Hacked webcam site is another reminder to improve security online

November 25 2014, by Gordon Fletcher

Snoopers are everywhere. Credit: adafruit, CC BY-NC-SA

The UK Information Commissioner Christopher Graham has drawn attention to a webcam-monitoring Russian website, which offers thousands of private video streams, raising fears of unwitting and continuous surveillance. Graham conceded that he has little legal power

to close such sites.

This revelation from one of the highest authorities on such matters should not come as a surprise to anyone who owns devices connected to the internet – and yet it has been treated in just this way. The rule of such devices is simple: "If it's connected, it's vulnerable."

Security is your responsibility, too

These reports raise a number of questions and concerns that all come down to a single key realisation. We are surrounded by poorly designed systems that are made worse – not better – when they are brought together in different combinations. Even worse, when systems include reliance upon the actions of people – as all do in some way – then the scope for disaster rises exponentially.

The response so far has been for calls to shut down the website, but little attention has been given to the fact that this situation can easily happen again at another domain and with other devices. The recent hacking of Apple's iCloud to gather compromising photographs of celebrities proved indirectly that smartphones are similarly at risk. The Russian website is just the publicly visible end result in a longer chain of activities. Hacking access to an IP camera can be done by anyone with access to the internet and with sufficient knowledge and patience.

The Russian site currently under scrutiny quite simply relies on using the default admin passwords for a variety of commercially available internet protocol (IP) cameras, which are sold as stand-alone units connected to the internet wirelessly. When a camera is sold out of the box it invariably has a default admin account which is combined with a default password. The instructions on that box will also direct the new owner to immediately change the admin password. But users often don't make the change and the Russian website proves that point.

Device-makers need to fix their ways

The immediate solution is clear. With the attention that the site has now received, owners of every single IP camera worldwide, whether they are currently displayed on the site or not, should change the admin password that enables access to the video stream. But even with this remedy, assuming the action was to be done completely by all of those camera owners, the result is only a superficial sticking plaster. Despite the now apparent demise of the site at the centre of the scrutiny a new version will only take another suitably determined programmer to take up The concept. The manufacturers of thousands of internet-connected devices need to design them to minimise the reliance upon people to setup minimum security protocols.

Examples of good information security can be taken from social media and online shopping websites where the potential risks are well-known and better acknowledged. For example, manufacturers could – and some now do – force the default admin passwords to be changed the first time a device is used (and to something different from the original default password). A device could also automatically monitor and alert an owner when a "foreign" computer is accessing it.

While the Internet of Things is still an exciting vision, it is important to ensure that it is also secure. This security should be available in a way that does not unnecessarily burden its users with responsibilities in the name of reducing costs. So much can be more effectively managed by software and automated processes to help protect us from privacy breaches.

Source: The Conversation