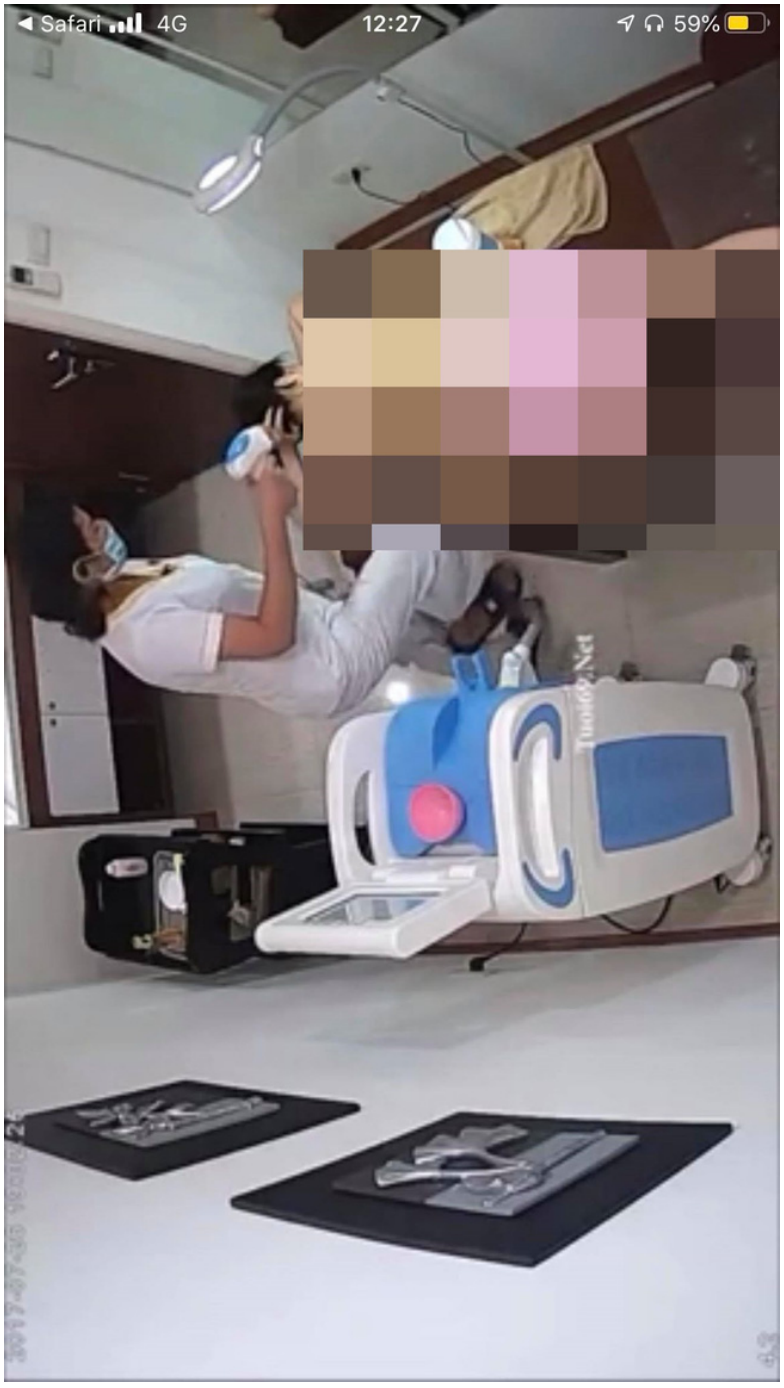
5 signs that your home security camera is being hacked along with 3 precautions from security experts

The rumor about singer Van Mai Huong revealing private photos from security cameras is making the online community worried. So what to do to prevent security means from becoming a privacy invasion tool?

Today, the online community in Vietnam suddenly stirred up with information that the **girl who looked like the singer Van Mai Huong was hit with a sensitive video from a security camera** . In particular, according to the date saved in the video, they were recorded from October 2015.

In it, this girl has just returned home, dressed carefree without knowing that her sensitive images were recorded by the camera.

Or like the pictures and **videos sneaking from security cameras** in spas - where women naturally take off their clothes to be cared for - are also taken by bad guys and spread on chat groups and social networks. Assembly or any platform that can send data.



Security cameras, as the name implies - are used primarily for security control, capturing images in places that are hard to keep an eye on. However, because of subjectivity, ignorance or intentional interference by bad guys, this means will likely turn out to be "anti-hostile".

Sensitive images and videos can be used to extort money, defame honor, or many other dirty tricks that God knows not. The consequences of these tricks are terrible.

