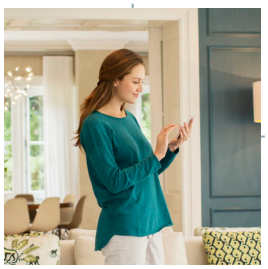
The smart consumer's guide

to home cybersecurity

EVERYTHING AS A GRID



Powering Business Worldwide

Simple, intuitive solutions
for home automation, connectivity and energy management.

Summary

While advancements in smart home technology are being widely lauded for making our lives easier and more convenient, the proliferation of Internet of Things (IoT) devices has simultaneously rolled out a welcome mat for a new era of hackers. Lured by potential entryways within smart home devices, hackers are increasingly targeting this equipment as the weak point within a home network. In fact, experts reveal that 98 percent of all IoT device traffic is unencrypted, exposing personal and confidential data on the network. Meanwhile, 57 percent of IoT devices are vulnerable to medium- or high-severity attacks ranging from device hijacking to distributed denial of service (DDoS) attacks.

Indeed, there has been no shortage of headline-grabbing hacking occurrences in recent years. From horrified parents who discovered intruders communicating with their young children via a compromised baby monitor to attackers gaining access to smart home hubs and listening in on private conversations, these — and numerous other incidents — underscore the need for proper cyber protection within every smart home.

The good news is, when it comes to safeguarding your smart devices, a little diligence goes a long way. Being aware of the dangers gives you the upper hand in creating the optimal defense that will allow you to securely enjoy all the benefits of smart home technology. **Start by considering the following tips:**

1. Recognize that small vulnerabilities can spark drastic consequences
2. Secure your home network
3. Be educated, aware and diligent
4. Protect every device
5. Understand the threats that are out there
6. Buy from reputable sources and follow all vendor recommendations
7. Be aware that hackers wear a variety of hats
8. Remain vigilant

Recognize that small vulnerabilities can spark drastic consequences.

A hacker's ability to compromise a home network is easier than you may think. Keep in mind that anything connected to the Internet can potentially be hacked, including smart TVs, home hubs/intelligent virtual assistants (IVAs), and even medical devices. Unfortunately, wireless signals don't honor boundaries; just open your phone or laptop and take a quick peek at the Wi-Fi and Bluetooth connections that pop up — they may belong to you, your neighbor or the church down the block. By the same token, your smart TV, tablet or laptop could be visible to anyone on the Internet — whether they are in your front yard or across the globe.

Every device that connects to the Internet is a potential gateway into your privacy, data and even your actual home. Imagine the ramifications if an intruder hacked one smart home device and was able to obtain all of your Wi-Fi credentials. The cybercriminal could listen in and learn when you'll be away, using that information to determine the best time to burglarize your home. Even more dangerous? The possibility that they could remotely unlock a door or alter a keypad PIN code to restrict entry. These are just a few of the possible outcomes when a hacker gains entry to an unprotected smart home.

Secure your home network.

It is imperative to change the factory settings on every device and always use strong credentials for Wi-Fi.

Safeguarding your smart home begins by ensuring that your Wi-Fi router is protected; if a hacker can access your network, they can essentially reach any connected device inside your home. In many cases, attackers can readily identify, connect to and gain access to devices via default credentials. Because of this, it is imperative to change the factory settings on every device and always use strong credentials for Wi-Fi. Most routers provide an array of features that you probably will never use; be sure to disable all services you don't need to thwart unsolicited incoming traffic. Investing in an additional firewall to place in front of your home router for extra protection will further bolster security. In addition, carefully read each device's manual around security. It is extremely important to be cautious when clicking on suspicious links or navigating unfamiliar web sites.

Be educated, aware and diligent.

Many cyber threats can be eliminated by following some simple steps. For every smart home device, know what you have, know how it is connected and configured, and know the current firmware/software version. Be sure to sign up for notifications and updates with each device manufacturer and follow all vendor recommendations. It is also essential to verify that software updates are being performed on schedule; some may do this automatically while others will require manual intervention. One way to ensure that you always have the latest version is to opt in to the manufacturer's push updates when you register a device. A push notification is a message that pops up on a mobile device to alert users to important information, such as a software upgrade.

