switchful
a helpful brand

Home Security > Home Security Resources > Current Page

How secure is my home security data?

Researched by
Tony Carrick | Contributing Writer

Reviewed by
Eric Paulsen | Content Manager

Updated **3/27/23**

We're committed to transparency. We may earn money when you follow our recommendations, but compensation doesn't affect our ratings. Learn more.

Table of contents

While that home security system you invested in may be doing a great job of keeping burglars at bay, it could be opening the door to hackers. Without the proper digital security precautions, cybercriminals can steal your security system password, giving them access to personal account information and even live camera footage of your family.

Fortunately, you don't need to be a tech whiz to thwart their efforts. By taking the simple measures described below you can ensure your security system is safe from hackers.

What happens when hackers gain access

In a cruel twist of irony, there are many instances of hackers using a home's internet connection and the very devices designed to make it more secure as a means to infiltrate it.

There's the case of the California family who suddenly found themselves in the middle of a *War of the Worlds*-like apocalyptic hoax when their hacked Google Nest surveillance camera began transmitting a warning of an imminent nuclear attack from North Korea. (1) Then there's the eight-year-old from Mississippi who was terrorized by a hacker who gained access to the Ring camera that was installed to protect her. (2) Even professionally installed systems aren't safe. An ADT technician was recently sentenced to four years in prison for giving himself access to the live video feeds of his female customers. (3)

Though such cases are rare, they are terrifying enough that anyone who owns or is considering investing in a home security system should stand up and take notice.

How hackers get into your security system

Security companies are constantly implementing new technologies and policies to prevent the above horror stories from happening, making such security breaches few and far between. But the fact remains that, regardless of whether your security system is **self-monitored** or professionally monitored, there is the potential for a hacker to gain access to sensitive account information and live and recorded footage from security cameras. And, once a hacker has hacked into one device, they can use that access to take over other devices connected to the same network, allowing them to steal more sensitive data.

As such, it's crucial to take the necessary steps to improve your data security to ensure the above nightmare scenarios don't happen to you. To do that, you first need to understand how hackers infiltrate home security systems.

- **Credential stuffing:** One of the most common ways hackers infiltrate your security system is through information they've stolen from data breaches at credit bureaus, banks, retail stores, utilities, and a host of other businesses that offer online account access to their customers. Once they take the username and password from these institutions, they attempt to reuse them to gain access to other accounts you have, including your security system. Since most people make the mistake of reusing their usernames and passwords to avoid forgetting them, this strategy works more often than it should. Once they have your username and password, no amount of encryption will stop them.
- **Outdated firmware:** Reputable security companies are constantly working to thwart hackers by upgrading their firmware to close security loopholes that can create access points for hackers. Customers who forget to keep their firmware up to date leave themselves vulnerable to attack.
- **Weak home network security:** Your security system uses Wi-Fi and Bluetooth signals to transfer data between its components and to grant remote access to the system. Home Wi-Fi networks with weak passwords, or worse, those that still have the default username and password, can allow would-be hackers to gain access to the home network. Aging equipment may also make your network vulnerable. If you're using a router that's more than five years old, its security options are likely obsolete. Once a hacker gains access to your home network, they can eavesdrop on your online activity and steal passwords to your online accounts, including the login credentials for your security system.
- **Weak encryption:** A good security system should encrypt data. Encryption converts data into unreadable code that can only be deciphered by an authorized user with an encryption key. Security systems that lack high-level encryption allow hackers to lift username and password data from the system relatively easily. When shopping for a security system, look for those that use the Advanced Encryption Standard (AES), which is the only encryption technology available to the public that is approved by the National Security Agency (NSA) for the transmission of Top Secret information. (4) Most reputable security systems, including ADT, SimpliSafe, Ring, and Vivint, use AES.

- **Local hack:** This type of hack requires the hacker to be within range of the camera's or window sensor signals, meaning they would need to be sitting outside in close proximity to your home. Systems with cameras that lack encryption and rely on wireless network security to prevent access are vulnerable to this type of attack. However, given that this involves a hacker that is specifically targeting your home, this type of hack is very unlikely.

