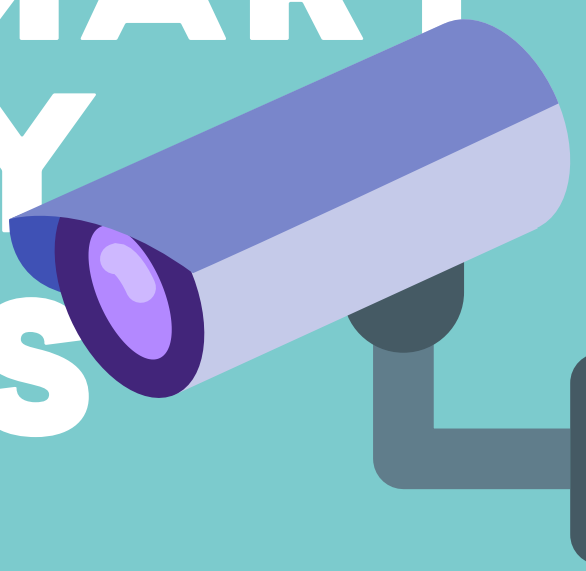
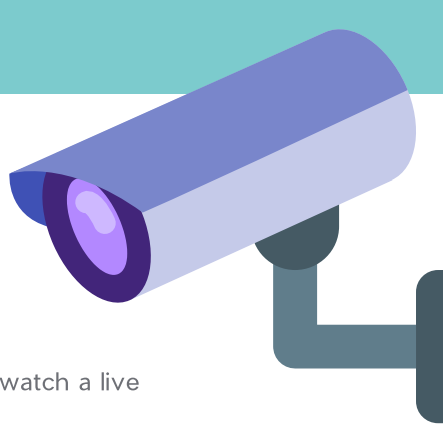
AWARE | SECURE | RESILIENT

USING SMART SECURITY CAMERAS SAFELY



Guidance to keep your smart security cameras safe from unauthorised access

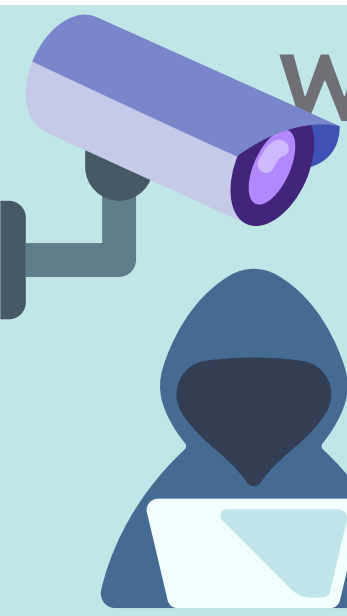
WHAT IS A SMART SECURITY CAMERA?



Smart cameras usually connect to the internet using your home Wi-Fi. This enables you to watch a live camera feed, receive alerts, and usually record footage.

However, as with any smart device that can connect to the internet, you should take a few steps to protect yourself.

WHAT IS THE ISSUE WITH SMART CAMERAS?

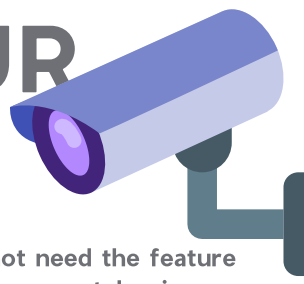


Live feeds or images from smart cameras can potentially be accessed by unauthorised users, putting our privacy at risk. This is possible because smart cameras are often configured so that you can access them whilst you're away from home.

The problem arises because some cameras are shipped with the default password set by the manufacturer, which is often predictable or well-known (e.g. 012345). Cyber-criminals can use these well-known passwords to access the camera remotely, and view live videos or images in your home.

Open and unsecured smart cameras are easy to find and connect to, using online search tools.

HOW DO YOU KEEP YOUR SMART DEVICE SAFE?



1 Change any default passwords to a secure one.

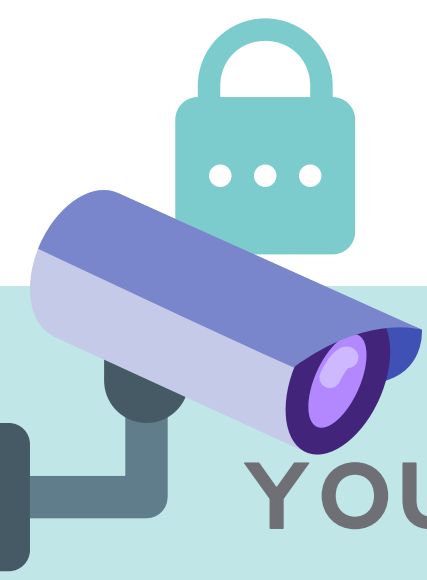
You can usually change it using the app you use to manage the device. When you change the password, make sure you avoid using common passwords.

2 Ensure your camera is regularly updated.

Set your device to automatically update if possible. Check your device settings for 'software' or 'firmware' update options.

3 If you do not need the feature that lets you remotely view camera footage via the internet, we recommend you disable it.

Keep in mind 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).



HAVE YOU CHECKED YOUR ROUTER SETTINGS?

Many routers use technologies called UPnP and port forwarding to allow devices to find other devices to connect to within your network. Cyber-criminals can exploit these technologies to potentially access devices on your home network.

Consider disabling UPnP and port forwarding on your router – some routers may already have these disabled by default.

Note: Disabling UPnP may prevent certain applications and devices from working, such as online gaming, media servers, and other smart devices.