Smart home security checklist

- Secure your network fully and make sure you have a firewall
- Rename and reboot your router regularly
- Change factory default configurations
- Change your passwords regularly
- Disable any services/features that are not needed
- Secure Wi-Fi using the strongest available encryption (WPA3)
- Set up two-factor authentication
- Know the software version you are on and update/patch regularly
- Maintain an inventory of connected devices and their current firmware/ software version
- Never manage your smart devices from public Wi-Fi networks
- Set up a guest Wi-Fi network
- Use biometric authentication where available
- Be wary of suspicious links and sites, and remain alert to possible scams or phishing attacks
- Ensure endpoint protection solutions for PCs and laptops

3

Protect every device.

While proper security measures should be established for every device that connects to the Internet, there are certain devices that offer heightened appeal to hackers. The most frequently accessed device is the wireless security camera, followed by home assistants, smart door locks, smart TVs and smart phones. On any given day, we use our phones to complete tasks including accessing financial accounts, checking work emails, and communicating with family and friends — making it surprisingly easy for cybercriminals to snatch personal data from your device. Phones can be compromised in several manners, including through a public Wi-Fi network, by implanting a bug, by leveraging a flaw in the operating system, or by infecting your device with malware through a web or email link.

If you're wondering how harmful it could possibly be if a hacker were to infiltrate your smart TV and flip between channels consider this: once the TV has connected to your computer, it has access to all of the data and credentials housed there — think tax returns, passwords and other personal data. Similarly, voice-controlled assistants and smart speakers, which are always listening, can provide hackers with a wealth of information about you — not to mention your credit cards, if you've ever connected accounts for services such as food delivery or shopping lists.

Think your garage is safe? Pump the brakes on that theory. Connected cars — essentially computers-on-wheels with their backup cameras, video screens, GPS systems and Wi-Fi networks — represent yet another access point for an attacker. Cybercriminals can take control of your vehicle by physically implanting a tiny device that grants access through a phone. Hacks can range from simple annoyance (for example, cranking the radio up) to downright dangerous (such as stalling the transmission, steering into oncoming traffic or disabling the brakes). Intruders can hack into telematics systems, so it is important to keep the software up to date.

Understand the threats that are out there.

Safeguarding against ransomware strikes has never been more critical. In 2020 alone, the prevalence of attacks in the U.S. skyrocketed by 109%, according to the 2020 SonicWall Cyber Threat Report.

At one time or another, we've all stumbled upon a network that isn't our own. As a smart home owner, you need to not only protect your network against innocent (or curious) neighbors, but also malicious attackers.

Some of the most common forms of cyberattacks include:

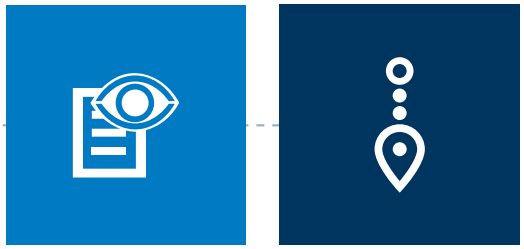
Device hijacking — These attacks, in which a criminal assumes control of a device, are difficult to detect because the intruder doesn't change the device's functionality. Yet by accessing a single device, an attacker can potentially infect all smart devices in the home, wreaking havoc on any other system.

Data and identity theft — In this scenario, a cybercriminal accesses personal information generated by unprotected wearables and smart appliances then exploits it for fraudulent transactions and identify theft.

Man-in-the-middle — In this type of breech, an attacker interrupts or spoofs communications between two systems; for example, generating fake temperature data from an environmental monitoring device or disabling an HVAC system during a heat wave. Reading sensitive data such as passwords is also very common.

Distributed Denial of Service (DDoS) — This type of attack attempts to render a machine or network resource unavailable by temporarily or indefinitely disrupting services of a host connected to the Internet. Experts reveal that DDoS attacks are rising rapidly, primarily due to the lack of security in IoT devices.

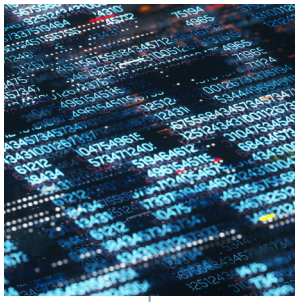
Permanent Denial of Service (PDoS) — Also known as phlashing, these attacks damage a device so severely that it requires replacement or reinstallation of hardware. Among the consequences of a PDoS attack are exploiting hard-coded passwords in IoT devices or faking data sent to devices.



Buy from reputable sources and follow all vendor recommendations.