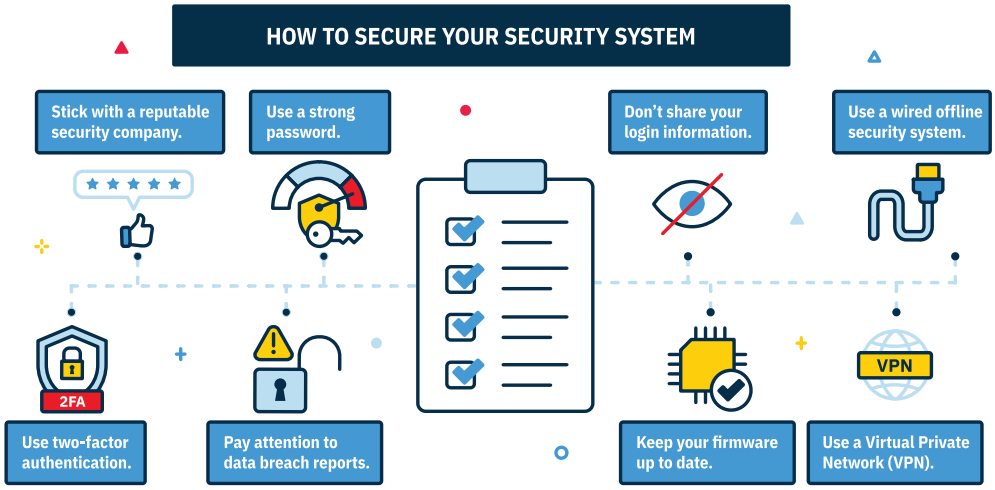
How to spot a security breach

Identifying if your security system has been hacked can be very difficult, but there are certain telltale signs you can look out for that go beyond that funny feeling that you're being watched.

- **Login credentials suddenly change:** If you attempt to log in to your security system and your username and password suddenly don't work anymore, that's a clear sign that your system has been hacked. Call your security system customer support line immediately to see if the password was recently changed.
- **Weird camera activity:** Pay attention to the LED light that comes on when a security camera is operating. If the camera is filming when it shouldn't be, then someone else may be controlling it. Also, if you have a 360-degree camera that begins panning on its own, and it's not set to follow motion automatically, it may be hacked.
- **Poor network performance:** Home security system surveillance cameras use a lot of data when they're running. That data usage, coupled with the fact that hackers typically take control of a big chunk of your Wi-Fi network's bandwidth, will likely cause your network to slow to a crawl. A slow network and spike in data usage can be indications that your network has been hacked.

Securing your security system

Whether you're using a professionally installed and monitored security system or one you install and monitor yourself, there is always the potential for someone to hack into it. And, while the horror stories of hackers taking control of security cameras may be enough to discourage some from investing in a security system at all, most of these breaches are preventable simply by taking a few precautionary measures.



- **Use two-factor authentication.** Many security companies encourage or even require their customers to set up two-factor authentication in order to access their security system. The most common two-factor authentication requires you to enter your password and then enter a one-time passcode sent to your mobile device to gain access to your account. Thus, even if a hacker has purloined your login credentials, they won't be able to access your account without your mobile device. Two-factor authentication may seem tedious when you're trying to access your account. But, like those long lines at the TSA checkpoint at the airport, the added level of security is worth the inconvenience.
- **Pay attention to data breach reports.** When a company suffers a data breach, they'll immediately notify the press and their customers (assuming they're a reputable company) to let them know their login information has been compromised. When a bank, online retailer, or other company that you do business with online reports such an attack, you should respond by immediately changing the username and password for that account and any accounts that use the same login credentials.
- **Stick with a reputable security company.** In the wake of the highly publicized internal ADT security breach, most security companies (including ADT) now maintain strict guidelines for their technicians and professional installers that prevent them from ever having access to live video feeds or recorded video. A reputable security company should allow only the primary account holder to add or remove authorized users.
- **Use a strong password.** Let's face it. Most of us reuse the same usernames and passwords in order to make our lives easier even though we know it's a bad idea. While reusing passwords may make our online lives more convenient, the practice also makes it much easier for others to hack into our accounts. Avoid reusing passwords and create a unique strong password that consists of random numbers and symbols for your security system password. Better yet, use a password manager, which will create a complex password for you and securely manage all of your passwords.
- **Keep your firmware up to date.** A security company's reputation is based entirely upon its ability to maintain your data privacy and security. As such, companies such as ADT, SimpliSafe, Ring, Vivint, and Google Nest use advanced encryption to ensure their systems cannot be hacked. All you need to do is make sure you update your apps and devices with the latest firmware. The best security systems and cameras will perform these vital updates automatically, so you don't have to keep up with them yourself.
- **Maintain a secure home network.** Since your security system ties into your home's Wi-Fi, you need to keep your home network secure by making sure your router has a secure password and definitely not the one it came with. You should also consider replacing a router that's more than five years old, which is when its security features start becoming obsolete.
- **Don't share your login information.** Limit who has access to your account information by using your home security system's shared user feature, which allows you to give others limited access to your security system without having to share the login credentials that give them administrative access.
- **Use a Virtual Private Network (VPN).** A VPN encrypts your internet connection, which prevents would-be hackers from being able to see the data you're transferring on the network, including

