'Smart' security cameras: Using them safely in your home

How to protect 'smart' security cameras and baby monitors from cyber attack.

This guidance explains how you can set up your smart camera to protect it from common cyber attacks.

Smart cameras (the security cameras and baby monitors used to monitor activity in and around your house) usually connect to the internet using your home Wi-Fi. This means you can watch a live camera feed, receive alerts when you're out and about, and sometimes record footage.

However, as with any 'smart' device that can connect to the internet, you should take a few steps to protect yourself. This page explains how you can do this.

What is the issue with smart cameras?

Live feeds or images from smart cameras can (in rare cases) be accessed by unauthorised users, putting your privacy at risk. This is possible because smart cameras are often configured so that you can access them whilst you're away from home. The problem arises because some cameras are shipped with the **default** password set by the manufacturer, which is often well-known or guessable (such as **admin** or **00000**). Cyber criminals can use these well-known passwords (or other techniques) to access the camera remotely, and view live video or images in your home.

How do I make sure my smart camera is safe?

Taking the following steps will make it **much** harder for cyber criminals to access your smart camera.

1. If your camera comes with a default password, change it to a secure one - connecting three random words which you'll remember is a good way to do this. You can usually change it using the app you use to manage the device. When you change the password, make sure you avoid the most commonly used passwords.
2. Keep your camera secure by regularly updating it, and if available switch on the option to install software updates automatically so you don't have to think about it. Using the latest software will not only improve your security, it often adds new features. Note that the software that runs your camera is sometimes referred to as **firmware**, so look for the words **update**, **firmware** or **software** within the app.
3. If you do not need the feature that lets you remotely view camera footage via the internet, we recommend you disable it. Note that doing this may also prevent you receiving alerts when movement is detected, and could stop the camera working with smart home devices (such as Alexa, Google Home or Siri).

You'll find instructions about how to make the above changes in the manufacturer's documentation, so consult the manual (if provided) or look up your specific model in the **support** section of their website. You'll probably need to look in the **settings** or **system** area of the camera's app, or access the camera using your browser.

Note: To change the password for older cameras, you may have to type the camera's IP address into your browser (for example, **http://192.168.0.127**). You can find your camera's IP address in your router settings; look for **connected devices** or similar, and you'll find a list of all devices connected to your router.

Check your router settings

Many routers use technologies called **UPnP** and **port forwarding** to allow devices to find other devices within your network. Unfortunately, cyber criminals can exploit these technologies to potentially access devices on your network, such as smart cameras. To avoid this risk you should consider disabling **UPnP** and **port**

forwarding on your router - check your router's manual or the manufacturer's website for details about how to do this.

Note that:

- Some routers will have UPnP disabled by default; if this is the case you don't have to do anything.
- Disabling UPnP may prevent certain applications and devices from working, such as online gaming, media servers, and other smart devices. If you decide that you need these applications, you'll have to decide whether to give up some security by allowing UPnP and port forwarding.

PUBLISHED

3 March 2020

REVIEWED

3 March 2020

VERSION

1.0

WRITTEN FOR

You & your family