By Rebecca Edwards
Researcher & Writer

Published on September 02, 2020

You have a security system to protect your home, but you also need to protect your system from hackers. We tell you what to watch out for and what you can do to improve security.

---

## All about home security and hackers



---

## Can my security system be hacked?

The short answer is yes.

But that doesn't mean it's a foregone conclusion. While any connected device or system is potentially vulnerable to hacking, there's a lot you can do to keep bad actors out.

### What makes my security system vulnerable?

Your home security system's wireless connections can potentially be interrupted or intercepted—giving access to hackers and thieves.

Wireless home security systems use Bluetooth or Wi-Fi to connect the system to components like motion sensors or door sensors.

Those signals are how sensors can talk to each other and the base station. Wireless communication is what triggers an alarm if a door or window is opened.

When an alarm is triggered, the Wi-Fi or cellular signal is routed to the monitoring center to alert the security pros that something is amiss.

### How easy is it to hack into my security system?

The good news is that even though hacking is possible, it's not necessarily probable. You need an almost perfect storm of circumstances to hack into most security systems.

**You need to be a target**

Most burglars are looking for the easiest score. They want to get in and out as quickly as possible. Alarm systems generally make that harder.

Wireless security systems require a direct, targeted attack. Taking down your system wirelessly involves a lot of more time, effort, and know-how than kicking in the door or picking a lock.

**They need to know the tech specs of your setup**

This is that know-how we were talking about. To hack into your specific security system, the intruder needs to know enough about your tech and its default security settings to choose the right approach.

There are ways to jam a security system signal and interrupt the communication between your sensors. Hackers can also set a false alarm to make you disarm your system, which gives them a window to sneak in.

But depending on the type of signal your security system uses (and built-in measures like encryption), it's not a one-size-fits-all kind of job. The hacker needs to know exactly what type of equipment will get the job done to defeat your unique setup.

On top of that, the hacker may also need to access your home Wi-Fi network, which takes a whole different set of knowledge and tools.

**They need to keep jamming your signal**

Getting into your system's communication signal is just the first step. They still need to overcome the physical security of your home—like a locked front door or window.

When the burglar breaks the window or picks the lock, your security system sensors will detect it and start sending out new signals to alert you and the monitoring center to the breach.

Plus, many security systems include anti-jamming protocols to keep thieves and hackers out.

This means that if someone does crack the proverbial code, your security system will most likely detect it and initiate steps to kick them out and sound the alarm.

The burglar would need to keep jamming the signal repeatedly as they make their way into the house to plunder your valuables.

**The latest security breach news**

We have a new column to keep you up-to-date on security breaches and what companies are doing about them. Bookmark this page to make sure you don't miss out on crucial info that could protect your security system, computer, or identity.

# How do I protect my home security system against hackers?

Even though hacking a security system to break into a house takes a lot of effort, it can definitely happen.

Your best defense is upping the security of your security system (it's not as mind-melting as it sounds). Here are the best ways to protect yourself against wireless home security system vulnerabilities.

## Do your research

Starting out with the right security system can save you a lot of trouble and worry. Go with a reputable brand that has transparent security defenses against hackers and signal jamming.

Make sure to read customer and expert reviews and search for news coverage of breaches or hacking issues.

## Protect your network

Securing your network is a first line of defense to protect all the devices that are connected to it. Rename your routers and network when you set up the system, use strong passwords (and update them regularly), and activate the firewalls that come with your router.

If you want to take it further, add multiple firewalls to make it even harder for bad actors to breach your network.

## Hide your network

It's hard to hack a system or network that can't be found. Set your wireless router to make your security system network invisible.

When you log into your router's settings, look for any option to hide the network name or hide the SSID (service set identifier), which is the technical identifier of your network.

## Use encryption

You should be able to enact encryption that's built into your Wi-Fi router. Look for the WPA2 setting and set the encryption type to AES.

And check with your security system company to make sure that all of its signals use end-to-end encryption so your transmissions can never be intercepted.

## Use two-factor authentication

Two-factor authentication for log-ins is always a good idea. Use it to log into everything including your home network, security system, and smart device apps.

**Did you know?**
Two-factor authentication requires a unique code (that's generated in real-time) in addition to entering the correct credentials. This means that a hacker may be able to guess your password, but they won't get the text or email with the special code. This is also a good way to get a heads-up when something fishy is going on.

### Update everything

Updates (to firmware, apps, software, etc.) are a pain. But not as painful as getting hacked. Update whenever you're prompted.

And set a reminder to check for updates on all devices and apps once a month or per quarter—do it along with checking the batteries in your smoke detector.

### Keep an eye on your camera footage

This can literally let you see if a stranger has accessed your network or security system. Most home security camera logs include the IP address of anyone who's accessed your camera. If you see something suspicious, change all of your passwords and report it.

## Can an ADT security system be hacked?

Other than the usual vulnerabilities of all wireless security systems, ADT doesn't have any alarming hacking risks.

There have been hacking reports about some ADT cameras with DVRs, but the attacks were limited to a certain model of DVR. Your safest bet is to go with ADT Pulse cameras, as they have stronger built-in resistance to hacking.

ADT's closest thing to a breach is a class action lawsuit that was filed in 2014. The suit alleged the company failed to encrypt and "otherwise secure" its wireless signal.

ADT settled the lawsuit with a $16 million payout to customers who had security systems that showed the hacking weakness. The primary basis of the suit and subsequent settlement was the failure to properly encrypt signals from contact sensors.

Read our full ADT review.

## Is SimpliSafe easily hacked?

In 2019, SimpliSafe nabbed headlines when a YouTube video popped up showing how a burglar could jam the security system's signal. The jam blocked the system's ability to send out an alert that something had been opened or tampered with.

A slew of coverage followed where both experts and amateurs tried to replicate the jamming results. Ultimately, it was possible to jam the system, but testers found flaws and roadblocks that don't make this an easy way to break-in.

Yes, the SimpliSafe signal was jammed with a device that cost just a few dollars. But some who copied the tactic—and the company itself—dismissed the technique as too complicated for a run-of-the-mill thief.

"In real life this is unlikely," SimpliSafe said in a statement to *The Verge*. ". . . In order for a real bad actor to effectively interfere with the system in this way they would likely have to already be inside the home and have had ample practice."

In August 2019, SimpliSafe revealed its plans to address the hacking concerns:

- Calibrating its algorithms to better differentiate between a deliberate attack and random interference.
- Offering Interactive Monitoring plan customers the option to have SimpliSafe investigate suspicious interference with your cameras.

Read our full SimpliSafe review.

## Can Ring be hacked?

Ring has been in the news consistently over claims that its security cameras can be (and have been) hacked.

The same vulnerabilities haven't been noted with the company's Ring Alarm home security system.

When it comes to Ring security and video doorbell cameras, the primary issue seems to be with back-end security. Users don't have a way to see how many people are logged in to the system, and there seems to be nothing in place to block unknown IP addresses.

In addition, *Motherboard* found that Ring doesn't check user credentials against passwords that are known to have been compromised.

Ring's initial response was to remind customers of best practices for cybersecurity. No immediate moves were made by the Amazon-owned security company to improve its practices and technology to better thwart hackers.

Read our full Ring review.