So how do families enhance security for security camera systems, avoiding bad guys?

Whether your home security camera has been hacked and 5 ways to identify and prevent to reveal private photos

We contacted Mr. Phan Anh Vu, a long-time technology expert to find out what security camera users have ways to protect themselves.

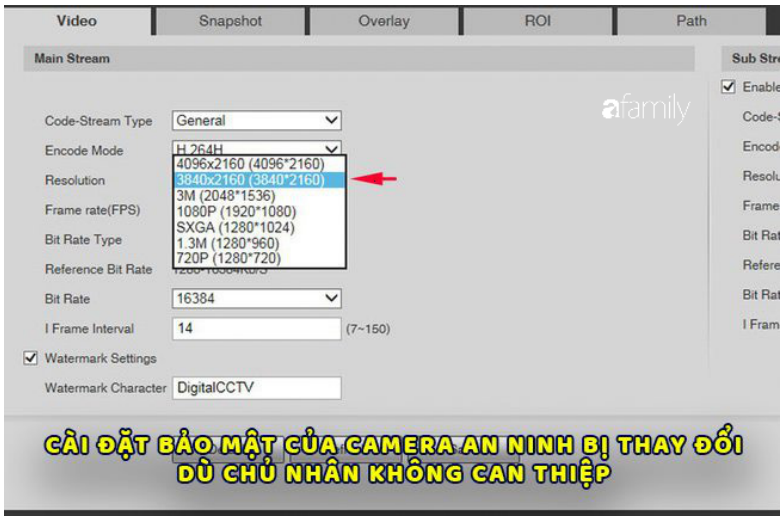
According to Vu, here are 5 ways to identify if your home camera has been hacked or not?

1. Security camera makes strange sound

It can be difficult to say or detect whether a CCTV has been hacked. One of the signs that a CCTV camera has been compromised or attacked is when there is a strange voice or abnormal noise.

This means that the hacker gained control of the CCTV and operated it.

2. The security camera's privacy settings are changed even if the owner does not interfere



Another indication that your CCTV has been hacked is when its security settings have been changed or the password has been set to the default.

3. The LED of the CCTV lights up abnormally, the camera is turned to another direction

An unnaturally blinking LED natural light is an indication that your security camera has been compromised. Besides, the camera often rotates to another direction with the initial setting is also a sign not to be missed.

4. Camera turns itself on after being turned off

If you find that the security camera's LED is on even when you are not using it, it is being controlled by someone else.

5. Spike in network traffic

One way to determine if your surveillance system has been compromised is to check the data traffic on your network and on your CCTV.

If there is a sudden increase in network traffic, it is possible that the system has been hacked to send video out.

5 user mistakes lead to compromised security camera

Mistake 1: Installing security cameras in sensitive locations

According to Vu, the security camera is a double-edged sword if installed in the wrong place. In the world, except for the security camera in the bedroom to look after babies, security companies never encourage users to install them in sensitive locations such as in private rooms, WC .

There are also only fitted in the corridor, the door, the corners are difficult to observe. Therefore, the location of installing security cameras is the number one note that you must keep in mind.

Mistake 2: Using security camera with the default password

This is a fatal mistake that many families have made. In the case of using a remotely accessible security camera, leaving the default password on means that we have given privacy to the bad guys.

Therefore, the first thing to do after installing a security camera is to immediately change a password that is difficult to guess. Should add special characters, mixed capitalization. In addition, you should change your password periodically from 1 to 3 months.

In fact, with a silly password like "123456", hackers only take . 0.23 seconds to track it.

Mistake 3: Subjective, not monitoring technician repairing / installing security cameras when there is a problem

Regardless of whether you are a normal person or a celebrity, bad guys always want to get sensitive images from us.

In the case of the girl who looks like Van Mai Huong mentioned above, the sensitive series from 2015 may still be in the hard drive of the camera but has just fallen into the wrong hands. What to do when installing / repairing security cameras is to have a supervisor.

Besides, although the mechanism of the security camera memory is to overwrite the data, delete videos when it runs out of space - hackers can restore them if they have a hard drive. Therefore, it is not allowed for people you do not trust to touch the camera in the family.

We sided with Van Mai Huong.

Women must respect and protect their rights wherever they are. Distributing private and sensitive images of women, for whatever reason, is not acceptable. Let's stand with Van Mai Huong and join hands to protect women, for a more civilized society.

You finished reading the article "**5 signs that your home security camera is being hacked along with 3 precautions from security experts**" 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.