Smart Home

Why Hackers Target Smart Homes & 7 Tips to Protect Yours

Emily Ferron

Updated Aug 27, 2020

6 min read

Cybersecurity experts weigh in on why hackers would want to attack your smart home products, and what you can do to protect yours.

As of this year, there are approximately 44.7 million smart households in the U.S. alone. With the exponential growth of the smart home industry comes horror stories about hacked baby monitors and surveillance cameras and ever-increasing concerns about data breaches, digital privacy and identity theft. Smart home devices intend to provide a sense of security and comfort, but is it possible to use them without risks? We talked to the experts to better understand how to protect smart home products from hackers.

All of them, cybersecurity experts are quick to emphasize. You may have heard smart home devices collectively referred to as the "Internet of Things" (IoT). Remembering the "I" in IoT can help you understand its vulnerabilities.

"All of these smart devices are really networked computers in addition to what they traditionally are: refrigerators, light bulbs, televisions, cat litter boxes, dog feeders, cameras, garage door openers, door locks," explains Professor Ralph Russo, Director of Information Technology Programs at Tulane University. "Many of these continually collect data from embedded sensors. Malicious actors could gain access to your home network through your device if they can exploit an IoT device vulnerability."

In other words, connected appliances can be hacked into like any other website or computer, and most of them are behind poorly secured consumer-grade home routers. Dr. Zahid Anwar of Fontbonne University gave us an overview of which smart devices are most at risk and why.

- **Most vulnerable:** Outdoor devices with embedded computers that support little or no security protocols. For example, garage door openers, wireless doorbells and smart sprinklers are all examples of devices that may be easily accessible to someone driving down the street with a computer or other Wi-Fi transmitter.
- **Second most vulnerable:** "Inside-the-home devices that can be controlled through an app from a smartphone or PC such as smart bulbs, smart switches, security cameras, baby monitors, smart door locks, smart thermostats, and personal home assistants," says Dr. Anwar. "These devices rely on weak security tokens and may be hacked due to weaknesses in the communication protocols used, configuration settings or vulnerable entry-points left open by the vendor for maintenance."
- **Less likely to be attacked:** Home appliances like refrigerators and ovens are the least likely to be attacked, but it can happen.

Why would someone attack your refrigerator?

establishing a beach-head through an IoT device can be the low-hanging fruit."

Through the connected network, smart home devices give hackers much more information than the contents of your fridge. Once they have a way into your network, people with malicious intent might be able to turn off your security cameras, access your personal information or spy on you and your family. An insecure home network therefore opens the door to burglary, identity theft, privacy violations and more.

The exact rate of security breaches is unknown. Manufacturers don't disseminate this information and it doesn't fall under the purview of any one regulatory body. What we do know is that anecdotal evidence is mounting. The FBI warned parents about the risks of connected toys, an Internet-connected fish tank helped hackers steal data from a Las Vegas casino, and there are even free live streams of hacked security cameras broadcasting for free on the web and smartphone apps. We also know that there is no shortage of sophisticated scammers and identity thieves, and that they continually refine their methods alongside changing culture and technology.

It's also possible for IoT devices to be hacked and operating maliciously without you even knowing it. "The most common reason for taking over smart home devices is to use them to build a botnet network," explains Maciej Markiewicz, Security CoP Coordinator & Sr. Android Developer at Netguru, a digital consultancy and software company. "These devices can be easily used to conduct more complex attacks. Very often, the management of such botnet networks consisting of smart home devices are sold on the darknet to be used in crimes." These "botnets" are typically programmed to orchestrate the large-scale capture of personal data for identity theft and other financial exploitation.

Help Hackproof Your Devices: Smart Home Safety Tips

Many homeowners don't want to go through the hassle of advanced electronics configurations. Don't worry – we've compiled the easiest-to-follow tech tips that dramatically lower your smart devices' susceptibility to hackers.

"Unfortunately, it is always worth remembering that there is no IT infrastructure that can be 100% secured. The only thing we can do is seek to reduce the risk. Therefore, when designing a smart home system, it is worth analyzing what is important to us and what the risk is," says Markiewicz.

Before you add to your home network, ask yourself: Is the convenience this device offers worth the potential risk of a hack? If not, don't buy one. Research every device and brand you buy.

Create a secure Wi-Fi network.

Purchase a router from a reputable brand and follow the manufacturer's instructions to change the name of the network and default password. Choose a network name that doesn't automatically give away your location or personal details. Consider also hiding your network from view, an option which can usually be found in the router's settings menu.

It's also possible to create a second Wi-Fi network specifically for your smart home devices. Many routers allow you to create multiple networks, each with their own name and password. This way, hacking your IoT device will confine an attacker to that network and keeping it segregated from where you do your banking and store your sensitive information. It's also a good idea to set up a Guest network for visitors' smartphones and computers, where they can't see or access your IoT devices.

Don't underestimate the importance of your passwords.

It's incredible that the humble, old-fashioned password system is the main line of defense protecting our most high-tech devices. Take your passwords seriously! Whenever you get a new device, change the default password immediately. Otherwise, the password to your Wi-Fi router or security camera might be just a Google search away. Use unique, hard to guess passwords with several characters, numbers and letters on all of your devices. A

Register every new device with the manufacturer and keep them up to date.

Registration is important because companies frequently push out software updates that address newfound bugs and security concerns. If a vulnerability has been discovered, you'll need the company's software updates to patch it up. Also, when you install the associated apps, be cognizant of what permissions you're granting. Don't allow access to anything that isn't necessary.

Consider professional installation.

If the previous tips are making your head spin, remember that the leading home security providers offer professional installation with great built-in smart home integration. Technicians can handle any necessary hardwiring for you and answer all of your questions about more advanced security measures.

Unplug devices that aren't in use.

When you leave town, unplug any appliances that won't be active. Not only will it save on your energy bill, it will also make them inaccessible to hackers. You'll probably want to leave important appliances like the security camera, video doorbell and the thermostat on, but you can unplug extra smart speakers, vacuums, etc.

Factory reset devices before getting rid of them.

If you decide to sell, throw out or give away one of your smart electronics, follow the manufacturer's instructions to remove all of your data. Otherwise, the next person who gets their hands on it may automatically access all of your information or communicate with other devices on your network.

Written by your home security expert

Emily Ferron

Emily is an experienced writer passionate about covering topics at the intersection of tech, health, safety and humanity.

Like what you've read?
Share it with your friends

Related Content

Smart Home

Best Smart Home Devices For Saving Money &...

Smart Home

Best Smart Light Bulbs

Smart Home

The Best Smart Thermostats

10 Quick Tips for Amazon Echo Safety &... 5 min

New Alexa Guard Feature 2 min

Connected Home: Linking Your Smart Home Devices to... 3 min

Home Automation Buying Guide 4 min

#StaySafe

Secure what matters most.

At Safety.com your privacy is very important to us. Accordingly, we have developed this policy in order for you to understand how we collect, use, communicate and disclose and make use of personal information. The following outlines our privacy policy