How to secure your home surveillance cameras from getting hacked

16 December 2019, by Dalvin Brown, Usa Today

Credit: CC0 Public Domain

Hackers are breaking into home security cameras, and the process isn't always as difficult as you may think.

This week, there were reports of hackers gaining access to Ring security cameras in Tennessee, Mississippi, Florida and Texas. And cybersecurity experts say incidents like these aren't very complex to execute because people often use passwords that are easily guessed.

"The easiest way for a hacker to gain access to something is to guess the username and password of the device's administrative account," said Brian Vecci, chief technology officer at the data protection company Varonis. "That's the most common way to get hacked."

He said bad actors are trolling through the internet, reading about devices that are exposed and keying in default usernames and simple passwords to see if they can gain access to real accounts.

If it works, and you're the unsuspecting subject, they can watch you and your family during your most intimate moments. Hacker can, and have, also talk through the camera's speaker, startling kids and harassing parents.

Home security cameras are also getting broken into because, like everything else that connects to the internet, they are inherently open to outside forces.

In order to monitor what's happening in your home remotely, security cameras have to be connected to the internet, Vecci said. And the moment you connect a device to the internet "hypothetically someone can get access to it."

What's even scarier is once a camera is compromised, hackers can make "lateral movements" onto other connected devices in your home.

So they could, in theory, disable your alarm system, unlock your front door if you have a smart lock, torment your household by blasting music and more, said Renaud Deraison, co-founder of the cybersecurity company Tenable.

"They can decrease your quality of life by hacking the tech that is supposed to improve your quality of life," Deraison said.

Still, there are things you can do to help decrease the likelihood that someone will gain access to your home's security camera. Here's what you should do:

1. Go with a big-name vendor

When choosing a specific brand, choose a familiar company that treats security more responsibility. Large manufacturers with household names are held to higher scrutiny than a "no-name company," Deraison said. Nest, Samsung, Panasonic, Ring and Arlo are popular choices.

2. Upgrade to a cloud-based system

Store your footage in a cloud. Tech companies that offer cloud-based storage systems can install software updates to patch vulnerabilities soon after they're discovered, Deriason said.

Earlier this week, Tenable researchers said they discovered "seven severe vulnerabilities" in Amazon's Blink XT2 camera systems. Amazon patched the problem with a firmware update.

3. Create complex passwords

"Don't use a default user name and password" that comes with your device, Vecci said. "Change your passwords to something long and difficult to break. Don't use last names, birthdays or addresses." Experts recommend a combination of upper and lower case letters, numbers and symbols.

4. Use two-factor authentication

Two-factor is favored by security pros because you have to log in twice to get into your account. Hackers will try you once, and if not successful, move on to other prey. If you've ever had a six-digit verification code sent to your smartphone in order to log in to an online account, you're familiar with two-factor authentication. It basically sends you a notification when someone new tries to log on to your network. And they can't get in without access to your phone or email address.

5. Update your devices regularly

Surveillance camera vendors often expect users to update the devices manually, experts said. So every few months, you should check to see if yours has an available update. Set up manual security updates, if that's an option.

"If you don't update your device, you end up with old software that's not undergoing rigorous testing," Deraison said. "All of it together, you have a recipe for something that's fairly insecure. You're risking a personal leak that could be devastating."

hacked.html