When selecting smart home products, do your homework and research offerings from trusted sources. Begin by verifying that the manufacturer has an established process to actively identify, evaluate and address vulnerabilities, including providing all necessary patches and updates. It is also wise to purchase products from an organization whose devices are validated by a third party for all applicable industry standards, such as IEC and UL.

In addition, try searching online for "how to exploit a vulnerability" in devices you are considering. Many times, this can provide valuable feedback on known threats. Homeowners can also search for established vulnerabilities within the National Institute for Standards and Technology's (NIST) national vulnerability database, as well as the U.S. Cybersecurity Infrastructure and Security Agency (CISA).



6

Be aware that hackers wear a variety of hats.

For many people, the term "hacker" conjures up an image from a big screen spy caper of a shifty foreign agent attempting to steal state secrets. While many people assume that hacking only happens in the movies, or don't believe they have any information that hackers would desire, nothing could be farther from the truth. In fact, cybercriminals often rely on automated software that specifically looks for systems that haven't been kept up-to-date, making them more vulnerable to cybersecurity "bugs." Once the vulnerable, unpatched system is identified, the software automatically exploits the weak link — enabling hackers to wreak havoc in a variety of manners, such as using it as part of a larger DDoS attack, stealing sensitive information or taking take control of the device.

Today's cyber landscape features a wide variety of potential disruptors, including:

- Cybercriminals looking to steal personal and financial data or maliciously use devices as part of a larger campaign
- Tech-savvy teens trying to impress peers or simply cause mischief
- Hobbyists looking to hack a device just because they can
- Ransomware criminals who encrypt an organization's critical systems or files and hold them hostage for payment
- Hacktivists, who steal data from government web sites and networks to use for personal, political or social gain
- Whistleblowers working inside an organization to expose confidential information or illegal activities

Remain vigilant.

"Things that were once the plot for a science fiction movie, such as household appliances being hacked and turned against humanity, now became a reality. IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems and way of life."

— Daniel Markuson, digital privacy expert at NordVPN

As you continue to enjoy your smart home and incorporate new devices, keep in mind that cybersecurity is an ongoing process. Because vulnerabilities are constantly being discovered in products — and as hackers become increasingly resourceful — effectively safeguarding your smart devices will remain a moving target.

Don't let your guard down; be sure to routinely follow the recommended tips outlined in the Smart Home Security Checklist in Section 3.

Assessing the biggest smart home threats, room-by-room

Garage

- Smart car
- Smart floodlights
- Smart garage door controller

Family room

- Smart TV
- Smart lights
- Smart speaker
- Smart thermostat or HVAC control
- Smart plugs
- Smart vacuum
- Streaming devices

Home office

- Computer or laptop
- Modem and router
- Smart printer, including all-in-one copiers and scanners

Bedroom

- Smart TV
- Smart alarm clock
- Cellphones connected to Wi-Fi
- Smart watch, fitness tracker or sleep monitor
- E-reader or tablet
- Video chat display
- Smart oil diffuser

Kid/baby room

- Smart toys
- Kids' tablets
- Smart baby monitor
- Smart soother

Entryway

- Smart doorbell
- Wi-Fi security system
- Smart locks

Kitchen

- Smart refrigerator
- Smart oven
- Smart coffee maker
- Smart slow cooker or Instant Pot™
- Smart hub

About Eaton

Eaton's electrical business is a global leader with deep regional application expertise in power distribution and circuit protection; power quality, backup power and energy storage; control and automation; life safety and security; structural solutions; and harsh and hazardous environment solutions. Through end-to-end services, channel and an integrated digital platform & insights Eaton is powering what matters across industries and around the world, helping customers solve their most critical electrical power management challenges. Eaton's mission is to improve the quality of life and the environment through the use of power management technologies and services. We provide sustainable solutions that help our customers effectively manage electrical, hydraulic, and mechanical power – more safely, more efficiently, and more reliably. For more information, visit Eaton.com

Everything as a Grid is our approach to helping partners across the world embrace energy transition, on their terms. Today, energy flows through the grid in more directions and through more devices than ever before. And although that decentralization creates more complexities and challenges, it also creates new potential. By viewing Everything as a Grid, we're simplifying those complexities, meeting those challenges and reinventing the ways power is distributed, stored, and consumed. The future is one of low-carbon, renewable power. The future is Everything as a Grid.

EVERYTHING
AS A GRID

Visit our website:
Eaton.com/MyHome

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

BR083057EN/wB
August 2021

Follow us on social media to get the latest product and support information.

Powering Business Worldwide