How to recognize when your camera is hacked and how to prevent it

Currently, cameras are quite popular devices chosen by many families to ensure security. However, this device is also the target of many hackers. Below are ways to help you recognize if your camera has been hacked and how to prevent it.

How to recognize when your camera has been attacked by hackers

Strange noise coming from the camera

If your camera makes strange sounds or noises, check your device. Because that can be one of the signs that hackers or cybercriminals are watching and recording all your activities and that noise is the sound they carelessly let into the camera through the 2-way voice feature. .

The shooting angle is changed

If you discover that your camera automatically rotates to different locations in the house or changes to a different angle even though you have not set it up, it is likely that your home camera is being controlled by hackers to collect information. inside your house.

The LED light on the camera flashes

If you see the LED light on the camera blinking continuously, it's likely that hackers are trying to access your home camera. Please restart the camera to check. If you still see the LED light on the camera flashing, it proves that your camera is being hacked.

Camera settings are changed

Check the security settings on your camera. Your camera is being hacked if it sees an alarm mode or some other parameters have been changed.

The camera turns on automatically after turning off

One of the things that can confirm that your security system has been hacked is when one of the cameras turns itself back on even though you have turned off the camera system.

Cannot access the camera

You are logged out of your camera account on the software and cannot access it even if you have entered the correct password. This is because the hacker changed the camera password so you cannot access the system.

Simple ways to protect your home security cameras and avoid being hacked

1. Enable two-step authentication if the camera supports it

If your security camera supports two-step authentication, enable it now. This will make it difficult for hackers to carry out the attack, because it requires both a password and a confirmation code sent to the homeowner's mobile phone.

2. Do not install security cameras in sensitive areas

Do not install security cameras in private, sensitive areas such as bedrooms, bathrooms.

3. Choose a location to install the security camera that is difficult to reach

One of the ways for bad guys to carry out an attack is to remove security cameras outside your home, then use them to access the network and the clips are recorded. Therefore, choose a location to install the security camera so that bad guys cannot access it and remember to attach it tightly.

4. Do not share any clips on social networks

Many users often share clips recorded from security cameras on social networks without knowing that this action also poses risks.

5. Regularly delete old videos from security cameras

Delete old videos recorded by security cameras to prevent being hacked, then bad guys will have access to less information about you and your family.

6. Change your password regularly

You should set strong passwords, avoid passwords related to family members' names and dates of birth, and change passwords regularly.

7. Regularly update the latest software

When manufacturers release regular software updates for security cameras, update them immediately because they often contain security patches.

You finished reading the article "**How to recognize when your camera is hacked and how to prevent it**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.