your security system login credentials. Just keep in mind that most reputable VPN software comes with a monthly subscription fee.

- **Use a wired offline security system.** The best way to protect your security system from hacking is by choosing a wired system that isn't connected to the internet. However, this type of system lacks the features that are must-haves for most people, including smartphone alerts when sensors are tripped, the ability to arm and disarm your security system remotely, and remote access to cameras.

Conclusion

The thought of a hacker invading the sanctity of your home may make you think twice about investing in a home security system; however, it's important to remember how rare such invasions of privacy are and how easily you can prevent them.

Since reputable security companies use high levels of encryption that are very difficult to hack, the most common way for hackers to access your security system data is by stealing login credentials or accessing a home network that has weak security. By implementing the above measures to beef up the security for both, you can make it much harder for unauthorized users to gain access to your security system data and cameras.

The people behind our research

We believe the best information comes from first-hand customer experience and methodical research by subject-matter experts. We never source information from "content farms," and we don't generate content using artificial intelligence (AI). You can trust that our recommendations are fact-checked meticulously and sourced appropriately by authentic, industry-recognized people.

Contributing researcher

Researched by

Tony Carrick | Contributing Writer

Tony Carrick is a full-time freelance writer who has contributed to a variety of publications, including Bob Vila, U.S. News and World Report, Field & Stream, Angi, Futurism, and Popular Science. Tony, who received a Bachelor of Arts in journalism from Elon University and Masters of Arts in English literature from Salisbury University, began his career as a reporter for local newspapers in North

See full bio

Contributing reviewer

Reviewed by

Eric Paulsen | Content Manager

Eric Paulsen is a writer, editor, and strategist who has been creating content in the B2B, healthcare, FinTech, home security, and government sectors for more than five years. He holds an MFA in creative writing and lets everyone in his life hang that over his head. When he doesn't have his hands deep in

See full bio

Endnotes and sources

1.
"'5 minutes of sheer terror': Hackers infiltrate East Bay family's Nest surveillance camera, send warning of incoming North Korea missile attack."
The Mercury News. Accessed 26 September 2022.

2.
"She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter."
The Washington Post. Accessed 27 September 2022.

3.
"Former ADT Technician Sentenced To 4+ Years In Prison For Hacking Home Security Cams In North Texas,"
CBS News. Accessed 26 September 2022.

4. "Cryptographic Standards and Guidelines," U.S. Commerce Department. National Institute of Standards and Technology. Accessed 29 September 2022.

switchful
a helpful brand

Editor's choice

Best internet providers

Cheapest internet providers

Fastest internet providers

Best satellite internet

Best TV providers

Cheapest TV providers

Best internet for gaming

Best rural internet

Best home security systems

Best DIY home security systems

Guides

Guide to internet speed

Guide to cutting the cord

How to save on your internet bill

How to get free TV

How to save money on home security

How to choose a home security system

Helpful resources

All internet providers

All internet resources

Internet near me

All TV providers

All TV resources

All home security providers

All home security resources

About

About us

How we rank providers

How we make money

Our editorial team

Contact us

Privacy Policy Terms & Conditions