door” into your Wi-Fi network. This could allow a hacker to gain access to your computer and other network-connected devices (in addition to being able to control the TV and do things like watch and listen to you or play inappropriate video for your children). One way to protect your network is to connect your TV and other smart home devices to a separate (or “guest”) network on your Wi-Fi router so that an intruder wouldn’t have access to your primary network. (Learn more at *https://www.pcmag.com/how-to/10-ways-to-set-up-your-wi-fi-for-guests*, or check the manufacturer’s website for instructions for your router model.)

The FBI offers some security tips for smart TV owners (*https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdaysmart-tvs/*).

your bank or credit card account information so that you can shop by voice through Alexa or another digital assistant, consider requiring a PIN for purchases (you provide it after placing the order). This would make it less likely, or impossible, for your child or someone else to make unapproved purchases through your home automation system. If your digital assistant doesn’t have this feature, you could disable the voice order feature entirely.

**Mute the mic.** If you’re concerned about what the microphone on your smart speaker is picking up when you aren’t actively using it, you could disable it (by voice command or, on some devices, by pressing a button on the device). You can also delete interactions that have already been recorded. Consumer Reports provides instructions for Amazon Alexa, Apple Siri and Google Assistant: *https://www.consumerreports.org/privacy/smart-speaker-privacy-settings/*. (Learn more at Lifehacker.com [*https://lifehacker.com/how-to-protect-your-privacy-on-your-smart-home-devices-1823181500*] and on the Google Home Safety, Privacy and Security Tips page [*https://www.safety.com/google-home-safety/*].)

**Cover the camera.** To maintain your personal privacy, position your cameras so that they’re not aimed at someplace where you want complete privacy, like your bathroom. If you’re concerned about a camera spying on you, you could put a sticky note or piece of masking tape over it, or you could disable it entirely. Signs that your camera has been hacked include noises or voices coming from it, the LED light being on (which indicates that someone is accessing it remotely), or a change in its field of view (some cameras offer the ability to pan or tilt slightly).

**Avoid public Wi-Fi.** When using your smartphone or other device to connect to your home automation system from someplace else, avoid using public Wi-Fi—use your wireless data plan, a VPN (virtual private network: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html) or an encrypted mobile website instead.

## Learn more

Selecting smart home devices can be a challenge—so many options!—but making wise choices is crucial for your personal and data privacy and security. Reading product reviews and recommendations is a good way to learn what to look for and narrow your options. These five tech product review websites can help:

**Tom's Guide** (https://www.tomsguide.com/)

**CNET** (https://www.cnet.com/)

**Gadget Review** (https://www.gadgetreview.com/)

**PCMag** (https://www.pcmag.com)

**TechRadar** (https://www.techradar.com/)

**Consumer Reports**, a non-profit research and rating organization, offers articles about, and reviews of, smart home devices, which can help you choose the right products for your needs. There's a lot of general information that is free to access; product ratings may require a subscription. (https://www.consumerreports.org/smart-home/smart-home-tech-devices-guide/)

**Norton**, a developer of antivirus software and other cyber security tools, outlines the vulnerabilities of home automation and offers "12 tips to help secure your smart home and IoT devices." (https://us.norton.com/internetsecurity-iot-smart-home-security-core.html)

Get a rundown on the privacy issues inherent in smart home devices and tips for managing them in the *Guardian* article "How to stop your smart home spying on you." (https://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy)

## About Consumer Action

www.consumer-action.org

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

**Consumer advice and assistance:** Submit consumer complaints to: https://complaints.consumer-action.org/forms/english-form or 415-777-9635. (Spanish-language complaints can be submitted to: https://complaints.consumer-action.org/forms/spanish-form/.)

Our hotline accepts calls in Chinese, English and Spanish.

## About this guide

This guide was created with a grant from Google.